Università degli Studi di Milano
UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI DIRITTO PUBBLICO
ITALIANO E SOVRANAZIONALE

Corso di Dottorato in Diritto pubblico, internazionale ed europeo
XXXIII ciclo

TESI DI DOTTORATO

BIG DATA TRA ESIGENZE SECURITARIE E DIRITTI ALLA RISERVATEZZA E ALLA PROTEZIONE DEI DATI: QUESTIONI NORMATIVE E GIURISPRUDENZIALI IN MATERIA DI *DATA RETENTION*

Tesi presentata da:
Dott.ssa Giulia Formici
Matricola: R12029

Tutor: Prof.ssa Alessandra Lang
Coordinatore: Prof.ssa Diana-Urania Galetta

Anno Accademico 2019/2020

INDICE

PARTE II

PARTE III

INTRODUZIONE

"La sola privacy che avete è nella vostra testa. E forse neppure in quella"
Nemico Pubblico, 1998 (regia di Tony Scott)

Il presente lavoro, come sovente accade nell'ambito della ricerca accademica, nasce da una curiosità, dal desiderio di comprensione di una specifica questione e dal tentativo ambizioso ed entusiasmante di fornire alcune risposte agli interrogativi che emergono dall'attività di studio e approfondimento. Ebbene, la curiosità che ha permesso di muovere i primi passi nella complessa tematica affrontata in questa tesi è scaturita dalla lettura di un celebre testo dello studioso statunitense Daniel Solove, John Marshall Harlan Research Professor of Law alla George Washington University Law School: "*Nothing to hide: the false trade-off between privacy and security*"[1]. L'utilizzo provocatorio del termine 'trade-off', solitamente impiegato in ambito economico, ha catturato sin da subito la mia attenzione: con tale espressione infatti si usa descrivere una "relazione funzionale tra due variabili tale che la crescita di una risulta incompatibile con la crescita dell'altra. Si parla di trade-off quando si deve operare una scelta tra due opzioni ugualmente desiderabili ma tra loro contrastanti"[2]. Sin dal titolo, dunque, l'autore ha voluto mettere in luce la dibattuta ed articolata questione della convivenza tra esigenze securitarie e tutela dei diritti fondamentali alla riservatezza (privacy o vita privata) e alla protezione dei dati, intese come variabili da taluni considerate incompatibili e non contemporaneamente sussistenti, mentre da altri, tra cui Solove stesso, che antepone significativamente l'aggettivo 'false' al termine 'trade-off', ritenute conciliabili seppure con sforzi notevoli da parte di legislatori e Corti.

La lettura di quel testo, che concentra la propria analisi primariamente sul diritto e sulle vicende giurisprudenziali che hanno caratterizzato gli USA, ha fatto sorgere numerosi quanto pressanti interrogativi: in un momento così particolare e complesso della storia dell'Occidente, scosso da eventi quali i brutali attentati terroristici che hanno colpito al cuore gli Stati Uniti l'11 settembre 2001 e che continuano purtroppo a ferire anche il Vecchio Continente, è davvero possibile parlare di bilanciamento tra sicurezza e diritti fondamentali quali la riservatezza e la protezione dei dati? É corretto ritenere che questi ultimi siano, in fondo, diritti dalla dimensione prettamente individuale, che possono pertanto essere considerati 'recessivi' rispetto all'interesse generale e collettivo alla sicurezza? E ancora, l'impiego di strumenti di sorveglianza e controllo dei consociati da parte di autorità *law enforcement* o agenzie di intelligence comporta necessariamente la rinuncia ai diritti alla vita privata e alla tutela dei propri dati? Quali possono essere le conseguenze di una tale rinuncia rispetto alla democraticità delle nostre società e ai diritti che esse riconoscono e tutelano?

Proprio rispetto a quest'ultimo profilo, nel 2013 le rivelazioni di Edward Snowden, uno dei più noti *whistleblower* della storia recente, ex dipendente di un *contractor* esterno fornitore di servizi per la *US National Security Agency* (NSA), hanno acceso un dibattito vivace e profondo sui rischi di una 'società della sorveglianza' nella quale, in nome della sicurezza, ogni cittadino diviene un sospetto ed i cui dati vengono sottoposti a vagli ed analisi, più o meno invasive, da parte di pubbliche autorità. Queste avevano operato, sino alla fuga di notizie pubblicate sul quotidiano *The Guardian*, in

[1] D. SOLOVE, *Nothing to hide. The false trade-off between privacy and security*, Yale University Press, 2011.
[2] Questa la definizione fornita dall'Enciclopedia Treccani.

completa segretezza e subordinate a controlli da molti ritenuti parziali ed insufficienti: la percezione, forse per la prima volta nei tempi moderni così chiara e netta, del potere vasto e poco circoscritto posto nelle mani di agenzie di intelligence e di *law enforcement* aveva ravvivato timori e paure nella società civile, nonché incitato a maggiori e più attente riflessioni sul rapporto sicurezza-riservatezza/protezione dei dati. Del resto, tra le brevi recensioni che accompagnano il libro di Solove, due hanno rafforzato la consapevolezza della rilevanza, interesse e complessità dell'argomento e dei quesiti che nel corso della lettura affioravano: il Professor Frank Pasquale scrive della abilità dell'autore di "encapsulate the 'big picture' in surveillance law. *Nothing to Hide* is a consistently fascinating effort to assure that the modern surveillance state respects the citizens it claims to protect"; e ancora il Professor David Cole evidenzia come Solove volesse ricordare a tutti nel suo studio che il diritto alla riservatezza è da intendersi quale "essential aspect of human existence, and of a healthy liberal democracy – a right that protects the innocent, not just the guilty". Tali rapidi ed incisivi commenti richiamano l'attenzione su di un aspetto che fino a quel momento risultava poco considerato e che il primo acceso dibattito sorto a seguito delle rivelazioni di Snowden aveva messo in primo piano, con più forza ed evidenza: la connessione e le ripercussioni che quella che chiamerei una 'deriva pro-securitaria' di legislatori e Corti – ovvero la tensione ad adottare e legittimare forme di sorveglianza massiva operate mediante controllo dei dati prodotti dai cittadini – potrebbe comportare non solo rispetto ai diritti alla privacy e protezione dei dati bensì nei confronti di una garanzia fattiva e coerente dei diritti e delle libertà fondamentali che dalla tutela della vita privata dipendono e si collegano.

Se si parte da queste considerazioni, diviene dunque necessario comprendere ed analizzare se, come e quali strumenti possano essere posti in campo al fine di arginare i rischi di una 'società della sorveglianza' e quale punto di equilibrio possa essere raggiunto per scongiurare quella visione di 'trade-off', permettendo così di inserire le misure volte alla impellente e prioritaria garanzia della sicurezza entro l'alveo dello Stato di diritto e della tutela dei diritti fondamentali.

Una tale analisi e comprensione, tuttavia, non può che muovere dalla consapevolezza – e concretezza – del contesto storico che ha caratterizzato gli ultimi decenni e che ha fortemente inciso sul rapporto – o lo scontro – tra sicurezza e riservatezza/protezione dei dati. Questo binomio, infatti, non può essere studiato senza tener conto, accanto alla situazione di 'emergenza normalizzata'[3] del cronicizzarsi delle esigenze securitarie da un lato e alla maggiore conoscenza dei rischi e dei pericoli derivanti da talune forme di garanzia della sicurezza dall'altro, di un ulteriore fattore 'destabilizzante' e determinante: il rapido ed inarrestabile progresso tecnologico. L'avvento dei c.d. Big Data, della produzione quotidiana e massiva di una enorme mole di dati, dell'utilizzo ormai vitale di dispositivi elettronici e di telecomunicazione, si sono indubbiamente fatti portatori di potenzialità sconfinate e fino a poco tempo fa inimmaginabili. Tutti i settori, dalla sanità al lavoro, dall'istruzione alla comunicazione ed informazione, dal trasporto alle previsioni metereologiche, sono stati rivoluzionati dal mondo dei *bit*, dei dati e dei c.d. metadati, ovvero, come si vedrà, delle informazioni che non attengono al contenuto di telecomunicazioni ma che sono mediante le stesse prodotti, quali data e ora di una chiamata, mittente e destinatario di una mail, localizzazione al momento di una telefonata

[3] G. DE VERGOTTINI, *La 'guerra' contro un nemico indeterminato*, in *Forum di Quaderni Costituzionali*, 5 ottobre 2001. Il concetto di 'normalizzazione dell'emergenza' viene ripreso anche da A. VEDASCHI, *A' la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Giappichelli, 2007; G. M. FLICK, *Dei diritti e delle paure*, in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, ESI, 2009; T. GROPPI, *Democrazia e terrorismo*, ESI, 2009; G. DE MINICO, *Costituzione. Emergenza e terrorismo*, Jovene, 2016.

o di un accesso al Web –. Anche la garanzia della sicurezza ha potuto beneficiare di strumenti avanzati, sofisticati e all'avanguardia, utili nella lotta al crimine e alle minacce alla sicurezza dello Stato: la disponibilità di sistemi automatizzati di analisi dei dati, mediante algoritmi ed Intelligenza Artificiale, hanno concesso di svolgere attività di prevenzione nonché di implementare ed accrescere le capacità investigative, che possono ora godere di un vasto insieme di informazioni in grado di creare collegamenti tra soggetti sconosciuti alle pubbliche autorità. Le nuove – ma già reali – frontiere del riconoscimento facciale, del *predictive policing*, l'impiego di banche dati genetiche e biometriche sempre più ampie, hanno rappresentato e rappresentano un'arma – da molti ritenuta determinante – certamente decisiva per la tutela della sicurezza. Tutti questi strumenti, tuttavia, rappresentano non solo opportunità da cogliere e sfruttare ma anche un pericolo concreto e tutt'altro che futuribile per i diritti alla vita privata e alla riservatezza, in particolare e in maniera diretta. I sistemi di sorveglianza, raccolta e analisi di dati personali, biometrici o genetici, si scontrano in maniera decisa con quelle prerogative ormai ampiamente affermate nelle Carte costituzionali e nelle Carte dei diritti fondamentali riconosciute a livello internazionale e nel contesto dell'Unione europea, oltre che in innovative e precise legislazioni finalizzate a regolare l'impiego di dati e l'ingerenza nella sfera privata.

Se da un lato gli attentati terroristici e la criminalità organizzata sempre più transfrontaliera ed articolata, hanno contribuito ad una più ampia tutela della sicurezza e all'impiego di strumenti di sorveglianza più incisivi e di vasta portata, dall'altro Snowden ha disvelato i rischi e le insidie che tali stessi strumenti, soprattutto se non debitamente regolati e sottoposti a limiti e controlli, rappresentano, mettendo in guardia da scenari tutt'altro che fantascientifici di un 'Grande Fratello' di orwelliana immaginazione[4] o di quel Panopticon di benthamiana origine[5] che rende la società 'trasparente'[6] grazie ad una sorveglianza tecnologicamente avanzata e sempre più 'liquida'[7]. Il fattore accelerante della complessa e storica tensione sicurezza-riservatezza, di cui già l'*Habeas Corpus* si faceva carico, è rinvenibile pertanto nel progresso tecnico-scientifico: questo 'terzo fattore' scatenante e dalla potenza dirompente ha imposto l'esigenza di un ancora più attento ripensamento del binomio analizzato e delle opportunità, rischi e tutele che devono accompagnare l'innovazione e la incessante 'datificazione' e 'digitalizzazione'.

Se Solove si è posto i dirompenti, compositi ed articolati quesiti scaturenti da questo inedito trinomio 'Big Data-sicurezza-riservatezza/protezione dei dati' e ha cercato risposte nella normativa e nella *case-law* statunitense, la curiosità e l'interesse rispetto a tale tema hanno invece portato a chiedermi quali approcci, quali posizioni e quali interventi legislativi e giurisprudenziali fossero stati

[4] G. ORWELL, *1984*, Secker&Warburg, 1949.

[5] J. BENTHAM, *Panopticon or the inspection-house*, Payne, 1791. Si legga anche però M. FOUCAULT, M. PIERROT (a cura di), *Jeremy Bentham. Panopticon ovvero la casa d'ispezione*, nella traduzione italiana di V. Fortunati, Marsilio, 1997. Seppur noto, si vuole ricordare come il progetto di carcere promosso da Bentham fosse basato sull'idea di realizzare una struttura circolare che garantisse una continua e perenne sorveglianza operata da un sorvegliante centrale, celato alla vista dei prigionieri. Il principio di fondo era quello secondo cui la convinzione della invisibile e costante sorveglianza inducesse, per sé stessa, i prigionieri – che non potevano stabilire in quale momento e se fossero sottoposti a osservazione o meno – a comportarsi sempre correttamente e in maniera retta.

[6] È l'espressione utilizzata da David Brin nel suo celebre *The transparent society. Will technology force us to choose between privacy and freedom?*, Perseus Books, 1998.

[7] Il termine è mutuato da Z. BAUMAN, D. LYON, *Liquid surveillance. A conversation*, Polity Press, 2013: la 'liquidità' ben trasmette l'idea di una sorveglianza pervasiva e dilagante in ogni ambito della vita moderna. Gli autori suggeriscono il superamento della visione Benthamiana e l'avvento di una modernità post-panottico, nella quale le nuove tecnologie e la loro architettura mobile, flessibile e mutevole rende ormai superflui muri e strutture in mattoni come quelli ideati da Bentham.

intrapresi e avessero caratterizzato la dimensione ed il contesto ordinamentale a me maggiormente famigliare, quello cioè dell'Unione europea, dei suoi Stati membri e, infine, quello più prossimo dell'Italia.

Nella consapevolezza però dell'ampiezza dei quesiti e della tematica sino ad ora tratteggiati, che rappresentano il *fil rouge* di tutto il presente lavoro, si è reso necessario individuare un punto prospettico dal quale poter osservare una specifica problematica ed un preciso aspetto di quella sfida sopra delineata che il mondo del diritto, legislatori e Corti sono chiamati ad affrontare, pur senza perdere di vista il panorama entro cui l'ambito di ricerca più ristretto necessariamente si inserisce e dal quale risulta fortemente influenzato. Un 'osservatorio privilegiato', che racchiude in sé quei complessi interrogativi che discendono dal trinomio citato e che ne è dunque espressione ed esemplificazione, è da rinvenirsi nello strumento della *data retention* ovvero della conservazione svolta da soggetti privati di dati e metadati derivanti da comunicazioni elettroniche, finalizzata al successivo – benché eventuale – accesso a tali informazioni da parte di autorità di *law enforcement* o agenzie di intelligence per scopi securitari. Le operazioni di raccolta e memorizzazione, effettuate da fornitori dei servizi di telecomunicazione, laddove svolte in maniera generalizzata ed indiscriminata, interessando dunque tutti gli utenti e tutte le comunicazioni, consentono alle autorità pubbliche di disporre di una enorme mole di dati e di poter così 'andare indietro nel tempo'[8] al fine di reperire informazioni utili a scopi investigativi, anche attinenti a soggetti previamente non noti alle forze dell'ordine e rispetto ai quali pertanto non vi era, al momento della conservazione, nessun sospetto tale da giustificare un controllo mirato delle comunicazioni[9]. Forme di *data retention* possono interessare diverse tipologie di dati e non limitarsi a quelli derivanti da telecomunicazioni: ne sono un esempio le discipline di conservazione aventi ad oggetto i c.d. PNR, i codici di prenotazione di passeggeri aviotrasportati, che hanno acquisito una particolare rilevanza ai fini securitari e di indagine soprattutto a seguito degli attentati terroristici alle Torri Gemelle. Il progresso tecnologico ha reso infatti possibile, anche mediante l'impiego di tecniche di Intelligenza Artificiale e di analisi algoritmica, l'esame di una grande quantità di dati che, letti in maniera aggregata o confrontati con informazioni contenute in altre banche dati a disposizione delle autorità pubbliche, consentono di addivenire ad una profilazione degli utenti o dei passeggeri di voli aerei, ricostruendo abitudini, connessioni tra soggetti, luoghi frequentati, conoscenze e, in taluni casi, anche preferenze, stato di salute ed orientamento politico. Per quanto ogni singolo dato, preso singolarmente, possa sembrare 'innocuo' e poco determinante, la disponibilità di una ingente massa di informazioni, relative all'intera popolazione, unitamente ai moderni e sofisticati mezzi di *data analytics*, rendono tutt'altro che marginale o difficile una invasione nella vita privata e costituiscono una minaccia seria e reale per la protezione dei dati e per un fattivo controllo su di essi, oltre al rischio di abusi e dunque di utilizzi di tale preziosa miniera di informazioni per finalità differenti da quelle per le quali essi

[8] I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 54, 2017. Come sottolineato da Murray e Fussey, "these methods of interrogating retained communications data benefit from the ability to look into the past. First, in the event of a crime, retained data allows security services to 'rewind' events, facilitating the identification of suspects and a better understanding of what happened. (..) Second, retained data allows analysts to look back and immediately identify a suspect's pre-existing network", D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, in *Israel Law Review*, 1, 2019, p. 40.

[9] Riassuntivamente ma incisivamente, "the aim of this bulk accumulation of data is to generate useful and reliable correlations and ultimately to generate suspects", M. ANDREJEVIC, *Surveillance in the big data era. Emerging pervasive information and communications technologies*, in *Law, Governance and Technology Series*, 11, 2014, p. 55.

vengono originariamente conservati. Ecco dunque che la disciplina della *data retention* diviene una perfetta esemplificazione di quelle potenzialità e criticità di cui si è accennato sopra, aprendo a tutti quegli interrogativi che già dalla *big picture* sono emersi: non a caso lo strumento della *data retention* e la sua disciplina sono stati definiti come uno dei terreni più delicati sul quale la tutela della sicurezza e quella dei diritti fondamentali alla riservatezza e protezione dei dati si sono scontrati.

Individuata così la disciplina della conservazione e accesso ai dati per esigenze di garanzia della sicurezza quale osservatorio privilegiato mediante il quale analizzare il trinomio 'Big Data-sicurezza-riservatezza/protezione dei dati', si rende necessario delimitare con ulteriore precisione e puntualità l'ambito della ricerca, restringendolo sotto il profilo dell'oggetto, del tempo e dello spazio.

Con riferimento al primo degli aspetti indicati, si è deciso di circoscrivere lo studio alle forme di *data retention* attinenti a dati e metadati derivanti da telecomunicazioni nonché ai PNR, per fini di prevenzione e contrasto alla criminalità grave[10]. La disciplina di *data retention* di cui primariamente ci si occupa, inoltre, sebbene questo aspetto verrà di volta in volta specificato al lettore, è quella che prevede l'intervento di un soggetto privato ovvero del fornitore di un servizio, sul quale ricade l'obbligo di conservazione e/o trasferimento dei dati ad autorità pubbliche per scopi di garanzia della sicurezza. Ci si concentrerà dunque solo per determinati profili alle pur importanti sfide che le intercettazioni dirette da parte di autorità di *law enforcement* pongono in essere e che attengono cioè a forme di indagine riguardanti uno o più *target* precisi; la tipologia di conservazione cui si dedicherà maggiormente il presente lavoro è infatti quella operata da *service providers* e avente carattere generalizzato ed indisciplinato, dunque massivo, coinvolgente la totalità dei mezzi di telecomunicazione così come l'insieme degli utenti.

Sotto il profilo temporale, la disamina trova un punto conclusivo nella metà del mese di luglio 2020: questa scelta così specifica, che merita di essere debitamente sottolineata, è motivata dalla volontà di svolgere uno studio quanto più possibile preciso ed accurato. A metà del mese di luglio 2020 e nell'ottobre del medesimo anno, infatti, sono avvenuti due accadimenti di grande rilievo e complessità: sono state pubblicate tre importanti decisioni emanate dalla Corte di giustizia dell'UE (d'ora in avanti CGUE), che assumono particolare rilievo ai fini dello studio della materia in esame. Si fa riferimento alle pronunce: 16 luglio 2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems* (c.d. Caso *Schrems II*); 6 ottobre 2020, C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e al.*, e, dello stesso giorno, la sentenza nei casi riuniti *La Quadrature du Net e al. c. Premier Ministre e al.*, C-512/18 e *Ordre des barreaux francophones et germanophone e al. c. Conseil des Ministres*, C-520/18. Ebbene tali articolate sentenze, estremamente attese e dalla storica portata oltre che dalle forti implicazioni, presentano molteplici aspetti degni di analisi e di riflessione seria e lucida. Pur non potendo ignorare tali importanti sviluppi, che saranno certamente oggetto di studio accurato in vista della discussione del presente lavoro, la scelta di non includerli nell'analisi svolta è dettata dalla consapevolezza che gli svariati profili da sondare e le composite analisi che ne sarebbero derivate non avrebbero certamente potuto essere debitamente colte e sviluppate nei pochi mesi rimasti prima della data di scadenza della consegna della tesi. I temi affrontati in queste decisioni – benché in parte

[10] Non è pertanto trattato il tema della conservazione di dati prodotti ad esempio da oggetti quali automobili senza guidatore o c.d. *wearable devices*, o ancora la raccolta e conservazione di dati biometrici e genetici, così come non sono trattate le forme di conservazione per scopi differenti da quello securitario: vengono escluse dunque le pur interessanti problematicità derivanti dalla conservazione di dati riguardanti i dipendenti nell'ambito di un rapporto di lavoro o ancora memorizzati da aziende e imprese ed utilizzati per scopi commerciali.

sviluppati e presenti nella disamina mediante una accurata analisi delle Conclusioni degli Avvocati generali, presentate alla fine del 2019 e nei primi mesi del 2020 – non avrebbero potuto trovare il tempo e lo spazio adeguati per uno studio realmente approfondito, nella convinzione che un commento o una lettura 'a caldo', non fondata neppure su una solida dottrina, possa rappresentare, più che un valore aggiunto, il pericolo di incorrere in una leggera e superficiale disamina, non in grado di uniformarsi a quella che ha voluto al contrario porsi – forse ambiziosamente – come una analisi meditata, attenta e non avventata di una tematica di estrema complessità e dalle molteplici e sottoli sfaccettature.

Sul profilo dello spazio, infine, la scelta è stata quella di incentrare lo studio sul contesto dell'Unione europea e dei suoi Stati membri: una decisione, questa, dettata dall'interesse e dalla rilevanza di quell'approccio e quelle vicende normative e giurisprudenziali, così uniche e particolari, che hanno caratterizzato l'esperienza europea. Non è un caso che sia rinvenibile proprio nella legislazione dell'UE una profonda e per certi versi innovativa ed anticipatrice attenzione alla protezione dei dati come diritto distinto rispetto a quello alla riservatezza, che trova invece le sue radici nel contesto statunitense: è proprio nella Carta di Nizza che si può ravvedere uno dei primi chiari riconoscimenti del diritto autonomo alla *data protection*, cui è attribuito un spazio preciso e differente rispetto all'art. 7 volto a tutelare la vita privata; così come è nei Trattati, nelle Direttive e nei Regolamenti, alla cui analisi verrà dedicato ampio spazio nei Capitoli di questo lavoro, che si può notare la decisa tensione alla creazione di un panorama legislativo articolato e ricco capace di garantire la tutela dei diritti fondamentali alla privacy e protezione dei dati in tutte le sue sfaccettature e di considerare in maniera precisa ed innovativa le sfide e le difficoltà poste dalle nuove tecnologie. È ancora nell'Unione europea che un dibattito vivace, composito e profondo sulla disciplina della *data retention* ha trovato ampio spazio, arricchito – e sicuramente reso più complesso ma anche interessante – dall'ulteriore elemento di peculiarità che consta nel rapporto articolato e talvolta difficile tra Unione europea e Stati membri.

In questo panorama, infatti, la discussione sulla conservazione dei dati e metadati per scopi securitari ha presentato toni contrastanti ed è stata oggetto di spinte differenti e contrapposte: sin dai primi anni Duemila l'adozione di normative che prevedessero un obbligo in capo agli Stati membri di introdurre discipline di *data retention* generalizzata in capo ai fornitori di servizi di telecomunicazione ha incontrato serie resistenze nelle numerose autorità preposte alla tutela dei diritti alla riservatezza e alla protezione dei dati e che hanno trovato nell'Unione Europea quanto negli Stati membri un terreno fertile e un attivismo interessato e acuto. I dubbi e le preoccupazioni sulla conformità rispetto alla Carta di Nizza di una invasione nella sfera privata e nel diritto alla protezione dei dati di tale portata e magnitudo, non hanno tuttavia impedito l'adozione di normative europee in questo ambito, grazie anche alla forte spinta esercitata dagli Stati membri che vedevano nella *data retention* uno strumento irrinunciabile nella lotta al terrorismo e alla criminalità grave che proprio agli inizi del XXI secolo si era imposta quale obiettivo centrale e priorità delle democrazie del Vecchio Continente.

Emerge da subito quindi come si siano fatti strada da un lato un orientamento 'pro-securitario', inteso a sfruttare tutte le potenzialità che le nuove tecnologie offrivano sul piano della tutela della sicurezza, e dall'altro una posizione maggiormente 'right-oriented', che chiedeva una seria riflessione circa la proporzionalità e necessità di tali strumenti invasivi e lesivi dei diritti fondamentali nonché capaci di incidere anche sul rapporto tra cittadini e Stato. Due approcci differenti e due modi opposti di leggere il rapporto tra le componenti di quel complesso trinomio di cui si è sopra parlato, che si sono poi manifestati con tutta la loro forza nelle vicende giurisprudenziali e nelle scelte

normative susseguitesi sino ad oggi e che ancora non hanno trovato un punto di arrivo conclusivo e definito. I molteplici interventi della CGUE si sono intrecciati con le 'resistenze' degli Stati membri e la difficoltà di attuare normative nazionali in grado di rispondere ed incorporare quei requisiti di proporzionalità e quelle salvaguardie indicate dai giudici di Lussemburgo; così che, nell'immobilismo del legislatore dell'UE, sono state le Corti nazionali, spesso, a farsi portatrici di quei dubbi interpretativi e a sottolineare quelle zone grigie che la c.d. *data retention saga* aveva – più o meno volutamente – lasciato, instaurando un dialogo con la CGUE e contribuendo, con decisioni di grande rilievo, a definire i contorni e le possibili soluzioni a quella domanda che già Solove oltreoceano si poneva, ovvero se fosse possibile ricomporre lo iato tra sicurezza e riservatezza nell'era degli strumenti di sorveglianza di massa, delle nuove tecnologie e dell'emergenza securitaria. Una questione, questa, che ha portato l'Unione europea a travalicare i confini territoriali e ad affrontare delicati interrogativi circa il trasferimento di dati verso Stati terzi e la possibilità o opportunità di garantire standard elevati di *data protection* e della privacy anche nel mondo digitale senza limiti, un mondo che trascende appunto dal concetto di territorialità e sovranità territoriale.

In questo contesto e alla base dell'analisi della dimensione dell'Unione europea, sotto il profilo dell'intervento della CGUE nonché dei legislatori, fondamentali sono state alcune più specifiche *research questions* che hanno mosso lo studio e l'approfondimento critico del presente lavoro e che evidenziano una chiara specificazione di quei più ampi quesiti inizialmente rilevati: una disciplina della *data retention* generalizzata ed indiscriminata, come quella a cui gli Stati membri sono restii a rinunciare, è compatibile con la Carta di Nizza? Può la lotta al terrorismo e alla criminalità grave giustificare una forma di sorveglianza massiva quale quella appunto di una conservazione generalizzata riguardante tutti gli utenti, indipendentemente da qualsiasi connessione con un sospetto o con una minaccia concreta e reale? Un totale divieto di una forma di conservazione siffatta è soluzione adeguata, proporzionata e praticabile o finisce invece per incidere fortemente ed irrimediabilmente sulla garanzia della sicurezza, inficiandone l'efficacia e la reale capacità operativa? Entro quali confini e limiti una ingerenza nei diritti fondamentali, perpetrata da autorità pubbliche mediante forme di sorveglianza che si avvalgono anche dell'azione di soggetti privati, può considerarsi legittimata da interessi quali la tutela della sicurezza e la repressione dei reati? È possibile trovare un punto di equilibrio tra sicurezza e diritti fondamentali alla riservatezza e alla protezione dei dati nell'ambito europeo? O ha prevalso una logica di 'trade-off'? Tali quesiti non possono che essere analizzati sulla base delle posizioni espresse in merito dalle diverse Istituzioni dell'UE ed in particolare della CGUE e dei legislatori; ciò tuttavia apre ad ulteriori ed importanti interrogativi: qual è l'impatto della particolare struttura dell'UE in tale ambito e dunque del riparto di competenze tra UE e Stati membri, che incidono anche in materie quali la garanzia della sicurezza nazionale e la lotta alla criminalità? Come l'affermarsi imperioso delle nuove tecnologie e di strumenti quali la *data retention* incide su di una chiara determinazione dell'ambito di applicazione del diritto dell'UE? Qual è il ruolo della CGUE e come essa ha interagito con il legislatore dell'UE nonché con le Corti nazionali? A chi spetta il compito delicato e difficile di determinare un corretto bilanciamento – o una scelta tra il diritto e l'interesse da tutelare, se si abbraccia un approccio di 'trade-off' – e può il legislatore europeo intervenire per ridurre l'attivismo e l'operato quasi 'sostitutivo' tenuto dalla CGUE? Quanto ha inciso nel dialogo multilivello la posizione assunta da giudici e legislatori nazionali? Senza dubbio la diversità degli orientamenti e del modo in cui i diversi Stati membri hanno risolto o tentato di risolvere il bilanciamento – o l'inevitabile prevalenza – tra sicurezza e diritti fondamentali nella disciplina della *data retention* hanno contribuito a creare un panorama articolato ed estremamente frammentario, all'interno del quale è nondimeno possibile

rinvenire linee comuni oltre a scelte e soluzioni, normative e giurisprudenziali, differenti e talvolta divergenti rispetto a quanto indicato sia dalla CGUE, sia dagli altri Stati membri stessi.

Proprio il continuo dialogo e rimando tra livello nazionale ed europeo è da porsi alla base della scelta di non concentrare l'attenzione solamente sul piano dell'Unione europea bensì di analizzare il tema e cercare di rispondere alle domande emerse anche attraverso la lente del diritto pubblico comparato, concentrandosi sulla disamina di tre realtà ordinamentali: Regno Unito, Belgio e Italia. È questo forse il profilo e l'aspetto meno esplorato ed approfondito dalla dottrina: se è vero infatti che serie e approfondite disamine sono state svolte nell'ambito del diritto dell'UE rispetto alle storiche e determinanti sentenze della CGUE, che pur rappresentano, anche nel presente lavoro, un punto di partenza fondamentale ed imprescindibile, poco ci si è interrogati invece quanto all'approccio e all'orientamento dei diversi Stati membri rispetto alla materia della *data retention*. Mentre grande rilievo è attribuito al momento sicuramente centrale della pronuncia dei giudici di Lussemburgo, pare altrettanto importante cogliere i motivi e le vicende giurisprudenziali che hanno portato all'intervento, spesso su rinvio pregiudiziale, della CGUE e quali siano le motivazioni che hanno mosso le Corti nazionali a richiedere l'intervento dei colleghi europei. Poco studiato, inoltre, è il profilo delle conseguenze delle sentenze della *data retention saga* sui legislatori e sui giudici degli Stati membri: quali sono cioè le caratteristiche delle scelte normative prese sulla base dei criteri fissati dalla CGUE? Qual è l'interpretazione di questi ultimi impiegata dai Governi e Parlamenti nazionali al fine di regolamentare la delicata disciplina della *data retention*? Quali le ragioni che hanno spesso spinto la società civile o le ONG a promuovere controversie dinnanzi ai giudici nazionali rispetto a tale disciplina? Come questi ultimi hanno letto la giurisprudenza europea e l'hanno utilizzata per giudicare sulla legittimità e conformità alla Carta di Nizza e alle Carte costituzionali di normative nazionali in materia di conservazione e accesso a dati e metadati? Quali sono le diversità di approccio e le motivazioni che hanno portato taluni Stati membri a promuovere un rinvio pregiudiziale, mentre altri non hanno affrontato, né dal punto di vista legislativo né giudiziario, la questione del bilanciamento sicurezza-riservatezza nel contesto della *data retention*? L'apporto della giurisprudenza della CGUE ha comportato un innalzamento del livello di tutela fornito dagli Stati membri in materia? Non tutti i rinvii pregiudiziali e neppure le soluzioni normative adottate sono mossi dalle medesime interpretazioni e approcci, che talvolta si sono dimostrati attenti a promuovere il dialogo con la CGUE o con le Istituzioni europee, nella consapevolezza delle criticità persistenti dell'orientamento giurisprudenziale europeo; talaltra si sono invece posti in una posizione di 'scontro' o comunque di maggior distanza rispetto ai criteri stabiliti dai giudici di Lussemburgo.

È allora alla luce di tali quesiti che la comparazione diviene una parte imprescindibile del presente lavoro: attraverso l'analisi e la conoscenza delle vicende nazionali e dunque del diritto straniero, è possibile accrescere il livello di conoscenza ed approfondimento della materia svolgendo un raffronto tra scelte e modelli, allo scopo di ispirare e coadiuvare non solo il legislatore, nazionale e non, nel proprio operato, ma anche le Corti nell'analisi dei casi ad esse sottoposte. Se comparare viene inteso come "confrontare e paragonare, esprimendo giudizi valutativi sul confronto"[11], le considerazioni di raffronto che verranno espresse nelle Conclusioni di questo elaborato mirano proprio a fornire una valutazione che, pur cogliendo ed evidenziando le differenze ordinamentali[12], permette di elaborare

[11] L. PEGORARO, A. RINELLA, *Sistemi costituzionali comparati*, Giappichelli, 2017, p. 34.

[12] Come si dirà, infatti, il riconoscimento dei diritti fondamentali alla privacy e protezione dei dati è differente nei diversi ordinamenti esaminati e anche le diversità e peculiarità in termini di accesso alla giustizia comportano un impatto di rilievo sull'intervento delle Corti e sul loro operato anche in materia di *data retention*.

riflessioni utili per le Istituzioni europee nonché per i legislatori e giudici nazionali che si trovano, tutti, dinnanzi alla medesima cruciale sfida di regolamentare lo strumento della conservazione e accesso ai dati e metadati. Tali analisi possono rappresentare uno stimolo ad un più approfondito raffronto di soluzioni normative ed interventi giurisprudenziali, consentendo infine l'individuazione delle pratiche migliori e più virtuose o delle scelte più appropriate e compatibili con l'assetto legislativo e con i principi giurisprudenziali individuati a livello dell'UE. Sebbene dunque i due piani, europeo e nazionale, siano inscindibilmente legati e connessi tra loro, e seppure sia maggiormente evidente l'incidenza della dimensione europea su quella nazionale, data anche la forza dirompente di alcune pronunce della CGUE in materia, pare altrettanto fondamentale volgere uno sguardo attento al profilo degli Stati membri e alle soluzioni trovate nella dimensione interna, al fine anche di stabilire un proficuo dialogo con il legislatore dell'UE ed effettuare scelte ragionate, anche sulla base delle valutazioni e riflessioni che in taluni Stati membri si sono già dimostrate profonde e serie, incentivando decisioni maggiormente condivise, realmente armonizzatrici e che possano reggere al vaglio attento tanto della CGUE quanto delle Corti nazionali. Comparare infine è utile a conoscere e capire sé stessi[13]: per questo la comparazione che qui si propone vuole essere spunto per instaurare un più ampio e consapevole dibattito nel contesto italiano, nel quale, ad oggi, il tema della disciplina della *data retention* è passato, nel complesso, piuttosto inosservato sia dal legislatore, sia dai giudici che poco hanno colto della complessità e dei molteplici quesiti ancora aperti e in attesa di definizione che caratterizzano la giurisprudenza europea e che invece altre Corti nazionali sono riusciti a meglio comprendere e che si sono poi concretizzati in innumerevoli rinvii pregiudiziali di grande spessore ed importanza.

Da tale convinzione quindi è scaturita la decisione di concentrarsi specificamente su tre Stati membri, Belgio, Italia e Regno Unito, – per quanto per quest'ultimo ovviamente tale attribuzione richieda cautela e debite precisazioni –: i motivi che hanno spinto ad individuare proprio questi tre ordinamenti risiedono in valutazioni preliminari sugli approcci in materia di *data retention* che ne determinano sia le vicende giurisprudenziali sia gli interventi normativi. Tali considerazioni, che saranno qui sotto riportate e che verranno trattate ed argomentate ampiamente nel presente lavoro, manifestano l'importanza della scelta di questi Stati in quanto paradigmaticamente rappresentativi di approcci differenti e, sotto taluni profili, divergenti tra loro, con riguardo tanto alle scelte e alle soluzioni normative adottate quanto alle decisioni giurisprudenziali, sebbene taluni esiti simili siano ravvisabili[14].

Il Regno Unito, infatti, è stato, sin dai primi anni Duemila, un protagonista importante del dibattito circa la regolamentazione dello strumento della conservazione generalizzata, adottando normative che si sono susseguite a rapido ritmo e che non hanno sempre considerato – e talvolta neppure atteso – le valutazioni ed i requisiti che la CGUE, soprattutto nelle decisioni *Digital Rights Ireland* e *Tele2*[15], hanno fissato con chiarezza anche con riferimento alle normative nazionali. Promuovendo

[13] Sul punto M. SMITS, *Comparative law and its influence on national legal systems*, in M. REIMANN, M. ZIMMERMANN (a cura di), *The Oxford handbook of comparative law*, Oxford University Press, 2006.

[14] Si vedrà infatti come il rinvio alla CGUE operato sia dalla Corte costituzionale belga, con riferimento tanto alla normativa in materia di *data retention* quanto a quella attinente al trasferimento di PNR, sia dal *Investigatory Powers Tribunal* inglese, risultino indicativi di una problematica e di criticità comunemente ravvisate e condivise, tutte aventi ad oggetto le principali posizioni espresse dalle sentenze della CGUE in tale complesso ambito.

[15] 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications e al.*; 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB c. Post-och telestyrelsen* e *Secretary of State for the Home Department c. Tom Watson e al.*

due rinvii pregiudiziali di enorme rilievo, le Corti nazionali inglesi hanno utilizzato tale strumento per avviare un dialogo dai toni aspri, che talvolta ha mirato a 'redarguire', sebbene tra le righe, i giudici di Lussemburgo, facendosi portatrici di una lettura del rapporto sicurezza-riservatezza nell'epoca dei Big Data molto pragmatica e orientata all'efficienza delle soluzioni e degli strumenti adottati rispetto alla finalità primaria e vitale della tutela della sicurezza. Nonostante questo approccio forse più di contrapposizione, che vuole anche ottenere una chiara e netta determinazione dell'ambito di applicazione del diritto dell'UE, così da svincolare taluni profili della regolamentazione della materia dai criteri fissati prevalentemente dalla giurisprudenza della CGUE e pur con tutte le incognite senza precedenti che ora si aprono dinnanzi alla c.d. Brexit anche per quanto riguarda la protezione dei dati e il flusso di dati tra l'UE e il Regno Unito, quest'ultimo ha comunque mostrato, soprattutto in tempi più recenti, una forte sensibilità al tema della *data retention* e alla promozione di un dibattito e di uno studio approfondito della tematica, ponendo in essere anche un serio tentativo di accogliere taluni dei rilievi emersi dalle decisioni dei giudici europei e cercando di inserirli nel contesto normativo interno.

Il Belgio, diversamente, ha visto l'intervento più netto ed inizialmente quasi 'ossequioso' della Corte costituzionale rispetto alle decisioni della CGUE. Il legislatore, invece, ha affrontato sin dalla prima normativa in materia significative difficoltà e scontri, anche con le Autorità nazionali garanti della protezione dei dati, che hanno reso complesso e tutt'altro che rapido il procedimento di predisposizione e approvazione di una normativa in materia di *data retention*, cercando dunque soluzioni che fossero quanto più possibile indirizzate ad un elevato standard di tutela dei diritti fondamentali. La discussione e lo studio attento anche e soprattutto della vasta giurisprudenza europea e di altri Stati membri emerge con chiarezza sia dalle più recenti decisioni dei giudici costituzionali belgi, che per ben due volte hanno rinviato alla CGUE, sia dai lavori preparatori che hanno accompagnato il percorso legislativo di adozione della attualmente vigente normativa sulla conservazione dei dati.

Una conoscenza e consapevolezza che non traspare, invece, come anticipato, né dalla giurisprudenza né dal dibattito parlamentare del nostro Paese, nel quale le confuse normative approvate, con strumenti inappropriati per una disciplina così delicata ed articolata, hanno finito con l'attribuire all'Italia il non invidiabile primato di un obbligo di conservazione dei metadati tra più ampi e lunghi dell'UE – ben settantadue mesi, a fronte di Stati come Regno Unito e Belgio che prevedono invece un massimo di dodici o sei mesi –. Nel nostro Paese, inoltre, le Corti hanno sempre mancato sia di adire la Corte costituzionale in via incidentale, sia di promuovere un rinvio pregiudiziale alla CGUE, negando un dialogo che, seppur con toni differenti, gli altri Stati membri hanno proficuamente instaurato.

Ecco quindi che, da tali valutazioni preliminari, emerge come, nonostante anche altri ordinamenti abbiano certamente mostrato un interessante attivismo in materia mediante decisioni di sicuro rilievo, Regno Unito, Belgio e Italia raffigurano gli esempi maggiormente emblematici dei diversi possibili orientamenti e reazioni adottate dagli Stati membri.

Lo studio degli ordinamenti individuati si è inoltre arricchito di due esperienze di studio e ricerca all'estero, che hanno permesso di reperire materiale e conoscere esperti – Professori, Ricercatori e Avvocati – che si sono occupati ampiamente della tematica studiata: il primo soggiorno ha avuto luogo in Belgio, in particolare al Centre for IP & IT Law della Katholieke Universiteit di Leuven, un centro di ricerca specializzato ed interamente dedicato allo studio delle nuove tecnologie e del loro impatto sul mondo del diritto, nel quale ho avuto modo di conoscere molti degli autori citati nel presente lavoro. Il secondo soggiorno, invece, ha avuto quale meta il Trinity College Dublin, in

Irlanda: durante tale periodo di studio ho avuto l'opportunità di confrontarmi con molti studiosi, i cui scritti sono stati di fondamentale importanza per la completa comprensione del tema affrontato, alcuni dei quali, come il Professor David Fennelly, sono stati Attorney in alcune delle controversie esaminate, giunte dinnanzi alla CGUE; questi incontri formativi ed interessanti mi hanno permesso di reperire materiale utile ed aggiornato e mi hanno soprattutto aiutato a cogliere e sviluppare un punto di vista ed un approccio anche pragmatico e concreto delle questioni complesse alla base di questo studio.

La sfida che caratterizza il percorso di ricerca e di elaborazione della presente tesi, dunque, è rappresentata anche dalla scelta di analizzare la tematica del trinomio 'Big Data-sicurezza-riservatezza/protezione dei dati' nello specifico caso della *data retention* per scopi securitari sotto il profilo tanto del diritto dell'Unione europea quanto di quello del diritto pubblico comparato. Il tentativo è stato quello di comporre tali due 'anime' in un lavoro che potesse presentare spunti di interesse e riflessioni approfondite, in grado di cogliere sia le peculiarità della visione e delle difficoltà affrontate sul piano europeo, sia quelle caratterizzanti la prospettiva nazionale, senza perdere di vista l'immagine più ampia e i continui intrecci e connessioni che identificano il particolare ed unico contesto dell'Unione europea[16].

Sulla base delle scelte illustrate, pertanto, la struttura del lavoro è stata ripartita in tre parti, inscindibilmente interconnesse tra loro e l'una funzionale all'altra e interdipendente dall'altra, a rappresentare come la dimensione generale del tema non possa leggersi disgiuntamente dal caso-studio individuato nella disciplina della *data retention*, i cui sviluppi non posso essere appieno compresi se non unendo gli approcci degli ordinamenti oggetto di analisi alle vicende proprie del legislatore e dei giudici dell'Unione europea.

Il lavoro si dipanerà quindi con la seguente scansione: nella Parte I e nel suo Capitolo I, verrà delineato il contesto generale, quella che è stata sopra denominata la '*big picture*', entro la quale la ricerca si inserisce e dalla quale non può prescindere. Verrà prestata particolare attenzione alle sfide che i Big Data, la società dell'algoritmo e la 'datizzazione' pongono rispetto al mondo del diritto in generale e alla tutela dei diritti fondamentali in particolare. Ampio spazio verrà dedicato alla determinazione delle molteplici potenzialità dei Big Data e degli strumenti di *data analytics*, anche mediante l'impiego dell'Intelligenza Artificiale, senza tralasciare di esaminare le minacce ed i pericoli che a tali sistemi sono connessi, ricostruendo così vicende, quali le rivelazioni di Snowden prima accennate o il caso Cambridge Analytica, essenziali per i rilievi che verranno svolti nei Capitoli successivi. Nel tracciare le coordinate di riferimento per una piena comprensione dello specifico caso di studio oggetto delle successive parti del lavoro, verranno dunque ricostruiti i diritti fondamentali alla riservatezza e alla protezione dei dati, mettendone in luce sia i profili evolutivi e il riconoscimento che hanno trovato all'interno delle Carte dei diritti fondamentali nel contesto europeo e nazionale, sia la stretta connessione con gli altri diritti fondamentali quali le libertà personali e la dignità della persona. Queste premesse risulteranno di particolare rilievo al fine di comprendere l'importanza e la complessità che la disciplina della *data retention* rappresenta. Verranno pertanto svolte considerazioni introduttive quanto allo strumento della conservazione e accesso a dati e metadati per finalità di lotta alla criminalità e garanzia della sicurezza – nazionale e pubblica –, il

[16] In questo senso si può abbracciare quanto affermato da Popper, che sosteneva "Noi non siamo studiosi di certe materie, bensì di problemi. E i problemi possono passare attraverso i confini di qualsiasi materia o disciplina", K. R. POPPER, *Congetture e confutazioni*, traduzione italiana di G. Pancaldi, Il Mulino, 1972, p. 118.

suo funzionamento, le potenzialità rispetto alla salvaguardia della sicurezza, nonché i rischi che esso implica per la garanzia dei diritti fondamentali.

Prendendo le mosse dai concetti e considerazioni illustrati nella Parte I, la Parte II si focalizzerà invece della *data retention* sotto il profilo della dimensione dell'Unione europea: seguendo un criterio cronologico, che ripercorre gli interventi legislativi nonché le vicende giurisprudenziali di cui la CGUE si è resa protagonista, verranno delineate le fondamentali fonti normative di riferimento, quali la Direttiva *e-Privacy* (Dir. 2002/58/CE) nonché la successiva e discussa *Data Retention Directive* (Dir. 2006/24/CE), ricostruendo anche l'importante dibattito che ha accompagnato l'adozione di tali legislazioni e che ha visto quali protagonisti oltre al Consiglio, la Commissione e il Parlamento europei, anche il Gruppo di Lavoro art. 29, il Garante europeo della protezione dei dati e, ovviamente, gli Stati membri. Le criticità emerse già in questa iniziale fase conducono alla trattazione della lunga *data retention saga*: nel Capitolo II ampio spazio verrà dedicato non solo alle decisioni della CGUE e alle Conclusioni degli Avvocati generali bensì anche alle reazioni degli Stati membri dinnanzi a tali pronunce, che risultano determinanti per la piena comprensione dei rinvii pregiudiziali che si sono succeduti nel corso degli anni. Il Capitolo III, invece, si concentrerà sugli effetti delle pronunce previamente analizzate in materia di *data retention* ed in particolare prestando attenzione alla dimensione esterna all'UE: si farà cioè riferimento alla disciplina del trasferimento e conservazione dei dati derivanti da telecomunicazioni o dei PNR verso Stati terzi, analizzando la normativa di riferimento, dalla Direttiva 95/46/CE al vigente Reg. UE 2016/679 (c.d. GDPR, *General Data Protection Regulation*), per poi passare alle storiche pronunce della CGUE, dal caso *Schrems* al *Parere 1/15*[17], sino ai rinvii pregiudiziali al momento ancora pendenti, sia mettendone in luce le conseguenze in materia di trasferimento dati al di fuori dei confini dell'UE, sia determinandone le connessioni fondamentali con la materia della *data retention*. Ne scaturiranno importanti considerazioni che mirano a riflettere sull'azione dell'UE nella dimensione esterna al proprio territorio, sulla affermazione di un modello eurocentrico di tutela extra-territoriale della riservatezza e protezione dei dati e sugli effetti che queste posizioni comportano nella dimensione interna all'UE e dunque sulle normative europee e nazionali (si pensi alla Direttiva PNR[18]). Il Capitolo IV, pur tenendo conto della limitazione temporale della presente ricerca, prenderà atto delle più recenti evoluzioni: è questo un ambito sino ad ora scarsamente trattato dalla dottrina, che si è spesso fermata all'analisi della decisione *Tele2* o tutt'al più e solo marginalmente della sentenza *Ministerio Fiscal*[19], mentre minore attenzione hanno attirato i rinvii pregiudiziali che si sono succeduti dal 2017 ad oggi. Essi rivestono, invece, a parere di chi scrive, un estremo rilievo per valutare i limiti e le criticità della materia: verranno quindi esaminati i rinvii pregiudiziali pendenti sino al luglio 2020 e le relative Conclusioni degli Avvocati generali, quali perfetto riflesso e risultato della complessità che ancora determina la materia, delle ampie zone grigie lasciate dalla giurisprudenza della CGUE nonché del dibattito, anche estremamente pragmatico, in seno agli Stati membri e alle difficoltà applicative ed interpretative da essi rilevate, quale rappresentazione emblematica di quei differenti approcci rinvenuti a livello nazionale e di cui più ampiamente si occuperà la Parte III. Questo Capitolo risulta dunque essere una fotografia della articolata situazione attuale, che non si limita al piano giurisprudenziale bensì presta debita attenzione anche al ruolo del

[17] 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*; 26 luglio 2017, *Parere 1/15*.
[18] Direttiva UE 2016/681 del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.
[19] 2 ottobre 2018, C-207/16, *Ministerio Fiscal*.

legislatore e alla posizione da esso assunta, vagliando le possibili prospettive future di azione e le proposte e il dibattito in essere. Il Capitolo V, infine, intende analizzare la materia della *data retention* e della sfida della convivenza tra diritti fondamentali e strumenti di sorveglianza massiva come affrontata dalla Corte europea dei diritti dell'uomo: verranno così esaminate alcune importanti pronunce che risultano di rilievo per comprendere sia l'evoluzione della giurisprudenza della Corte di Strasburgo, sia per evidenziarne le convergenze o divergenze rispetto all'orientamento seguito e ormai cristallizzato della CGUE. Tale disamina si rende interessante ed utile per riflettere anche sul livello di salvaguardia e di tutela che gli Stati europei sono chiamati a rispettare per quelle materie che risultano escluse dall'ambito di applicazione del diritto dell'UE.

La Parte III, come premesso, si occuperà invece dell'analisi della disciplina della *data retention* nel contesto dei tre Stati membri individuati: se è vero che la comparazione non può che poggiare sulla conoscenza e sull'esame primario e preventivo delle diverse esperienze che si vogliono porre a confronto, da tale consapevolezza nasce la decisione di esaminare ciascun ordinamento nazionale singolarmente, prima di svolgere la delicata ma necessaria operazione di raffronto che occuperà un apposito spazio nelle Conclusioni. I tre Capitoli che compongono l'ultima Parte, dunque, seguono una struttura simile e condivisa: si passa dallo studio della normativa e dei diversi interventi susseguitisi nel tempo, scanditi anche dall'evolversi della disciplina e della giurisprudenza europea, alla dettagliata analisi delle più significative sentenze delle Corti nazionali, sempre rapportate, necessariamente, alla parallela *case law* della CGUE, in modo da mettere così in luce le peculiarità proprie di ciascuno Stato dinnanzi alla tematica e dunque l'approccio seguito. Particolare importanza inoltre verrà dedicata al ruolo delle Autorità nazionali garanti della protezione dei dati, del Parlamento nonché della società civile e della dottrina nel dibattito, più o meno profondo e vivace, che ha caratterizzato la disciplina della *data retention* nei tre Stati considerati.

Le Conclusioni vogliono ragionare sulle implicazioni e considerazioni che dallo studio critico elaborato nelle diverse Parti del presente lavoro derivano, provando a delineare alcune risposte alle pur complesse – e forse ambiziose – *research questions* sopra individuate. Si muoveranno così alcune finali riflessioni sulla disciplina della *data retention*: con riferimento alla dimensione dell'UE si partirà dai punti fermi e dalle posizioni di cui i legislatori ma anche e soprattutto i giudici di Lussemburgo si sono fatti portatori, per delineare l'equilibrio ad ora promosso, pur ancora vacillante, e che vede nel rapporto tra Istituzioni dell'UE stessa così come tra UE e Stati membri fattori di complessità e instabilità; uno spazio particolare verrà però lasciato ad alcune valutazioni attinenti al fronte esterno, quello cioè del trasferimento di dati oltre i confini europei: la disciplina e la giurisprudenza in materia di trasferimento dei dati verso Stati terzi sta infatti divenendo lo strumento mediante il quale promuovere, se non addirittura imporre – con più o meno successo a seconda dei profili analizzati e con un approccio che resta ancora fortemente discusso quanto all'opportunità e all'efficacia – un livello di tutela e standard di protezione elevati, che accompagnino i dati anche una volta fuoriusciti dal territorio dell'Unione stessa, conducendo peraltro a discutere quanto all'esigenza di una disciplina internazionale che fissi requisiti e garanzie minime. Verrà poi affrontata la delicata comparazione tra l'approccio e l'orientamento caratterizzante gli Stati membri analizzati, tanto nel loro rapporto con la giurisprudenza e con il dibattito europeo, quanto tra di essi, cogliendone differenze, convergenze e soluzioni che possono divenire un utile spunto di analisi e riflessione. Tutte queste considerazioni, pur connesse allo specifico caso-studio della *data retention* consentono al contempo di astrarre da esso, per tornare a quella *big picture* iniziale e per comprendere quali siano gli impatti delle valutazioni svolte rispetto a quella sfida in rapida e continua evoluzione rappresentata dal complesso e difficile rapporto tra tecnologia, esigenze securitarie e diritti

fondamentali alla riservatezza e protezione dei dati. L'interazione tra gli elementi di tale trinomio è inoltre resa ancor più ardua e mutevole dal rapido progresso tecnologico nonché dal variabile sentire della coscienza generale e dagli avvenimenti storici, capaci di incidere sulle scelte politiche, legislative e giurisprudenziali che assumono un peso determinante per le nostre società. Ciò nella consapevolezza, ben espressa dalla Corte europea dei diritti dell'uomo in maniera efficace e diretta, che misure di sorveglianza, soprattutto se massive e fondate su strumenti tecnologicamente avanzati ed invasivi, costituiscono il concreto pericolo di "undermining or even destroying democracy on the ground of defending it"[20]. Ed ecco perché rispondere alla iniziale domanda sulla possibilità di individuare negli elementi del trinomio un ineluttabile rapporto di 'trade-off' o, al contrario, una coesistenza equilibrata, diviene uno degli sforzi di maggior rilievo che il diritto deve sostenere.

[20] Corte europea dei diritti dell'uomo, 6 settembre 1978, *Klass e al. c. Germania*, n. 5029/71, par. 49.

PARTE I

CAPITOLO I

BIG DATA, *DATA RETENTION* E DIRITTI FONDAMENTALI ALLA RISERVATEZZA E ALLA PROTEZIONE DEI DATI: COORDINATE DI RIFERIMENTO

L'avvento di Internet, del mondo digitale e l'affermarsi della globalizzazione che viaggia anche attraverso una rete, il Web, che ha per sua natura carattere a-territoriale ed intangibile, hanno provocato profondi cambiamenti, rivoluzionando il nostro modo di vivere. Toccando i più disparati aspetti della vita, dalla quotidianità al modo in cui comunichiamo, dal lavoro al tempo libero, dalle modalità con cui facciamo acquisti e prenotiamo servizi, anche pubblici, all'accesso a fonti di informazione e di conoscenza, l'evoluzione tecnologica e digitale non ha lasciato intoccato neppure il mondo del diritto. Quest'ultimo è stato chiamato ad interrogarsi sull'impatto dell'innovazione rispetto al ruolo di giudici e legislatori, al rapporto tra potere e cittadini, nonché ad esaminare quali adattamenti ed evoluzioni venissero richiesti rispetto ai tradizionali concetti e categorie del diritto; si è reso inoltre necessario riflettere sulle conseguenze che il progresso scientifico e tecnologico e l'uso sempre più massiccio ed esteso di nuove strumenti ha comportato e continua a comportare rispetto al godimento di diritti fondamentali: l'innovazione ha infatti avuto un significativo effetto sul godimento e sui mezzi di tutela predisposti dagli ordinamenti a protezione dei diritti fondamentali, talvolta determinando l'evoluzione e il rafforzamento di garanzie riferite a diritti già affermati e riconosciuti, talaltra portando alla affermazione di veri e propri nuovi diritti – si pensi al diritto all'oblio, al diritto di accesso ad internet, il diritto di rettifica o di opposizione legato alle informazioni riguardanti la propria persona –.

In questo contesto, la crescente e sempre più permeante digitalizzazione, intesa nella sua accezione di fenomeno che ha portato alla creazione di una enorme mole di dati digitali (c.d. Big Data), unitamente ad Internet, hanno reso la produzione, circolazione e trasferimento, rilevazione, raccolta, conservazione e trattamento dei dati operazioni molto più semplici, immediate ed accessibili oltre che ad attribuire alle stesse un enorme valore economico. I Big Data contengono, per la maggior parte, come si dirà, informazioni personali riguardanti diversi aspetti della vita del soggetto che li ha prodotti e che sono dunque capaci di dire molto su di esso. Gli strumenti avanzati e sofisticati che consentono di leggere in maniera aggregata i diversi dati raccolti, permettono anche di trasformarli e di impiegarli per le più disparate finalità, spesso differenti rispetto a quelle per le quali i dati stessi sono stati prodotti e raccolti: a titolo di esempio, e solo preliminarmente, si pensi alla complessa e grave vicenda di Cambridge Analytica, nella quale i dati derivanti da diversi profili degli utenti del noto colosso dei *social network* Facebook sono stati impiegati per profilazione e marketing a scopi politici ed elettorali, con una forte incidenza sulle informazioni messe a disposizione dei cittadini ed influenzando così la loro capacità decisionale.

Ecco dunque che emerge con chiarezza come la digitalizzazione e l'impiego della ingente quantità di dati prodotti quotidianamente dagli utenti di servizi di telecomunicazione o del Web abbiano posto grandi sfide rispetto al godimento e alla tutela di due diritti di grande rilievo: il diritto alla riservatezza e il diritto alla protezione dei dati. Questi, tuttavia, lungi dall'essere intesi separatamente ed indipendentemente da altri diritti fondamentali ampiamente riconosciuti, impongono di considerare con grande attenzione le importanti implicazioni che una adeguata tutela della vita privata e delle informazioni che ci riguardano possono comportare: se si tengono a mente le enormi potenzialità che la tecnologia insieme alla digitalizzazione offrono, potendo risultare anche in forme più o meno occulte di

controllo e sorveglianza da parte tanto di soggetti privati quanto pubblici, si comprende bene come il trattamento e dunque l'utilizzo di dati possa giungere ad incidere ad esempio sulla libertà di espressione, di voto, sul rispetto della dignità umana, della libertà di associazione, del giusto processo, del principio della presunzione di innocenza nonché, in ultima istanza, dello stato di diritto, del rapporto sussistente tra cittadini e autorità pubblica e, dunque, delle stesse fondamenta su cui la società democratica si basa. Dinnanzi a tali scenari, tutt'altro che futuribili o visionari bensì ormai ineludibile realtà, il mondo del diritto non può non esaminare approfonditamente ed affrontare le minacce e le sfide che vengono poste dalle innovazioni e dal progresso tecnico-scientifico, cercando soluzioni normative o giurisprudenziali adeguate alla rapida evoluzione della tecnologia e al sempre più elevato grado di tecnicità delle questioni e delle problematiche. Nel fare ciò, il giurista, il legislatore o il giudice debbono necessariamente comprendere la complessità delle questioni sottese all'impiego di nuovi strumenti tecnologici e valutarne i rischi ed i pericoli rispetto al godimento di diritti fondamentali.

Un caso di studio che consente di comprendere e mettere in luce, con estrema chiarezza, le diverse minacce e i rischi che l'innovazione e la digitalizzazione[1] comportano, è da individuarsi nella c.d. *data retention* ovvero nel regime che comporta l'obbligo di conservazione di dati e metadati da parte di soggetti privati ed il relativo accesso ad essi da parte di autorità pubbliche per finalità di lotta alla criminalità. Questo strumento, ormai divenuto fondamentale per agenzie di intelligence e di *law enforcement*, alle quali viene così consentito di 'andare indietro nel tempo' e di reperire informazioni relative a soggetti che prima della commissione di un reato non erano sottoposte ad indagine e neppure sospettate, ha aperto un ampio dibattito politico, dottrinario, legislativo e giurisprudenziale: da un lato infatti vi sono esigenze sempre più sentite di garanzia della sicurezza, in un mondo che si è riconosciuto negli ultimi decenni fragile ed esposto alla minaccia terroristica, mentre dall'altro lato vi è una innegabile restrizione e compressione primariamente dei diritti fondamentali alla riservatezza e alla protezione dei dati, con un forte impatto però anche su altri diritti parimenti riconosciuti e tutelati tanto a livello sovranazionale quanto nazionale.

Proprio su tale caso di studio questo lavoro vuole concentrarsi, per poter svolgere riflessioni più ampie riguardo alle sfide che l'impiego della conservazione e accesso ai dati comportano per il mondo del diritto e per la tutela dei diritti fondamentali in particolare: se, con riferimento alle criticità e alla rilevante discussione instauratasi in tale complessa materia, la risposta dell'ordinamento europeo e di taluni Stati membri occuperà l'analisi svolta nelle Parti II e III di questo elaborato, pare di grande importanza provvedere ad una analisi preliminare ed introduttiva, propedeutica alla maggiore e migliore comprensione della disamina successiva, in grado di fornire tutte le 'coordinate' contenutistiche e concettuali utili e necessarie. In questo Capitolo si vuole innanzitutto partire dalla ricostruzione del significato di Big Data, delle potenzialità e delle minacce che essi possono comportare, ponendo attenzione ai correlati e conseguenti interrogativi che il mondo del diritto è chiamato ad affrontare. Questa riflessione imporrà, conseguentemente, di svolgere una panoramica dei diritti fondamentali principalmente colpiti ed interessati dal fenomeno del progresso tecnologico e della digitalizzazione, che rappresentano quindi i parametri di riferimento per comprendere poi la successiva analisi del caso di studio individuato: in una prospettiva che dal generale procede verso il particolare, infatti, si vogliono poi fornire fondamentali indicazioni relative alla disciplina della *data retention* e del successivo – ma eventuale – accesso alle informazioni conservate. Il funzionamento, gli scopi e l'utilità di questo

[1] Tale termine è spesso affiancato alla parola "datificazione" – trasposizione italianizzata del termine inglese *datification* –, volta a designare "la centralità acquisita dai dati personali in ogni ramo dell'attività umana, suscettibile di essere appunto 'datificata' ovvero ridotta ad informazione e rappresentata mediante serie di dati; e in un'accezione più specifica indica la possibilità, attraverso analisi predittive, di estrarre nuove informazioni a carattere personale da dati già raccolti in precedenza", così R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, Giappichelli, 2019, p. 67.

strumento verranno così esaminati, ponendone in evidenza il potenziale impatto sui diritti e le libertà degli utenti, come premesse per l'analisi che occuperà le ulteriori Parti del presente lavoro.

Fornendo la cornice ed i riferimenti determinanti entro cui la successiva e più dettagliata disamina si dovrà muovere, si potranno quindi dare per acquisiti i concetti che formano il contesto ampio entro cui la *data retention* si inserisce e che vede protagonisti l'innovazione e mondo del diritto, la sfida rappresentata dai Big Data, lo sfruttamento dell'innovazione per finalità legittime e di interesse generale, nonché il contenuto, il significato e il rilievo che, anche mediante un processo evolutivo, hanno assunto i diritti alla riservatezza e alla protezione dei dati, minacciati sempre più dall'impatto delle nuove tecnologie e dal loro impiego da parte di soggetti privati o autorità pubbliche.

1. – Il mondo del diritto al tempo dei Big Data e della 'società dell'algoritmo': digitalizzazione, 'datizzazione' e diritti fondamentali

1.1. – Big Data: un difficile sforzo definitorio

Per quanto ampiamente impiegato nei più disparati ambiti, esiste ancora oggi una accesa discussione quanto all'origine del termine 'Big Data' ed al suo significato: non è possibile infatti rinvenire una spiegazione precisa ed univoca di tale locuzione, per quanto la stessa sia stata da più parti oggetto di uno sforzo definitorio[2]. Come riportato da Mayer-Schonberger e Cukier[3], un noto studio pubblicato da Doug Laney[4] e risalente al 2001 parlava di Big Data come di quell'insieme di dati caratterizzati da 'tre V' ovvero volume, velocità e varietà, mettendone quindi in evidenza le principali qualità, che possono anche essere sintetizzate in: "the huge volume, the speed at which it is collected, the variety of data, its relational nature – allowing linkages to be made to other data sets – and potentially exhaustive scope"[5]. Questa classificazione è stata poi ripresa nel 2012 da IBM[6], che alle tre V sopra richiamate ne ha aggiunta una quarta: veridicità; tale termine "includes questions of trust and uncertainty with regards to data and the outcome of analysis of the data"[7].

La definizione basata sulle 'V', per quanto molto conosciuta ed inizialmente ampiamente condivisa, è stata tuttavia messa in discussione nel corso del tempo: focalizzare una spiegazione del concetto di Big Data sugli elementi della quantità e qualità dei dati è infatti ben presto risultata limitativa ed incapace di rispecchiare la complessa realtà cui l'evoluzione tecnologica aveva portato. Il termine Big Data quindi è stato descritto non solo con riferimento alla dimensione enorme delle informazioni prodotte e raccolte – che, è bene precisarlo sin da ora, non sempre sono definibili come 'dati personali'[8] – ma anche tenendo

---

[2] Diebold ha cercato di individuare le origini e il primo utilizzo di questo termine, che può essere fatto risalire già agli anni '90, sebbene con una accezione piuttosto incerta e che, come si vedrà, ha conosciuto una significativa evoluzione nel corso del tempo (F. X. DIEBOLD, *On the origin(s) and development of 'Big Data': the phenomenon, the term and the discipline*, PIER Working Paper, 13, 2012).

[3] V. MAYER-SCHONBERGER, K. CUKIER, *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, traduzione di Roberto Merlini, Garzanti, 2013, p. 17 ss.

[4] D. LANEY, *3-D data management: controlling data volume, velocity and variety*, 2001, in https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

[5] Così Y. MCDERMOTT, *Conceptualising the right to data protection in an era of Big Data*, in *Big Data & Society*, 1, 2017, p. 4, richiamando la ricostruzione di R. KITCHIN, *Big data and human geography: opportunities, challenges and risks*, in *Dialogues in human geography*, 3, 2013.

[6] IBM, *What is big data? Bringing big data to the enterprise*, luglio 2013.

[7] J. S. WARD, A. BARKER, *Undefined by data: a survey of Big Data definitions*, in *arXiv Cornell University*, 2013, p. 1.

[8] Se si pensa all'enorme mole di dati raccolti da sensori o macchinari relativamente alla situazione del traffico o alle condizioni meteo, si può comprendere come tali dati non possano essere considerati 'dati personali'. I Big

conto delle procedure e degli strumenti che vengono impiegati per analizzare e 'processare' tali dati e che sono necessariamente differenti rispetto ai tradizionali metodi utilizzati per vagliare una quantità meno significativa di informazioni. Accogliendo questo più articolato ed ampio profilo definitorio, due ulteriori precisazioni e specificazioni risultano particolarmente utili: Ward e Barker, svolgendo una ricostruzione delle diverse categorizzazioni prodotte nel corso del tempo in materia, sono giunti a proporre una lettura complessiva del concetto di Big Data, capace di unire e comprendere tutti gli elementi ricorrenti nelle analisi svolte; così, "despite the range and differencies existing within each of the aforementioned definitions there are some points of similarity. Notably, all definitions make at least one of the following assertions: a) size: the volume of the datasets is a critical factor; b) complexity: the structure, behavior and permutations of the datasets is a critical factor; c) technologies: the tools and techniques which are used to process a sizeable or complex dataset is a critical factor. (..) An extrapolation of these factors would therefore postulate the following: big data is a term describing the storage and analysis of large and or complex data sets using a series of techniques including, but not limited to machine learining"[9]. Anche Mayer-Schonberger e Cukier hanno posto l'attenzione sul profilo della analisi e delle attività svolte sui e mediante i dati, anziché sulla natura – qualità e quantità – dei dati stessi, fornendo una spiegazione ritenuta più moderna dell'espressione di Big Data, che "designa delle cose che si possono fare solo su larga scala, per estrapolare nuove indicazioni o creare nuove forme di valore, con modalità che vengono a modificare i mercati, le organizzazioni, le relazioni tra cittadini e governi e altro ancora"[10]. Del resto, il legame tra le informazioni e le successive operazioni svolte per loro tramite[11] è uno degli aspetti evidenziati anche dalla riflessione della Commissione europea, che si è più volte interrogata sui Big Data, sul significato di tale espressione e sull'impatto rispetto ai diritti fondamentali: la Commissione si è espressa in questi termini, definendo i Big Data "una grande quantità

Data e le tecniche di Data Analytics possono inoltre, come si vedrà, impiegare anche dati anonimi che non sono più, pertanto, definibili come 'personali'. È tuttavia da precisare, sin da subito, come "the line between what is personal and non-personal data is increasingly difficult to draw for several reasons. (..) Big Data can increase the risk of re-identification, and in some cases, inadvertently re-identify large swaths of de-identified data all at once. The problem is magnified in the context of the Internet of Things, where inferences about our behaviors and actions can more easily be drawn from the capture of data from objects in our possession. (..) The world of Big Data feeds off this growing ambiguity about what is, and what is not, personally identifiable information", C. BENNETT, R. BAYLEY, *Privacy protection in the era of 'big data': regulatory challenges and social assessments*, in B. VAN DER SLOOT, D. BROEDERS, E. SCHRIJVERS (a cura di), *Exploring the boundaries of Big Data*, Amsterdam University Press, 2016. La distinzione e differenziazione tra dati personali, non personali e anonimi diviene, nel contesto digitale, sempre più sfumata.

[9] J. S. WARD, A. BARKER, *Undefined by data: a survey of Big Data definitions*, op. cit., p. 2. Sul punto, per approfondimenti sulle potenzialità rappresentate dal *machine learning* e dalla lettura aggregata di dati, si rinvia anche a A. DE MAURO, *Big Data Analytics. Analizzare e interpretare dati con il machine learning*, Apogeo, 2019; F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffré, 2019; ma anche, sulle potenzialità della Data Analytics, a: PARLAMENTO EUROPEO, *Big Data and Data Analytics. The potential for innovation and growth*, Briefing Paper, settembre 2016.

[10] V. MAYER-SCHONBERGER, K. CUKIER, *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, op. cit., p. 16.

[11] Come ben sintetizzato da Nunziante, dunque, "il valore delle informazioni non è intrinseco ma dato dalla capacità di organizzarle, analizzarle, misurarle e conseguentemente ricavarne fattori e decisioni. Ciò significa che le attività di analisi dei Big Data riposano su due piani: software e algoritmi per l'analisi, da un lato, e l'insieme dei dati raccolti e aggregati dall'altro", E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *MediaLaws. Law and Media working paper series*, 6, 2017. Anche il Garante Europeo per la Protezione dei Dati (European Data Protection Supervisor), nella sua Opinion 7/2015, dal titolo *Meeting the challenges of Big Data* (2015), ha definito i Big Data come "the practice of combining huge volumes of diversely sourced information and analysing them, using more sophisticated algorithms to inform decisions. Big Data relies not only on the increasing ability of technology to support collection and storage of large amounts of data, but also on its ability to analyse, understand and take advantage of the full value of data", mettendo quindi in luce l'importanza delle operazioni di trattamento dei dati che permettono di trarre un significato ulteriore e diverso rispetto alle informazioni di partenza e che rappresentano il vero valore aggiunto dei Big Data.

di tipi diversi di dati prodotti con un'alta velocità, da un grande numero di fonti di diverso tipo. La gestione di tali aggregati di dati richiede oggi nuovi strumenti e metodi, come processori potenti, software e algoritmi"[12]. Se si comprende dunque l'ampiezza di significato del termine in esame, si riesce a cogliere come "Big Data are not simply a bigger phenomenon to which one can simply apply well known rules. Big Data are ontologically different from 'small data' because of the use which is made of them and their potentialities for human decisions, cooperation and commerce"[13].

Partendo da queste considerazioni, ne deriva che lo sforzo ricostruttivo ed il percorso evolutivo che hanno portato a delineare il significato dei Big Data nelle sue molteplici sfaccettature, lungi dal rappresentare un arido esercizio definitorio fine a sé stesso, permettono di meglio comprendere le coordinate entro cui è chiamata a muoversi la riflessione anche e in particolar modo del mondo del diritto: nel tentativo di spiegare cosa sia questo insieme di produzione e analisi massiva dei dati, emerge con tutta evidenza la complessità della tematica, dai contorni e confini per certi versi ancora confusi e vaghi e, soprattutto, in continua evoluzione. La difficoltà di addivenire ad una definizione univoca riflette l'ampiezza del fenomeno e permette di costruire una immagine articolata del concetto di Big Data e di cogliere così la ricchezza sia delle diverse potenzialità che essi comportano che delle sfide e minacce connesse. Questo insieme di 'pro' e 'contro' viene riassunto in maniera estremamente efficace dalla Commissione europea: "questa tendenza mondiale [all'impiego e sfruttamento di Big Data e di connesse tecniche di analisi] presenta potenzialità enormi in vari campi: sanità, sicurezza alimentare, clima, uso efficiente delle risorse, energia, sistemi di trasporto intelligenti e città intelligenti. (..) L'accelerazione del processo di digitalizzazione dei servizi pubblici, giustificata dalla necessità di modernizzare, tagliare i costi e fornire servizi innovativi, apre nuove opportunità per ottimizzare l'archiviazione, il trasferimento, l'elaborazione e l'analisi dei dati. Allo stesso tempo, le notizie sull'utilizzo di tecnologie simili a fini di sorveglianza da parte di soggetti pubblici o privati possono alimentare preoccupazioni"[14].

Da tale sintesi risulta chiaro come leggere ed interrogarsi sui Big Data non possa che portare ad analizzarne luci e ombre, e di come entrambe tali dimensioni assumano grande rilievo e profondità.

1.2. – 'Asset' economico e 'motore' per lo sviluppo di algoritmi e sistemi di AI: le sconfinate potenzialità dei Big Data

Partendo dall'esame delle luci e dunque delle potenzialità che i Big Data rappresentano, non si può che prendere atto di come nel mondo della *digital economy*, dove i dati sono stati definiti "il nuovo petrolio"[15] e una vera e propria "materia prima, un input economico d'importanza vitale, utilizzato per creare una nuova forma di valore"[16], non sia più possibile fare a meno dei Big Data, intesi sia come mole

[12] COMMISSIONE EUROPEA, *Verso una florida economia basata sui dati*, COM(2014) 442 Final, p. 4. Similmente, il Parlamento Europeo ha sottolineato come i Big Data si riferiscano "alla raccolta, all'analisi e all'accumulo ricorrente di ingenti quantità di dati, compresi i dati personali, provenienti da una serie di fonti diverse, che sono oggetto di un trattamento automatizzato mediante algoritmi informatici e tecniche avanzate di trattamento dei dati, che usano sia informazioni memorizzate sia in streaming, al fine di individuare determinate correlazioni, tendenze e modelli (*Big data analysis*)", PARLAMENTO EUROPEO, *Risoluzione del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto* (2016/2225(INI)).

[13] V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the 'big data revolution'*, in *Concorrenza e mercato*, 23, 2016, *Numero speciale: Big Data e concorrenza*, a cura di F. DI PORTO.

[14] COMMISSIONE EUROPEA, *Verso una florida economia basata sui dati*, op. cit.

[15] Citazione mutuata da un articolo del 6 maggio 2017, apparso su THE ECONOMIST ONLINE, dal titolo *The world most valuable's resource is no longer oil, but data*.

[16] V. MAYER-SCHONBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, op. cit., p. 13.

ingente di dati che come processi e strumenti di analisi degli stessi; essi rappresentano opportunità di innovazione, progresso ed efficienza nei più svariati ambiti, aprendo a possibilità prima inimmaginabili: si pensi ai motori di ricerca che permettono di svolgere ricerche, di conoscere e creare collegamenti tra notizie, banche dati e risorse documentali; si pensi ai *social network* e alle infinite possibilità – non sempre positive, come si vedrà – che essi rappresentano sotto il profilo economico, sociale e lavorativo; si pensi ai mezzi di telecomunicazione rapidi e veloci; si pensi alle grandi risorse che l'*e-commerce* ormai mobilita e all'impatto dei Big Data e del Data Analytics sul marketing e sul modo stesso in cui il mercato agisce[17]; si pensi al progresso nel campo della ricerca scientifica – in svariati ambiti –, rappresentato dall'impiego di studi, anche statistici, svolti su grandi quantità di dati, persino nell'ambito della tutela della salute[18]; si pensi, ancora, all'impatto che i dati hanno avuto nella recente pandemia Covid-19: in taluni Stati (Cina e Corea del Sud ad esempio) sono state impiegate *app* che, proprio mediante la raccolta di dati di geolocalizzazione, come quelli derivanti dall'uso di GPS, hanno concesso di operare un più rapido tracciamento dei soggetti entrati a contatto con persone risultate positive al virus[19]. Persino nell'ambito dell'agricoltura e di un più efficace impiego delle risorse naturali i dati si

[17] L'analisi dei Big Data rappresenta una ricchezza per le aziende che possono ad esempio targettizzare i destinatari delle operazioni di marketing dei propri prodotti o servizi mediante una lettura aggregata di quei dati che noi quotidianamente e spesso inconsapevolmente produciamo. I c.d. *cookies*, i 'like' sui *social network*, i siti che visitiamo e i prodotti che visualizziamo sono tutte informazioni mediante le quali è possibile elaborare strategie indirizzate ai consumatori, anche sulla base di mezzi di profilazione. Come evidenziato da Soro, già Presidente dell'Autorità garante per la protezione dei dati personali italiana, "chi possiede il profilo dei consumatori indirizza la produzione commerciale verso specifici modelli di utenza, così da assecondarne i gusti ed insieme orientare selettivamente le scelte individuali. Dobbiamo chiederci quante delle nostre decisioni siano in realtà fortemente condizionate dai risultati che un qualche algoritmo ha selezionato per noi e ci ha messo davanti agli occhi", A. SORO, Garante per la protezione dei dati personali, *Big Data e Privacy. La nuova geografia dei poteri*, Atti del Convegno 30 gennaio 2017, p. 6. Sul punto, anche, S. EREVELLES, N. FUKAWA, L. SWAYNE, *Big Data consumer analytics and the transformation of marketing*, in *Journal of Business Research*, 2, 2016; P. VERHOEF, E. KOOGE, N. WALK, *Creating value with Big Data analytics*, Routledge, 2016; S. MATZ, *Using Big Data as a window into consumers' psychology*, in *Current Opinion in Behavioral Sciences*, 18, 2017.

[18] Un esempio di grande interesse, quanto di estrema attualità, vista la pandemia da Covid-19 in corso, risulta essere quello riportato da Mayer-Schonberger e Cukier: nel 2009 il mondo ha scoperto l'esistenza di un nuovo virus influenzale, l'H1N1; ebbene, "poche settimane prima che il virus finisse sulle prime pagine dei giornali, gli ingegneri del colosso informatico Google aveva pubblicato uno studio molto importante sulla rivista scientifica Nature (..). Gli autori spiegavano che Google era in grado di prevedere la diffusione dell'influenza invernale negli USA, non solo a livello nazionale ma anche a livello regionale e dei singoli Stati. Poteva costruire quella previsione in base all'oggetto delle queries (ricerche) effettuate dagli utilizzatori di Internet. Ricevendo ogni giorno più di tre miliardi di queries e archiviandole tutte, Google aveva a disposizione una mole infinita di dati. (..) L'idea era quella di identificare aree infette dal virus in base alle ricerche effettuate su Internet. (..) Il software predisposto ha scoperto una combinazione di 45 parole-chiave che, quando venivano impiegate insieme in un modello matematico, presentavano una forte correlazione tra la loro previsione e i dati ufficiali relativi all'intero territorio nazionale. Così nel 2009, il sistema previsionale di Google si è rivelato un indicatore più utile e tempestivo delle statistiche governative, strutturalmente in ritardo rispetto al dato reale, e ha fornito informazioni preziosissime alle autorità sanitarie. [Tale sistema] è costruito sui Big Data, ovvero la capacità di sfruttare le informazioni con modalità innovative per ricavarne utili indicazioni", V. MAYER-SCHONBERGER, K. CUKIER, *Big Data. Una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, op. cit., p. 14. Questo esempio è solo uno dei molti possibili impieghi dei Big Data nel settore della sanità così come in quello della ricerca scientifica.

[19] Queste tecnologie si sono rivelate particolarmente efficaci nel difficile quanto prioritario compito di arginare la diffusione del contagio, tanto che anche alle nostre latitudini si è aperto un ampio e vivace dibattito sulla opportunità di replicare tali strumenti. Pur non volendo entrare nel dettaglio delle discussioni e delle diverse posizioni espresse, è interessante notare come le valutazioni circa la possibilità e le modalità con cui sviluppare e gestire simili *app* siano state sin da subito accompagnate da forti perplessità e preoccupazioni quanto alla significativa invasività ed intrusione nella sfera privata che il controllo – mediante operazioni di raccolta e conservazione massiva – di dati di tracciamento degli spostamenti dei cittadini indubitabilmente comporta, insieme ai rischi di possibili abusi o utilizzi illegittimi delle informazioni ottenute per finalità sanitarie. Si sono così aperti profondi interrogativi circa la proporzionalità della misura rispetto allo scopo, di certo interesse generale e di forte urgenza, di prevenire e limitare la pandemia, a discapito però di diritti quali la riservatezza e la protezione dei dati.

sono rivelati materie prime di grande importanza: in questo ambito sono già infatti impiegati sistemi che, attraverso una lettura unitaria e una analisi di tutti i dati raccolti da dispositivi e sensori posti nei campi – o in alcuni casi addirittura mediante l'uso di droni –, sono in grado di stabilire con precisione lo stato del terreno, se esso necessiti di irrigazione, di diserbanti o di fertilizzanti, permettendo quindi all'agricoltore un quadro dettagliato della situazione delle proprie coltivazioni e un ricorso più efficiente ed oculato di pesticidi, concimanti o acqua, consentendo un risparmio in termini economici ma anche e soprattutto di risorse idriche e di potenziali sostanze inquinanti[20]. In questo senso i dati possono essere impiegati per consentire uno sviluppo maggiormente sostenibile in un ambito tanto delicato e determinante in termini di impiego di risorse e di impatto ambientale quale l'agricoltura.

Non è un caso, infatti, che in Paesi come la Cina e la Corea del Sud, nei quali i sistemi di tracciamento sono stati ampiamente impiegati senza grandi restrizioni e senza un ampio dibattito sull'impatto per i diritti fondamentali, la disciplina della *data protection* risulti meno sviluppata e meno garantista rispetto al regime di tutela dei dati personali istituito nel Vecchio Continente. La delicatezza del tema e dei diritti ed interessi in gioco hanno portato anche molte Istituzioni ed autorità europee a pronunciarsi e a fornire direttive a Governi e Parlamenti nazionali quanto ai rischi e alle possibili soluzioni delle criticità legate all'impiego di strumenti di tracciamento dei contagi. Così il Comitato europeo per la protezione dei dati (un organo europeo indipendente, composto dai rappresentati delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati, cui è attribuito il compito di promuovere la cooperazione tra le autorità competenti in materia di protezione dei dati nell'UE e di fornire indicazioni e pareri sulla corretta e coerente applicazioni delle norme sulla *data protection*) ha elaborato la *Dichiarazione sul trattamento di dati personali nel contesto dell'epidemia da Covid-19*, 19 marzo 2020; la *European Agency for Fundamental Rights* ha predisposto lo studio *Coronavirus pandemy in the EU. Fundamental rights implications* (20 marzo 2020), nel quale particolare attenzione è stata posta alle conseguenze che l'impiego di strumenti di tracciamento comportano rispetto ai diritti alla riservatezza e alla protezione dei dati. Per una ampia analisi di questa complessa tematica, si legga, tra i tanti: M. FASAN, *La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del coronavirus*, in *BioLaw Journal – Instant Forum: Diritto, diritti ed emergenza ai tempi del Coronavirus*, 20 marzo 2020; G. F. ITALIANO, *Raccogliere, analizzare e prevedere. L'importanza dei dati al tempo del Covid-19*, in *Luiss Open – Focus Covid*, 7 aprile 2020; G. TROPEA, *Il contact tracing digitale e l'epidemia: sindrome cinese?*, in *LaCostituzione.info*, 9 aprile 2020. Per alcune riflessioni sul bilanciamento tra i diversi diritti in gioco: F. P. MICOZZI, *Le tecnologie, alla protezione dei dati e l'emergenza coronavirus: rapporto tra il possibile e il legalmente consentito*, in *BioLaw Journal*, 15 marzo 2020 e nella stessa rivista M. FARINA, *La data protection ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, 20 marzo 2020; G. BISCONTINI et al., *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *federalismi.it – Osservatorio emergenza Covid-19*, 23 marzo 2020; G. DELLA MORTE, *La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, in *SIDI Blog*, 30 marzo 2020; G. DE MINICO, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *LaCostituzione.info*, 1 aprile 2020; S. CRESPI, *Applicazione di tracciamento Immuni tra normative nazionale e diritto UE in materia di protezione dei dati personali*, in *Freedom, Security & Justice*, 2, 2020, pp. 20-44. In ambito europeo ed internazionale: H. VAN KOLFSCHOOTEN et al., *Covid-19 and privacy in the EU: a legal perspective on contact tracing*, in *Contemporary Security Policy*, 3, 2020; R. KITCHIN, *Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of Covid-19*, in *Space and Polity*, 3 luglio 2020; A. DUBOV et al., *The value and ethics of using technology to contain the Covid-19 epidemic*, in *The American Journal of Bioethics*, 7, 2020; J. LI, X. GUO, *Covid-19 contact-tracing apps: a survey on the global deployment and challenges*, in *ArXiv*, 2020; H. CHO, D. IPPOLITO, Y. YU, *Contact tracing mobile apps for Covid-19: privacy considerations and related trade-offs*, in *arXiv*, 2020; A. GUINCHARD, *Our digital footprint under Covid-19: should we fear the digital contact tracing app?*, in *International Review of Law, Computers & Technology*, 15 luglio 2020; ancora, a livello internazionale è interessante lo studio elaborato dalla Organizzazione per la cooperazione e lo sviluppo economico (OECD), *Tracking and tracing COVID: protecting privacy and data while using apps and biometrics*, 2020.

[20] Sul punto si rimanda, per approfondimenti, a: K. BRONSON, I. KNEZEVIC, *Big Data in food and agriculture*, in *Big Data and Society*, 1, 2016; EUROPEAN COMMISSION, *Industry 4.0 in agriculture: focus on IoT aspects*, 2017; M. CAROLAN, *Publicising food: Big Data, precision agriculture and co-experimental techniques of addition*, in *Sociologia Ruralis*, 2, 2017; M. TRIPOLI, J. SCHIMDHUBER, *Emerging opportunities for the application of blockchain in the Agri-food Industry*, in *FAO Issue Paper*, 2018; J. P. BELAND et. Al., *Big Data for agri-food 4.0: application to sustainability management for by-products supply chain*, in *Computers in Industry*, 1, 2019.

I Big Data, come nella maggior parte degli esempi di utilizzo sopra riportati, debbono essere connessi e letti congiuntamente ad altri due termini, tra loro associati: "Intelligenza Artificiale"[21] (d'ora in avanti AI) e algoritmi. I Big Data infatti sono impiegati per l''addestramento' di strumenti di AI: questi si 'nutrono' ed imparano a funzionare proprio mediante e sulla base della enorme mole di dati che, tramite gli algoritmi[22], istruiscono l'AI a diventare sempre più 'intelligente' ed efficiente. I Big Data dunque hanno contribuito – e continuano a farlo – alla evoluzione dell'AI: "i Big Data, insieme alle reti neurali [cioè un metodo di apprendimento e training dell'AI che tende a riprodurre il funzionamento del cervello umano] hanno generato un nuovo paradigma nel modo di programmare l'AI: non più un approccio logico-deduttivo, dove si pone un problema, lo si formalizza matematicamente e poi lo si traduce in un algoritmo, ma un approccio statistico, dove la macchina impara direttamente dai dati. Ed è questo cambiamento che ha portato a straordinari successi nel campo dell'AI"[23].

Ecco quindi che la commistione delle enormi potenzialità dei Big Data con l'AI ha prodotto strumenti preziosi e ormai insostituibili che pervadono i più disparati ambiti del vivere sociale e vengono impiegati per i più diversi scopi: nell'ambito dell'assistenza sanitaria, ad esempio, nuovi strumenti applicati alla diagnostica hanno la capacità di consentire una diagnosi più precisa ed oggettiva, fondata sui dati ed input forniti, rappresentando un valido supporto – e non un sostituto – per il medico[24]; i sistemi di

---

[21] La Commissione europea, nel *Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, pubblicato il 19 febbraio 2020 ha definito l'AI come "un insieme di tecnologie che combina dati, algoritmi e potenza di calcolo". Anche con riferimento all'Intelligenza Artificiale, similmente a quanto avvenuto per i Big Data, non esiste una definizione universalmente condivisa: Kaplan la descrive come "la capacità di fare generalizzazioni appropriate in modo tempestivo e su una base dati limitata. Tanto più è vasto il campo di applicazione, tanto più rapidamente vengono tratte le conclusioni con informazioni minime, tanto più intelligente è il comportamento osservato" (J. KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, 2017); ancora l'AI è stata definita come "a program which in an arbitrary world will cope not worse than a human", D. DOBREV, *A definition of Artificial Intelligence*, in *arXiv*, 2004. Floridi e Taddeo parlano di AI come "a growing resource of interactive, autonomous, self-learning agency, which enables computational artifacts to perform tasks that otherwise would require human intelligence to be executed successfully (..). On the one hand, AI is fueled by data and therefore faces ethical challenges related to data governance, including consent, ownership and privacy. On the other hand, AI is a distinct form of autonomous and self-learning agency and thus raises unique ethical challenges", M. TADDEO, L. FLORIDI, *How AI can be a force for good*, in *Science*, 24 agosto 2018, p. 751. Simoncini e Suweis fanno riferimento alla "capacità di macchine di riprodurre o attuare operazioni tipiche delle funzioni cognitive umane, quali per esempio l'apprendimento, il *problem solving*, il riconoscimento di volti, la traduzione del linguaggio etc.", A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019. Per approfondimenti, si rimanda anche a: E. ANCONA, *Soggettività, responsabilità, normatività 4.0. Profili filosofico-giuridici dell'intelligenza artificiale*, in *Rivista di Filosofia del Diritto*, 1, 2019; A. D'ALOIA (a cura di), *Intelligenza artificiale (Contributi del Convegno su 'Intelligenza artificiale e diritto. Come regolare un mondo nuovo', Parma, 12 ottobre 2018),* in *BioLaw Journal*, 1, 2019.

[22] Per chiarezza e in estrema sintesi, "da un punto di vista tecnico, gli algoritmi sono semplici metodi matematici che esprimono risultati entro una quantità limitata di spazio e tempo e in un linguaggio formale definito, trasformando gli input, costituiti da dati, in output sulla base di un processo di calcolo specificato; da un punto di vista sociale, tali tecnologie costituiscono processi decisionali automatizzati il cui percorso decisionale è stato programmato da uno sviluppatore. (..) In altre parole, gli algoritmi esprimono risultati che, seppur determinati dal loro codice, costituiscono determinazioni soggettive fornite da parte di sistemi automatizzati", G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy digitale*, Giuffré, 2019, p. 450.

[23] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, op. cit., p. 92.

[24] Sul punto, si legga A. SPINA, *La medicina degli algoritmi: intelligenza artificiale, medicina digitale e regolazione dei dati personali,* in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018, p. 319; M. RATH, B. PATTANAYAK, *Technological improvement in modern health care applications using IoT and proposal of novel health care approach*, in *International Journal of Human Rights in Healthcare*, 2, 2019; ma anche la Comunicazione della Commissione europea *on enabling the digital transformation of health and care in the Digital Single Market: empowering citizens and building a healthier society*, SWD(2018)126, 2018.

riconoscimento facciale consentono in maniera automatica di confrontare fotografie digitali contenute in un database con le immagini – ovvero i dati biometrici di un soggetto – riprese in tempo reale da una telecamera e poter così determinare, rapidamente, se vi siano delle corrispondenze: questo sistema è sempre più impiegato dalle autorità di *law enforcement* per controllare e tutelare la sicurezza e l'ordine pubblico in occasione di eventi sportivi e concerti o in luoghi considerati sensibili a possibili attacchi terroristici o particolarmente affollati e garantire così una più efficace azione di repressione e prevenzione[25]; ancora, strumenti di AI, algoritmi e Big Data vengono impiegati sempre di più dalle pubbliche amministrazioni, che stanno conoscendo un forte percorso di digitalizzazione: diversi strumenti vengono così impiegati per garantire maggiore velocità ed efficienza e per automatizzare le più diverse operazioni. È esemplificativo l'impiego di meccanismi automatizzati di controllo delle frodi, soprattutto in ambito fiscale, che si basano su una lettura aggregata di tutti i dati a disposizione delle pubbliche amministrazioni – e non solo –, consentendo la determinazione della correttezza e veridicità delle dichiarazioni fornite[26].

Tutti questi strumenti, che pure possono sembrare fantascientifici e futuribili, sono già realtà operativa: la frontiera in rapida espansione della c.d. Internet of Things (IoT)[27] sta aprendo nuovi ed

[25] Per approfondimenti sulle potenzialità che la sofisticata tecnica del riconoscimento facciale comporta nonché sui profili tecnici, si rimanda a: R. DUCATO, *Il riconoscimento facciale tra rischi di 'mitridatizzazione sociale' e prospettive di regolamentazione*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, in corso di pubblicazione. Come si vedrà in seguito, tale tecnologia è foriera anche di notevoli dubbi e timori quanto all'impatto sui diritti fondamentali, anche in considerazione della sua non infallibilità e delle problematiche connesse all'impiego di algoritmi che, lo si dirà nei successivi paragrafi, non sono neutri ed anzi si aprono alla presenza di *bias* e 'pregiudizi'.

[26] Si fa riferimento, ad esempio, al sistema recentemente adottato dall'Olanda, c.d. SyRI (Systeem Risico Indicatie): tale strumento di *risk management* è utilizzato da diverse autorità pubbliche, tra cui il Social Affairs and Employment Inspectorate. SyRI può essere definito come "a tool aimed at detecting different types of fraud by matching data collected and held by different government agencies involved in the SyRI project. Similarly to the Australian Robodebt, the use of SyRI in the area of welfare fraud is precisely embodied in the law, namely in Article 64 and 65 of the Dutch Work and Income act (SUWI). The data processed by SyRI include personal data and information concerning employment, administrative sanctions and penalties, personal debt, education, housing, pension, healthcare and tax history", L. SCARCELLA, *Wrong and biased: automized welfare called to the stand*, in corso di pubblicazione; si legga anche V. GANTCHEV, *Data protection in the age of welfare conditionality: respect for basic rights or a race to the bottom?*, in *European Journal of Social Security*, 1, 2019; S. RANCHORDAS, *Public law and technology: automating welfare, outsourcing the State*, in *International Journal of Consistutional law Blog*, 15 gennaio 2020. Similmente anche altri Stati hanno impiegato sistemi che, mediante l'utilizzo di una enorme mole di dati, permettono di individuare casi di frode fiscale o di furto di identità: ne sono esempio il c.d. Robodebt ("*Online Compliance System*"), impiegato dal Governo autraliano a partire dal 2016 e finalizzato ad individuare in maniera totalmente automatizzata discrepanze ed irregolarità tra le informazioni fornite dai cittadini a Centrelink, l'agenzia nazionale che si occupa della riscossione di tasse riguardanti l'area del welfare, e i dati a disposizione dell'Australian Taxation Office (si rimanda a T. CARNEY, *The new digital future for welfare: debts without legal proofs or moral authority?*, in *UNSW Law Journal Forum*, 1, 2018); o ancora il c.d. sistema Aadhaar, creato dal Governo indiano, che utilizza i dati biometrici dei propri cittadini, raccolti e memorizzati in un enorme database centralizzato, al fine di individuare furti o duplicazione di identità e conseguenti richieste illecite di accesso a servizi di welfare, quali sussidi o prestazioni sanitarie, così da meglio controllare la corretta allocazione di risorse pubbliche a soggetti realmente bisognosi ed evitare errori e sprechi. Su questo sistema sia concesso il rinvio a G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti*, in *DPCE Online*, 2, 2019.

[27] "Il concetto di Internet degli oggetti (IoT) si riferisce a un'infrastruttura nella quale miliardi di sensori incorporati in dispositivi comuni di uso quotidiano ("oggetti" a sé stanti oppure oggetti connessi ad altri oggetti o persone) sono progettati per registrare, trattare, conservare e trasferire dati e, essendo associati a identificativi univoci, interagiscono con altri dispositivi o sistemi che sfruttano le capacità di collegamento in rete. Dal momento che l'IoT si basa sul principio del trattamento esteso dei dati attraverso tali sensori, che sono progettati per comunicare con discrezione e scambiarsi dati continuamente, esso è strettamente connesso alle nozioni di 'pervasività' e 'onnipresenza' dell'informatica", in questi termini viene definita l'IoT dal Gruppo di Lavoro Art. 29, nel *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet of Things*, 2014 (WP223). In tale documento, il Gruppo di Lavoro Art. 29 (un organo indipendente istituito sulla base dell'art. 29 della Direttiva 95/46/CE, al quale era attribuita la funzione di controllo e analisi di questioni connesse alla protezione della vita privata e alla tutela dei

impensabili orizzonti sotto il profilo della *e-Health* e delle Smart Cities, puntando, nel primo caso, a migliorare la qualità di vita di malati cronici che possono essere tenuti sotto controllo e monitorati, anche a distanza, mediante i dati continuamente forniti e condivisi con operatori sanitari da dispositivi indossabili (*wearable devices*), mentre nel secondo esempio tali tecnologie mirano ad ottimizzare la qualità di vita nelle città, la loro sostenibilità ambientale e la loro sicurezza[28] proprio mediante l'elaborazione di dati prodotti, raccolti, trattati ed analizzati grazie a sensori, telecamere o droni.

Dalla analisi, seppur veloce e sintetica, sino a qui svolta, si può comprendere come il fenomeno dei Big Data, alla base dell'affermarsi di tecniche sempre più sofisticate di AI e della nascita della c.d. 'società dell'algoritmo'[29], abbia aperto a realtà ed opportunità enormi e di grande impatto, mettendo a disposizione strumenti efficaci per risolvere alcune delle problematiche più complesse che la società moderna si trova ad affrontare[30], quali la garanzia di uno sviluppo sostenibile o la tutela della sicurezza dinnanzi a fenomeni di terrorismo internazionale.

1.3. – I diritti fondamentali dinnanzi ai Big Data: pericoli e rischi

Tutte queste 'luci' e potenzialità certamente positive e dall'impatto dirompente in svariati settori, non devono però abbagliare lo sguardo: in un contesto così complesso, spesso in rapida ed incontrollabile evoluzione, risulta anzi più che mai necessario prendere consapevolezza delle molte ombre che sono intrinsecamente legate alla produzione e allo sfruttamento massivo di dati e al loro

---

dati personali, poi sostituito dal Comitato europeo per la protezione dei dati a seguito dell'entrata in vigore del Reg. 2016/679 c.d. GDPR, di cui si parlerà in seguito) si è ampiamente interrogato sulle diverse minacce e problematiche legate allo sviluppo della tecnologia IoT, che tocca i più svariati ambiti, dalla domotica alla *e-health*. Per approfondire il funzionamento, le grandi opportunità ed i rischi legati allo sviluppo dell'IoT, si rimanda, tra i tanti, a: R. WEBER, *IoT: new security and privacy challenges*, in *Computer Law and Security Report*, 26, 2010; J. STANKOVIC, *Research directions for the IoT*, in *Internet of Things Journal*, 1, 2014; U. PAGALLO, M. DURANTE, S. MONTELEONE, *What is new with the IoT in privacy and data protection? Four legal challenges on sharing and control in IoT*, in R. LEENES, R. VAN BRAKEL, S. GUTWIRTH, P. DE HERT (a cura di), *Data protection and privacy: (in)visibilities and infrastructures*, Springer, 2017; C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, op. cit., p. 669 e nello stesso volume anche F. GIOVANELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, p. 1231. Anche la Commissione europea si è interrogata sul tema, cercando di trovare un equilibrio tra esigenze di tutela dei diritti fondamentali da un lato e la riconosciuta importanza di sostenere innovazione e progresso dall'altro: COMMISSIONE EUROPEA, *Advancing the IoT in Europe*, SWD(2016)110final, 2016.

[28] Lo sviluppo di tecnologie IoT applicate alle città, alla gestione del traffico, alla misurazione e controllo della qualità dell'aria, portano alla predisposizione di soluzioni che, proprio grazie alla lettura aggregata dei dati derivanti da telecamere e sensori, risultano in grado di coniugare efficacia e sostenibilità ambientale. La Commissione europea si è da tempo interrogata su tale delicata tematica, a partire dal 2012 con la *Communication on smart cities and communities* (COM(2012)4701). Per una ricostruzione delle potenzialità legate allo sviluppo di Smart Cities e all'impatto positivo per ambiente e qualità della vita, si rinvia a V. SCUOTTO, A. FERRARIS, S. BRESCIANI, *IoT: applications and challenges in smart cities*, in *Business Process Management Journal*, 2, 2016; T. KIM, C. RAMOS, S. MOHAMMED, *Smart city and IoT*, Elsevier, 2017; O. SCHWARZ-HERION, *The role of Smart Cities for the realization of the sustainable development goals*, in A. OMRAN, O. SCHWARZ-HERION, *Sustaining our environment for better future*, Springer, 2020.

[29] M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, op. cit., p. 334.

[30] Del resto la stessa Commissione europea ha riconosciuto come l'AI, i Big Data e la 'società dell'algoritmo' cambieranno le nostre vite "migliorando l'assistenza sanitaria, aumentando l'efficienza dell'agricoltura, contribuendo alla mitigazione dei cambiamenti climatici e all'adattamento ai medesimi, miglioranza l'efficienza dei sistemi di produzione, aumentando la sicurezza dei cittadini europei e in molti altri modi che possiamo solo iniziare a immaginare", COMMISSIONE EUROPEA, *Libro Bianco sull'intelligenza artificiale*, op. cit., p. 1. Non è un caso che Big Data e AI siano considerati "fattori abilitanti fondamentali" per conseguire diversi obiettivi dell'UE, quali il Green Deal e dunque uno sviluppo economico e sociale sostenibile (*Libro Bianco*, p. 2).

impiego mediante strumenti di AI. Osservando con attenzione, infatti, emerge come tutte le potenzialità che la progressiva e sempre più pervasiva 'datizzazione' – dunque la continua e incessante creazione di dati e informazioni – produce, nascondono in realtà anche grandi insidie. Gli stessi strumenti in grado di determinare effettivi positivi e significativi miglioramenti possono essere impiegati, più o meno volontariamente, anche per finalità che hanno invece la capacità di impattare negativamente sulla nostra società, sulla sua democraticità e sulla garanzia effettiva dei diritti fondamentali, trasformandosi in pericolosi meccanismi di controllo e sorveglianza, dagli effetti dirompenti.
Ed è proprio dalla 'datizzazione' che bisogna partire per poter comprendere l'origine e l'entità dei rischi e dei pericoli del mondo digitale, che assumono poi, mediante gli strumenti di AI e gli algoritmi, una dimensione ed una profondità ancora maggiore: è infatti proprio "la disponibilità di grandi quantità di dati e di elaboratori sempre più veloci a rendere possibile che tecniche già note siano in grado di estrarre in maniera più affidabile l'informazione necessaria, a separare il segnale utile dal rumore, così da generare algoritmi sempre più intelligenti. Ma perché proprio oggi abbiamo a disposizione questa enorme quantità di dati, che è alla base del successo di molti sistemi di Intelligenza Artificiale? Da dove nascono questi dati? Oltre ai dati disponibili dalla digitalizzazione di molti documenti, in realtà è proprio ognuno di noi a generare ogni giorno una quantità notevole di dati"[31]. Usando una immagine affascinante ed efficace, una delle prime minacce può essere individuata proprio nel fatto che "sta accadendo in Internet quanto capitava a Pollicino, che nell'attraversare il bosco lasciava cadere a terra briciole di pane per ritrovare la via di casa. Anche noi durante la navigazione lasciamo cadere frammenti della nostra identità, che raccolti e riorganizzati da chi verrà dopo comporranno il patrimonio virtuale della sua attività d'impresa, cioè gioveranno fondamentalmente a chi li ha raccolti, non alla persona alla quale i dati appartenevano"[32].

1.3.1. – Dalle rivelazioni di Snowden al caso Cambridge Analytica: le minacce della 'profilazione' e della 'sorveglianza massiva'

In questo nostro essere divenuti, oltre che soggetti in carne ed ossa, anche milioni di dati[33], il pericolo è quello di perdere il controllo delle informazioni che 'lasciamo dietro di noi' e di non riuscire ad esercitare alcun potere su di esse e sul loro impiego da parte dei soggetti che li raccolgono e trattano, correndo anzi in ultima analisi il rischio che siano proprio questi nostri dati e le notizie che forniamo su di noi a rappresentare uno strumento di controllo delle nostre vite. Se inizialmente, infatti, non risultava chiaro chi e come fosse interessato a conservare ed impiegare i dati prodotti dal quotidiano utilizzo di servizi di telecomunicazione, app e *devices* – e forse neppure pensavamo fosse utile ed importante saperlo – alcuni eventi, definiti come vere e proprie 'rivelazioni', hanno contribuito a svelare il lato più oscuro e pericoloso dei Big Data e dei sistemi di AI: due episodi fondamentali di tale 'percorso' verso una maggiore consapevolezza delle minacce che si nascondono dietro alle innumerevoli potenzialità di cui si è prima parlato, possono essere individuati nello scandalo Snowden e nel caso Cambridge Analytica. Questi due avvenimenti che hanno segnato la storia della modernità hanno permesso per la prima volta e su larga scala di comprendere quanto tutte le 'tracce digitali' che ognuno di noi produce

[31] G. F. ITALIANO, *Intelligenza artificiale: passato, presente, futuro*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, op. cit., p. 215. Non bisogna dimenticare poi come ai dati prodotti da tutti noi utenti del Web e di servizi digitali, si debba sommare la quantità sempre più considerevole di dati prodotta dalle autorità pubbliche – ad esempio le pubbliche amministrazioni – nonché le informazioni che ad oggi sono addirittura sviluppate da oggetti (si fa riferimento alla IoT e ai dispositivi in grado di creare dati).
[32] G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto Pubblico*, 1, 2019, p. 90.
[33] Usando le parole di V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2, 2018.

siano controllate, raccolte, sistematizzate ed utilizzate per finalità diverse da soggetti pubblici e privati e quanto tali informazioni ci definiscano e consentano di ricreare un vero e proprio profilo delle nostre abitudini, preferenze, stili di vita e opinioni, anche politiche, con profonde conseguenze non solo sul singolo individuo bensì sull'intera società. Seppure in estrema sintesi, questi due eventi meritano pertanto di essere analizzati, per la rilevanza, anche mediatica, che hanno assunto e soprattutto per gli effetti che hanno prodotto: la consapevolezza dei rischi per la riservatezza e protezione dei dati ma anche per altri diritti fondamentali, quali la libertà di espressione e di associazione, capaci di incidere sulle stesse fondamenta su cui poggiano le democrazie odierne, ha provocato una reazione da parte del mondo delle istituzioni nonché della società civile, con conseguenze dirette e tangibili sostanziatesi in interventi legislativi, prese di posizione politiche, azioni da parte di ONG dinnanzi ad autorità giudiziarie, nazionali e sovranazionali, innescando così un lento ma importante percorso di cambiamento.

Il caso Snowden ha portato, ad esempio, nel contesto statunitense, all'approvazione di nuove regole nell'ambito dei poteri e delle prerogative affidate alle agenzie di intelligence, di cui si parlerà più approfonditamente anche in seguito: fattore scatenante furono proprio le rivelazioni di uno dei più noti 'whistleblower' della storia, Edward Snowden, ex dipendente di un *contractor* esterno fornitore di servizi per la US National Security Agency (NSA) ovvero l'agenzia di intelligence nazionale che si occupa delle operazioni di sorveglianza aventi ad oggetto attività oltre i confini nazionali[34]. Apparse in un articolo del 5 giugno 2013 sul giornale The Guardian[35], le informazioni e i documenti classificati rilasciati da Snowden – ancora oggi ricercato dagli USA, accusato di spionaggio e furto di proprietà governative – portavano alla luce i sistemi di sorveglianza segreta massiva posti in essere dalla NSA e basati proprio sulla raccolta, conservazione e accesso generalizzato a dati provenienti da telecomunicazioni per, da e negli USA, talvolta sfruttando atteggiamenti collaborativi da parte dei fornitori di servizi, c.d. Over the Top (OTT), quali i colossi del mercato digitale Google e Facebook, talaltra impiegando programmi di accesso sistematico e in tempo reale ai dati[36]. Strumenti di controllo

[34] Negli USA le attività di intelligence, riguardanti cioè principalmente la prevenzione e lotta alle minacce provenienti dall'esterno e quindi al di fuori dei confini nazionali, sono attribuite alla NSA (National Security Agency), che è dunque distinta dalla FBI (Federal Bureau of Investigation) che invece si occupa delle operazioni di 'domestic surveillance'. La NSA dunque, operando sulla base del Patriot Act del 2001, non ha quali obiettivi e target i cittadini statunitensi – rispetto ai quali, altrimenti, le operazioni di sorveglianza dovrebbero rispettare il Quarto Emendamento che richiede la presenza di un mandato giudiziario, di una 'probable cause' e che lo scopo perseguito sia la lotta al crimine – e dovrebbe occuparsi solo di operazioni di intelligence non legate alla lotta alla criminalità 'comune' bensì alle minacce alla sicurezza nazionale, quali ad esempio attentati terroristici. Come evidenziato da Serena, è tuttavia vero che i sistemi di sorveglianza impiegati dalla NSA si sono ben presto estesi anche all'ambito di azione dell'FBI, così che "those searches and the data obtained thereby, have been used to prosecute common criminals, from murderers to drug dealers, who should have been granted the protection of the Fourth Amendment. (..) It is a clear example of what we might term the 'natural' tendency of the executive to expand its powers beyond the limits of the law", A. SERENA, *The leviathan, the chains, the lock: dynamics of power in the digital surveillance state*, in *MediaLaws. Law and media Working Paper Series*, 8, 2017.

[35] Per approfondimenti si rimanda a G. GREENWALD, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Hamish Hamilton, 2014; nonché a E. SNOWDEN, *Errore di Sistema*, Longanesi (traduzione italiana a cura di Netphilo Publishing), 2019.

[36] "Date le modalità di funzionamento del sistema e la tipologia dei dati richiesti, soprattutto se considerati nell'ambito delle fonti utilizzate per ottenerli, emerge con evidenza che si è in presenza di un formidabile sistema di controllo potenzialmente a scala mondiale", così F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *federalismi.it*, 13, 2013. Sul tema si legga anche D. BENDER, *What you need to know about NSA mass acquisition of telephony metadata*, in *Computer and Internet Lawyer*, 9, 2013. Ampiamente e accuratamente sui programmi di sorveglianza di massa utilizzati dagli Stati Uniti ed emersi in occasione del c.d. *datagate*, ovvero della rivelazione di informazioni secretate riguardanti le attività di intelligence statunitense: C. BOWDEN, *The US Surveillance programmes and their impact on EU citizens' fundamental rights*. *Note to the European Parliament*, 2013; F. BIGNAMI, G. RESTA, *Transatlantic privacy regulation: conflict and cooperation*, in *Law and contemporary problems*, 4, 2015; L. P. VANONI, *Il IV emendamento della Costituzione americana tra terrorismo internazionale e datagate: security v. privacy*, in *federalismi.it*, 1, 2015; I. TOURKOCHORITI, *The transatlantic flow of data and the national security exception in*

simili, finalizzati a garantire la sicurezza ed utilizzati principalmente per scopi di prevenzione, indagine e repressione di reati, sono stati poi individuati e svelati in molti altri Stati, anche nel Continente europeo, quali Regno Unito, Germania e Francia. Benché lo scopo di garanzia della sicurezza rappresenti un indubbio interesse generale, fortemente percepito come essenziale soprattutto a seguito degli attentati terroristici che hanno scosso negli ultimi decenni gli USA e l'Europa, il carattere massivo dei programmi di sorveglianza impiegati comportava un controllo su tutti gli utenti, indipendentemente da qualsiasi sospetto o connessione con reati, traducendosi così in forme di controllo illimitate e pervasive[37]. Uno dei portati di queste rivelazioni è da individuarsi innanzitutto nell'intervento normativo che ha condotto alla approvazione negli USA del USA Freedom Act del 2015 (Pub. L. No. 114-23, 2 giugno 2015) che ha ridisegnato profondamente i poteri assegnati alle agenzie di intelligence, predisponendo restrizioni e salvaguardie – seppur ancora discusse sotto il profilo della proporzionalità ed efficacia –; ulteriore conseguenza di tali scoperte, inoltre, è rappresentata dal noto caso *Schrems*, deciso dalla Corte di giustizia dell'UE, di cui si parlerà ampiamente nella Parte II: tale procedimento giudiziario ha preso avvio proprio dalle vicende originate dalle rivelazioni di Snowden e dal loro impatto sulla disciplina dell'UE, con particolare riferimento al livello di tutela della riservatezza e protezione dei dati garantiti alle informazioni prodotte e raccolte nel territorio dell'Unione ma trasferite, conservate e trattate negli USA.

Mentre le rivelazioni di Snowden hanno aiutato a comprendere come i dati derivanti dalle telecomunicazioni o dalla nostra navigazione sul Web e sui *social network* siano raccolti, vagliati e trattenuti da autorità pubbliche per finalità certamente di interesse generale ma in maniera massiva ed indiscriminata, senza che siano posti limiti o controlli effettivi agli ampi poteri di accesso attribuiti ad agenzie di intelligence o autorità di *law enforcement*, il caso Cambridge Analytica ha portato alla luce un ulteriore fenomeno, altrettanto preoccupante: l'impiego dei dati da parte di soggetti privati per influenzare le nostre preferenze e le informazioni cui abbiano accesso, incidendo così sulla nostra capacità di conoscere, giudicare e decidere. La società di consulenza e marketing Cambridge Analytica, infatti, come messo in luce dagli articoli pubblicati ancora una volta sui quotidiani The Guardian[38] e New York Times[39] nel marzo del 2018, aveva utilizzato una enorme mole di dati sottratti illegalmente a Facebook per profilare gli utenti, le loro idee ed orientamenti politici allo scopo di predisporre messaggi pubblicitari mirati, facendo circolare *fake news* mediante profili *bot* e incidendo così, anche mediante una selezione di informazioni e notizie specificamente targettizzate a seconda dell'utente, sulle decisioni e sui convincimenti personali. Queste operazioni avrebbero avuto, secondo i giornalisti, un impatto decisivo o comunque estremamente rilevante sia sull'esito delle elezioni presidenziali americane che sul voto relativo alla Brexit (uscita dell'UE) nel Regno Unito. Le rivelazioni di alcuni

the European data privacy regulation: in search for legal protection against surveillance, in *University of Pennsylvania Journal of International Law*, 3, 2015; M. BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti 'violabili' in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 3, 2016. Per una ricostruzione ampia, si rimanda a: R. A. MILLER, *Privacy and Power: a transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, 2017.

[37] Le considerazioni che hanno spinto Snowden ad infrangere la legge e rivelare al mondo i sistemi impiegati dalla NSA e da altre agenzie di intelligence si basano essenzialmente su due assunti: innanzitutto una sorveglianza massiva e globale, non fondata su sospetti specifici o quantomeno ristretti, non ha la reale ed effettiva capacità di evitare attacchi terroristici e garantire la sicurezza nazionale, costituendo dunque una ingerenza nella sfera privata sproporzionata e non necessaria; il secondo assunto invece si fonda sulla considerazione secondo cui l'analisi dei dati effettuata da sistemi automatizzati o da analisti, e dunque non da investigatori, comporti una ingerenza poco controllata e solo limitatamente disciplinata da norme e regole e pertanto ampiamente lasciata alla discrezionalità dei sistemi tecnologici.

[38] In particolare si fa riferimento all'articolo del 17 marzo 2018, pubblicato sul The Guardian, dal titolo: *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*.

[39] Si tratta dell'articolo di M. Rosemberg, *Bolton was early beneficiary of Cambridge Anlytica's Facebook data*, pubblicato il 23 marzo 2018.

whistleblowers – per lo più ex dipendenti di Cambridge Analytica – hanno svelato innanzitutto come i nostri dati siano costantemente sottoposti al rischio di uso scorretto e quanto dunque sia difficile controllare e tutelare le informazioni che siti e *social networks* raccolgono: le falle nel sistema di *data security* del colosso Facebook hanno messo in luce quanto gli utilizzi illeciti e non autorizzati o i furti di dati (o *data breach*) siano frequenti e avvengano spesso su larga scala[40]. Ma lo scandalo che ha portato il fondatore stesso di Facebook ad ammettere la pericolosità e la fragilità del proprio sistema di raccolta e conservazione dei dati e di ri-utilizzo da parte di soggetti terzi, ha dimostrato anche e soprattutto quanto delicate siano le informazioni che lasciamo sul Web e quanto rivelino di noi, tanto da poter essere impiegate per influenzarci e condizionare le nostre scelte. Le operazioni di profilazione e marketing mirato, come quelle poste in atto da Cambridge Analytica, hanno un impatto ben più profondo e determinante dei banner pubblicitari di prodotti di abbigliamento che compaiono durante la navigazione online: ogni 'like', ogni commento, ogni contenuto condiviso, ogni tweet viene analizzato, letto in maniera sistematica ed utilizzato per creare un profilo psicologico dell'utente e selezionare per lui i contenuti che compariranno sulla "Home", e che dunque potranno essere immediatamente letti, impedendo ad altre notizie di avere risalto[41]. Queste tecniche, laddove impiegate per scopi di propaganda elettorale, hanno aperto a grandi interrogativi sulla liceità di tali mezzi e sulla necessità di una stringente regolamentazione in materia, tanto che su entrambe le sponde dell'Oceano Atlantico sono state avviate indagini, da un lato da parte della Electoral Commission inglese avverso il gruppo Leave.EU per illeciti e irregolarità nell'ambito della campagna pro-Brexit, e dall'altro da parte dello Special Counsel Robert Mueller nell'ambito della inchiesta c.d. Russiagate[42].

---

[40] Il CEO di Facebook, Mark Zuckerberg, è stato chiamato a testimoniare più volte dinnanzi al Senato degli USA a seguito dello scandalo di Cambridge Analytica. In una dichiarazione pubblica egli ha ammesso il fallimento delle *policies* poste a tutela della privacy e della protezione dei dati e l'incapacità di evitare episodi di uso illecito di dati da parte di soggetti terzi. Il dibattito apertosi in quella sede ha interessato anche le procedure e gli strumenti che i *social network* dovrebbero porre in campo al fine di arginare – o quantomeno controllare – fenomeni di *hate speech* e *fake news* (*post*, contenuti, immagini o video che inneggiano alla violenza e all'odio i primi; mentre con il termine *fake news* si fa riferimento ai *post* che contengono volutamente e appositamente informazioni e notizie false ed infondate e che quindi si fanno veicolo di una sempre più preoccupante disinformazione). Su questo aspetto, estremamente complesso e problematico, che ha ingenti ripercussioni sotto il profilo politico e sociale, si legga, ex multis: G. PITRUZZELLA, O POLLICINO, S. QUINTARELLI (a cura di), *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, 2017; G. PITRUZZELLA, O. POLLICIINO (eds.), *Disinformation and hate speech. A European constitutional perspective*, Bocconi University Press, 2020; A. DI ROSA, *Hate speech e discriminazione. Un'analisi performativa tra diritti umani e teorie della libertà*, Mucchi, 2020; K. SHU et al., *Disinformation, misinformation and fake news in social media: emerging research challenges and opportunities*, Springer, 2020.

[41] Si parla, in gergo tecnico, di 'segmentazione psicografica' e 'targeting psicografico' per intendere quei metodi qualitativi impiegati per 'segmentare' e dunque suddividere in gruppi i consumatori o, più in generale, gli utenti di servizi, basandosi su criteri psicologici (preferenze, interessi, opinioni, abitudini, stili di vita, classe sociale di appartenenza, orientamento politico, sessuale, religioso). Ulteriori definizioni, esempi e riflessioni sull'impatto di questa tecnica rispetto ai tradizionali strumenti di marketing, nonché per approfondimenti sull'impiego di questo delicato strumento nell'ambito elettorale, si rinvia a: K. WARD, *Social networks, the 2016 US Presidential election and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting*, in *Journal of Media Ethics*, 3, 2018; G. R. MURRAY, *Microtargeting and electoral segmentation: data mining the american national elections studies*, in *Journal of Political Marketing*, 3, 2018; P. HOWARD, *Algorithms, bots and political communication in the US 2016 Election: the challenge of automated political communication for election law and administration*, in *Journal of Information Technology and Politics*, 2, 2018; A. PERUZZI, F. ZOLLO, W: QUATTROCCHI, A. SCALA, *How new ways affect markets complex structure: the case of Cambridge Analytica*, in *Entropy*, 10, 2018.

[42] Per ulteriori approfondimenti sulle molteplici implicazioni di questi complessi casi e dei loro articolati risvolti, si rimanda a E. ASSANTE, *Cosa ci può insegnare il caso Cambridge Analytica*, in *federalismi.it*, 9, 2018; D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Anlaytica"*, in *federalismi.it*, 20, 2018; J. HIND, E. WILLIAMS, A. JONSON, *'It wouldn't happen to me': privacy concerns and perspectives following the Cambridge Analytica scandal*, in *International Journal of Human-Computer*, 143, 2020.

Entrambi gli eventi sopra riportati hanno fatto affiorare con forza la consapevolezza degli inquietanti rischi connessi ad una raccolta ed utilizzo incontrollato di dati digitali: se infatti la capacità di soggetti privati di appropriarsi dei dati derivanti dalle nostre attività sui *social network* e, mediante la loro elaborazione e la tecnica di c.d. *data mining*[43], di inviarci pubblicità mirate, banner e campagne marketing targetizzate potrebbe apparire, laddove ci colpisca come consumatori, una pratica tutto sommato sopportabile per quanto percepita come scorretta, risulta certamente più sconvolgente ed inaccettabile pensare ad un utilizzo di simili tecniche al fine di captare le nostre preferenze ed opinioni politiche e di influenzare così il nostro voto, incidendo sull'esito di elezioni e votazioni importanti e quindi colpendoci nella nostra natura di cittadini ed elettori[44].

Questi esempi svelano altresì la capacità dei Big Data di rivelare informazioni su noi stessi, anche mediante quei dati che riteniamo irrilevanti o incapaci di svelare alcunché se presi singolarmente: questo perché "more often than not, it is not the information collected in itself that is sensitive, but rather, the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern"[45]. Sono dunque i dati nel loro insieme e nella loro lettura aggregata o come 'fonte' e 'motore' di algoritmi e sistemi di AI che sono in grado di fornire informazioni sulle nostre abitudini, preferenze, orientamenti politici, sessuali e religiosi. La profilazione, dunque, intesa come "qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona"[46], comporta pericoli di grande entità e non solo limitatamente agli esempi svolti, attinenti all'ambito della sicurezza

---

[43] "Per *data mining* si intende, in senso molto lato, il potere e la capacità di trattare grandi informazioni di dati correlandole con strumenti elettronici. (..) Il *data mining* rende possibile all'essere umano un'attività di selezione e di estrazione di informazioni che sarebbe impossibile con il tempo e la mente/memoria a disposizione. È un sistema che supera, così, i limiti intellettuali e di lavoro dell'uomo a fronte di masse di dati sempre maggiori, anche tramite apprendimento automatico o elaborazione di *patterns* comportamentali ricorrenti", G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina, 2015.

[44] Utilizza il termine 'profilazione degli elettori' L. CALIFANO, in *Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, in *federalismi.it*, 9, 2017, sottolineando la pericolosità intrinseca di queste operazioni: "Le operazioni di raccolta, analisi e rielaborazione di dati personali degli elettori, infatti, possono riguardare l'adesione o affiliazione a un partito politico così come opinioni politiche espresse sui profili dei social network; a loro volta questi dati sensibili possono poi essere incrociati con dati anagrafici e demografici, rientranti nella categoria dei dati cd. comuni (età, reddito, stato civile), recuperati sia tramite internet che con mezzi più tradizionali come la propaganda e il contatto porta a porta effettuato dai militanti. Operazioni di questo tipo servono a isolare e comprendere le preferenze sociali dei cittadini, ovverosia cosa i cittadini desiderano che i loro rappresentanti realizzino e, dunque, cosa è bene che i candidati propongano per poter essere eletti", p. 4. Per ulteriori approfondimenti sulle implicazioni dei Big Data nel mondo della politica, si legga: S. RODOTÀ, *Iperdemocrazia. Come cambia la sovranità democratica con il web*, Laterza, 2013; E. GIOVANNINI, *Scegliere il futuro. Conoscenza e politica al tempo dei Big Data*, Il Mulino, 2014; D. GAMBETTA, *Datacrazia, politica, cultura algoritmica e conflitti al tempo dei Big Data*, D Editore, 2018; A. SORO, *Democrazia e potere dei dati. Libertà, algoritmi e umanesimo digitale*, Baldini+Castoldi, 2019, con particolare riferimento al Capitolo "Dall'urna al click. Postverità, microtargting politico e democrazia diretta". Sullo specifico ruolo dei *social networks*, si rimanda anche a: S. VAIDHYANATHAN, *Antisocial media: how Facebook disconnects us and undermines democracy*, Oxford University Press, 2018; G. ZICCARDI, *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina, 2019.

[45] Gruppo di Lavoro Art. 29, *Opinion 3/2013: Purpose Limitation*, WP 203, 2 aprile 2013.

[46] Definizione fornita all'art. 4, co. 4, Reg. 2016/679. È bene sin da ora precisare come il Regolamento generale sulla protezione dei dati (meglio noto come General Data Protection Regulation o GDPR) rappresenti uno dei testi normativi di riferimento attualmente vigenti nel panorama europeo in materia di protezione dei dati. Esso delinea un insieme complesso ed articolato di norme da rispettare ogniqualvolta avvenga un trattamento dei dati personali. Per una ricostruzione del significato e delle ampie implicazioni delle operazioni di profilazione, si rimanda a M. HILDEBRAND, *Profiling and the rule of law*, in *Identity in the information society*, 1, 2008; P. DE HERT, H. LAMMERANT, *Predictive profiling and its legal limits: effectiveness gone forever?*, in B. VAN DER SLOOT, D. BROEDERS, E. SCHRIJVERS (eds.), *Exploring the boundaries of Big Data*, Amsterdam University Press, 2016.

o della propaganda politica ed elettorale, bensì nei settori più svariati e mediante l'impiego dei dati più disparati[47]: dall'utilizzo della profilazione come strumento di operazioni di marketing a quello nell'ambito delle assicurazioni[48], sino alla profilazione effettuata mediante i dati raccolti dai diversi *devices* impiegati nella domotica e dunque rientranti nell'ambito della c.d. IoT[49]. In tutti questi campi di utilizzo tale tecnica è in grado di ricreare, partendo da una moltitudine di dati differenti, un nostro profilo e rischia di tradursi pertanto in insidiose pratiche discriminatorie che sfruttano la scarsa consapevolezza degli utenti ed esasperano la forte asimmetria informativa esistente tra gli utenti da un lato e dall'altro chi invece dispone dei nostri dati e li impiega per trarne informazioni utili al perseguimento dei propri obiettivi[50]. Ancora una volta e anche sotto tale profilo, quindi, "il mondo dei BD mostra la natura bifronte dei dati personali: da un lato diretti prodotti della persona e dall'altro asset dal valore commerciale capaci di essere scambiati e commercializzati"[51].

---

[47] Per uno sguardo generale sul tema, risultano particolarmente utili: F. PASQUALE, *The black box society. The secret algorithms that control money and information*, Harvard University Press, 2015. C. O'NEIL, *Armi di distruzione di matematica. Come i big data aumentano la diseguaglianza e minacciano la democrazia*, traduzione italiana di Bompiani, 2017; si legga anche D. TALIA, *La società calcolabile e i Big Data. Algoritmi e persone nel mondo digitale*, Rubettino, 2019.

[48] "L'utilizzo di algoritmi predittivi che gestiscono enormi quantità di dati si rivela così uno strumento di grande interesse per l'impresa assicuratrice laddove le permetterebbe di: aumentare l'accuratezza e precisione delle previsioni sul rischio, meglio determinare i costi e adempiere ai requisiti della nuova disciplina prudenziale in un'ottica *customer* centrica", G. D'IPPOLITO, *Processi decisionali automatizzati nel settore assicurativo. Un'indagine preliminare*, in *MediaLaws*, 2, 2019. Sul punto, si legga anche, ex multis: C. ALVISI, *I trattamenti nel settore bancario, finanziario e assicurativo*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, Editoriale Scientifica, 2017, p. 629; B. KELLER, *Big Data and insurance: implications for innovation, competition and privacy*, The Geneva Association, 2018; J. CANNATACI, V. FALCE, O. POLLICINO, *Legal challenges of Big Data*, Elgar, 2020.

[49] Come sottolineato anche dal Gruppo di Lavoro Art. 29 (*Parere 8/2014 sui recenti sviluppi nel campo dell'Internet of Things*, 2014 (WP223), l'analisi dei dati prodotti da IoT è in grado di rivelare informazioni rilevanti sullo stile di vita, le abitudini e le scelte degli utenti: si pensi alla domotica, ad esempio, e la possibilità che i dati raccolti dai *devices* svelino gli orari di utilizzo degli elettrodomestici o le impostazioni di avvio degli stessi, così da indicare anche le abitudini e la usuale presenza in casa dei suoi abitanti. Per approfondimenti sul tema della profilazione anche mediante strumenti IoT, si rimanda a O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, op. cit., p. 573.

[50] Proprio su tale aspetto della asimmetria informativa si fonda la grande fortuna dei c.d. *Smart contracts*, ovvero "attività negoziali gestite da un programma che opera attraverso tecnologie c.d. blockchain che ne assicurano la certezza, la riferibilità, la non modificabilità ed automatica esecuzione". Ebbene in tali tipologie di contratti, "l'asimmetria si amplia poiché non solo il produttore/fornitore sa tutto di ciò che offre, ma, soprattutto – e qui sta l'elemento di assoluta novità – sa tutto della sua controparte, addirittura più di quanto questa sa di sé medesima. Questo per la semplice ragione che il produttore/fornitore acquista sul mercato il profilo quanto più completo possibile delle scelte di consumo, delle preferenze, delle attitudini e soprattutto del reddito dell'altra parte. Dunque il contratto viene ricondotto ad una assoluta razionalità, algoritmicamente predeterminata, economica la quale stabilisce qual è il prezzo che quel contraente reputa accettabile, il livello di rischio nel caso di dilazione del pagamento, le prestazioni accessorie che possono essere inserite nel pacchetto", V. ZENO-ZENCOVICH, *La 'datasfera'. Regole giuridiche per il mondo digitale parallelo*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, 2018, p. 102 ss. Si può comprendere dunque come Big Data e algoritmi incidano anche sul contratto comunemente inteso e sull'aspetto delicato e dibattuto della (a)simmetria informativa e sull'equilibrio delle relazioni contrattuali.

[51] E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, op. cit. Sotto questo profilo poi pare necessario evidenziare come le aziende private (soprattutto i c.d. OTT) che riescono a disporre di una grande mole di dati ed informazioni, riuscendo ad applicare anche sofisticate tecniche di profilazione e Data Analytics, abbiano acquisito sempre più rilievo, tanto da mutare fortemente i rapporti di potere nella società globale: "un numero esiguo di aziende possiede un patrimonio di conoscenza gigantesco e dispone di tutti i mezzi per indirizzare la propria influenza verso ciascuno di noi. (..) Fanno giornalmente notizia le iniziative e le sperimentazioni anche avveniristiche dei giganti del web, assai lontane dalle loro originarie vocazioni, ma che permettono loro di assumere un ruolo sempre maggiore in campi (dalla finanza alla genetica, dall'automazione alla realtà aumentata) che hanno un impatto significativo nelle nostre vite sul piano sociale, culturale ed economico", A. SORO, Garante per la protezione dei dati personali, *Big Data e*

1.3.2. – L'inadeguatezza delle tutele e degli istituti 'tradizionali' del diritto nel mondo digitale: un necessario ripensamento

I Big Data e dunque la disponibilità di una mole senza precedenti di informazioni, l'uso di sistemi di profilazione, basati anche su tecniche di AI ed algoritmi comportano, come si è visto, minacce forti e reali che impongono una seria riflessione capace di guardare oltre le positive potenzialità che il progresso tecnologico comporta e in grado dunque di comprenderne i rischi e predisporre regole e salvaguardie adeguate a prevenirli. L'intervento del giurista diventa pertanto, in tale contesto, quanto mai necessario e complesso: il nuovo linguaggio della scienza e della tecnologia mette in crisi gli istituti classici e le tradizionali categorie del diritto. Taluni degli esempi svolti in precedenza hanno già in parte messo in luce queste criticità e possono risultare dunque utili per cogliere la grande sfida che oggi il legislatore, il giudice e gli studiosi stessi del diritto sono chiamati ad affrontare.

Ci si riferisce al valore e alla portata del 'consenso' nell'ambito digitale: "se si guarda ai servizi online, sono gli stessi utenti di questi servizi che – sia pure di sovente perché forzati in un'ottica di *take it or leave it* o in quanto abbacinati da una formale gratuità di detti servizi – rendono disponibili le proprie informazioni e dati personali, facilitando la propria profilazione ai fini pubblicitari, a cui verranno massicciamente sottoposti"[52]. Nel mondo digitale, dunque, il consenso conosce uno svuotamento 'sostanziale' della propria portata e della tutela che è in grado di offrire: da un lato la scelta di accettare che i nostri dati di navigazione vengano trattati, e spesso anche trasferiti a soggetti terzi, per finalità descritte e definite in maniera molto generica e indeterminata, è sovente obbligata se si vuole accedere al contenuto di un sito o alla fruizione di un servizio, così che il consenso non può dirsi realmente e totalmente libero; dall'altro lato la possibilità di selezionare e dunque limitare la memorizzazione e l'impiego delle nostre informazioni non è una facoltà sempre facilmente comprensibile per gli utenti, che finiscono così spesso per accettare tutte le tipologie di trattamento dati senza capire appieno cosa stanno cedendo, quali sono i rischi che si corrono o le alternative possibili: ne deriva che anche sotto tale profilo il consenso non può dirsi del tutto informato e consapevole[53]. Del resto, un ulteriore elemento tecnico che limita l'efficacia tutelante del consenso nel contesto digitale è rappresentato dalla difficoltà, da parte del gestore di un sito o di un servizio di telecomunicazione, di una app o di un *wearable device*, di determinare in anticipo tutti i possibili o necessari utilizzi dei nostri dati: l'impiego delle informazioni raccolte infatti non è sempre noto o identificabile neppure dal gestore stesso, che potrebbe in un secondo momento scoprire potenzialità e possibilità di utilizzo dei dati anche per finalità altre ed ulteriori rispetto a quelle inizialmente considerate[54]. Per questo motivo e dato anche

---

Privacy. La nuova geografia dei poteri, op. cit. Ciò è del resto chiaramente emerso dalle vicende approfondite in questo paragrafo, Cambridge Analytica su tutte, che hanno messo in luce le ampie possibilità e disponibilità che sono ormai in capo a poche aziende. I maggiori rischi che da ciò derivano sono rappresentati oltre che dalla creazione di squilibri tra poteri, soprattutto tra autorità private e pubbliche a tutto favore delle prime, e dalla concentrazione nelle mani di grandi 'giganti del Web' di una enorme quantità di informazioni, anche dal fatto che tali grandi capacità, anche fortemente invasive della nostra privacy, non sono state accompagnate né da responsabilità altrettanto forti in capo alle aziende private né da tutele decise dei diritti dei consumatori e degli utenti. Sul punto, criticamente, A. MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Diritto dell'Informazione e dell'Informatica*, 1, 2012.

[52] G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, op. cit., p. 450.

[53] Come ben sottolineato da Orefice, "la cessione dei dati agli OTT per finalità non meglio specificate è automaticamente collegata all'installazione delle applicazioni sui dispositivi elettronici ed è condizione necessaria per la fruizione dei servizi offerti", M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne, 2018.

[54] Nello stesso GDPR, ad esempio, si legge come "In molti casi non è possibile individuare pienamente la finalità del trattamento dei dati personali a fini di ricerca scientifica al momento della raccolta dei dati. Pertanto, dovrebbe essere consentito agli interessati di prestare il proprio consenso a taluni settori della ricerca scientifica laddove vi sia rispetto delle norme deontologiche riconosciute per la ricerca scientifica", Considerando 33. Viene dunque ammesso dallo stesso legislatore europeo che spesso non risulta tecnicamente fattibile e concretamente possibile

il rapido evolversi della tecnica, gli scopi indicati ai fini del consenso sono sempre più di frequente estremamente ampi nel loro dettato, a tutto detrimento del rispetto di quel fondamentale principio di finalità[55] che implica che il trattamento dei dati sia limitato agli scopi per i quali il consenso è stato prestato[56]. Risulta evidente quindi che le garanzie che normalmente il consenso contribuisce a creare non sono automaticamente applicabili e trasponibili nel mondo digitale ma anzi impongono una riflessione ed un ripensamento di tale istituto e delle reali e concrete tutele che è in grado di fornire nel complesso contesto del Web, dei Big Data e dell'impiego di algoritmi[57].

Un ulteriore esempio delle sfide cui il mondo del diritto deve cercare di fornire una risposta è da individuarsi nel concetto di 'anonimizzazione' e di dati anonimi: nonostante la procedura di anonimizzazione abbia da sempre rappresentato una delle fondamentali tutele della riservatezza, garantendo la perdita di informazioni identificative del soggetto da cui i dati provengono, è necessario

---

provvedere ad un consenso preciso e puntuale, ben potendo dunque quest'ultimo assumere un carattere più generico e contorni più ampi ed indeterminati.

[55] Per approfondimenti si legga: N. FORGO, S. HANOLD, B. SCHTZE, *The principle of purpose limitation and Big Data*, in M. CORRALES et al. (a cura di), *New technology, Big Data and the Law*, Springer, 2017. Il principio di finalità è strettamente connesso al concetto di trasparenza e correttezza del trattamento dei dati, legandosi dunque anche all'istituto del consenso, che può essere effettivo ed informato solo laddove risultino chiare le finalità per le quali il trattamento viene effettuato ed il relativo consenso raccolto. Il principio di finalità nello specifico prevede che i dati debbano essere "raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo che non sia incompatibile con tali finalità" (art. 5, co. 1, lett. b) GDPR).

[56] Come afferma Bravo, "è ben nota l'insufficienza del consenso a fornire un adeguato livello di tutela dell'interessato, soprattutto in quelle situazioni in cui l'esistenza di condizionamenti (ad es. quelli legati alla stessa possibilità di ricevere la fornitura di servizi essenziali) fa apparire solamente formale il principio della libertà del consenso, con un suo svuotamento sul piano sostanziale", F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, 2017, p. 139. Della stessa opinione anche Faini: "nell'universo dei grandi dati vacillano nella sostanza anche l'informativa da parte del titolare del trattamento e il consenso libero, preventivo, specifico, inequivocabile e revocabile dell'interessato, dal momento che per lo più non si conoscono preventivamente obiettivi e finalità di utilizzo: è dubbio che in tale contesto siano rese informazioni capaci di fornire una conoscenza reale, completa e profonda e, altresì, di conseguenza, che il consenso possa considerarsi libero", F. FAINI, *Big data, algoritmi e diritto*, in *DPCE Online*, 3, 2019, p. 1878. Ancora, sul tema: "The process of collection and processing data is lawful and fair if consent is given after receiving exhaustive information and when it is expressed freely and in specific terms. The reality, however, reveals a significant divergence from the legal provisions, and very often the data subject's intentions are not truly ascertained, as users often appear disoriented and unaware when expressing their consent. These conditions undermine the safeguards underlying the rule of consent, marking its downward spiral. The user's vulnerability depends on the asymmetry that arises in relation to internet service providers, principally due a to technical information deficit on the data subject's side. In effect, users frequently do not understand the terms and conditions surrounding the use of their data because they are written in unclear and incomprehensible language, or else they are difficult to find on websites, or again, users may not have a sufficient level of technological literacy", A. VIVARELLI, *The crisis of the rights to informational self-determination*, in *The Italian Law Journal*, 1, 2020, p. 306. Sul punto si leggano anche le riflessioni di L. MONTUORI, M. SIANO, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Aracne, 2017; F. CAGGIA, *Libertà ed espressione del consenso*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, op. cit., p. 249-274.

[57] Sulla necessità di ripensare al consenso e al significato che esso assume dinnanzi alla produzione e al trattamento massivo di dati, si è interrogato anche il Gruppo di Lavoro Art. 29 che nelle *Linee guida sul consenso ai sensi del Reg. UE 2016/679*, 28 novembre 2017, modificate il 10 aprile 2018, WP259, ha sottolineato come laddove vi sia uno squilibrio di potere e non siano presenti delle reali e concrete alternative all'accettazione dei termini di trattamento, il consenso non possa essere considerato libero. Rodotà inoltre ha evidenziato un ulteriore limite del consenso nel mondo dei *bit*: il dislivello di poteri tra utente e 'app' che raccoglie i dati "non si può colmare con interventi che obbligano l'interessato a una continua attenzione e a una continua necessità di accompagnare gesti abituali e quotidiani, quali sono ormai quelli legati all'ordinario navigare in rete o al portare con sé una carta elettronica, con un supplemento di azioni che possono sembrargli pure fastidiose, inutili", S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, 2014.

tuttavia precisare come questa garanzia non sempre sia reale e concreta nell'ambito digitale. L'avanzamento tecnologico e la mole di dati sempre più vasta quotidianamente prodotta e reperibile in diversi siti e banche dati, hanno reso non solo possibili ma anche semplici le operazioni di re-identificazione, anche partendo da dati anonimi[58]. Ne deriva dunque che il semplice fatto che un dato sia anonimo[59] non può più essere considerato elemento idoneo a comportare una garanzia assoluta e totale di riservatezza o di maggior protezione dei dati.

Vi sono, poi, una molteplicità di ulteriori questioni, che pur in questa sede si vogliono solo accennare, che risultano tuttavia di grande rilievo al fine di permettere una più completa comprensione della molteplicità degli ambiti, delle categorie e degli istituti che risultano profondamente toccati dal progresso tecnologico e per i quali si rende necessario un adeguamento ed una seria riflessione. Si può fare riferimento alla determinazione della appartenenza del dato digitale: i dati appartengono a chi li produce (all'utente di un sito Web)? Oppure al gestore del sito Web all'interno del quale sono prodotti? O ancora al soggetto che li raccoglie, conserva ed elabora? È possibile ricondurre i dati al concetto di proprietà di un bene?

Come ben sottolineato da Zeno-Zencovich, un ulteriore elemento di complessità è dato dal carattere non solo immateriale ma anche a-territoriale dei dati, che rende quindi ancor più arduo determinare la corretta normativa da applicare: quella dello Stato nel quale il dato viene prodotto? Quella dello Stato in cui viene raccolto e conservato? Quella in cui il dato viene trattato? Tutti questi quesiti, per i quali è difficile applicare le categorie e definizioni tradizionalmente elaborate dal diritto (proprietà, sovranità, territorialità), costituiscono aspetti di estrema importanza, non solo giuridica bensì applicativa e persino economica, considerato il grande valore che i dati ormai rappresentano[60]. La centralità di tali domande, come si vedrà nella Parte II, emerge con forza nel contesto dell'Unione europea che si è ampiamente interrogata sul concetto di territorialità applicato al mondo digitale e, con esso, delle tutele e garanzie che possono essere offerte ad un dato personale una volta uscito – o meglio trasferito – oltre i confini europei. Una questione tutt'altro che semplice da risolvere e che si scontra con molteplici e delicate problematiche giuridiche ma dai rilevanti risvolti politici ed economici.

Se si fa riferimento poi all'ambito, attualmente in pieno sviluppo, della IoT o delle auto senza guidatore, viene da chiedersi quali regole debbano essere applicate a tali oggetti, che pure agiscono autonomamente ed automaticamente, elaborando dati sulla base di algoritmi e prendendo conseguentemente decisioni: a chi deve essere imputato un incidente causato da una auto priva di un conducente 'umano'? La responsabilità civile e penale è da attribuirsi al proprietario dell'auto? O a chi ha programmato l'algoritmo che ne determina il funzionamento e, talvolta, il malfunzionamento?

---

[58] Per supportare queste affermazioni si può citare, quale esempio concreto, il caso dei ricercatori dell'Università di Austin (Texas) che, partendo dalle valutazioni di gradimento di sei film, provenienti da mezzo milione di utenti Netflix e diffuse da quest'ultimo in forma del tutto anonima e deindicizzata, e confrontando tali informazioni con altri dati pubblicamente disponibili online, sono riusciti ad identificare lo specifico utente che aveva espresso le citate valutazioni ben 84 volte su 100. Ciò dimostra quanto la deindicizzazione e la eliminazione di ogni dato identificativo non sia in realtà in grado di garantire, nel sistema dei Big Data, una protezione assoluta ed efficace della privacy. L'esempio è tratto dall'analisi di V. MAYER-SCHONBERGER, K. CUKIER, *Big Data una rivoluzione che trasformerà il nostro modo di vivere e che già minaccia la nostra libertà*, op. cit.

[59] È da sottolineare sin da ora come la qualificazione di un dato come anonimo rilevi in maniera particolare soprattutto con riferimento al diritto dell'UE: il richiamato GDPR infatti non si applica laddove ad essere interessati siano dati anonimizzati. Il Considerando 26 sul punto specifica come "I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato. Il presente regolamento non si applica pertanto al trattamento di tali informazioni anonime, anche per finalità statistiche o di ricerca".

[60] Su tali quesiti si rimanda anche a G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche*, op. cit.; nonché a V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the 'big data revolution'*, op. cit., p. 29 ss.

Questi interrogativi del resto derivano e mettono in luce un ulteriore profilo di criticità e di complessità legato al rapido progresso tecnologico: essere in grado di porsi quesiti relativi alle problematiche strettamente funzionali e tecniche derivanti dai nuovi strumenti diviene esercizio di fondamentale importanza al fine di poter trovare soluzioni e istituti capaci di fornire risposte adeguate a sfide inedite.

1.3.3. – Dagli algoritmi discriminatori al 'digital divide': il bisogno di una seria conoscenza delle criticità tecniche per comprendere i rischi e promuovere salvaguardie efficaci

Se comprendere le problematiche che l'innovazione e le nuove tecnologie pongono risulta una tappa propedeutica e preliminare alla determinazione di un idoneo insieme di tutele e salvaguardie, diviene altresì fondamentale comprendere come, per fare ciò, si renda necessario possedere una solida conoscenza o, quantomeno, una profonda comprensione di questioni tecniche, attinenti anche ai meccanismi di funzionamento concreto e alle caratteristiche degli strumenti sviluppati e impiegati. Ne è un esempio paradigmatico l'utilizzo di algoritmi e sistemi di AI: in questo campo così articolato, porsi i corretti quesiti giuridici richiede e presuppone una chiara consapevolezza circa la natura degli algoritmi, il loro sviluppo e il modo in cui operano.

Si pensi, a titolo esemplificativo, all'impiego di strumenti di AI nelle aule di Tribunale: il caso più noto e studiato è senza dubbio rappresentato dal sistema Compas, utilizzato dai giudici di talune Corti statali e federali negli USA. Tale software, fondato su di un algoritmo, è stato progettato per determinare il livello di rischio e pericolosità sociale di un soggetto condannato per un reato, elaborando la probabilità di recidiva sulla base di diversi dati forniti (un questionario compilato dall'imputato, i suoi precedenti giudiziari ed altri elementi non conosciuti e facenti parte della progettazione stessa dell'algoritmo, coperti dalla tutela della proprietà intellettuale). Come è facile comprendere, l'impiego da parte di un giudice di tale strumento potrebbe indurre a ritenere la decisione finale maggiormente oggettiva e neutrale, in quanto stabilita non sulla base di valutazioni soggettive del magistrato bensì su dati oggettivamente elaborati da un algoritmo. Nulla di più erroneo: solo mediante una conoscenza approfondita del funzionamento della AI, infatti, è possibile individuare uno dei profili fortemente problematici caratterizzanti strumenti quali Compas, consistente cioè nel concetto di *bias* o pregiudizio. Tale termine definisce, in questo contesto, un sistema informatico che "discrimina sistematicamente e ingiustamente determinati individui o gruppi a favore di altri"[61]. Ebbene il software sopra richiamato è risultato possedere, sulla base di alcuni studi svolti da esperti di analisi statistica che ne hanno testato il funzionamento, un margine di errore nella predizione di recidiva pari al 30%, mostrando oltretutto una percentuale di errore (ovvero di soggetti considerati ad alto rischio di recidiva sulla base dell'elaborazione algoritmica che però non hanno nella realtà dei fatti commesso reati nei due anni successivi) maggiore rispetto ad imputati di colore. Questo *bias* discriminatorio e sistematico, intrinseco al funzionamento dell'algoritmo stesso, dipende e deriva da come l'algoritmo è stato progettato e creato nonché dai dati impiegati per 'istruire' l'AI, dalla loro tipologia e dal campione preso in esame per elaborare lo studio statistico: come rilevato da Resta, "se si calcolasse l'attitudine a delinquere esclusivamente sulla base delle statistiche relative alla popolazione carceraria negli USA, se ne trarrebbe un risultato viziato in partenza, poiché è noto che gli Afro americani rappresentano una quota

[61] A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, op. cit. Si legga anche: B. FRIEDMAN, H. NISSENBAUM, *Bias in computer systems*, in *ACM transactions on information systems*, 3, 1996; A. SUTTON, T. LANSDALL, N. CRISTIANINI, *Biased embeddedings from wild data: measuring, understanding and removing*, in *International symposium on Intelligent data analysis*, Spinger, 2018; FRA, *Big Data: discrimination in data-supported decision making*, 2018.

preponderante di tale popolazione"[62], il che porterebbe quindi a generalizzare il binomio "imputato di colore – alto rischio di recidiva"; questo malfunzionamento o pregiudizio insito nell'algoritmo può dunque spiegare l'elevato tasso di "falsi positivi" nelle persone di colore, ovvero di soggetti considerati ad alto rischio ma che si sono poi rivelati non recidivanti. Similmente, una forte influenza sull'esito della valutazione automatizzata è determinata dal luogo di residenza o di nascita del soggetto e dal tasso di criminalità di tale area: ciò può contribuire ad incrementare l'effetto discriminatorio del sistema, portato, sulla base di tali dati, a ritenere maggiormente a rischio imputati che presentano una connessione con una zona ad alta criminalità. Questo esempio consente di comprendere come non esistano algoritmi definibili realmente neutrali o che si "limitano a riflettere la realtà: essi anzi propongono una loro versione fatta dalle formule classificanti, dal peso attribuito ai singoli parametri inseriti, dalle procedure che determinano il risultato"[63]. Solo la consapevolezza di queste caratteristiche e, in particolare, dell'attitudine discriminatoria dell'algoritmo stesso[64], può consentire non solo una migliore *digital ethics*, ovvero una programmazione 'etica' dell'algoritmo[65] cioè ispirata a principi volti a limitare quanto più possibile derive discriminatorie o pregiudizievoli, ma anche una efficace *digital regulation*[66] cioè la predisposizione di norme adeguate, appropriate, specificamente ideate per risolvere ed affrontare le sfide peculiari dei sistemi di AI, risultando in una 'infrastruttura giuridica' solida e quanto più possibile rispondente alle evoluzioni tecnologiche.

La rilevanza di simili considerazioni diviene evidente anche con riferimento ad altri strumenti fondati su sistemi di AI, che hanno mostrato problematiche connesse al concetto di *bias* del tutto analoghe a quelle già sottolineate con riferimento al sistema Compas: richiamando la tecnologia del riconoscimento facciale, precedentemente analizzata e rispetto alla quale sono state messe in rilievo le potenzialità soprattutto in ambito securitario e dunque di prevenzione e repressione di reati, emerge da numerosi studi come anch'essa sollevi dubbi ed interrogativi etici e giudici; essi possono essere riassuntivamente individuati "in primo luogo, [nel]lo stadio di sviluppo della tecnologia stessa, che presenta ancora problemi nell'accuratezza del riconoscimento; in secondo luogo, [nel]le peculiarità proprie del dato biometrico, che è idoneo a rivelare informazioni, anche sensibili, ulteriori rispetto allo scopo per cui è trattato; infine, [nel]l'intrinseca capacità intrusiva delle tecnologie di riconoscimento facciale e la possibilità che queste contribuiscano alla creazione di sistemi di sorveglianza di massa"[67]. Il *bias*

---

[62] G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Forum disuguaglianze e diversità*, 2020.

[63] A. C. AMATO MANGIAMELI, *Algoritmi e big data. Dalla carta sulla robotica*, in *Rivista di filosofia del diritto*, 1, 2019, p. 110.

[64] Interessante sul punto è il contributo di A. CHANDER, *The racist algorithm?*, in *Michigan Law Review*, 115, 2017.

[65] Per ampie considerazioni su tale aspetto, si rinvia, tra i tanti, a: L. FLORIDI, *Soft ethics and the governance of the digital*, in *Philosophy and Technology*, 1, 2018 e dello stesso autore: *What the near future of AI could be*, in *Philosophy and Technology*, 7 aprile 2020. Anche la Commissione europea ha avviato una lunga consultazione ed un ampio dibattito sul tema, i cui punti fondamentali e risultati sono contenuti nel già richiamato *Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, nel quale sono stati evidenziati non solo gli effetti positivi e le grandi opportunità, anche sul piano economico, rappresentate da tale tecnologia, bensì anche i rischi derivanti da meccanismi decisionali opachi, da possibili distorsioni e discriminazioni (dovuti sia ai dati impiegati per 'addestrare' l'AI, sia a difetti di progettazione) che possono pregiudicare "i valori su cui si fonda l'Unione e causare violazioni dei diritti fondamentali, compresi i diritti alle libertà di espressione e di riunione, la dignità umana, la non discriminazione fondata sul sesso, sulla razza, sull'origine etnica, sulla religione o sulle convinzioni personali, sulla disabilità, sull'età o sull'orientamento sessuale (ove applicabili in determinati settori), la protezione dei dati personali e della vita privata o il diritto a un ricorso giurisdizionale effettivo e a un giudice imparziale, nonché la tutela dei consumatori", p. 12.

[66] Espressioni usate efficacemente da G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, op. cit., p. 210 ss.

[67] Sulla delicatezza dei dati biometrici, dovuta al loro carattere insostituibile e unico, si rimanda, tra i molti, a: R. DUCATO, *I dati biometrici*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, op. cit., p. 1285; C. GRAZIANI, *La creazione di database di dati biometrici: l'Unione europea tra sfide*

intrinsecamente individuabile in questo strumento – che presenta ad esempio maggiori difficoltà di funzionamento ed un più elevato margine di errore nella corretta identificazione (c.d. operazione di *match*) di soggetti di colore, asiatici o donne[68] – , nonché i pericoli che esso comporta rispetto ai diritti fondamentali quali la protezione dei dati, la riservatezza ma anche il diritto alla libertà di associazione e di espressione, spesso con un effetto ancor più dirompente sulle minoranze etniche o razzali[69], determinano il bisogno di una seria riflessione quanto alle regole e alla disciplina normativa, che dovrebbe essere in grado di bilanciare da un lato le potenzialità di questa tecnologia e dall'altro la tutela dei diritti[70] nonché l'equilibrio del rapporto tra poteri pubblici e cittadini che rischia di trovarsi fortemente sbilanciato a favore del primo laddove, anche mediante l'impiego di una simile tecnologia, venga perpetrato un controllo pervasivo di tutti i consociati[71].

---

alla sicurezza e data protection, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, op. cit.; L. SCAFFARDI, *Dati genetici e dati biometrici: nuove frontiere per le attività investigative,* in L. SCAFFARDI (a cura di), *I 'profili' del diritto*, op. cit.

[68] Come sottolineato dalla Commissione europea, "alcuni programmi di IA per l'analisi facciale riflettono distorsioni legate al genere e alla razza, in quanto identificano con maggiore facilità il genere degli uomini di carnagione chiara mentre commettono più errori nel determinare il genere delle donne di pelle più scura. Fonte: Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency (Atti della 1ª conferenza sull'equità, sulla responsabilità e sulla trasparenza), PMLR 81:77-91, 2018", COMMISSIONE EUROPEA, *Libro bianco sull'intelligenza artificiale*, op. cit.

[69] "Even if the technology becomes more accurate, its dominance over the public realm and potential impact on vulnerable residents have long worried privacy and civil liberties advocates. Historically, poor and marginalized communities – and by extension the spaces in which they live – have been disproportionate targets of state surveillance, and new technologies and techniques are often first used on such individuals before they are rolled out more widely (see, for example, the Chinese surveillance on the Uyighur Muslim community). These communities are often exposed to unique privacy risks if the database in which their biometric information is stored is breached or hacked", come affermato da T. MISRA, *The tenants fighting back against facial recognition technology*, in *Citylab*, 7 maggio 2019, richiamata da E. BIANDA, *Riconoscimento facciale e capitalismo della sorveglianza*, in *Problemi dell'informazione*, 2, 2019.

[70] Sui pericoli e i rischi per i diritti fondamentali provocati dall'impiego, da parte di diversi soggetti – pubblici e privati –, di questa tecnologia, si rimanda, tra i molti, a: K. RINGROSE, *Law enforcement's pairing of facial recognition technology with body-worn cameras escalates privacy concerns*, in *Virginia law Review Online*, 105, 2019; H. RUHRMANN, *Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement*, University of California Berkley, 2019; FRA, *Facial recognition technology: fundamental rights considerations in the context of law enforcement,* 2019; CONSIGLIO D'EUROPA, *Facial recognition: situation and issues*, 2019; mentre per una analisi anche tecnica del funzionamento di tale tecnologia, si legga: B. BUCKLEY, M. HUNTER, *Say cheese! Privacy and facial recognition*, in *Computer Law and Security Review*, 6, 2011. È stato aperto ampio dibattito quanto alla opportunità di impiego di tale strumento e alla possibilità di correggerne i difetti intrinseci mediante la predisposizione di una normativa adeguata, spingendo così la dottrina e i legislatori ad interrogarsi sui limiti da imporre e sull'impatto rispetto ai diritti fondamentali. Anche i giudici stanno iniziando ad affrontare tale tematica: nel 2019 la divisione gallese della High Court of Justice si è pronunciata, in un caso [2019EWHC2341] che non ha trovato precedenti neppure in altre giurisdizioni, in merito all'utilizzo da parte della Polizia locale di sistemi di riconoscimento facciale per finalità di prevenzione ed individuazione di reati, ritenendo l'utilizzo di tale tecnologia e le salvaguardie previste come proporzionate e necessarie, dunque conformi ai diritti fondamentali tutelati a livello nazionale ed europeo (per una dettagliata analisi si rimanda a A. PIN, *Non esiste la 'pallottola d'argento': l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *DPCE Online*, 4, 2019). Nonostante tale positivo vaglio, alcune autorità pubbliche nonché soggetti privati si sono rifiutati o hanno espresso la volontà decisa di non sviluppare ed applicare tale tecnologia, ritenendo i rischi e le incertezze maggiori rispetto alle opportunità: in questo senso ad esempio IBM ha dichiarato nel 2020 di non voler implementare e produrre sistemi di riconoscimento facciale (*IBM's decision to abandon facial recognition technology fueled by years of debate*, in *WashingtonPost*, 11 giugno2020), mentre città come San Francisco, San Diego e Oakland hanno approvato decisioni che vietano l'impiego di tale strumento, anche per scopi di garanzia della sicurezza pubblica e in occasioni specifiche quali festival o eventi sportivi (*San Francisco is the first US city to ban facial recognition*, in *BBCNews*, 14 maggio 2018).

[71] L'idea sottesa a tecnologie quali il riconoscimento facciale, finalizzate alla prevenzione di reati e alla individuazione di soggetti potenzialmente pericolosi in un momento antecedente alla commissione di reati (si pensi all'impiego del riconoscimento facciale in occasione di eventi sportivi, allo scopo di individuare soggetti sottoposti a Daspo o che sono stati in passato condannati per rissa e dunque potenzialmente inclini a provocare situazioni

Le medesime osservazioni possono peraltro essere applicate con riferimento a sistemi di AI e di decisione algoritmica, anche fondati sulla raccolta di dati biometrici, impiegati da autorità pubbliche per garantire un più efficiente funzionamento dei servizi di Welfare State: la digitalizzazione della pubblica amministrazione, come si è detto, si sostanzia anche nel crescente utilizzo di strumenti tecnologicamente avanzati che consentono ad esempio di determinare frodi contributive e fiscali, dichiarazioni mendaci o furti d'identità; tali sistemi tuttavia si fondano su un impiego estensivo di dati, anche particolarmente sensibili ed unici, quali i dati biometrici appunto, spesso conservati in enormi banche dati centralizzate. Risulta evidente dunque come tale conservazione massiva ponga significativi rischi per la riservatezza e la protezione dei dati, dato il pericolo concreto di *data breach* o di utilizzi non autorizzati (c.d. *purpose* o *function creep* ovvero l'impiego di dati per finalità differenti da quelle per le quali erano stati raccolti). Le minacce evidenziate si traducono poi in risultati ancor più seri e dai dirompenti effetti se pensiamo che malfunzionamenti, errori, difetti o perdite di dati in tali sistemi automatizzati di controllo o di autenticazione possono realizzarsi in una negazione dell'accesso a servizi essenziali (sanità, istruzione) o nella mancata erogazione di benefici e sussidi dai quali spesso la vita dei segmenti più poveri e disagiati della popolazione dipendono[72]. Ne deriva, pertanto, che il c.d. *Digital Welfare State* comporta anche serie implicazioni, capaci di concretizzarsi in forme di discriminazione che rischiano di accentuare il divario e le diseguaglianze sociali già esistenti: l'automatizzazione e la digitalizzazione possono infatti portare ad acuire quello che è stato denominato '*digital divide*', costituendo un ostacolo all'accesso a servizi pubblici soprattutto per i soggetti più vulnerabili, meno abbienti o meno 'digitalizzati' – cioè

pericolose) è quella della c.d. analisi predittiva. Questa tipologia di analisi si basa sull'impiego di metodi statistici che, mediante la lettura aggregata e la combinazione di dati, mirano a determinare soggetti maggiormente inclini a compiere un crimine. In questo contesto, "The development of suspect profiles involves the collection and processing of information in order to make assumptions about a data subject and his or her future behaviour. Profiles are constructed based on correlations between certain actions and certain behaviours or associations. (..) A powerful machine learning algorithm can analyse exponentially more data points and can identify more complex relationships than is possible when applying a traditional police profile" (E. SIEGEL, *Predictive analytics: the power to predict who will click, buy, lie or die*, Wiley, 2016). Come affermato da Andrejevic, quindi, "the promise of predictive analytics is to incorporate the future as a set of anticipated data points into the decision-making process" (M. ANDREJEVIC, *Infoglut: how too much information is changing the way we think and know*, Routledge, 2013). Tale strumento ha posto significativi dubbi e preoccupazioni, espressi anche da numerosi giuristi, soprattutto con riferimento alla tutela dei diritti fondamentali e alle implicazioni che misure predittive possono comportare rispetto a principi quali la presunzione di innocenza e la non discriminazione. Con riferimento a quest'ultimo aspetto, in particolare, è stato da molti messo in evidenza come, basandosi sull'impiego di algoritmi a loro volta funzionanti mediante l'utilizzo e analisi di dati, la tecnologia predittiva possa risultare discriminatoria laddove nei dati inseriti sia presente un pregiudizio, ad esempio di tipo razziale: il vizio che colpisce i dati infatti si trasferisce all'algoritmo e dunque all'esito della procedura predittiva stessa, similmente a quanto già evidenziato rispetto alla tecnologia Compas. Sul punto si rimanda, ex multis, a M. H. MURPHY, *Algorithmic surveillance: the collection conundrum*, in *International Review of Law, Computers and technology*, 2, 2017, p. 227; A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, 3, 2018.

[72] L'esempio prima richiamato del progetto Aadhaar indiano ha ben presto svelato tutti questi pericoli, talvolta legati a difetti tecnici ed intrinseci al sistema di identificazione basato su dati biometrici – ad esempio l'impiego della scansione dell'iride e delle impronte digitali non risulta sempre affidabile poiché tali dati biometrici sono suscettibili di modifiche nel corso del tempo, anche a causa di determinate patologie –, con il risultato che il *match* negativo tra dati forniti dal cittadino al momento della richiesta di identificazione e quelli conservati nel database centrale comporta il mancato accesso ad un servizio pubblico, spesso vitale o di fondamentale rilievo. Tale sistema è peraltro stato impiegato, nel corso degli anni, anche quale condizione di accesso a servizi erogati da soggetti ed operatori economici privati (servizi di telefonia o bancari), mentre l'accesso al database centralizzato è stato concesso anche ad autorità di *law enforcement* per scopi differenti da quelli meramente identificativi. Il sistema di identificazione biometrica ha così rischiato di tradursi in un potenziale strumento in grado di 'schedare' l'intera popolazione indiana e conservare dati biometrici di soggetti mai sospettati di aver commesso reati, rispetto ai quali dunque l'invasione nella sfera privata risulta difficilmente considerabile come proporzionata e necessaria. Proprio su tali aspetti critici e problematici si è pronunciata la Suprema Corte indiana, in una determinante e storica sentenza: per una analisi dettagliata di tale decisione, sia consentito il rimando a G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti*, op. cit.

meno capaci di impiegare sistemi elettronici – e traducendosi dunque non solo in "an economic or infrastructural problem. Rather, the digital divide has acquired a new meaning in recent years: it means that individuals cannot participate equally on the digital world because they do not have the educational, social, and political means to do so effectively"[73]. Ecco che, nonostante l'efficienza e *good governance* che sistemi e strumenti di digitalizzazione come quelli descritti possono contribuire a rafforzare[74], i rischi che essi comportano rispetto ai diritti alla riservatezza e alla protezione dei dati sono suscettibili di produrre effetti anche sul godimento di altri diritti fondamentali che ne risultano connessi, con un possibile impatto negativo sul godimento di servizi essenziali e di diritti sociali riconosciuti nell'ambito del Welfare e che a loro volta sono in grado di incrementare – se non addirittura 'automatizzare'[75] – diseguaglianze ed ingiustizie, ledendo così, in ultima istanza, anche la dignità della persona quale principio fondamentale di ogni società democratica.

Dalla ricostruzione sin qui fornita delle minacce e delle problematiche che Big Data, algoritmi e AI provocano e che sono spesso connesse alla natura stessa di tali strumenti, emerge tutta la complessità delle nuove sfide che il mondo del diritto deve con urgenza affrontare: sebbene gli esempi forniti in questa analisi non abbiano certamente la pretesa di completezza, essi nondimeno risultano sufficienti per tratteggiare un quadro articolato e in chiaro-scuro, composto da potenzialità ed opportunità positive, affiancate però da pericoli dai toni più cupi e preoccupanti. Insieme, queste tinte ricostruiscono l'immagine complessiva e generale, della quale si studierà poi, nel prosieguo di questo lavoro, una porzione più circoscritta ma significativa, quella della disciplina della *data retention*, rappresentativa di quanto sino ad ora evidenziato e la cui rilevanza non può essere colta se non preliminarmente inserita nella immagine più ampia che qui si è cercato di delineare.

Tale quadro unitario aiuta altresì a comprendere lo sforzo ingente che legislatori, giuristi e Corti debbono sostenere dinnanzi alla vastità di interrogativi, dubbi e problematiche che sono talvolta ignorate

---

[73] S. RANCHORDAS, *Automation of public services and digital exclusion*, in *International Constitutional Law Blog*, 11 marzo 2020. Sul punto si leggano anche: M. ZALNIERIUTE, L. BENNETT MOSES, G. WILLIAMS, *The rule of law and automation of Government decision-making*, in *The modern law review*, 3, 2019; E. BERTOLINI, *Is technology really inclusive? Some suggestions from States run algorithmic programmes*, in *Global Jurist*, 1, 2020; non a caso, su tale aspetto grande attenzione è stata prestata anche da Philip Alston, UN Special Rapporteur on extreme poverty and human rights, nel Report del 11 ottobre 2019 (A/74/493), che ha messo in luce i pericoli connessi ad una ampia diffusione del *digital welfare state*, nel quale l'utilizzo senza debite e specifiche tutele di nuovi strumenti di sorveglianza può condurre alla esasperazione di diseguaglianze e discriminazioni già esistenti, a discapito soprattutto dei soggetti più fragili ed emarginati e con il pericolo di creare quella che viene definita una "digital dystopia". Più ampiamente sull'impatto della digitalizzazione ed automatizzazione nell'ambito dei servizi di welfare nei confronti delle fasce più disagiate della popolazione, si legga: V. EUBANKS, *Automating inequality: how high-tech tools profile, police and punish the poor*, St. Martin's Press, 2018; S. O'SULLIVAN, C. WALKER, *From the interpersonal to the internet: social service digitization and the implications for vulnerable individuals and communities*, in *Australian Journal of Political Sciences*, 4, 2018.

[74] Per una ricostruzione dei diversi impieghi e potenzialità dei Big Data nell'ambito delle pubbliche amministrazioni, si legga G. KIM, S. TRIMI, J. CHUNG, *Big data applications in the Government sector*, in *Communications of the ACM*, 3, 2014.

[75] L'incremento e l'acuirsi di diseguaglianze e divari sociali anche a causa della digitalizzazione ed automazione delle pubbliche amministrazioni e dell'accesso a servizi pubblici di Welfare sono stati efficacemente riassunti in alcune espressioni, quali 'automating inequality' impiegata da Eubanks (V. EUBANKS, *Automating inequality: how high-tech tools profile, police and punish the poor*, op. cit.), o ancora 'digitizing discrimination', utilizzata da alcune ONG attive nell'ambito della tutela della riservatezza e della protezione dei dati dinnanzi alle minacce della digitalizzazione anche e soprattutto delle Pubbliche Amministrazioni (ad esempio il termine è stato impiegato in alcune dichiarazioni dal Nubian Rights Forum, una ONG keniota che si è battuta contro l'adozione di un sistema nazionale di identificazione biometrica). Questi termini mettono chiaramente in evidenza quanto un *digital welfare state* rischi di tradursi in una automazione e digitalizzazione sia di diseguaglianze già esistenti sia di nuove diseguaglianze, derivanti cioè dalla digitalizzazione stessa, che non sempre rende facilmente accessibili a tutti servizi vitali e fondamentali, o dalla automazione di talune procedure e controlli – si pensi ai sistemi di controllo fiscale automatizzati o a quelli di identificazione biometrica – che non tengono spesso in considerazione i possibili malfunzionamenti o errori di sistema e che rendono quindi necessaria l'adozione di correttivi, vie di accesso alternative nonché l'intervento dell'uomo.

dagli sviluppatori dei nuovi strumenti tecnologici e che invece devono essere ben conosciuti e compresi dal diritto, che pure si trova ad affrontare un intreccio articolato di eterogenee questioni giuridiche, strettamente interrelate a problematiche ed aspetti etico-sociali e politici[76]. Proprio la conoscenza degli strumenti consente di prendere consapevolezza del loro funzionamento e delle criticità intrinseche che esse comportano[77], costituendo la base indispensabile e primaria per trovare idonee ed adeguate soluzioni normative capaci di non imbrigliare il progresso e le opportunità che esso rappresenta ma, al contempo, di tutelare e garantire il rispetto di quei diritti fondamentali che rappresentano le radici della società moderna. Come ben affermato da Casonato, con una asserzione riferita all'AI ma che ben può essere estesa ai Big Data e al progresso delle nuove tecnologie e della 'datizzazione', "come la realizzazione di forme di pesi e contrappesi per i classici poteri statali non ne ha depotenziato la funzione, ma ne ha anzi rinforzato l'andamento e la responsabilità in termini liberali e democratici, allo stesso modo il diritto che si occupa dell'intelligenza artificiale dovrà essere attento a promuovere un pieno sviluppo del suo potenziale, evitando allo stesso tempo che si realizzino abusi e utilizzazioni contrarie ai diritti delle persone"[78].

In estrema sintesi, quanto risulta da tale citazione così come dall'analisi dei precedenti paragrafi, è come, da un lato, non sia possibile e neppure auspicabile fermare il progresso tecnologico in rapida e continua espansione: esso infatti si presenta come portatore di significative potenzialità ed opportunità, rappresentando uno strumento utile non solo a migliorare, talvolta in maniera radicale e senza precedenti, la nostra vita quotidiana, ma anche a rendere più efficienti le autorità pubbliche nello svolgimento dei loro diversi compiti. Dall'altro lato, tuttavia, sono altrettanto evidenti i rischi e i pericoli per i diritti fondamentali e per la democraticità delle nostre società: l'innovazione ha in sé la capacità di sovvertire e rivoluzionare i rapporti tra Stato e cittadini, instaurando una sorveglianza pervasiva e pericolosa, che diviene tanto più insidiosa se si pensa che la deriva verso un controllo pervasivo della vita di ogni utente è, in misura sempre maggiore, determinata dall'azione di soggetti privati,

[76] Se si pensa a quanto il potere di grandi aziende private del settore digitale abbia modificato ed inciso sullo Stato stesso e sui suoi poteri, non possono non essere richiamate vicende quali Cambridge Analytica, che hanno svelato l'enorme influenza che i colossi del web possono esercitare: le capacità di cui dispongono, che si concretizzano nella abilità di controllare i dati, di impiegarli per scopi di profilazione e di incidere così sulle decisioni dei singoli, oltre a svolgere un ruolo preponderante nel settore della informazione, scardinano quelli che prima erano i poteri centrali dello Stato e la capacità di quest'ultimo di governare e regolare tali fenomeni.

[77] Pare interessante sottolineare come una seria consapevolezza dei rischi e dei pericoli che tali strumenti possono provocare rispetto ai diritti fondamentali sia spesso carente negli stessi utenti, nei cittadini e nella società civile più generalmente intesa. Sebbene infatti negli ultimi decenni si siano moltiplicate le campagne di sensibilizzazione e informazione, mentre le diverse rivelazioni quanto alla esistenza di sistemi di sorveglianza o di utilizzi opachi dei nostri dati hanno portato all'attenzione del grande pubblico queste complesse tematiche, gli utenti sono comunque disposti a correre rischi e a concedere/cedere i propri dati. Tale atteggiamento contraddittorio viene definito comunemente *privacy paradox*: "People will often claim to be concerned about their privacy, to later disclose personal information for relatively little in return, such as their income or date of birth for a discount in an online shop, or their phone number/address to use financial services. Numerous researchers have sought to understand the privacy paradox, and as a result have offered a range of explanations, including a lack of understanding of risk and knowledge of privacy-protective behaviors, inexperience of first-hand online privacy invasions, and social influences (e.g. sharing data because their friends and family do)", in R. NORBERG, DAN HORNE, DAVID HORNE, *The privacy paradox: personal information disclosure intentions versus behaviors*, in *Journal of Consumer Affairs*, 1, 2007. Per approfondimenti si rimanda anche a: A. VIVARELLI, *The crisis of the rights to informational self-determination*, op. cit. Del resto anche Soro ha avvertito che: "poiché i dati rappresentano la proiezione digitale delle nostre persone, aumenta in modo esponenziale anche la nostra vulnerabilità. La libertà di ciascuno è insidiata da forme sottili e pervasive di controllo, che noi stessi, più o meno consapevolmente, alimentiamo per l'incontenibile desiderio di continua connessione e condivisione" (A. Soro, Garante per la protezione dei dati personali, *Big Data e Privacy. La nuova geografia dei poteri*, op. cit., p. 5), riconoscendo dunque l'impatto che la scarsa consapevolezza dei rischi o l'incapacità di 'uscire' da una logica di condivisione che ormai pervade la nostra quotidianità comporta rispetto alla tutela della riservatezza e la protezione dei nostri dati.

[78] C. CASONATO, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal*, 1, 2019, p. 179.

identificabili nelle grandi piattaforme online e nei *social network*, da Google a Facebook[79]. Da questa visione dunque, richiamando i termini impiegati da Pollicino, si può riconoscere la presenza di una concezione utopistica del progresso tecnologico dettato dai Big Data e dai sistemi di AI, contrapposta ad una concezione distopica dell'innovazione; lo stesso autore, tuttavia, propone una terza via, quella del c.d. umanesimo digitale, ovvero un allontanamento dagli eccessi di una idealizzazione in positivo o in negativo, per vedere nella digitalizzazione e nel mondo digitale un processo evolutivo che deve avere al suo centro la persona, la sua dignità e il rispetto dei diritti fondamentali[80].

Se si abbraccia dunque questa ultima visione, risulta necessario che il mondo del diritto prosegua quel dibattito e studio, già avviato ma che abbisogna di essere continuamente alimentato ed approfondito, che può condurlo a comprendere, denunciare i rischi, dialogare con il mondo della scienza e sviluppare soluzioni capaci di adeguare il diritto e i suoi istituti al progresso e a regolamentare quest'ultimo in modo da difendere e salvaguardare da rischi e minacce i suoi stessi fruitori. Prima di addentrarsi nell'analisi di questo difficile percorso, del quale si approfondirà in particolare la sfida rappresentata dallo strumento della *data retention* e le scelte adottate in tale ambito da legislatori, Corti e dottrina, si ritiene determinante comprendere preliminarmente quali diritti fondamentali risultino interessati da tale cammino, in modo da fornire così i parametri e le coordinate di riferimento utili ad orientarsi nello studio che si intende intraprendere.

2. – I diritti fondamentali alla riservatezza e alla protezione dei dati dinnanzi al progresso tecnologico: la necessaria ricostruzione di un lento ma significativo processo di affermazione

2.1. – Il diritto alla riservatezza: dalle origini negli USA al riconoscimento nel Continente europeo

Per comprendere appieno la portata delle minacce e dei pericoli che il progresso tecnologico – nelle forme sopra analizzate della 'datizzazione', della profilazione e dell'impiego di sistemi di AI – comporta, è necessario innanzitutto esaminare i diritti che, in tale contesto, risultano principalmente toccati e colpiti: si deve quindi fare riferimento al diritto alla riservatezza e al diritto alla protezione dei dati. Questi, sebbene strettamente correlati tra loro e nonostante siano spesso confusi e sovrapposti, hanno in realtà una origine ed un contenuto molto differenti, il cui percorso di affermazione e distinzione è peraltro fortemente interrelato al progresso tecnologico stesso. Come vedremo, infatti, il diritto alla riservatezza o alla vita privata viene teorizzato negli USA alla fine dell'Ottocento proprio a seguito di alcune intrusioni nella sfera privata perpetrate da uno strumento all'epoca tecnologicamente avanzato, ovvero la fotografia, che aveva fatto sorgere il bisogno di riconoscere il diritto 'ad essere lasciati soli'[81]; il diritto alla protezione dei dati, invece, nasce dall'esigenza di tutelare le informazioni e i dati originati soprattutto nel mondo digitale e in quantità senza precedenti. Proprio il susseguirsi delle innovazioni e

[79] Non a caso e con grande efficacia, Shoshana Zuboff parla di "Capitalismo della sorveglianza", sottotitolando nel suo omonimo libro "Capitalismo della sorveglianza. Il futuro dell'umanità nell'era dei nuovi poteri", come la monetizzazione dei dati da parte dei colossi del Web e delle piattaforme online abbia aperto ad una nuova forma di capitalismo fondata proprio sui dati che noi quotidianamente produciamo e cediamo e dalla elaborazione ed analisi dei quali viene tratto un enorme profitto (S. ZUBOFF, *Il capitalismo della sorveglianza*, traduzione italiana di P. Bassotti, Luiss University Press, 2019).

[80] O. POLLICINO, *Riflettere su distonie e utopie del rapporto tra tecnologia e società*, in *Giustizia Insieme*, 18 aprile 2020, p. 2.

[81] Anticipando qui le considerazioni di Warren e Brandeis nel loro *The right to privacy*, di cui si parlerà ampiamente a breve, pare utile richiamare quanto scritto dai due autori americani a proposito dell'impatto sui diritti fondamentali delle nuove tecnologie sviluppatesi a fine '800: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'", S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 4, 1890, p. 195.

l'affermarsi crescente della digitalizzazione e dunque della difficoltà di mantenere un controllo effettivo sui propri dati, sono divenuti motore di una evoluzione del diritto alla riservatezza rispetto alla sua accezione originaria.

Procedendo in ordine cronologico e dunque prendendo avvio dal diritto alla 'privacy' o alla 'riservatezza', o ancora 'alla vita privata' – termini che sono stati impiegati come sinonimi –, esso trova le sue radici, come anticipato, nella dottrina statunitense: in particolare, Warren e Brandeis, nel celebre articolo apparso sulla prestigiosa rivista Harvard Law Review del 1890 (n. 4, Vol. 193) con il titolo "The right to privacy" [82], affermavano il "right to be let alone", ovvero il diritto ad essere lasciati soli o in pace e il bisogno quindi di proteggere e regolamentare la compressione della vita privata. Il riconoscimento di questa specifica situazione giuridica soggettiva nasceva dalla necessità, concretamente percepita dai due autori, di proteggere la propria vita famigliare, il proprio domicilio e la propria sfera privata da invasioni perpetrate ad opera di fotografi (o 'paparazzi', per utilizzare un termine più moderno) di riviste di gossip. Seppure, ad un primo sguardo, il diritto alla riservatezza possa apparire, in questa sua forma embrionale, "poco più che un capriccio della borghesia avvezza alla mondanità, che chiedeva di condurre un'esistenza libera al di fuori dei riflettori della cronache scandalistiche"[83], esso in realtà esprimeva l'esigenza di tutela della sfera privata e personalistica da interferenze esterne, collegandosi così al godimento delle libertà personali e al diritto all'immunità personale. Da una attenta analisi di diversi casi giurisprudenziali della *Common Law* – in materia ad esempio di sequestro di documenti – che tutelavano la segretezza di corrispondenza e documenti sulla base dei *property rights*, Warren e Brandeis avevano infatti ritenuto di poter dedurre l'esistenza di un diritto del tutto autonomo, quello alla riservatezza appunto, che era qualcosa di più sia di un semplice privilegio della classe borghese posto a tutela della propria rispettabilità, sia del mero diritto alla proprietà privata. Il tentativo dei due autori pertanto era quello di affermare l'esistenza di una "fattispecie giuridica autonoma, non più esclusivamente legata al diritto di proprietà né coincidente con il diritto alla riservatezza delle comunicazioni interpersonali"[84], bensì identificabile nel diritto 'ad essere lasciati soli'; secondo Warren e Brandeis, "nel diritto alla privacy il contenuto spirituale ivi protetto non è tutelato per il valore che esso ha o può avere nel pubblico, nei rapporti di mercato o nei traffici giuridici, ma, al contrario, riceve protezione dal *common law* unicamente per il valore intimo, privato, che esso ha per il suo titolare"[85].

Tale diritto, così come teorizzato per la prima volta[86] alla fine dell'Ottocento[87], ha però avuto difficoltà ad affermarsi negli USA, anche per l'assenza di un espresso riconoscimento nel testo

---

[82] S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, op. cit.

[83] O. POLLICINO, M. BASSINI, *Social network e tutela dei dati personali*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, op. cit., p. 66.

[84] M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws*, 2, 2018, p. 11.

[85] A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, 1974, p. 43.

[86] "Prima di allora non è mai stata cioè formulata una specifica teoria giuridica del diritto alla privacy, ma sono stati riconosciuti e occasionalmente precisati soltanto alcuni degli aspetti che compongono il complesso quadro di questo diritto", A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, op. cit., p. 9.

[87] Merita precisare come l'esigenza di tutela della vita privata fosse emersa già nel 1849 nel Regno Unito: nella decisione *Prince Albert v. Strange*, pronunciata dalla High Court of Chancery, era stato impiegato per la prima volta il termine privacy nella sua accezione di libertà da interferenze della propria sfera privata. Non deve stupire che il caso, similmente a quello che ha dato origine al *right to be let alone* negli USA, derivasse dalla diffusione da parte di un dipendente della Royal House di alcune immagini (incisioni e disegni) raffiguranti la Regina Vittoria e il marito Alberto in un contesto privato e famigliare. Come ben sottolineato da Famiglietti, da questo caso risulta come la riservatezza nella concezione inglese fosse strettamente legata al concetto di *property*, come 'diritto borghese' e privilegio di classe: "frequenti sono state infatti le violazioni della privacy come *trespass*, ossia come violazione del diritto di proprietà o di un altro diritto della persona. La giurisprudenza inglese non ha individuato una tutela specifica della privacy, ma singoli rimedi per i casi concreti, i quali però avrebbero mostrato tutta la loro inadeguatezza ogniqualvolta la lesione della vita privata si fosse realizzata senza un'azione materiale o senza la

costituzionale federale: in questo contesto, la giurisprudenza, in particolare quella della Corte Suprema, ha quindi giocato un ruolo fondamentale nella determinazione di una tutela effettiva del diritto alla riservatezza, talvolta richiamando e facendo riferimento alle tutele inserite nel Primo Emendamento, talaltra nel Quattordicesimo (ma anche, talvolta, nel Terzo, Quarto e Nono Emendamento) e cercando nei diritti e principi in essi riconosciuti l'ancoraggio costituzionale del *right to privacy* nelle sue differenti sfaccettature (dal diritto alla riservatezza nella sua dimensione di tutela della segretezza dei convincimenti personali, degli orientamenti politici o religiosi o ancora nella dimensione di protezione della vita famigliare o ancora della corrispondenza). Così il diritto alla riservatezza, grazie allo stratificarsi della *case law*, emergeva nella sua dimensione 'negativa' di garanzia di una 'non intrusione' nella sfera personale.

Le decisioni delle Corti, che ne hanno tuttavia gradualmente colto la portata e l'ampiezza, hanno portato ad una lenta ma significativa evoluzione di tale diritto: esso è stato riconosciuto come diritto dal contenuto ben più profondo di una semplice "difesa della solitudine fisica", dovendo quindi essere inteso come strumento di garanzia "dei valori di autonomia e dignità dell'individuo", che si esemplificano e manifestano anche nella protezione della vita privata intesa nella sua dimensione di relazione, di vita all'interno della famiglia o della società[88]. Si è dunque affermato un *right to be let alone* che non era da intendersi solo restrittivamente riferito alla persona nella sua singolarità e nelle sue scelte ed orientamenti ma che, anzi, si è andato pian piano ampliando alla tutela del contesto entro cui il singolo si colloca, vive ed opera. Mediante tale progressiva lettura ed interpretazione, il diritto alla riservatezza è divenuto parte ed espressione del più ampio diritto alla immunità della persona umana, affiancandosi quindi ad "una serie di privilegi o immunità, come quello di non essere assalito o percosso, quello di non essere imprigionato arbitrariamente o dolosamente accusato, quello di non autoincriminarsi, oppure quello di non essere diffamato, i quali costituiscono l'armatura giuridica del generale diritto alla propria personalità"[89].

Il percorso che ha portato al riconoscimento di questa ulteriore e più ampia accezione del diritto alla riservatezza nella sua dimensione di connessione personalità, alla dignità umana e alle libertà fondamentali, non è stato tuttavia semplice ed immediato: i giudici, tanto statali quanto federali[90] hanno

violazione di un vincolo contrattuale o fiduciario", in questo distinguendosi dalla giurisprudenza americana che invece, seppur lentamente, si distanzia dal binomio *privacy-property* per proporre una concezione di riservatezza connessa a personalità, identità e libertà. Così G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto*, in A. D'ALOIA (a cura di), *Bio-tecnologie e valori costituzionali. Il contributo della giustizia costituzionale*, Giappichelli, 2004. Per maggiori approfondimenti sulla giurisprudenza inglese che già nell'Ottocento aveva riconosciuto la necessità di tutela della riservatezza pur senza definirla come un diritto autonomo, si rimanda a F. PETRUCCO, *The right to privacy and new technologies: between evolution and decay*, in *MediaLaws*, 1, 2019.

[88] T.E. FROSINI, *La tutela dei dati e il diritto all'oblio*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, op. cit., p. 89.

[89] A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, op. cit., p. 46. Certamente come rilevato da Solove, la teorizzazione di Warren e Brandeis presentava grandi potenzialità ma anche limiti: "the article was far ahead of its time, and it contained flashes of insight into a more robust theory of privacy. And to be fair, Warren and Brandeis' aim was not to provide a comprehensive conception of privacy but instead ato explore the roots of a right to privacy in the common law and explain how such a right could develop. The article was certainly a profound beginning toward developing a conception of privacy. However, while the right to be let alone has often been invoked by judges and commentators, it still remains a rather broad and vague conception of privacy", D. SOLOVE, *Conceptualizing privacy*, in *California Law Review*, 90, 2002, p. 1102.

[90] Nella nota pronuncia *Olmstead v. United States* (n. 277 US 438 del 1928), la Corte Suprema, con una maggioranza invero minima (5 voti contro 4), aveva ritenuto legittime le prove raccolte mediante intercettazioni telefoniche da parte degli agenti federali senza un previo mandato del giudice; gli avvocati dell'imputato Olmstead invece avevano invocato la violazione del IV Emendamento, che garantiva da intrusioni immotivate ed ingiustificate nel domicilio e nelle comunicazioni private. Diversamente dalla maggioranza, che non aveva riconosciuto quella accezione del diritto alla riservatezza inteso come diritto ad essere lasciati soli rispetto ad intrusioni nella sfera privata, considerata nelle sue diverse dimensioni – quindi anche quella delle comunicazioni telefoniche –, il giudice Brandeis, lo stesso che nel 1890 aveva teorizzato il *right to privacy* insieme a Warren,

con difficoltà e solo gradualmente superato quel binomio *privacy-property* che la Common Law aveva largamente impiegato sino agli anni sessanta del Novecento nelle cause nelle quali il *right to privacy* veniva invocato[91]. Pur non volendo entrare nei dettagli, è interessante notare come nel caso *Griswold v. Connecticut* (n. 381 US 479, del 7 giugno 1965) la Corte Suprema abbia affermato per la prima volta l'esistenza di un diritto fondamentale alla privacy emancipandolo dalla sua connessione con la proprietà privata e riconoscendone il legame con la libertà personale mediante il richiamo agli Emendamenti I, III, IV, V, IX e XIV. Nella pronuncia richiamata, così come nella successiva *Whalen v. Roe* (n. 429 US 589, del 1977), la stessa Corte Suprema ha evidenziato gli ulteriori aspetti connessi al diritto alla privacy: quelle che vengono definite "zone of privacy" non proteggono solo "the individual interest in avoiding disclosure of personal matters" ma anche "an individual's independence in making certain kinds of important decisions" (par. 599-600)[92].

La giurisprudenza americana nel corso degli anni ha quindi progressivamente inserito tra i diritti che non sono espressamente previsti dal Bill of Rights ma che debbono comunque godere di tutela costituzionale anche il diritto alla privacy che, proprio perché ancorato a diverse disposizioni costituzionali, si sostanzia in diverse declinazioni, connesse alla inviolabilità personale sotto il profilo della vita intima, delle relazioni famigliari e sociali, del domicilio, della libertà da arresti, perquisizioni e sequestri irragionevoli e immotivati, della libertà personale intesa come intangibilità del corpo, della libertà personale intesa come libertà di espressione o più ampiamente nella sua connessione alla dignità umana[93]. Già nel 1954, il giudice della Corte Suprema Douglas, nella sua *dissenting opinion* al caso *Irvine v. California* (347 US 128, 1954), aveva riconosciuto l'importanza della tutela della riservatezza come garanzia e precondizione per l'affermazione del diritto alla autodeterminazione: "the right of privacy should include the right to pick and choose from competing entertainments, competing propaganda, competing political philosophies. If people are let alone in those choices, the right to privacy will pay dividends in character and integrity. The strength of our system is in the dignity, the resourcefulness, and the independence of our people. Our confidence is in their ability as individuals to make the wisest choice. That system cannot flourish if regimentation takes hold. The right of privacy, today violated, is a powerful deterrent to anyone who would control men's minds". Iniziava dunque già

---

aveva manifestato invece una opposta opinione. Nella sua celebre *dissenting opinion*, il giudice della Corte Suprema aveva infatti ribadito: "The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings, and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone -- the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth".

[91] Per una dettagliata e ampia ricostruzione delle difficoltà riscontrate nel processo di affermazione del diritto alla privacy come teorizzato da Warren e Brandeis, nonché della giurisprudenza statunitense in materia e dell'evoluzione dal binomio *privacy-property* a *privacy-dignity/liberty* nella dottrina e nella Common Law americana, si rimanda a A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, op. cit. e a E. BLOUNSTEIN, *Privacy as an aspect of human dignity*, in *New York University Law Review*, 39, 1964; di recente: A. DI MARTINO, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, 2017.

[92] In questo caso dunque "the US Supreme Court derived a right to privacy from the various 'zones of privacy' emanating from several constitutional guarantees and prohibiting government intrusion into the intimate matters of married couples. (..) The US conception sees privacy as a 'right of the individual to decide for himself, found in the penumbras of several provisions of the Bill of Rights", M. J. CEPEDA ESPINOSA, *Privacy*, in M. ROSENFELD, A. SAJO, *The Oxford handbook of comparative constitutional law*, Oxford University Press, 2013.

[93] Come sottolineato anche da Pollicino e Bassini, il sempre più ampio significato attribuito al diritto alla riservatezza e dunque la "capacità espansiva del diritto alla privacy si è rivelata [negli USA] direttamente proporzionale alla capacità delle Corti di leggerne il fondamento – anche costituzionale – nelle maglie di principi anche molto diversi fra loro", O. POLLICINO, M. BASSINI, *Social network e tutela dei dati personali*, op. cit., p. 68.

da quegli anni a farsi strada una concezione sempre più ampia del diritto alla riservatezza[94], che si lega così al godimento di altri diritti e che può essere individuata come fondamento di una società democratica, nella quale la privacy viene concepita come baluardo avverso forme di intrusione e controllo da parte di soggetti pubblici o privati, che possono altrimenti minacciare il reale esercizio delle diverse libertà civili e politiche così faticosamente riconosciute nelle Carte costituzionali[95]. Un modo di intendere la riservatezza, questo, che, come si analizzerà più avanti, risulta estremamente anticipatorio di minacce e timori più che mai attuali nell'era della sorveglianza e della digitalizzazione, e che attribuisce grande importanza e rilievo alla tutela della privacy, della sfera intima di ciascuno di noi come espressione di libertà, anche nelle relazioni sociali ed anche nella formazione dei nostri convincimenti e scelte.

Ecco quindi che sin da questa breve ricostruzione della evoluzione del concetto di 'riservatezza', da quello originario di *right to be let alone* tutelato sulla base di *property rights* al riconoscimento di un diritto fondamentale connesso, nelle sue varie sfaccettature, alla dignità umana, è possibile comprendere, da un lato, come il diritto alla privacy sia strettamente interconnesso con altri diritti e libertà dell'individuo, aspetto sul quale verranno mosse specifiche riflessioni nei successivi paragrafi; dall'altro come sia difficile, proprio per le diverse sfaccettature di cui si compone e dei diritti cui si collega, fornirne una definizione chiara e univoca. Del resto, come affermato anche da Solove, che ricostruisce in un celebre scritto il *right to privacy* nel contesto statunitense, "Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations"[96].

Nella sua ricchezza di sfumature e nel suo esser oggetto di una continua evoluzione ed arricchimento nel contesto giurisprudenziale statunitense, il diritto alla riservatezza è approdato poi anche nel continente europeo a partire dalla metà del Novecento.

Volendosi concentrare soprattutto sul piano europeo sovranazionale – mentre a livello nazionale è da registrarsi un riconoscimento espresso del diritto alla privacy solo in taluni testi costituzionali mentre in altri, pur in mancanza di un autonomo riferimento costituzionale, tale diritto è stato affermato dalla giurisprudenza anche mediante il riferimento ad altri diritti previsti, quale quello all'identità personale[97]

---

[94] Diviene chiaro, dalle parole richiamate, l'affermarsi di un certo allontanamento o quanto meno di una importante, seppur lenta, evoluzione rispetto a quella concezione originaria, affermatasi soprattutto nella dottrina di inizi Novecento, del diritto alla privacy che si fondava su una lettura fortemente ancorata alla materia degli illeciti, prendendo "in esame l'amplissima casistica giurisprudenziale in materia di riservatezza e rendendosi conto che questa poteva essere ricondotta a quattro tipi ben definiti di *torts*. Questi ultimi, peraltro, nonostante fossero riferiti dai giudici alla figura della *privacy*, in realtà garantivano la tutela di interessi privati già garantiti dal diritto della *common law* e indipendenti dall'interesse alla riservatezza, il quale, quindi, risultava solo apparentemente rilevante nelle controversie". È solo dalla seconda metà del Novecento, dunque, che si è affermato un "differente filone giurisprudenziale costituzionale che ha utilizzato la categoria della *privacy* non nella sua veste di diritto inter-privato, e, correlativamente di illecito civile, ma come libertà fondamentale da esercitare nei confronti del potere pubblico", così F. MIDIRI, *La giuridificazione della protezione dei dati in Italia*, in *Giustamm*, 5, 2016.

[95] Westin definisce infatti la privacy come "the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others", sottolineando quindi l'aspetto relazionale e la connessione con l'autodeterminazione e la formazione della propria personalità (A. WESTIN, *Privacy and freedom*, in *Washington and Lee Law Review*, 20, 1968, p. 7); Friedman poi parla di privacy come della tutela delle scelte di vita contro qualsiasi tipo di controllo pubblico, censura o discriminazione sociale (L. FRIEDMAN, *The Republic of choice, law, authority and culture*, Harvard University Press, 1990).

[96] D. SOLOVE, *Conceptualizing privacy*, op. cit., p. 1088.

[97] Il diritto alla riservatezza è stato accolto e riconosciuto in maniera differente nei vari ordinamenti nazionali del Continente europeo: vi sono Costituzioni che riconoscono espressamente, ispirandosi al testo dell'art. 8 della Convenzione EDU, il diritto alla vita privata: basti pensare all'art. 18 della Costituzione spagnola del 1978, all'art. 35 della Costituzione slovena del 1991 che tutela il "diritto alla riservatezza e i diritti della personalità", o ancora all'art. 26 della Costituzione portoghese del 1976 che inserisce nella medesima disposizione il diritto alla riservatezza "dell'intimità della vita privata e famigliare" e quello all'identità personale e allo sviluppo della

–, il Consiglio d'Europa ha mostrato in maniera decisa di voler affermare il diritto alla privacy come diritto fondamentale: nella Convenzione europea dei diritti dell'uomo (CEDU) del 1950, infatti, l'art. 8 tutela il diritto alla vita privata e famigliare, nella sua ampia dimensione che ricomprende anche domicilio e corrispondenza; tale diritto, tuttavia, non ha carattere assoluto ed anzi al comma 2 stesso vengono ammesse alcune restrizioni ed ingerenze, accompagnate da debite limitazioni e garanzie, espressione moderna, se si vuole, delle salvaguardie che avevano portato, secoli prima, al riconoscimento dell'*habeas corpus*. Così l'ingerenza nella sfera privata da parte di autorità pubbliche può essere legittimata solo se prevista dalla legge e se si riveli come necessaria, in una società democratica, per raggiungere scopi ben specificati, per quanto ampi, quali la sicurezza nazionale, la sicurezza pubblica, il benessere economico del Paese, la difesa dell'ordine e la prevenzione di reati, la protezione della salute e della morale, la protezione dei diritti e libertà altrui (art. 8, co. 2). Certo, come si vedrà nel Capitolo IV, Parte II con specifico riferimento ai sistemi di sorveglianza per scopi securitari, l'ampiezza dei termini utilizzati nel dettato della CEDU nonché i labili confini di quanto possa realmente essere considerato 'necessario in una società democratica', hanno comportato non poche incertezze interpretative cui la Corte europea dei diritti dell'uomo (Corte EDU) ha tuttavia cercato di sopperire con la sua giurisprudenza, chiarendo i contorni ed i confini dell'art. 8 CEDU rispetto ad intrusioni nella sfera privata, anche e soprattutto da parte di pubbliche autorità.

Al di là di tali riflessioni, comunque, quanto è in questa sede importante sottolineare è come già nel 1950 nel Vecchio Continente fosse stato dato pieno riconoscimento al diritto alla riservatezza, quanto meno nella sua accezione 'negativa' di *right to be let alone*, di rispetto della vita privata, delle relazioni famigliari e sociali, nonché della abitazione e delle forme di comunicazione. Anche l'Art. 8 CEDU dunque evidenzia come il diritto alla riservatezza si componga di due dimensioni, già individuate anche da Warren e Brandeis: quella individuale e quella relazionale. Non limitandosi infatti alla tutela della sola vita privata, ma anche dei rapporti sociali, viene riconosciuto come il diritto alla privacy non sia solo da intendersi come salvaguardia "against arbitrary interference by the public authorities in his private family life"[98], ma anche come "right to personal development". In questa ultima e forse più complessa accezione riconosciuta dai giudici di Strasburgo, "Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world"[99]. L'intervento della Corte EDU e le sue rilevanti decisioni dunque hanno permesso l'affermarsi di una visione del diritto alla riservatezza del tutto simile a quella richiamata dal giudice Douglas già nel 1954, capace di cogliere la privacy nelle sue ulteriori declinazioni, diverse rispetto al

---

personalità. In altri ordinamenti, invece, il diritto alla privacy non ha ottenuto esplicito riconoscimento nel testo costituzionale: in Francia è solo nell'art. 9 del Code Civil che viene fatto riferimento al diritto alla vita privata; in Italia la Costituzione riconosce l'inviolabilità del domicilio (art. 14) e la segretezza e libertà della corrispondenza (art. 15), mentre non trova spazio autonomo il diritto alla vita privata e famigliare; a riconoscere però il diritto alla privacy come valore costituzionale e diritto fondamentale è stata la giurisprudenza: sentenze quali la n. 366 del 1991 della Corte costituzionale o la n. 5525 del 2012 della Sez. III Civ. della Corte di Cassazione hanno attribuito rango di diritto fondamentale al diritto alla riservatezza, che trova il proprio ancoraggio costituzionale in libertà espressamente riconosciute quali quelle di cui agli artt. 2, 3, 13, 15, 21 e 32 (per approfondimenti sul punto, tra i tanti, si rimanda a G. ALPA, B. MARKESINIS, *Il diritto alla privacy nell'esperienza di common law e nell'esperienza italiana*, in *Rivista trimestrale di diritto civile e procedura civile*, 1974; T. M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, Cedam, 2004; U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffré, 2008). Come sottolineato da Cepeda Espinosa, merita comunque rilevare come, similmente al legislatore nazionale, anche l'intervento giurisprudenziale sia stato portatore, nei diversi Stati, di diversi approcci al diritto alla privacy e alla sua definizione, risentendo anche delle differenze riscontrabili nella cultura – giuridica e non – dei diversi ordinamenti. Così "privacy in some countries is associated with specific legal ideas, such as inviolability of domicile and the secrecy of correspondence, whereas in others it is related to broad concepts such as freedom, dignity, autonomy", M. J. CEPEDA ESPINOSA, *Privacy*, op. cit., p. 968.

[98] Corte EDU, *Case "relating to certain aspects of the laws on the use of languages in education in Belgium" v. Belgium*, n. 1474/62, 9 febbraio 1967.

[99] Corte EDU, *Bensaid v. UK*, n. 44599/98, 6 febbraio 2001.

mero diritto ad essere lasciati soli[100]. Si determina così anche nel Continente europeo quella che Mantelero chiama la *decisional privacy* ovvero la "libertà di autodeterminarsi rispetto alle scelte personali, siano esse pertinenti alla procreazione, la libertà sessuale o la libertà di organizzazione"[101]. Viene dunque accolto quel passaggio, di cui già Warren e Brandeis avevano – seppur in termini più vaghi – parlato e che più lentamente si era affermato nella dottrina e nella giurisprudenza statunitense, da una "configurazione individualistica" del diritto alla privacy ad una "concezione sociale", come diritto "funzionale al libero esplicarsi della persona"[102] e come "diritto della personalità"[103].

Una ulteriore e significativa conferma del riconoscimento e della tutela del diritto alla riservatezza nel contesto europeo è da rinvenirsi poi nella Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza) adottata nel 2000 ma che, come noto, ha acquisito il medesimo valore giuridico dei Trattati solo nel 2009 con il Trattato di Lisbona[104]. In tale testo ha trovato espressa affermazione, all'art. 7, il diritto al rispetto della vita privata e della vita famigliare, con un dettato del tutto simile a quello della CEDU: "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni". Come vedremo, tuttavia, la maggiore innovazione apportata dalla Carta di Nizza è quella di aver riconosciuto uno spazio autonomo al diritto alla protezione dei dati, considerato frutto dell'evoluzione del diritto alla vita privata e dello sviluppo della tecnologia e della digitalizzazione che hanno portato all'esigenza di garantire agli individui una forma di controllo sulle informazioni ed i dati che essi stessi producono e che li riguardano e, per certi versi, definiscono.

Rimandando al paragrafo successivo l'approfondimento circa questo particolare aspetto, l'analisi sin qui svolta permette di trarre alcune considerazioni sul diritto alla riservatezza: sebbene non sia questa la sede per ricostruire gli interventi dei giudici di Strasburgo e di Lussemburgo in materia di riservatezza generalmente intesa – si esaminerà invece tale diritto mediante la specifica lente della disciplina della *data retention*, con particolare attenzione a come in essa il diritto alla privacy è stato tutelato da giudici tanto sovranazionali quanto nazionali –, si può sin da ora cogliere la complessità del diritto alla riservatezza, dalla sua prima teorizzazione come diritto ad essere lasciati soli, inizialmente letto alla luce dei canoni dei *property rights*, ad una accezione più ampia e comprensiva dei diversi aspetti che compongono la sfera privata, identificati non solo nella parte più intimistica o nel domicilio o corrispondenza bensì anche in una dimensione più vasta, di costruzione della personalità e della identità mediante la relazione con l'esterno. Ed è da questa evoluzione, affermatasi anche e soprattutto attraverso l'intervento della giurisprudenza – come si è visto negli USA ma come è avvenuto anche a livello

[100] Come sottolineato da Tiberi, il fatto che sia stato proprio l'intervento della Corte EDU ad ampliare e, se vogliamo, a riempire di significato l'art. 8 CEDU, "non dovrebbe destare sorpresa: è del resto tipico della giurisprudenza della Corte di Strasburgo il procedere secondo un approccio casistico. È stato anzi lo stesso giudice europeo ad aver rinunciato scientemente a definire quale sia la nozione di vita privata, constatandone la valenza estremamente dinamica con il mutare delle epoche, dei contesti, dei costumi sociali in cui vive l'individuo", proteggendo così la Convenzione stessa dal rischio "di diventare un testo anacronistico". Mediante la sua giurisprudenza, dunque, i giudici di Strasburgo hanno affermato che "sarebbe troppo restrittivo limitare la nozione di vita privata ad una cerchia intima nella quale ciascuno può condurre la sua vita personale come crede, ed escludere completamente il mondo esterno a tale cerchia. Il rispetto alla vita privata deve perciò anche comprendere una sfera esterna del soggetto, cioè il diritto dell'individuo di stringere e sviluppare relazioni sociali con altri individui e con il mondo esterno in generale, che si tratti di sfera intima o sessuale, o che riguardi invece il campo professionale e commerciale", G. TIBERI, *Il diritto alla protezione dei dati personali nelle Carte e nelle Corti sovranazionali (in attesa del Trattato di Lisbona)*, in *Cassazione Penale*, 11, 2009.

[101] A. MANTELERO, *Il costo della privacy tra valore della persona e ragione dell'impresa*, Giuffré, 2007. In questa prospettiva quindi il diritto alla vita privata "riguarda la stessa libertà personale del soggetto, la sua individualità, il suo diritto a sviluppare liberamente la sua personalità", come scrive M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *EJJL*, 1, 2013.

[102] S. BONFIGLIO, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Diritto e Sicurezza*, 3, 2014.

[103] L. CALIFANO, *Privacy e sicurezza*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli, 2013.

[104] Il Trattato di Lisbona è stato sottoscritto il 13 dicembre 2007 ma è entrato in vigore il 1 dicembre 2009.

europeo –, che il diritto alla riservatezza si è sempre più espanso e arricchito di contenuti e significati, assumendo così un carattere trasversale[105] e difficile da definire in maniera fissa ed univoca ma senza dubbio "sempre più accostato al valore persona come mezzo per tutelare la sua dignità e il suo sviluppo all'interno della società"[106].

2.2. – Dalla dimensione negativa del diritto alla riservatezza a quella positiva del diritto alla protezione dei dati: la progressiva 'datizzazione' e la necessità di un riconoscimento autonomo alla **data protection**

L'avvento delle nuove tecnologie, nonché l'affermarsi della digitalizzazione e della 'datizzazione' hanno imposto nuovi bisogni ed esigenze di tutela, evidenziando altresì i limiti della protezione offerta dal diritto alla riservatezza inteso sia nella sua dimensione 'negativa' di diritto ad essere lasciati soli quanto in quella di diritto alla autodeterminazione, inteso cioè nella sua accezione di *right to personal development*. Le insidie legate alle innovazioni e al progresso tecnico-scientifico sono infatti divenute sempre più complesse e difficili da identificare, così che il solo diritto alla vita privata, pur nel suo significato più ampio, si è rivelato insufficiente a proteggere da invasioni della sfera privata estremamente pervasive ed insidiose, prodotte da operazioni concretizzatesi sempre più in forme di controllo, raccolta, archiviazione e utilizzo di dati prodotti nel Web o dall'utilizzo di sistemi e dispositivi elettronici.

Mentre l'invasione nella sfera personale che Warren e Brandeis avevano subìto mediante l'operato di fotografi, che erano 'entrati' nelle loro case riprendendo feste e vita famigliare, era del tutto palese e chiara nel suo risultato, le moderne tecnologie, attraverso l'impiego di algoritmi, sistemi di AI o creazione di banche dati, appaiono molto più articolate, subdole e meno manifeste: molte volte l'utilizzo che viene fatto dei nostri dati non risulta affatto chiaro o evidente e dunque non sempre ci consente di comprendere di essere sottoposti a sorveglianza o di subire una compressione indebita della sfera privata[107]. Come le rivelazioni di Snowden e il caso Cambridge Analytica hanno messo drammaticamente in evidenza, perdiamo spesso ogni controllo sui dati che produciamo quotidianamente, sovente senza averne alcuna consapevolezza; i sistemi di sorveglianza ed analisi dei dati, spesso segreti, traggono vantaggio da letture aggregate delle nostre tracce digitali, in modi e per finalità che difficilmente riusciamo a comprendere e quindi a limitare; l'affermazione di un *Welfare State* sempre più digitalizzato e dunque di un numero crescente di dati raccolti da soggetti pubblici, l'espansione significativa delle attività di soggetti privati le cui attività economiche si fondano proprio sulla raccolta e analisi di dati – anche non personali –, unitamente alle potenzialità enormi che la lettura aggregata di dati e le tecniche di profilazione comportano, hanno creato un panorama in cui la sfera

---

[105] S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006.

[106] E. BRUGIOTTI, *La privacy attraverso le 'generazioni dei diritti'. Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *Dirittifondamentali.it*, 2, 2013, p. 4. Come osservato anche da Rodotà, "l'originaria definizione della privacy come diritto a essere lasciato solo non è stata cancellata, ma fa parte di un contesto via via arricchito da diversi punti di vista: il diritto di controllare l'uso che altri fanno delle informazioni che mi riguardano, la tutela delle scelte di vita contro ogni forma di controllo" (S. RODOTÀ, *Il diritto di avere diritti*, Laterza, 2013, p. 320).

[107] Come rilevato da Tiberi, infatti, "Se le limitate possibilità di incisione della sfera privata, ridotte sostanzialmente alla stampa e alla fotografia, avevano inizialmente fatto convergere il dibattito sui profili dell'aggressione e interferenza nella vita privata da parte dei mezzi di comunicazione e, di conseguenza, sulla pretesa dell'individuo leso alla divulgazione di fatti e notizie private, i nuovi mezzi informatici, avendo moltiplicato esponenzialmente le occasioni di possibili violazioni dell'intimità, hanno conferito una dimensione del tutto nuova al tema, finendo per conferire un 'nuovo volto' alla originaria riservatezza", G. TIBERI, *Il diritto alla protezione dei dati personali*, op. cit.

privata risulta essere posta ancor più sotto pressione rispetto al passato, con notevoli rischi, come si è detto, anche per quella libertà di scelte e di autodeterminazione che chi controlla i nostri dati può realmente influenzare e comprimere. Come affermato in maniera lungimirante da Vittorio Frosini, precursore del diritto alla protezione dei dati che con lucidità aveva riconosciuto sin dagli anni '80 dello scorso secolo le minacce della digitalizzazione e 'datificazione', "la dinamica interna della società massificata comporta la tendenza all'accrescimento costante dei dati di riferimento nella memoria elettronica, questa coscienza artificiale collettiva della società del nostro tempo che consiste in un procedimento di riduzione e di omogeneizzazione statistica delle operazioni individuali, e in una progressiva sottrazione delle azioni alla sfera della riservatezza"[108].

Se quindi prima dell'affermazione massiva delle nuove tecnologie e della loro pervasività nella sfera privata era la diffusione di notizie e di fatti attinenti alla vita privata, famigliare o sociale di un soggetto a rappresentare la più grande minaccia alla riservatezza, ora invece il pericolo maggiore è rappresentato dal fatto che i dati che lasciamo dietro di noi ogni giorno possono essere impiegati per ricostruire nel dettaglio la nostra vita, abitudini, preferenze, orientamenti politici o sessuali. Proprio per questo viene affermato come l'interesse da proteggere debba essere ampliato: "non solo l'interesse che non siano raccolte e diffuse informazioni che non si intende fornire o di cui si è disposti a dare conoscenza entro ambiti limitati, ma anche l'interesse ad impedire il collegamento di informazioni diverse che ci riguardano, anche da noi stessi fornite, al fine di evitare aggregazioni di informazioni per scopi non voluti o non previsti"[109]. L'attenzione e l'esigenza di tutela forte e specifica si sposta quindi sui dati e sulla loro raccolta, impiego, trattamento, conservazione, accesso.

È in questo contesto mutato dal progresso tecnologico e caratterizzato da nuove minacce che viene ad affermarsi lentamente ma in maniera decisa una evoluzione dal diritto alla riservatezza inteso come tutela statica e negativa, ad una tutela dinamica e positiva, che segue cioè non il soggetto ma i dati da esso prodotti: si viene a delineare il diritto alla protezione dei dati, proiezione del diritto alla privacy nella dimensione tecnologica[110], che attribuisce caratteri del tutto nuovi sia rispetto alla originaria dimensione negativa della riservatezza di origine statunitense, sia rispetto alla evoluzione, negli USA e nel continente europeo, di una tutela della vita privata intesa anche quale autodeterminazione e libertà di scelte riguardanti la propria personalità. Sotto quest'ultimo profilo, infatti, il diritto alla protezione dei dati, consentendo e tutelando un controllo sui dati e sugli usi che vengono fatti delle informazioni che produciamo, si connette ad una diversa dimensione del diritto all'autodeterminazione, che non è più quella *decisional privacy* di cui si è parlato sopra, bensì diviene una *informational privacy* che si "manifesta cioè in una sorta di signoria sulle informazioni inerenti la propria persona, traducendosi in un limite non solo alla diffusione di indiscrezioni sulla vita privata, ma anche, più in generale, alla raccolta ed all'impiego arbitrario dei dati personali"[111]. Questo concetto di una nuova e diversa dimensione della autodeterminazione è stato del resto sottolineato tanto dalla dottrina quanto dalla giurisprudenza: sotto il primo profilo, Frosini già nel 1981 parlava di libertà informatica nella sua accezione positiva che esprime cioè "la facoltà di esercitare un diritto di controllo sui dati concernenti la propria persona che sono fuoriusciti dalla cerchia della privacy per essere divenuti input di un programma elettronico; e dunque libertà informatica positiva, o diritto soggettivo riconosciuto, di conoscere, correggere, togliere o aggiungere dati in una scheda personale elettronica"[112]. Un diritto

[108] V. FROSINI, *Teoria e tecnica dei diritti umani: i diritti umani nella società tecnologica*, ESI, 1993, p. 37.
[109] G. TIBERI, *Il diritto alla protezione dei dati personali*, op. cit., p. 4469.
[110] S. RODOTÀ, *Tecnologia e diritti*, Il Mulino, 1995.
[111] A. MANTELERO, *Il costo della privacy tra valore della persona e ragione dell'impresa*, op. cit.
[112] Relazione di V. FROSINI, *La protezione della riservatezza nella società informatica*, in N. MATTEUCCI, *Privacy e banche dei dati*, Il Mulino, 1981. Ma anche in V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in AA. VV., *Il riserbo e la notizia*, Jovene, 1983. Le opere ed il pensiero di Frosini rappresentano ancora oggi un punto fermo ed un imprescindibile spunto di riflessione sul rapporto tra diritto e società informatica, nonché sull'impatto dell'evoluzione tecnologica rispetto a quella giuridica e normativa – quello che è stato efficacemente

quindi all'autodeterminazione informativa che trova, proprio negli stessi anni in cui tale diritto inizia ad affermarsi in dottrina, una storica e rilevante conferma nella c.d. 'decisione sul censimento' (Volkszahlungsentscheidung, BVerfG 65, NJW) del Tribunale costituzionale federale tedesco e risalente al 15 dicembre 1983. Con tale pronuncia i giudici riconoscono il diritto all'autodeterminazione informativa che, come riassunto da Di Martino, "presuppone che a ciascuno sia assicurata la libertà di decidere in ordine alle azioni da intraprendere o da omettere, per poi comportarsi di conseguenza. Chi non può valutare la diffusione delle informazioni che lo riguardano in un determinato ambiente sociale, può essere sostanzialmente dissuaso dall'intraprendere azioni che altrimenti avrebbe liberamente scelto", così che "tale diritto è ricostruito come una concretizzazione del diritto generale della personalità di cui agli artt. 1, I co., 2, II co., GG, (..) nel potere di ciascuno di decidere sostanzialmente da sé circa la rivelazione e l'utilizzo dei propri dati personali"[113]. Proprio da questo legame tra libero sviluppo della personalità e adeguata protezione dei dati che ci riguardano deriva l'invocazione da parte della dottrina e della giurisprudenza del riconoscimento di un diritto al controllo sulle informazioni e sui dati prodotti: è quello che Rodotà chiama con il suggestivo termine dell'*habeas data*, inteso come sviluppo del più antico *habeas corpus*, ovvero di una esigenza, maturata dal mutare delle circostanze, di passare dalla tutela della libertà del corpo, nella sua accezione fisica e di intendimento, alla tutela della libertà della persona nella sua dimensione 'datizzata', cioè di ciò che i nostri dati rappresentano e consentono di rappresentare di noi stessi. Il diritto alla protezione dei dati come espressione di questo *habeas data*, non protegge, a differenza del diritto alla riservatezza, la vita privata, famigliare, sociale nella quale e mediante la quale si può formare e sviluppare la personalità ed identità dell'individuo, bensì il dato, l'informazione prodotta di noi stessi o da noi stessi in quanto utenti di servizi. Proprio perché tali informazioni possono rivelare tanto di noi, esse devono essere oggetto di debita tutela rispetto a possibili utilizzi illeciti ed operazioni di raccolta, trattamento, conservazione, accesso, trasferimento e circolazione. Dunque, come magistralmente riassunto da Rodotà, "Il cambiamento è stato colto quando ci si è resi conto che la tradizionale nozione di privacy, come diritto a essere lasciato solo, non era più in grado di comprendere una dimensione così profondamente mutata. (..) La rivoluzione elettronica ha trasformato la nozione stessa di sfera privata, divenuta sempre più intensamente luogo di scambi, di condivisione di dati personali, di informazioni la cui circolazione non riguarda più soltanto quelle in uscita, di cui altri possono appropriarsi o venire a conoscenza. Interessa anche quelle in entrata, con le quali altri invadono quella sfera, in forme sempre più massicce e indesiderate e così la modificano continuamente. (..) Si è così prodotto un mutamento qualitativo. Nata come diritto dell'individuo borghese di escludere gli altri da ogni forma di invasione della propria sfera privata, la tutela della privacy si è sempre più strutturata come diritto d'ogni persona al mantenimento del controllo sui propri dati, così riflettendo la nuova situazione nella quale ogni persona cede continuamente, e nelle forme più diverse, dati che la riguardano"[114].

---

chiamato "l'orizzonte giuridico di Internet", V. FROSINI, *L'orizzonte giuridico di Internet*, in *Il diritto dell'informazione e dell'informatica*, 2, 2000, p. 271 ss –. In questo senso debbono essere lette le intuizioni e gli studi innovativi di Frosini che, sin dal volume *Cibernetica, diritto e società*, Edizioni di Comunità, 1968, ha messo in luce i profondi interrogativi che devono muovere il giurista 'tecnologico', sia sotto il profilo teorico quanto sotto quello pratico (sul punto V. FROSINI, *The lawyer in technological society*, in *European journal of law, philosphy and computer science*, 1-2, 1998, p. 293 ss.).

[113] A. DI MARTINO, *La protezione dei dati personali*, in S. PANUNZIO (a cura di), *I diritti fondamentali e le Corti in Europa*, Jovene, 2005. Vivarelli, a commento di tale pronuncia, sottolinea come "an individual not only decides if and how to disclose personal information; s/he also has the power to control its subsequent dissemination. This result definitively marks the transition from a static view of privacy to a dynamic one known as 'informational privacy'", A. VIVARELLI, *The crisis of the rights to informational self-determination*, op. cit., p. 308.

[114] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, op. cit., p. 35. Come poi ribadito e sottolineato da altri esperti in materia, il "percorso di costruzione del diritto alla protezione dei dati personali si intreccia con il crescente sviluppo dell'innovazione tecnologica delle comunicazioni elettroniche alla base della nostra società digitale e della globalizzazione delle relazioni interpersonali, economiche, finanziarie e sociali", L. CALIFANO,

Ebbene, il riconoscimento sino ad ora descritto di un diritto autonomo alla protezione dei dati come distinto e differente da quello alla riservatezza ha visto un lento e complesso percorso di affermazione nel contesto europeo. Volendo ripercorrere le tappe che hanno contrassegnato tale fondamentale diritto, non si può che partire dalla già richiamata Convenzione EDU e, in particolare, dall'analizzato art. 8: esso, infatti, come si è visto, garantisce il diritto alla vita privata senza fare alcun cenno alla protezione dei dati. Tale mancanza può essere facilmente spiegata ricordando che all'epoca della redazione di tale testo la tecnologia era prevalentemente intesa come strumento volto al raggiungimento di uno scopo e non come "fattore capace di influenzare le modalità di esercizio di un diritto o addirittura capace di elaborarne di nuovi"[115]. Così il nucleo duro dell'art. 8 CEDU, nel suo dettato normativo, non pare lasciare spazio ad una visione dinamica e positiva della privacy nella dimensione di tutela del dato[116].

Proprio per questo limite del testo dell'art. 8 CEDU rispetto al mutare della società e delle esigenze di tutela[117], il Consiglio d'Europa si è mostrato sin dagli anni '80 del Novecento consapevole della necessità di integrare la Convenzione con indicazioni che fornissero una base comune di protezione dei dati, anche e soprattutto per fronteggiare l'emergere confuso e disomogeneo, in quegli stessi anni, di normative nazionali in materia di *data protection*[118]. Frutto di questo bisogno, sempre più avvertito, è

Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, op. cit., p. 2. Così che "la stessa definizione ed il contenuto essenziale della riservatezza devono allora adeguarsi, dal momento che il problema non è più soltanto quello di evitare l'ingerenza e la diffusione, che rappresentano l'aspetto primitivo della questione, essendosi il baricentro adesso spostato dall'esigenza di isolamento al potere di controllo sulle informazioni rilevanti per l'interessato, anche dopo che siano divenute conosciute all'esterno", G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto*, op. cit., p. 320.

[115] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016, p. 57.

[116] Secondo Pollicino, infatti, il dettato dell'art. 8 CEDU è portatore di "una dimensione statica, dunque, di riservatezza e a contenuto prevalentemente negativo, non in grado di cogliere appieno il dinamismo del processo tecnologico che ha portato alla emersione di un'autonomia concettuale del diritto alla protezione del dato personale nell'ambito di quel processo, *work in progress*, che coincide con il trattamento del dato stesso", O. POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in *www.forumcostituzionale.it*, 31 dicembre 2013.

[117] G. BUQUICCHIO, *Aspetti internazionali della protezione dei dati: il ruolo svolto dal Consiglio d'Europa*, in MATTEUCCI, *Privacy e banche dati*, Il Mulino, 1981. Tiberi sul punto evidenzia come "nel 1969 l'Assemblea Parlamentare del Consiglio d'Europa pose al Consiglio dei Ministri la questione relativa all'effettiva capacità dell'art. 8 CEDU di salvaguardare i soggetti privati nei confronti di un utilizzo abusivo della tecnologia informatica. Il Comitato dei Ministri, nel rispondere negativamente, adottò due risoluzioni in materia, che definirono le guidelines entro cui poi fu predisposta la successiva Convenzione n. 108 del 1981", G. TIBERI, *Il diritto alla protezione dei dati personali*, op. cit. Su questa tematica si legga anche E. PAVARANI, *Diritto al rispetto della vita privata e familiare*, in C. DEFILIPPI, D. BOSI, R. HARVEY, *La Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, ESI, 2006, p. 291 ss.

[118] La Germania fu il primo Stato europeo ad approvare leggi in materia di protezione dei dati personali: la prima disciplina in tema, infatti, fu quella adottata dal Land dell'Assia che nel 1970 aveva predisposto una normativa a tutela dei lavoratori e dei loro dati personali dinnanzi a forme di schedatura indebita e di conservazione di dati all'interno di banche dati apposite create dai datori di lavoro. Risale poi al 1992 la "Ley Organica de regulacion del tratamiento automatizado de los datos de caracter personal" adottata in Spagna qualche anno prima della Direttiva 95/46/CE. Merita poi sottolineare come anche in alcuni testi costituzionali di fine anni '70 sia possibile trovare il riconoscimento di un autonomo diritto alla protezione dei dati: è il caso dell'art. 35 della Costituzione portoghese che stabilisce che: "tutti i cittadini hanno il diritto di accesso ai dati informatici che li riguardano, potendone esigere la rettifica e l'aggiornamento, e il diritto di conoscere la finalità cui sono destinati, nei termini della legge. 2. La legge definisce il concetto di dati personali così come le condizioni applicabili ad essi quanto a trattamento automatizzato, connessione, trasmissione e utilizzazione, garantendone la protezione specificatamente attraverso organismi amministrativi indipendenti. 3. L'informatica non può essere utilizzata per il trattamento di dati relativi a convinzioni filosofiche o politiche, affiliazione a partiti o sindacati, fede religiosa, vita privata e origine etnica, salvo mediante consenso espresso del titolare, autorizzazione prevista per legge con garanzie di non discriminazione o nel caso di elaborazione di dati statistici non identificabili individualmente. 4. È vietato l'accesso ai dati personali di terzi, salvo in casi eccezionali previsti dalla legge. 5. È vietata l'attribuzione di un numero nazionale unico ai cittadini"; la Costituzione dei Paesi Bassi invece dispone all'art. 10, co. 2 che debba essere

l'adozione della Convenzione di Strasburgo n. 108/1981 "sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale", non a caso il primo strumento normativo a livello internazionale che ha riconosciuto e stabilito principi in ambito di tutela dei dati[119]. Anche grazie a tale intervento, cui poi la stessa Corte EDU si è ispirata e ha fatto riferimento[120], si è dunque ampliato l'ambito di tutela fornito dallo statico art. 8, estendendolo anche ai dati che necessitano di protezione specifica dinnanzi alle invasive e sempre più pregnanti nuove tecnologie. Viene così per la prima volta fornita, all'interno di un testo normativo di diritto internazionale, la definizione di dato personale, inteso come "ogni informazione concernente una persona fisica identificata o identificabile" (art. 2, lett. a), e vengono espresse una serie di tutele e principi quali la correttezza del trattamento, la liceità dello stesso nonché il divieto di trattamento di "categorie speciali di dati", quelle che noi chiamiamo comunemente 'dati sensibili', ovvero i dati di carattere personale "indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale" che "non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzia adatte" (art. 6). Si ha dunque una prima concretizzazione del diritto positivo alla protezione dei dati che resta tuttavia qui legato all'art. 8 CEDU, risultandone una sorta di 'appendice' o ulteriore esplicazione, come "diritto alla vita privata nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano" (art. 1). Pur nella sua forma embrionale, ancora legata al diritto alla vita privata, non può essere comunque negata l'importanza di questo atto normativo, che viene riconosciuto come il "minimo comune denominatore della protezione dei dati in Europa, su cui sarà costruita la successiva normazione a livello comunitario"[121]. Sarà proprio a livello dell'Unione europea, infatti, che tale diritto ottiene un solido ed autonomo riconoscimento[122]: "pochi altri diritti appartenenti alla c.d. 'nuova generazione' possono vantare l'autentica e solida matrice europea che è propria del diritto alla protezione dei dati personali"[123].

Sulla scia dell'intervento del Consiglio d'Europa, infatti, l'Unione europea nel 1995 ha adottato la nota Direttiva 95/46/CE 'relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati', al cui Considerando 3, significativamente, si leggeva: "l'instaurazione e il funzionamento del mercato interno, nel quale è assicurata la libera

affidato ad una legge ordinaria il compito di determinare una disciplina normativa completa sul trattamento dei dati personali.

[119] Tale Convenzione era peraltro aperta alla firma e ratifica non solo degli Stati membri del Consiglio d'Europa bensì anche di Stati terzi.

[120] Pur non potendo, in questa sede, analizzare tutte le pronunce della Corte EDU nelle quali vi è un riconoscimento del diritto alla protezione dei dati come riconducibile alla tutela offerta dall'art. 8 della Convenzione, pare utile e chiara la sintesi proposta da De Hert e Gutwirth: "without having at its disposal an explicit data protection right, the Court has brought many data protection aspects under the scope of Art. 8 of the Convention. (..) The Strasbourg Court has expressed the view that the protection of personal data is fundamentally important to a person's enjoyment of his or her right to respect for private life. Through its references to the 1981 Data Protection Convention, the Strasbourg Court has endorsed and spread the idea that data protection is more than just technical regulation. (..) But we have also to underline some of the shortcomings of the Strasbourg reception of data protection: not all data are protected, the recognition of the rights to information and access is far from straightforward", P. DE HERT, S. GUTWIRTH, *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, in S. GUTWIRTH, Y. POULLET, P. DE HERT. C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing data protection?*, Springer, 2009, p. 27.

[121] G. TIBERI, *Il diritto alla protezione dei dati personali*, op. cit.

[122] In questo senso, e proprio riconoscendo l'importanza della dottrina, di alcuni interventi giurisprudenziali nazionali come quello tedesco sopra richiamato nonché dell'intervento del Consiglio d'Europa, è possibile condividere l'affermazione secondo cui "Le radici europee della privacy e della protezione dei dati personali non sono solo il risultato dell'evoluzione del paradigma negativo americano, ma anche di una maturazione europea avvenuta nella seconda metà del XX secolo", G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, op. cit.

[123] L. CALIFANO, *Introduzione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, op. cit.

circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona". Tale premessa risulta riassuntiva dell'iniziale approccio del legislatore europeo in materia: la vocazione economica e l'obiettivo di realizzare il Mercato Unico emergono con chiarezza quale espressione del modello di Unione europea posto alla base del Trattato di Maastricht e fondato sull'obiettivo di abbattere le barriere alla libera circolazione di merci, servizi e persone. Proprio prendendo atto che le disomogeneità riscontrate nelle differenti normative in materia di protezione dei dati che nel frattempo vari Stati membri avevano adottato rappresentavano barriere immateriali che rendevano difficoltosa la realizzazione di un mercato unico e libero, è stata adottata la Direttiva 95/46 che trovava infatti la propria base giuridica nell'art. 95 TCE (Trattato che istituisce la Comunità europea) che consentiva l'adozione da parte della Comunità europea di misure di ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri aventi per oggetto appunto l'instaurazione ed il funzionamento del mercato interno. La Direttiva del 1995, la prima in materia di protezione dei dati a livello comunitario, viene denominata "Direttiva madre" poiché, riprendendo ma anche ampliando ed approfondendo i principi delineati nella Convenzione di Strasburgo, ha aperto la strada ad altri atti normativi relativi alla protezione dei dati, uno dei quali, la Direttiva 2002/58 (c.d. Direttiva *e-privacy*), che verrà ripresa approfonditamente nella successiva analisi, è finalizzata a determinare la disciplina della *data protection* nello specifico ambito delle telecomunicazioni.

Se la Direttiva 95/46 metteva così in rilievo quel preponderante interesse economico che aveva ispirato e mosso l'azione della Comunità europea ai suoi esordi, proponendo così un bilanciamento tra libertà e diritti fondamentali, tra cui il riconosciuto ed affermato diritto alla vita privata da un lato, e la libera circolazione dei dati dall'altro, la successiva tappa rappresentata dalla adozione della Carta di Nizza propone invece una evoluzione ben più decisa e significativa: con tale atto, infatti, viene riconosciuto, accanto al diritto alla riservatezza – l'art. 7 di cui si è sopra parlato –, il diritto alla protezione dei dati all'art. 8, nel quale viene affermato che "Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".

Questa distinzione tra diritto alla vita privata e diritto alla protezione dei dati è tutt'altro che una mera differenziazione di facciata, rappresentando al contrario un riconoscimento della dignità propria che si è voluto attribuire alla nuova dimensione dinamica della riservatezza, riscontrata appunto nel controllo e nella protezione dei dati e delle informazioni personali. L'affermazione di una fattispecie autonoma ha permesso di attribuire al diritto alla protezione dei dati un rilievo che non trovava precedenti nella Convenzione EDU, consentendo così anche un chiaro ed espresso "recepimento di un patrimonio inestimabile costituito dalla pluridecennale giurisprudenza della Corte EDU" che aveva arricchito, insieme alla Convenzione di Strasburgo e ai principi in essa affermati, il dettato dell'art. 8 Convenzione EDU, adattandolo all'evoluzione dei tempi[124].

L'ultima tappa del processo europeo di riconoscimento del diritto alla protezione dei dati come diritto distinto da quello alla vita privata è da rinvenirsi infine nel già richiamato Trattato di Lisbona ed in particolare nel Trattato sul Funzionamento dell'UE: all'art. 16 TFUE viene riconosciuto espressamente il diritto di ogni individuo alla protezione dei dati di carattere personale che lo riguardano, mentre al comma 2 viene previsto che "Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi

[124] F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA, M. D'AMICO (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, 2009, p. 86.

dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti". Viene pertanto attribuita competenza all'UE di adottare norme materia di *data protection*, consentendo una protezione attiva dei dati mediante l'intervento del legislatore europeo stesso[125]. Ed è proprio con riferimento a tale disposizione che il vigente ed imponente Regolamento generale sulla protezione dei dati (c.d. GDPR, Reg. UE 2016/679) trova la propria base giuridica[126]: tale normativa predispone una ampia disciplina, aggiornata ed adeguata al mutare dei tempi, che ha sostituito l'ormai anacronistica Direttiva madre del 1995 pur non abbandonando del tutto quella vocazione economica che ha contraddistinto la disciplina della protezione dei dati a livello europeo sin dalla sua prima affermazione[127].

Sebbene più approfondite analisi e riflessioni critiche sulla normativa europea in materia di protezione dei dati verranno svolte nella Parte II di questo lavoro, ponendo peraltro particolare attenzione in quella sede al ruolo fondamentale svolto dalla Corte di Giustizia dell'UE, la ricostruzione elaborata in questo paragrafo consente di cogliere l'unicità e l'importanza del percorso europeo – inteso in senso lato – di affermazione del diritto alla protezione dei dati e del suo rilievo soprattutto dinnanzi al progresso tecnologico, che rappresenta oggi, al contempo, la spinta che ha consentito a tale diritto di essere riconosciuto ma anche la maggiore e più insidiosa fonte di minacce e serie problematiche che ne stanno mettendo a dura prova la concreta garanzia.

Il processo che, nel Continente europeo, ha portato alla decisa e forte affermazione del diritto alla riservatezza, nonché del diritto alla protezione dei dati come diritto autonomo, mette inoltre in luce le differenze rispetto alla originaria affermazione della privacy negli Stati Uniti d'America: ci si allontana sempre più dalla dimensione esclusiva del *tort* o dell'illecito civile, per realizzare una tutela della riservatezza e soprattutto della protezione dei dati mediante obblighi legislativi ed un apparato normativo solido e articolato, anche ed in particolare a livello dell'UE. Questo riconoscimento viene identificato come "punto di approdo di una lunga evoluzione concettuale che, nelle sue varie tappe, ha arricchito di implicazioni e significati nuovi e ulteriori un concetto che si è caratterizzato e che si

[125] Per un commento a tale articolo si rimanda a P. PIRODDI, *Art. 16 TFUE*, in F. POCAR, M. C. BARUFFI, *Commentario breve ai Trattati dell'Unione europea*, Cedam, II Ed., 2014, pp. 189-198.

[126] Come precisato da Finocchiaro, il Regolamento "non ha ad oggetto il diritto alla riservatezza: ha un ambito molto più ampio della riservatezza, ma che non è necessariamente connesso alla sfera più intima della persona. I dati personali costituiscono il tema disciplinato anche se non si riferiscono a vicende private, intime o familiari. Qualunque informazione, quale che sia il suo contenuto, è oggetto del Regolamento", ribadendo come "il diritto alla protezione dei dati deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni", G. FINOCCHIARO, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quaderni costituzionali*, 4, 2018, p. 896.

[127] Al Considerando 13 GDPR si legge infatti: "Per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri". La doppia natura ed obiettivo di tutela dei diritti fondamentali da un lato e garanzia della efficienza del Mercato Unico e della libera circolazione di merci dall'altro, resta evidente. Per ulteriori approfondimenti si rimanda, ex multis, a: P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffré, 2002; G. GONZALES FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Spinger, 2014; F. BALDUCCI ROMANO, *La protezione dei dati personali nell'UE tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario,* 6, 2015.

caratterizza ancora oggi per la sua incessante mutevolezza contenutistica e per la capacità di racchiudere in sé una serie di esigenze multiformi"[128].

2.2.1. – Dignità della persona e libertà personali: la stretta connessione tra diritto alla riservatezza, diritto alla protezione dei dati e diritti fondamentali in una società democratica

L'analisi sin qui svolta ha permesso di delineare i due diritti alla riservatezza e alla protezione dei dati nei loro diversi contenuti e nel loro percorso evolutivo, fortemente segnato dall'avvento delle nuove tecnologie e dalle nuove sfide che il progresso tecnologico ha comportato rispetto alla loro effettiva tutela. Lo studio delle caratteristiche e dagli interessi protetti da questi diritti fondamentali, anche e soprattutto nel contesto dell'Unione europea e degli Stati membri, non può però dirsi completa senza una riflessione circa il rapporto intercorrente tra i due diritti analizzati e gli altri diritti o principi su cui l'Unione stessa si fonda e che sono riconosciuti e protetti nella Carta di Nizza, nella Convenzione EDU ma anche nelle Carte costituzionali nazionali. Per comprendere appieno la portata tanto del diritto alla riservatezza quanto di quello alla protezione dei dati e per procedere all'approfondimento dello specifico caso studio rappresentato dal regime della *data retention*, è necessario dunque chiedersi quale rilievo abbiano assunto la privacy e la *data protection* e la loro effettiva garanzia e, conseguentemente, quali effetti produca una loro violazione rispetto al godimento di altri diritti fondamentali, egualmente affermati e tutelati.

Ebbene, ponendosi quale finalità la determinazione di questa connessione[129], non si può non richiamare quanto riconosciuto dal Tribunale federale tedesco nella decisione, già sopra esaminata, del 1983, nella quale il diritto alla autodeterminazione informativa come controllo sulle informazioni che ci riguardano o da noi prodotte viene considerato meritevole di tutela costituzionale. In quella occasione, infatti, i giudici di Karlsruhe avevano fondato la propria pronuncia sulla protezione dei diritti alla dignità e alla libertà personale: veniva così riconosciuto che il potere sui propri dati, la possibilità di decidere se diffonderli, di accertarne la correttezza e l'utilizzo che ne viene fatto, siano da intendersi come

---

[128] L. MIGLIETTI, *Profilo storico-comparativi del diritto alla privacy*, in *Diritti Comparati*, 4 dicembre 2014. E similmente: "il diritto alla privacy che Warren e Brandeis immaginarono come *right to be let alone* ha conosciuto un processo di migrazione dagli USA verso l'Europa, arricchendosi progressivamente di una dimensione che non tutela esclusivamente l'aspettativa di riservatezza dell'individuo ma che vede nella definizione di un sistema di principi e regole a tutela dei dati un ulteriore momento essenziale a presidio della personalità individuale", O. POLLICINO, M. BASSINI, *Social network e tutela dei dati personali*, op. cit., p. 74.

[129] Si vuole prescindere, in questa analisi, dalla discussione, pur presente in dottrina, circa il rapporto intercorrente tra i due diritti analizzati ed in particolare se il diritto alla protezione dei dati possa essere considerato autonomo ed indipendente da quello alla riservatezza. Si sono interrogati su tale aspetto, chiedendosi se il diritto alla protezione dei dati possa realmente sussistere in maniera autonoma e svincolata da quello alla riservatezza: M. TZANOU, *Data protection as a fundamental right next to privacy*? *Reconstructing a not so new right*, in *International data privacy law*, 2, 2013; B. VAN DER SLOOT, *Legal fundamentalism: is data protection really a fundamental right?*, in R. LEENES et al. (a cura di), *Data protection and privacy. (In)visibilities and infrastructure*, Springer, 2017, p. 3-30; G. GONZALEZ FUSTER, *The emergence of personal data protection as a fundamental right in Europe*, op. cit.; O. LYNSKEY, *The foundations of EU data protection law*, Oxford University Press, 2015. Anche Califano riconosce la complessa correlazione tra i due diritti, "anzitutto in ragione della coesistenza, all'interno del nuovo diritto alla protezione dei dati, di due profili solo in parte sovrapponibili, ma radicati entrambi nella tutela della dignità della persona come valore e come oggetto dei diritti fondamentali", L. CALIFANO, *Il Reg. UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, op. cit., p. 7. Tale questione, che in questa sede non si vuole affrontare sotto il profilo teorico e dottrinale, emergerà tuttavia con chiarezza nella Parte II di questo elaborato, laddove si analizzerà la giurisprudenza della Corte di giustizia dell'UE (CGUE) in materia di riservatezza e protezione dei dati con riferimento allo specifico regime della *data retention* e nella quale i giudici di Lussemburgo offriranno osservazioni interessanti per meglio comprendere il rapporto tra art. 7 e art. 8 della Carta di Nizza.

precondizione necessaria a che la personalità possa liberamente esplicarsi nella società e nelle relazioni interpersonali, legandosi così a quella capacità di libertà e autonomia di scelta che è fondamento della dignità umana. Non è un caso che proprio in Germania questa connessione tra tutela della sfera privata, tutela dei dati, libertà e dignità abbia incontrato una così significativa affermazione: gli orrori del totalitarismo nazista si erano realizzati anche grazie ad un annientamento della sfera privata, ad un controllo delle scelte che perdevano così la loro stessa natura di decisioni libere, per essere invece governate dall'alto anche mediante l'impiego di forme pervasive di sorveglianza delle relazioni, delle preferenze, delle abitudini dei cittadini, delle opinioni politiche e degli orientamenti sessuali o religiosi. Entrando nella vita privata ed esercitando sorveglianza e coazione che non conoscevano limite né nella dimensione delle abitazioni private né nella corrispondenza, dunque disconoscendo i diritti alla riservatezza e alla tutela delle informazioni che ci riguardano, il potere nazista violava la dignità umana, la capacità di autodeterminazione, per ammettere solo asservimento ed omologazione[130]. Non stupisce dunque che i giudici tedeschi, consapevoli dell'impatto che la negazione della dimensione privata aveva comportato nella tragica esperienza del non lontano passato, avessero riconosciuto l'intrinseco legame che la garanzia della privacy e della *data protection* intesse con l'esercizio effettivo e reale delle libertà personali, della dignità e, con uno sguardo più ampio e complessivo, della stessa democraticità delle nostre società. In altre parole, l'affermazione della identità individuale, dell'indipendenza e della sua correlata autonomia e libertà, nelle sue diverse accezioni – di espressione, politica, di associazione, di pensiero – non possono svilupparsi se non nella dimensione della sfera privata, che deve essere dunque tutelata da ingerenze esterne, nonché nel controllo positivo e attivo sui dati e sulle informazioni che ci definiscono e che potrebbero, altrimenti, finire col controllarci[131].

E così sinteticamente, viene determinato come sia il diritto alla riservatezza che quello alla protezione dei dati rivestano una importanza strumentale e finalistica "tale da poter compromettere, in caso di [loro] violazione, tutta un'altra serie di principi, diritti e libertà che vanno dalla libertà di espressione alla libertà religiosa, dalla libertà d'impresa al diritto di difesa, dal divieto di discriminazione a tutti quei diritti di prestazione posti a tutela dei soggetti più deboli. A fronte di un'autorevole posizione dottrinale che configura il diritto alla protezione dei dati quale presupposto della salvaguardia di ogni diritto costituzionalmente protetto [il riferimento è a F. Pizzetti, nel suo scritto *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016], non vi è dubbio in ogni caso che una compressione del diritto del singolo all'autodeterminazione informativa pone in discussione la salvaguardia della dignità stessa della persona, intesa quale valore

[130] Come ben sottolineato da Porcedda, "totalitarian regimes crushed private and family life, home and correspondence with the use of ideology and terror, with a view to curbing individuals' spontaneity and leeway for action, and substituted autonomy with automatic processes", M. G. PORCEDDA, *The recrudescence of 'Security v. Privacy' after the 2015 terrorist attacks and the value of privacy rights in the European Union*, in E. ORRÙ, M. G. PORCEDDA, S. WEYDNER-VOLKMANN (a cura di), *Rethinking surveillance and control: beyond the 'security versus privacy' debate*, Nomos, 2017. L'autrice fa derivare da queste considerazioni che "both rights are instrumental in fostering personhood, one's unique identity, protected as an expression of dignity and enabling autonomy as concepts emerged out of modernity". Sul tema, anche Rodotà ha più volte messo in luce la correlazione tra totalitarismo e violazione della riservatezza e della protezione dei dati: "non bisogna mai perdere la memoria di quel che è avvenuto nei regimi totalitari, dove violazioni profonde dei diritti fondamentali sono state possibili proprio grazie a massicce raccolte di informazioni che hanno consentito un controllo continuo della vita quotidiana", S. RODOTÀ, *Privacy, libertà, dignità, discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, disponibile all'indirizzo www.privacy.it/archivio/rodo20040916.html, 2004.

[131] "Privacy prevents interference, pressures to conform, ridicule, punishment, unfavorable decisions, and other forms of hostile reaction. To the extent that privacy does this, it functions to promote liberty of action, removing the unpleasant consequences of certain actions and thus increasing the liberty to perform", R. GAVISON, *Privacy and the limits of law*, in F. D. SCHOEMAN (a cura di), *Philosofical dimensions of privacy: an anthology*, Cambridge University Press, 1984, p. 363.

costituzionale indisponibile. In questo si fonda il principale collegamento con l'intera e più complessa costellazione dei diritti fondamentali"[132].

I due diritti analizzati, pertanto, non possono essere visti come monadi isolate: il loro valore e l'importanza della loro effettiva garanzia devono essere tenute in debita considerazione nelle scelte tanto del legislatore quanto del giudice nazionale e sovranazionale, anche per evitare derive pericolose – peraltro rese sempre più reali dal progresso tecnologico – che possono concretizzarsi nella creazione di una società sorvegliata e nella concentrazione del potere derivante da tale pervasivo controllo nelle mani di pochi soggetti. Il diritto alla riservatezza e alla protezione dei dati possono quindi rappresentare barriere a tali minacce[133], a tutela della libertà, del libero sviluppo della personalità e dell'identità[134] e di una "costituzionalizzazione della persona"[135] che è infine garanzia nei confronti di discriminazioni e diseguaglianze fondate sulla disponibilità di informazioni personali. Per usare le efficaci parole di Rodotà, dunque, la riservatezza e la protezione dei dati si presentano quali elementi fondamentali della società dell'eguaglianza, della società della partecipazione[136], della società della dignità[137] e della società della libertà[138].

---

[132] L. CALIFANO, *Principi e contenuti del Regolamento UE 2016/679*, op. cit., p. 1.

[133] Rodotà, sul punto, aveva infatti affermato: "In questo momento storico il termine privacy sintetizza un insieme di poteri che, originati dall'antico nucleo del diritto a essere lasciato in pace, si sono via via evoluti e diffusi nella società proprio per consentire forme di controllo sui diversi soggetti che possono esercitare forme di sorveglianza", S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, op. cit., p. 31. Anche Califano non ha mancato di evidenziare come: "l'importanza che la disciplina sulla protezione dei dati personali ha assunto nel mondo contemporaneo è in stretta correlazione al mondo in cui l'ordinamento giuridico intende garantire alla persona non solo il dominio sui dati che la identificano ma la stessa possibilità di libero sviluppo della sua personalità. Una tutela costituzionale che, come si è già avuto modo di sottolineare, si incardina sul concetto della inviolabilità, della dignità e libertà della persona umana", L. CALIFANO, *Il Reg. UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, op. cit., p. 16.

[134] Il diritto all'identità personale viene inteso come "diritto a non veder travisare la propria personalità individuale, non vedendosi all'esterno alterato, travisato e offuscato", A. PISAPIA, *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, in *federalismi.it*, 3, 2018, che richiama tra gli altri R. CORDONE, *Il diritto all'identità personale*, in G. CASSANO (a cura di), *Nuovi diritti della persona e risarcimento del danno*, Tomo I, Giappichelli, 2003, p. 373. In tale contesto, il legame tra affermazione dell'identità personale da un lato e diritto alla riservatezza e protezione dei dati dall'altro viene posto in evidenza da Resta: "la libera costruzione dell'identità può essere concretamente posta in pericolo non soltanto nelle ipotesi di travisamento o de-contestualizzazione da parte dei mass media, ma anche qualora il flusso delle informazioni che riguardano la persona non avvenga attraverso canali trasparenti e all'interno di un ben preciso quadro di garanzie. Le tecniche di raccolta dei dati e profilazione individuale determinano il rischio che l'io venga frammentato, a sua insaputa, in una molteplicità di banche dati, offrendo così una raffigurazione parziale e potenzialmente pregiudizievole della persona, la quale verrebbe così ridotta alla mera sommatoria delle sue proiezioni elettroniche", G. RESTA, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica*, 3, 2007, p. 523.

[135] S. RODOTÀ, *Il diritto di avere diritti*, op. cit., p. 321.

[136] Sotto questo profilo della partecipazione alla vita politica e dunque della garanzia di una reale ed effettiva democrazia, viene affermato come "privacy and data protection regimes are not there merely to protect the best rights holders' interests, but are necessary in a democratic society to sustain a vivid democracy", A. ROUVROY, Y. POULLET, *The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy*, in S. GURTWIRTH et al. (eds.), *Reinventing data protection?*, op. cit., p. 57.

[137] Flick giunge a sostenere che "la privacy e l'identità del singolo sono fattori coessenziale alla sua dignità", G. M. FLICK, *Elogio della dignità (se non ora, quando?)*, in *Rivista AIC*, 4, 2014.

[138] S. RODOTÀ, *Privacy, libertà, dignità*, op. cit. L'autorevole studioso italiano non è certo il solo ad esprimere tale posizione, che possiamo leggere anzi anche nelle parole del Giudice Douglas della Corte Suprema USA. Quest'ultimo nella sua Dissenting Opinion nel caso *Public Utilities Commission v. Pollak* (US, 451, 467 del 1952), ha affermato che: "The right to be let alone is indeed the beginning of all freedom". In tempi più recenti, proprio sulla base di tali considerazioni, alcuni autori sono giunti a ritenere che la privacy rappresenti una vera e propria precondizione al godimento di altri diritti fondamentali: "Privacy is not only one of the core fundamental rights, but it also plays a central role for exertion of other fundamental rights and freedoms, for balancing powers between the state and citizens, for democratic development, societal and economic innovativeness or individual autonomy. Privacy is a precondition for thinking and expressing oneself freely, in general and in particular when new media or social networks come into play. (..) Whether the Internet can continue to be an infrastructure for unrestricted

Solo se si prende avvio da queste considerazioni, si può comprendere appieno la complessità dei due diritti esaminati: essi sono ben lontani dal ricoprire un rilievo unicamente per il singolo e per l'individuo, ma al contrario la garanzia della riservatezza e protezione dei dati si ripercuotono anche sull'intera collettività, sulla democraticità della società, sul rispetto dei diritti fondamentali di cui tutti beneficiano e di cui anche il rapporto tra Stato e cittadino dipende[139].

Se questo rapporto di interconnessione e di relazione tra privacy, *data protection* e diritti fondamentali assume il carattere di un imprescindibile e rilevante punto di partenza per qualsiasi riflessione sul tema, risulta altrettanto fondamentale specificare come neppure alla luce delle considerazioni sopra svolte i diritti alla riservatezza e alla protezione dei dati possano essere considerati diritti assoluti: l'approccio seguito dal Consiglio d'Europa nonché dal legislatore dell'UE nella redazione tanto della Carta dei diritti fondamentali quanto di Regolamenti e Direttive è in tal senso significativo e riflette un chiaro approccio pragmatico.

L'art. 8, co. 2, CEDU, come si è visto, ammette a determinate condizioni forme di invasione della sfera privata da parte di autorità pubbliche e anche l'art. 8 della Carta di Nizza, laddove tutela il diritto alla protezione dei dati, acconsente a che i dati vengano trattati purché secondo principi di lealtà, finalità determinate, sulla base del consenso o di altro fondamento legittimo previsto dalla legge. Non viene, in altre parole, espresso un divieto assoluto di trattamento dei dati, che risulterebbe peraltro del tutto irrealizzabile oltre che inutile, vista l'importanza e l'utilità che l'impiego dei dati rappresenta nella nostra quotidianità e per il funzionamento delle società moderne. Come ben riassunto da De Hert e Gutwirth, "data protection regulation does not protect us from data processing but from unlawful and/or disproportionate data processing. Data protection regulation's real objective is to protect individual citizens against unjustified collection, storage, use and dissemination of their personal details"[140]. Ciò si estende anche al diritto alla vita privata, soprattutto tenendo in considerazione il rilievo dell'art. 52 della Carta di Nizza stessa che riconosce, al co. 1, che "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

I diritti alla riservatezza e alla protezione dei dati dunque non escludono *tout court* forme di invasione nella sfera privata o di accesso e trattamento dei dati ma ammettono, al contrario, una compressione degli stessi a determinate condizioni; una compressione che si rende necessaria al fine di tutelare altri diritti fondamentali o interessi coinvolti: una totale tutela della riservatezza inciderebbe negativamente ad esempio sul diritto all'informazione, sulla trasparenza delle pubbliche amministrazioni, sul diritto

---

communication and access to information, supporting the freedom of expression and political participation or whether it is converted into an instrument of control and surveillance depends predominantly on the respect for privacy", J. CAS, R. BELLANOVA, J. P. BURGESS, M. FRIEDWALD, W. PEISSL, *Introduction: Surveillance, privacy and security*, in J. CAS, R. BELLANOVA, J. P. BURGESS, M. FRIEDWALD, W. PEISSL (a cura di), *Surveillance, privacy and security: Citizens' perspectives*, Routledge, 2017, p. 8, in cui si richiama il pensiero di D. SOLOVE, *Understanding privacy*, Harvard University Press, 2008. Anche Baldassarre ha sostenuto che "il diritto alla privacy è il più penetrante e comprensivo sviluppo della libertà individuale nelle Costituzioni moderne", A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, op. cit., p. 152.

[139] Regan osserva come "Privacy has value beyond its usefulness in helping the individual to maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize the individual is better off if privacy exists. I maintain that the society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public and collective purposes", P. M. REGAN, *Legislating privacy, technology, social values and public policy*, 1995.

[140] P. DE HERT, S. GUTWIRTH, *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, op. cit., p. 25. Ciò è del resto ribadito anche dal legislatore europeo che nel GDPR, al Considerando 4, ammette che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ottemperanza al principio di proporzionalità".

all'accesso a documenti e procedure; condizionerebbe anche la sicurezza e la capacità delle autorità pubbliche di garantire l'ordine pubblico e di svolgere attività investigative, di controllo e prevenzione del crimine; o ancora una totale impossibilità di trattamento dei dati non consentirebbe lo svolgimento di attività che implicano o si fondano sul trattamento di dati, quali l'erogazione di servizi Web o di telefonia, comportando dunque una limitazione dell'iniziativa economica. Ne deriva come i diritti alla privacy e alla protezione dei dati possano scontrarsi talvolta con la necessità di garantire e tutelare altri diritti o interessi altrettanto fondamentali, che impongono dunque attente e delicate considerazioni e valutazioni circa la proporzionalità, la necessità e la legittimità di restrizioni e ingerenze.

La ricostruzione sino ad ora fornita, pur senza pretesa di completezza ed esaustività, mira a fornire le coordinate utili a comprendere l'approfondimento che occuperà i prossimi paragrafi e che intende calare in un caso concreto le considerazioni sin qui svolte: si osserverà come la compressione dei due diritti analizzati, sotto i colpi del progresso tecnologico, venga posta in essere al fine di garantire la sicurezza dinnanzi a minacce sempre più frequenti e rilevanti quali il terrorismo e la criminalità organizzata e transfrontaliera; la particolare disciplina della *data retention* ha così imposto a livello europeo quanto nazionale di riflettere da un lato sull'impatto di una limitazione dei diritti alla riservatezza e protezione dei dati e sulle conseguenze rispetto al godimento di altri diritti fondamentali e della democraticità stessa della società; dall'altro sul se e come sia possibile determinare un punto di equilibrio e un bilanciamento tra esigenze securitarie e tutela dei diritti fondamentali o se la salvaguardia delle prime comporti necessariamente una rinuncia dei secondi. I rilievi che hanno posto in evidenza il contenuto e le finalità dei due diritti alla privacy e *data protection* nonché il loro legame con altri diritti riconosciuti e con le sfide che il progresso scientifico e l'innovazione pongono al mondo del diritto, costituiscono le basi per approcciarsi all'oggetto di approfondimento di questo elaborato.

3. – La data retention *come osservatorio privilegiato: la sfida di un possibile bilanciamento tra diritto alla riservatezza, diritto alla protezione dei dati ed esigenze securitarie*

3.1. – Minacce alla sicurezza e terrorismo internazionale: la conservazione e accesso ai metadati come efficace strumento di lotta alla criminalità

Successivamente agli attentati terroristici che hanno colpito gli Stati Uniti d'America nel 2001, seguiti da numerosi altri tragici eventi che hanno scosso – anche – il Continente europeo, la garanzia della sicurezza dei confini nazionali da minacce tanto esterne quanto interne è divenuto obiettivo prioritario dei Governi nonché sul piano internazionale. L'acceso dibattito politico che ne è seguito si è così focalizzato sulle strategie e sui mezzi maggiormente efficaci per raggiungere un alto livello di prevenzione e una solida lotta al terrorismo. In questo contesto – quantomeno inizialmente – emergenziale, la scelta operata dalla quasi totalità degli Stati occidentali, a partire dagli USA, è da identificarsi nel potenziamento di strumenti di sorveglianza segreta e di intelligence[141], anche mediante

[141] Pare utile fornire preliminarmente una possibile definizione di 'servizi di intelligence'; tra le molte, interessante è quella proposta da Scheinin, *UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*: "Intelligence services play an important role in protecting national security and upholding the rule of law. Their main purpose is to collect, analyse and disseminate information that assists policymakers and other public entities in taking measures to protect national security. This includes the protection of the population and their human rights", M. SCHEININ, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, Doc. A/HRC/14/46, 17 maggio 2010. Come evidente dalla definizione proposta, le attività di *intelligence* si legano al concetto di difesa della 'sicurezza nazionale', che pare doversi tenere distinta dalla sicurezza pubblica o ordine pubblico. Del resto, riconducendo la questione all'ambito di interesse del presente elaborato, ovvero limitatamente

l'implementazione di strumenti di controllo delle comunicazioni elettroniche[142].

In particolare, uno degli strumenti maggiormente impiegati e che aveva, già all'indomani dell'11 settembre 2001, catturato l'attenzione di Governi e autorità di intelligence, è quello della *data retention*. Con questo termine, difficilmente traducibile in italiano se non con la limitativa locuzione 'conservazione dei dati', assume in realtà un significato più ampio: la *data retention,* nello specifico campo della prevenzione e lotta alla criminalità e con riferimento ai servizi di telecomunicazione, consiste nell'"obbligo imposto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione di conservare, per un certo periodo di tempo, i dati relativi al traffico e all'ubicazione e per identificare l'abbonato o l'utente"[143]; ad essa poi si accostano misure di

al contesto europeo, emerge anche negli atti normativi l'impiego dei differenti termini 'sicurezza nazionale' e 'sicurezza pubblica'. Pur non volendo in questa sede proporre una ricostruzione del dibattito dottrinario che si è concentrato proprio sulla distinzione tra questi termini, sul loro significato e sulla reale possibilità di differenziazione tra di essi nella situazione attuale, si ritiene comunque utile riportare alcune definizioni di massima, per quanto discusse. Il legislatore dell'UE ha infatti impiegato più volte il termine 'sicurezza nazionale' come distinto da quello di 'sicurezza pubblica': se uno degli esempi più rilevanti di tale riferimento verranno analizzati approfonditamente nella Parte II di questo elaborato, ovvero nell'esame della Direttiva 2002/58/CE, un primo importante impiego del termine 'sicurezza nazionale' è certamente da rilevarsi nell'art. 4, co. 2, Trattato sull'Unione europea (TUE) nel quale si legge: "L'Unione rispetta l'uguaglianza degli Stati membri davanti ai trattati e la loro identità nazionale insita nella loro struttura fondamentale, politica e costituzionale, compreso il sistema delle autonomie locali e regionali. Rispetta le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro". Nonostante l'utilizzo del termine in più fonti normative, nel diritto europeo non si trova in alcun luogo una definizione specifica di sicurezza nazionale. Neppure il GDPR, che all'art. 23, relativo alle limitazioni che la disciplina in materia di protezione dei dati può subire, cita distintamente le finalità di 'sicurezza nazionale' e quelle di 'sicurezza pubblica', ne fornisce una definizione espressa. Il Parlamento europeo, nel documento "*Public security exception in the Area of non-personal data in the EU*" (PE 618.986, aprile 2018) ha affermato come "There is no unified definition of national security but activities to counter a threat to the state's independence, sovereignty, territorial integrity, constitutional order, of that magnitude, are recognized". Similmente il Gruppo di Lavoro Art. 29, nel *Working Document on surveillance of electronic communications for intelligence and national security purposes* (WP 228, del 5 dicembre 2014), ha stabilito come "In absence of a clear definition of 'national security', the Working Party has examined how this notion should be interpreted, especially since the thin line between law enforcement and national security sometimes seems to fade. In any case, national security needs to be distinguished from the security of the European Union, but also from State security, public security and defence. All of these notions are referred to separately in the EU treaties and underlying legislation, although they are inextricably linked. Whether or not something should be defined as falling under the national security exemption therefore cannot only be explained by strictly legal arguments. What can be said is that, whereas activities by intelligence and security services are generally accepted as falling under the national security exemption, this is not always the case when general law enforcement authorities fulfil similar tasks". Viene dunque chiaramente messa in evidenza la difficoltà – soprattutto a causa delle moderne e sempre più sofisticate tecniche di indagine nonché dinnanzi a forme di criminalità organizzata dalle dimensioni e ramificazioni internazionali – di tracciare una linea netta di confine tra attività volte alla tutela della sicurezza nazionale e quelle invece affidate alle autorità di *law enforcement* e finalizzate alla protezione della sicurezza pubblica. Come si vedrà, rispetto a questa distinzione si entrerà maggiormente nel dettaglio nel complesso dibattito che occuperà la Parte II riferita alla specifica disciplina della *data retention*. Sulle possibili distinzioni tra il concetto di sicurezza nazionale e pubblica, si rimanda comunque a: P. VOGIATZOGLOU, S. FANTIN, *National and public security within and beyond the Police Directive*, in A. VEDDER, J. SCHROERS, C. DUCUING, P. VALCKE (a cura di), *Security and Law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Intersentia, 2019, pp. 27-62; ma anche a G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della 'emergenza normalizzata'*, in *federalismi.it*, 4, 2019.

[142] "L'attività di controllo non [è] più un'esclusiva di regimi che, un tempo, comparati al nostro sistema legale e alla nostra idea di tutela dei diritti, erano definiti autoritari o fautori di politiche liberticide, ma che possa avvenire in qualsiasi contesto politico e costituzionale e, anzi, per tale motivo sia ancora più subdola e complessa da interpretare. (..) La tendenza diffusa è quella di uno Stato che sorveglia le comunicazioni elettroniche con tutti i mezzi possibili", G. ZICCARDI, *Internet, controllo e libertà*, op. cit., p. 225.

[143] Parere del Garante europeo della protezione dei dati sulla relazione di valutazione relativa all'applicazione della Direttiva sulla conservazione di dati (Direttiva 2006/24/CE) presentata dalla Commissione al Consiglio e al

accesso ai dati conservati da parte di autorità specificamente individuate, alle quali i fornitori di servizi di telecomunicazione debbono consentire l'analisi dei dati raccolti.

La conservazione dei dati permette quindi di disporre di informazioni vaste ed ampie, che non riguardano però il contenuto delle comunicazioni: lo strumento della *data retention* infatti, nella maggioranza dei casi, impone l'obbligo di trattenere e memorizzare quei dati, c.d. metadati, che sono prodotti dalle telecomunicazioni – dunque dall'utilizzo di dispositivi elettronici quali telefoni e computer – e che vengono necessariamente raccolti dagli operatori per la corretta erogazione dei servizi e per scopi di fatturazione nonché abitualmente cancellati dagli operatori stessi quando non più utili per tali finalità operative. Per metadati o dati relativi al traffico si fa riferimento pertanto all'"involucro delle comunicazioni elettroniche"[144], cioè a tutti quei dati che non attengono al contenuto bensì forniscono informazioni circa luogo, data, ora, durata e destinatario di una comunicazione, unitamente all'ubicazione e identità dell'utilizzatore di un servizio di telecomunicazione. Per questo è utile preliminarmente distinguere lo strumento della conservazione dei dati (o meglio metadati) dalle intercettazioni: queste ultime attengono al contenuto, si svolgono in 'tempo reale' e ad opera direttamente delle autorità di intelligence o *law enforcement*, mentre mediante la *data retention* i dati vengono conservati e trattenuti dall'operatore, ovvero dal soggetto privato, e non dall'autorità pubblica, per essere poi solo eventualmente e in un secondo momento analizzati mediante accesso ai dati su richiesta delle autorità autorizzate a tali operazioni[145].

Questo strumento quindi è stato percepito come una carta vincente nel campo delle attività investigative poiché permette di effettuare controlli sui dati di individui che al momento dell'atto terroristico o criminale non risultavano essere ancora soggetti noti alle forze dell'ordine e che quindi non erano sottoposti ad alcuna forma di sorveglianza[146]; in questo modo, per impiegare il termine utilizzato da Cameron, è possibile andare "indietro nel tempo"[147] durante la fase investigativa, consegnando alle forze dell'ordine un enorme 'pagliaio' di metadati entro cui, con le moderne tecniche

Parlamento europeo (2011/C 279/01), par. 16. Drewry definisce la *data retention* come "measures that aim at requiring (some or all) operators to retain non-content data generated or processed as a result of activities of all users of operators' communications or network services so that they can be accessed by state authorities and used for public order purposes when necessary and lawful", L. DREWRY, *Crimes without culprits: why the EU needs data retention and how it can be balanced with the right to privacy*, in *Wisconsin International Law Journal*, 4, 2015, p. 726.

144 G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Medialaws*, 2, 2018.

145 "L'acquisizione, necessariamente post factum, dei dati esterni del traffico presso il fornitore dei servizi telefonici o telematici interessati vale a marcare la distanza della *data retention* rispetto a fenomeni solo apparentemente analoghi, come il c.d. pedinamento satellitare, in cui gli organi dell'investigazione inseriscono un GPS su oggetti che la persona reca con sé e ne registrano i movimenti nel momento in cui essi avvengono o comunque quando interessi geolocalizzare la persona stessa", S. MARCOLINI, *L'istituto della DR dopo la sentenza della CGUE del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA (a cura di), *Cybercrime*, Utet, 2019, p. 1580.

146 Si pensi alla raccolta, conservazione e accesso ai cd. Passenger Name Records relativi ai passeggeri di voli aerei: "il trattamento [dei PNR] mira a identificare il rischio per la sicurezza pubblica che potrebbero eventualmente presentare persone che non sono, in tale fase, conosciute dai servizi competenti e che potrebbero essere, a motivo di tale rischio, soggette a un esame approfondito" (par. 187, Parere 1/15, CGUE). Risulta chiara la rilevanza che questi dati ricoprono ai fini di garantire la sicurezza e repressione di reati transfrontalieri quali terrorismo, traffico di droga, traffico di esseri umani.

147 I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 54, 2017. Come sottolineato da Murray e Fussey, "these methods of interrogating retained communications data benefit from the ability to look into the past. First, in the event of a crime, retained data allows security services to 'rewind' events, facilitating the identification of suspects and a better understanding of what happened. (..) Second, retained data allows analysts to look back and immediately identify a suspect's pre-existing network", D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, in *Israel Law Review*, 1, 2019, p. 40.

di indagine, si è in grado, nella maggior parte dei casi, di trovare un singolo 'ago'[148]. Queste operazioni però risultano realizzabili solo se i metadati sono preventivamente conservati e trattenuti al fine di consentire l'eventuale accesso delle autorità pubbliche: per questo lo strumento della *data retention* permette di compiere investigazioni – che non sarebbero altrimenti possibili – riguardanti soggetti che non erano, al momento della produzione dei metadati stessi, sospettati di alcunché; ad esempio, raccogliendo i metadati relativi alle telefonate, le autorità investigative sono in grado di risalire alla frequenza di chiamate ricevute da o indirizzate ad un determinato soggetto, creando così collegamenti tra persone o fatti, che non sarebbero diversamente ricostruibili se i metadati venissero cancellati dagli operatori di servizi di telecomunicazione e che risultano utili per contrastare il fenomeno del terrorismo e della criminalità organizzata. Non è un caso dunque che tale strumento, inizialmente pensato per la lotta al terrorismo, sia stato in breve tempo impiegato anche nella lotta alla criminalità in generale, sebbene, come si vedrà, taluni Stati abbiano stabilito soglie specifiche di gravità dei reati per i quali è possibile fare ricorso a questo 'andare indietro nel tempo'.

Le potenzialità significative che la *data retention* rappresenta, tuttavia, non hanno offuscato i rischi che questa tecnica comporta: l'utilizzo, accesso e analisi ma anche, prima ancora, la conservazione di una grande quantità di informazioni, in maniera indiscriminata e generalizzata, senza che sussista dunque alcun sospetto circa la connessione con un reato o una minaccia alla sicurezza (c.d. *bulk* o *blanket data retention*), provocano indubbie e forti ingerenze entro la sfera privata di tutti gli utenti, incidendo anche sulla tutela e protezione dei dati. Sotto quest'ultimo profilo, infatti, la conservazione massiva di metadati comporta rischi tecnici seri quali il già richiamato *purpose creep* cioè l'utilizzo di dati per finalità differenti da quelle per le quali erano stati raccolti e conservati: si pensi ad esempio al fatto che i dati che i servizi di telecomunicazioni sono obbligati a conservare per finalità securitarie, e dunque per consentire l'accesso alle autorità pubbliche di *intelligence* o *law enforcement*, possono essere impiegati dai soggetti privati stessi per finalità commerciali, di marketing o di profilazione del cliente. Vi sono poi concreti rischi di *data breaches* e dunque furto o manomissione di dati, pericolo tipico ed ineludibile di sicurezza dei dati (*data security*) che aumenta esponenzialmente in base alla numerosità dei dati raccolti e memorizzati nonché all'ampiezza delle banche dati, che peraltro rappresentano un costo economico e gestionale di non trascurabile entità per gli operatori sui quali l'obbligo ricade. Vi è poi un ulteriore e ben più insidioso rischio: sebbene i metadati non attengano al contenuto delle comunicazioni (siano esse telefonate o email) e possano quindi apparire, singolarmente considerati, del tutto innocui, essi una volta aggregati sono in grado di fornire una immagine completa ed ampia della vita e delle abitudini degli individui, causando una compressione del diritto alla riservatezza. Come sarà più volte chiaramente affermato sia dalla Corte di giustizia dell'UE, che dalla Corte Europea dei Diritti dell'Uomo e dal legislatore europeo, i metadati consentono di rivelare, non meno dei dati attinenti al contenuto, una enorme quantità di informazioni circa la vita privata di un soggetto, le sue relazioni famigliari e sociali e persino gli orientamenti politici o sessuali[149].

---

[148] Richiamando ancora Marcolini, "mediante *data retention* si potrebbe ad esempio sottoporre a verifica la tesi difensiva dell'imputato che afferma che, nel momento in cui avrebbe commesso il delitto, era in realtà al telefono con una certa persona. Nella prassi, a rivestire interesse investigativo è anche il c.d. positioning cioè la collocazione del soggetto durante la telefonata, dedotta appunto dall'aggancio delle celle telefoniche. Non sfugge a nessuno che il movimento del cellulare non equivalga al movimento della persona, e che quindi occorrerà poi dimostrare che il soggetto interessato avesse la reale disponibilità di quell'utenza telefonica in quel momento. Non sfugge nemmeno che essere agganciati ad una certa cella, di per sé, non dia nessuna certezza circa la precisa collocazione della persona, atteso che un ponte telefonico copra a volte territori di svariati chilometri quadrati, ma appare altrettanto innegabile che l'aggancio alla cella valga ad escludere il posizionamento del cellulare del soggetto in ogni altro luogo; e, soprattutto nel caso di suo movimento, serve a dare l'idea precisa della direzione tenuta dall'utenza dell'indagato od imputato in un certo momento, circostanza significativa in un numero non trascurabile di procedimenti", S. MARCOLINI, *L'istituto della DR dopo la sentenza della CGUE del 2014*, op. cit., p. 1581.

[149] "This information can reveal extensive insights, such as a near comprehensive record of an individual's movements, with whom he or she communicates, how frequently and for how long. Communications data is not

Grazie e sulla base dell'analisi sopra svolta, possiamo comprendere chiaramente come tali rischi, principalmente e direttamente attinenti ai diritti alla riservatezza e alla protezione dei dati, abbiano in realtà un impatto significativo anche sulla libertà personale ed sul godimento di diritti quali la libertà di espressione, di associazione, di iniziativa economica, ricadendo così anche sul rapporto tra cittadino e Stato: quest'ultimo, imponendo un obbligo di *data retention*, laddove privo di adeguate salvaguardie e limitazioni, può disporre di un potente mezzo che gli può consentire di esercitare forme di controllo e di sorveglianza capaci di minare e compromettere la democrazia delle nostre società. Per quanto lo strumento della conservazione e accesso ai metadati sia dunque funzionale ad una maggiore garanzia della sicurezza, esso nondimeno pone serie preoccupazioni e forti interrogativi in termini di tutela dei diritti fondamentali. In tale contesto, il già articolato e difficile rapporto tra sicurezza e diritti fondamentali, in particolare di quelli alla privacy e alla *data protection* – rispetto al quale invero si era già aperto un significativo dibattito politico, giurisprudenziale e dottrinario[150] – si tinge di nuovi colori e di quella maggiore quanto inedita complessità di cui il mondo digitale da un lato e la minaccia terroristica dall'altro sono portatori.

Non è un caso, infatti, che la data dell'11 settembre 2001 sia stata individuata come il "momento che ha segnato un cambiamento radicale nella percezione del rapporto tra sicurezza e privacy"[151]: è nelle situazioni di emergenza, e forse ancor più nel contesto di 'emergenza normalizzata' e del cronicizzarsi quindi delle esigenze securitarie[152] che hanno caratterizzato lo scenario apertosi a seguito degli attentati alle Torri Gemelle, che si concretizza nel suo più alto livello il rischio che l'obbiettivo della sicurezza "divenga l'esclusivo criterio di riferimento, finendo così con l'autorizzare ingerenze nella nostra sfera privata e con il trasformare le nostre organizzazioni sociali, il modo in cui ci rapportiamo con i pubblici poteri ma anche il modo in cui possiamo realmente godere delle nostre libertà"[153]. La percezione di un pericolo imminente e, per certi versi, difficilmente prevedibile, produce quale esito quello di individuare nel sacrificio di talune libertà e diritti fondamentali, quali la riservatezza e la protezione dei propri dati, il mezzo necessario per ottenere più profonde garanzie di sicurezza ed una maggiore efficienza dei servizi di *intelligence* e delle autorità di *law enforcement*[154]. Il rischio però, in tal modo, è quello che "il

---

restricted to conventional communications such as phone calls, emails or messaging, but also includes communications between computers and internet browsing histories", D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, op. cit., p. 34.

[150] G. DE VERGOTTINI, *La 'guerra' contro un nemico indeterminato*, in *Forum di Quaderni Costituzionali*, 5 ottobre 2001; C. WALTER (a cura di), *Terrorism as challenge for national and international law: security versus liberty?*, Springer, 2004; A. VEDASCHI, *A' la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Giappichelli, 2007; S. GAMBINO, A. SCERBO, *Diritti fondamentali ed emergenza nel costituzionalismo contemporaneo. Un'analisi comparata*, in *DPCE*, 4, 2009; L. CALIFANO, *Privacy e sicurezza*, in *Democrazia e Sicurezza*, 3, 2013; F. CLEMENTI, G. TIBERI, *Sicurezza interna, diritti e cooperazioni internazionale nella lotta al terrorismo*, in *Astrid-online.it*, 1, 2013; L. SCAFFARDI, *Nuove tecnologie, prevenzione del crimine e privacy, alla ricerca di un difficile bilanciamento*, in A. TORRE (a cura di), Costituzioni e sicurezza dello Stato, Maggioli, 2013; M. BARBERIS, *Liberté, égalité, sécurité. Gli equivoci della guerra al terrore*, in *Il Mulino*, 4, 2016.

[151] G. ZICCARDI, *Internet, controllo e libertà*, op. cit., p. 31.

[152] M. ROSENFELD, *Judicial balancing in times of stress: comparing diverse approaches to the war of terror*, Benjamin N. Cardozo School of Law Working Paper, 119, 2005. Giovanni Maria Flick, parla di "una sorta di cronicizzazione e di normalizzazione dell'emergenza, idonee a trasformare il ricorso a misure eccezionali – quali ad esempio, la limitazione o la sospensione dei diritti fondamentali – in una sorta di prevenzione senza fine, giustificata dal pericolo del terrorismo", in G. M. FLICK, *Dei diritti e delle paure* in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, ESI, 2009; ma anche, tra i tanti: A. CARDONE, *La "normalizzazione" dell'emergenza*, Giappichelli, 2011; G. AGAMBEN, *Stato di eccezione*, Bollato-Boringhieri, 2003; P. BONETTI, *Terrorismo, emergenza e costituzioni democratiche*, Il Mulino, 2006; T. GROPPI, *Democrazia e terrorismo*, ESI, 2009; G. DE MINICO, *Costituzione. Emergenza e terrorismo*, Jovene, 2016.

[153] S. RODOTÀ, *Il diritto di avere diritti*, op. cit., p. 325.

[154] Come riassunto da Sartoretti, che riprende il pensiero di Foucault, "la ragione di fondo della accettazione ad essere sorvegliati è, nella modernità, la ricerca di sicurezza, che porta a rinunciare a porzioni di libertà in cambio

bene della sicurezza, a mò di buco nero, finisca con l'attrarre a sé e fagocitare ogni altro bene costituzionalmente protetto"[155]; tale insidia è certamente acuita dalle enormi potenzialità ormai fornite dal progresso tecnologico, grazie al quale sono aumentati i mezzi e gli strumenti certamente utili alla lotta al terrorismo e ad altre minacce alla sicurezza, ma anche fortemente invasivi della sfera privata e ancorati all'uso massivo di dati[156]. Se gli attentati terroristici, l'aumentare dei pericoli derivanti dal carattere transnazionale della criminalità e dai reati perpetrati anche nel Web o grazie alle nuove tecnologie hanno rappresentato i fattori contingenti che hanno spinto da un lato i Governi ad implementare sistemi di controllo e dall'altro i cittadini a percepire come sopportabile e financo legittima la restrizione della privacy e della *data protection*[157], altrettanto determinanti sono risultate invece le già citate rivelazioni di Edward Snowden, che hanno contribuito a determinare una maggiore consapevolezza dei rischi concreti e reali derivanti da una sistematica e incontrollata sorveglianza occulta dei dati che ci riguardano, anche in assenza di qualsiasi sospetto o di qualsiasi connessione con una minaccia più o meno incombente; una consapevolezza che ha altresì portato a richiedere maggiori tutele e salvaguardie a protezione della sfera privata e di quei dati che contribuiscono a determinare la nostra identità personale e, con essa, l'esercizio e il godimento delle libertà riconosciute nelle Costituzioni democratiche.

3.2. – I rischi della data retention*: la tensione costante ad una sorveglianza di massa e il delicato ruolo di legislatori e le Corti*

La ricostruzione fornita nei primi paragrafi avente ad oggetto lo studio delle potenzialità ma anche le minacce rappresentate dalla disponibilità ed utilizzo di Big Data, sistemi di AI ed algoritmi, trova chiara ed esemplificativa concretizzazione nella *data retention* e nelle complesse vicende normative e giurisprudenziali che attengono alla sua disciplina, tanto a livello nazionale quanto sovranazionale.

L'impiego, per finalità securitarie e di lotta alla criminalità, della vasta mole di dati e metadati prodotti mediante sistemi di telecomunicazione, è una tentazione cui ormai pare difficile opporre resistenza, così che negli ultimi decenni i Governi e legislatori, nazionali ed europei, hanno sempre più optato per scelte estensive di conservazione, accesso e trattamento di dati. Tra queste, rientra certamente lo strumento della *data retention* che diviene pertanto un osservatorio privilegiato che consente di esaminare le questioni enucleate in questo Capitolo sotto il profilo concreto delle delicate questioni che legislatori e Corti hanno affrontato nella determinazione di un corretto regime regolatorio della conservazione dei dati derivanti da telecomunicazioni. La sfida di garantire una adeguata tutela dei diritti fondamentali, sopra analizzati, alla riservatezza e alla protezione dei dati nel contesto di 'emergenza

---

di rassicurazioni sulla propria vita e il proprio benessere", C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *federalismi.it*, 13, 2019.

[155] A. RUGGERI, *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)*, in *Consulta Online*, III, 2016. Del resto "le tradizionali libertà negative sono i primi diritti fondamentali dell'uomo a risultare potenzialmente compressi dall'inasprimento delle misure di sicurezza", M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it*, 23, 2016.

[156] "La percezione del concetto di sorveglianza, che ha avuto un picco negli ultimi vent'anni appoggiandosi alla giustificazione della lotta al terrorismo, non viene più considerate, in molti casi, quale evento eccezionale ma come fenomeno normale, quotidiano, che è rivolto alla massa, a tutte le persone e non a uno in particolare, sino a dar vita, come ricorda Rodotà, all'ombra del cosiddetto uomo di vetro", G. ZICCARDI, *Internet, controllo e libertà*, op. cit., p. 92.

[157] Quella che Solove chiama efficacemente la teoria del "I have nothing to hide, I have nothing to fear": il fatto di non avere nulla da nascondere, porta a pensare che non debba esserci nulla da temere nel vedere la propria vita privata e le proprie comunicazioni controllate o analizzate. Proprio sulla confutazione di questa diffusa posizione, si fonda il libro di D. SOLOVE, *Nothing to hide. The false tradeoff between privacy and security*, Yale University Press, 2011.

normalizzata' e dinnanzi agli strumenti sempre più pervasivi offerti dal progresso tecnologico, si è così giocata sul campo delle complesse operazioni di bilanciamento, che si mostrano ancor più articolate laddove si trovi da un lato la finalità di tutela della sicurezza e dall'altro diritti quali la privacy e la protezione dei dati la cui rilevanza costituzionale ed importanza ai fini della tenuta della democrazia e delle libertà fondamentali sono sempre più riconosciute ed evidenti.

La disciplina della *data retention*, dunque, solleva quesiti, frutto e riflesso di quella complessità che si è sin qui cercato di tratteggiare, che richiedono pertanto decisioni e valutazioni determinanti, di profondo rilievo e dalle molteplici ricadute: non deve quindi stupire che le Corti europee e nazionali siano stati più volte chiamati a pronunciarsi in materia, con decisioni che sono ben presto state riconosciute di storica portata. Interrogandosi così sulla reale possibilità di individuare un punto di equilibrio ed un bilanciamento nel binomio sicurezza-riservatezza, i Parlamenti ed i Governi degli Stati membri così come le Istituzioni dell'UE si sono scontrate con visioni che promuovevano una logica di *trade-off* ovvero di esclusione della compatibilità di raggiungere obiettivi di garanzia della sicurezza e, contemporaneamente, di tutela dei diritti alla riservatezza e alla protezione dei dati; logica peraltro coerente con quella visione, di cui prima si parlava, che identificava nella rinuncia alla propria sfera privata un sacrificio sopportabile quanto necessario al raggiungimento di un elevato grado di sicurezza e nella garanzia dei diritti fondamentali una inevitabile limitazione dell'efficacia delle misure messe in campo nella lotta al terrorismo e alla criminalità. In questo contesto, le sentenze delle Corti di Lussemburgo e Strasburgo ma anche di talune Corti nazionali hanno assunto ruolo dirimente, producendo effetti anche sulle legislazioni nazionali e sulle scelte dei Governi, sempre più preoccupati e occupati dalla emergenza securitaria e protesi a sfruttare le potenzialità offerte dallo sviluppo tecnologico. Per tale motivo le questioni affrontate nella disciplina della *data retention* sono risultate fortemente intrecciate ad interrogativi profondi legati al rapporto tra legislatori europei e Corte di giustizia, tra competenze dell'UE e degli Stati membri, tra legislatori nazionali e giudici europei. A ciò sono da aggiungersi le difficoltà già evidenziate, dovute all'innovazione tecnologica, rapida ed incontrollata, che necessita di norme e regole chiare e flessibili, capaci di mostrare da un lato una profonda e concreta comprensione degli strumenti tecnologici e dall'altra la capacità di tradurre tali conoscenze in un linguaggio giuridico in grado di inserire nell'avanzamento della tecnica la tutela dei diritti fondamentali.

E la posta in gioco non è di poco conto: scongiurare il rischio di una società della sorveglianza e di una sproporzionata ingerenza e compressione della sfera privata, che mina la democrazia e le libertà fondamentali, per evitare di cedere sia alla tentazione di una garanzia della sicurezza a tutti i costi, sia al pericolo di divenire schiavi di un incontrollato e rapido progresso tecnico-scientifico[158].

[158] Per usare le parole di Soro, "se la tecnologia sconvolge l'antropologia, al diritto spetta ricomporne i frantumi, governare l'evoluzione perché l'uomo non ne sia sopraffatto", Intervento del Presidente del Garante all'incontro "Verso una nuova privacy?", 6 ottobre 2017, disponibile all'indirizzo: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6937167.

PARTE II

CAPITOLO I

LA DISCIPLINA LEGISLATIVA DELLA *DATA RETENTION* NELL'UNIONE EUROPEA: DALLA C.D. *E-PRIVACY DIRECTIVE* ALLA *DATA RETENTION DIRECTIVE*

Come emerso ed anticipato già nell'analisi svolta nella Parte I di questo elaborato, la grande sensibilità ed interesse che sin dagli ultimi decenni dello scorso secolo sono stati riservati, a livello comunitario, alla tutela della riservatezza e alla protezione dei dati sono sfociati nell'adozione di molteplici normative, a partire dalla nota Direttiva 95/46/CE "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", recante una disciplina generale ed ampia in materia di tutela dei dati. Dinnanzi al progresso tecnologico e alla complessità delle sfide derivanti dalla diffusione dei mezzi di comunicazione elettronica – telefonia e internet –, il legislatore europeo ha però ben presto sentito l'esigenza di intervenire mediante l'adozione di disposizioni specifiche, capaci di fronteggiare in maniera puntuale ed adeguata le problematiche derivanti dalla produzione, conservazione, raccolta e utilizzo dei dati e metadati prodotti, in enormi quantità, dai servizi di telecomunicazione. In questo contesto si collocano le prime disposizioni riguardanti espressamente la *data retention*, inserite inizialmente all'interno della Direttiva 2002/58/CE e successivamente in una normativa *ad hoc*, dedicata interamente alla regolamentazione della conservazione dei metadati: la controversa Direttiva 2006/24/CE.

La delicatezza delle questioni affrontate con queste misure e il loro impatto sui diritti fondamentali tutelati dalla Carta di Nizza, di cui si è già parlato precedentemente, sono alla base delle articolate vicende giudiziarie la cui analisi occuperà i prossimi capitoli: se la sentenza *Digital Rights Ireland* infatti avrà ad oggetto la c.d. Data Retention Directive, la pronuncia *Tele2 Sverige e Watson* riguarderà invece l'interpretazione della Direttiva 2002/58/CE e del suo problematico art. 15. È quindi da queste due normative che deve prendere abbrivio l'esame della disciplina europea in materia di *data retention*, prestando attenzione non solo al contenuto delle misure ma anche alle motivazioni e al dibattito politico e dottrinario che hanno caratterizzato l'adozione di specifiche scelte normative e che si riveleranno fondamentali per comprendere i rinvii pregiudiziali operati dalle Corti nazionali e, conseguentemente, le decisioni dei giudici europei.

1. – Dalla Direttiva 95/46/CE alla Direttiva 2002/58/CE: una prima disciplina in materia di conservazione dei dati derivanti da comunicazioni elettroniche

La storia e lo sviluppo di strumenti normativi posti a garanzia della riservatezza e della protezione dei dati nel contesto europeo trovano la propria origine nella nota Direttiva 95/46/CE, che per la prima volta ha visto la Comunità europea impegnata a determinare un punto di equilibrio tra libera circolazione di dati e servizi da un lato e diritti fondamentali alla riservatezza e alla protezione dei dati dall'altro. Con tale normativa veniva pertanto fissato uno standard di tutela della vita privata a livello sovranazionale, mediante il ravvicinamento delle legislazioni nazionali e l'imposizione di un grado di protezione dei dati e di privacy equivalente in tutti gli Stati membri, anche al fine di evitare che "i divari nei livelli di tutela dei diritti e delle libertà personali, in particolare della vita privata, garantiti negli Stati membri relativamente al trattamento di dati personali possano impedire la trasmissione dei dati stessi fra territori degli Stati membri e che tale divario possa pertanto costituire un ostacolo all'esercizio di una serie di attività economiche su scala comunitaria" (Considerando 7). Nel contesto appena delineato e come già

messo in evidenza nel Capitolo I, Parte I, risulta chiaro come l'azione della Comunità europea fosse, in tale momento 'iniziale', incentrata prevalentemente sulla costruzione di un mercato comune: ecco perché la predisposizione di una tutela comunitaria dei diritti fondamentali alla privacy e protezione dei dati, volta innanzitutto ad evitare che le difformità normative si traducessero in barriere e freni capaci di falsare la concorrenza, era diretta a regolare primariamente il trattamento di dati personali da parte di operatori economici privati o di autorità pubbliche solo qualora svolgano funzioni in qualità di *service providers*[1]. Le attività di raccolta, conservazione, accesso e utilizzo dei dati poste in essere da pubblici poteri ma finalizzate alla salvaguardia della pubblica sicurezza, difesa o sicurezza dello Stato o ancora del suo benessere economico non rientravano dunque nell'ambito di applicazione della Direttiva 95/46/CE[2].

Come spesso accade, tuttavia, i grandi mutamenti storici, politici e socio-economici pongono nuove sfide al mondo del diritto e impattano sulle scelte legislative: in primis, a partire dalla seconda metà degli anni '90, il grande progresso tecnologico – di cui si è già ampiamente parlato – nonché lo sviluppo di quella che viene definita 'società dell'informazione', caratterizzata dall'utilizzo massivo di nuovi servizi di comunicazione elettronica, avevano portato le Istituzioni europee a riflettere sull'esigenza di rafforzare e meglio garantire la tutela dei diritti fondamentali e, parallelamente, la libera circolazione dei dati e dei relativi servizi nel mercato unico. Il mutato panorama, caratterizzato dalla emergente specificità dei nuovi mezzi di comunicazione elettronica e dalla natura sempre più transfrontaliera di tali servizi, aveva fatto affiorare dunque l'importanza di un adeguamento delle già esistenti normative comunitarie poste a tutela dei dati mediante l'adozione di disposizioni mirate e plasmate sulla base delle peculiari necessità di protezione dei dati derivanti dalle innovazioni tecnologiche e dalle telecomunicazioni.

Ecco quindi che se un primo intervento in tal senso è da ravvisarsi nella Direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, una seconda e più strutturata disposizione veniva posta in essere invece nel 2002: si fa riferimento alla Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche,

[1] In altre parole, "The focus was large-scale data collection by the government and by the few private actors with the resources and technology to engage in such data processing-mostly banks and telecommunications providers. On the public side, these early laws largely affected those parts of government administration that routinely collected large amounts of information from citizens for purposes of providing services such as health care, education, and welfare", F. BIGNAMI, *Privacy and law enforcement in the European Union: the Data Retention Directive*, in *Chicago Journal of International Law*, 1, 2007, p. 234. Nonostante questa limitazione del suo ambito di applicazione, dovuta anche allo specifico riparto delle competenze tra Unione europea e Stati membri nonché alla divisione in Pilastri propria del funzionamento e dell'attività dell'Unione europea sino al Trattato di Lisbona, non bisogna affatto sottovalutare l'importanza della Direttiva 95/46/CE. Mediante tale normativa infatti "per la prima volta viene fissato uno standard di tutela obbligatoriamente vincolante per gli Stati appartenenti all'UE. Questa Direttiva rappresenta uno snodo cruciale se si vuol capire come l'Unione europea sia in grado di tutelare la nostra privacy permettendo congiuntamente la libera circolazione delle informazioni tra gli Stati membri. La sfida più importante cui la società e le istituzioni europee sono chiamate a rispondere è proprio questa: riuscire a dimostrare che un equo bilanciamento tra queste due differenti esigenze è possibile. (..) Un eventuale conflitto di norme nazionali sulla protezione dei dati presenti in vari paesi interromperebbe gli scambi internazionali, frenando il mercato e il processo di integrazione economica e sociale", L. CURICCIATI, *Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della* Data Retention Directive, in *Democrazia e Sicurezza*, 2, 2017, p. 95. Anche da queste parole emerge dunque quello stretto legame, di cui si è parlato anche nel previo Capitolo I, Parte I, tra libera circolazione delle merci e mercato unico da un lato e tutela dei diritti alla riservatezza e protezione dei dati dall'altro caratterizzanti l'intervento europeo.

[2] Art. 3, co. 2, Dir. 95/46/CE. L'art. 13 co. 1, poi, stabilisce che gli Stati membri possono adottare disposizioni volte a limitare la portata degli obblighi indicati nella medesima Direttiva "qualora tale restrizione costituisca una misura necessaria alla salvaguardia a) della sicurezza dello Stato; b) della difesa; c) della pubblica sicurezza; d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali (..)".

c.d. Direttiva *e-Privacy*)[3]. Questa normativa, facente parte di quello che era stato denominato il "Pacchetto Telecom"[4], nasceva dalla consapevolezza che "l'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata"[5]. Ed è da questa presa di coscienza che emergeva la necessità di predisporre regole armonizzate nel contesto europeo, "finalizzate a tutelare i diritti e le libertà fondamentali delle persone fisiche e i legittimi interessi delle persone giuridiche, con particolare riferimento all'accresciuta capacità di memorizzazione e trattamento dei dati relativi agli abbonati e agli utenti"[6].

Come ben si comprende dalle affermazioni richiamate, le Istituzioni europee iniziavano quindi a mostrare seria preoccupazione per i pericoli e le minacce derivanti dalle operazioni di 'memorizzazione' – e dunque di conservazione – su vasta scala della enorme mole di dati e metadati prodotti dai servizi di telecomunicazione. Proprio per scongiurare i rischi derivanti dalla ampia disponibilità di informazioni relative agli utenti e garantire la riservatezza sia delle comunicazioni svolte mediante rete pubblica di comunicazione e servizi di comunicazioni elettronica accessibili al pubblico, che dei 'dati sul traffico'– dunque i c.d. metadati[7] –, la regola generale espressa all'art. 5 era quella del divieto di memorizzazione. L'art. 6 della Direttiva *e-Privacy* imponeva di conseguenza l'obbligo in capo ai fornitori di servizi di comunicazioni elettronica di cancellare o rendere anonimi tutti i dati sul traffico relativi ai propri abbonati ed utenti, non appena tali informazioni non fossero più necessarie ai fini della trasmissione della comunicazione stessa oppure allo scopo di rendere possibile la fatturazione e i pagamenti (si parla in questa caso di 'memorizzazione tecnica').

Tale disciplina sembrava pertanto andare nella direzione di una forte tutela della protezione dei dati e della riservatezza delle comunicazioni, non solo con riferimento al loro contenuto bensì anche ai meri metadati: tale strada era frutto di quella rilevante e lucida consapevolezza, che già si affermava con forza

[3] Mentre la Direttiva 97/66/CE "ha tradotto i principi enunciati dalla Direttiva 95/46/CE in norme specifiche per il settore delle telecomunicazioni", a distanza di non molti anni emergeva la necessità di un adeguamento "agli sviluppi verificatisi nei mercati e nelle tecnologie dei servizi di comunicazione elettronica, in guida di fornire un pari livello di tutela dei dati personali e della vita privata agli utenti dei servizi di comunicazione elettronica accessibili al pubblico, indipendentemente dalle tecnologie utilizzate. Tale Direttiva [97/66/CE] dovrebbe pertanto essere abrogata e sostituita dalla presente Direttiva", Considerando n. 4, Direttiva *e-Privacy*.

[4] La Direttiva infatti si inseriva in un articolato quadro normativo (c.d. pacchetto Telecom) adottato nel 2002 ed emendato nel 2009, volto a regolare specifici aspetti del settore delle comunicazioni elettroniche e ad adeguare la disciplina europea al rapido sviluppo tecnologico. Ne facevano parte, oltre alla Direttiva richiamata, la Direttiva 2002/20/CE in materia di autorizzazioni per le reti e i servizi di comunicazione elettronica; la Direttiva 2002/19/CE in materia di accesso alle reti di comunicazione elettronica e alle risorse correlate; la Direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica. Sono inoltre stati aggiunti successivamente due regolamenti: il n. 1211/2009 che ha istituito l'Organismo dei regolatori europei delle comunicazioni elettroniche e il n. 531/2012 relativo al roaming sulle reti pubbliche di comunicazioni mobili.

[5] Direttiva 2002/58/CE, Considerando 6.

[6] Direttiva 2002/58/CE, Considerando 7.

[7] Sebbene nella Parte I di questo elaborato sia già stata fornita una definizione di metadati o dati sul traffico, merita qui ricordare l'indicazione ampia delineata dal legislatore europeo ed inserita nella Direttiva 2002/58/CE: "Una comunicazione può comprendere qualsiasi informazione relativa al nome, al numero e all'indirizzo fornita da chi emette la comunicazione o dall'utente di un collegamento al fine di effettuare la comunicazione. I dati relativi al traffico possono comprendere qualsiasi traslazione dell'informazione da parte della rete sulla quale la comunicazione è trasmessa allo scopo di effettuare la trasmissione. I dati relativi al traffico possono tra l'altro consistere in dati che si riferiscono all'instradamento, alla durata, al tempo o al volume di una comunicazione, al protocollo usato, all'ubicazione dell'apparecchio terminale di chi invia o riceve, alla rete sulla quale la comunicazione si origina o termina, all'inizio, alla fine o alla durata di un collegamento. Possono anche consistere nel formato in cui la comunicazione è trasmessa dalla rete", Considerando 15.

agli inizi del nuovo millennio, di quanto anche i dati sul traffico e la loro conservazione potessero ingerire nell'esistenza privata dei fruitori di servizi.

Purtuttavia la Direttiva in esame prevedeva anche una disciplina eccezionale rispetto al principio generale di cancellazione sopra delineato e che traeva origine, anch'essa, da una diversa ma rilevante consapevolezza: l'importanza sempre maggiore dei dati e metadati derivanti da comunicazioni elettroniche per scopi di garanzia della sicurezza pubblica e nazionale. L'art. 15, co. 1 della Direttiva 2002/58/CE, infatti, introduceva, come già aveva fatto la previa Direttiva 97/66/CE, una deroga al divieto di conservazione dei dati raccolti dagli operatori di telecomunicazione, stabilendo che gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi dell'art. 6 "qualora tale restrizione costituisca, ai sensi dell'art. 13, co. 1 della Direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri *possono* tra l'altro *adottare misure legislative che prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo*" (enfasi aggiunta). Se è sempre necessario contestualizzare le normative nel periodo storico entro cui vengono emanate, ecco che tale esercizio risulta determinante per comprendere l'ampia disciplina eccezionale appena richiamata: dopo i drammatici attentati terroristici del 2001 negli USA, anche molti Stati europei avevano deciso di rafforzare pratiche di prevenzione e contrasto delle minacce alla sicurezza nazionale o di repressione di reati gravi basate sull'analisi di dati e informazioni e sull'utilizzo di tecniche sofisticate di *data mining* (o *data fishing*) ad opera di autorità di intelligence o di *law enforcement*[8]. Gli Stati avevano quindi progressivamente riconosciuto le grandi possibilità derivanti dalla disponibilità di una vasta mole di informazioni da poter scandagliare e controllare: in tale contesto, come si è preliminarmente sottolineato nel previo Capitolo, "la conservazione e l'accesso ai metadati prodotti dalle comunicazioni elettroniche si collocavano in un complesso piano di *data surveillance* deciso a sfruttare le potenzialità delle nuove tecnologie per contrastare il fenomeno terroristico"[9].

Attribuendo così la facoltà – dunque non un obbligo ma una discrezionalità[10] – ai legislatori nazionali di disciplinare la *data retention* ed imporre agli operatori di telecomunicazioni la conservazione, per una durata più o meno ampia, dei metadati a scopi securitari[11], si percepisce l'accettazione da parte del

[8] "Electronic communications are increasingly used in the course of, and for the purpose of, criminal activity and threats to national security such as terrorism. As a result, access to the telecommunications data of criminals and their victims can play a vitally important role in the investigation of crime. Indeed, with the rise in cybercrime, access to such data may in some cases be indispensable", così D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018, che richiama sul punto D. ANDERSON, *A question of trust: report of the investigatory power review*, HM Stationery Office, 2015 e le considerazioni, sulle quali si dirà in seguito nel dettaglio, della Commissione europea contenute nella "Valutazione dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)", COM(2011)225.

[9] E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, in *IANUS*, 15, 2017, p. 283.

[10] Il testo normativo infatti stabilisce che "gli Stati membri *possono*" e non "devono" adottare misure derogatorie rispetto alla regola generale. Merita comunque rilevare come la possibilità in capo ai legislatori nazionali di adottare disposizioni contenenti "limitazioni della portata degli obblighi e dei diritti" riconosciuti dalla normativa europea, allo scopo di salvaguardare la "sicurezza dello Stato, della difesa, della pubblica sicurezza, della prevenzione, della ricerca, dell'accertamento e del perseguimento di reati" fosse già prevista all'art. 14 della sopra richiamata Direttiva 97/66/CE; in quella normativa tuttavia non vi era alcun espresso riferimento alla possibilità di adottare misure riguardanti la conservazione dei dati e metadati derivanti dai servizi di telecomunicazione.

[11] "Data surveillance has indeed occupied a special place in the European Union's response agenda for countering global security threats such as terrorism and organized crime. Cooperation between private and public actors has been crucial for the retention of data related to the use of electronic communications services for the purposes of combating crime", T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, in *European Current Law Issue*, 1, 2012.

legislatore europeo di un certo stemperamento della tutela della riservatezza e protezione dei dati qualora entrino in campo finalità di garanzia della sicurezza tali da giustificare l'adozione di strumenti normativi ritenuti maggiormente capaci di fronteggiare la minaccia terroristica ma al contempo più invasivi della sfera privata. Questa possibilità lasciata ai singoli legislatori degli Stati membri non era accompagnata, nella Direttiva 2002/58/CE, da alcuna specifica limitazione temporale mentre, sotto il profilo sostanziale, le condizioni e i limiti di utilizzo di tale potere derogatorio risultavano piuttosto ampie, essendo previsto all'art. 15 solo un generico riferimento agli ampi criteri di necessità, opportunità e proporzionalità che rimanevano purtuttavia piuttosto vaghi[12]. In altre parole, i margini di intervento lasciati agli Stati membri in tale ambito erano ampi e non veniva previsto un approccio comune alla disciplina della conservazione dei dati per scopi securitari. "In partenza si registra quindi l'assenza (..) – qualora entrino in gioco questioni di pubblica sicurezza – di un'intenzione forte dell'Unione europea di armonizzare la materia, sia verso l'alto (dettando termini massimi di conservazione, a tutela della riservatezza) che verso il basso (dettando termini minimi di conservazione, a tutela della sicurezza comune)"[13]; tale mancanza sfociava inevitabilmente nel riconoscimento di una vasta autonomia in capo agli Stati membri.

Questi elementi e considerazioni preliminari risultano di fondamentale importanza al fine di comprendere le problematiche emerse a seguito delle scelte dei legislatori nazionali e il successivo nuovo intervento del legislatore europeo.

2. – La Direttiva 2006/24/CE: il legislatore europeo alla prova della **data retention**

2.1. – La frammentaria regolamentazione degli Stati membri in materia di conservazione dei dati a scopi securitari: la necessità di una disciplina armonizzata a livello europeo

Dinnanzi alle sempre più concreta minaccia terroristica che incombeva anche sul territorio europeo dopo gli attentati che avevano colpito gli USA nel 2001, si erano andati moltiplicando gli interventi legislativi nazionali volti ad imporre in capo ai gestori di servizi di telecomunicazione una ampia conservazione di metadati per finalità securitarie. Tali disposizioni[14], fondate proprio sulla disciplina derogatoria garantita dall'art. 15 della Direttiva *e-Privacy*, sopra analizzata, si basavano sulla convinzione che la *data retention* – e dunque la conseguente possibilità per le autorità di *law enforcement* di disporre, accedere ed utilizzare le informazioni conservate – rappresentasse uno

[12] Viene previsto inoltre all'ultimo comma dell'art. 15 che "tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'art. 6, par. 1 e 2 TUE". Tale ultima disposizione faceva ovviamente riferimento alla versione del TUE risalente al 1992 (c.d. Trattato di Maastricht): essa all'art. 6 individuava il fondamento dell'Unione europea nei principi di libertà, democrazia, rispetto dei diritti dell'uomo e delle libertà fondamentali, dello stato di diritto (par. 1), nonché stabiliva il rispetto dei diritti fondamentali garantiti dalla Convenzione EDU e dalle tradizioni costituzionali comuni degli Stati membri (par. 2).

[13] F. GUELLA, Data retention *e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina EU al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE Online*, 2, 2017, p. 350. L'autore prosegue rilevando come "la Direttiva del 2002 era del resto intervenuta in un contesto normativo in cui i legislatori nazionali avevano talvolta già disciplinato la materia, come ad esempio nel caso italiano, dove il cd. Codice della privacy aveva fissato in 30 mesi il periodo di conservazione generalizzata dei dati. Tali opzioni, in sede di prima applicazione della Direttiva 2002, non sembravano per nulla precluse alle autorità nazionali, che potevano conservare discipline di questo genere accedendo ad un'interpretazione della Direttiva che riconosceva ampia autonomia procedurale e un esteso margine di apprezzamento agli ordinamenti nazionali, omettendo di dettare più precise prescrizioni utili per un controllo di proporzionalità", p. 351.

[14] Si pensi a titolo di esempio al Criminal Justice Terrorist Offenses Act n. 64 del 2005, adottato in Irlanda, che imponeva ai *service providers* una conservazione della durata di tre anni di tutti i metadati derivanti da comunicazioni elettroniche.

strumento fondamentale per la tutela della sicurezza nazionale e pubblica, sia in fase preventiva che successiva di indagine.

L'adozione di misure normative eccezionali rispetto alla regola generale della cancellazione o anonimizzazione dei dati di traffico aveva creato però un panorama estremamente frammentario all'interno dell'Unione europea[15], non mancando di sollevare rilevanti problematiche giuridiche ed economiche: le leggi sulla conservazione dei dati differivano anche considerevolmente da Stato a Stato e ponevano difficoltà applicative di non poco conto, oltre a notevoli costi, in capo agli attori privati operanti nel settore delle telecomunicazioni, che dovevano così adeguarsi a diversi obblighi legislativi a seconda del territorio in cui operavano, con ripercussioni negative sulla libera circolazione di merci e servizi[16]. Oltre a tale aspetto impattante sul mercato interno europeo, vi erano certamente forti preoccupazioni e timori sul fronte della tutela dei diritti fondamentali ed in particolare dei diritti alla riservatezza e alla protezione dei dati: iniziavano infatti a porsi questioni ed interrogativi sui limiti e sulle condizioni dell'accesso ai dati nonché sulla proporzionalità delle misure di conservazione stessa, che rappresentavano *per se* una ingerenza nella sfera privata di tutti gli utenti che vedevano così i propri dati e metadati, senza alcuna distinzione o senza che ricorresse alcun sospetto o alcuna connessione con il pericolo o la minaccia di un reato (c.d. *bulk data retention*), sottoposti a memorizzazione per periodi di tempo anche considerevoli.

A questo già articolato e complesso contesto è da aggiungersi l'emergenza securitaria resa ancora più evidente a seguito dei drammatici attacchi che avevano colpito Madrid e Londra negli anni 2004 e 2005; da tali vicende, in particolare, era affiorata l'esigenza di una risposta comune europea in materia di lotta al terrorismo e di un'azione, quanto più congiunta e condivisa tra i vari Stati membri, che fosse capace, tra i vari aspetti, di rafforzare la cooperazione a livello comunitario anche mediante un più efficiente ed efficace sistema di scambio di dati e informazioni tra Stati[17]. Se la disponibilità di metadati aveva dunque assunto un rilievo di fondamentale importanza anche a livello europeo, diveniva necessario allora fronteggiare la lacunosità derivante dalla frammentaria disciplina della conservazione

[15] Come riportato nell'Extendend Impact Assessment elaborato dalla Commissione europea e relativo alla proposta di Direttiva in materia di *data retention* (SEC(2005)1131), nel 2005 le discipline nazionali regolanti la conservazione dei dati derivanti da telecomunicazioni adottate sulla base di quella eccezione garantita all'art. 15 Direttiva *e-Privacy* differivano in termini sia di tipologia dei dati da conservare, che di scopo della conservazione, durata e condizioni di accesso ai dati stessi. Secondo gli studi svolti, "a majority of Member States at present do not have mandatory data retention obligations; in about half of the Member States with mandatory data retention obligations laws in place, data retention is not operational since implementing measures are still missing; in those Member States with data retention obligations in operation, the period (between 3 months and 4 years) and scope vary substantially e.g. just pre-paid mobile, not the Internet, all services etc.", p. 6.

[16] I costi in capo ai fornitori di servizi aumentavano infatti dinnanzi agli obblighi disomogenei stabiliti dai vari Stati. Nell'Extendend Impact Assessment elaborato dalla Commissione europea e richiamato nella precedente nota, veniva sottolineato come "the impact of the current situation is mainly twofold. On the one hand, diverging national legislations on traffic data retention have a significant negative impact on this major economic sector. This point has also been stressed time and again by the contributions from industry to the public debate on data retention. On the other hand, obligations related to traffic data retention have in any event cost effects on the providers of electronic communication services. As analysed below, these costs are notably associated with the adaptation of existing systems, the storage, and the resources to deal with requests for access to data from law enforcement authorities. These depend in particular on the types of data which need to be retained; the actual length of the retention period, and whether or not these periods are harmonized throughout the EU", p. 7.

[17] Come ben spiega Bignami "In the past few years cooperation on criminal matters under the legal umbrella of the EU has intensified. In theory, the terrorist attacks might have provoked no more than closer pan-European cooperation on fighting terrorism. Instead, these attacks have triggered cooperation on a wide range of law enforcement matters. The exchange of personal data to prevent and prosecute criminal acts is a critical form of such collaboration", F. BIGNAMI, *Privacy and law enforcement in the European Union: the Data Retention Directive*, op. cit., p. 237. Anche Fennelly ha sottolineato come "following the Madrid and London terrorist attacks in 2004 and 2005, proposals to regulate data retention at EU level gained momentum", D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, op. cit., p. 3.

dei dati, che vedeva, come si è visto, una regolamentazione assolutamente disomogenea a seconda degli Stati membri, rendendo spesso ardua una effettiva collaborazione e condivisione di informazioni.

Per far fronte a tali sfide e problematiche, il dibattito circa la necessità di un intervento legislativo comunitario che predisponesse una normativa *ad hoc* in materia di conservazione dei dati derivanti dalle telecomunicazioni elettroniche si era intensificato, non senza difficoltà e perplessità espresse da parte delle Istituzioni e autorità coinvolte nonché dell'opinione pubblica.

In questo panorama, la Comunicazione della Commissione "Migliorare l'accesso all'informazione da parte delle autorità incaricate del mantenimento dell'ordine pubblico e del rispetto della legge" (COM (2004) 429 def) metteva in luce l'importanza di una maggiore interazione tra Stati membri nella lotta al terrorismo; tale obiettivo, secondo la Commissione, doveva essere raggiunto anche attraverso la predisposizione di misure "indispensabili per rendere accessibili i dati e le informazioni pertinenti e necessarie alle autorità UE incaricate della repressione del crimine, allo scopo di prevenire e combattere il terrorismo e le altre forme di criminalità grave o organizzata, come pure le minacce che da esse derivano" (p. 4). Per ottenere questo risultato era quindi fondamentale "garantire che i dati pertinenti raccolti a fini diversi dell'applicazione della legge siano disponibili", benché "solo fino a quanto ciò sia adeguato, necessario e proporzionato agli scopi specifici e legittimi perseguiti". Anche in questo documento tuttavia emergevano preoccupazioni circa l'utilizzo di operazioni significativamente invasive della vita privata di ciascun utente e non veniva taciuta quindi l'esigenza di "ricercare un adeguato equilibrio tra una protezione rigorosa dei dati e il debito rispetto degli altri diritti fondamentali da un lato e, dall'altro, un utilizzo davvero efficace delle informazioni da parte delle autorità incaricate della repressione dei reati al fine di garantire gli interessi pubblici essenziali come la sicurezza nazionale e la prevenzione, l'individuazione e il perseguimento dei reati" (p. 5).

L'importanza della disponibilità di dati e metadati – anche e soprattutto quelli derivanti da servizi di telecomunicazione – come strumento funzionale alla possibilità di un successivo utilizzo di tali informazioni al fine di creare forme di cooperazione tra i diversi Stati risultava anche da quanto affermato dal Consiglio europeo nella Dichiarazione sulla lotta al terrorismo, adottata il 25 marzo 2004, nella quale veniva dato peso prioritario alla adozione di un quadro normativo comunitario in materia di conservazione dei dati relativi al traffico delle comunicazioni da parte dei prestatori di servizi. Proprio in questa direzione si muoveva la proposta di una Decisione Quadro sulla conservazione dei dati presentata da quattro Stati membri – Francia, Irlanda, Svezia e Regno Unito – al Consiglio GAI nell'aprile 2004 (Doc 8954/04, Crimorg 36, Telecom 82)[18], recante misure volte ad agevolare la cooperazione giudiziaria e di polizia in materia penale mediante l'adeguamento delle norme nazionali disciplinanti la *data retention*. L'idea era quella di introdurre un obbligo in capo agli Stati membri di adozione di discipline volte ad imporre ai *service providers* la conservazione di tutti i metadati derivanti da servizi di comunicazione elettronica, escludendo dunque i contenuti delle comunicazioni stesse e lasciando alla scelta dei legislatori nazionali la determinazione del periodo di *retention* entro il limite minimo di 12 mesi e massimo di 3 anni, con alcune possibilità di proroga. La proposta quindi mirava a rappresentare una spinta verso l'armonizzazione della disciplina in materia di conservazione dei dati a livello europeo, motivata, come si è detto, dalla esigenza di una maggiore uniformità regolatoria capace di garantire sia una più efficiente cooperazione e scambio di informazioni per contrastare la minaccia

[18] In realtà una proposta in tal senso era già stata promossa nel 2001: "The Belgian Presidency in 2001 prepared a Draft Council Framework Decision on the retention of traffic data and on access to these data in connection with criminal investigations and prosecutions, where they proposed the retention of traffic data 'for the purpose of criminal investigations and prosecutions, either on the part of the telecommunications and prosecutions, either on the part of the telecommunications service providers who holds the data in question, or on the part of a trusted third party, for a period of 12 months minimum and 24 maximum". This initiative was never officially discussed in the EU", E. KOSTA, P. VALCKE, *Retaining the data retention directive*, in *Computer Law & Security Report*, 22, 2006, p. 371.

terroristica[19], sia l'eliminazione degli ostacoli alla libera circolazione di dati e servizi, permettendo così di scongiurare distorsioni del mercato e della concorrenza tra operatori del settore.

Vari dubbi e timori erano stati tuttavia avanzati rispetto a questa proposta, tanto sotto il profilo della base giuridica scelta – la Decisione Quadro rientrava nel Terzo Pilastro (artt. 31, co. 1, lett. c e art. 34, co. 2, lett. b) – quanto sotto il profilo sostanziale con riguardo alla proporzionalità e necessità della *data retention* stessa e della sua compatibilità con l'art. 8 della Convenzione EDU, con l'art. 15 della Direttiva *e-Privacy* e ancora con il principio di presunzione di non colpevolezza, tenendo in considerazione il carattere del tutto generalizzato ed indiscriminato che la conservazione assumeva. Questi limiti erano stati sottolineati anche dal relatore della Commissione per le libertà pubbliche, giustizia e affari interni del Parlamento Europeo[20].

Prendendo atto infatti della duplicità degli obiettivi della disciplina della *data retention* e quindi della sua capacità di incidere sia sul mercato che sulla cooperazione in materia di giustizia e sicurezza, una prima criticità era stata ravvisata nella individuazione della corretta base giuridica: in particolare, con riferimento a tale punto che, come si vedrà anche nel prossimo Capitolo, è stato ed è tuttora oggetto di

[19] Sotto questo profilo, l'armonizzazione della disciplina della conservazione dei dati avrebbe risolto un ulteriore problema: "approximation is necessary to effectively deal with serious crime as otherwise criminals may take advantage of the differences between criminal justice systems to identify less effective ones as safe havens (a kind of 'forum shopping'", F. GALLI, *Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions*, in *Maastricht of European and Comparative Law Journal*, 3, 2016, p. 463.

[20] Sul punto si rimanda ampiamente al *Documento di lavoro sulla proposta di una decisione quadro relativa alla conservazione preventiva di dati che sono elaborati e conservati per fornire servizi elettronici pubblici, ovvero di dati presenti nelle reti di comunicazione pubbliche, a fini di prevenzione, indagini, accertamento e perseguimento di reati, compresi atti di natura terroristica*, elaborato dalla Commissione per le libertà pubbliche, giustizia e affari interni del Parlamento Europeo (DT/553885IT.doc, del 31 maggio 2005). In questo documento si legge: "Il relatore mette in questione la proporzionalità stessa dei provvedimenti in esame. Il rapporto tra mezzi e scopi appare infatti poco equilibrato: le misure in esame non sono né idonee né indispensabili e i loro effetti sugli interessati appaiono inaccettabilmente duri. Considerando il volume dei dati da conservare, in particolare nell'ambito di Internet, è controverso se sia possibile nella pratica una valutazione dei dati che sia di ausilio al raggiungimento dell'obiettivo. Gli utenti provenienti dalla sfera della criminalità organizzata e del terrorismo sapranno facilmente come eludere la tracciabilità dei loro dati. Tra le possibilità atte allo scopo potrebbero figurare l'acquisto di carte telefoniche da parte di soggetti prestanome oppure l'impiego alternato di telefoni cellulari di operatori stranieri, l'utilizzo di cabine telefoniche pubbliche, la modifica dell'indirizzo IP o dell'indirizzo e-mail per l'uso di un servizio di posta elettronica oppure direttamente l'uso di provider di servizi Internet che hanno la loro sede al di fuori dell'Europa e non sono soggetti ad obblighi in merito alla conservazione preventiva di dati. Nel caso in cui dovessero essere effettivamente conservati tutti i dati di traffico interessati dalla decisione, inclusi i dati Internet, la rete di un grande provider di servizi Internet già con il volume di traffico odierno raccoglierebbe una quantità di dati pari a 20-40.000 terabyte. Si tratta di un volume di dati corrispondente a quello di un raccoglitore cartaceo dello spessore di circa 4 mln. di km, il che corrisponde a sua volta a dieci montagne di atti ognuna delle quali coprirebbe la distanza dalla terra alla luna. Con tale gigantesca mole di dati, per una sola ricerca che utilizzi le tecnologie disponibili senza investimenti aggiuntivi occorrerebbero 50-100 anni, il che fa nutrire dubbi sulla rapida disponibilità dei dati richiesti". Da tale documento emergevano anche dubbi relativi alla correttezza della scelta della base giuridica: una normativa in materia di conservazione dei dati capace di incidere e rappresentare un obbligo in capo agli operatori di telecomunicazioni avrebbe dovuto essere regolata sulla base del Primo Pilastro mentre nel Terzo Pilastro avrebbe dovuto rientrare una normativa relativa unicamente all'accesso e scambio di dati tra autorità di *law enforcement*, regolamentazione che però non era stata ritenuta necessaria dalla Commissione stessa. Per questo la relazione si concludeva con il respingimento del progetto di Decisione Quadro da parte del relatore nonché con l'invito alla Commissione affinché, nell'attesa che gli Stati membri presentassero uno studio in grado di provare in modo inconfutabile la necessità della progettata conservazione dei dati, elaborasse una proposta di Direttiva nella quale si trattasse l'obbligo di memorizzazione dei dati, la definizione dei dati da conservare e la durata della conservazione. Conformemente alla posizione del Relatore, il Parlamento europeo aveva votato, il 7 giugno 2005, per respingere la proposta degli Stati membri. Merita ricordare, comunque, come tale decisione del Parlamento avesse valenza meramente consultiva, visto che la proposta si inseriva nel procedimento di approvazione di una Decisione Quadro nell'ambito del Terzo Pilastro, che escludeva quindi il Parlamento dalla procedura di approvazione stessa. Per approfondimenti su questa prima posizione del Parlamento europeo in materia di *data retention*, si manda a S. SAXBY, *European Parliament says 'No!' to Member States' data retention proposal*, in *Computer Law & Security Report*, 21, 2005, p. 279.

forte dibattito, venivano sollevati alcuni dubbi quanto alla riconducibilità delle misure in materia di conservazione dei dati al Primo Pilastro oppure al Terzo. Se per limitare il ricorso al metodo intergovernativo proprio degli atti del Terzo Pilastro, l'art. 47 TUE riconosceva la *primauté* del diritto comunitario e dunque del Primo Pilastro[21], la disciplina della conservazione dei dati e la duplicità dei suoi obiettivi poneva problematiche di non poco conto, collocandosi in una posizione 'interpilastro'[22]. Merita solo brevemente ricordare come tale questione abbia un impatto tutt'altro che formale, incidendo anche sul procedimento di adozione degli atti[23].

Il dibattito che si era venuto a creare e le perplessità evidenziate avevano dunque portato al definitivo naufragio della proposta di Decisione Quadro analizzata.

Accantonato tale primo tentativo ma riconoscendo l'importanza di addivenire ad una regolamentazione europea della conservazione dei dati, la Commissione, forte della spinta acceleratrice degli attentati di Londra, decideva di promuovere, il 21 settembre 2005, l'adozione di una Direttiva, utilizzando però in questo caso quale base giuridica il Primo Pilastro, optando quindi per una armonizzazione della disciplina in grado di ridurre quel margine di discrezionalità attribuito agli Stati membri dall'art. 15 della Direttiva *e-Privacy*[24] e stabilendo così un bilanciamento tra sicurezza e riservatezza che fosse, quanto meno nei principi generali, uguale per tutti gli Stati membri. Nell'Extended Impact Assessment allegato alla proposta di Direttiva (SEC(2005)1131), la Commissione aveva evidenziato da subito la grande difficoltà di fornire una adeguata protezione dei dati e del diritto alla riservatezza e, contemporaneamente, rispondere al bisogno dello Stato di disporre di adeguati strumenti di salvaguardia della vita dei propri cittadini (pp. 5-6). Pur consapevole quindi dell'impatto che una conservazione generalizzata di informazioni attinenti a tutti gli utenti di servizi di telecomunicazioni finiva col rappresentare per la vita privata degli utenti europei, la richiamata regola generale stabilita dalla Direttiva *e-Privacy* e determinante l'obbligo di cancellazione o anonimizzazione dei dati raccolti dai *service providers* era stata ritenuta dalla Commissione eccessivamente limitativa, rendendo troppo arduo per le autorità pubbliche assolvere ai propri doveri di prevenzione e indagine dei crimini gravi e terroristici[25]: la mancata disponibilità dei dati rendeva infatti "easier for criminals to

[21] Per una lettura più ampia su questo punto, si legga, tra i tanti, il commento all'art. 47 TUE di V. R. MASTROIANNI in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Giuffré, 2014, p.233 ss.

[22] Come ben richiamato da E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, op. cit., p. 285 e come ripreso anche da L. PALADINI, *I conflitti tra Pilastri dell'Unione europea e le prospettive del Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, 1, 2010, p. 89 ss. e da F. FONTANELLI, *La Corte di Giustizia e il 'favor communitatis'. Il percorso della giurisprudenza della Corte di Giustizia delle Comunità europee sul fondamento normativo degli atti dell'Unione*, in *Rivista di diritto pubblico comunitario*, 1, 2010, p. 177 ss. Il punto verrà affrontato più ampiamente nel Capitolo II di questa Parte II, in particolare nell'analisi delle decisioni della CGUE in materia.

[23] La scelta di proporre una Decisione Quadro sulla base del Terzo Pilastro escludeva, infatti, come richiamato già nella nota 20, il Parlamento europeo dal procedimento di adozione e approvazione dell'atto e limitava anche l'intervento successivo della CGUE (ai sensi dell'art. 35 TUE) mentre, diversamente dagli atti riguardanti il Primo Pilastro, veniva richiesto il voto all'unanimità del Consiglio. Con riferimento a questi profili, per una più compiuta riflessione si rimanda a B. NASCIMBENE, *European Judicial Cooperation in criminal matters: what protection for individuals under the Lisbon Treaty?*, in *ERA Forum*, 10, 2009, p. 397 ss.

[24] "A regulation would have been too stringent, notably in view of the different technical architectures used by the various operators in different countries. the Directive will leave sufficient margin to Member States to adapt to national constraints", COMMISSIONE EUROPEA, *Extended Impact Assessment. Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*, SEC(2005)1131, 21 settembre 2005.

[25] Nel documento richiamato infatti viene affermato come "there is no doubt that the availability of traffic data can indeed be important for certain 'public order' purposes such as specific national security threats or specific investigations into criminal offences. This is why public authorities in the Member States are in principle, if necessary and in accordance with applicable law, able to request access to traffic data stored by electronic communications operators for their own business purposes. Legitimate requests for the retention of specific data – otherwise called data preservation – are also allowed when necessary for specific purposes, such as investigations

communicate with each other without the fear that their communications data can be used by law enforcement authorities to thwart them"[26].

Riconosciuta la necessità di introdurre forme di memorizzazione dei dati, la Commissione procedeva quindi ad una interessante valutazione tra due differenti approcci ed alternative possibili: *data preservation* e *data retention*. La prima, suggerita in particolare dai fornitori di servizi di telecomunicazione, dalle autorità nazionali garanti della protezione dei dati e dagli attivisti del settore, avrebbe consentito alle autorità di *law enforcement* di richiedere agli operatori la conservazione dei soli dati relativi a determinate persone mentre la seconda avrebbe previsto, come già si è detto, una *data retention* generalizzata cioè riguardante i metadati relativi alle telecomunicazioni di tutti gli utenti. Mentre la *data preservation* risultava meno invasiva dei diritti alla riservatezza e alla protezione dei dati e anche meno costosa per i *service providers* stessi, essa presentava, ad opinione della Commissione, una efficacia maggiormente limitata: benché fosse considerata uno strumento estremamente utile laddove uno o più sospetti fossero già individuati a seguito di investigazioni, la sua efficacia valeva così solo per il futuro, così da non poter consentire, a differenza della *data retention,* una indagine del passato ovvero di metadati prodotti quando ancora non vi era alcun sospetto nei confronti di un soggetto o addirittura nei casi in cui si volesse prevenire un reato non ancora commesso. Usando le parole della Commissione, "data preservation is only useful as of the moment when suspects have been identified; data retention is indispensable in many cases to actually identify those suspects"[27]. Sulla base di tali considerazioni, la Commissione aveva ritenuto di dover scartare l'opzione della *data preservation* a favore di una più ampia *data retention* avente ad oggetto tutti i metadati prodotti dagli utenti di servizi di telecomunicazione. La proposta pertanto si era concretizzata nella disposizione di un obbligo in capo ad ogni Stato membro di adottare normative in materia di conservazione dei dati per finalità securitarie e dunque per scopi di repressione di reati 'gravi' ed entro i termini e le condizioni stabilite nella Direttiva stessa, che verrà più ampiamente analizzata nel prossimo paragrafo. Quanto merita preliminarmente comprendere è come tale scelta si discostasse fortemente dal panorama normativo precedente: ai sensi dell'art. 15 della Direttiva *e-Privacy*, infatti, ai legislatori degli Stati membri veniva attribuita la facoltà e la discrezionalità di stabilire, per finalità eccezionali, normative 'straordinarie' e in deroga alla disciplina generale di cancellazione dei metadati, imponenti la conservazione delle informazioni raccolte nella normale erogazione di un servizio di telecomunicazione; con la Direttiva proposta dalla Commissione, invece, veniva *imposta* l'adozione di una disciplina nazionale sulla conservazione,

---

and prosecutions", p. 3. E ancora, sul punto: "In terms of the importance of traffic data for serious criminal offences and terrorism numerous examples were provided to the Commission in the consultation process, ranging from the investigation in the Madrid bombing, where telephone data up to six months old was investigated, to the Omagh bombing, the murder of French Prefect Erignac, of famous Irish journalist Veronica Guerin, other murder cases, extortion attempts etc. Examples were also given where traffic data was used to exculpate the defendant" (p. 5).

[26] COMMISSIONE EUROPEA, *Extended Impact Assessment*, op. cit., p. 3. Viene poi riportato come "the law enforcement authorities of another Member State indicated that of requests made for Internet related data, 30 to 40% remained unanswered because the data has already been deleted" p. 6.

[27] "The simple scenario given by one of the law enforcement experts during consultations already indicates that data preservation by itself is not enough for law enforcement authorities to actually be able to investigate and solve crime and terrorism cases. As indicated above as well, the investigation into the Madrid bombings relied heavily on obtaining and analyzing traffic data going back 3 to 6 months. It should be clear to anyone that depriving law enforcement authorities of the possibility to look into what happened prior to the crime being committed makes their work next to impossible. One can draw a comparison with investigations in the physical world – how effective would law enforcement be if prior to the start of an investigation all physical evidence were to be removed from the crime scene?", COMMISSIONE EUROPEA, *Extended Impact Assessment*, op. cit., p. 12. In questo stesso documento veniva richiamata l'opinione di alcuni esperti nel settore di *law enfocement*, che avevano equiparato i metadati alle impronte digitali: "whereas in the physical world physical evidence can be gathered, in a digital world traffic data is the digital equivalent to fingerprints", p. 5. John Abbott, Direttore generale del National Criminal Intelligence Service del Regno Unito, in occasione del First Plenary Session of the European Union Forum on Cyber crime aveva affermato anche: "in the case of a crime committed wholly or partially in the E-World, if there is not traffic data, there can be no investigation. It is as simple as that".

riducendo così quella discrezionalità fornita dalla Direttiva del 2002 e ordinando "l'utilizzo di questi strumenti come normale metodo investigativo per la repressione di gravi reati"[28].

La Commissione, quindi, come emerge dall'Impact Assessment e dalle riflessioni sopra indicate, aveva ritenuto la misura proposta corretta e legittima, in piena conformità agli artt. 52, 7 e 8 della Carta di Nizza, introducendo una compressione proporzionata e necessaria dei diritti fondamentali per il raggiungimento di un legittimo interesse. La scelta di una conservazione generalizzata dei metadati, tuttavia, come già era accaduto per la simile proposta di Decisione Quadro, non aveva mancato di destare forti dubbi espressi sia dal Garante Europeo della Protezione dei Dati (GEPD) che dal Gruppo di Lavoro Art. 29 per la tutela dei dati personali. Quest'ultimo, sin dalla proposta avanzata da alcuni Stati membri nel 2004 e con riflessioni che ugualmente valgono per la Direttiva, aveva espresso profonde perplessità quanto alla proporzionalità della *data retention* considerata *per se*: "the routine, comprehensive storage of all traffic data, user and participant data proposed in the draft decision would make surveillance that is authorised in exceptional circumstances the rule. This would clearly be disproportionate. The draft framework would apply, not only to some people who would be monitored in application with specific laws, but to all natural persons who use electronic communications. (..)". Usando come parametro di riferimento la giurisprudenza della Corte EDU – di cui si parlerà ampiamente nel Capitolo V – e l'art. 8 della Convenzione EDU, il Gruppo di Lavoro arrivava alla conclusione che "the mandatory retention of all types of data on every use of telecommunication services for public order purposes, under the conditions provided in the draft Framework Decision [ma similmente anche nella Direttiva], is not acceptable within the legal framework set in Article 8"[29]. Nella Opinione 4/2005, riferita espressamente alla proposta di Direttiva in materia di *data retention,* venivano nuovamente ribaditi i dubbi circa la necessità e proporzionalità della conservazione dei dati generalizzata, richiamando espressamente l'esistenza di diversi e ulteriori mezzi utili a fini investigativi ma in grado di avere un minore impatto sui diritti fondamentali degli utenti: veniva citata la c.d. "procedura *quick freeze* [altro termine con cui è definita la *data preservation*] nella quale né i fornitori di comunicazione né i fornitori di servizi Internet sono tenuti a memorizzare i dati sul traffico. Per esempio, nei casi che lo giustifichino, gli organi di contrasto consultano le società e chiedono di memorizzare certi dati. Quegli organi dispongono quindi di alcune settimane per raccogliere le prove necessarie per ottenere un provvedimento giudiziario. Solo allora potranno accedere ai dati"[30]. Anche il GEPD nel suo Parere sulla proposta di Direttiva aveva esposto la propria opinione negativa rispetto alla necessità e proporzionalità della *data retention* quale strumento di lotta alla criminalità, così come proposto dalla Commissione: "Il GEPD riconosce i mutamenti intervenuti, ma non è ancora convinto della necessità della conservazione dei dati relativi al traffico e all'ubicazione per finalità legate alle attività delle forze dell'ordine, come stabilito nella proposta. Sottolinea l'importanza del principio di diritto stabilito dalla Direttiva 2002/58/CE secondo

[28] E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, op. cit., p. 287.

[29] ARTICLE 29 DATA PROTECTION WORKING PARTY, *Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism*, 11885/04, 9 novembre 2004.

[30] GRUPPO DI LAVORO ART. 29, *Parere 4/2005 sulla proposta di Direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la Direttiva 2002/58/CE (COM(2005)438 definitivo del 21.9.2005)*, 1868/05, 21 ottobre 2005. Come sottolineato da Guild e Carrera, "[Data preservation] occurs when a tribunal orders a service provider to retain (from the date of the preservation order) the data of specified individuals who are suspected of criminal activities. Data preservation is a specific targeted law enforcement measure maned by judicial authorities across the EU member states and often used as a less intrusive alternative to data retention. In the case of preservation, a judge must be convinced that it is necessary in a specific case of law enforcement to quick-freeze someone's data. Thus the criminal justice systems control the issuing of data preservation orders, and these institutions are familiar with the necessity of acting within the confines of due process and fair trial", E. GUILD, S. CARRERA, *The political and judicial life of metadata: Digital Rights Ireland and the trial of the Data Retention Directive*, CEPS Paper in Liberty and Security in Europe, 65, 2014.

cui i dati relativi al traffico devono essere cancellati non appena la memorizzazione non è più necessaria per finalità che non sono connesse con la comunicazione stessa. Inoltre, le cifre fornite non provano che il quadro giuridico esistente non offra gli strumenti necessari per tutelare la sicurezza fisica, né che gli Stati membri utilizzino appieno le loro competenze ai sensi del diritto europeo per cooperare come consentito loro dal quadro giuridico vigente (ma senza i risultati necessari)"[31]. Più di 80 *service providers* e 90 ONG, tra cui Privacy International e Digital Rights, che troveremo protagoniste degli interventi giurisprudenziali promossi a livello nazionale e approdati poi dinnanzi alla CGUE, avevano scritto un accorato appello al Parlamento europeo affinché quest'ultimo respingesse la direttiva proposta[32].

Nonostante le critiche piuttosto rilevanti che avevano messo in discussione sin dalle sue fondamenta la scelta delle Istituzioni europee e dopo un ampio dibattito tra Commissione, Consiglio e Parlamento, che aveva portato peraltro a notevoli modifiche rispetto al testo originario predisposto dalla Commissione[33], il legislatore comunitario comunque approvava, il 15 marzo 2006, la Direttiva 2006/24/CE "riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica

[31] GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di Direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della Direttiva 2002/58/CE*, 26 settembre 2005. È interessante ricordare quanto riportato da T. KONSTADINIDES (in *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, op. cit., p. XV) riguardo al parere espresso dal Comitato Economico e Sociale Europeo: "the EESC expressed surprise and concern over the submission of such a proposal for a Directive. The EESC predicted that the Directive, in its proposed form, was at risk of being declared unconstitutional by national constitutional courts because the fundamental rights test used by the Commission was both flimsy and flawed. For instance, the EESC suggested that the Commission's proposal only mentioned arts. 7 and 8 ECHR as safeguards, while it ignored arts. 36 (access to services of general interests), 38 (consumer protection), 47 (right to an effective remedy) and 48 (presumption of innocence)".

[32] "The retention of personal data resulting from communications, or of traffic data, is necessarily an invasive act. With the progress of technology, this data is well beyond being simple logs of who we've called and when we called them. Traffic data can now be used to create a map of human associations and more importantly, a map of human activity and intention. It is beyond our understanding as to why the EU Presidency and some select EU Member States insist on increasing the surveillance of traffic data even as this data becomes more and more sensitive, concomitant to a decreasing regard for civil liberties. (..) The European Parliament now faces a crucial decision. Is this the type of society we would like to live in? A society where all our actions are recorded, all of our interactions may be mapped, treating the use of communications infrastructures as criminal activity; just in case that it may be of use at some point in the future by countless agencies in innumerable countries around the world with minimal oversight and even weaker safeguards", questo il testo dell'appello di numerose ONG, riportato da C. JONES, B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, in *Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness – Paper*, 2013.

[33] Nel testo originario promosso dalla Commissione infatti veniva previsto un termine di tempo 'fisso' di conservazione di un anno per i metadati relativi alle telecomunicazioni, con l'unica eccezione dei dati derivanti da comunicazioni elettroniche che avessero usato solo o in misura maggiore Internet, che vedevano il periodo di conservazione ridotto a 6 mesi. Il testo della Commissione prevedeva anche un rimborso dei costi addizionali che i *providers* erano chiamati a sostenere per rispettare gli obblighi di conservazione imposti, rimborso poi scomparso nella versione finale del testo. Nella prima stesura, inoltre, tra gli scopi per i quali la conservazione e l'accesso erano consentiti, veniva anche inserito quello di *prevenzione* dei crimini gravi mentre, come si vedrà, nel dettato finale era stato omesso ogni riferimento alla prevenzione, rimanendo solo la possibilità di conservare i dati per scopi di investigazione e repressione dei crimini. In questo senso è interessante vedere che "the decision to limit the use of traffic data to 'serious crime offenses' and to exclude crime prevention can be traced to the Working party and the European Parliament. Both were extremely critical of the nearly unfettered rights of access that such broad purposes would confer upon police authorities", F. BIGNAMI, *Protecting privacy against the Police in the European Union: the Data Retention Directive*, in AA VV., *Melanges en l'honneur de Philippe Leger*, Editions Pedone, 2006, p. 119.

la Direttiva 2002/58/CE"[34] (c.d. *Data Retention Directive*, d'ora in avanti DRD), segnando così un "vero e proprio *revirement* securitario, passando da una politica volta ad incoraggiare la *data protection* (segnatamente con le dir. 95/46 e 2002/58) alla graduale legittimazione della *data retention*" [35]. Anche il Parlamento europeo, dunque, pur avendo espresso un parere di segno contrario in occasione della consultazione attinente alla adozione della previa Decisione Quadro, aveva votato infine a favore della DRD, forse condizionato dal differente contesto storico-politico e legislativo[36].

2.2. – La Data Retention Directive*: contenuto normativo ed elementi di criticità*

Riconoscendo "l'importanza dei dati relativi al traffico e dei dati relativi all'ubicazione per l'indagine, l'accertamento e il perseguimento dei reati, come dimostrato da lavori di ricerca e dall'esperienza pratica di diversi Stati membri" [37] e la conseguente necessità di garantire a livello europeo la conservazione dei dati generati o trattati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, la DRD sanciva l'onere in capo agli Stati Membri – anche quelli che non avevano ancora adottato nessuna normativa specifica in materia di *data rentention* utilizzando la deroga garantita dall'art. 15 della Direttiva *e-Privacy*[38] – di "adottare misure per garantire che i dati [relativi al traffico, all'ubicazione e quelli necessari per identificare l'abbonato o l'utente], qualora generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati (..), siano conservati conformemente alle disposizioni della presente direttiva" (art. 3, co. 1), allo scopo di garantirne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale (art. 1, co. 1). Non era stata quindi prevista una delimitazione dei soggetti i cui metadati dovevano essere sottoposti a conservazione, in conformità a quella scelta iniziale della Commissione di escludere forme di *data preservation*: "Cette conservation se fait, a priori, pour l'ensamble des citoyens sans distinction d'aucune sorte. Ni entre ceux qui font l'object d'enquetes judiciaires et ceux qui n'en font pas l'objet, ni entre ceux qui sont tenus

[34] Merita ricordare che tale Direttiva era stata anche denominata 'Direttiva Frattini', dal nome dell'allora Vice-Presidente della Commissione Europea e Commissario responsabile per il portafoglio Giustizia, Libertà e Sicurezza.

[35] E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, op. cit., p. 283. Anche Vedaschi e Lubello sottolineano come, dopo i drammatici attentati di Madrid e Londra, "the European policy focus has shifted subtly but enormous implications from one of data protection to data retention, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crimes, including terrorist offences. This radical change in policy, enacted in the relative blandness and dry language of a Directive, has been made largely without the media attention that the dramatic revelations of covert government surveillance have attracted in the USA. (..) This significant change in the EU approach, more oriented toward security, had already emerged with the increased EU attention on electronic comminications sector triggered by Directive 2002/58/EC", mettendo in luce così come la DRD abbia segnato una "transition from a fundamental concern with protection to the pragmatic desire for retention", A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy*, in *Tilburg Law Review*, 20, 2015, p. 19.

[36] "The Parliament, willing to prove its participation in anti-terrorism matters, finally swiftly adopted thee DRD, not least because the Council had insisted to adopt a Framework Decision in case the Parliament would refuse to agree to the draft Directive. Within three months of the Proposal the Parliament voted in favour and in February 2006 the DRD was finally adopted in the quickest legislative process in EU history until then", F. BOEHM, M. COLE, *Data Retention after the judgement of the Court of Justice of the European Union*, The Greens in the EP Working Paper, 2014, p. 12. È da evidenziare inoltre come la Direttiva rappresentasse una chiara risposta alla critica, mossa in occasione della proposta di Decisione Quadro, attinente la scelta della base giuridica.

[37] Considerando 11 della Direttiva 2006/24/CE.

[38] Tale articolo veniva infatti modificato dalla DRD stessa, mediante l'inserimento dell'art. 15, co. 1 bis: "Il paragrafo 1 non si applica ai dati la cui conservazione è specificamente prevista dalla Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, ai fini di cui all'articolo 1, paragrafo 1, di tale Direttiva".

d'un secret professionnel et ceux qui ne sont pas tenus d'une telle obligation"[39]. La memorizzazione imposta ai fornitori di servizi di telecomunicazione riguardava quindi tutti gli utenti e tutte le comunicazioni elettroniche aventi luogo nel territorio europeo, coinvolgenti cittadini europei o non, senza che dovesse sussistere alcun collegamento tra *data retention* e indagini in corso e senza richiedere un legittimo sospetto o un previo ordine da parte di un giudice, bensì solo nell'eventualità – che non poteva essere prevista anticipatamente nel momento della raccolta dei dati stessi – di successive possibili indagini riguardanti gravi reati.

I metadati che dovevano essere oggetto di conservazione erano stati espressamente indicati all'art. 5 e riguardavano sostanzialmente le informazioni volte a rintracciare la fonte di una comunicazione (numero telefonico o identificativo dell'utente di un servizio Internet o di posta elettronica), la destinazione di una comunicazione (ad esempio il numero del destinatario di una telefonata), la data, ora e durata della comunicazione (telefonata o accesso Internet), il tipo di comunicazione e l'attrezzatura utilizzata (comprensiva di codice IMEI cioè identificativo del cellulare impiegato dal chiamante) nonché i dati determinanti l'ubicazione delle apparecchiature di comunicazione mobile[40]. Risultavano invece completamente esclusi dalla conservazione i dati relativi al contenuto delle comunicazioni: sebben ciò di primo acchito possa sembrare una misura fortemente protettiva e in grado di limitare l'ingerenza nella sfera privata, facendo salva la confidenzialità delle comunicazioni, come già sottolineato, in realtà l'enorme quantità di metadati raccolti e trattenuti, se letta in maniera aggregata, è in grado di fornire notevoli ed ampie informazioni sulla vita degli utenti, sulle abitudini e sulle preferenze, anche senza alcun riferimento al contenuto. Inoltre alcuni autori[41] non hanno mancato di evidenziare come la distinzione tra metadati e contenuto apparisse sin dall'inizio non del tutto chiara e semplice da determinare, soprattutto con riferimento ai dati derivanti dall'utilizzo di Internet.

Quanto alla durata della conservazione, la direttiva stabiliva, non senza incontrare critiche e dopo un lungo dibattito[42], una forbice temporale indicata dai 6 mesi ai 2 anni, entro la quale i legislatori nazionali

---

[39] A. CASSART, J-F. HENROTTE, *L'invalidation de la directive 2006/24 sur la conservation des données de communication èlectronique oy la chronique d'une mort annoncée*, in *Jurisprudence de Liege, Mons et Bruxelles*, 20, 2014, p. 955.

[40] Per una completa e dettagliata analisi dei diversi metadati oggetto di conservazione ai sensi della DRD, si rimanda a L. FEILER, *The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection*, in *European journal of Law and Technology*, 3, 2010. Merita comunque sottolineare come numerose critiche fossero state mosse quanto alla vaghezza della terminologia utilizzata dal legislatore e alla mancanza di precise definizioni: "the wording of the definition [of electronic communications networks] can lead to a very broad interpretation of the term and thus to a vert broad group of providers that qualify as 'providers of public communications networks. (..) The directive missed the opportunity to define the term 'providers of publicly available communications services or public communication networks' in detail and avoid deviating interpretations among Member States. according to the recent data retention legislation in France the data retention obligations apply to Internet cafes, hotels, restaurants and generally to any person or organization providing Internet access, free or for a fee, as a main or side activity. In Italy Internet cafes are already obliged to seek an identification document from their customers and to further log the owner's name and the type of the identification document provided", E. KOSTA, P. VALCKE, *Retaining the data retention directive*, in *Computer Law & Security Report*, op. cit., p. 374.

[41] E. KOSTA, P. VALCKE, *Retaining the data retention directive*, in *Computer Law & Security Report*, op. cit. Le autrici riportano un esempio molto chiaro di come, mediante i soli metadati, sia possibile ricostruire preferenze ed interessi degli utenti: "When the user visits a 'search engine' his/her IP address is treated as traffic data. The same happens most commonly with the 'URL' of the requested search. If for example the user gives 'Google' the command to look for 'scuba diving', the URL: 'http://www.google.com/search?hl¼en&lr¼&q¼scubaþdiving&btnG¼Search' will be generated; an information that is automatically logged together with the time and the IP address of the user. When the URL that results from a search request is combined with the IP address of the user, the aforementioned information turns into an information 'relating to an identified or identifiable natural person' and thus to personal data", p. 375.

[42] Tale scelta temporale aveva incontrato la resistenza del GEPD che non riteneva i dati presentati a sostegno di tale decisione e valutati dalle Istituzioni europee, anche nell'*Impact Assessment*, come sufficienti a dimostrare la necessità di una conservazione protratta per una durata superiore ad un anno: "Il fatto che in alcuni casi la

potevano liberamente muoversi nel determinare il periodo di *data retention* ritenuto maggiormente opportuno e necessario[43].

Era invece lasciata ampia discrezionalità ad ogni Stato membro quanto alla definizione delle "procedure da seguire e le condizioni da rispettare per aver accesso ai dati conservati, in conformità dei criteri di necessità e di proporzionalità", che "sono definite da ogni Stato membro nella legislazione nazionale, con riserva delle disposizioni in materia del diritto dell'Unione europea o del diritto pubblico internazionale e in particolare della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo" (art. 4).

Ecco che dalla ricostruzione delle disposizioni maggiormente rilevanti della direttiva, che risultava comunque piuttosto breve e succinta, emergono alcune problematiche ed osservazioni che troveranno poi ampio spazio nel dibattito legislativo apertosi a livello degli Stati membri ma di quello anche giurisprudenziale, che aveva avuto luogo sia nelle Corti nazionali che in seno alla CGUE. Innanzitutto nella normativa analizzata non era presente alcun riferimento ad una definizione di 'reati gravi' per la repressione dei quali i metadati potevano essere conservati ed utilizzati. Ciò accresceva dunque il rischio che il concetto di 'gravità' venisse interpretato in maniera eccessivamente ampia da parte degli Stati membri, benché il Consiglio, nel proprio documento 5777/06 ADD 1 (1 febbraio 2006) avesse suggerito di considerare la lista di reati presenti all'art. 2, co. 2 della Decisione Quadro sul Mandato di Arresto Europeo[44]. Veniva inoltre lasciata, come si è visto, discrezionalità ai legislatori nazionali quanto alla determinazione del periodo di *data retention* e alla regolamentazione dell'accesso, interamente demandata agli Stati membri. Mancava inoltre qualsiasi indicazione relativa alle autorità nazionali che dovevano essere deputate all'accesso ai metadati e non era dunque prevista alcuna limitazione alle sole autorità di *law enforcement*: è interessante su questo fronte anticipare come, nelle normative nazionali di attuazione della DRD, ben 14 dei 28 Stati membri avessero incluso nella definizione di 'autorità

---

disponibilità di dati relativi al traffico e/o all'ubicazione abbia contribuito a individuare l'autore di un reato non significa automaticamente che tali dati siano necessari (in generale) come strumento per le forze dell'ordine. Le cifre non possono tuttavia essere ignorate. Esse rappresentano almeno un tentativo serio di dimostrare la necessità della conservazione. Inoltre, le cifre indicano chiaramente che un periodo di conservazione superiore a un anno non è necessario se si considerano le attuali prassi delle forze dell'ordine", GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di Direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della Direttiva 2002/58/CE*, 26 settembre 2005, par. 17. Contrariamente a questa posizione, invece, si era pronunciata la Commissione nell'*Extended Impact Assessment* più volte richiamato: "The Interpol High Tech Crime Working Group has indicated in its contribution to the debate that a minimum period of one year is necessary. Other contributions from law enforcement authorities indicate that most of the requests for traffic data will take place within the first few months after the crime under investigation has been committed. One UK expert indicated that for volume crime, 95% of case demand is satisfied within 3 months. He went on to state, however, that for serious and organized crime, 85% of cases require data between 6 and 24 months and for murder and terrorist cases there are examples of requirements for data up to 5 years old. Experts from other countries have confirmed this", p. 17.

[43] Veniva comunque prevista all'art. 12, co. 3 della DRD la possibilità di prorogare tali termini qualora "uno Stato membro si trovi ad affrontare circostanze particolari che giustificano una proroga, per un periodo limitato, del periodo massimo di conservazione di cui all'art. 6", notificando tale decisione alla Commissione e informando gli altri Stati membri, motivandone l'adozione. È interessante rimarcare come anche su questo punto il dibattito tra le Istituzioni europee nel corso del procedimento legislativo fosse stato ampio: mentre la Commissione aveva inizialmente proposto un termine fisso di 12 mesi di conservazione, ridotto a 6 mesi per i dati legati all'uso di internet, il Parlamento europeo aveva richiesto l'abbassamento di tale periodo a 3 mesi, con una possibile estensione massima di 6 mesi. Il Consiglio propendeva invece per l'opzione di una forbice temporale che lasciasse maggiore discrezionalità agli Stati membri: a seguito di negoziazioni tra le Istituzioni europee, la scelta finale fu proprio quella di introdurre un periodo di conservazione tra 6 mesi e 2 anni; questa decisione peraltro risultava in linea di continuità con quanto era stato proposto da alcuni Stati membri nella bozza di Decisione Quadro sopra studiata, che prevedeva però un intervallo temporale ben più esteso, da 1 anno a 3 anni.

[44] Decisione quadro del Consiglio 2002/584/GAI, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri.

competenti' anche i servizi di intelligence nazionali[45]. Quanto al profilo della sicurezza dei dati conservati, pur avendo imposto in capo agli operatori di servizi di telecomunicazione l'adozione di adeguate misure volte a garantire la protezione dei dati, restava fortemente discrezionale il livello di tutela e di misure poste in essere da ciascun *service provider*, con più o meno elevati rischi di violazione della privacy, abuso o accesso non autorizzato ai metadati memorizzati. Era assente, infine, la previsione di un obbligo per gli operatori di provvedere alla conservazione dei dati unicamente all'interno del territorio europeo, con la conseguenza che i database di raccolta avrebbero ben potuto essere collocati al di fuori dell'UE e dunque risultare finanche accessibili da autorità nazionali extra-europee sulla base delle discipline fissate dai diversi ordinamenti statali, esponendo in quel caso i metadati raccolti nel territorio europeo a rischi ulteriori di accesso e utilizzo incontrollati.

Ovviamente le carenze sopra individuate così come il margine di discrezionalità lasciato agli Stati membri su alcuni punti di centrale importanza e di grande delicatezza, avevano destato non poche preoccupazioni, nella consapevolezza che "how Member States interpret and implement these aspects of the Directive will significantly affect how broadly access can be obtained to retained data"[46]. Oltre agli impatti sul fronte della maggiore o minore ingerenza nella sfera privata che le diverse disposizioni normative potevano determinare, le difformità nella scelta del periodo di conservazione o della possibilità o meno di rimborsare ai *service providers* i costi sostenuti per la conservazione imposta – aspetto che veniva lasciato alla discrezionalità dei legislatori nazionali, diversamente dalla proposta originaria della Commissione che prevedeva l'obbligo di rimborso in capo a tutti gli Stati membri – rischiavano in conclusione di condurre a differenze anche significative tra le diverse discipline normative nazionali, con la conseguenza di impedire il raggiungimento di quella armonizzazione che era stata posta alla base della DRD stessa, volta ad eliminare gli ostacoli al mercato interno e le possibili distorsioni concorrenziali derivanti dalla presenza di legislazioni fortemente disomogenee.

Ulteriore aspetto critico rimaneva poi quello della base giuridica scelta: pur avendo quale spiccato obiettivo quello di garantire l'efficacia delle indagini e dell'operato delle autorità di *law enforcement* rispetto alla repressione di crimini gravi, come emerge anche dai Considerando della direttiva stessa, la base giuridica era stata individuata, come già anticipato, nel Primo Pilastro ed in particolare nell'art. 95 TCE (attualmente art. 114 TFUE) che, come noto, attribuiva al livello sovranazionale il potere di adottare "le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno". Individuando nella armonizzazione degli obblighi dei fornitori di servizi di telecomunicazione la finalità primaria, con la conseguente esclusione, come invece era stato in precedenza proposto da alcuni Stati membri, della possibilità di adottare una misura normativa sulla base del Titolo VI TUE e dunque sul Terzo Pilastro, veniva anche rifiutata la possibilità di regolare a livello europeo l'accesso ai dati conservati, disciplina che sarebbe rientrata invece nell'ambito della cooperazione nei settori della giustizia e degli affari interni. Nel Considerando 25 della DRD veniva infatti specificato come "Le questioni relative all'accesso ai dati conservati ai sensi della presente direttiva da parte di autorità nazionali per attività di cui all'articolo 3, paragrafo 2, primo trattino, della Direttiva 95/46/CE, ricadono al di fuori del campo di applicazione del diritto comunitario. Esse tuttavia

[45] Come sottolineato da C. JONES, B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, SELICE Project D2.4, 2013, citato da A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy*, in *Tilburg Law Review*, op. cit.

[46] M. TAYLOR, *The EU Data Retention Directive*, in *Computer Law & Security Report*, 22, 2006. L'autore sottolinea come "in contrast to the proposal, the Directive only achieves harmonisation of a minimum retention period for data, namely six months. In practice, the extent to which data are retained in excess of this minimum may still vary from Member State to Member State, subject only to a maximum retention period of two years. Thus, service providers will not benefit from a consistent regime across the EU. They will still be required to implement data retention arrangements in all Member States in which they operate, but may need to retain some data longer than others and to delate or destroy some data earlier than others", p. 310.

possono formare oggetto di legislazione nazionale o di azione ai sensi del titolo VI del trattato sull'Unione europea. Tali normative o azioni devono rispettare pienamente i diritti fondamentali che risultano dalle tradizioni costituzionali comuni degli Stati membri e che sono garantiti dalla CEDU. L'articolo 8 della CEDU, nell'interpretazione della Corte europea dei diritti dell'uomo, prescrive che l'ingerenza di un'autorità pubblica nel diritto alla riservatezza deve rispondere a criteri di necessità e proporzionalità e deve quindi perseguire scopi specifici, espliciti e legittimi nonché essere esercitata in modo adeguato, pertinente e non eccessivo rispetto allo scopo ricercato".

La scelta della base giuridica non risultava essere così pacificamente accettata ed accolta, ed era anzi sin da subito risultata oggetto di discussione[47]: il GEPD sul punto aveva manifestato forti dubbi, sottolineando come la finalità ultima della DRD fosse in realtà da individuarsi nel rendere disponibili i metadati per scopi securitari con il risultato che, anche a causa della base giuridica scelta, la delicata regolamentazione dell'accesso veniva lasciata alla determinazione discrezionale degli Stati membri, essendo le disposizioni stabilite dal testo normativo europeo estremamente vaghe ed ampie. A parere del Garante Europeo quindi "l'accesso e l'ulteriore uso [dovrebbero] essere regolamentati esplicitamente dalla Direttiva e sono necessarie garanzie aggiuntive"[48]; anche il Gruppo di Lavoro Art. 29, nel già richiamato Parere 4/2005, aveva ribadito la grave carenza di tutele nella fase di accesso ai dati da parte delle autorità di *law enforcement*, ritenendo fondamentale la previsione obbligatoria quantomeno di un preventivo vaglio giudiziario: "L'accesso ai dati dovrebbe, in linea di principio, essere debitamente autorizzato, caso per caso, da un'autorità giudiziaria, fatti salvi i paesi in cui la legge autorizza una possibilità specifica di accesso, ed essere soggetto a controllo indipendente. Se del caso, le autorizzazioni dovrebbero precisare i dati richiesti per gli specifici casi in questione". I dubbi sino ad ora delineati circa la correttezza della base giuridica e dunque i limiti e le differenze nella disciplina della conservazione o dell'accesso ai dati saranno gli elementi determinanti che, come si vedrà nel Capitolo II, porteranno alla pronuncia della CGUE sulla validità della DRD.

Più in generale, tutte le criticità sin qui messe in rilievo e che hanno caratterizzato la DRD dalla sua origine, si manifesteranno con ancor più forza e rilevanza sia nella attuazione della direttiva da parte dei singoli Stati membri, sia nelle decisioni delle Corti nazionali e nel successivo intervento della CGUE. Alla base del dibattito politico e giurisprudenziale vi è sempre, infatti, la difficile individuazione del corretto punto di equilibrio – solo presunto e irraggiungibile laddove si legga la materia in chiave di *trade-off* – tra l'imposizione di oneri in capo agli operatori dei servizi di telecomunicazione, la tutela dei diritti alla riservatezza e alla protezione dei dati, nonché la garanzia di un elevato livello di sicurezza e di strumenti efficaci a disposizione delle autorità di *law enforcement*[49]. Fin dall'inizio, quindi, la proporzionalità e necessità della *data retention* generalizzata, così come concepita dal legislatore europeo, nonché la sua conformità alla Carta di Nizza sono risultate tutt'altro che incontestate e la ricostruzione del dibattito sorto tra le Istituzioni europee, la società civile e le autorità garanti della protezione dei dati risulta premessa necessaria per cogliere appieno le sfide giuridiche legate alla

[47] Contrariamente a quanto sostenuto da parte della dottrina e da alcune autorità europee, taluni autori si sono invece espressi positivamente quanto alla scelta della base giuridica: "The decision to go forward under the First Pillar was salutary. Giving the European Parliament co-decision powers meant that the Council's decision to amass huge amounts of personal data concerning ordinary citizens was more visible and was debated more vigorously than it otherwise would have been (..) In other words, involving the EP had the great merit of putting data retention and its privacy implications in the public eye", F. BIGNAMI, *Protecting privacy against the Police in the European Union: the Data Retention Directive*, op. cit., p. 122.

[48] GEPD, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di Direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della Direttiva 2002/58/CE*, op. cit.

[49] È la stessa Commissione a parlare di contrasto "between the costs for industry and the MSs as well as a limitation of privacy of individuals, against a society which is more secure through more effective law enforcement action in preventing and combating serious forms of crime such as organized crime and terrorism", COMMISSIONE EUROPEA, *Extended Impact Assessment*, op. cit., p. 25.

disciplina della conservazione dei dati e, di riflesso, a quella più ampia necessità di rispondere alle serie esigenze securitarie senza rinunciare al riconoscimento e alla tutela dei diritti fondamentali.

CAPITOLO II

LA LUNGA E COMPLESSA *DATA RETENTION SAGA*, DALLA SENTENZA *DIGITAL RIGHTS IRELAND* A *TELE2 SVERIGE & WATSON*: L'INTERVENTO DELLA CORTE DI GIUSTIZIA DELL'UE E IL DIALOGO CON LE CORTI NAZIONALI

1. – La disciplina della conservazione dei metadati nell'Unione europea all'indomani della Direttiva 2006/24/CE: le reazioni degli Stati membri, tra interventi legislativi e decisioni delle Corti nazionali

La Direttiva 2006/24/CE, meglio nota come DRD e ampiamente analizzata nel precedente Capitolo, attribuiva agli Stati membri il compito di adottare normative di trasposizione della disciplina europea entro il 15 settembre 2007, mentre con riferimento alla sola conservazione dei dati derivanti dall'utilizzo di Internet veniva data la possibilità, accolta da 16 Stati membri, di posporre tale adempimento al 15 marzo 2009. L'esecuzione di tale obbligo aveva tuttavia comportato, sin dall'inizio, notevoli problematiche e accese discussioni a livello nazionale: le perplessità e preoccupazioni, già espresse da GEPD, Gruppo di Lavoro Art. 29, oltre che da numerose ONG, con riferimento alla proporzionalità e necessità della *data retention* nonché alla validità della Direttiva stessa, sono ben presto emerse con forza anche nel dibattito politico e dottrinario dei singoli Stati membri, giungendo, in taluni casi, anche dinnanzi alle Corti nazionali.

Alcuni legislatori nazionali avevano infatti riscontrato difficoltà nell'inserire l'obbligo di conservazione generalizzata dei metadati (c.d. *bulk data retention*) sancito dalla DRD all'interno del proprio ordinamento statale: tale previsione avrebbe comportato non trascurabili problematiche in termini di compatibilità di un simile regime di conservazione dei dati rispetto ai diritti e principi contenuti nelle Carte costituzioni nazionali, a conferma della natura controversa della Direttiva stessa e delle scelte da essa operate. Pur non volendo in questa sede esaminare nel dettaglio tutte le complesse quanto rilevanti questioni sorte in numerosi Stati membri[1], nondimeno pare di estremo interesse fornire almeno un quadro generale delle reazioni nazionali dinnanzi alla sfida della trasposizione della DRD, ponendo particolare attenzione ad alcune pronunce delle Corti costituzionali. Questi casi giurisprudenziali ben possono essere visti come precursori del più ampio intervento successivo della Corte di Giustizia dell'UE: sebbene i giudici nazionali, ancora restii al dialogo con i giudici di

[1] Per una ampia e dettagliata analisi delle normative di recepimento della DRD a livello nazionale e della giurisprudenza in materia, si rimanda a: T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, in *European Current Law*, 1, 2012, p. xi-xxiii; E. KOSTA, *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, in *SCRPITed*, 3, 2013, p. 339-363; J. DURICA, *Directive on the retention of data on electronic communication in the rulings of the Constitutional Courts of EU Member States and efforts for its renewed implementation*, in *The Lawyer Quarterly*, 2, 2013, p. 143-158; L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, in *German Law Journal*, 6, 2015, p. 1727 ss.; L. CURICCIATI, *Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della Data Retention Directive*, in *Democrazia e Sicurezza*, 2, 2017, p. 89 ss. ma in particolare, per quanto qui interessa, pp. 109-117.

Lussemburgo, non abbiano toccato la questione della validità della Direttiva in sé, decidendo di non rinviare tale valutazione alla CGUE bensì concentrandosi solo sulle disposizioni interne attuative della DRD, essi hanno tuttavia sviluppato considerazioni rilevanti quanto alla proporzionalità e necessità della *data retention* generalizzata stessa; tali posizioni non possono che assumere grande importanza nella presente ricostruzione poiché consentono di giungere ad una piena comprensione delle criticità legate alla disciplina della conservazione dei dati per scopi securitari e al dibattito che ha preceduto ed aperto la strada alla articolata giurisprudenza europea.

1.1. – Le decisioni della Corte costituzionale romena e del Tribunale costituzionale federale tedesco in materia di data retention*: prime valutazioni sulla costituzionalità delle normative nazionali di trasposizione della DRD*

Insieme alle sentenze delle Corti di Bulgaria (sentenza della *Varhoven administrativen sad*, la Corte suprema amministrativa, del 11 dicembre 2008), Cipro (sentenza della *Ανώτατο Δικαστήριο της Κυπριακής Δημοκρατίας*, Corte suprema, del 1 febbraio 2011) e Repubblica Ceca (sentenza della *Ústavní soud České republiky*, Corte costituzionale, del 22 marzo 2011), che si sono pronunciate nel biennio 2008-2010 sulla compatibilità con l'ordinamento nazionale delle leggi di trasposizione della Direttiva 2006/24/CE, dichiarandone l'invalidità parziale o totale, le decisioni nazionali in materia maggiormente note e significative sono senza dubbio quelle emanate dalla *Curtea Constituţională a României* (Corte costituzionale romena) il 8 ottobre 2009[2] e dal *Bundesverfassungsgerich* (il Tribunale costituzionale federale tedesco) del 2 marzo 2010[3].

La Corte costituzionale romena aveva dichiarato l'illegittimità costituzionale della normativa nazionale sulla conservazione dei dati (Legge n. 298/2008), ritenuta in violazione dell'art. 26 della Costituzione, posto a tutela del diritto alla vita privata, nonché dell'art. 8 della Convenzione EDU[4]. Facendo ampio e continuo riferimento alla giurisprudenza dei giudici di Strasburgo[5], la Corte romena aveva considerato la legge di trasposizione della DRD eccessivamente vaga quanto alle finalità di conservazione e accesso ai dati (genericamente indicate con il termine 'minacce alla sicurezza nazionale') e carente sotto il profilo delle salvaguardie poste in essere. Ciò che risulta ancor più interessante però è la decisa dichiarazione di incompatibilità con il diritto alla riservatezza di una forma di conservazione generalizzata, obbligatoria e permanente[6]: "the Court held that the data retention

[2] Decisione n. 1258, 8 ottobre 2009, 23 novembre 2009. Per la presente analisi è stata impiegata una traduzione inglese della sentenza disponibile sul sito www.legi-internet.ro, all'indirizzo: http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf. Si è inoltre fatto ampiamente riferimento alla traduzione effettuata da Murphy e alla sua analisi in C. C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, in *Common Market Law Review*, 3, 2010, pp. 933-941.

[3] BVerfG, Vorratsdatenspeicherung, BvR 256/08, 2 marzo 2010. L'analisi di tale pronuncia è stata svolta sulla base della traduzione di A. DI MARTINO, *Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, in *Giurisprudenza costituzionale*, 5, 2010, p. 4059.

[4] Il caso giunto dinnanzi alla Corte costituzionale era stato promosso da una ONG romena, la Civil Society Commissariat, dinnanzi al Tribunale di Bucharest: citando in causa l'operatore di telecomunicazione che, sulla base della normativa romena in materia di *data retention*, conservava i metadati relativi alle comunicazioni degli attivisti della ONG, quest'ultima ha poi sollevato una questione di illegittimità costituzionale quanto alla compatibilità della Legge n. 298/2008 con la Costituzioni romena.

[5] In particolare, viene ampiamente richiamata la sentenza *Klass v Germania*, ricorso n. 5029/71, deciso il 6 settembre 1978. Per una ricostruzione della casistica e della posizione della Corte EDU in materia di *data retention* e di altre forme di sorveglianza massiva, si rimanda al Capitolo V.

[6] Sul punto si leggano C. JONES, B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, in *Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness – Paper*, 2013, p. 22, nonché specificamente: C. C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, op. cit. In quest'ultimo contributo viene sottolineato come lo stesso

legislation reverses the presumption that the rights to privacy and free expression are only subject to limited interference as all electronic communication is targeted for surveillance. (..) The scheme under Law 298/2008 affected all communications users, rendering the entire public as potential suspects. (..) By applying the data retention to all electronic communications users, the rights in question – to privacy and freedom of expression – become 'theoretical and illusory' and the legislation may overturn the presumption of innocence"[7]. Diviene chiaro dunque come la posizione della Corte costituzionale romena, pur senza mai – piuttosto sorprendentemente – citare la DRD, sia risultata in una forte critica della conservazione generalizzata *per se*, della sua necessità e proporzionalità in una società democratica: i giudici si erano così spinti oltre il mero vaglio della normativa nazionale di trasposizione della disciplina europea, condannando invece, direttamente alle sue fondamenta, quello che veniva considerato un sistema di sorveglianza indiscriminata fortemente invasivo della vita privata della generalità dei cittadini, tramutati in potenziali sospetti. Se la Corte si fosse limitata a considerare illegittimo l'impiego da parte del legislatore romeno di termini eccessivamente vaghi o l'assenza di idonee tutele e garanzie, la pronuncia avrebbe unicamente riguardato le scelte nazionali di attuazione della DRD; condannando però più ampiamente la *data retention* stessa così come imposta dalla disciplina europea – seppure, come si è detto, indirettamente e senza nominare la Direttiva –, i giudici ponevano il Parlamento nella difficile condizione di non poter approvare una normativa nazionale che prevedesse forme di conservazione generalizzata: essa, pur conforme a quanto richiesto a livello dell'Unione europea, non poteva che essere, secondo la lettura della Corte romena, in contrasto con la Costituzione nazionale e con la Convenzione EDU[8].

Anche il Tribunale federale tedesco si era pronunciato, a distanza di un anno dalla decisione romena, sulla normativa nazionale in materia di conservazione dei dati[9], ritenendo le disposizioni in essa contenute non conformi all'art. 10, co. 1 della *Grundgesetz* (GG), posto a tutela dei diritti alla riservatezza e alla segretezza delle comunicazioni, diritti che – merita ricordarlo – si estendono, sulla base della consolidata giurisprudenza tedesca in materia, non solo al contenuto delle comunicazioni bensì anche ai metadati. La controversia che aveva dato origine all'intervento del Tribunale era stata

---

legislatore romeno avesse riscontrato e dichiarato notevoli difficoltà e dubbi già nella fase di predisposizione della normativa di trasposizione della DRD: "despite describing the implementing law as a '100% translation' of the Directive, the State Secretary Constantin Teodorescu stated that the requirements were 'not easy to fulfil and they leave huge gaps'", p. 935.

[7] C. C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, op. cit., p. 936.

[8] Come acutamente osservato da Murphy, neppure una modifica della Costituzione nazionale avrebbe potuto rendere l'attuazione di forme di conservazione generalizzata conforme e compatibile con i diritti fondamentali: "the Court strongest criticism, relating to the general scheme of the legislation, cannot be addressed without amending either the Directive or Romanian constitutional law. In fact, given that the Romanian Constitutional Court invokes the ECHR in addition to the domestic Constitution, an amendment to the latter may not suffice to protect any implementing law", C. C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, op. cit., p. 940.

[9] Il Telekommunikationsgesetz (TKG), in conformità alla DRD, prevedeva l'obbligo per gli operatori del settore delle telecomunicazioni di conservare i metadati di tutti gli utenti per un periodo di 6 mesi (Section 113a), consentendo poi l'accesso ed utilizzo di tali informazioni da parte delle autorità di *law enforcement*, senza però limitare tale possibilità alla repressione di reati gravi e senza richiedere – se non in taluni casi – un previo controllo da parte di un'autorità giudiziaria o un dovere di notifica ai cittadini interessati dall'accesso ai propri metadati. Anche in questo caso, i giudici costituzionali tedeschi hanno sottolineato che "la verifica di legittimità costituzionale riguarda non le disposizioni della Direttiva europea, ma le soluzioni legislative adottate dal legislatore tedesco per raggiungere gli scopi prefissati dall'Unione. La questione della prevalenza del diritto comunitario e della sua eventuale incidenza sui diritti fondamentali non è stata, dunque, in discussione o, almeno, non direttamente. La Direttiva, infatti, conferisce agli Stati un'ampia discrezionalità e le sue previsioni sono limitate essenzialmente all'obbligo di conservazione dei dati, non prevedendo la disciplina sull'accesso e l'utilizzo degli stessi da parte delle autorità statali", R. FLOR, *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constitutionala*, in *Cassazione Penale*, 5, 2011, p. 1953.

promossa da una nota ONG attiva proprio nell'ambito specifico della tutela dei diritti fondamentali avverso strumenti di conservazione dei dati, la 'Working Group on Data Retention". Quest'ultima era poi stata sostenuta anche da ben 34.000 cittadini[10]: ciò consente di comprendere la sensibilità e attenzione sempre maggiore posta dalla società civile rispetto a temi complessi e delicati quali la tutela della riservatezza dinnanzi all'ingerenza di autorità pubbliche. Ebbene, venendo all'analisi della decisione, pur evidenziando che regimi di *data retention* generalizzata possono "ingenerare un sentimento diffuso e minaccioso dell'essere osservati, che può pregiudicare in molti settori un libero esercizio dei diritti fondamentali" (Par. 212), il Tribunale tedesco non giungeva, diversamente dalla Corte romena, a condannare l'utilizzo e la natura stessa di sistemi di *data retention* generalizzata. La conservazione in blocco non veniva pertanto considerata di per sé in contrasto con l'art. 10 GG, purché il ricorso a tali strumenti superasse il vaglio di proporzionalità e venissero quindi previste chiare e precise salvaguardie e condizioni relative alle operazioni di raccolta e utilizzo dei dati[11]. Ciò che veniva ritenuto contrastante rispetto alla legge fondamentale, pertanto, era il mancato rispetto del principio di proporzionalità riscontrato in diversi punti della disciplina normativa nazionale, che non risultava circoscrivere adeguatamente e disporre idonee garanzie avverso l'ingerenza nella sfera privata. Veniva infatti criticato il periodo di memorizzazione che, per considerarsi necessario e proporzionato, doveva prevedere una estensione massima di 6 mesi, secondo il ragionamento dei giudici tedeschi; ma anche l'assenza di idonee tutele nella fase di accesso ai dati, che doveva avvenire solo in presenza di un sospetto di reato grave o di un pericolo concreto per la vita o per la sicurezza; a ciò si aggiungevano la mancanza di un obbligo di notificazione o informazione al soggetto interessato nonché la carenza di solide salvaguardie tecnico-informatiche[12]. Dunque, pur affermando la costituzionalità di forme

[10] Merita solo preliminarmente rilevare come la Grundgesetz preveda all'articolo 93(4a) lo strumento del ricorso diretto individuale dinnanzi al Tribunale costituzionale federale (Verfassungsbeschwerde), per finalità di tutela dei diritti fondamentali.

[11] Così afferma il Tribunale: "Una conservazione preventiva, senza un motivo concreto, dei dati di traffico telematico da parte dei gestori privati dei servizi, come prevista dalla Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, non è, in quanto tale, incompatibile con l'art. 10 GG; non rileva pertanto un eventuale primato di questa Direttiva. Il principio di proporzionalità richiede che la conformazione legislativa di siffatta conservazione dei dati tenga conto della particolare intensità dell'interferenza nei diritti fondamentali, conseguente alla conservazione. Sono necessarie regole complete e chiare per quanto concerne la sicurezza dei dati, il loro utilizzo, la trasparenza e la tutela dei diritti (...). Con riguardo alla sicurezza dei dati, occorrono regole che prospettino in modo chiaro e vincolante uno standard di sicurezza particolarmente elevato. E, tuttavia, va assicurato per via legislativa che tale standard si orienti secondo lo stadio raggiunto dalla discussione degli esperti, tenendo conto delle nuove conoscenze e dei punti di vista provvisoriamente acquisiti, e che non venga posto sotto la riserva di un libero bilanciamento con generali esigenze economiche. Il prelievo e l'immediata utilizzazione dei dati sono proporzionati soltanto qualora servano ai compiti, importanti e prevalenti, della tutela dei diritti. Nell'ambito della repressione penale, ciò presuppone il sospetto di un reato grave, fondato su elementi di fatto determinati. Con riguardo alla prevenzione dai pericoli (Gefahrenabwehr) e all'adempimento delle funzioni dei servizi segreti, essi [prelievo e utilizzazione] possono essere ammessi soltanto in presenza di «punti di appoggio» effettivi, relativi ad un pericolo concreto per il corpo, la vita o la libertà di una persona, ovvero per l'esistenza o la sicurezza del Bund o di un Land", traduzione di A. DI MARTINO, *Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, op. cit., p. 4059.

[12] Pare utile ed interessante contestualizzare comunque questo intervento del Tribunale costituzionale tedesco: come viene rilevato da Di Martino, la lettura di questa pronuncia non può essere "disgiunta da tutte quelle che, negli ultimi sei anni, hanno ribadito l'irriducibilità delle istanze di libertà dinanzi all'emergenza terroristica. Benché sia chiaro l'intento, da parte del Tribunale costituzionale federale, di contrastare politiche troppo disinvolte del legislatore in attuazione dei compiti statali di sicurezza, non va dimenticato che il terreno, per queste sentenze era stato preparato da un'ampia riflessione dottrinale sul c.d. Stato di prevenzione, sviluppatasi almeno un decennio prima degli attentati dell'11 settembre 2001". Per un approfondimento su questo punto si rimanda a A. DI MARTINO, *Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, op. cit., p. 4063 e ss.

generalizzate di conservazione dei dati, i giudici tedeschi ne limitavano il ricorso solo in circostanze particolari e nel pieno rispetto del principio di proporzionalità[13].

Le pronunce sopra esaminate evidenziano una sostanziale differenza negli approcci adottati dalle due Corti nazionali: quella tedesca ha concentrato la propria attenzione – anche per non rinviare la questione dinnanzi alla CGUE – unicamente sulla normativa interna ed in particolare sulla disciplina dell'accesso ai dati, senza mettere in discussione la compatibilità con i diritti fondamentali del regime di conservazione dei dati generalizzato inteso nella sua stessa natura; tale approccio ha portato i giudici tedeschi a focalizzarsi sulle salvaguardie e sulle limitazioni da porre in essere al fine di rendere la *data retention* proporzionata e limitata a quanto necessario e, pertanto, legittima[14]. La Corte romena invece ha considerato direttamente la questione della costituzionalità dello strumento della conservazione generalizzata, ritenendolo, come si è visto, *per se* in contrasto con le prerogative garantite dalla Carta costituzionale nazionale. In altre parole, mentre la Corte tedesca affermava "that the judgement was simply related to the extent of state discretion implied in the implementation of the Directive", giungendo solo a sospendere la normativa interna in attesa di appropriati emendamenti da parte del Parlamento nazionale, la Corte romena "rejected altogether the obligation of data rentention. Thus, the Romanian Constitutional Court's attack was not limited to the relevant implementation process but to the Europeanisation of the system of data retention"[15].

---

[13] "The Court divided the need for proportionality as arising from the constitutional court into the following four criteria: proportional security standards, proportional purpose limitation, transparency, judicial control and effective legal remedies. The Court found that the challenged provisions guarantee neither adequate data security nor an adequate restriction of the purpose of use of the data. Nor do they in every respect satisfy the constitutional requirements of transparency and legal protection. The provision is therefore as a whole unconstitutional and void", E. KOSTA, *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, op. cit., p. 351; Per un ampio commento a tale pronuncia si rimanda anche a: C. DE SIMONE, *Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU Data Retention Directive*, in *German Law Journal*, 11, 2010; K. DE VRIES, R. BELLANOVA, P. DE HERT, S. GUTWIRTH, *The German Constitutional Court judgement on data retention: proportionality overrides unlimited surveillance (doesn't it?)*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, R. LEENS (a cura di), *Computers, privacy and data protection: an element of choice*, Springer, 2011, pp. 3-23; D. WESTPHAL, *German federal constitutional Court delivers roadmap for national data retention laws – without transferal to ECJ*, in *Vienna Journal on International Constitutional Law*, 5, 2011.

[14] "The reluctance of the national Courts to criticize data retention should not be interpreted as accepting its compatibility with fundamental rights and the right to privacy in particular. Most of those Courts did not examine the compatibility of the DRD itself with their Constitutions and with fundamental rights because by their own assessment their competence to do so was limited by the supremacy of EU law in this area", E. KOSTA, *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, op. cit., p. 361. Sul punto Konstadinides ha affermato: "The BVerfG distinguished between the internal market aspect of the Directive (data retention by service providers) and its criminal aspects (access to data and their use and exchange between law enforcement authorities). While it attributed competence to regulate the former to the EU, it characterized the latter (in accordance to arts. 7 and 13 of Directive 2006/24) as an issue that was intimate to the competence of the Member States. This orthodox analysis of competence delimitation by the BVefrG saved it from having to refer the matter to the ECJ", T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, op. cit., p. XX. Una visione, quella della Corte tedesca, che caratterizza anche il ragionamento seguito dalla CGUE nella sentenza, che si analizzerà a breve e di poco precedente rispetto a quella tedesca, 25 febbraio 2009, C-301/06, *Irlanda c. Parlamento europeo e Consiglio*, relativa alla base giuridica della DRD. Il BVerfG dunque provvede ad una analisi dettagliata delle salvaguardie e, come farà in seguito anche la CGUE, propone "detailed guidelines for legislation, affirming the need of a proportionality test which requires the respect of the following four criteria: proportionality data security standards; proportional purpose limitation; transparency; judicial control and effective legal remedies", A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy. A European perspective*, in *Tilburg Law Review*, 20, 2015, p. 26.

[15] T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, op. cit., p. XX.

Al di là di questa pur rilevante diversità, ciò che il dibattito venutosi a creare all'interno degli Stati membri e, in particolare, ciò che tutte le decisioni delle Corti nazionali avevano sottolineato era l'alto livello di rischio per i diritti fondamentali rappresentato da un regime quale quello di *data retention* generalizzata e massiva proposto e imposto a livello europeo: "nel susseguirsi di pronunce [dei giudici nazionali] la complessa natura della disciplina era stata dunque messa in forte discussione. Si è avvertita così l'esigenza di ridefinire i valori in gioco, non limitandosi a considerare i meri interessi economici della prima ora, ma estendendo l'analisi anche ai profili fino a quel momento trascurati, in primis la tutela dei diritti"[16]. Il comune denominatore di questa prima ricca giurisprudenza nazionale è da individuarsi pertanto nell'ampio riconoscimento dell'importanza dei diritti alla privacy e alla protezione dei dati, che non potevano essere considerati sempre remissivi di fronte al pur legittimo compito dello Stato di garantire la sicurezza. Se le esigenze securitarie possono giustificare una compressione dei diritti fondamentali, misure di sorveglianza massiva e totalizzante quali quelle derivanti da una conservazione generalizzata dei metadati debbono essere attentamente e scrupolosamente elaborate dai legislatori nazionali e vagliate dalle Corti alla luce del principio di proporzionalità.

D'altra parte, però, non può non osservarsi come nel mancato rinvio alla CGUE, che avverrà solo dopo alcuni anni da parte di Austria e Irlanda, sia individuabile un atteggiamento poco cooperativo da parte delle Corti nazionali, ancora riluttanti a rinviare le questioni ad esse sottoposte ai giudici di Lussemburgo, anche in casi come quello in esame, nei quali l'impatto e la rilevanza della normativa europea erano chiaramente e fortemente incidenti e determinanti sulla disciplina nazionale, rendendo auspicabile e dirimente un intervento 'alla fonte' e quindi avente ad oggetto la validità della Direttiva stessa.

Nonostante quest'ultimo aspetto, le pronunce sin qui analizzate, pur nelle loro diversità, hanno senza dubbio il merito di aver alimentato un interessante dibattito sulla disciplina europea in materia di *bulk data retention*, mettendo in dubbio e gettando significative ombre sulla legittimità e proporzionalità di tale strumento invasivo. Diventava quindi sempre più evidente la necessità di un intervento delle Istituzioni europee capace di far tesoro di queste osservazioni e volto così a rivedere il bilanciamento effettuato tra tutela dei diritti fondamentali ed esigenze securitarie.

1.2. – La reazione della Commissione europea alle problematiche e ai dibattiti aperti negli Stati membri: tra procedimenti di infrazione e riconosciuto fallimento della DRD

In tale complesso contesto e nonostante le richiamate ampie discussioni sul piano politico, dottrinale[17] e giurisprudenziale che si erano aperte, come si è visto, in molti degli Stati membri, la

[16] E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, in *IANUS*, 15, 2017.

[17] Parte della dottrina, infatti, aveva continuato ad interrogarsi, anche prima dell'intervento della CGUE, circa la validità della DRD e la sua conformità rispetto alla Carta di Nizza, in particolare agli artt. 7 e 8. Tale valutazione portava gran parte degli studiosi a concludere per una risposta negativa alla questione, ritenendo che l'interferenza nella sfera privata provocata da una conservazione generalizzata non potesse superare il vaglio di proporzionalità *stricto sensu*; a ciò si giungeva considerando la limitata efficacia della *data retention* così disciplinata – valutato il tasso di errore (falsi positivi o falsi negativi) e la capacità di terroristi ed organizzazioni criminali di aggirare tali controlli e dunque limitare l'efficacia di tale strumento –, la durata eccessiva e sproporzionata nel suo massimo di 2 anni e la carenza di misure adeguate ed efficaci contro gli abusi che potrebbero essere perpetrati da autorità pubbliche o soggetti terzi, in mancanza di controlli da parte di autorità o soggetti indipendenti. Di questa opinione era L. FEILER, *The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection*, in *European Journal of Law and Technology*, 3, 2010. Merita per completezza però rilevare come alcuni autori, tra cui F. BIGNAMI, *Protecting privacy against the Police in the European Union: the Data Retention Directive*, in AA VV., *Melanges en l'honneur de Philippe Léger*, Editions Pedone, 2006, avessero invece espresso una opinione differente, ritenendo nel complesso la DRD conforme alla Carta di Nizza in quanto necessaria e proporzionata, grazie alle limitazioni introdotte (accesso consentito solo per la lotta a crimini gravi e previsione di un termine massimo di due anni ritenuto adeguato).

Commissione europea aveva attivato procedimenti di infrazione a carico degli Stati membri inadempienti quali Grecia, Irlanda, Olanda, Svezia, Austria e Germania[18], che avevano cioè mancato di traporre la Direttiva nell'ordinamento nazionale entro i termini previsti. In questi casi, molti Stati, tra cui Svezia e Austria, avevano motivato il proprio ritardo facendo espressamente riferimento alle preoccupazioni e ai dubbi circa la compatibilità della *data retention* disposta nella DRD rispetto ai diritti fondamentali sanciti nella Carta di Nizza, nella Convenzione EDU o nell'ordinamento nazionale. La questione, inoltre, diveniva ancora più articolata e di difficile soluzione per quegli Stati, come la Germania, nei quali il Parlamento aveva sì tempestivamente adottato una normativa apposita di trasposizione, salvo poi essere oggetto di una dichiarazione di incostituzionalità[19]. Proprio per la delicatezza di questi profili, alcuni autori hanno ritenuto "hazardous for the Commission to rule with an iron fist by forcing Member States to adopt data retention legislation that is incompatible with their Constitutions"[20]. A seguito di tali procedure, Austria, Grecia, Olanda, Irlanda e Svezia avevano conseguentemente provveduto ad adottare una normativa interna di attuazione della DRD[21] ma i dibattiti su tale controversa disciplina non erano certamente sopiti né destinati a concludersi.

È da rilevare infatti che, nonostante le procedure di infrazione attivate, le critiche e le problematiche emerse sul piano prima europeo – in sede di approvazione della DRD – e poi nazionale – nella fase di trasposizione della normativa europea – non erano del tutto passate inosservate dalle Istituzioni europee: ciò emerge con chiarezza nella valutazione sulla applicazione e sull'impatto della DRD, redatta nel 2011 dalla Commissione europea. In tale documento[22], preceduto da un'apposita conferenza, denominata significativamente "Taking on the Data Retention Directive", così da far trasparire la volontà di mantenere una qualche forma di conservazione dei metadati, la Commissione giungeva alla conclusione che "il contributo della Direttiva all'armonizzazione della conservazione dei dati è stato limitato (..). Considerate le implicazioni e i rischi per il mercato interno e per il diritto al rispetto della vita privata e

[18] La controversia 11 novembre 2009, C-192/09, *Commissione c. Olanda*, si era conclusa con una cancellazione della causa dal ruolo poiché l'Olanda, nelle more del giudizio, aveva provveduto ad adottare una normativa nazionale di trasposizione della DRD. Nella decisione 26 novembre 2009, C-202/09, *Commissione c. Irlanda*, del invece la CGUE aveva affermato come l'Irlanda fosse venuta meno agli obblighi stabiliti dalla DRD; stesso epilogo ha caratterizzato la decisione 30 gennaio 2010, C-211/09, *Commissione c. Grecia*, e la pronuncia 4 febbraio 2010, C-185/09, *Commissione c. Svezia* e 29 luglio 2010, C-189/09, *Commissione c. Austria*; conclusione differente ha avuto la controversia 5 giugno 2014, C-329/12, *Commissione c. Germania*: a seguito della sentenza *Digital Rights Ireland* del 8 aprile 2014, di cui si parlerà ampiamente in seguito e che aveva portato alla invalidazione della DRD, la Commissione aveva infatti rinunciato agli atti, ex art. 148 del Regolamento di procedura della Corte di Giustizia.

[19] Con riferimento alla Romania, nonostante la forte decisione della Corte costituzionale nazionale, il Parlamento aveva comunque deciso di approvare una normativa nazionale di attuazione della DRD quale rapida risposta alla procedura di infrazione minacciata dalla Commissione e attivata poi il 16 giugno 2011, con lettera di costituzione in mora. Il testo di tale normativa, approvata nel 2012, con legge n. 82/2012, aveva posto notevoli problemi, essendo molto simile alla previa legga dichiarata incostituzionale e attirando dunque numerose critiche da parte di ONG e società civile. Il Ministro proponente stesso aveva ammesso di sentirsi in una posizione estremamente complessa e senza alternative: "According to the Constitutional Court one may not retain data for a period of six months for a person who is not under investigation for committing crime. On the other hand, this is in contravention of the Directive, which calls for the retention of data on all users for a minimum period", come riportato da J. DURICA, *Directive on the retention of data on electronic communication in the rulings of the Constitutional Courts of EU Member States and efforts for its renewed implementation*, op. cit., p. 155. Per maggiori approfondimenti si rimanda anche a: S. SANDRU, *About data protection and data retention in Romania*, in *Masaryk University Journal of Law and Technology*, 2, 2013.

[20] T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, op. cit., p. 733.

[21] Per una analisi di tali normative, riperibili peraltro sul sito Eur-lex alla voce della DRD, si rimanda a C. JONES, B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, in *Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness – Paper*, op. cit., p. 15.

[22] COMMISSIONE EUROPEA, *Valutazione dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*, COM (2011) 225 def.

alla protezione dei dati personali, l'UE dovrebbe continuare a garantire, tramite norme comuni, il mantenimento di standard elevati in materia di immagazzinamento, estrazione e uso dei dati relativi al traffico e all'ubicazione. Tenuto conto di queste conclusioni, la Commissione intende proporre modifiche alla Direttiva, sulla base di una valutazione d'impatto" (p. 1) [23]. Pur scartando nuovamente l'opzione di una *data preservation* (o *quick freeze*)[24] e pur confermando l'utilità ed anzi il carattere indispensabile di un obbligo di conservazione dei metadati, la Commissione ammetteva che l'armonizzazione parziale cui puntava la DRD non era stata raggiunta. Le persistenti differenze nelle normative nazionali, frutto di quella disciplina 'a maglie larghe' prevista nella Direttiva in esame, avevano continuato a creare difficoltà agli operatori dei servizi di telecomunicazione, riconoscendone infine l'impatto significativo sui diritti fondamentali[25]. Il documento di valutazione affermava, in

[23] Interessante è notare, ad esempio, come le finalità poste alla base dell'accesso ai metadati da parte dei legislatori nazionali fossero anche molto differenti da Stato a Stato, arrivando ad includere scopi che eccedevano quelli previsti dalla DRD (ad esempio per finalità di prevenzione e contrasto della criminalità in generale e non solamente grave) e per i quali la *data retention* era consentita sulla base dell'art. 15 Direttiva *e-Privacy*, richiamata ampiamente nel Capitolo I. Ciò provocava non pochi problemi: "le differenze nelle finalità della conservazione dei dati verosimilmente influiscono sul volume e sulla frequenza delle richieste e quindi sui costi da sostenere per ottemperare agli obblighi imposti dalla Direttiva. Questa situazione può inoltre comportare una mancanza di prevedibilità, la quale deve essere garantita da qualsiasi disposizione legislativa che limiti il diritto al rispetto della vita privata", COMMISSIONE EUROPEA, *Valutazione dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*, op. cit., p. 9. Anche sul fronte della disciplina dell'accesso, pur lasciata alla regolamentazione dei singoli Stati, si continuavano a rilevare grandi differenze quanto alle autorità autorizzate all'accesso, alle modalità di accesso e alla procedura da seguire (previa autorizzazione giudiziaria o meno).

[24] "I sostenitori della conservazione per ordine giudiziario (il c.d. congelamento rapido), ritengono che questo strumento comporti una minore ingerenza nella vita privata rispetto alla conservazione dei dati. Tuttavia, secondo la maggior parte degli Stati membri, qualsiasi modalità di conservazione per ordine giudiziario non può sostituire adeguatamente la conservazione dei dati, in quanto quest'ultima rende disponibili dati storici, mentre la conservazione per ordine giudiziario non garantisce la possibilità di individuare tracce anteriormente all'ordine di conservazione, né consente di condurre indagini quando un soggetto è ignoto o di raccogliere prove, per esempio, sugli spostamenti delle vittime o dei testimoni di reato", e la Commissione si premura di sottolineare come "ciò sia stato riconosciuto anche dalla Corte costituzionale tedesca nella sentenza con la quale ha dichiarato incostituzionale la legge tedesca di attuazione delle Direttiva", COMMISSIONE EUROPEA, *Valutazione dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*, op. cit., p. 6. Simili considerazioni erano inserite anche nel successivo Report della Commissione titolato "Evidence of potential impacts of options for revising the Data Retention Directive: current approaches to data preservation in the EU and in Third Countries", del novembre 2012. In questo documento infatti veniva confermato come *data retention* e *data preservation* fossero strumenti complementari – e non alternativi – ed entrambi importanti nella lotta al crimine: "notwithstanding the differences, data retention plays a role in ensuring that data is kept and that this is sometimes a prerequisite for data preservation, as data may have already been delated before a data preservation order is issued. (..) The reason behind data preservation is the need for information about the content of the communication, which cannot be provided under data retention". Venivano così messe in evidenza le diverse finalità e scopi dei due strumenti, mentre, sotto il profilo dell'impatto rispetto ai diritti fondamentali alla privacy e protezione dei dati, veniva sottolineato come "some experts and NGOs stated that while a system of data preservation and targeted data collection had a lesser impact on fundamental rights, a risk remained in particular in view of that content data may be preserved as well as sensitive information about social contacts, movements and private, sometimes health-related contacts (with physicians, lawyers, worker councils, psychologists, helplines etc.)".

[25] Nel testo della valutazione venivano riprese le posizioni espresse da ONG, Gruppo di lavoro Art. 29 e Garante europeo della protezione dei dati, che avevano ribadito nel corso degli anni successivi alla entrata in vigore della DRD che la conservazione obbligatoria generalizzata dei metadati, così come disciplinata dalla DRD, non risultava limitata allo stretto necessario e avrebbe dovuto peraltro contenere anche norme in materia di accesso e utilizzo dei dati, in modo da fornire un quadro normativo completo e garantire la certezza del diritto (p. 33). Sotto questo specifico profilo dell'accesso, da alcuni studi effettuati a livello comparato sulle scelte legislative adottate nei vari Stati membri, erano emersi con chiarezza i punti deboli della DRD e delle ampie 'maglie' e spazi di manovra lasciati ai legislatori nazionali; uno tra tutti era da ravvisarsi, come già anticipato nel Capitolo I, nella mancata definizione di 'reati gravi': "because of the lack of a definition on what constituted serious crime at the EU level, Member States extended, on one hand, the scope of the access to these data and, on another hand, the authorities who may have access, including in particular intelligence services. The Directive contributes to the blur of

conclusione, la necessità di una revisione della normativa all'epoca vigente, assumendo anche l'impegno di considerare la possibile adozione di misure alternative più restrittive in termini di conservazione ma che fossero parimenti efficaci se comparate alla *data retention* generalizzata. In questo senso, la Commissione pareva aver recepito, o quanto meno ascoltato, le indicazioni pervenute dalle Corti nazionali nella giurisprudenza sopra analizzata[26].

Le problematiche rilevanti e profonde scaturite dal confronto tra Istituzioni europee, Stati membri e società civile, proseguite in maniera forte anche dopo l'adozione della DRD e rilevate dalla stessa Commissione, avevano messo in evidenza da un lato il fallimento della Direttiva e il mancato raggiungimento di molti dei suoi obiettivi, mentre dall'altro i dubbi considerevoli sorti con riferimento alla sua compatibilità con i diritti fondamentali riconosciuti a livello nazionale ed europeo (in senso stretto nella Carta di Nizza, ma anche nella Convenzione EDU). Dalla panoramica svolta sulle difficoltà attuative riscontrate dagli Stati membri, non si può in conclusione che concordare con l'affermazione di Jones e Hayes, risalente al 2013, secondo la quale: "the DRD ranks among the most controversial pieces of counter-terrorism legislation the EU has ever adopted and fierce debate as to its legitimacy and effectiveness has raged since the earliest stages of its drafting to the present day"[27].

2. – I primi interventi della Corte di giustizia dell'UE in materia di data retention

2.1. – La sentenza Irlanda c. Parlamento europeo e Consiglio *e il dibattito sulla base giuridica della DRD*

Le criticità sottolineate sin dalla adozione della DRD nonché il dibattito a livello nazionale da essa scaturito avevano reso ben presto chiara la necessità di un intervento da parte della Corte di Giustizia dell'UE. Non deve stupire quindi che l'attenzione e la delicatezza della disciplina della conservazione dei dati abbiano portato i giudici di Lussemburgo a pronunciarsi numerose volte, a partire dal 2009, in materia di *data retention*. Tali decisioni, che verranno analizzate in questo e nei prossimi Capitoli, segnano un'importante apertura nella direzione di un maggiore dialogo tra Corti nazionali e CGUE, dopo che le prime avevano messo in discussione, come si è visto nei precedenti paragrafi, unicamente le normative interne di trasposizione della DRD anziché la normativa europea stessa. Proprio con riferimento a tale discussa Direttiva, la Corte di Giustizia ha avuto modo di pronunciarsi ben due volte: la prima decisione, del 2009, aveva ad oggetto il vaglio di validità della DRD sotto il profilo della base giuridica, mentre la seconda, nel 2014, si concentrava invece sulla compatibilità della Direttiva rispetto ai diritti fondamentali sanciti nella Carta di Nizza. Sebbene quest'ultima sentenza, la nota *Digital Rights Ireland* (d'ora in avanti *DRI*), abbia certamente avuto un impatto ed un rilievo ben maggiore, non si può prescindere in questa sede dallo studio della prima pronuncia *Irlanda c. Parlamento europeo e Consiglio* (C-301/06, del 25 febbraio 2009) che, pur concentrandosi su profili formali, rivela alcune considerazioni dai risvolti sostanziali, che risultano indispensabili per poter poi muovere alcune riflessioni sulla giurisprudenza europea successiva ed evidenziarne divergenze o continuità negli approcci.

---

competences between law enforcement authorities and intelligence services in the prevention and investigation of serious crime as well as to a general shift towards prevention, proactive investigations and intelligence-led policing within the criminal justice system", C. COCQ, F. GALLI, *Comparative law paper on data retention regulation in a sample of EU Member States* (Deliverable 4.3 of the EU Project Surveille), 2013, p. 32.

[26] Per una analisi della posizione della Commissione in questa fase valutativa, si rimanda a: M. COLE, F. BOEHM, *EU Data Retention – Finally abolished? Eight years in light of Article 8*, in *Critical Quarterly for Legislation and Law*, 1, 2014, pp. 58-78.

[27] Così C. JONES, B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, in *Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness – Paper*, op. cit.

Ebbene, prendendo avvio da questa iniziale sentenza, è da sottolinearsi come essa abbia trovato origine nel complesso e travagliato percorso di adozione della DRD, la quale, come si ricorderà, era stata non a caso preceduta da una proposta di Decisione Quadro fondata sul Terzo Pilastro e promossa da alcuni Stati membri. Proprio – e solo – con riferimento al dibattuto profilo della corretta individuazione della base giuridica, i numerosi dubbi espressi da alcuni Governi degli Stati membri ma anche dal GEPD e dal Gruppo di Lavoro Art. 29 (analizzati nel Cap. I), si sono poi tradotti nel ricorso di annullamento promosso dall'Irlanda il 6 luglio 2006 dinnanzi alla CGUE, ai sensi dell'art. 230, co. 2, TCE. Supportato dalla Slovacchia, il Governo irlandese riteneva infatti che la DRD poggiasse erroneamente sul Primo Pilastro[28]: l'obiettivo della disciplina europea in materia di conservazione dei dati era primariamente e chiaramente quello di garantire la sicurezza e fungere quale strumento di lotta al crimine, mentre risultava solo secondario l'impatto sul funzionamento del mercato interno, che non poteva essere considerato lo scopo principale della normativa adottata. L'art. 95 TCE non poteva pertanto costituire, a parere dell'Irlanda, una base giuridica adeguata.

Per supportare tale posizione, la ricorrente faceva riferimento alla di poco precedente sentenza C-317/04 e 318/04, *Parlamento europeo c. Consiglio e Commissione*: questa pronuncia aveva ad oggetto la Decisione del Consiglio 2004/496 relativa alla conclusione di un accordo tra Comunità europea e USA in materia di trattamento e trasferimento dei dati PNR – cioè dei codici di prenotazione relativi ai passeggeri aviotrasportati, in partenza dall'UE e diretti verso gli Stati Uniti – da parte dei vettori aerei al *Bureau of Customs and Border Protection* statunitense. Sebbene su questa pronuncia – così come sul più ampio e complesso tema del trasferimento dati verso Paesi terzi – si concentrerà il Capitolo III, quanto risulta ora utile è l'analisi della posizione all'epoca espressa dalla CGUE con riferimento alla base giuridica della Decisione. Ebbene in quel caso, sebbene piuttosto sbrigativamente, i giudici di Lussemburgo avevano deciso di annullare la Decisione del Consiglio, ritenendola erroneamente fondata sul Primo Pilastro; sebbene la raccolta dei dati da parte delle compagnie aree rientrasse certamente nell'ambito del diritto comunitario, in quanto operazione svolta da soggetti privati nell'esercizio della propria attività commerciale, lo stesso non poteva dirsi per il successivo trattamento dei PNR, consistente nel trasferimento delle informazioni raccolte dall'UE agli USA: tale trattamento era infatti finalizzato non alla prestazione di servizi bensì alla salvaguardia della sicurezza pubblica degli USA, come richiesto dalle autorità di *law enforcement* di questo Stato terzo (par. 57). Da tale considerazione la CGUE concludeva che il trattamento dei dati personali dei viaggiatori dovesse essere ritenuto rientrante nelle attività di cui all'art. 3, n. 2 della Direttiva 95/46/CE: tale disposizione escludeva dal proprio ambito di applicazione il trattamento di dati effettuati per l'esercizio di attività o finalità che non rientravano nel diritto comunitario, tra cui quelle disciplinate dai Titoli V e VI del TUE quali pubblica sicurezza, difesa, sicurezza nazionale e attività in materia di diritto penale. Il trattamento dei PNR

[28] Merita sottolineare come, a differenza di alcuni dubbi 'sostanziali' espressi dalla Slovacchia, l'Irlanda "was not concerned with issues of human rights, as it had one of the toughest state regimes on data retention for law enforcement purposes at the time, and was actually challenging the DRD because it would have forced it to increase the domestic protections applying to the retention of personal data processed in the context of electronic communications", F. FABBRINI, *Human rights in the digital age: the European Court of Justice ruling in the Data Retention Case and its lessons for privacy and surveillance in the United States*, in *Harvard Human Rights Journal*, 28, 2015. La Repubblica Slovacca sosteneva invece che "la conservazione dei dati personali nella misura richiesta dalla Direttiva 2006/24 condurrebbe ad una notevole ingerenza nel diritto dei singoli al rispetto della loro vita privata, tutelato dall'art. 8 della CEDU. Sarebbe dubbio che un'ingerenza così grave possa essere giustificata da motivi economici, nella specie un migliore funzionamento del mercato interno. L'adozione di un atto al di fuori della competenza della Comunità, il cui scopo principale e non dissimulato sarebbe il contrasto della criminalità e del terrorismo, rappresenterebbe una soluzione più appropriata, che offrirebbe una motivazione più adeguata per l'ingerenza nel diritto al rispetto della vita privata" (par. 34, *Irlanda c. Parlamento europeo e Consiglio dell'UE*). Ironicamente giungerà poi, a distanza di anni, proprio dalla High Court irlandese il rinvio pregiudiziale, dalle prorompenti conseguenze, che riguarderà invece specificamente la compatibilità della DRD rispetto ai diritti fondamentali.

stabilito nella Decisione del Consiglio aveva proprio quale scopo quello della salvaguardia della sicurezza e della lotta alla criminalità, entrambi esclusi dall'ambito di applicazione della Dir. 95/46/CE: l'accordo in materia di trasferimento di PNR tra UE ed USA non poteva quindi considerarsi correttamente fondato sull'art. 95 TCE.

L'Irlanda aveva pertanto ritenuto che simili conclusioni della Corte di giustizia ben potessero essere applicate anche con riferimento alla DRD che, pur disciplinando la condotta di soggetti privati, quali i fornitori di servizi di telecomunicazioni, aveva tuttavia quale obiettivo ultimo quello di garantire la conservazione e dunque la disponibilità dei metadati per un eventuale successivo accesso da parte delle autorità di *law enforcement* per scopi di repressione di reati gravi. Secondo la ricorrente, entrambe le misure, della DRD e della Decisione del Consiglio in materia di PNR, riguardavano casi in cui un operatore economico raccoglieva dati relativi ai propri utenti primariamente e inizialmente per scopi commerciali e per la fornitura dei propri servizi; in entrambi i casi tali dati venivano però successivamente trattati – nel primo caso conservati per essere resi accessibili alle autorità pubbliche, mentre nel secondo caso trasferiti alle autorità statunitensi – per finalità diverse e ulteriori rispetto a quelle originarie, ovvero, in entrambi i casi, per scopi di garanzia della sicurezza pubblica e nazionale[29].

Questi parallelismi sono invece stati, invero piuttosto sorprendentemente[30], negati dalla CGUE nella sentenza del 2009: nel motivare la distanza tra i due casi, i giudici di Lussemburgo avevano ritenuto che, contrariamente a quanto previsto nella DRD, il trattamento dei dati stabilito dall'accordo di trasferimento dei PNR tra UE e USA non fosse "necessario alla realizzazione di una prestazione di servizi da parte dei vettori aerei ma necessario per salvaguardare la sicurezza pubblica e a fini repressivi" (par. 88), scopi peraltro esclusi dall'ambito di applicazione della Direttiva 95/46[31]. Nessuna similitudine

[29] Secondo l'Irlanda infatti "l'unico scopo o, in subordine, lo scopo principale o predominante della Direttiva in parola è agevolare l'indagine, l'accertamento e il perseguimento di reati, ivi inclusi quelli in materia di terrorismo. (..) Per tale Stato membro è assodato che i provvedimenti fondati sull'art. 95 TCE devono avere quale 'centro di gravità' il ravvicinamento delle legislazioni nazionali al fine di migliorare il funzionamento del mercato interno" (par. 31, *Irlanda c. Parlamento europeo e Consiglio dell'UE*). Le disposizioni della Direttiva 2006/24 riguardavano invece principalmente la repressione dei reati e non avrebbero potuto essere considerate come dirette meramente o fondamentalmente a porre rimedio agli eventuali difetti del mercato interno. In subordine, quand'anche, in contrasto con la tesi fondamentale sostenuta dell'Irlanda, la Corte avesse individuato effettivamente lo scopo della Direttiva nella prevenzione di distorsioni della concorrenza od ostacoli al mercato interno, l'Irlanda "sostiene che tale scopo dovrebbe essere considerato meramente incidentale rispetto allo scopo principale o predominante, cioè il contrasto della criminalità" (par. 31, *Irlanda c. Parlamento europeo e Consiglio dell'UE*).

[30] "The outcome in this case would have provided good odds at an EC constitutional betting forum. Indeed, few would have thought that the internal market provision of Art. 95 EC was capable of regulating the fight against terrorism and organized crime in the context of data retention. Yet, apparently, it is", E. HERLIN-KARNELL, *Annotation of Ireland v. Parliament and Council*, in *Common Market law Review*, 46, 2009, p. 1667.

[31] Nelle sue Conclusioni, l'Avvocato generale Bot aveva sul punto affermato: "Nella causa che ha dato luogo alla citata sentenza *Parlamento/Consiglio e Commissione*, l'accordo mirava principalmente ad imporre ai vettori aerei che assicurano il trasporto internazionale di passeggeri da e per gli Stati Uniti d'America di fornire al CBP un accesso elettronico ai dati PNR raccolti e conservati nei sistemi automatici di prenotazione/controllo dei vettori aerei. L'accordo istituiva quindi una forma di cooperazione internazionale tra le parti contraenti, destinata a conseguire l'obiettivo della lotta contro il terrorismo e altri reati gravi, tentando al contempo di conciliare tale obiettivo con quello di tutelare i dati personali dei passeggeri aerei. L'esistenza di tale forma di cooperazione internazionale con un'autorità pubblica di un paese terzo costituisce già una differenza importante rispetto alla presente causa. Occorre inoltre sottolineare che il trattamento dei dati in discussione nella causa che ha dato luogo alla citata sentenza Parlamento/Consiglio e Commissione, riguardava una fase successiva a quella della raccolta iniziale dei dati da parte delle compagnie aeree. Tale trattamento verteva sulla consultazione, sull'utilizzo da parte del CBP e sulla messa a disposizione di quest'ultimo dei dati dei passeggeri aerei provenienti da sistemi di prenotazione dei vettori aerei situati sul territorio degli Stati membri. Si trattava quindi di una forma di cooperazione che coinvolgeva non solo operatori privati, ma anche un'autorità pubblica, nella fattispecie il CBP, ai fini della lotta contro il terrorismo e altri gravi reati. (..) La dimensione internazionale della cooperazione e le modalità della collaborazione istituita fra i vettori aerei e il CBP, modalità che, a mio parere, fanno rientrare tale

era quindi riscontrabile tra le due discipline della *data retention* e del trasferimento di PNR, con ovvie conseguenze quanto alla base giuridica da individuare.

La posizione assunta della CGUE non ha mancato di sollevare perplessità e domande: se è certamente vero che, diversamente dall'accordo in materia di PNR che stabilisce alcuni limiti e tutele quanto al trattamento dei dati da parte delle autorità dello Stato terzo ricevente, la DRD non si occupa della disciplina delle fasi di accesso e utilizzo dei dati conservati – la cui disciplina è lasciata, seppur entro certi limiti, alla discrezionalità del legislatore nazionale –, è altrettanto vero che in entrambi i casi la raccolta e *data retention* da parte di operatori privati era diretta in un primo momento alla fornitura di un servizio e successivamente, sulla base della normativa DRD con riferimento ai metadati derivanti da telecomunicazioni e sulla base dell'accordo UE-USA con riferimento ai dati PNR, al perseguimento di scopi ulteriori volti alla garanzia della sicurezza nel contesto dell'UE nel primo caso mentre nel secondo ad essere tutelata era la sicurezza dello Stato terzo ricevente ovvero gli USA[32]. La linea di demarcazione tra le operazioni svolte dagli operatori economici per scopi commerciali e la finalità ulteriore della conservazione richiesta dalla normativa DRD risulta piuttosto sfumata e ha senza dubbio posto in evidenza come "the limits between data collected and used in the First and the Third Pillar are not always clear. The growing involvement of the private sector in law enforcement entails that personal data move from the one pillar to another and the distinction in pillars results in a situation where although the data are the same, the protection offered by the European legal system is different"[33].

Se queste criticità legate ad una 'hot area of cross-pillar litigation'[34] verranno certamente risolte, come si vedrà, a seguito dell'entrata in vigore del Trattato di Lisbona e del superamento del sistema a Pilastri, ciò che di questa sentenza risulta essere di fondamentale importanza, al fine di meglio comprendere e riflettere sulla successiva giurisprudenza europea, è la distinzione adottata dalla CGUE tra disciplina della conservazione e regolamentazione dell'accesso/utilizzo dei metadati da parte di autorità pubbliche. È proprio tale differenziazione a determinare la decisione dei giudici circa la correttezza della base giuridica scelta per l'adozione della DRD: quest'ultima, limitandosi esclusivamente alla regolamentazione della *data retention* e non dell'accesso, non sconfinava nelle competenze degli Stati membri in materia di repressione della criminalità, esclusa dall'ambito di applicazione del diritto europeo. Per la Corte dunque la DRD, regolando primariamente l'operato e gli obblighi posti in capo ai *service providers*, non poteva che trovare quale unica e corretta base giuridica il Primo Pilastro, quello comunitario[35]; come si è visto nel Capitolo I, le normative nazionali fortemente

collaborazione nell'ambito di applicazione del titolo VI del Trattato UE, costituiscono quindi due differenze fondamentali rispetto alla situazione controversa nel caso di specie", par. 116-118.

[32] "The decisions of the ECJ on competence in the data surveillance cases leave many questions pertaining to the legal basis provided by Article 95 EC and the competence of the EU more generally. It is difficult to reconcile the decisions in the two cases. Whereas the PNR decision appears to adopt a strict division of competences between the market and criminal justice, the clear lines of that decision are blurred by the ruling on the Data Retention Directive. The latter judgement allowed a particularly broad reading of Article 95 EC in terms of the relationship between market rules and public security. Many aspects of criminal law and procedure may have an effect on the internal market and yet it would be unsustainable to use Article 95 EC as a basis for EU action in every case", C. MURPHY, *Fundamental rights and security: the difficult position of the European judiciary*, in *European Public Law*, 16, 2010, p. 307.

[33] E. KOSTA, F. COUDERT, J. DUMORTIER, *Data protection in the Third pillar: in the aftermath of the ECJ decision on PNR data and the Data Retention Directive*, in *International Review of Law Computers and Technology*, 3, 2007, p. 349.

[34] Come definita da E. HERLIN-KARNELL, *Annotation of Ireland v. Parliament and Council*, cit., p. 1667.

[35] Una ulteriore motivazione addotta dalla CGUE a sostegno della correttezza della base giuridica scelta per la DRD si fondava sul fatto che tale normativa andasse a modificare la Direttiva *e-Privacy*, adottata sulla base dell'art. 95 CE: "In forza dell'art. 47 UE, nessuna disposizione del Trattato CE può essere intaccata da una disposizione del Trattato UE. Il medesimo principio figura al primo comma dell'art. 29 UE, che introduce il titolo VI di quest'ultimo Trattato, rubricato «Disposizioni sulla cooperazione di polizia e giudiziaria in materia penale» (sentenza Commissione/Consiglio, cit., punto 52). Stabilendo che nessuna disposizione del Trattato UE pregiudica i Trattati istitutivi delle Comunità europee o i Trattati e gli atti susseguenti che li hanno modificati o completati,

disomogenee adottate sulla base dell'art. 15 della Direttiva *e-Privacy* avevano infatti avuto un forte impatto sul mercato interno e sul lavoro degli operatori di servizi di telecomunicazione, col rischio ultimo di incidere negativamente in materia di concorrenza e libera circolazione dei servizi, essendo i diversi *service providers* chiamati a rispettare normative nazionali spesso molto differenti tra loro e più o meno onerose. Le disposizioni della DRD miravano a correggere ed armonizzare proprio tale ambito, avendo ad oggetto la regolamentazione di attività di soggetti privati del tutto "indipendenti dall'attuazione di qualsiasi eventuale azione di cooperazione di polizia e giudiziaria in materia penale" (par. 83). Tanto era bastato per rigettare il ricorso promosso dall'Irlanda.

Nel giudizio del 2009, la CGUE si limitava a vagliare la validità della DRD sul piano formale della base giuridica: del resto i giudici di Lussemburgo sono vincolati, lo si ricorda, a pronunziarsi su quanto avanzato dalla ricorrente che, nel caso specifico esaminato, non aveva sottoposto questioni attinenti la compatibilità di una *bulk data retention* con i diritti fondamentali. Nonostante questo profilo, alcuni autori non hanno mancato di rilevare gli impliciti risvolti sostanziali della decisione *Irlanda c. Parlamento europeo e Consiglio*: "anche se in questa occasione la Corte non si è pronunciata direttamente sulla questione della compatibilità della Direttiva con i diritti fondamentali dell'Unione, la conferma della sua base legale (..) si è ripercossa in via mediata sulla protezione dei diritti nel campo investigativo e processual-penalistico, restringendone l'ambito di rilevanza. Lo spostamento del baricentro (..) verso l'ex Primo Pilastro ha comportato un'accentuazione dei fattori pro-concorrenziali e pro-liberoscambisti della disciplina, spingendone ai margini gli autentici obiettivi – riconosciuti invece dalla sentenza sui PNR – che la stessa Direttiva individua nello 'scopo di garantire la disponibilità [dei dati] a fini di indagine, accertamento e perseguimento di reati gravi' (art. 1)'"[36], con la conseguenza che la analizzata decisione della Corte risultava poco attenta alle implicazioni sostanziali della propria posizione. Senza dubbio il fatto di aver confermato il Pilastro 'comunitario' quale fondamento di una normativa in materia di conservazione dei dati risulta "una presa di posizione rilevante a favore dell'adozione di atti normativi comunitari nell'elaborazione delle politiche europee anti-terrorismo, che rafforza il ruolo del Parlamento europeo (e degli stessi giudici comunitari) nei periodi dell'emergenza"[37]: una lettura quindi che prende atto degli effetti che gli obblighi posti in capo agli operatori privati

---

l'art. 47 UE si prefigge infatti, conformemente agli artt. 2, quinto trattino, UE e 3, primo comma, UE, di mantenere integralmente l'*acquis communautaire* e di svilupparlo (sentenza 20 maggio 2008, C-91/05, Commissione/Consiglio, Racc. pag. I-3651, punto 59). Spetta dunque alla Corte vigilare affinché gli atti che il Consiglio considera rientrare nell'ambito del titolo VI del Trattato UE e che per loro stessa natura sono idonei a produrre effetti giuridici non sconfinino nelle competenze che le disposizioni del Trattato CE attribuiscono alla Comunità (sentenza 20 maggio 2008, Commissione/Consiglio, cit., punto 33 e giurisprudenza ivi citata). Nei limiti in cui la modifica della Direttiva 2002/58 operata attraverso la Direttiva 2006/24 rientra nelle competenze comunitarie, quest'ultima non poteva essere fondata su una disposizione del Trattato UE senza violare l'art. 47 di quest'ultimo" (par. 75-78).

[36] A. DI MARTINO, *Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, op. cit., p. 4063 e ss. Per quanto il ricorso di annullamento promosso dall'Irlanda vertesse appunto su questioni connesse alla base giuridica della DRD, le preoccupazioni relative alla compatibilità di tale disciplina rispetto ai diritti fondamentale erano talmente profonde e sentite che la ONG 'Working Group on Data Retention', insieme ad altre 43 ONG europee, avevano presentato alla CGUE, in tale occasione, una memoria in qualità di *amicus curiae*, incitando i giudici a pronunciarsi sul piano sostanziale: "we urge the Court to base its decision on the incompatibility with human rights rather than the lack of competence. A decision on the compatibility with human rights is essential to prevent member states from replacing the directive with a framework decision that equally violates human rights", sottolineando come la DRD violasse il diritto alla vita privata e protezione dei dati, la libertà di espressione nonché la protezione della proprietà (più ampiamente si legga *Submission concerning the action brought on 6 July 2006, Ireland v. Council, European Parliament*, 8 aprile 2008). Risulta chiaro quindi come una questione così delicata e che aveva così tanto attirato l'attenzione della società civile, benché non trattata nella pronuncia in esame dalla CGUE, non potesse rimanere a lungo senza risposta.

[37] F. FABBRINI, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quaderni Costituzionali*, 2, 2009, p. 422.

nell'ambito del mercato interno producono rispetto alla strategia nazionale e sovranazionale di lotta alla minaccia terroristica e della criminalità grave. Se da un lato la posizione finale della Corte di giustizia ha avuto il merito di confermare la correttezza della base giuridica e, di riflesso, la partecipazione del Parlamento europeo e del Garante Europeo per la Protezione dei Dati al processo di approvazione di una disciplina così delicata[38], dall'altro lato proprio tale scelta non manca di essere alla base di quei limiti, lacune e problematiche che già le Corti nazionali avevano rilevato e rispetto alle quali si erano scontrate: "grounding the instrument on a legal basis that is meant for criminal law rather than internal market measures could indeed allow the EU policy maker to better seize the definition of specific concepts. The use of the specific criminal law legal basis would avoid the problem encountered by the EU legislator when drafting the Data Retention Directive of having to establish provisions which are vague in scope. The vagueness of specific criminal law provisions was due to the fact that the centre of gravity requirement meant that the emphasis in the measure had to be placed on internal market provisions rather than criminal law ones (..), leav[ing] a wide margin of manoeuvre to Member States in the implementation process and eventually to law enforcement authorities in their use of data retention means"[39]. La base giuridica scelta per la DRD, ristretta entro i confini del funzionamento del mercato unico, si tramuta inoltre, nella realtà, in un limite al raggiungimento di una completa ed efficace armonizzazione della materia della conservazione dei dati a livello europeo, materia che, nonostante quanto affermato dalla Corte, risultava nella pratica strettamente e consequenzialmente legata al successivo utilizzo dei dati conservati da parte delle autorità pubbliche nazionali[40]. Anche l'Avvocato generale Bot aveva sottolineato questo profilo, rilevando la problematicità di una distinzione netta tra i due momenti e le due operazioni di conservazione e accesso: "tale linea di demarcazione non è sicuramente esente da critiche e può sembrare artificiosa sotto alcuni aspetti. Concordo che sarebbe più soddisfacente che il problema globale della conservazione dei dati da parte dei fornitori di servizi di comunicazione elettronica e delle modalità della loro cooperazione con le autorità nazionali competenti in materia di contrasto fosse oggetto di un atto unico che garantisse la coerenza tra queste due componenti. Per quanto possa non piacere, l'architettura costituzionale composta da tre pilastri impone tuttavia una separazione tra i settori di intervento. La priorità consiste, in tale contesto, nel garantire la certezza del diritto chiarendo, nei limiti del possibile, il confine tra i settori di azione rientranti nei diversi pilastri", (par. 108).

Proprio questa discussa e sottile linea di divisione, disegnata dalla CGUE in questa pronuncia, risulta in una differenziazione non solo tra base giuridica del Primo o del Terzo Pilastro bensì anche tra aree di competenza dell'UE e degli Stati membri, portando ad una distinzione che non mancherà di essere sottolineata e riproposta con forza nella successiva giurisprudenza europea: dalla *Digital Rights Ireland*,

---

[38] "If the Court had annulled the first pillar choice, the Directive would have needed an alternative legal basis, which would have been most likely a third pillar option. This option would have excluded both the European Parliament and the European Data Protection Supervisor from the legislative process and the Directive from democratic control", M. COLE, F. BOEHM, *EU Data Retention – Finally abolished? Eight years in light of Article 8*, op. cit. Sul punto si legga anche T. KONSTADINIDES, *Wavering between Centres of Gravity: comment on Ireland v. Parliament and Council*¸ in *European Law Review*, 35, 2010, p. 88;

[39] F. GALLI, *Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions*, in *Maastricht of European and Comparative Law Journal*, 3, 2016, p. 463.

[40] Alcuni autori, infatti, con riferimento proprio a questa distinzione tra conservazione e accesso, sostenevano come in realtà non fosse del tutto corretto affermare che la DRD non si occupasse della disciplina dell'accesso ai dati: prendendo in considerazione l'art. 4 DRD, "this provision obliges member states to adopt measures granting access to data to competent (national) authorities and as such, should have been inserted in a third-pillar instrument. Although art. 4 was intended to limit the conditions under which competent authorities are granted access, it cannot be denied that it at the same time enables law enforcement authorities to get hold of retained data", giungendo alla conclusion che "the Court could have declared that Article 4 has no basis in the first pillar and therefore it should have been inserted into a third-pillar instrument", S. POLI, *The legal basis of Internal market measures with a security dimension: comment on case C-301/06, Ireland vs. Parliament/Council*, in *European Constitutional Law Review*, 6, 2010, p. 153.

alla *Tele2*, fino alla *Ministerio Fiscal*, sino a giungere ai rinvii pregiudiziali attualmente pendenti. Lo stretto rapporto di funzionalità intercorrente tra conservazione e accesso e il loro intersecare competenze differenti, quella della protezione dei dati e della riservatezza da un lato e quella di garanzia della sicurezza pubblica e nazionale dall'altro, in quella che è stata definita come una "of the most sensitive fault lines between EU and Member States competence"[41], continueranno ad essere al centro dell'attenzione dei giudici nazionali ed europei. Come vedremo, questi ultimi si spingeranno, nelle successive pronunce, ad indicare le condizioni di legittimità dell'accesso stesso, rendendo così ancor più sfumato quel discusso confine tra diverse operazioni – conservazione e accesso – stabilito per la prima volta nella pronuncia qui analizzata. Ciò che certamente emerge da tale prima decisione della CGUE è una situazione piuttosto confusa, che lascia ampio margine di discrezionalità agli Stati membri quanto alla disciplina dell'accesso, con tutte le difficoltà e criticità già evidenziate in precedenza: "by imposing an obligation to retain data but excluding from its scope the issue of access to it - a closely inter-related step capable of affecting the privacy related acceptability of data retention -, the [Data Retention] Directive has placed a bomb in the privacy of European citizens and has allowed the Member States alone to take measures to prevent it from exploding. Several Member States did not do well on this task and the bomb has exploded as has the negativity surrounding the particular measure"[42].

2.2. – La storica pronuncia Digital Rights Ireland: la CGUE invalida la Data Retention Directive

2.2.1. – Dal mutato assetto istituzionale dell'UE a seguito del Trattato di Lisbona alle rivelazioni di Snowden: una necessaria premessa di contesto

Il forte dibattito che aveva caratterizzato la DRD, dalla sua adozione sino alla sua attuazione da parte degli Stati membri, non si limitava, come si è visto, ad una questione formale inerente la correttezza della base giuridica: i dubbi e le critiche sollevate, anche a livello nazionale e rilevate da taluni giudici statali, assumevano carattere sostanziale, riguardando la compatibilità di un regime di conservazione generalizzata con i diritti fondamentali. Come emerso dal par. 1, tuttavia, nonostante la travagliata trasposizione della Direttiva 24/2006 nel contesto nazionale, la Corte di Giustizia dell'UE non era mai stata chiamata mediante rinvio pregiudiziale a vagliare la validità della normativa europea, benché la dottrina avesse sottolineato più volte l'importanza di un intervento chiarificatore dei giudici di Lussemburgo[43]. Sarà comunque necessario attendere sino al 2012 affinché a questi ultimi venga offerta l'occasione di pronunciarsi nuovamente e, questa volta, in maniera sostanziale, sulla DRD.

---

[41] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018, p. 6.

[42] C. MARKOU, *The Cyprus and other EU Courts rulings on data retention: the Directive as a privacy bomb*, in *Computer Law & Security Review*, 28, 2012, p. 475.

[43] Osservando come tutte le controversie sorte negli Stati membri fossero *de facto* derivanti da serie perplessità circa la legittimità della DRD stessa, molto autori auspicavano un coinvolgimento diretto della CGUE: "It is to be hoped that the Court will at least provide guidance to the EU legislator and the Member States on the minimum safeguards that must be observed in the context of the mere retention of communications data to ensure the adequate protection of the fundamental rights of EU citizens under the Charter. In addition, it would be useful to see how the Court of Justice views the distinction currently contained in the Directive between retention and access. Arguably, it is this distinction – where the EU law regulates the former, while national law is left to regulate the latter – that is the source of many of the substantive and procedural issues that have arisen in the context of this legislative project. It is likely that guidance on a more comprehensive approach dealing not just with the types of data to be retained but also with the types of authorities that should have to access them and for what purpose, would be welcomed by citizens, law enforcement authorities and communications service providers alike. It is to be hoped that the Court will rise to that challenge when it finally gets to hand down its decision", E. KOSTA, *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, op. cit., p. 363. Sulla scorta di tali considerazioni, alcuni autori avevano ritenuto inaspettata e sorprendente la scelta delle Corti nazionali di non attivare l'intervento della CGUE (L. BENEDIZIONE,

Nel frattempo, durante il lungo percorso che ha portato alla formulazione dei rinvii pregiudiziali, significativi mutamenti ed evoluzioni erano intercorsi nel panorama europeo, sotto il profilo dell'assetto istituzionale e delle fonti. Innanzitutto il Trattato di Lisbona, adottato nel 2007 ed in entrato in vigore nel 2009, ha comportato, come si è già visto nel Capitolo I, Parte I, l'inserimento nel Trattato sul Funzionamento dell'UE (TFUE) dell'art. 16. Pur rassomigliando al previo art. 286 del TCE[44], tale disposizione fornisce ora una più ampia e completa tutela del diritto alla protezione dei dati, rappresentando la base giuridica per l'adozione di qualsiasi normativa relativa alla privacy e *data protection*: tale materia, sulla base della divisione in Pilastri tipica dell'assetto europeo precedente, risultava divisa e frammentata tra Primo e Terzo Pilastro, comportando così diversità sotto il profilo del procedimento approvativo e criticità derivanti dalla difficoltà di stabilire chiaramente la riconducibilità all'una o all'altra area di intervento dell'UE. Queste problematiche sono risultate quindi superate con il Trattato di Lisbona e la predisposizione di un unico articolo quale base giuridica unitaria e più solida, in grado peraltro di integrare nel processo legislativo anche il Parlamento europeo[45]: qualsiasi disciplina che abbia ad oggetto la regolamentazione della protezione dei dati di carattere personale, indipendentemente dal settore del diritto dell'Unione cui afferisce (che sia quello del funzionamento del mercato interno o quello attinente allo spazio di libertà, sicurezza e giustizia) può trovare così base giuridica nell'art. 16 TFUE. L'art. 6 del Trattato sull'Unione europea, come modificato nel 2007, inoltre ha riconosciuto alla Carta di Nizza (Carta dei Diritti Fondamentali dell'UE) lo stesso valore giuridico dei Trattati, facendola dunque divenire fonte vincolante del diritto europeo e parametro che la CGUE può utilizzare per vagliare la validità e conformità al diritto dell'UE degli atti sopposti al suo controllo. Questi aspetti di carattere generale, seppur brevemente richiamati, non possono certo essere ignorati poiché incidono sia sul ragionamento e sulle argomentazioni dei giudici di Lussemburgo sia sul rapporto Stati membri-Unione europea, nonché sul funzionamento stesso di quest'ultima, con ovvie ripercussioni sull'intervento normativo europeo in temi quali quelli in esame.

A ciò però è da aggiungersi anche una evoluzione sul piano politico-sociale, intervenuta a partire dall'anno 2013: le rivelazioni di Edward Snowden, richiamate nella Parte I, avevano accresciuto la sensibilità dell'opinione pubblica verso tematiche quali l'ingerenza nella sfera privata da parte delle

---

E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, op. cit., p. 1736), che pareva invece la via più logica per superare i problemi derivanti dalla violazione dei diritti fondamentali e dalla assenza di proporzionalità insite nella disciplina europea stessa e di cui le normative nazionali non erano che una trasposizione. Nonostante questo profilo critico, tuttavia, non può non essere, sin da ora, riconosciuto alle decisioni dei giudici degli Stati membri in materia di *data retention* un peso e una influenza positiva, fornendo importanti spunti di riflessione sia alle Corti irlandesi e austriaca che alla CGUE stessa. Come riportato da Caggiano, ad esempio, "secondo molti commentatori, l'argomentazione del Tribunale [costituzionale tedesco] avrebbe ispirato la sentenza *Digital Rights Ireland* della Corte di giustizia", G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, 2, 2018, p. 2.

[44] "Although there was a provision in art. 286 EC Treaty dealing with the application of existing data protection rules to all European Institutions and bodies, there was no general data protection provision as can be found since entry into force of the Treaty of Lisbon art. 16 TFUE. According to this provision there is not only a re-statement of the right to data protection, but it also gives the EU a general legal basis to create rules concerning processing of data by the Union and the MSs in connection with EU law. And although the equivalence table attached to the Treaty of Lisbon suggests the new art. 16 TFEU is a replacement of the former art. 286 TEC, in reality the new provision significantly expands the scope of data protection in the EU context", M. COLE, F. BOEHM, *EU Data Retention – Finally abolished? Eight years in light of Article 8*, op. cit., p. 62.

[45] "Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte di istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti", art. 16, co. 2, TFUE.

autorità pubbliche, perpetrata – anche – mediante strumenti di raccolta e conservazione massiva di dati e metadati derivanti dalle comunicazioni elettroniche. La consapevolezza circa l'utilizzo di tali strumenti aveva indotto la società ma anche numerose ONG, a guardare con maggiore attenzione a normative passibili di fornire allo Stato mezzi di sorveglianza e di invasione nella vita di ciascun individuo e a prendere coscienza dei rischi che una tale legittimazione, anche quando motivata da scopi di interesse generale quali la sicurezza, può determinare rispetto ai diritti fondamentali e ad un equilibrato rapporto tra autorità pubbliche e cittadini. È quindi in questo mutato contesto istituzionale e sociale che il successivo intervento della CGUE in materia di *data retention* deve essere inserito.

2.2.2. – I rinvii pregiudiziali della High Court irlandese e della Corte costituzionale austriaca

Mentre nei casi analizzati nel Paragrafo 1, le Corti nazionali avevano deciso di non richiedere l'intervento dei giudici di Lussemburgo, la High Court irlandese e la *Verfassungsgerichtshof* (Corte costituzionale austriaca) avevano invece ritenuto opportuno indirizzare due differenti rinvii pregiudiziali alla CGUE, offrendo a quest'ultima "l'occasione di pronunciarsi sulle condizioni alle quali è costituzionalmente possibile per l'Unione europea prevedere una limitazione all'esercizio dei diritti fondamentali nel senso particolare di cui all'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE, mediante una Direttiva e i relativi provvedimenti nazionali di recepimento"[46]. La scelta di queste due Corti nazionali è stata accolta, anche dalla dottrina, in modo estremamente positivo, poiché ha consentito finalmente di affrontare il problema della disciplina della *data retention* alla radice, ovvero alla sua origine europea, e di permettere alla CGUE di prendere così posizione dinnanzi a tutte quelle criticità 'sostanziali' che, sin dalla sua origine, ne avevano caratterizzato la disciplina[47]. Vista l'importanza della tanto attesa pronuncia della Corte e il suo potenziale rilevante impatto anche e soprattutto rispetto agli Stati membri, non stupisce che la *Ústavný súd Slovenskej republiky* (Corte costituzionale slovacca) avesse deciso di sospendere l'applicazione della normativa interna di trasposizione della DRD nelle more del giudizio dinnanzi ai giudici di Lussemburgo[48]. Similmente, anche la *Ustavno sodišče Republike Slovenije* (Corte costituzionale slovena), investita dal ricorso dello ***Informacijski pooblaščenec***[49] che chiedeva di valutare la legittimità costituzionale della normativa nazionale di trasposizione della DRD, aveva concluso, mediante ordinanza del 26 settembre 2013, col sospendere il procedimento in attesa dell'esito dei rinvii pregiudiziali pendenti dinnanzi alla CGUE: pur non ricorrendo essa stessa a promuovere un rinvio ai giudici di Lussemburgo, anche la Corte slovena, per decidere sulla legislazione interna, aveva dunque ritenuto essenziale un preliminare vaglio della validità e legittimità della Direttiva europea in materia di *data retention*[50].

---

[46] Così viene messo in evidenza dall'Avvocato generale Pedro Cruz Villalon, nelle sue Conclusioni presentate il 12 dicembre 2013 nella causa *Digital Rights Ireland*.

[47] "The decisions – albeit after lengthy considerations – of first the Irish High Court and subsequently the Austrian Constitutional Court were welcomed with relief as they gave the CJEU the chance to revisit the fundamental rights questions left open in its initial (competency) judgement on the DRD". Anticipando qui la decisione della Corte, il fatto che si sia giunti ad una invalidazione della DRD, secondo i medesimi autori, porta a considerare "retrospectively speaking, an even stronger disappointment that the national Courts did not act earlier and thereby contributed to a more swift clarification of the validity (or actually invalidity) of this important piece of EU secondary law", F. BOEHM, M. COLE, *Data retention after the judgement of the Court of Justice of the EU*, The Greens in the EP Working Paper, 2014, p. 19.

[48] A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy*, op. cit., p. 23.

[49] Autorità indipendente slovacca che supervisiona il rispetto delle normative in materia di protezione dei dati e di accesso agli atti delle pubbliche amministrazioni.

[50] Sul punto, nonché per una ampia ricostruzione dei rinvii pregiudiziali irlandese ed austriaco, si rimanda a: L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, op. cit. Ma anche a M.

Partendo dalla breve ricostruzione dei rinvii promossi, importante per comprendere le perplessità dei cittadini e delle ONG che avevano azionato i ricorsi dinnanzi alle Corti nazionali nonché per capire i dubbi avanzati dai giudici del rinvio, la controversia irlandese aveva avuto origine dal ricorso promosso nel 2006 dinnanzi alla High Court irlandese da Digital Rights Ireland, una nota società avente operante nell'ambito della protezione e promozione dei diritti fondamentali, con particolare attenzione alle insidie derivanti dall'utilizzo delle nuove tecnologie. La ricorrente riteneva illegittimo il trattamento, conservazione e accesso ai dati relativi alle proprie comunicazioni telefoniche: tali operazioni erano legittimate sulla base di una normativa interna (*Criminal Justice Terrorist Offences Act 2005*) che imponeva, conformemente a quanto disposto dalla DRD, ai fornitori di servizi di telecomunicazioni una *data retention* generalizzata, estesa cioè a tutti gli utenti. Tale legislazione risultava, a parere della ricorrente, incostituzionale e incompatibile con il diritto dell'UE, invitando peraltro il giudice nazionale a sottoporre alla CGUE questioni pregiudiziali volte a constatare la conformità della DRD – della quale la legge interna era attuazione – rispetto alla Carta di Nizza.

In Austria invece il Governo del Land della Carinzia prima, il sig. Seitlinger poi, seguito da un ricorso promosso da ben 11.130 cittadini, avevano lamentato l'incostituzionalità – nonché l'incompatibilità con l'art. 8 della Carta di Nizza – dell'art. 102 bis della legge austriaca sulle telecomunicazioni, introdotto quale trasposizione della DRD e che obbligava gli operatori di telecomunicazioni a conservare i dati prodotti dai propri utenti, anche senza il loro consenso e senza una specifica necessità di repressione di crimini gravi.

Le questioni pregiudiziali promosse dalla High Court irlandese (nella causa C-293/12) e dalla Corte costituzionale austriaca (C-594/12), poi riunite dalla CGUE nel 2013, muovevano dalla impossibilità per i giudici nazionali di risolvere le questioni attinenti alle normative nazionali in materia di *data retention* senza che prima fosse valutata la validità della DRD da cui esse discendevano: entrambe le Corti del rinvio condividevano dubbi quanto legittimità della disciplina della conservazione dei dati che non prevedeva la necessaria esistenza di un legame o una connessione tra trattenimento del dato e un sospetto o un rischio per la sicurezza; le perplessità quindi attenevano alla proporzionalità della conservazione generalizzata stessa che, di per sé, rappresentava una forte ingerenza nella sfera privata dell'individuo, impattando anche sulla possibilità di godere di altri diritti e libertà costituzionalmente garantiti e riconosciuti anche a livello europeo. I quesiti posti dai giudici nazionali erano dunque molteplici e toccavano svariati profili che possono essenzialmente essere sintetizzati in quattro interrogativi[51] che, lo si anticipa, non hanno trovato tutti risposta nella pronuncia dei giudici di Lussemburgo. Questi ultimi, infatti, si sono concentrati sulla questione attinente alla validità della DRD alla luce degli artt. 7, 8 e 11 della Carta di Nizza[52].

DICOSOLA, *La data retention directive e il dialogo tra Corti costituzionali e Corte di giustizia nel sistema multilivello europeo*, in *Diritti Comparati*, 20 febbraio 2014, che ritiene la decisione di sospensione della Corte costituzionale slovena un importante esempio di dialogo tra le Corti nazionali ed europea.

[51] In estrema sintesi, le questioni pregiudiziali sono attinenti: a) alla compatibilità della DRD con diverse disposizioni della Carta di Nizza ed in particolare con l'art. 7 sul diritto al rispetto della vita privata, l'art. 8 sul diritto alla protezione dei dati di carattere personale, l'art. 11 sulla libertà di espressione, l'art. 52 sulla proporzionalità della disciplina normativa imposta; b) ai rapporti tra l'art. 8 della Carta di Nizza e la Dir. 95/46 nonché le norme della CEDU ed in particolare l'art. 8; c) alla questione se la DRD sia da considerarsi, ai sensi dell'art. 5, par. 4, TUE, proporzionata, necessaria ed adeguata a conseguire gli obiettivi perseguiti; d) alla questione se i giudici nazionali debbano, per dovere di leale cooperazione, vagliare la validità della normativa nazionale di trasposizione della DRD alla luce della Carta di Nizza.

[52] Merita sottolineare come la High Court irlandese avesse fatto riferimento non solo al diritto alla privacy, alla protezione dei dati e alla libertà di espressione, bensì anche alla libertà di movimento (art. 21 TFUE) e al diritto ad una buona amministrazione (art. 41 Carta di Nizza). La Corte costituzionale slovena nella propria decisione di sospendere il giudizio in attesa della pronuncia della CGUE sulla DRD, aveva fatto anche riferimento alla compatibilità della Direttiva europea rispetto al diritto di cui all'art. 48 Carta di Nizza che afferma la presunzione di innocenza dell'imputato. Nonostante il richiamo a diversi diritti fondamentali coinvolti, tutte le Corti nazionali avevano certamente fatto primario riferimento ai diritti alla riservatezza e alla protezione dei dati, cui vengono

2.2.3. – L'analisi della CGUE: la distinzione tra metadati e contenuto delle comunicazioni, la compressione del nucleo essenziale dei diritti alla riservatezza e protezione dei dati e la sussistenza di un interesse generale

Iniziando ad esaminare la sentenza della CGUE, risulta necessario prendere avvio dall'analisi di una prima affermazione di grande rilievo espressa dai giudici di Lussemburgo: è stato specificato, infatti, che le informazioni oggetto di conservazione non riguardavano i contenuti delle comunicazioni o dell'utilizzo di una rete Internet, bensì rappresentavano i dati necessari per rintracciare e identificare la fonte di una comunicazione, la destinazione, data, ora, durata e tipo di una comunicazione nonché l'attrezzatura di comunicazione degli utenti e la loro ubicazione, nome e indirizzo dell'utente, numero del chiamante e del chiamato o indirizzo IP nel caso di servizi Internet; da questa constatazione, che dimostra certamente una forte attenzione all'utilizzo concreto dei Big Data e dei metadati nonché una lucida conoscenza delle potenzialità che essi rappresentano, i giudici hanno riconosciuto che "questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati" (par. 27, *DRI*)[53]. Pur potendo incidere anche sulla libertà di espressione tutelata all'art. 11 della Carta di Nizza, la Corte ha riscontrato nella *data retention*, finalizzata all'eventuale accesso ai dati da parte delle autorità nazionali competenti, una incidenza specifica e diretta principalmente sui diritti alla vita privata e al trattamento dei dati personali, dunque sugli artt. 7 e 8 della Carta stessa. Ed è di questi che si è quindi primariamente occupata la pronuncia in esame: proseguendo nel suo ragionamento, infatti, i giudici hanno ribadito l'esistenza di una ingerenza nei diritti alla riservatezza e alla protezione dei dati rappresentata innanzitutto dalla conservazione, *per se* considerata, nonché dall'accesso eventuale e successivo da parte della autorità di *law enforcement*, che costituisce una "ingerenza supplementare" (par. 35, *DRI*).

La Corte ha quindi individuato già nella sola fase della conservazione, indipendentemente dal successivo momento dell'accesso, l'esistenza di una ingerenza, che è stata poi, ancor più significativamente, definita "di vasta portata e considerata particolarmente grave. Il fatto che la conservazione dei dati e l'utilizzo ulteriore degli stessi siano effettuati senza che l'abbonato o l'utente registrato ne siano informati può ingenerare nelle persone interessate (..) la *sensazione che la loro vita privata sia oggetto di costante sorveglianza*" (par. 37, *DRI*, enfasi aggiunta). Questa affermazione è di grande impatto, a dimostrazione del chiaro riconoscimento da parte dei giudici della profonda ingerenza che anche la mera conservazione, oltre all'ipotetico successivo accesso, rappresenta; le parole utilizzate dall'Avvocato generale, in tal senso, sono estremamente forti: "la raccolta di dati crea le condizioni per un possibile controllo ex post delle attività personali e professionali che, seppur esercitato soltanto a posteriori in occasione del loro impiego, minaccia tuttavia in modo permanente, per tutto il periodo della loro conservazione, il diritto dei cittadini dell'Unione alla riservatezza della loro vita privata. La *diffusa*

riconosciuti "predominant importance, using the alleged violation of the others as an ancillary argumentation aimed at confirming the thesis of a disproportionate sacrifice imposed by the Directive's dispositions on the exercise of fundamental rights", L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, op. cit., p. 1749.

[53] Sul punto l'Avvocato generale aveva significativamente affermato come "i dati di cui trattasi (..) non sono dati personali nel senso classico del termine, che si riferiscono a informazioni specifiche sull'identità delle persone, ma dati personali, per così dire qualificati, il cui impiego può permettere di creare una mappatura tanto fedele quanto esaustiva di una parte importante dei comportamenti di una persona facenti strettamente parte della sua vita privata, se non addirittura un ritratto completo e preciso della sua identità privata", par. 74.

sensazione di controllo così generata solleva in modo particolarmente acuto la questione del periodo di conservazione dei dati" (par. 72, Conclusioni Avvocato generale, enfasi aggiunta)[54].

Ne derivava che una tale invasività, al fine di essere giustificata e legittima, deve possedere tutti quei requisiti indicati dal già richiamato art. 52 della Carta di Nizza, disposizione che viene posta al centro del vaglio della Corte. Quest'ultima è chiamata quindi a valutare che la limitazione all'esercizio di diritti e libertà posta in essere dalla DRD e dai relativi obblighi in capo ai fornitori di servizi di telecomunicazione sia prevista dalla legge, rispetti il contenuto essenziale dei diritti, nonché rispetti il principio di proporzionalità secondo cui le misure debbono essere necessarie e rispondere a finalità di interesse generale riconosciute dell'UE o all'esigenza di proteggere i diritti e libertà altrui.

Nello svolgere tale complesso vaglio, i giudici hanno saltato quasi totalmente l'esame della 'qualità della legge' – requisito sul quale l'Avvocato generale aveva invece ampiamente concentrato la propria analisi – per focalizzarsi piuttosto sulla valutazione del rispetto del contenuto essenziale dei diritti alla vita privata e alla protezione dei dati. Con riferimento a quest'ultimo requisito, i giudici europei hanno ritenuto che, benché l'ingerenza fosse grave, la conservazione generalizzata non pregiudicasse il contenuto essenziale né relativamente al diritto alla vita privata – poiché non veniva intaccato il contenuto delle comunicazioni – e neppure al diritto alla protezione dei dati in quanto erano predisposte regole a protezione e sicurezza dei dati stessi. Come si avrà modo di vedere più approfonditamente nel prosieguo di questo e nel successivo Capitolo, la lettura avanzata dalla Corte e fondata sulla distinzione tra metadati e contenuto quale elemento determinante al fine di stabilire la sussistenza o meno della lesione del nucleo essenziale dei diritti alla riservatezza e alla protezione dei dati verrà riproposta anche nella sentenza *Schrems*[55] e riconfermata nella successiva pronuncia *Tele2*; una tale posizione tuttavia ha destato non poche perplessità in dottrina quanto alla determinazione del significato da attribuire al concetto di 'contenuto essenziale' e quanto alla compatibilità di una differenziazione metadati-contenuto con la premessa, anche qui evidenziata, della enorme invasività rappresentata dalla raccolta massiva dei soli metadati che permettono di ricostruire, talvolta al pari del contenuto di una comunicazione, la vita privata di un soggetto[56].

---

[54] Merita sottolineare che, con riferimento a tale posizione, espressa sia dall'Avvocato generale che dalla Corte stessa, veniva fatto ampio richiamo alla giurisprudenza della Corte EDU e, in particolare, alle sentenze attinenti al diritto alla vita privata tutelato all'art. 8 della CEDU e che avevano valutato la legittimità di normative nazionali in materia di accesso da parte di autorità nazionali a dati – di diversa natura e più o meno sensibili – relativi ai propri cittadini (ad esempio *Weber e Saravia c. Germania*, n. 54934/00 del 2006 e ancora *S. e Marper c. Regno Unito*, n. 30562/04 del 2008). Come si approfondirà nel Capitolo V, la Corte EDU avrà poi modo, più volte e anche in tempi estremamente recenti, di pronunciarsi sulla tutela della privacy e sulle ingerenze causate da sistemi di sorveglianza – anche riguardanti dati e metadati – adottati dagli Stati per scopi di sicurezza e repressione dei crimini. In questa sede si vuole preliminarmente evidenziare il consolidarsi, in questa pronuncia, della tendenza ad un dialogo e costante rimando tra le due Corti europee – si vedrà poi se ciò verrà mantenuto nel tempo e se l'indirizzo dei due giudici europei verrà mantenuto coerente e convergente –: "the EU Court of Justice used both the parameters of the Charter and those codified by the ECHR, along with the case-law of ECHR-underlining the strong relationship between the two courts and their dialogue in the field of human rights. (..) In this judgement, the CJEU applied the proportionality test as strictly as the ECtHR does in case-law on similar matters. In fact, the CJEU employed principles set forth by the ECtHR, making it clear that, when fundamental rights such as the right to privacy are at stake, any abridgement of these rights should correspond to a 'pressing social need'. Furthermore, proportionality between such pressing need and the measures taken should be demonstrated on the basis of relevant reasons. Treating each and every European citizen as a potential suspect goes far beyond the scope of the global fight against international terrorism. It should, therefore, be rejected: 'taking surveillance measures without adequate and sufficient safeguards can lead to destroying democracy on the ground of defending it' (Klass v. Germany, ECtHR)", A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy. A European perspective*, op. cit., p. 27 e 34.

[55] 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*.

[56] Su questo punto si rimanda più ampiamente al Par. 5 di questo Capitolo nonché al Capitolo III, nel quale l'analisi della importante sentenza *Schrems* permetterà di muovere alcune più puntuali considerazioni sul tema.

Dovendo poi determinare se l'ingerenza perpetrata dalla DRD rispondesse o meno ad un interesse generale, la Corte, quasi con una certa leggerezza, ha in parte rivisto la propria posizione rispetto alla previa sentenza *Irlanda c. Parlamento europeo e Consiglio*, analizzata nelle pagine precedenti: "sebbene la Direttiva sia destinata ad armonizzare le disposizioni degli Stati membri relative agli obblighi dei suddetti fornitori in materia di conservazione di taluni dati da essi generati o trattati, *l'obiettivo sostanziale della Direttiva consiste (..) nel garantire la disponibilità dei suddetti dati a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale. L'obiettivo sostanziale della Direttiva è pertanto quello di contribuire alla lotta contro la criminalità grave e, di conseguenza, in ultima analisi, alla sicurezza pubblica*" (par. 41). Tale finalità, tutelata anche dall'art. 6 della Carta di Nizza che riconosce il diritto alla sicurezza, costituisce un obiettivo di interesse generale dell'Unione[57]. Emerge quindi con forza come, alla base dell'obbligo generalizzato di conservazione imposto dalla DRD, la Corte abbia indicato quale obiettivo 'sostanziale' – quasi vi fosse una distinzione rispetto allo scopo 'formalmente' indicato ovvero quello del funzionamento del mercato interno – quello della repressione della criminalità e, in ultima analisi, della garanzia della sicurezza. Una premessa che pare quindi discostarsi dalle affermazioni della sentenza C-301/06, nella quale invece, dinnanzi alle posizioni di Irlanda e Repubblica Slovacca che ritenevano vero 'centro di gravità' della DRD l'accertamento e perseguimento di reati, i giudici di Lussemburgo avevano individuato quale obiettivo della disciplina europea la tutela del buon funzionamento del mercato interno[58].

2.2.4. – Il delicato vaglio di proporzionalità e necessità della **data retention** *disciplinata nella DRD*

Muovendo dalla significativa constatazione circa la sussistenza di un obiettivo legittimo, sopra indicata, l'ulteriore analisi che la Corte ha sviluppato è quella relativa alla proporzionalità dell'ingerenza, che deve cioè risultare idonea al raggiungimento della finalità indicata nonché necessaria al perseguimento dello scopo stesso. Questi requisiti sono stati però vagliati mediante un controllo giurisdizionale definito 'stretto': la discrezionalità riconosciuta al legislatore europeo, infatti, è da ritenersi più o meno limitata a seconda della natura del diritto, della gravità dell'ingerenza, della finalità e del settore interessato (par. 47). Ebbene nello specifico caso in esame, valutando l'importanza fondamentale della protezione dei dati personali e della garanzia della riservatezza nel panorama europeo nonché la significativa gravità dell'ingerenza rappresentata dalla conservazione generalizzata dei dati, come rilevata dalla Corte stessa, il margine di discrezionalità in capo al legislatore dell'Unione non poteva che essere ritenuto ristretto e il conseguente vaglio dei giudici particolarmente rigido.

Sotto il profilo dell'idoneità al raggiungimento dell'obiettivo, la valutazione della Corte è stata in realtà piuttosto sbrigativa: i metadati conservati rappresentano, a parere dei giudici, una fonte 'supplementare' di informazioni per l'accertamento di reati gravi e la *data retention* non può che essere

[57] "E' giocoforza costatare che la conservazione dei dati per permettere alle autorità nazionali competenti di disporre di un accesso eventuale agli stessi, come imposto dalla Direttiva 2006/24, risponde effettivamente a un obiettivo di interesse generale", par. 44, *DRI*.

[58] Merita tuttavia costatare, sin da ora, come l'Avvocato generale nelle sue Conclusioni avesse evidenziato invece più volte che la Direttiva 24/2006 si caratterizzava per il suo obiettivo primario di armonizzazione delle normative nazionali riguardanti la conservazione dei metadati derivanti da comunicazioni elettroniche. Diversamente dalla Corte che, pur rilevando l'obiettivo di armonizzazione, giungeva poi ad affermare come "l'obiettivo sostanziale della Direttiva consiste nel garantire la disponibilità dei suddetti dati a fini di indagine, accertamento e perseguimento di reati gravi" (par. 41, *DRI*), l'Avvocato generale individuava invece quale primo obiettivo quello di armonizzazione e solo quale secondario quello di stabilire, anche nella sua funzione armonizzatrice, "obblighi, in particolare di conservazione dei dati, che integrano, come mostrerò nel prosieguo, gravi ingerenze nel godimento dei diritti fondamentali garantiti ai cittadini europei dalla Carta" (par. 46, Conclusioni).

considerata, conseguentemente, idonea al raggiungimento dello scopo securitario posto alla base della DRD[59].

Ciò che è stato rilevato invece come problematico e carente nella Direttiva in esame è il requisito della stretta necessità: la Direttiva 2006/24, infatti, vista l'importanza che la tutela dei dati personali rappresenta anche per la garanzia del diritto al rispetto della vita privata – così riconoscendo una sorta di legame, interdipendenza e funzionalità tra gli artt. 7 e 8 della Carta di Nizza –, avrebbe dovuto "prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati" (par. 54). Proprio sotto tale profilo della chiarezza e precisione della normativa, la DRD è stata ritenuta carente e non limitata a quanto strettamente necessario sotto quattro differenti aspetti, che la Corte ha analizzato con attenzione: la disciplina della conservazione, quella dell'accesso nonché la durata della conservazione stessa e le condizioni di sicurezza e protezione dei dati.

Per quanto attiene alla *data retention* e alle modalità e condizioni entro le quali essa è stata imposta, i giudici hanno osservato come la Direttiva obbligasse gli operatori ad una conservazione generalizzata, che riguardava cioè tutti i metadati prodotti da telefonia fissa, mobile, accesso a Internet, posta elettronica, telefonia via Internet, con riferimento poi a tutti gli utenti e tutti gli abbonati, comportando così una "ingerenza nei diritti fondamentali della quasi totalità della popolazione europea" e "senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi" (par. 57). La conservazione, così come prevista nella DRD, non veniva quindi subordinata alla sussistenza di un legame o una relazione tra i dati conservati e una minaccia per la sicurezza pubblica e non veniva neppure richiesto che i soggetti i cui dati erano sottoposti a conservazione si trovassero "anche indirettamente, in una situazione che po[tesse] dar luogo ad indagini penali" (par. 59). Questa specificazione portava la CGUE a stabilire la necessità di una qualche connessione tra ingerenza nella vita privata perpetrata mediante *data retention* e un indizio a carico dei soggetti i cui dati vengono conservati, "tale da far credere che il loro comportamento possa avere un *nesso, anche indiretto o lontano*, con reati gravi" (par. 58, enfasi aggiunta). Veniva richiesta, conseguentemente, una delimitazione dei 'confini' e delle 'dimensioni' della conservazione che, al fine di essere considerata proporzionata e dunque legittima, non poteva assumere carattere generalizzato bensì doveva limitarsi ai soli casi in cui fosse presente una minaccia per la pubblica sicurezza, anche solo in maniera 'blanda' e mediante un collegamento indiretto. Una *retention* legittima, dunque, poteva concretizzarsi in una conservazione limitata ad un determinato periodo di tempo e/o ad un'area geografica determinata e/o ad una cerchia di persone determinate "che possano essere coinvolte, in un modo o nell'altro, in un reato grave, o alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, accertamento o perseguimento di reati gravi" (par. 59). Ciò che pareva emergere dalla sentenza – sebbene sul punto vi sia stata, come si vedrà, una grande incertezza interpretativa – era l'illegittimità di una conservazione generalizzata, così come sancita nella DRD: essa non poteva superare il vaglio di proporzionalità stabilito dall'art. 52 della Carta; ciò che, dal dato letterale della decisione, sembrava risultare una soluzione possibile, proporzionata e legittima, era l'adozione di una c.d. *targeted data retention* – contrapposta alla *bulk data retention* – ovvero una conservazione 'mirata', fondata sulla presenza e sul rispetto di specifici criteri di 'delimitazione' capaci di giustificare l'ingerenza nella sfera privata e nel diritto alla protezione dei dati.

[59] L'Avvocato generale faceva anch'esso sbrigativamente riferimento alla valutazione effettuata dal Consiglio 'Giustizia e Affari interni' che nel dicembre 2002 aveva considerato l'utilizzo dei metadati come uno strumento particolarmente importante ed efficace nella prevenzione dei reati e nella lotta contro la criminalità, in particolare organizzata (par. 44, Conclusioni).

Ma la Corte, piuttosto singolarmente, non si è limitata al vaglio di proporzionalità della disciplina della *data retention*, che la DRD regolava espressamente: lo scrutinio è stato infatti esteso anche alla successiva ed eventuale fase dell'accesso, la cui regolamentazione era lasciata al legislatore nazionale, per espressa indicazione della Direttiva. I giudici avevano rilevato, anche sotto tale profilo, la mancanza di criteri oggettivi capaci di limitare "l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore ai fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la Direttiva 2006/24 si limita invece a rinviare in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno" (par. 60). Veniva dunque criticata e considerata in contrasto con la Carta di Nizza la scelta del legislatore europeo di non stabilire condizioni sostanziali e procedurali a disciplina dell'accesso e di rimettere interamente tale regolamentazione agli Stati membri, con la sola generale indicazione (art. 1, co. 1, DRD) di rispettare i criteri di necessità e proporzionalità[60]. La Corte, pertanto, riteneva necessaria la previsione, in maniera chiara, di criteri oggettivi tali da permettere una limitazione del numero di soggetti autorizzati ad accedere e ad usare i dati conservati; operazioni, queste, che avrebbero dovuto essere consentite solo per quanto strettamente necessario alla luce dell'obiettivo perseguito; l'accesso, in particolar modo, doveva essere preceduto e subordinato ad uno specifico controllo svolto da un giudice o da un'entità amministrativa indipendente, sulla base di una domanda motivata promossa dall'autorità pubblica "nell'ambito di procedure di prevenzione, di accertamento o di indagini penali" (par. 62). La Corte stabiliva così un vero e proprio vademecum di requisiti che dovevano necessariamente essere fissati a livello europeo a disciplina – anche – della fase dell'accesso e che le normative nazionali in materia dovevano essere chiamate a rispettare.

I giudici di Lussemburgo, infine, tornando alla disciplina specifica della conservazione dei dati, hanno analizzato ulteriori due aspetti: quanto alla durata, veniva rilevato come la forbice temporale (6 mesi-24 mesi) fosse fissata dal legislatore europeo senza che fossero precisati criteri obiettivi tali da limitare la durata della conservazione allo stretto necessario e senza che venisse stabilita una distinzione tra tipologie di dati "a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate" (par. 63); quanto poi all'ulteriore profilo della sicurezza e protezione dei dati, le norme della DRD non solo non garantivano tutele sufficienti contro eventuali accessi e usi illeciti dei dati ma neppure la distruzione irreversibile dei metadati stessi al termine della conservazione, né tantomeno l'obbligo di *retention* limitato al solo territorio dell'UE. La possibilità che i metadati venissero trasferiti in Paesi extra-UE comportava una seria restrizione del controllo effettuato da autorità indipendenti, controllo riconosciuto come essenziale al fine di garantire un effettivo rispetto della tutela del diritto alla protezione dei dati personali[61].

---

[60] "L'art. 4 della Direttiva, che regola l'accesso di tali autorità ai dati conservati, non stabilisce espressamente che tale accesso e l'uso ulteriore dei dati di cui trattasi debbano essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative", par. 61.

[61] Anche l'Avvocato generale si era concentrato su questo aspetto rilevando innanzitutto come i dati non fossero sottoposti al controllo delle autorità pubbliche ma restassero conservati dai fornitori di servizi di comunicazione elettronica, "sui quali grava la maggior parte degli obblighi di garantire la loro protezione e la loro sicurezza. La Direttiva impone, è vero, agli Stati membri di provvedere affinché i dati siano conservati in conformità ad essa. È tuttavia interessante osservare che ciò è richiesto solo per permettere che tali dati e ogni altra informazione necessaria ad essi collegata possano essere trasmessi immediatamente alle autorità competenti su loro richiesta" (par. 78). Non vi sono poi nella DRD disposizioni che impongano agli operatori di servizi di telecomunicazioni di conservare i metadati raccolti e relativi ai propri utenti all'interno del territorio degli Stati membri stessi: questa mancata specificazione veniva ritenuta dall'Avvocato generale una "circostanza che aggrava considerevolmente il rischio che tali dati possano essere accessibili o divulgati in violazione di tale normativa" (par. 78). Se è dunque vero da un lato che l'esternalizzazione della *data retention* nei server di operatori privati consente di limitare i rischi di una ingerenza vasta e incontrollata da parte delle autorità pubbliche, è altrettanto vero che ciò aumenta il pericolo di abusi e usi non conformi da parte di ulteriori soggetti, anche esterni all'UE. Sotto questo profilo "the EU judges display an acute awareness of today's global data flows and the possibility for data to reside in cloud

Alla luce di tutte queste considerazioni, che denotavano la mancanza di norme chiare e precise in grado di limitare l'ingerenza nei diritti fondamentali a quanto strettamente necessario, i giudici di Lussemburgo sono giunti ad affermare che la DRD eccedeva i limiti indicati dal principio di proporzionalità e non poteva pertanto che ritenersi invalida[62]. In questo punto conclusivo, pare importante sottolineare come la Corte si fosse distanziata dalla posizione espressa dall'Avvocato generale: quest'ultimo, infatti, pur avendo dichiarato l'invalidità della Direttiva, aveva proposto di sospendere gli effetti di tale decisione "per dar tempo al legislatore dell'Unione di adottare le misure necessarie per porre rimedio all'invalidità accertata, restando inteso che tali misure devono essere adottate entro un lasso di tempo ragionevole" (par. 158)[63]. I giudici di Lussemburgo non hanno accolto tale modulazione degli effetti nel tempo della invalidità della DRD e non ne hanno sospeso dunque l'efficacia immediata.

2.2.5. – La sentenza della CGUE e le posizioni espresse dall'Avvocato generale: alcune significative divergenze

Quella appena indicata non risulta essere l'unica distinzione rinvenibile tra le considerazioni presentate dall'Avvocato generale e le conclusioni della Corte: mentre quest'ultima ha assunto una posizione piuttosto decisa rispetto alla proporzionalità di una *data retention* generalizzata, fissando condizioni e requisiti che *de facto* ne impediscono l'attuazione effettiva, l'Avvocato generale riteneva la DRD invalida per la mancanza di sufficienti garanzie volte a disciplinare la fase dell'accesso ai dati conservati da parte delle autorità nazionali; tali conclusioni risultano di particolare interesse, poiché mettono in luce alcune significative problematiche, già emerse in verità sin dall'approvazione della Direttiva in esame nonché nella previa sentenza della Corte stessa sulla validità della base giuridica. Innanzitutto l'Avvocato generale aveva espresso una posizione differente rispetto a quella netta distinzione tra conservazione ed accesso, proposta nella causa *Irlanda c. Parlamento europeo e Consiglio*: "pur condividendo il punto di vista [dell'Avvocato generale Bot nella citata pronuncia] secondo cui era difficile, quantomeno all'epoca, includere le garanzie relative all'accesso ai dati conservati, nulla ostava a che il legislatore dell'Unione, nel definire l'obbligo di raccolta e di conservazione dei dati, contornasse quest'ultimo di una serie di garanzie sotto forma quantomeno di principi, da sviluppare da parte degli Stati membri, miranti a inquadrare l'uso di tali dati e, con ciò stesso, a definire l'esatta portata e il profilo completo dell'ingerenza che comporta un obbligo siffatto" (par. 124). Si nota dunque come le considerazioni circa l'invalidità della DRD si concentrassero, nella analisi svolta dall'Avvocato generale, unicamente sulla disciplina dell'accesso, ritenendo che i principi fondamentali e le garanzie minime per questa fase dovessero essere stabilite già a livello europeo, pur lasciando ai singoli legislatori nazionali il compito di definire normative di dettaglio; doveva ad esempio essere prevista, a giudizio dell'Avvocato, una descrizione puntuale delle attività criminali che consentono e giustificano l'accesso ai metadati e, conseguentemente, una specificazione maggiore

services worldwide", M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review*, 6, 2014, p. 849.

[62] Dinnanzi alla dichiarazione di invalidità della DRD, le ulteriori questioni promosse dai giudici nazionali nei rinvii pregiudiziali (quali la validità alla luce dell'art. 11 della Carta di Nizza; i rapporti tra l'art. 8 della Carta di Nizza e la Dir. 95/46 nonché le norme della CEDU ed in particolare l'art. 8; la questione se i giudici nazionali debbano vagliare la validità della normativa nazionale di trasposizione della DRD alla luce della Carta di Nizza) non vengono affrontate dalla CGUE.

[63] L'Avvocato generale infatti si riferisce alla possibilità, prevista dall'art. 264, co. 2, TFUE, che concede alla Corte di stabilire e modulare gli effetti nel tempo della dichiarazione di invalidità di un atto normativo e dunque quali effetti debbano considerarsi definitivi, qualora ciò si renda necessario per rispondere ad esigenze imperative connesse alla certezza del diritto.

quanto al significato da attribuire al termine 'gravità' dei reati; dovevano poi essere previste a livello dell'UE disposizioni volte ad 'indirizzare' il legislatore nazionale e ad imporgli la predisposizione di una previa autorizzazione all'accesso ai dati conservati, "riservando tale accesso, se non alle sole autorità giudiziarie, quanto meno ad autorità indipendenti o, altrimenti, subordinando qualsiasi richiesta di accesso al controllo da parte di autorità giudiziarie o di autorità indipendenti" (par. 127).

Sebbene questi punti paiano abbastanza simili a quanto indicato dalla Corte, richiedendo condizioni e requisiti che limitino il rischio di accessi incontrollati, l'Avvocato generale, diversamente dai giudici di Lussemburgo, non aveva preso alcuna posizione quanto alla *data retention* in sé considerata, se non sul fronte della durata della conservazione stessa: partendo dal presupposto che la *retention* – definita con la significativa espressione dell'"accumularsi in luoghi imprecisati del ciberspazio di dati che riguardano sempre persone concrete e determinate" (par. 144) – deve essere considerata come una eccezione, una anomalia che non può essere giustificata se non per il tempo strettamente necessario al raggiungimento di un obiettivo, l'Avvocato generale giungeva alla conclusione che "nessun argomento è stato in grado di persuader[lo] della necessità di prolungare il periodo di conservazione dei dati oltre un anno" (par. 149). Anche questa considerazione quindi sembra distanziarsi da quanto affermato dalla Corte che invece ha ritenuto problematica la cornice temporale della DRD sotto il profilo della mancata previsione di criteri obiettivi volti a determinare la durata e a modularla a seconda dei risultati da raggiungere e dei soggetti coinvolti.

Di rilievo è infine una ulteriore posizione dell'Avvocato generale Villalon, che emerge dalla sua analisi circa la proporzionalità svolta ai sensi dell'art. 5, co. 4, TUE e pertanto differente rispetto al controllo di proporzionalità poi effettuato alla luce dell'art. 52 della Carta di Nizza[64]. Come si è già avuto modo di riportare sopra, la valutazione della Corte circa l'obiettivo primario e principale, individuato nella repressione dei reati gravi, ha posto qualche perplessità rispetto alla coerenza di tale posizione con le conclusioni cui invece erano giunti i medesimi giudici nella analizzata sentenza *Irlanda c. Parlamento europeo e Consiglio*. L'Avvocato generale, sotto tale profilo, ha svolto riflessioni più articolate e meno sbrigative rispetto a quelle proposte dalla Corte, vagliando anche le conseguenze che il propendere per un obiettivo possono comportare rispetto alla corretta individuazione della base giuridica ma anche alla determinazione della proporzionalità della normativa: Villalon ha infatti più volte individuato quale obiettivo formale e preponderante della Direttiva l'armonizzazione delle normative nazionali in materia di conservazione dei dati e la garanzia del buon funzionamento del mercato interno, pur riconoscendo le criticità derivanti da questa constatazione. Se si considera lo scopo legato all'armonizzazione e al mercato unico, viene certamente giustificata l'adozione della Direttiva sulla base dell'art. 95 TCE, confermando così anche la correttezza della precedente sentenza della Corte in materia, che aveva fatto salva, proprio sulla scorta di tale lettura, la validità della base giuridica utilizzata per l'adozione della DRD; di contro però l'Avvocato, svolgendo tale ragionamento, ha ritenuto sussistente una evidente sproporzione, sulla base dell'art. 5 TUE, tra l'intensità dell'incidenza sui diritti fondamentali determinata dall'intervento normativo e la mera finalità di armonizzazione e mercato interno (par. 100). In altre parole, "la Direttiva 2006/24 non riuscirebbe a superare l'esame di proporzionalità per le stesse ragioni che ne giustificavano il fondamento normativo. I motivi che determinano la sua legittimità dal punto di vista del fondamento normativo sarebbero, paradossalmente, i motivi della sua carenza sotto il profilo della proporzionalità" (par. 102). L'Avvocato proseguiva il suo ragionamento ritenendo però che fosse necessario considerare l'obiettivo preponderante e formale come non esclusivo, tenendo quindi conto dell'esistenza di un ulteriore scopo "ultimo" della DRD: la repressione dei reati gravi. Ebbene, osservate da tale prospettiva e per tale finalità securitaria, la

[64] Con riferimento al vaglio di proporzionalità ai sensi dell'art. 52 della Carta di Nizza, infatti, l'Avvocato generale affermava: "ciò che è richiesto in tale contesto non è la proporzionalità come principio generale dell'azione dell'Unione ma, più specificamente, la proporzionalità quale condizione costitutiva per qualsiasi limitazione ai diritti fondamentali", par. 133.

normativa e l'obbligo di *data retention* generalizzata potevano risultare – sulla base del solo art. 5, co. TUE richiamato – adeguate, necessarie e proporzionate. Questo diverso esito del vaglio di proporzionalità a seconda che la DRD fosse considerata alla luce del suo obiettivo principale – quello cioè che la Corte stessa nella sua previa pronuncia del 2009 e l'Avvocato generale avevano individuato nel corretto funzionamento del mercato interno – o del suo obiettivo 'secondario', risulta un aspetto particolarmente critico: "la questione che in definitiva si pone è di stabilire se i problemi di proporzionalità in senso stretto che presenta un atto dell'Unione alla luce dell'obiettivo preponderante da esso perseguito possano essere superati prendendo in considerazione un obiettivo che è posto in 'secondo piano'. La risposta a siffatta questione pare ancor più difficile in quanto essa si presenta in un contesto in cui la validità del fondamento normativo dell'atto considerato è stata riconosciuta proprio in ragione del suo obiettivo preponderante" (par. 104). L'Avvocato generale concludeva e chiudeva la questione ritenendo che la valutazione da effettuarsi sulla base dell'art. 52 della Carta di Nizza non rendesse necessario risolvere in modo definitivo il complesso quesito delineato. Le considerazioni svolte, seppure non definitive, aiutano comunque a comprendere ancor meglio la profondità e rilevanza dei dubbi sorti in seguito alla prima pronuncia *Irlanda c. Parlamento europeo e Consiglio* e le perplessità legate alla duplice finalità perseguita dalla DRD, nonché alla sua corretta base giuridica. La Corte nella sua pronuncia ha deciso invece di distinguere tra 'obiettivo' e 'obiettivo sostanziale' (nella versione inglese 'aim' e 'material objective') e, sulla base di tale distinzione, di valutare la sussistenza o meno di un interesse generale (par. 41): tale approccio, che si è più sopra esaminato, non è certamente in grado di risolvere l'interrogativo posto dall'Avvocato generale e le conseguenze complesse che la determinazione di un certo obiettivo comporta rispetto alla individuazione della base giuridica[65].

Tale ultima questione, dunque, appare, anche nella sentenza della CGUE, piuttosto confusa e, insieme ad altri punti problematici emersi dalla *DRI*, già in parte sottolineati nell'analisi della pronuncia, diventerà uno dei quesiti ricorrenti nei successivi e numerosi rinvii pregiudiziali in materia, rendendo la conservazione dei metadati e il loro utilizzo per scopi securitari una disciplina ancora estremamente controversa e dibattuta.

2.2.6. – Questioni irrisolte e profili problematici della sentenza DRI

Pur dichiarando per la prima volta l'invalidità – totale e senza alcuna restrizione temporale[66] – di un atto dell'Unione europea per contrarietà alla Carta di Nizza, la Corte nella sentenza *DRI* ha dimostrato di spingersi oltre. Nella valutazione circa la proporzionalità e nell'analisi delle carenze e criticità della normativa europea in materia di *data retention*, i giudici di Lussemburgo hanno delineato e stabilito anche precise condizioni e requisiti – quello che alcuni commentatori hanno definito come un vero e proprio vademecum – sia per quanto concerne la disciplina della conservazione che per quella

[65] "Legislative measures based on Art. 114 TFEU [ovvero l'art 95 TCE su cui si fondava la DRD] may pursue twofold objectives, with one being predominant objective and the other being 'a decisive factor in the choices to be made'. This broad reading of art. 114 TFEU seemingly entitles the Court to assess proportionality in light of a measure's secondary objective, in this case security. However, one could question whether the Court's proportionality assessment should be undertaken solely by reference to this secondary objective, particularly given that the Advocate General had opined that a proportionality assessment based solely on the predominant objective would render the Directive invalid", O. LYNSKEY, *The DRD is incompatible with the rights to privacy*, in *Common Market Law Review*, 2014, p. 1802.

[66] Optando per una invalidazione totale e senza restrizioni temporali, la CGUE "ha sollecitato la Commissione e il legislatore UE a ripensare all'intero impianto dell'atto, offrendo peraltro anche indicazioni positive in merito quale, ad esempio, l'introduzione di limiti sostanziali e procedurali alla raccolta, alla conservazione e all'uso di dati personali, nonché norme specifiche per garantire la conservazione sul territorio dell'Unione e dunque in conformità al diritto UE", S. CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del Sistema UE di protezione dei dati*, in *Rivista italiana di Diritto Pubblico Comparato*, 3, 2016, p. 834.

dell'accesso, rivolgendosi, sebbene solo indirettamente, anche ai legislatori nazionali. Così facendo, la Corte ha *de facto* superato quella distinzione in due fasi, conservazione e accesso, che aveva posto alla base del suo ragionamento nella previa pronuncia attinente alla base giuridica: prevedendo i criteri e le condizioni che devono caratterizzare anche l'accesso, i giudici europei si sono inseriti in quell'area della repressione di reati e della garanzia della sicurezza che era stata lasciata, dalla DRD medesima, nelle mani degli Stati membri, riguardando una competenza propria nazionale. Questa posizione si connette inestricabilmente anche con quella relativa all'obiettivo perseguito dalla *data retention* stessa, che non viene più identificato nella garanzia del corretto funzionamento del mercato interno bensì nella lotta alla criminalità; occupandosi anche di accesso e delle sue condizioni, la Corte ha sfumato il confine tra competenze e ambito d'azione dell'Unione europea e aree invece di pertinenza degli Stati membri: pur consapevole della delicatezza della questione e della necessità di non invadere competenze nazionali, i giudici hanno ritenuto che un ampio margine di discrezionalità in capo agli Stati membri quanto alla disciplina dell'accesso avrebbe comportato un serio rischio in termini di rispetto della Carta di Nizza e dei diritti fondamentali, concludendo che fosse quindi compito del legislatore europeo fissare garanzie minime contro il rischio di abusi[67]. Il mero richiamo, effettuato nella DRD, ai principi delineati nel diritto europeo o internazionale pubblico e in particolare nella giurisprudenza della Corte EDU, era stato considerato troppo generico e dai confini vaghi.

Più nella sostanza poi la *DRI* aveva affermato piuttosto frettolosamente sia la distinzione tra contenuto delle comunicazioni e metadati per determinare l'avvenuta lesione del nucleo essenziale del diritto alla vita privata, sia l'idoneità della conservazione generalizzata a raggiungere l'obiettivo della garanzia della sicurezza e di un più efficiente contrasto alla criminalità: entrambe queste posizioni sono state invero, come già visto e come si vedrà anche in seguito, oggetto di critiche[68]; la Corte si è limitata ad affermare come, vista la crescente importanza delle nuove tecnologie e dei dati a disposizione, strumenti di conservazione delle informazioni rappresentino opportunità e potenzialità significative, che le autorità pubbliche non possono ignorare: è stato tuttavia rilevato come sul punto manchi una seria valutazione dell'efficacia della *data retention* generalizzata e che "the Court's failure to rigorously assess the suitability of data retention as a measure to tackle serious crime is regrettable, given the increasingly prevalent use of mass surveillance techiniques by governments and private entities"[69].

---

[67] Nonostante quindi fosse stata promossa una distinzione tra i due momenti e le due ingerenze nella vita privata, la Corte poi sembrava leggere conservazione e accesso come fossero inseparabili, l'uno funzionale all'altro, ritenendo dunque necessari per entrambi la predisposizione di minime garanzie.

[68] Con riferimento al primo profilo, quello della distinzione della ingerenza nei diritti fondamentali a seconda che si tratti di conservazione e accesso ai contenuti o ai metadati, si rimanda al Par. 5 di questo Capitolo nonché a quanto già sottolineato nel Par. 2.2.3.

[69] O. LYNSKEY, *The DRD is incompatible with the rights to privacy*, op. cit., p. 1799. Più avanti nel medesimo contributo, l'autrice afferma come "The Commission's statistical data is not very reliable. Moreover, the data available show significant disparities between the number of requests per Member State (e. g. the Commission's statistics demonstrate that French law enforcement agencies made over 503.000 requests in 2008 while German authorities made just less than 13.000 requests). The Court did not examine these, or other, quantitative data when determining whether data retention is an effective tool for law enforcement purposes. (..) This omission is perhaps explained as reluctance on the Court's part to tread on the toes of the Member States regarding a matter which is deemed to relate closely to national security", p. 1810. La frettolosa analisi di un punto in realtà così estremamente delicato è stata fortemente criticata anche da Guild e Carrera, che hanno richiamato le diverse opinioni elaborate ad esempio dal GEPD: "the necessity of data retention as a law enforcement technique has been contested since its inception. In his opinion on the Commission proposal of 2005, the EDPS (European Data Protection Supervisor) said that he was not convinced by the assumption of its necessity and called for further evidence. In the opinion published in May 2011 on the Commission evaluation report, the EDPS concluded that on the basis of the available quantitative findings it remained doubtful whether the European Commission could conclude that data retention was considered necessary for law enforcement by most member states and there is still a problematic lack of evidence substantiating its value", E. GUILD, S. CARRERA, *The political and judicial life of metadata: Digital Rights Ireland and the trial of the Data Retention Directive*, CEPS Paper in Liberty and Security in Europe, 65, 2014, p. 7.

Quanto invece ai precisi requisiti di legittimità per la conservazione dei dati, la richiesta di un nesso, anche solo indiretto, tra *retention* e reati gravi e dunque una minaccia per la sicurezza pubblica, ha portato alla nascita di considerevoli dubbi sulla accettabilità di una conservazione generalizzata *per se*, sulla sua proporzionalità e sulla sua compatibilità con il diritto europeo. "From the wording of the judgement, it is not fully clear what the position of the Court was: there was indeed the option to think that bulk data retention was prohibited unless it was paired with a strict access regime providing the necessary guarantees"[70]: una lettura meno rigida delle parole della Corte, che non vada nella direzione di considerare totalmente incompatibile col diritto UE la conservazione generalizzata, avrebbe consentito agli Stati membri di ricorrere comunque a tale strumento di repressione e indagine[71], pur circondandolo di ulteriori tutele nella successiva fase dell'accesso.

In conclusione, senza dubbio nella sentenza *DRI*, la Corte ha preso una iniziale posizione rispetto a tutte quelle perplessità già manifestate nel corso degli anni rispetto alla DRD, tanto al momento della sua adozione quanto della sua trasposizione nel contesto nazionale. I giudici di Lussemburgo, similmente a quanto già alcune Corti nazionali avevano sottolineato, hanno ritenuto la disciplina europea carente sotto il profilo della tutela dei diritti e della proporzionalità delle misure adottate. Proprio per questa ragione tale decisione è stata definita un 'landmark case' e accolta come una vittoria per i diritti civili in Europa[72], contribuendo alla "redefinition of the basis of the European integration in favour of constitutionalism and human rights"[73]. Questa sentenza, che ispirerà non solo le successive decisioni della CGUE ma che verrà anche ampiamente richiamata dai giudici nazionali e dalla Corte EDU, ha sicuramente rappresentato un primo profondo e significativo momento di riflessione sull'impatto dei Big Data e delle potenzialità che derivano dall'utilizzo massivo di tali informazioni rispetto ai diritti fondamentali, in particolare della privacy e della protezione dei dati[74]. In questa pronuncia, pur con tutte

---

[70] E. CELESTE, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019. Kuhling e Heitzer hanno similmente affermato come "this decision constitutes remarkable guidelines to be followed by proposed future data retention laws but it also features a weakness: the weighting of every single aspect of this ECJ quintet [con riferimento alle cinque criticità riscontrate dai giudici] is not entirely clear. The Court's ruling may be comprehended in such a way that the five failings in their entirety caused the invalidity of the Directive, but a reading in favour of one individual point of criticism being sufficient is not precluded", J. KUHLING, S. HEITZER, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in *European Law Review*, 2, 2015, p. 266.

[71] Interessante è peraltro sottolineare come i giudici europei nella sentenza parlino anche di 'prevenzione' dei reati e non solo di repressione. La DRD tuttavia stabiliva la conservazione dei dati allo scopo di consentirne la disponibilità e l'uso a fini di 'indagine, accertamento e perseguimento' di reati gravi (art. 1), eliminando qualsiasi riferimento, pur inizialmente promosso dalla Commissione, ad una finalità di prevenzione del crimine.

[72] Sul punto si legga L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the UK after the European Data Retention*, in R. A. MILLER, *Privacy and power. A transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, 2017, che riporta ad esempio le reazioni e dichiarazioni della ONG Privacy International che aveva applaudito la decisione della CGUE come una significativa affermazione, senza precedenti, dell'importanza dei diritti fondamentali alla privacy e alla protezione dei dati.

[73] M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, op. cit., p. 840. Della stessa opinione Nino che afferma: "con tale sentenza la Corte dimostra un atteggiamento particolarmente maturo ed attento verso la tutela dei diritti umani nel contesto europeo, in quanto da un lato sopperisce all'inerzia politica delle Istituzioni europee, che si è concretizzata in un atteggiamento di sostanziale indifferenza del Commissario europeo, in occasione della Conferenza del 2010 sullo stato di applicazione della Direttiva, rispetto alle problematiche sollevate dalla stessa; dall'altro colma le lacune del legislatore UE, assumendosi a tale riguardo una importante responsabilità, in quanto si è dichiarata pronta ad effettuare un controllo giurisdizionale pieno sulla legittimità della Direttiva alla luce del ridimensionamento del potere discrezionale del legislatore comunitario nell'ambito *de qua*", M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Diritto dell'Unione europea*, 4, 2014, p. 825.

[74] Questa pronuncia poi ha segnato anche un importante momento per l'affermazione, più in generale, di un approccio *human rights-oriented* della CGUE stessa: "Until DRI, with few exceptions, the Court had been overall

le zone grigie e le problematiche che sono state rilevate, i giudici europei hanno trasposto i principi di proporzionalità e necessità per cercare di integrare la tutela dei diritti all'interno di misure normative che, pur ponendosi quale obiettivo finale la lotta alla criminalità, non potevano tradursi in una lesione eccessiva ed illimitata dei diritti fondamentali[75]. La Corte dunque ha affermato con forza come anche discipline volte alla garanzia della sicurezza – anche in un momento di allarme e di attenzione elevata dinnanzi alla minaccia terroristica internazionale nonché in un periodo di 'emergenza normalizzata' di cui si è parlato nel Capitolo I, Parte I – non possano sottrarsi ad uno stretto esame di proporzionalità, necessità e compatibilità con la Carta di Nizza. In questo senso, se l'adozione della DRD aveva segnato un passaggio dalla *data protection* alla *data collection* e *retention*, la sentenza *DRI* ha rappresentato invece una sorta di inversione di rotta: da un approccio securitario, che aveva compresso i diritti fondamentali, ad uno invece connotato da un bilanciamento tra tutela della vita privata e protezione dei dati da un lato e raccolta e conservazione massiva dei dati dall'altro[76]. Ecco allora che alcuni commentatori hanno letto nella sentenza analizzata la testimonianza della "ritrovata vocazione costituzionale della Corte di giustizia. Scegliendo di far propri gli argomenti con cui i giudici tedeschi, cechi, bulgari e rumeni hanno a vario titolo bloccato i provvedimenti nazionali di attuazione, i giudici del Lussemburgo non hanno soltanto eliminato una delle più importanti cause di attrito con le giurisdizioni nazionali, ma hanno anche posto le basi per il superamento di una pratica pericolosamente lesiva di basilari libertà individuali e fissato dei limiti precisi per l'eventuale futura adozione di testi normativi in materia di sicurezza"[77]. I giudici di Lussemburgo hanno stabilito una posizione forte "in favor of strengthening privacy protections in the digital age and abandoning sweeping programs of data retention that alter at their roots the relationship between citizens and government in a democratic society, [by redefining] a broad view of the right to privacy and data protection, updating its scope and strengthening its safeguards to face the challenges of the digital age"[78]. È risultata pertanto ampiamente

---

deferential towards EU framework laws, even when directives and framework decisions left room for serious interference with human rights. Its usual technique was to 'pass' these laws and then to instruct the Member States to use their discretionary powers to implement the measure in a manner compatible with EU human rights standards. in contrast, in DRI, the Court of Justice shifts the responsibility to protect human rights onto the EU legislator. When EU legislative acts themselves impose serious interference with human rights, they must, simultaneously, provide for necessary safeguards, expressed in a clear and precise way, to prevent the interference from going beyond what is strictly necessary. If taken up by the EU legislator, this instruction could result in more human rights-loaded EU legislation, which would, incidentally, increase the scope and legitimacy of the Court of Justice's monitoring of corresponding national measures for human rights violations", M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, op. cit., p. 845.

[75] Come ben sintetizzato da Benedizione e Paris, "The DRD case has posed a milestone for the future developments of EU legislation in two key areas of recent emergence: EU anti-terrorism and security legislation and fundamental rights in the framework of new technologies. (..) The CJEU has, with this case, decided a landmark case in the field of rights balancing, asserting that the importance, generality and width of a collective fundamental right such as the one to security is in no case to be considered as allowing for measures disproportionately detrimental to other fundamental rights, such as the ones to privacy and protection of personal data", L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, op. cit., p. 1768.

[76] Alcuni autori non hanno mancato di rilevare in questa pronuncia il rifiuto della Corte di giustizia di forme di sorveglianza massiva e indiscriminata, facendo prevalere o comunque garantendo un maggiore bilanciamento e proporzionalità tra tutela dei diritti fondamentali ed interesse collettivo alla sicurezza: "In fact, the core of the Court's decision lies in the rejection of mass surveillance and in particular indiscriminate monitoring of the entire European population", A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy. A European perspective*, op. cit., p. 27; della stessa autrice anche A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Diritto pubblico comparato ed europeo*, 3, 2014.

[77] F. VECCHIO, *L'ingloriosa fine della Direttiva data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy,* in *Diritti Comparati*, 12 giugno 2014.

[78] F. FABBRINI, *Human rights in the digital age: the European Court of Justice ruling in the Data Retention Case and its lessons for privacy and surveillance in the United States*, op. cit., p. 81.

riconosciuta quella rilevanza del diritto alla protezione dei dati – soprattutto nel contesto della estrema digitalizzazione e della proliferazione dei Big Data – nella sua dimensione di legame e interconnessione con altri diritti fondamentali e con la garanzia di valori e principi democratici.

I giudici inoltre hanno stabilito condizioni che dovranno essere seguite non solo dal legislatore europeo ma anche dai legislatori nazionali: in questo senso, "the decision is not only important in terms of the balance of powers in a horizontal perspective, strenghening the power of the ECJ in relation to the European legislature, but also in a vertical perspective: the normative setting has to be more detailed at a supranational level"[79]. Come si vedrà, infatti, a seguito di questa analisi si sono resi necessari significativi e profondi cambiamenti nella disciplina, tanto europea quanto nazionale, in materia di conservazione dei metadati.

In questa successiva fase, però, le zone grigie e gli aspetti poco chiari o coerenti rilevati in questa decisione, non hanno mancato di creare, soprattutto negli Stati membri, criticità in termini applicativi ed interpretativi: il ruolo di giudice (para-)costituzionale assunto dalla CGUE e il deciso approccio orientato ad una affermazione dei diritti fondamentali si è infatti scontrata con le esigenze concrete delle autorità statali e con la difficoltà di conciliare un elevato standard di tutela della privacy e protezione dei dati con l'efficacia degli strumenti di conservazione e accesso ai dati, nonché con i limiti della struttura europea stessa e della divisione di competenze tra Unione e Stati membri che, come si è già visto e come si vedrà, emergono con particolare forza in un'area normativa di estrema delicatezza. Detto altrimenti, "l'epocale sentenza della Corte di Giustizia, di cui si condivide l'iter argomentativo e motivazionale, che fonda le proprie basi nel percorso già intrapreso da numerose Corti costituzionali europee, si scontra con la complessità dell'attuale società dell'informazione, governata dalla inarrestabile rivoluzione informatica e dalla esasperata velocità evolutiva delle tecnologie, che hanno trasformato i dati e le informazioni in 'beni immateriali' di inestimabile valore. Nell'attuale assetto sociale ed economico il ricorso a strumenti investigativi a 'contenuto tecnologico' e alla *data retention* risulta indispensabile, per prevenire e per accertare gravi reati lesivi di importanti beni giuridici"[80].

Ecco perché, di fronte a queste difficoltà e problematiche interpretative, nonché alla più generale sfida di tracciare un punto di equilibrio tra riservatezza e protezione dei dati da un lato e garanzia della sicurezza dall'altro, che è stata ampiamente illustrata nel Capitolo I, Parte I, le successive reazioni che si sono registrate, a livello nazionale ed europeo, hanno assunto un carattere assolutamente scomposto e disomogeneo, in un panorama complesso e a tratti confuso che perdura sino ad oggi, in quello che vedremo essere un vivace e ancora aperto dialogo tra Stati membri e CGUE in materia.

---

[79] J. KUHLING, S. HEITZER, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, op. cit.; inoltre, "from this point of view, *Digital Rights Ireland* (..) can be understood as instance of a constitutional dialogue between the CJEU and the EU legislature in which the CJEU does not only invalidate a legal measure but also indicates how the legislator could enact valid legislation accomplishing the main objective of the invalidated law", T. OJANEN, *Rights-based review of electronic surveillance after DRI and Schrems in the European Union*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, 2017, p. 27.

[80] R. FLOR, *Dalla 'data retention' al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de jure condendo'*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, 2015, p. 252.

3. – Le reazioni alla sentenza **DRI***: una situazione ancora confusa tra vuoto normativo a livello europeo e ri-espansione del discusso art. 15 Direttiva* **e-Privacy**

3.1. – L'impatto della invalidazione della DRD sulla esistente normativa dell'UE riguardante il trasferimento dati verso Stati terzi e la (non) risposta delle Istituzioni europee

La storica pronuncia *DRI*, che per certe realtà statuali si poneva in perfetta continuità e coerenza rispetto alla giurisprudenza nazionale in materia di *data retention*[81], ha mostrato sin da subito i propri dirompenti effetti sia negli Stati membri che nello stesso contesto dell'Unione europea. La dichiarazione di invalidità della DRD ha imposto, infatti, un ripensamento della disciplina della conservazione dei dati, dei suoi limiti e delle condizioni necessarie affinché potesse essere considerata compatibile con i diritti fondamentali riconosciuti nella Carta di Nizza e nelle Carte costituzionali statali: una seria riflessione sui successivi passi da intraprendere si è quindi resa necessaria sia da parte delle Istituzioni europee, chiamate a valutare se e come colmare il vuoto normativo lasciato dalla decisione della Corte, sia da parte degli Stati membri – legislatori e Corti nazionali – con riferimento alla sorte delle legislazioni statali attuative della disciplina europea invalidata[82].

Prendendo avvio dalle conseguenze venutesi a creare a livello europeo, è innanzitutto da notare come, all'indomani della sentenza *DRI*, la Commissione avesse abbandonato le procedure di infrazione ancora pendenti – di cui si è parlato precedentemente – promosse avverso gli Stati che non avevano adempiuto all'onere di trasposizione nell'ordinamento interno della Direttiva 2006/24[83].

Questo tuttavia non è stato che il primo, e forse più semplice, passo atteso dall'Unione europea: la vera sfida, ben più difficile, era quella di elaborare una nuova regolamentazione della *data retention*, modulata sulla base dei principi e dei criteri indicati dalla CGUE e, al contempo, capace di tenere in considerazione le esigenze securitarie e di efficienza di tale strumento, che pure non potevano essere ignorate. Così, mentre numerosi Stati membri e gran parte della dottrina auspicavano e richiedevano con decisione e urgenza l'avvio di una iniziativa legislativa a livello europeo[84], quello che è invece accaduto

---

[81] Viene infatti osservato come "la pronuncia costituisce l'espressione di un importante dialogo tra corti nazionali e giudici di Lussemburgo, se si considera che la stessa appare fortemente influenzata dagli orientamenti espressi dai tribunali nazionali interni in merito alle problematiche di compatibilità con il diritto alla privacy e il diritto alla protezione dei dati personali sollevate dal regime istituito dalla Direttiva sulla *data retention*. La decisione espressa dalla Corte, in definitiva, ha trovato conferma ma anche supporto nella tendenza emersa nella prassi giurisprudenziale nazionale tesa e rilevare l'illegittimità di tale sistema, alla luce dei diritti fondamentali, così come protetti dalle Carte costituzionali nazionali nonché dall'ordinamento giuridico UE", M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, op. cit., p. 826.

[82] "Adesso però è il momento che anche gli altri attori coinvolti in questa vicenda (istituzioni europee, giudici costituzionali, giudici ordinari, autorità amministrative coinvolte) si assumano fino in fondo le loro responsabilità e provvedano a cancellare definitivamente una pratica tanto pericolosa quanto inquietante", F. VECCHIO, *L'ingloriosa fine della Direttiva data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy,* op. cit.

[83] Questo è il caso, ad esempio, della Germania: come già richiamato in questo Capitolo, la Commissione aveva rinunciato agli atti, ex art. 148 del Regolamento di procedura della Corte di Giustizia, proprio a seguito della sentenza *DRI*.

[84] Nino, ad esempio, ricostruendo i punti essenziali indicati dai giudici di Lussemburgo nella sentenza *DRI*, li ha considerati elementi imprescindibili che non avrebbero potuto essere ignorati dal legislatore europeo nella determinazione di una nuova disciplina della *data retention*: "seguendo tali *guidelines*, potrebbe essere possibile costruire un sistema europeo di *data retention* sostenibile, che da un lato sia in grado di soddisfare adeguatamente le esigenze di sicurezza, nazionale ed internazionale, imposte dalla lotta al terrorismo e alla criminalità organizzata, e dall'altro risulti tale da garantire in maniera effettiva l'osservanza dei fondamentali principi europei sulla protezione della privacy e dei dati personali", M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, op. cit., p. 830. Anche Guild e Carrera (in *The political and judicial life of metadata: Digital Rights Ireland and the trial of the Data Retention Directive*, op. cit.) avevano messo in evidenza la necessità

è stato una completa inazione delle Istituzioni sovranazionali, che, lo si vuole anticipare, perdura sino ad oggi, sebbene negli ultimi anni si sia registrato qualche timido tentativo di riportare il tema all'attenzione del legislatore dell'UE. Sebbene l'allora Commissario europeo per gli Affari Interni Avramopoulos avesse, infatti, annunciato nel 2015 l'apertura di una fase di consultazioni volte a valutare l'opportunità di adozione di una nuova normativa, non molto tempo dopo tale proposito era stato abbandonato: "it has been announced that there will be no legislative initiative on this matter. In the European Agenda on security (2015), the Commission reaffirms the value of communication data for the purpose of an effective prevention and prosecution of terrorism and organized crime but there is no mention of a possible legislative initiative and the Commission simply commits itself to continue monitoring legislative developments at national level and the situation is on hold"[85]. Nonostante le precedenti dichiarazioni, emergeva dunque la chiara scelta della Commissione di non intervenire mediante la predisposizione di una disciplina europea *ad hoc*, limitandosi invece al controllo delle regolamentazioni adottate a livello nazionale: tale approccio, come si avrà modo di vedere, sarà causa di quel panorama normativo confuso e disomogeneo che aveva già spinto in passato alla adozione della DRD.

Se questa cosciente e pensata inazione da parte del legislatore europeo è senza dubbio la reazione più diretta della invalidazione della DRD, pare tuttavia utile e necessario accennare quanto verrà più ampiamente esaminato nel Capitolo III: la pronuncia *DRI*, infatti, pur avendo espresso effetti immediati solo ed esclusivamente con riferimento alla Direttiva 2006/24, ha nondimeno imposto significative riflessioni anche rispetto a tutte quelle normative sovranazionali che implicavano – ed implicano tutt'ora – operazioni di raccolta, conservazione e trattamento di ingenti quantità di dati personali in forma generalizzata. Si pensi, ad esempio, alla disciplina del trasferimento di dati verso Stati terzi sulla base di specifici accordi o decisioni di adeguatezza da parte delle Istituzioni europee, nonché il trasferimento, per scopi securitari, di dati PNR (Passenger Name Records) relativi a tutti i passeggeri di voli aerei in partenza dall'UE e diretti verso Stati terzi. In questi casi, il trattamento e l'invio di tali dati nonché la loro successiva conservazione in territorio extra-UE non erano subordinati all'esistenza di un legame, anche indiretto, con il sospetto di commissione di reati gravi o di minacce alla sicurezza pubblica o nazionale e non era neppure previsto l'obbligo, in capo alle autorità straniere, di garantire quel livello di tutela e protezione che era invece affermato dal legislatore e dai giudici di Lussemburgo entro i confini dell'UE[86]. Ecco dunque che, alla luce della netta posizione espressa dalla CGUE con riferimento alla DRD, iniziavano a sorgere rilevanti perplessità quanto alla compatibilità col diritto europeo di sistemi di trasferimento – e trattamento – dati che non prevedessero, anche per la successiva fase di *retention* nello Stato terzo ricevente, un insieme di regole e garanzie simili a quelle indicate nella pronuncia *DRI*: ci si chiedeva, in altre parole, se anche con riferimento ad accordi quali quello tra UE ed USA per il trasferimento di dati personali (c.d. Safe Harbor) dovessero ritenersi applicabili quei rigidi criteri e

di ricorrere ad un intervento europeo capace di definire con maggiore chiarezza, precisione ed uniformità alcuni degli aspetti più rilevanti della disciplina in materia di *data retention*, quali la definizione di 'crimini gravi' e la reale necessità ed adeguatezza di tale strumento per raggiungere il fine della garanzia della sicurezza e della lotta alla criminalità.

[85] F. GALLI, *Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions*, op. cit., p. 476, che fa riferimento alla dichiarazione della Commissione contenuta della *Agenda europea sulla sicurezza*, COM (2015) 185, final, del 28 aprile 2015.

[86] Altri esempi di normative europee che prevedono forme di conservazione generalizzata sono ampiamente analizzati da F. BOEHM e M. COLE, in *Data retention after the judgement of the Court of Justice of the EU*, op. cit., che richiamano non solo gli accordi di trasferimento dei dati PNR ma anche il sistema Eurodac per il confronto delle impronte digitali dei richiedenti asilo, creato con il Reg. 603/2013, nonché l'accordo tra UE e USA sul trasferimento dei dati di messaggistica finanziaria (Terrorist Finance Tracking Program, TFTP), entrato in vigore nell'agosto 2010. Sul punto si legga anche E. GUILD, S. CARRERA, *The political and judicial life of metadata: Digital Rights Ireland and the trial of the Data Retention Directive*, op. cit.

requisiti delineati con riferimento alla disciplina interna all'UE[87]. Questi dubbi porteranno, come si avrà modo di vedere, ad un ripetuto intervento della Corte di giustizia finalizzato a determinare l'estensione, anche al di là dei confini europei, dei principi sanciti in materia di *bulk data retention*, in quello che alcuni autori hanno definito, con una immagine d'impatto, "Trojan horse effect" della sentenza *DRI*[88].

3.2. – I prorompenti, seppur indiretti, effetti dalla DRI *sul piano nazionale: i differenti approcci degli Stati membri*

Oltre alle esaminate rilevanti conseguenze sul piano europeo, il dirompente effetto della *DRI* si è verificato certamente anche a livello nazionale; giungendo dunque all'analisi delle conseguenze e delle ripercussioni della sentenza analizzata rispetto agli Stati membri, è necessario partire da una significativa affermazione della Commissione europea: "National legislation needs to be amended only with regard to aspects that become contrary to EU law after a judgment by the European Court of Justice. Furthermore, a finding of invalidity of the Directive does not cancel the ability for Member States under the e-Privacy Directive (2002/58/EC) to oblige retention of data"[89]. Da questa frase è possibile muovere alcune importanti riflessioni.

È necessario così partire da una fondamentale e preliminare considerazione, che ben emerge dalla statuizione sopra indicata: la dichiarazione di invalidità di una Direttiva non ha effetti, se non indiretti, sulla legislazione di recepimento a livello nazionale[90]. In altre parole, la sentenza *DRI* non ha avuto alcun impatto automatico sulle normative nazionali in materia di *data retention* adottate quale trasposizione della Direttiva europea. È stato pertanto lasciato all'iniziativa dei singoli Stati membri il compito di valutare la legittimità delle discipline interne, la compatibilità tanto con i diritti garantiti dal

[87] Del resto già in precedenza il Gruppo di Lavoro Art. 29, nel Parere 5/2012 (1 luglio 2012) avente ad oggetto la possibilità di creare un sistema di *Cloud Computing* europeo, aveva avvertito circa i pericoli derivanti da una conservazione dei dati provenienti dall'UE in uno Stato terzo: tale pratica avrebbe impedito alle autorità indipendenti per la protezione dei dati di esercitare qualsiasi forma di controllo sui dati trasferiti una volta superati i confini europei. In questo senso il Gruppo di Lavoro Art. 29 aveva suggerito: "consideration might be given by national governments and European Union institutions to further investigate the concept of a European Governmental cloud as a supra national virtual space where a consistent and harmonized set of rules could be applied. (..) Transferring personal data to a European cloud provider, sovereignly governed by European data protection law, could bring great data protection advantages to customers", come riportato anche da X. TRACOL, *Legislative genesis and judicial death of a directive: the European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it*, in *Computer Law & Security Review*, 30, 2014, p. 745.

[88] Tale efficace espressione è stata utilizzata da Celeste che ha evidenziato come la c.d. *data retention saga* si sia poi espansa in due direzioni, orizzontale e verticale, come meglio si vedrà nel Capitolo III: "in the first case [horizontally] the requirements developed by the Court of Justice could potentially apply to EU acts implying forms of data retention. In the second case [vertically] there is the possibility that the Court's prescriptions will eventually affect other branches of member states' law that presuppose a system of bulk data retention, and in particular those regulating national security authorities", E. CELESTE, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, op. cit. L'autore quindi mette in luce il grande potenziale espansivo della sentenza *DRI*, sia rispetto al diritto dell'UE e dunque a quelle discipline, sopra brevemente indicate, che prevedono forme di raccolta e conservazione generalizzata o ampia di dati, sia rispetto al diritto interno degli Stati membri e a tutte quelle normative che pongono in essere, per finalità securitarie, forme di *data retention* e accesso ai dati da parte di autorità pubbliche.

[89] Così si legge nelle FAQs relative alla disciplina della *data retention*, che la Commissione si era premurata di aggiornare nell'aprile 2014, a seguito della pronuncia della CGUE. Quanto affermato è consultabile all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_269.

[90] "It is the task of national Courts to apply the interpretations suggested by the ECJ to their national rules and, if necessary, to annul them. That might well be the consequence if national implementation laws orient themselves by the wording of the Directive", J. KUHLING, S. HEITZER, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, op. cit., p. 262.

proprio ordinamento quanto col diritto dell'UE, così come interpretato dalla giurisprudenza della CGUE e decidere quindi, in ultima analisi, se mantenerle, modificarle o annullarle, a seconda dell'esito di tale valutazione. In questo contesto, però, il mancato intervento, da parte del legislatore nazionale, di revisione e adeguamento della normativa interna ai criteri delineati dalla CGUE avrebbe potuto portare, come avvenuto in passato, all'avvio di procedure giudiziarie dinnanzi alle Corti nazionali, promosse da ONG, cittadini o aziende interessate nel settore delle telecomunicazioni[91]. I giudici in quel caso non avrebbero potuto ignorare la posizione espressa dalla CGUE in materia di *data retention* e l'interpretazione da essa fornita circa una disciplina della conservazione dei dati compatibile con la Carta di Nizza. L'esito di un tale procedimento quindi avrebbe potuto essere quello di una disapplicazione della normativa nazionale in contrasto con il diritto dell'UE[92] oppure di una dichiarazione di incostituzionalità della normativa nazionale[93]. Tale risultato tuttavia non avrebbe potuto dirsi completamente certo: i dubbi e le 'zone grigie' di questa complessa disciplina, emersi anche nella giurisprudenza europea, avrebbero potuto condurre le Corti ad assumere una differente posizione,

[91] Sotto questo profilo è interessante precisare come soggetti interessati a far valere dinnanzi alle Corti nazionali i principi e le tutele stabilite dalla giurisprudenza europea potrebbero essere anche gli stessi *service providers*: "because companies active in the electronic communications sector are concerned in multiple ways they also could have an interest in bringing proceeding before Courts. On the one hand they are under the obligation to retain data on a massive scale, for which in many cases they have to cover the costs themselves which may be detrimental to their business success. On the other hand, individuals may have justified claims against the companies in view of their retention activities. Therefore, they are in a precarious situation. Complying with the national rules about data retention might lead them to be in violation of EU law. (..) Service providers could further argue that they are no longer bound by the data retention requirements because the still existing national law are inconsistent with supreme EU law. Should they argue like this and star delating the retained data, they may in turn infringe national law with the risk of legal consequences, too", F. BOEHM e M. COLE, in *Data retention after the judgement of the Court of Justice of the EU*, op. cit.

[92] "Judges across Europe, who are requested to apply transposition provisions of the invalid Directive, have to disapply provisions that are no longer in line with European law following the invalidity decision taken by the CJEU. This principle has also been confirmed in the case Aklagaren, according to which there is an obligation for the national courts to disapply 'any provision contrary to a fundamental right guaranteed by the Charter conditional upon that infringement being clear from the text of the Charter or the case-law related to it'", A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy. A European perspective*, op. cit., p. 32.

[93] Come ben riassunto, con riferimento alle leggi nazionali di trasposizione della DRD, "queste ultime non sono automaticamente nulle per effetto della sentenza della Corte, cosicché spetta a ogni Paese membro stabilire la sorte di questi atti. I legislatori nazionali, in virtù della giurisprudenza ERT e del principio di supremazia del diritto UE su quelli interni, si trovano così davanti alla scelta (i) di abrogare le leggi inerenti sistemi nazionali di raccolta dei dati modellati sulla Direttiva annullata, attendendo poi l'iniziativa della Commissione europea in merito o invece (ii) di modificare tali leggi alla luce degli articoli 7 e 8 della Carta così come interpretati dalla Corte nella sentenza *DRI*, nonché degli articoli 13 della Direttiva 95/46 e art. 15 della Direttiva 2002/58. A seguito dell'annullamento della Direttiva 2006/24, infatti, l'applicazione senza adattamento di tali leggi esporrebbe i sistemi interni al rischio sia di procedure d'infrazione sia di ricorsi proposti davanti ai giudici nazionali da propri cittadini, organizzazioni non governative o dalle stesse società attive nel settore delle comunicazioni telefoniche o elettroniche. In tali casi, i giudici interni potranno poi disapplicare tali leggi per incompatibilità con il diritto UE (se direttamente applicabile) o dichiararne, se del caso, l'invalidità per violazione del diritto costituzionale alla protezione dei dati o dell'articolo 8 CEDU, i quali sembrano parimenti configgere con leggi nazionali come quelle in esame", S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di Diritto Pubblico Comparato*, 3-4, 2015, p. 835. Similmente, Boehm e Cole avevano sottolineato come "If States do not react and change their data retention regime that were based on the now void DD, claims before national Courts and/or proceedings in front of the ECtHR (after having exhausted domestic remedies) remain possible within the constraints of the respective national procedural laws. Individuals, NGOs as well as companies may initiate such proceedings claiming a violation of Arts. 7 and 8 CFR, 8 ECHR and the respective provisions of national Constitutions. National Courts confronted with such claims, would then be obliged to review national data retention measures and take EU law, in particular the respective guarantees stemming from Art. 7 and 8 CFR, into account. Therefore, there is a high chance that Courts and Member States will also declare the national transposing act void", F. BOEHM, M. COLE, *Data retention after the judgement of the Court of Justice of the EU*, op. cit., p. 49.

laddove queste non avessero ritenuto, anche sulla base di una lettura meno rigida dei requisiti delineati dalla CGUE, la disciplina statale incompatibile con il diritto dell'Unione e con i diritti fondamentali[94].

Proprio questi scenari, di inazione del legislatore e di successivo intervento dei giudici nazionali, con i due differenti esiti sopra richiamati, si sono rivelati corretti e si sono effettivamente verificati all'indomani della sentenza *DRI*: le risposte degli Stati membri alla invalidazione della DRD hanno presentato caratteristiche anche molto differenti, frutto di quella forte incertezza che si era venuta a creare a seguito del 'vuoto normativo' lasciato dalla pronuncia della CGUE[95].

Seguendo una utile ripartizione delle reazioni a livello nazionale in tre gruppi[96], un primo insieme risulta composto da quegli ordinamenti che avevano cercato di incorporare nella normativa interna i principi e requisiti emersi nella sentenza *DRI* e che avevano comunque reagito alla giurisprudenza della CGUE mediante un nuovo intervento normativo o la modifica della disciplina esistente, su iniziativa talvolta del Governo e talaltra del Parlamento. È il caso del Regno Unito che, dinnanzi alla pronuncia della CGUE, ha reputato opportuno superare la previa *Data Retention Regulation* del 2009, legge di trasposizione della DRD, adottando il *Data Retention and Investigatory Powers Act* (c.d. DRIPA) del 17 luglio 2014, a soli tre mesi dall'intervento dei giudici di Lussemburgo. Con riferimento a tale normativa, che pur si voleva porre come risposta alla giurisprudenza europea e in conformità ad essa, erano in realtà ben presto emersi significativi dubbi circa la sua concreta corrispondenza ai requisiti fissati dalla CGUE: interrogativi ed obiezioni che, come si avrà modo di vedere, sfoceranno in un nuovo rinvio pregiudiziale motivato dall'esigenza di meglio comprendere i limiti di quanto stabilito nella *DRI*. Sebbene non si voglia ora approfondire questo aspetto ed indipendentemente dal fatto che tale intervento normativo potesse considerarsi adottato nella direzione indicata dai giudici di Lussemburgo, resta chiaro come il Regno Unito sia stato uno dei primi Stati membri ad intervenire a modifica del proprio assetto

[94] Come si avrà modo di vedere approfonditamente in seguito, alcune Corti nazionali alle quali era stato sottoposto il vaglio delle normative interne in materia di *data retention* avevano concluso col ritenerle compatibili con i diritti tutelati dalla Costituzione nonché con il diritto dell'UE, la Carta di Nizza e i principi fissati dalla giurisprudenza europea sul punto. Questo esito, lo si vuole sin da ora anticipare, può essere ricondotto ad una lettura più flessibile dei criteri stabiliti dalla CGUE e dunque della proporzionalità di una forma di conservazione dei dati generalizzata; lettura motivata, in taluni casi, anche dalla sussistenza di rigide tutele previste dal legislatore nazionale attinenti alla fase dell'accesso. Non è da escludersi, infatti, come notava anche l'Avvocato generale nelle sue Conclusioni relative alla causa *DRI*, che "alcune discipline nazionali potrebbero essere compatibili alla Carta [di Nizza], nella misura in cui si sono discostate dalla Direttiva 2006/24, attenuandone le criticità. L'Avvocato generale, ad esempio, ha affermato che, alle insufficienti garanzie offerte da detta Direttiva in materia di accesso ed impiego dei dati raccolti, potrebbe essere stato posto rimedio nell'ambito delle misure di trasposizione adottate dagli Stati membri (punto 157, quarto periodo). Del pari, nelle conclusioni si evidenzia la 'moderazione' con cui gli Stati membri hanno esercitato le proprie competenze nel disciplinare la durata massima del periodo di conservazione dei dati (punto 157)", A. ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014, p. 723; questo approccio, che mira ad affermare come le normative nazionali di trasposizione della DRD non debbano necessariamente ed automaticamente essere considerate incompatibili con la Carta di Nizza, si basa però su una interpretazione della posizione della CGUE nella sentenza *DRI* meno rigida, che non bandisce cioè *in toto* e *per se* una forma di conservazione generalizzata dei metadati. Come vedremo, proprio questa tipologia di interpretazione porterà ad una grande disomogeneità nelle reazioni degli Stati membri nonché alla necessità di un nuovo intervento della CGUE.

[95] Proprio di 'incertezza giuridica' parla Vecchio, che nota come "se ci [potevano] essere ben pochi dubbi che i giudici irlandesi e austriaci [avrebbero provveduto] presto a bloccare l'efficacia delle rispettive normative interne e a riordinare il quadro normativo e se ci [potevano] essere pochi dubbi sul fatto che anche la Corte costituzionale slovena (che, in attesa della pronuncia del giudice europeo sulla validità della Direttiva, aveva sospeso il procedimento di controllo di costituzionalità dell'atto interno) [sarebbe arrivata] ad una celere definizione della questione, in tutti gli altri Paesi membri ci si [sarebbe trovati] di fronte ad una grave situazione di incertezza giuridica", F. VECCHIO, *L'ingloriosa fine della Direttiva data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy,* op. cit.

[96] J. KUHLING, S. HEITZER, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, op. cit.

normativo, basato sulla disciplina dalla invalidata DRD[97]. Allo stesso gruppo appartiene il Lussemburgo, in cui una nuova normativa in materia di *data retention* era stata prevista, su iniziativa del Ministro della Giustizia, nel 2015. Molto interessante e degna di menzione è anche la legge adottata dalla Germania che, come analizzato nei previ paragrafi, si è mostrata molto attenta alla disciplina della *data retention* sin da prima che la CGUE intervenisse con la sentenza *DRI*. La normativa adottata nell'ottobre 2015[98] rappresenta, a parere di molti commentatori, un serio tentativo di trasporre, nel contesto nazionale, le indicazioni espresse dai giudici di Lussemburgo: il periodo di conservazione era stato così limitato ad una forbice di 4-10 settimane a seconda della tipologia di dati interessati; era stato previsto un previo vaglio effettuato da un giudice volto ad autorizzare l'accesso da parte di autorità pubbliche; le categorie di dati conservati erano state ristrette mediante l'esclusione dei dati derivanti da e-mail; erano inoltre introdotte nuove misure a garanzia della sicurezza dei dati, per esempio limitando i soggetti abilitati all'accesso; era imposto l'obbligo di conservazione unicamente nel territorio tedesco. Questa normativa quindi pareva "at first glance, to be a serious effort to meet the requirements set by the Karlsruhe and Luxembourg Courts. It does not however, address the major issue raised by the CJEU in paras. 57-59 of *DRI*: blanket retention of all users of telecommunication without any limitation based on suspicion, geography, time or group"[99], evidenziando così come anche questa disciplina, per quanto attenta al rispetto dei requisiti fissati nella *DRI* e piuttosto restrittiva nella fase dell'accesso, non era purtuttavia giunta ad interpretare in maniera rigida la posizione della CGUE in materia di *data retention*, non prevedendo quindi una esclusione della conservazione generalizzata.

Il secondo insieme di Stati giunge ad un risultato simile a quello caratterizzante il primo gruppo, ovvero il superamento della esistente normativa in materia di *data retention*, prodromico all'adozione di una nuova disciplina di 'rottura' rispetto a quella precedente: tale esito tuttavia emergeva non come frutto dell'intervento del legislatore bensì a seguito della posizione espressa da una Corte nazionale. In tale raggruppamento infatti si ritrovano quegli Stati che, nel silenzio del legislatore o nell'inazione del potere esecutivo statale, avevano conosciuto un mutamento dell'assetto normativo grazie all'azione dei giudici nazionali, che arrivavano a dichiararne l'incompatibilità rispetto ai diritti sanciti a livello interno nonché a quelli stabiliti a livello europeo, secondo l'interpretazione fornita dalla CGUE. Ci si riferisce, ad esempio, ad Austria, Belgio, Olanda, Polonia, Romania e Slovenia[100], le cui Corti, la maggior parte

---

[97] Sul punto, si entrerà più ampiamente nel dettaglio nella Parte III, nella quale attenzione specifica verrà dedicata alla disciplina normativa e agli interventi giurisprudenziali caratterizzanti il Regno Unito in materia di *data retention*.

[98] *Gesetz zur Einfuhrung einer Speicherflicht und einer Hochstspeicherfrist fur Verkehsdaten*, 26 ottobre 2015. Per approfondimenti su tale normativa, si rimanda più ampiamente a S. SCHWEDA, *Parliament adopts new data retention law*, in *European Data Protection Law Review*, 1, 2015, pp. 223-226.

[99] N. VAINIO, *Fundamental rights compliance and the politics of interpretation: explaining Member State and Court reactions to Digital Rights Ireland*, in T. BRAUTIGAM, S. MIETTINEN (a cura di), *Data protection, privacy and European regulation in the digital age*, Unigrafia, 2016, p. 245.

[100] La Corte costituzionale austriaca si era pronunciata nel caso G 47/2012-49, il 27 giugno 2014, dichiarando l'illegittimità della normativa in materia di *data retention*; la Corte costituzionale belga era intervenuta l'11 giugno 2015 annullando la Loi du 30 juillet 2013 in materia di *data retention*; la normativa olandese è stata invalidata da una ordinanza di un tribunale olandese nel 2015; il Tribunale costituzionale polacco si era pronunciato, nello stesso senso, il 30 luglio 2014 (caso K 23/11); la Corte costituzionale romena con decisione n. 40 del 8 luglio 2014 si era nuovamente pronunciata sulla normativa nazionale attinente alla conservazione dei dati, ritenendo tale regime ancora una volta incostituzionale; la Corte costituzionale slovena, nel caso U-I-65/13-19, deciso il 3 luglio 2014 – dopo la sospensione decisa dai giudici stessi e volta ad attendere la sentenza della CGUE sulla DRD – aveva dichiarato l'illegittimità costituzionale delle disposizioni regolanti la conservazione generalizzata di metadati, ordinando anche la cancellazione di tutti i dati conservati sulla base di tale normativa. Per approfondimenti su tali pronunce e sulle reazioni degli Stati membri, si rimanda a: L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, op. cit., p. 1764 ss.; ma anche N. VAINIO, S. MIETTINEN, *Telecommunications data retention after DR: legislative and judicial reactions in the Member States*, in *International Journal of Law and Information Technology*, 23, 2015.

delle volte costituzionali, avevano affermato l'incostituzionalità – totale o parziale – delle disposizioni statali attuative della DRD. La necessità, registratasi in questi Stati, di ricorrere alla valutazione forte e decisa del giudice interno aiuta a comprendere come la reazione delle autorità nazionali alla sentenza *DRI* non sia sempre stata pronta e spontanea bensì abbia richiesto l'attivazione di soggetti interessati, per avviare un processo di cambiamento e superamento dell'assetto precedente, mettendo così in luce una certa reticenza – o difficoltà – del legislatore nazionale ad intervenire su questa delicata disciplina.

L'ultimo insieme di Stati si caratterizza infine per non aver provveduto, in alcun modo, a modificare la normativa interna: salvo alcune eccezioni[101], negli ordinamenti rientranti in questo gruppo la scelta di mantenere intatta la legislazione di recepimento della DRD si è registrata a seguito di una forma di controllo circa la compatibilità della normativa esistente rispetto ai criteri indicati dalla giurisprudenza europea in materia, esercitata mediante l'intervento dei giudici nazionali oppure ad opera di soggetti o organismi ad hoc cui era stato attribuito tale specifico compito di valutazione. Al termine del controllo e diversamente dal primo e dal secondo gruppo, le autorità preposte erano giunte ad una considerazione di conformità della disciplina interna sulla conservazione dei metadati e dunque al suo mantenimento in vita, senza bisogno di alcun intervento o modifica. È il caso della Danimarca e della Svezia che, dopo aver sottoposto la normativa in materia di *data retention* a controlli e valutazioni effettuate da apposite commissioni governative o esperti specificamente individuati, avevano ritenuto la leggi statali in linea con la giurisprudenza europea e rispettose dei diritti fondamentali[102]. O ancora è il caso di Ungheria, Spagna e Cipro, le cui Corti avevano ritenuto il regime di conservazione dei dati fissato in epoca precedente all'intervento dei giudici di Lussemburgo come compatibile con quanto emerso dalla sentenza *DRI*[103].

[101] Merita infatti rilevare come in alcuni degli Stati rientranti in questo ultimo gruppo, quali Croazia, Italia e Portogallo, non si fosse registrato né un intervento dei giudici nazionali né del legislatore o del Governo finalizzato a vagliare, ed eventualmente modificare, la normativa esistente in materia di *data retention*. Il risultato di mantenere immodificata la disciplina precedente alla sentenza *DRI* era stato pertanto ottenuto non da una decisione attestante la legittimità e compatibilità della regolamentazione statale bensì da una totale inazione di tutte le autorità nazionali e una mancata attivazione del controllo giudiziario.

[102] L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, op. cit., p. 1767. Con riferimento alla Svezia ad esempio è interessante notare come "In a first response to the annulment of the DRD, the Swedish Post and Telecom

Authority stopped enforcing their implementation law and apparently tacitly approved the Swedish internet service provider deleting all data that has been stored on the grounds of data retention law. However, after scrutinizing more precisely the requirements determined by the ECJ in *DRI*, the Swedish authorities changed course. In August 2014, they started to enforce unaltered data retention law and instructed providers to start retaining data again", J. KUHLING, S. HEITZER, *Returning through the national back door?*, op. cit., p. 275. Come vedremo, proprio tale decisione del governo svedese sarà alla base del successivo e ulteriore intervento della CGUE in materia di conservazione dei dati.

[103] È quanto risulta dal Report predisposto dalla ONG Privacy International, *National Data Retention Laws since the CJEU's Tele2/Watson judgement*, del settembre 2017. Secondo tale documento, questa inazione e mantenimento invariato delle normative nazionali, nonostante la posizione espressa dalla CGUE, è da considerarsi fortemente preoccupante: "the most concerning fact is that in an alarmigly large number of Member States (roughly 40% of all Countries surveyed in this report) the pre-*DRI* regime transposing Directive 2006/24 is still in place", p. 13. Bisogna comunque sottolineare come alcune Corti nazionali, pur ritenendo la normativa in materia di *data retention* legittima e proporzionata, avessero stabilito l'importanza di talune tutele e garanzie più stringenti nella fase dell'accesso: è il caso di Cipro, la cui Corte Suprema aveva dichiarato necessaria l'esistenza di un controllo giudiziario preventivo all'accesso ai dati.

3.3. – Un panorama disomogeneo e frammentario quale risultato delle 'zone grigie' lasciate dalla pronuncia **DRI***: il venir meno dell'obbligo di conservazione dei dati dettato nella DRD e l'art. 15 Direttiva* **e-Privacy**

Dinnanzi alle reazioni sopra esaminate, che mettono in evidenza le problematiche applicative ed attuative dell'interpretazione fornita dalla CGUE e dei principi da essa stabiliti, può essere condiviso il pensiero espresso dalla ONG Privacy International nel Report redatto nel 2017, nel quale viene sottolineato, con preoccupazione, come "It is evident that in most of the countries Privacy International has surveyed, change is being promoted through litigation by human rights NGOs instead of through proactive reform of the laws by Parliament. Legal proceedings are currently under way in about 35% of all Countries considered (..). Nonetheless, in the course of these proceedings we have seen some alarming attempts by Governments to water-down the CJEU's judgements through improper interpretation"[104].

Volendo così trarre alcune considerazioni dalla ricognizione sin qui svolta, emerge da un lato la difficoltà e, per certi versi, reticenza delle autorità governative ad applicare quelle garanzie e limitazioni stabilite nella *DRI* ai sistemi di conservazione di dati: garanzie che, come già evidenziato, avrebbero finito inevitabilmente col comprimere efficacia ed utilità di tali strumenti, ritenuti imprescindibili e irrinunciabili 'armi' per la lotta e indagine alla criminalità organizzata[105]. Dall'altro lato, sul fronte giurisprudenziale, si registra una disomogenea risposta delle Corti nazionali chiamate ad intervenire a

---

[104] PRIVACY INTERNATIONAL, *National Data Retention Laws since the CJEU's Tele2/Watson judgement*, op. cit., p. 13. Anche Kulhing e Heitzer, nelle proprie considerazioni, affermavano come "the ECJ judgement, owing to its vagueness regarding the weight of the single failing, could not eliminate the longstanding legal uncertainties accompanying data retention law. Admittedly, other MSs such as Slovakia have proceeded more carefully and have decided to suspend enforcement of data retention law until the final juridical decision on a national level, but for many EU citizens the actual data retention situation has so far remained unchanged", J. KUHLING, S. HEITZER, *Returning through the national back door?*, op. cit., p. 276.

[105] Sul punto pare di estrema utilità ricostruire quanto riportato da Eurojust all'esito del *Consultative forum of Prosecutors General and Directors of Public Prosecutors of the MSs of the EU* e del *Workshop on data retention in the fight against serious crime: the way forward*, tenutisi il 11 dicembre 2015. Nel Report adottato a conclusione di tali eventi, emergono con chiarezza le difficoltà applicative riscontrate dalle autorità di *law enforcement* a seguito della sentenza *DRI* e delle reazioni adottate a livello nazionale: "where national data retention laws have been struck down, access by law enforcement agencies to retained data is limited or non-existent given that there is no longer an obligation for telecommunication service providers to retain data or because this obligation covers only certain categories of data"; a ciò è da aggiungere un ulteriore aspetto di grande rilievo: "challenges to the admissibility of evidence have been lodged in some Member States". Considerate tutte queste complicazioni e la disomogeneità delle discipline vigenti nei diversi Stati membri all'indomani della decisione *DRI*, "the Consultative Forum calls for an EU solution on data retention. A European common framework to harmonise retention of, and access to, data is deemed necessary. The Forum therefore invites the EU Commission to take action in this regard in line with the requirements established by the CJEU in *Digital Rights Ireland*". La richiesta dei rappresentanti delle forze investigative presenti al Forum, peraltro conformemente alla posizione espressa da molti Governi degli SM, era dunque quella di ristabilire un obbligo di *data retention* generalizzata a livello europeo, prevedendo idonee garanzie nella successiva fase di accesso e determinando una durata di conservazione uguale per tutti. La *bulk data retention* era considerata uno strumento tanto essenziale quanto non lesivo dei diritti alla privacy e alla protezione dei dati: "retention of bulk electronic communication for criminal justice puroposes must be distinguished from bulk surveillance of data for national security purposes. (..) Generalized data retention schemes are important, if not essential, for the investigation and prosecution of serious crimes. Data retention must be carried out in a generalized manner as it is impossible to know beforehand whose data will be relevant in the course of a specific criminal investigation prosecution. Generalised data retention is not only a useful tool to link suspects to an offence, but also to delink suspects from an offence. There are no equally effective alternatives to data retention. Metadata that are generated by telecommunications (e.g. traffic data, location data and other customer related data) are often the only way to identify a suspect or their whereabouts. These data can also be crucial to decide in a specific case whether it is justified or not to use more intrusive surveillance tools such as telephone interception". Sulla base di queste considerazioni, si comprende quindi la reticenza e la resistenza mostrata verso l'attuazione delle limitazioni indicate dalla CGUE nella sua sentenza.

seguito della invalidazione della DRD: queste infatti hanno mostrato approcci fortemente diversi, talvolta in linea con l'indirizzo dei giudici di Lussemburgo, mediante l'adozione di un rigido vaglio di proporzionalità e stretta necessità delle normative nazionali e della sussistenza dei criteri indicati dalla Corte europea; talaltra invece adottando una lettura meno rigida rispetto a quella fornita a livello europeo, giungendo dunque a far salve, in toto o in parte, le normative nazionali in materia di *data retention* generalizzata, adottate sulla base della DRD, considerandole conformi ai requisiti sanciti a livello sovranazionale.

Si vengono così a distinguere quelle che Vanio e Miettenin descrivono come "permissive interpretation" e "strict interpretation" di quanto sancito nella sentenza *DRI*[106]: la prima tipologia di interpretazione mirava a far salva la conservazione generalizzata purché essa fosse accompagnata da idonee garanzie nella fase di accesso successiva, ritenendo quindi i criteri delineati dalla Corte come non cumulativi e non necessari nella loro totalità; l'invalidità determinata dalla CGUE infatti derivava, secondo tale linea interpretativa, non dalla esistenza di una *bulk data retention*, bensì dalla sussistenza di tale forma di conservazione unitamente alla mancanza di adeguate salvaguardie quanto all'accesso e alla sicurezza dei dati. Era quindi nella assenza di adeguate tutele che doveva individuarsi l'incompatibilità col diritto dell'UE della DRD nel suo complesso.

L'interpretazione restrittiva invece riscontrava nella posizione dei giudici di Lussemburgo una chiara dichiarazione di invalidità *tout court* della conservazione generalizzata che, per sua natura, non poteva essere considerata compatibile con il principio di proporzionalità e stretta necessità.

Del resto, è proprio nelle 'zone grigie' lasciate dai giudici di Lussemburgo e negli aspetti problematici emersi dalla sentenza *DRI*, sottolineati nei paragrafi precedenti, che si devono individuare le ragioni della diversità di interpretazioni e reazioni sopra analizzate: "the CJEU leaves open the conditions that are absolutly required for proportionality: is it all conditions listed in *DRI* or just some of them? (..) Vagueness of the judgement leaves these MSs room to argue their implementation is proportionate because it addresses some of the worries the Court listed"[107].

Da questo primo ordine di riflessioni, che ha permesso di fotografare il panorama europeo all'indomani della storica pronuncia della CGUE, bisogna però muovere una seconda considerazione: la diretta conseguenza prodotta dalla *DRI* è stata il venir meno dell'obbligo introdotto dal legislatore europeo con la DRD, che, come noto, stabiliva in capo agli Stati membri l'onere di prevedere disposizioni interne tali da imporre agli operatori di servizi di telecomunicazione la conservazione generalizzata dei metadati dei propri utenti. L'introduzione di un obbligo di *data retention* tornava quindi ad essere uno strumento di lotta alla criminalità non più imposto bensì volontariamente adottabile dai singoli Stati sulla base del 'redivivo' art. 15 della Direttiva *e-Privacy*. Proprio quest'ultima disposizione tornava ad essere, in assenza di una nuova normativa specifica, l'unica indicazione europea a disciplinare la possibilità per gli Stati di adottare normative in materia di conservazione di metadati per scopi securitari. Conseguentemente, dopo l'invalidazione della DRD, nel caso in cui uno Stato membro avesse deciso di predisporre una tale disciplina, essa sarebbe rientrata nell'ambito di applicazione dell'art. 15 citato. Come già analizzato nel Capitolo I, questa eccezione rispetto alla regola

---

[106] Secondo l'approccio 'permissivo', "the observations Court makes in paragraphs 57-68 are a checklist of changes that would make the law proportionate, but it is not an absolute list. Yet, the basic undertone of the judgement nonetheless seems to be that some form of mandatory data retention in order to combat serious crime and terrorism might indeed be compatible with the EU Charter of Fundamental Rights. According to the strict interpretation, the ruling in practice forbids any indiscriminate blanket data retention per se by requiring that the retained data must have a connection to serious crime and terrorism", N. VAINIO, S. MIETTINEN, *Telecommunications data retention after DR: legislative and judicial reactions in the Member States*, op. cit., p. 300. In questo senso gli autori hanno ritenuto generalmente – anche se non sempre, come si è visto – che le Corti degli Stati membri avessero adottato una interpretazione 'rigida', mentre quella 'permissiva' fosse interpretazione tipica dei Governi nazionali.

[107] N. VAINIO, *Fundamental rights compliance and the politics of interpretation: explaining Member State and Court reactions to Digital Rights Ireland*, op. cit., p. 249.

generale di cancellazione e anonimizzazione dei metadati era però concessa solo per specifiche finalità (salvaguardia della sicurezza nazionale, difesa e sicurezza pubblica, prevenzione, ricerca, accertamento e perseguimento di reati) e nel limite di quanto necessario, opportuno e proporzionato all'interno di una società democratica. Tali requisiti e criteri, lo si ricorda, erano stati però sin dall'inizio considerati estremamente vaghi e generici, così come eccessivamente ampio era stato ritenuto il richiamo ai principi generali del diritto comunitario. A seguito dell'entrata in vigore del Trattato di Lisbona nonché in particolare successivamente alla sentenza *DRI*, tuttavia, i requisiti inseriti nell'art. 15 avrebbero dovuto riempirsi di più precisi contenuti e significati, da rinvenirsi non solo nei diritti riconosciuti dalla Carta di Nizza e aventi valore parificato a quello dei Trattati ma anche nell'interpretazione di essi fornita dalla Corte di giustizia nella sua giurisprudenza[108]. Proprio con riferimento a questo aspetto, si giunge alla terza ed ultima considerazione che da questo panorama normativo può essere tratta: sebbene sia vero che l'intervento della Corte di giustizia aveva delineato condizioni e requisiti della disciplina della *data retention*, che ben potevano essere estesi ed applicati anche all'adozione di normative nazionali attuative dell'art. 15 Direttiva *e-Privacy*, è altrettanto vero che quelle 'zone grigie' e quei dubbi riscontrati nella posizione espressa dai giudici di Lussemburgo erano inevitabilmente destinati a riflettersi anche sull'interpretazione dell'art. 15 stesso, determinando quindi una nuova situazione di incertezza e di disomogeneità nel panorama europeo, proprio come avvenuto prima della adozione della DRD. In estrema sintesi, "despite *DRI* being an important milestone, it did not end data retention. (..) The judgement leaves room for the MSs to interpret it according to their needs"[109] e non risultava pertanto in grado di rappresentare un punto risolutivo di quei dubbi che si era registrati rispetto all'art. 15, anche prima dell'adozione della DRD. Come Rauhofer e Sithigh avevano preannunciato, l'intervento della CGUE e la "ri-espansione" dell'ambito di applicazione dell'art. 15 Direttiva *e-Privacy* avevano infatti portato ad un nuovo "sustained period of legal uncertainty", con l'avvertimento che "the prudent MSs should hesistate before readopting provisions along the lines of the now invalid Directive"[110].

[108] In realtà, tale visione non era totalmente condivisa e pacifica. Come si vedrà anche nel prosieguo di questo Capitolo, vi erano dubbi quanto al fatto che i criteri indicati dalla CGUE nella sentenza *DRI* e, più genericamente, la garanzia dei diritti fondamentali sancita dalla Carta di Nizza fossero applicabili anche alle normative adottate sulla base della facoltà derogatoria prevista dall'art. 15 Direttiva *e-Privacy*. Tale dubbio originava dalla considerazione secondo cui la previsione di una conservazione dei dati per scopi securitari attiene alla sfera del trattamento di dati per finalità di sicurezza pubblica e nazionale, la cui disciplina viene lasciata agli Stati membri sulla base sia dell'art. 1, co. 3 della Direttiva e-*Privacy* stessa ("La presente Direttiva non si applica alle attività che esulano dal campo di applicazione del trattato che istituisce la Comunità europea, quali quelle disciplinate dai titoli V e VI del trattato sull'Unione europea né, comunque, alle attività riguardanti la sicurezza pubblica, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) o alle attività dello Stato in settori che rientrano nel diritto penale") che dell'art. 13 della Direttiva 95/46/CE, già in precedenza richiamato. Considerando le normative nazionali in materia di *data retention* adottate sulla base dell'art. 15 come non rientranti nell'ambito di applicazione del diritto dell'UE, ne deriverebbe una conseguenza di grande impatto: la non applicabilità e vincolatività della Carta di Nizza la quale, come espresso dall'art. 51, "non estende l'ambito di applicazione del diritto dell'Unione al di là delle competenze dell'Unione, né introduce competenze nuove o compiti nuovi per l'Unione, né modifica le competenze e i compiti definiti nei trattati". Ciò comporterebbe quindi che la tutela dei diritti e l'interpretazione fornita dai giudici di Lussemburgo non dovrebbe limitare la disciplina nazionale adottata ex art. 15. Questo punto resterà estremamente dibattuto e, come si avrà modo di vedere, non mancherà di essere evidenziato nei rinvii pregiudiziali in materia promossi, a seguito della sentenza *DRI*, dinnanzi alla CGUE.

[109] N. VAINIO, S. MIETTINEN, *Telecommunications data retention after DR: legislative and judicial reactions in the Member States*, op. cit., p. 308.

[110] J. RAUHOFER, D. MAC SITHIGH, *The data retention directive never existed*, in *Scripted* n. 118, 2014, citato da L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the UK after the European Data Retention*, in R. A. MILLER, *Privacy and power. A transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, 2017.

Ecco perché, dinnanzi a questa situazione piuttosto confusa[111], una strada percorribile diveniva quella di chiedere nuovamente l'intervento della Corte di giustizia dell'UE al fine di ottenere chiarimenti in merito all'interpretazione ed applicazione dell'art. 15 Direttiva *e-Privacy*: in tal modo si sarebbe offerta ai giudici di Lussemburgo la possibilità di spiegare se e come i criteri indicati nella *DRI* con riferimento alla disciplina europea potevano o dovevano essere applicati anche alle normative nazionali attuative di quella facoltà derogatoria garantita – a determinate condizioni – dall'art. 15 stesso.

4. – La CGUE chiamata nuovamente a pronunciarsi in materia di data retention: *la sentenza Tele 2 Sverige e Watson*

4.1. – I rinvii pregiudiziali promossi dai giudici di Svezia e Regno Unito: la richiesta di un intervento chiarificatore circa l'applicazione dell'art. 15 Direttiva e-Privacy *e l'impatto della sentenza* DRI

Dalla situazione esaminata nel precedente paragrafo diviene evidente come il panorama venutosi a creare all'indomani della sentenza *DRI* fosse fortemente complesso: l'analisi delle differenti reazioni degli Stati membri hanno messo in luce come i dubbi e i quesiti apertisi in materia di *data retention* sin dalla DRD fossero da considerarsi tutt'altro che risolti. La riluttanza a sacrificare sistemi di conservazione generalizzata in nome della tutela dei diritti fondamentali e del rispetto dei principi di proporzionalità e necessità si scontrava con una giurisprudenza – e una società civile – fortemente attenta ad evitare che l'utilizzo di strumenti di repressione dei reati potessero tradursi in disastrose derive di sorveglianza massiva. È in questo contesto che le Corti nazionali del Regno Unito e Svezia hanno richiesto l'ulteriore intervento della CGUE nei rinvii, poi riuniti, C-203/15 *Tele2 Sverige AB c. Post- och telestyrelsen (PTS)* e C-698/15 *Secretary of State for the Home Department c. Tom Watson et al.*, aventi ad oggetto l'interpretazione dell'art. 15 della Direttiva e-*Privacy* letto alla luce degli artt. 7, 8 e 52 della Carta di Nizza: le significative incertezze applicative di tale disposizione, in grado – come si vedrà – di creare forti problemi anche agli operatori economici, sono state alla base dei quesiti posti nei rinvii pregiudiziali, volti essenzialmente a comprendere l'estensione dei requisiti indicati nella giurisprudenza europea richiamata, sia per quanto attiene alla fase di conservazione che a quella di accesso[112].

Prendendo avvio da una breve analisi dei casi dai quali la sentenza della CGUE ha avuto origine, il rinvio proveniente dalla Svezia è scaturito dall'azione della società Tele2 Sverige, fornitrice di servizi di telecomunicazione con sede nel territorio svedese: quest'ultima, dopo la pronuncia *DRI*, aveva interrotto la conservazione dei metadati relativi ai propri utenti imposta dalla *Lagen om Elektronisk Kommunikation* (c.d. LEK, ovvero la legge nazionale sulle comunicazioni elettroniche), ritenendo tale disposizione normativa non più applicabile alla luce della posizione espressa dalla CGUE[113]. La LEK,

[111] Nel Doc. 14246/15 del 24 novembre 2015, che riassumeva gli esiti del dibattito apertosi in seno al Consiglio europeo ed avente ad oggetto la disciplina della *data retention*, la stessa Presidenza aveva evidenziato le disomogeneità sorte a seguito della sentenza *DRI*: "Opinions diverge on the interpretation of the Court's judgement and thus on the legality schemes for retaining bulk electronic communication data. This has inter alia resulted in a large variety of situations at national level. Some Member States have already adopted or are in a process of preparing new legislation on data retention, that, according to the information received by delegations, aims at ensuring strengthened procedural guarantees and safeguards in compliance with the Charter and in line with the ruling of the Court, including some MSs where the national law has been invalidated by the constitutional Court".

[112] Come ben riassumeva l'Avvocato generale Henrik Saugmandsgaard Øe nelle sue conclusioni del 19 luglio 2016, "la Corte dovrà segnatamente precisare quale interpretazione occorra dare in un contesto nazionale alla sentenza *DRI*", par. 7.

[113] Interessante notare come svariate fossero le ragioni alla base della decisione della compagnia di telecomunicazioni svedese di interrompere la conservazione dei metadati: "the Swedish telecomunications market

modificata a seguito della entrata in vigore della DRD, stabiliva un obbligo di *bulk data retention* della durata di 6 mesi ed era però stata sottoposta, all'indomani della *DRI*, ad un apposito scrutinio da parte di un relatore speciale incaricato dal Ministro della Giustizia; al termine di tale vaglio la disciplina nazionale era stata considerata compatibile con il diritto dell'UE e con la Convenzione EDU. Tale risultato era stato ottenuto adottando quella 'interpretazione flessibile' dei principi fissati dalla giurisprudenza europea di cui si è sopra parlato: la lettura non cumulativa ma separata e 'compensativa' dei requisiti di conservazione ed accesso ai metadati aveva portato a ritenere praticabile una conservazione generalizzata purché accompagnata da appropriate tutele nella successiva fase dell'accesso, che erano state ritenute, dal relatore speciale, esistenti ed adeguate all'interno della normativa svedese[114]. Per questo motivo e proprio a ragione della confermata legittimità della LEK, la *Post-och telestyrelsen* cioè l'autorità svedese di sorveglianza delle poste e delle telecomunicazioni (d'ora in avanti PTS) aveva ingiunto alla Tele2 di riprendere la *data retention* per una durata di sei mesi così come imposta dalla legge svedese: ritenendo però che la relazione disposta del relatore speciale fosse frutto di un'erronea valutazione e di una scorretta applicazione di quanto stabilito dai giudici di Lussemburgo, l'azienda fornitrice di telecomunicazioni promuoveva ricorso al Tribunale amministrativo di Stoccolma e, a seguito del negativo esito dello stesso, impugnava la sentenza di primo grado dinnanzi alla Corte d'appello amministrativa di Stoccolma. Quest'ultima, ritenendo che la normativa svedese in materia di *data retention* avrebbe dovuto essere valutata sulla base dell'art. 15 della Direttiva *e-Privacy*, riteneva infine essenziale un intervento chiarificatore della CGUE volto a stabilire "se un obbligo generalizzato di conservazione dei dati, concernente tutte le persone, tutti i mezzi di comunicazione elettronica e tutti i dati relativi al traffico, senza che sia prevista alcuna distinzione, limitazione o eccezione in funzione dell'obiettivo della lotta alla criminalità, sia compatibile con l'art. 15, par. 1, della Direttiva 2002/58, tenuto conto degli articoli 7 e 8 nonché dell'art. 52, par. 1, della Carta" (par. 51), alla luce anche di quanto affermato nella sentenza *DRI*. In caso di risposta negativa e dunque nel caso in cui la conservazione generalizzata venisse considerata incompatibile con l'art. 15 e con il diritto dell'UE, il giudice del rinvio proponeva altri quesiti pregiudiziali finalizzati a comprendere se una forma di conservazione potesse essere comunque consentita laddove fossero previste specifiche e stringenti tutele quanto all'accesso, alla sicurezza dei dati e alla durata di conservazione.

L'ulteriore rinvio pregiudiziale, proveniente dal Regno Unito, scaturiva invece da un ricorso avanzato non da un operatore economico bensì da tre cittadini, Watson, Brice e Lewis, dinnanzi alla High Court of Justice, finalizzato a promuovere un vaglio di legittimità dell'art. 1 del *Data Retention and Investigatory Powers Act* (c.d. DRIPA) rispetto agli artt. 7 e 8 della Carta di Nizza e 8 della Convenzione EDU. Ebbene, come emerso dal precedente paragrafo, il Regno Unito, poco dopo la sentenza *DRI*, aveva approvato una normativa in materia di conservazione dei metadati per scopi securitari, il DRIPA appunto, che non aveva mancato, sin dall'inizio, di scatenare forti perplessità circa la compatibilità della disciplina con quanto enunciato dai giudici europei: tale normativa infatti consentiva al Ministro dell'Interno di imporre una conservazione generalizzata dei metadati in capo ai

is very competitive; integrity issues are taken seriously by the Swedish public, and certain telecomunications companies have sought to profile themselves as particularly protective of customes' integrity. Another factor behind telecommunications companies' resistance to the Directive – generally speaking, not simply in Sweden – is the fact that storing this data in an accessible form costs them a lot of money", I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 54, 2017, p. 1471.

[114] È rilevante notare come "il relatore speciale ha sottolineato che la sentenza *DRI* non poteva essere interpretata nel senso che essa avesse censurato il principio stesso di una conservazione generalizzata e indifferenziata dei dati. Dal suo punto di vista, la sentenza non doveva neppure essere intesa nel senso che la Corte avesse con essa stabilito una serie di criteri da soddisfarsi nella loro totalità affinché una normativa potesse considerarsi proporzionata. Sarebbe stato necessario valutare tutte le circostanze al fine di accertare la conformità della normativa svedese al diritto dell'Unione, come l'ampiezza della conservazione dei dati alla luce delle disposizioni sull'accesso ai dati stessi, sulla durata della loro conservazione, sulla loro protezione, nonché sulla loro sicurezza", par. 46, *Tele2*.

fornitori di servizi di telecomunicazione, per una durata massima di un anno e senza alcun preventivo intervento autorizzativo o di controllo da parte di autorità giudiziarie o amministrative indipendenti. Questa previsione era stata considerata dal giudice della High Court come fortemente simile a quella stabilita nella DRD: se quest'ultima era stata considerata manchevole sotto il profilo della proporzionalità, "una normativa dal contenuto identico a quello di tale Direttiva non [avrebbe potuto] anch'essa essere compatibile con il suddetto principio. Risulterebbe dalla logica sottesa alla sentenza *DRI* che una normativa istituente un regime generalizzato di conservazione dei dati relativi a comunicazioni viola i diritti garantiti dagli artt. 7 e 8 della Carta, *a meno che tale normativa non sia completata da un regime di accesso ai dati, definito dal diritto nazionale, il quale preveda garanzie sufficienti per la salvaguardia di tali diritti*" (par. 53, *Tele2*, enfasi aggiunta). Veniva quindi chiaramente riproposta nel ragionamento della Corte nazionale l'interpretazione 'flessibile', fatta propria anche dal relatore speciale svedese, secondo cui i requisiti fissati dai giudici di Lussemburgo non dovevano essere considerati come tutti contemporaneamente necessari ma anzi la presenza di idonee tutele nella fase di accesso fosse sufficiente per colmare l'ampiezza ed invasività della conservazione. Il giudice inglese di prima istanza concludeva comunque per l'illegittimità della normativa interna in quanto, anche alla luce di tale più flessibile lettura, la disciplina del DRIPA, che imponeva una *bulk data retention*, risultava priva di regole chiare e precise sull'accesso e utilizzo dei dati conservati nonché della previsione di un controllo preventivo da parte di autorità indipendenti (giudiziarie o non). Dinnanzi a tale pronuncia tuttavia il Ministro dell'Interno aveva promosso appello alla Court of Appeal; questo giudice, ritenendo necessario valutare la normativa nazionale alla luce dell'art. 15 Direttiva *e-Privacy*, avanzava alcune significative riflessioni sull'impatto della sentenza *DRI*: "la Corte [di giustizia dell'UE] non avrebbe inteso enunciare, in detta pronuncia, prescrizioni imperative applicabili alle normative nazionali in materia di accesso ai dati non recanti attuazione del diritto dell'Unione" (par. 57, *Tele2*). Nonostante questo ragionamento – che se applicato al caso inglese avrebbe portato i giudici nazionali a non valutare necessariamente il DRIPA sulla base dei criteri individuati dalla giurisprudenza europea –, la Corte inglese osservava come sei giudici di diversi Stati membri avessero annullato le discipline nazionali in materia di conservazione e accesso ai metadati proprio basandosi sui requisiti e sulle conclusioni dei giudici europei nella storica pronuncia del 2014. È "alla luce di queste circostanze" (par. 59, *Tele2*) e considerando quindi la diversa interpretazione seguita da differenti Corti, che il giudice della Corte d'Appello decideva di presentare un rinvio pregiudiziale alla CGUE, chiedendo "se la sentenza *DRI*, con particolare riferimento ai punti da 60 a 62 [ovvero quelli attinenti alla disciplina dell'accesso da parte delle autorità di *law enforcement*], fissi requisiti imperativi di diritto dell'Unione, applicabili al regime nazionale di uno Stato membro che disciplina l'accesso ai dati conservati ai sensi della normativa nazionale, al fine di rispettare gli artt. 7 e 8 della Carta" (par. 59). È evidente pertanto come la visione dei giudici inglesi, sia di prima che di seconda istanza, avesse fatto salva la disciplina di *bulk data retention*, non considerata, per sua natura, incompatibile con il diritto dell'UE, concentrandosi invece sulle condizioni dell'acceso.

4.2. – La decisione della CGUE (I): la determinazione dell'ambito di applicazione della Direttiva **e-Privacy** *e una più netta presa di posizione circa la proporzionalità di un regime di* **bulk data retention**

La Corte di giustizia dell'UE (Grande Sezione), con sentenza del 21 dicembre 2016, si è pronunciata con una ulteriore storica sentenza, dal forte impatto e dalle enormi conseguenze. I giudici di Lussemburgo, infatti, hanno chiarito pressoché definitivamente la dibattuta questione della compatibilità con il diritto europeo di forme di conservazione generalizzata ed indiscriminata, punto sul quale erano

sorte, come si è visto anche dalla ricostruzione dei due rinvii pregiudiziali, diverse letture e differenti approcci all'interno degli Stati membri.

Se questo primo fondamentale aspetto imponeva di operare una interpretazione dell'art. 15 Direttiva *e-Privacy*, si rendeva però preliminarmente necessaria la soluzione di un quesito, anch'esso, come si è visto nel precedente paragrafo, piuttosto dibattuto: una normativa nazionale adottata ai sensi dell'art. 15 richiamato, rientra nell'ambito di applicazione del diritto dell'UE? Su questo aspetto, gli Stati che erano intervenuti con osservazioni scritte al procedimento dinnanzi alla CGUE avevano mostrato orientamenti divergenti: interessante è la posizione del governo ceco che rimarcava come, essendo l'obiettivo di queste discipline quello di lotta alla criminalità, tali previsioni sfociassero nelle competenze proprie degli Stati membri, sfuggendo dunque all'ambito di applicazione del diritto europeo; similmente, il Regno Unito riteneva rientranti nell'ambito di regolamentazione europeo solo le disposizioni nazionali attinenti alla *data retention* e dunque agli obblighi in capo agli operatori economici e non anche quelle riguardanti l'accesso delle autorità pubbliche, che afferivano alla sfera della repressione degli illeciti, sottratta al diritto europeo[115].

La CGUE invece si è allontanata da entrambe queste interpretazioni, giungendo alla conclusione che una normativa nazionale regolante conservazione ed accesso, rientra, *in toto*, nell'ambito di applicazione del diritto europeo: se è vero che le disposizioni adottate sulla base dell'art. 15 Direttiva *e-Privacy* si riferiscono ad attività proprie degli Stati e che l'art. 1, co. 3, della Direttiva stessa esclude dalla propria disciplina le attività statali in materia penale e attinenti alla sicurezza pubblica, difesa e sicurezza dello Stato, i giudici hanno tuttavia ritenuto che "alla luce *dell'economia generale* della Direttiva 2002/58, [tali] elementi non consentono di concludere che le misure legislative contemplate dall'art. 15 siano escluse dall'ambito di applicazione di tale Direttiva, *a pena di privare detta disposizione di qualsiasi effetto utile*, (..) dato che la Direttiva autorizza espressamente gli Stati membri ad adottare le misure in questione unicamente a condizione di rispettare i requisiti da essa previsti" (par. 73, *Tele2*)[116]. Anche la regolazione della fase di accesso era da ritenersi attuativa dell'art. 15 della Direttiva e dunque in applicazione del diritto europeo: scopo della Direttiva stessa infatti era quello di tutelare gli utenti da qualsiasi accesso non autorizzato, indipendentemente dal fatto che ciò venisse realizzato da soggetti privati – gli operatori economici – o pubblici – le autorità di *law enforcement*. Inoltre l'accesso prevedeva un intervento dei fornitori che dovevano "accordare" alle autorità nazionali l'accesso e quindi operare un trattamento sui dati, considerato attività per questo rientrante nell'ambito di applicazione della Direttiva; la *data retention* stessa inoltre era effettuata al solo ed unico scopo di rendere i dati accessibili e quindi "una normativa nazionale che preveda la conservazione di dati implica, necessariamente, in linea di principio, l'esistenza di disposizioni in materia di accesso" (par. 78-81)[117].

---

[115] Per completezza e per restituire l'immagine della complessità della questione in esame, si vuole riportare anche la posizione della Commissione, la quale aveva sostenuto che "soltanto le norme nazionali relative alla conservazione dei dati, e non anche quelle relative all'accesso delle autorità nazionali a tali dati, rientrano nell'ambito di applicazione di detta Direttiva [2002/58]. Queste ultime norme dovrebbero però, a suo parere, essere prese in considerazione al fine di valutare se una normativa nazionale disciplinante la conservazione dei dati da parte dei fornitori di servizi di comunicazione elettronica costituisca una ingerenza proporzionata nei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta", par. 66, *Tele2*.

[116] Veniva inoltre nuovamente rimarcato, riprendendo quella linea interpretativa già fornita nella sentenza *DRI* e nella precedente *Irlanda c. Parlamento europeo e Consiglio*, come le misure normative adottate sulla base dell'art. 15 disciplinassero l'attività non di soggetti pubblici bensì degli operatori economici (par. 74, *Tele2*) ed influissero dunque sulle attività economiche da essi poste in essere nel mercato interno.

[117] Anche l'Avvocato generale, nelle richiamate Conclusioni, sosteneva che la formulazione stessa dell'art. 15 della Direttiva 2002/58 confermava come la disciplina della conservazione dei metadati adottata in via derogatoria dagli Stati membri dovesse rientrare nell'ambito di applicazione della Direttiva medesima, costituendone anzi un'attuazione. Richiamando poi la sentenza *Irlanda c. Parlamento e Consiglio*, la regolamentazione della *data retention* non poteva considerarsi rientrante nella materia penale e dunque neppure in quelle attività di cui agli art. 3 della Direttiva 95/46/CE e 1, co. 3, della Direttiva *e-Privacy*, escluse dall'ambito di applicazione del diritto dell'UE in quanto attività proprie degli Stati. Da tale valutazione, l'Avvocato faceva derivare che "neanche le

Appurato dunque che sia la disciplina derogatoria della conservazione dei metadati che la regolamentazione della successiva ed eventuale operazione di accesso rientrano nell'ambito di applicazione della Direttiva *e-Privacy* e del diritto europeo, la Corte ha fornito l'interpretazione dell'art. 15 alla luce della Carta di Nizza che, lo si ricorda, risulta applicabile limitatamente alle competenze dell'UE definite nei Trattati (art. 51).

È stato così innanzitutto precisato che la facoltà concessa dalla disposizione in esame di derogare all'obbligo generale di cancellazione ed anonimizzazione dei dati dovesse essere considerata una eccezione e quindi interpretata in maniera restrittiva: questo perché finalità della Direttiva 2002/58 nel suo complesso era quella di garantire un elevato livello di riservatezza delle comunicazioni e dei dati sul traffico e minimizzare i rischi di abusi. Ne derivava, conseguentemente, che anche l'elenco degli obiettivi che giustificavano il ricorso alla facoltà sancita nell'art. 15 doveva essere valutato restrittivamente e dunque considerato come esaustivo, non ammettendosi scopi ulteriori e diversi legittimanti la *data retention*. Questa visione e lettura 'restrittiva' della disciplina derogatoria veniva poi attuata anche con riferimento agli ulteriori criteri e condizioni previste all'art. 15. In primis, la Corte osservava che una normativa nazionale introducente un obbligo di conservazione sollevava questioni circa il rispetto di alcuni diritti fondamentali: quello alla garanzia della vita privata, alla protezione dei dati ma anche alla libertà di espressione, che costituisce "uno dei fondamenti essenziali di una società democratica e pluralista, facente parte dei valori sui quali, a norma dell'art. 2 TUE, l'Unione è fondata" (par. 93, *Tele2*). Proprio alla luce di tale impatto sui diritti riconosciuti dalla Carta di Nizza, diveniva necessaria una valutazione della ingerenza ai sensi dell'art. 52 della Carta stessa: similmente a quanto già effettuato nella sentenza *DRI*, i giudici hanno quindi considerato se la limitazione all'esercizio dei diritti e libertà riscontrata e causata dalle normative introducenti un obbligo di *data retention* fosse prevista per legge, nel rispetto del contenuto essenziale dei diritti, nonché necessaria, rispondente ad un obiettivo di interesse generale e proporzionata. Il criterio di legittimità quindi doveva essere quello della stretta necessità, peraltro indicato anche come requisito dall'art. 15 stesso, che consente la deroga alla regola generale solo qualora la normativa nazionale adottata sia "necessaria, opportuna e proporzionata all'interno di una società democratica", limitata per un periodo di tempo specifico e giustificata solo dal raggiungimento di uno degli obiettivi espressamente indicati dalla disposizione e sopra già richiamati. Sulla base di questi specifici e stringenti requisiti i giudici di Lussemburgo ribadiscono innanzitutto che i metadati raccolti per la fornitura di un servizio di telecomunicazione, presi nel loro insieme, "sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse frequentati. Tali dati forniscono gli strumenti per stabilire il profilo delle persone interessate, informazioni tanto sensibili, in rapporto al diritto al rispetto della vita privato, quanto il contenuto stesso delle comunicazioni" (par. 99, *Tele2*). L'ingerenza che se ne ricava è di vasta portata e particolarmente grave in quanto idonea ad ingenerare nei cittadini un senso di sorveglianza continua (par. 100, *Tele2*): nella scelta di queste parole non può non cogliersi la forte somiglianza alle

disposizioni di diritto nazionale che stabiliscono un obbligo di conservazione simile a quello previsto dalla Direttiva 2006/24 riguardano la materia penale" (par. 96). Con riferimento poi alla applicabilità della Carta di Nizza anche alle disposizioni nazionali che disciplinano l'accesso, veniva ribadito come esse non rientrassero di per sé nell'ambito di applicazione della Carta (par. 123), riguardando attività dello Stato nell'ambito del diritto penale che non attuano quindi il diritto dell'Unione. Se ci si limita a questa affermazione, sembrerebbe che l'Avvocato avesse deciso di riprendere e riproporre quella distinzione tra regolamentazione della conservazione e disciplina dell'accesso, che aveva caratterizzato la previa giurisprudenza della CGUE. Se si prosegue nella lettura delle conclusioni tuttavia si nota come l'Avvocato si fosse spinto oltre, giungendo ad affermare che "la ratio di un obbligo di conservazione di dati è quella di consentire alle autorità di contrasto di accedere ai dati conservati, cosicché le problematiche della conservazione e dell'accesso non possono essere completamente dissociate" (par. 125).

decise considerazioni mosse già nella sentenza del 2014, la cui fondatezza e correttezza veniva così rimarcata e riaffermata.

Come già espresso nelle sentenza *DRI* e nonostante le forti critiche e i dubbi emersi da quella lettura, l'ingerenza prodotta dalla conservazione non veniva ritenuta in grado di pregiudicare il contenuto essenziale dei diritti alla riservatezza e protezione dei dati, in quanto limitata ai metadati e non anche al contenuto delle comunicazioni; veniva inoltre ritenuto rispettato il requisito dell'obiettivo legittimo, individuato nella lotta alla criminalità *grave*: proprio la gravità del crimine veniva considerata una qualifica fondamentale al fine di giustificare una ingerenza anch'essa grave. Questo punto, lo si vuole premettere, non è da sottovalutare e anzi merita appropriato rilievo: il dettato normativo dell'art. 15 infatti non fa alcuna menzione al criterio della "gravità" del reato, a differenza della DRD che invece all'art. 1 indicava quale scopo della conservazione quello della lotta alla specifica categoria di "reati gravi", pur lasciandone la determinazione ai legislatori nazionali. Non è quindi scontato o di poco conto il fatto che i giudici, pur nella mancata specificazione della norma in esame, stabiliscano il necessario carattere 'grave' dei reati, definendo così ancor più restrittivamente i criteri previsti nel testo normativo stesso.

Chiarita quindi la sussistenza di una ingerenza che non comprime il nucleo essenziale dei diritti e che persegue un obiettivo legittimo, la Corte ha valutato la stretta necessità di un obbligo di conservazione generalizzata: pur affrontando in maniera assai veloce l'efficacia della normativa e dunque la sua capacità di raggiungere lo scopo preposto[118], sono stati presi in considerazione i requisiti già indicati nella sentenza *DRI* e 'trasposti' nel contesto dell'art. 15 Direttiva *e-Privacy*. Viene quindi criticata la mancata previsione della necessaria sussistenza sia di un indizio che permettesse di stabilire un nesso, "sia pure indiretto o remoto", tra conservazione dei dati e violazioni penali gravi (par. 105, *Tele2*), sia di una correlazione tra dati conservati e minaccia per la sicurezza pubblica (par. 106, *Tele2*) [119]; veniva inoltre rilevata l'assenza di eccezioni stabilite a maggior tutela delle comunicazioni sottoposte a segreto professionale. Tutte queste carenze di criteri e requisiti atti a delimitare l'ampiezza della conservazione finivano col determinare una *data retention* generalizzata cioè coinvolgente tutti gli utenti e tutti i mezzi di comunicazione, producendo quale risultato finale la trasformazione di quella che avrebbe dovuto essere una eccezione (la conservazione) in regola, diversamente da quanto previsto nella Direttiva *e-Privacy*. I giudici di Lussemburgo giungevano così ad affermare che una normativa contenente una siffatta disciplina, carente sotto il profilo di specifiche salvaguardie e limitazioni, travalicava i limiti di quanto strettamente necessario. La Corte poi si spingeva oltre una visione meramente 'in negativo', delineando 'positivamente' le caratteristiche di una normativa in materia di conservazione dei dati che potesse dirsi conforme alla Carta di Nizza: quest'ultima "non osta a che uno Stato membro adotti una normativa la quale consenta, a titolo preventivo, la conservazione *mirata* dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate nonché la durata di conservazione prevista, limitata allo stretto necessario" (par. 108, *Tele2*, enfasi aggiunta), mediante la previsione di norme chiare e precise sulla estensione e sulle condizioni della conservazione, unitamente a criteri oggettivi in grado di istituire un rapporto tra dati da conservare e scopo da perseguire. "Una siffatta delimitazione può essere ottenuta mediante un criterio geografico qualora le autorità nazionali competenti considerino,

[118] "L'efficacia della lotta contro la criminalità grave, e in particolare contro la criminalità organizzata e il terrorismo, può dipendere in larga misura dall'utilizzo delle moderne tecniche di indagine", par. 102. Viene pertanto sbrigativamente individuata l'adeguatezza del sistema di conservazione dei dati al raggiungimento dell'obiettivo legittimo.

[119] La *data retention* "non è limitata ad una conservazione avente ad oggetto dati relativi ad un periodo di tempo e/o una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità" (par. 106, *Tele2*).

sulla base di elementi oggettivi, che esiste, in una o più zone geografiche, un rischio elevato di preparazione o di commissione di atti di questo tipo" (par. 111, *Tele2*). Veniva così individuata come legittima e proporzionata solamente una forma di conservazione targettizzata, mirata e limitata nella sua ampiezza: una normativa priva dei criteri 'positivi' individuati dai giudici, sulla falsa riga di quanto affermato nella previa sentenza del 2014, non avrebbe potuto considerarsi compatibile con la Carta di Nizza e con il diritto europeo. In questo senso e sotto questo primo profilo relativo alla disciplina della *data retention* pare chiarirsi quella zona grigia e la relativa disomogeneità interpretativa apertasi a seguito della pronuncia *DRI*: "l'art. 15 della Direttiva 2002/58, letto alla luce degli artt. 7, 8 e 11 nonché 52, par. 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica" (par. 112, *Tele2*). Come si avrà modo di vedere, questa forte affermazione, che andava nella direzione di un abbandono totale dei sistemi di conservazione generalizzata, aprirà le porte a notevoli difficoltà attuative da parte dei legislatori nazionali e delle autorità di *law enforcement*, restie a sacrificare definitivamente uno strumento ritenuto così importante e dunque decise a trovare e promuovere, anche in questo caso, una lettura più flessibile della netta posizione espressa dalla Corte.

4.3. – La decisione della CGUE (II): la delicata disciplina dell'accesso e la conferma delle più stringenti limitazioni indicate nella pronuncia DRI

La seconda questione affrontata dai giudici di Lussemburgo attiene poi alla disciplina dell'accesso, alla quale era stata attribuita grande attenzione nel rinvio pregiudiziale promosso dalla Corte d'Appello del Regno Unito. Su tale fronte è stato innanzitutto ribadito come l'elenco degli obiettivi per i quali l'art. 15 Direttiva *e-Privacy* concedeva la possibilità di adottare normative derogatorie della propria disciplina fosse da intendersi esaustivo: l'obiettivo idoneo a consentire l'accesso ai metadati conservati poteva essere motivato solo dal fine di lotta contro la criminalità di carattere "grave". Nella disposizione in esame tuttavia, come anche nella DRD, mancava del tutto una qualificazione o indicazione capace di determinare il significato della 'gravità' richiesta, la cui definizione quindi era lasciata ai legislatori nazionali.

Oltre alla limitazione derivante dallo scopo, l'accesso poteva poi essere effettuato solo entro i limiti di stretta necessità: dovevano quindi essere stabilite norme chiare e precise sulle condizioni alle quali gli operatori economici che avevano conservato i dati erano tenuti a concederne l'accesso alle autorità pubbliche. Così, nell'interpretazione dei giudici di Lussemburgo, l'art. 15 attribuiva a ciascuno Stato membro il compito di stabilire una normativa interna che prevedesse requisiti "sostanziali e procedurali" (par. 118, *Tele2*) sull'accesso e dunque criteri oggettivi in grado di determinare una connessione, anche indiretta, tra accesso e finalità di repressione del crimine. Ne derivava che "un accesso può essere consentito (..) soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso una violazione grave, o anche di essere implicate in una maniera o in un'altra in una violazione siffatta" (par. 119, *Tele2*). Unica eccezione prevista a tali restrizioni era individuabile in caso di sussistenza di una minaccia agli interessi vitali della sicurezza nazionale, difesa o sicurezza pubblica, come nel caso di attività terroristiche: in queste specifiche situazioni, "l'accesso ai dati di altre persone potrebbe essere parimenti concesso quando sussistano elementi oggettivi che consentano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro simili attività" (par. 119, *Tele2*). Ulteriore criterio necessario per la disciplina dell'accesso veniva individuato nel controllo preventivo di un giudice o di una entità amministrativa indipendente subordinato alla presentazione di una richiesta motivata da parte delle autorità di *law enforcement* nell'ambito di una procedura di

prevenzione, accertamento o esercizio dell'azione penale, salvo casi di urgenza debitamente giustificati. A ciò si aggiungeva anche la previsione di una notifica alle persone interessate, "a partire dal momento in cui tale comunicazione non è suscettibile di compromettere le indagini condotte dalle autorità summenzionate", allo scopo di consentire al soggetto cui i dati appartengono di poter esercitare eventualmente il diritto di ricorso. Anche con riferimento all'accesso dunque, similmente a quanto deciso per la conservazione, veniva consentita una forma di utilizzo dei dati fortemente mirata e ristretta, subordinata al rispetto di stringenti condizioni e controlli, preventivi e successivi, espressamente indicati.

La CGUE, al termine della disamina circa i requisiti necessari per determinare la legittimità della conservazione e dell'accesso, specificava infine come sussistesse in capo ai fornitori, anche nel caso di normative nazionali derogatorie della disciplina generale, l'obbligo di stabilire misure tecniche e organizzative appropriate a garanzia della protezione dei dati. La disciplina interna doveva a tal fine comunque prevedere l'obbligo di conservazione nel solo territorio dell'Unione e la distruzione "irreversibile" dei dati alla scadenza del termine fissato (par. 122, *Tele2*), come già enunciato nella precedente sentenza *DRI*, nonché la determinazione di controlli da parte di autorità indipendenti circa il rispetto "del livello di protezione garantito dal diritto dell'Unione in materia di tutela delle persone fisiche riguardo al trattamento dei dati personali" (par. 123, *Tele2*).

La sentenza *Tele2*, quindi, "richiama a fondamento del percorso interpretativo della diversa Direttiva del 2002 numerosi passaggi della sentenza *Digital Rights* qualificando espressamente l'opportunità argomentativa di tali richiami in una logica 'per analogia'. Sebbene la Grande Sezione del 2014 non abbia inteso enunciare prescrizioni imperative applicabili alle normative nazionali, la pronuncia *Tele2* del 2016 rileva quindi come il ragionamento da svolgere rispetto alla Direttiva 2002 – che continua a fissare i confini dell'autonomia procedurale degli Stati membri in materia – sia strettamente legato all'obiettivo perseguito dalla Direttiva invalidata, che condiziona quindi l'interpretazione della residua disciplina europea"[120]. In questo senso, la pronuncia sin qui analizzata è intervenuta nella direzione di un consolidamento e integrazione dell'interpretazione già fornita nella sentenza *DRI*, in tal modo estendendola anche con riferimento alle discipline nazionali attuative dell'art. 15 Direttiva *e-Privacy*; proprio rispetto a tale disposizione, i giudici dunque hanno chiarito – e per certi versi ribadito – la portata eccezionale di un obbligo di conservazione rispetto alla regola generale, fornendone una lettura più rigida e circoscritta, limitativa della discrezionalità dei legislatori nazionali. É stata così chiarita ed inequivocabilmente affermata l'incompatibilità rispetto alla Carta di Nizza, ed in particolare con i diritti di cui agli artt. 7, 8 e 52, di un sistema di *blanket* o *bulk data retention*, che preveda cioè una conservazione generalizzata e indiscriminata riguardante tutti gli utenti e tutti i mezzi di comunicazione. L'unica forma di memorizzazione dei metadati che pare concessa è quella mirata, la c.d. *targeted data retention*, i cui requisiti vengono espressamente indicati dai giudici di Lussemburgo mediante un approccio 'positivo', diverso da quello adottato nella sentenza sulla DRD, nella quale erano stati sottolineati gli aspetti negativi ed invalidanti della disciplina europea. Con questa visione più netta rispetto a quella emersa dalla previa sentenza, venivano quindi fugati alcuni dei dubbi e delle interpretazioni fornite a livello nazionale, volte a far salvo l'assetto legislativo esistente e fondate su una lettura 'flessibile' dei molteplici requisiti indicati dai giudici europei. La Corte, coerentemente alla previa sentenza *DRI*, pare invece mantenere una posizione in controtendenza con il clima securitario che aveva caratterizzato l'approccio – forse più pragmatico – degli Stati membri e del legislatore

[120] F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE Online*, 2, 2017, p. 353; l'autore prosegue ritenendo che il caso da cui origina l'importante sentenza *Tele2* rappresenti un "rinvio pregiudiziale di interpretazione attuativo del precedente rinvio pregiudiziale di validità, il quale colpisce l'autonomia procedurale degli Stati membri che la Direttiva del 2002 aveva lasciato residuare in materia di pubblica sicurezza, riducendo la discrezionalità alla luce delle argomentazioni della pronuncia *Digital Rights*".

europeo e che aveva portato a ritenere legittima una conservazione estesa a tutti gli utenti e tutti i mezzi di comunicazione purché accompagnata da idonee tutele e salvaguardie, soprattutto nella successiva ed eventuale fase dell'accesso.

4.4. – Le Conclusioni dell'Avvocato generale tra divergenze e concordanze con la posizione dei giudici di Lussemburgo

La lettura maggiormente flessibile dei criteri sanciti nella sentenza *DRI* e adottata da numerosi Stati membri e Corti nazionali, era stata peraltro seguita anche dall'Avvocato generale che era giunto ad affermare come i diritti tutelati dalla Carta di Nizza "non ostino a che uno Stato membro imponga ai fornitori di servizi di comunicazione elettronica un obbligo di conservare tutti i dati relativi alle comunicazioni effettuate dagli utenti dei loro servizi, qualora siano soddisfatte tutte le condizioni seguenti", individuate: a) nella previsione dell'obbligo di conservazione all'interno di una disposizione legislativa o regolamentare accessibile, prevedibile e inclusiva di tutele adeguate nei confronti dell'arbitrio[121]; b) nel rispetto del contenuto essenziale dei diritti alla privacy e alla protezione dei dati; c) nella stretta necessità dell'obbligo di conservazione rispetto al fine di lotta contro i crimini gravi[122]; d) nella previsione delle garanzie stabilite nella sentenza *DRI* riguardanti l'accesso, la sicurezza dei dati e la durata della conservazione; e) nella proporzionalità, in una società democratica, dell'obbligo di conservazione generalizzata (par. 263, Conclusioni).

Come si nota immediatamente, la posizione dell'Avvocato generale Saugmandsgaard Øe non giungeva alla ben più rigida decisione della Corte: secondo l'Avvocato generale infatti la *bulk data retention* non era da considerarsi *per se* eccedente i limiti dello strettamente necessario e dunque, per sua stessa natura, incompatibile con il diritto dell'UE. Tale incompatibilità si riscontrava solo laddove

[121] È interessante notare come l'Avvocato generale si fosse rifatto, nella valutazione di questo requisito, alla copiosa giurisprudenza elaborata dalla Corte EDU, concludendo che, nello specifico caso della delicata ed incisiva disciplina della conservazione dei dati, tale regolamentazione avrebbe dovuto essere auspicabilmente adottata dal potere legislativo (par. 138-153).

[122] Con riferimento a questo aspetto, così come sulla questione attinente alla lesione del contenuto essenziale dei diritti alla riservatezza e alla protezione dei dati, la posizione della Corte si presentava in linea con quella dell'Avvocato generale: quest'ultimo infatti aveva affermato come "il requisito di proporzionalità in una società democratica escluda che la lotta contro i reati minori o il corretto svolgimento di procedimenti non penali possa giustificare un obbligo generale di conservazione dei dati. In effetti, i notevoli rischi causati da un siffatto obbligo sono sproporzionati rispetto ai vantaggi che esso offrirebbe nella lotta contro i reati minori o nel contesto di procedimenti non penali", par. 172. Nello specifico, l'Avvocato, valutata la sussistenza di un interesse generale, riscontrato nella lotta al terrorismo, nel mantenimento della pace e della sicurezza internazionali così come nella lotta alla criminalità grave al fine di garantire la sicurezza, garantita peraltro dall'art. 6 della Carta di Nizza (par. 163), si era poi concentrato sulla adeguatezza della conservazione generalizzata dei metadati al raggiungimento dello scopo individuato. Per effettuare tale vaglio, l'Avvocato aveva spiegato in modo efficace le potenzialità derivanti dalla disponibilità di dati in maniera generalizzata: "una misura di sorveglianza mirata riguarda persone che sono state precedentemente individuate come aventi potenzialmente un collegamento, anche indiretto o lontano, con un reato grave. Siffatte misure mirate consentono alle autorità competenti di avere accesso ai dati relativi alle comunicazioni effettuate da dette persone, e persino al contenuto di tali comunicazioni. Tuttavia tale accesso può riguardare soltanto le comunicazioni effettuate da dette persone successivamente alla loro individuazione. Al contrario l'obbligo generale di conservazione di dati riguarda l'insieme delle comunicazioni effettuate da tutti gli utenti, senza che sia richiesto un qualsiasi collegamento con un reato grave. Tale obbligo consente alle autorità competenti di avere accesso alla cronologia delle comunicazioni effettuate da una persona prima di essere stata individuata come avente un siffatto collegamento. È in questo senso che siffatto obbligo conferisce alle autorità di contrasto una capacità limitata di leggere il passato, offrendo loro un accesso alle comunicazioni effettuate da dette persone precedentemente alla loro individuazione", cioè ancor prima che un soggetto fosse sospettato di alcunché (par. 179-180).

l'obbligo generale di conservazione[123] non fosse accompagnato dalle adeguate garanzie previste dalla Direttiva *e-Privacy*, dalla Carta di Nizza e dalla giurisprudenza emersa nella sentenza *DRI*, ed individuate nelle misure riguardanti l'accesso ai dati, la durata di conservazione e la protezione e sicurezza dei dati stessi. La sussistenza di siffatte salvaguardie era peraltro da affidarsi alla valutazione dei giudici nazionali, chiamati a vagliare tali elementi "alla luce di tutte le caratteristiche rilevanti dei regimi nazionali" (par. 263, Conclusioni). Tale visione così differente adottata dall'Avvocato derivava innanzitutto dalla constatazione secondo cui "l'intenzione del legislatore dell'Unione era non già quella di pregiudicare la facoltà degli Stati membri di adottare le misure previste dall'art. 15, par. 1, della Direttiva 2002/58, bensì quella di subordinare tale facoltà a taluni requisiti relativi, in particolare, agli scopi perseguiti e alla proporzionalità di dette misure" (par. 108, Conclusioni), cosicché non solo un obbligo generale di conservazione non era da considerarsi *per se* incompatibile con la Direttiva ma la facoltà di cui all'art. 15 non rappresentava neppure una deroga e non doveva dunque essere interpretata restrittivamente (par. 110, Conclusioni)[124]. Nella sua lettura della sentenza *DRI*, l'Avvocato giungeva infatti significativamente a ritenere che "l'obbligo generale di conservazione dei dati previsto dalla Direttiva 2006/24 non eccedeva, di per sé, i limiti dello stretto necessario. Tale Direttiva eccedeva i limiti dello stretto necessario a causa dell'*effetto combinato* della conservazione generalizzata dei dati e dell'assenza di garanzie volte a limitare allo stretto necessario la lesione dei diritti sanciti dagli artt. 7 e 8 della Carta" (par. 202, Conclusioni, enfasi aggiunta)[125]: questa interpretazione sembrava pertanto avallare la lettura più flessibile promossa da numerosi Stati membri all'indomani della sentenza *DRI* stessa, mentre si distanziava fortemente dalla posizione poi assunta dalla Corte nella sua pronuncia.

È comunque da sottolineare come, nonostante questa significativa differenza nella determinazione della necessità della disciplina della conservazione generalizzata, l'Avvocato si fosse poi mostrato, nel prosieguo del proprio ragionamento, più cauto quanto alla valutazione della proporzionalità, in una società democratica, di un obbligo generale di *data retention* per fini securitari: mentre nella sentenza del 2014 la CGUE non era giunta ad esaminare il carattere di proporzionalità del regime indicato nella DRD poiché quest'ultimo era stato trovato già eccedente i limiti dello stretto necessario, l'Avvocato aveva reputato opportuno in questa pronuncia attribuire ai giudici del rinvio il compito di verificare che gli "inconvenienti", provocati da una disciplina nazionale in materia di *data retention* rispetto ai diritti fondamentali garantiti in una società democratica, non fossero sproporzionati rispetto agli scopi perseguiti (par. 247, Conclusioni)[126]. Su tale punto l'Avvocato sviluppava alcune considerazioni utili e

[123] Per "obbligo generale di conservazione" l'Avvocato intendeva una forma di *bulk data retention* cioè una conservazione riguardante tutti i mezzi di comunicazione e tutti gli utenti (par. 2).

[124] Mentre l'orientamento promosso dalla compagnia Tele2 – accolto dalla Corte nella sua pronuncia – vedeva l'obbligo di conservazione generalizzata come eccedente *per se* i limiti dello stretto necessario, indipendentemente da eventuali ulteriori garanzie, l'Avvocato accoglieva una interpretazione differente, condivisa dalla maggioranza delle parti che avevano presentato osservazioni nel corso del giudizio: "secondo la mia lettura della sentenza *DRI*, la Corte ha dichiarato che un obbligo generale di conservazione dei dati eccede i limiti dello stretto necessario qualora esso non sia accompagnato da garanzie rigorose riguardanti l'accesso ai dati, la durata di conservazione nonché la protezione e la sicurezza dei dati. (..) A questo proposito sottolineo che i punti da 56 a 59 della sentenza *DRI* non contengono alcuna dichiarazione della Corte nel senso che un obbligo generale di conservazione di dati ecceda, di per sé, i limiti dello stretto necessario" (par. 193).

[125] L'Avvocato infatti proseguiva ritenendo che "se la mera conservazione generalizzata dei dati fosse stata sufficiente a causare l'invalidità della Direttiva 2006/24, la Corte non avrebbe avuto bisogno di esaminare, per di più in maniera dettagliata, l'assenza delle garanzie menzionate ai punti da 60 a 68 di detta sentenza", par. 202.

[126] L'Avvocato voleva precisare la distinzione tra requisiti e valutazioni inerenti la necessità ed adeguatezza di una misura di conservazione e quelli invece attinenti alla proporzionalità: "la specificità del requisito di proporzionalità stricto sensu, rispetto ai requisiti del carattere adeguato e necessario, può essere illustrata con il seguente esempio. Immaginiamo che uno Stato membro imponga a tutte le persone residenti nel proprio territorio l'iniezione di un microchip di geolocalizzazione che consenta alle autorità di ricostruire i movimenti del suo portatore nel corso dell'ultimo anno. Una tale misura potrebbe essere considerata 'necessaria' qualora nessun'altra misura consentisse di ottenere il medesimo livello di efficacia nella lotta contro i reati gravi. Tuttavia, a mio avviso, detta misura sarebbe sproporzionata in una società democratica, poiché gli inconvenienti risultanti dalla lesione dei diritti

di interesse: nel valutare infatti le ingerenze nella sfera privata, affermava come l'obbligo generale di conservazione finisse col colpire soggetti che, nella maggioranza dei casi, non avrebbero mai avuto alcun collegamento con un reato grave. Ne derivava che "in un contesto individuale, un obbligo generale di conservazione di dati consente ingerenze tanto gravi quanto quelle permesse da misure di sorveglianza mirate, comprese quelle che intercettano il contenuto delle comunicazioni effettuate" (par. 254, Conclusioni). Ma la reale gravità ed impatto sui diritti fondamentali causata da una conservazione generalizzata poteva essere maggiormente compresa, a parere dell'Avvocato, guardando al contesto delle ingerenze "di massa", che colpiscono cioè una parte sostanziale o l'insieme della popolazione: è da questo punto prospettico e in tale dimensione che si esplica la potenzialità – negativa – propria di una analisi generalizzata dei metadati, capace di consentire una "classificazione quasi istantanea di un'intera popolazione" (par. 259, Conclusioni)[127]. Ciò, sommato alla consapevolezza dei rischi di accesso abusivo o illegale ai dati conservati, considerati "connaturati all'esistenza stessa di banche dati archiviate su supporti informatici" (par. 260, Conclusioni), portava l'Avvocato a concludere che spetta ai giudici del rinvio "bilanciare i rischi e i vantaggi connessi ad un obbligo [generale di conservazione] e, precisamente, da una parte, i vantaggi connessi alla concessione di una capacità limitata di leggere il passato alle autorità preposte alla lotta contro i reati gravi e, dall'altra, i gravi rischi derivanti, in una società democratica, dal potere di mappatura della vita privata di un individuo e dal potere di classificazione di un'intera popolazione" (par. 261, Conclusioni). Nello svolgere tale delicata valutazione, il giudice nazionale dovrebbe – anche ma non solo – considerare il rispetto dei criteri espressi nei punti 60 a 68 della sentenza *DRI* (accesso, durata della conservazione e sicurezza e protezione dei dati da parte dei fornitori) che, a parere dell'Avvocato, debbono essere considerati *tutti* come imperativi. Con riferimento a tali specifici requisiti è stata quindi adottata dall'Avvocato una lettura maggiormente restrittiva e rigida sia rispetto alla visione più flessibile proposta da alcuni Stati membri, quali la Germania, che ritenevano invece le garanzie indicate dalla CGUE come meramente indicative e non necessariamente contemporanee e cumulative[128], sia rispetto alla successiva posizione

all'integrità fisica, al rispetto della vita privata e alla protezione dei dati di carattere personale sarebbero sproporzionati rispetto ai vantaggi che ne deriverebbero nella lotta contro i reati gravi", nota 81.

[127] L'Avvocato ha mostrato una profonda sensibilità e conoscenza del funzionamento di sistemi di lettura aggregate dei metadati, riportando anche interessanti esempi: "supponiamo che [una persona che ha accesso ai dati conservati] desideri identificare gli individui contrari alla politica del governo in carica. Anche in questo caso, l'analisi a tal fine del contenuto delle comunicazioni richiederebbe risorse considerevoli, invece, l'utilizzo dei dati relativi alle comunicazioni consentirebbe di identificare tutti gli individui iscritti in elenchi di distribuzione di email che criticano la politica del governo. Inoltre, tali dati consentirebbero altresì di identificare gli individui che partecipano a una qualsiasi manifestazione pubblica di opposizione al governo", par. 258. Da tali considerazioni, l'Avvocato fa derivare come "i rischi legati all'accesso ai metadati possano essere equivalenti, se non addirittura superiori a quelli risultanti dall'accesso al contenuto di tali comunicazioni" (par. 259), richiamando anche quanto emerso dalla relazione *Il diritto alla privacy nell'era digitale*, del 30 giugno 2014, A/HRC/27/37, nella quale l'Alto Commissariato delle Nazioni Unite per i diritti umani affermava: "Alcuni sostengono che l'intercettazione – o la raccolta – di dati su una comunicazione, e non anche del contenuto della comunicazione, non costituisce di per sé un'ingerenza nella vita privata. Orbene, dal punto di vista del diritto alla vita privata, tale distinzione non convince. Le aggregazioni di informazioni comunemente denominate metadati possono fornire indicazioni sulla condotta di un individuo, sulle sue relazioni sociali, sulle sue preferenze personali e sulla sua identità che vanno ben al di là di ciò che si ottiene accedendo al contenuto di una comunicazione privata".

[128] Di grande interesse è la tesi promossa dei governi tedesco, estone, irlandese, francese e del Regno Unito che ritenevano appunto i criteri indicati ai punti da 60 a 68 della sentenza *DRI* come meramente indicativi: in quella pronuncia infatti "la Corte avrebbe proceduto ad una valutazione complessiva delle garanzie assenti nel regime previsto dalla Direttiva 2006/24, senza che una qualsiasi di tali garanzie possa, in maniera isolata, essere considerata imperativa alla luce del requisito di stretta necessità. Per illustrare tale tesi il governo tedesco ha evocato l'immagine dei vasi comunicanti, in virtù della quale un approccio meno rigoroso su uno dei tre aspetti individuati dalla Corte (ad esempio, l'accesso ai dati conservati) potrebbe essere compensato da un approccio più rigoroso per quanto riguarda gli altri due aspetti (la durata della conservazione nonché la sicurezza e la protezione dei dati)", par. 220. L'Avvocato generale appariva fortemente critico rispetto a tale posizione, ritenendo che una teoria dei 'vasi comunicanti' finisse per svilire totalmente l'utilità e l'efficacia delle tutele proposte dalla CGUE.

dei giudici di Lussemburgo stessi; questi ultimi infatti non solo non si sono pronunciati così chiaramente ed espressamente sul carattere cumulativo ed obbligatorio di tutti i criteri indicati ma non hanno neppure seguito la linea più stringente invocata dall'Avvocato, che aveva proposto di prevedere l'obbligo di conservazione dei metadati in ciascun singolo territorio nazionale: la CGUE infatti sul punto parla di conservazione entro i confini dell'UE; sotto questi profili – e solo rispetto ad essi – la posizione di Saugmandsgaard Øe è certamente più rigida di quella adottata nella sentenza finale.

Il punto di maggiore lontananza rinvenibile tra la pronuncia *Tele2* e le Conclusioni dell'Avvocato resta tuttavia certamente quello relativo alla legittimità di una forma di conservazione generalizzata e indiscriminata, considerata dai giudici *per se* incompatibile con il diritto dell'UE, indipendentemente dalle tutele caratterizzanti la successiva fase dell'accesso nonché le condizioni di conservazione stessa, mentre in questo la posizione dell'Avvocato si è mostrata più flessibile e non così netta. Allontanandosi quindi dalla visione proposta da alcuni Stati membri, tra cui la Svezia, nonché da quella dell'Avvocato generale, i giudici di Lussemburgo hanno voluto non solo cristallizzare quanto già affermato nella sentenza *DRI* ma applicare con maggiore rigidità i requisiti di proporzionalità e stretta necessità, adottando un approccio restrittivo. Ne esce una rilettura del tradizionale dibattito sul bilanciamento tra riservatezza-sicurezza volta a proporre strumenti di lotta e indagine della criminalità grave conformi ai diritti fondamentali grazie ad una serie di stringenti salvaguardie e condizioni. Le questioni derivanti da questo approccio, che trova le sue radici già nella pronuncia del 2014, sono state, come facile immaginare, di significativa portata ed hanno condotto i legislatori e i giudici nazionali ad interrogarsi ancora sulla disciplina della *data retention* e sulla corretta attuazione della giurisprudenza europea.

5. – Conservazione dei metadati e tutela dei diritti fondamentali alla luce della 'data retention saga': un difficile punto di equilibrio in cerca di definizione

5.1. – Le implicazioni di natura sostanziale derivanti dalle sentenze DRI *e* Tele2*: dubbi e timori sulla concreta efficacia, realizzabilità e legittimità di una* targeted data retention

Alla luce dalla previa analisi e guardando alla portata complessiva della pronuncia *Tele2*, non si può che concordare con l'affermazione secondo cui "If the judgement in *DRI* was far-reaching, the Court of Justice's judgement in *Tele2* was even more radical in a number of important respects"[129]. Alcuni di questi profili particolarmente significativi e determinanti, sono connotati da un carattere 'sostanziale' e hanno un forte impatto sul bilanciamento tra sicurezza, riservatezza e protezione dei dati proposto dalla Corte sin dalla previa sentenza *DRI*. Altri profili innovativi emersi dalla sentenza esaminata, invece,

A supporto della propria posizione proponeva alcuni efficaci esempi: "L'effetto distruttivo di siffatta tesi può essere facilmente illustrato mediante i seguenti esempi. Un regime nazionale che limitasse rigorosamente l'accesso ai soli fini della lotta al terrorismo e che limitasse la durata di conservazione a tre mesi (approccio rigoroso quanto all'accesso e alla durata di conservazione), ma che non obbligasse i fornitori a conservare i dati sul proprio territorio nazionale e in forma criptata (approccio permissivo quanto alla sicurezza), esporrebbe tutta la propria popolazione a un rischio elevato di accesso illegale ai dati conservati. Analogamente, un regime nazionale che prevedesse una durata di conservazione di tre mesi nonché una conservazione dei dati sul proprio territorio nazionale e in forma criptata (approcci rigorosi quanto alla durata e alla sicurezza), ma che consentisse a tutti i dipendenti di tutte le autorità pubbliche di accedere ai dati conservati (approccio permissivo quanto all'accesso), esporrebbe tutta la propria popolazione a un rischio elevato di abusi da parte delle autorità nazionali.", par. 225. Ecco perché l'Avvocato generale ribadiva che i requisiti della previa autorizzazione da parte di una autorità amministrativa indipendente o giudiziaria con riferimento all'accesso, l'obbligo di distruzione dei dati conservati alla scadenza del periodo indicato, la limitazione della durata di conservazione, l'obbligo di conservazione sul territorio nazionale di ciascuno Stato membro fossero tutte condizioni imperative e che dovevano pertanto "accompagnare un obbligo generale di conservazione dei dati al fine di limitare allo stretto necessario la lesione dei diritti sanciti dalla Direttiva 2002/58 e dagli art. 7 e 8 della Carta", par. 244.

[129] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, op. cit., p. 16.

hanno un profilo maggiormente 'formale' e inducono a svolgere alcune profonde riflessioni sul ruolo della Corte di giustizia dell'UE e del suo rapporto con il legislatore europeo e nazionale, nonché sulla delicata questione della divisione di competenze tra Stati membri ed Unione europea. Come si vedrà, con riferimento ad entrambi questi aspetti permanevano, anche a seguito della *Tele2*, significativi dubbi ed interrogativi, che permettono di comprendere da un lato – e ancora una volta – la complessità della disciplina della *data retention* e delle questioni ad essa connesse e, dall'altro, le ragioni che hanno portato numerose Corti nazionali a rinviare nuovamente alla Corte di giustizia su tale tematica, tutt'altro che definita.

Prendendo avvio dalle considerazioni di carattere più sostanziale, uno dei punti di maggior rilievo è sicuramente da riscontrarsi nella posizione attinente alla disciplina della conservazione dei dati, considerata *in se* e quindi indipendentemente dalla successiva fase dell'accesso: la sentenza *Tele2* è giunta infatti ad affermare, con maggiore chiarezza e forza rispetto alla previa pronuncia *DRI*, l'incompatibilità con il diritto dell'UE di una normativa nazionale che preveda, per finalità di lotta alla criminalità, una conservazione generalizzata ed indifferenziata. Con tale posizione, i giudici di Lussemburgo hanno espresso una più netta chiusura verso forme di *bulk data retention*, bocciando quella interpretazione maggiormente flessibile che molti Governi nazionali avevano abbracciato a seguito della invalidazione della DRD. Se all'indomani della prima sentenza della Corte in materia si era registrato, come si è visto, il tentativo di far salve le normative statali che sancivano un obbligo di conservazione generalizzato purché fossero accompagnate da tutele specifiche sulla sicurezza dei dati e sull'accesso ad essi, la decisa posizione espressa nella pronuncia *Tele2* ha sin da subito portato a significative prese di posizione da parte degli Stati membri: i legislatori nazionali hanno manifestato la propria difficoltà nel predisporre discipline in materia di conservazione dei metadati per scopi securitari che fossero conformi ai principi delineati dalla giurisprudenza della CGUE e, al contempo, utili ed efficaci strumenti di indagine nelle mani delle autorità di *law enforcement*. In questo contesto, la criticità maggiore e le più profonde perplessità erano riscontrate nella 'soluzione' proposta e promossa dai giudici di Lussemburgo che, con grande chiarezza rispetto alla previa giurisprudenza, avevano individuato quale unica possibile e legittima forma di conservazione dei metadati quella mirata. Ebbene, rispetto ad essa, i governi degli Stati membri, la dottrina e molte autorità europee avevano da tempo manifestato, sin da prima della sentenza *Tele2*, dubbi e resistenze, evidenziando come la *targeted data retention* fosse stata ideata dalla Corte stessa senza che alcuna parte nel corso del giudizio ne avesse mai menzionato l'opportunità e realizzabilità e senza che una tale soluzione fosse stata considerata sotto il profilo della efficacia, cioè "without referring to any evidence which supported either the feasibility or utility of targeted retention"[130]. L'idea di poter limitare la conservazione a specifiche aree geografiche o soggetti era stata fortemente criticata sin dagli accenni che ad essa aveva fatto la Corte nella sentenza *DRI*: in occasione del già richiamato *Consultative forum of Prosecutors General and Directors of Public Prosecutors of the MSs of the EU* e dello specifico *Workshop on data retention in the fight against serious crime: the way forward*, tenutisi in data 11 dicembre 2015 e ai quali avevano partecipato rappresentanti delle autorità di *law enforcement* degli Stati membri, era emerso un approccio favorevole a mantenere una conservazione generalizzata dei dati, ritenuta essenziale e insostituibile, basandosi su una lettura della sentenza *DRI* come non determinante l'illegittimità *tour court* della *bulk data retention*. L'alternativa avanzata dalla CGUE di ricorrere ad una conservazione mirata era parsa del resto irrealizzabile ed inutile: "While it is possible to differentiate technically and legally between categories of data, limiting retention to specific categories or particular persons reduces the effectiveness of investigations and may apply nebulous distinctions, leading to allegations of prejudice, profiling and unlawful discrimination. Moreover, as a matter of law, 'limited' data retention constitutes surveillance or preservation of data (not 'data retention' as such)". Tale ragionamento aveva spinto, come già

[130] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, op. cit., p. 14.

rilevato, ad indicare come unica percorribile soluzione quella di accompagnare una conservazione generalizzata con maggiori e più profonde tutele relative alla fase successiva ed eventuale dell'accesso ai metadati: "properly regulating access to data is likely to be part of the solution to overcome challenges related to the existing fragmented legal framework in the EU. The right to privacy can be adequately protected by the introduction of effective procedural safeguards regarding access to data. Such procedural safeguards should include e.g. (a) prior authorisation by an independent judicial authority; (b) limitations on the purpose of access and persons entitled to access; (c) management regulations; (d) linkage of access to the seriousness of the crime; (e) assessment of proportionality; (f) evaluation of alternative investigative techniques; (g) destruction of data following the retention period; and (h) exceptions for certain professionals bound by the duty of confidentiality. However, a special regime for certain professional categories may open the way to impunity gaps. Reliable security conditions relating to storage – including location within the EU – are critical. Having a common retention period is crucial: the general view is that it should be longer than six months, preferably a minimum of one year"[131].

A ciò è da aggiungersi che, come anche la dottrina aveva sottolineato, una *targeted data retention* posta in essere sulla base di criteri soggettivi o geografici avrebbe finito col porre problemi in termini di rispetto del diritto di non discriminazione: "while this power [to use the geographic criterion] would enable temporary monitoring of large public gatherings (such as sporting events), it also raises the spectre of permanent monitoring of, not simply zones surrounding government offices and other obvious terrorist targets, or even targets of organized crime, such as concentrations of banks, but, more disturbingly, large urban areas with marginalized populations, such as immigrants communities"[132]. Del resto, su questo specifico aspetto della legittimità e utilità di una conservazione targettizzata, anche l'Avvocato generale Saugmandsgaard Øe nelle proprie Conclusioni relative al rinvio *Tele2* aveva mostrato significative perplessità: "Una limitazione sostanziale della portata di un obbligo generale di conservazione dei dati rischia di ridurre considerevolmente l'utilità offerta da tale regime nella lotta contro i reati gravi. Da una parte, diversi governi hanno sottolineato la difficoltà o addirittura l'impossibilità di determinare in anticipo i dati che possano presentare un collegamento con un reato grave. Pertanto, una siffatta limitazione rischia di escludere la conservazione di dati che potrebbero rivelarsi rilevanti ai fini della lotta contro i reati gravi. Dall'altra, come ha sostenuto il Governo estone, la criminalità grave è un fenomeno dinamico, capace di adattarsi agli strumenti investigativi di cui dispongono le autorità di contrasto. Pertanto, una limitazione a un'area geografica o a un mezzo di comunicazione determinati rischierebbe di provocare un trasferimento delle attività legate ai reati gravi verso un'area geografica e/o un mezzo di comunicazione non coperti da detto regime" (Par. 213-214, Conclusioni). L'Avvocato generale, a supporto di tali considerazioni, aveva riportato anche la relazione elaborata dal Conseil d'État francese (Consiglio di Stato), dal titolo *Le numérique et les droits fondamentaux*, del 2014 – citato dal Governo francese nelle memorie presentate alla CGUE stessa nel caso *Tele2* –: in tale documento, veniva sottolineato come un sistema di sorveglianza mirata e targettizzata "sarebbe nettamente meno efficace della conservazione sistematica dal punto di vista della sicurezza nazionale e della ricerca degli autori di reati. Infatti, esso non consentirebbe un accesso retrospettivo agli scambi che hanno avuto luogo prima che l'autorità individuasse una minaccia o un reato: il suo carattere operativo dipenderebbe quindi dalla capacità delle autorità di conoscere in anticipo l'identità delle persone i cui dati di connessione possano essere utili, il che è impossibile nell'ambito della polizia giudiziaria. Ad esempio, nel caso di un reato, l'autorità giudiziaria non potrebbe avere accesso alle comunicazioni precedenti a quest'ultimo, elementi tuttavia preziosi e talvolta persino indispensabili per l'identificazione del suo autore e dei suoi complici, come hanno dimostrato casi

[131] *Report of the Consultative forum of Prosecutors General and Directors of Public Prosecutors of the MSs of the EU and of the Workshop on data retention in the fight against serious crime: the way forward*, 11 dicembre 2015, p. 9.
[132] I. CAMERON, *Balancing data protection and law enforcement needs*, op. cit., p. 1489.

recenti di attentati terroristici. Nel campo della prevenzione degli attentati alla sicurezza nazionale, i nuovi programmi tecnici si basano su una capacità di rilevamento dei segnali deboli, incompatibile con l'idea dell'individuazione preventiva delle persone pericolose"[133]. Una tale visione è stata peraltro ribadita non solo da alcuni commentatori della sentenza *Tele2*, particolarmente critici quanto alla reale possibilità di attuare forme utili di conservazione seguendo i criteri indicati dai giudici europei[134], ma anche, in un momento successivo alla pronuncia *Tele2,* da Europol nel documento *Proportionate data retention for law enforcement purposes*, come riportato dalla dottrina: "a data retention measure that is 'targeted', as CJEU provides in the Digital Rights Ireland and Tele 2 Sverige rulings, is practically impossible, since the 'potential relevance amongst data and the purposes pursued cannot be foreseen in advance'. In this way, EUROPOL seems to provide for an interpretation that would 'fit for law enforcement reality', where 'restricted' data retention may still be considered to abide by the CJEU requirement as discussed above, since, in the opinion of EUROPOL, the subsequent access to the retained data must always be 'targeted'. This wordplay portends to the confusion that may be born in relation to the interpretation and implementation of the judicial criteria and the surrounding requirement of objectivity on measures ordering data retention within private databases and access to the data by security actors in general, and for the purpose of prevention of crime in question"[135].

Per completezza tuttavia merita sottolineare come alle critiche mosse avverso una visione troppo "rights-oriented" della giurisprudenza europea, ritenuta sproporzionatamente ed eccessivamente impattante su una effettiva ed efficiente tutela della sicurezza e della lotta alla criminalità grave[136], è da riscontrarsi anche una critica di senso opposto, da parte di chi ha ritenuto lacunoso e carente il ragionamento della Corte nella parte in cui non veniva considerata la reale efficacia dell'adozione di sistemi, anche solo targettizzati, di conservazione dei metadati. In altre parole, alcune ONG, nonché parte della dottrina e della società civile hanno mostrato preoccupazioni quanto al fatto che i giudici, pur essendo giunti alla conclusione che una *bulk data retention* sia da considerarsi sproporzionata, non abbiano basato su elementi empirici la propria valutazione circa l'adeguatezza della conservazione stessa e cioè la sua idoneità a raggiungere l'interesse legittimo della lotta alla criminalità grave. Ciò che viene ritenuto preoccupante quindi è la sbrigatività con la quale la Corte ha affermato l'idoneità dello strumento della *data retention*: "the Court did not base its ruling on evidence relating to the effectiveness of the instrument of the data retention. The ruling is rather based on a theoretical reasoning that data

[133] Conclusioni Avvocato generale, nota 54.

[134] "Removing a general duty of retention thus severely undermines the investigative ability of the police and intelligence services. It does not totally remove the usefulness of metadata as an investigative tool. When a serious crime, e.g. a murder or armed robbery, has been committed in a given area, the relevant base station can still be emptied, and the active devices in the zone can be identified. But it becomes very much more difficult to identify suspicious devices if there is no historical data to link these to. The communications in the future of persons of interest can be tagged and made subject to a data preservation order, but criminals constantly change their phones and without some historical data, there will be 'black spots' and contact chaining in many cases will be made much more difficult, or even impossible", I. CAMERON, *Balancing data protection and law enforcement needs*, op. cit., p. 1483 e della stessa opinione anche D. FENNELLY in *Data retention: the life, death and afterlife of a directive*, op. cit.

[135] P. VOGIATZOGLOU, *Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity*, in *European Journal of Law and Technology*, 1, 2019, p. 8.

[136] Proprio in una delle molteplici occasioni di dibattito sul tema della *data retention* organizzate da Europol, è stata significativamente riassunta la forte e sentita discussione in materia, determinata "amongst those who deem data retention an indication for the rise of a police state versus those who consider it indispensable in the fight against serious crime and terrorism. A key message conveyed was that law enforcement is not advocating the general or indiscriminate retention of any available information, but is making best efforts to implement the criteria established by the ECJ. Nonetheless, it aimed at raising awareness on the severe detrimental consequences of the status-quo", EUROPOL, *Conference report: freedom AND security. Killing the zero sum process,* 23 novembre 2018, p. 18.

retention genuinely satisfies an objective of general interest"[137]. Questa critica apre ad un ampio ma interessante dibattito, di cui si parlerà ampiamente nel Capitolo IV, circa l'importanza che qualsiasi valutazione sulla compatibilità con i diritti fondamentali di strumenti di conservazione dei metadati sia fondata sulla previa determinazione della reale necessità ed utilità di forme di sorveglianza, aspetti questi tutt'altro che condivisi e assodati e che meritano pertanto una debita riflessione, capace di influire sul bilanciamento da effettuare e sulla proporzionalità e stretta necessità dell'ingerenza nei diritti fondamentali.

Tutti questi profili sostanziali, appena rilevati, attinenti alla necessità ed adeguatezza di strumenti di conservazione dei metadati così come alla fattibilità ed utilità di forme mirate di *data retention*, estendono i propri effetti in almeno altre due direzioni: innanzitutto, affermando con maggior chiarezza l'incompatibilità al diritto europeo di forme di conservazione generalizzata, la giurisprudenza esaminata conferma timori e perplessità, già sorti a seguito della sentenza *DRI*, circa la legittimità di sistemi di raccolta, conservazione e accesso a diversi dati, basati sempre su una memorizzazione e *retention* di tipo indiscriminato, quali la raccolta, conservazione e/o trasferimento di PNR, sia all'interno che all'esterno dei confini europei. Sebbene questo delicato quanto complesso profilo verrà meglio analizzato nel Capitolo III, pare utile sin da ora sottolineare come "The Court's ruling has significant implications not only in questioning the constitutionality of data retention frameworks, but also in questioning the compatibility with the Charter of the surveillance systems established and legitimised by the transatlantic PNR and TFTP Agreements as well as the proposals for an internal EU PNR and TFTP instruments"[138].

Un ulteriore ed altrettanto preoccupante impatto della pronuncia *Tele2* è da rilevarsi sul piano strettamente nazionale: come incide la nuova posizione della Corte – e la relativa determinazione di criteri specifici circa conservazione e accesso ai metadati – sulle normative statali, in particolare con riferimento alle disposizioni sulla base delle quali sono state raccolte prove, talvolta determinanti in procedimenti penali? Laddove cioè i metadati, capaci di rivelare informazioni di estrema importanza – ad esempio relativi alla ubicazione di un soggetto che ha effettuato una chiamata in un determinato momento –, siano stati ottenuti grazie alla sussistenza di forme di conservazione generalizzata da considerarsi sproporzionate e lesive dei diritti fondamentali, come debbono essere valutate tali informazioni? Facile immaginare quali potrebbero essere le conseguenze di una dichiarata illegittimità delle prove fondate su metadati conservati illegittimamente. Queste, come ben comprensibile, sono conseguenze pratiche di estrema rilevanza, soprattutto nel contesto nazionale e non sono dunque sfuggite ai Governi degli Stati membri, alle Corti e neppure alla dottrina: mentre, come si vedrà approfonditamente nel Capitolo IV, la Corte costituzionale belga ha posto tale specifico e diretto quesito alla Corte di giustizia, nel rinvio pregiudiziale C-520/18, sempre vertente sulla interpretazione dell'art. 15 Direttiva *e-Privacy*, il più recente rinvio in materia di *data retention* avanzato dalla Corte Suprema irlandese ha avuto origine proprio da un procedimento penale nel quale il Sig. Dwyer, accusato di omicidio sulla base dei metadati relativi al proprio telefono cellulare, ha ritenuto tali prove illegittime in quanto fondate sulla normativa irlandese attuativa della DRD e dunque non compatibile con il diritto dell'UE e la Carta di Nizza. Questo caso e le fortissime implicazioni che ne potrebbero derivare in ambito penale negli Stati membri contribuiscono ancora una volta a comprendere quanto delicata sia la questione in esame e quanti i profili sostanziali ad essa connessi.

Tutte le problematiche e criticità sorte a seguito della pronuncia *Tele2* ed evidenziate in questo paragrafo, emergono del resto con evidenza nel documento redatto da Eurojust per il Consiglio dell'UE

[137] H. HIJIMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 116 TFEU*, Springer, 2016.
[138] S. MITSILEGAS, *Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime*, in *Columbia Human Rights Law Review*, 3, 2016, p. 19.

nel novembre 2017 e reso pubblicamente accessibile nel 2019[139]: "the vast majority of the Countries do not have targeted data retention rules within categories of location/traffic data, users/subscribers and means of communication (internet/telephone); one Country (DE) reported that it excludes some targeted users/subscribers from the retention obligation in the legislation that is to come into force in July 2017 (..); finally some countries reported that they do not have data retention laws for law enforcement purposes only, following the annulment of their previous laws by their constitutional/high courts in accordance with the DRD judgement (..). It can be concluded that none of the Countries have national legislation that obliges the targeted retention of data linked to specific persons or geographical locations" (p. 6). Ecco perché dinnanzi alle difficoltà, quando non reticenze, degli Stati membri ad apportare modifiche e a ridimensionare l'estensione della conservazione dei dati, ciò che alcuni autori avevano ipotizzato, già all'indomani della sentenza *Tele2* era l'adozione da parte degli Stati membri di c.d. "defensive reactions", basate su una concezione che potesse, ancora una volta, far salva una forma di conservazione generalizzata. Tale interpretazione, in questo caso ancor più complessa rispetto a quella promossa a seguito della *DRI*, si basa sulla concezione secondo cui solo una conservazione che interessi al contempo tutti gli utenti, tutti i metadati e tutti i mezzi di comunicazione sia da intendersi non conforme al diritto dell'UE. In altre parole, "States may argue that the Court has only ruled out the general *and* indiscriminate retention of *all* traffic and location data of *all* subscribers and registered users relating to *all* means of electronic communications. If simply removing one category of traffic data from the retention obligation means that it is not general, then the judgement will be easy to comply with"[140]. Questi aspetti ben verranno sottolineati in quei rinvii pregiudiziali ad oggi pendenti, di cui ci si occuperà nel Capitolo IV, e che muovono, nella maggior parte dei casi, proprio dal tentativo dei Governi di promuovere, di nuovo e anche dinnanzi alla più chiara posizione espressa in *Tele2*, una lettura maggiormente permissiva e flessibile della giurisprudenza della CGUE.

5.2. – Interrogativi ancora aperti sotto il profilo formale: dal significato di 'gravità' del reato al riparto di competenze tra UE e Stati membri

Se dunque quelli indicati sino ad ora sono i rilevanti profili problematici sul piano sostanziale, la sentenza *Tele2* ha lasciato aperti anche numerosi interrogativi sotto il profilo più strettamente formale, pure in grado di incidere con forza sulle questioni sostanziali e sul bilanciamento operato dalla Corte stessa.

Un primo dubbio è da individuarsi con riferimento al carattere di "gravità" del reato, delineato come elemento fondamentale per garantire la proporzionalità della ingerenza nei diritti fondamentali degli utenti: come si è già evidenziato, nel testo dell'art. 15 della Direttiva *e-Privacy* si parlava unicamente e ben più genericamente dello scopo di "prevenzione, ricerca, accertamento e perseguimento dei reati", senza alcun accenno al carattere di 'gravità' del reato, che quindi, con riferimento alla disciplina derogatoria prevista nell'art. 15, veniva individuato come necessario ed imprescindibile requisito solo dalla giurisprudenza della CGUE, che pure non ne stabiliva le caratteristiche o gli elementi da considerare. Non deve dunque stupire che i legislatori nazionali abbiano interpretato in maniera assai differente il livello di serietà del reato tale da determinarne il carattere 'grave', manifestando anche perplessità e difficoltà nello stabilire tale aspetto: proprio tale elemento sarà, non a caso, al centro di un nuovo rinvio pregiudiziale, culminato con la pronuncia *Ministerio Fiscal*, che verrà analizzata nel Capitolo IV.

---

[139] EUROJUST, *Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15*, 6 novembre 2017, reso parzialmente accessibile il 6 giugno 2019 (10098/17 Eurojust 91).
[140] I. CAMERON, *Balancing data protection and law enforcement needs*, op. cit., p. 1486.

Altra profilo problematico, che trova le sue radici sin dalla sentenza *DRI*, è quello relativo alla scelta di fondare sulla distinzione tra contenuto e metadati la determinazione dell'ingerenza o meno nel contenuto essenziale dei diritti alla riservatezza e alla protezione dei dati. Come si è in parte già detto e come si avrà modo di approfondire nel Capitolo III, tale differenziazione, confermata ed anzi ulteriormente arricchita nella sentenza *Schrems* e ripresa nella successiva *Tele2*, desta non poche perplessità: la compressione del 'nucleo essenziale' dei diritti di cui agli artt. 7 e 8 della Carta di Nizza, individuata solo laddove la conservazione o il trattamento dei dati riguardino il contenuto delle comunicazioni pare infatti contrastare con quella consapevolezza lungimirante dimostrata della stessa Corte – ma affermata con chiarezza anche dagli Avvocati generali nella cause *DRI* e *Tele2* – che ha riconosciuto invece l'invasività e la capacità di ricostruire la vita privata di ciascun utente, le sue abitudini, preferenze e spostamenti, anche a partire dai soli metadati, letti in maniera aggregata, senza alcun bisogno di vagliarne i contenuti. Proprio tale considerazione, a parere di molti commentatori e studiosi, rende semplicistica, obsoleta e non realistica una individuazione della lesione del nucleo essenziale dei diritti fondamentali in gioco solo laddove le misure normative prevedano un impatto sul contenuto delle comunicazioni[141]. Come evidenziato da Brkan, sebbene nella sentenza *Tele2* emerga con ancora più forza il riconoscimento di equivalenza tra contenuti e metadati[142], "the mantra of interference with the essence of fundamental right to privacy whenever the measure allows access to content of electronic communications strangely persists in both the Court's and Advocate General's further reasoning in Tele2 Sverige"[143], rilevando quindi una tensione e una incongruenza nel ragionamento adottato. Per questo gran parte della dottrina giunge alla conclusione che l'artificiale distinzione promossa dalla Corte debba essere rimossa: "removing the distinction between communications data and content data in terms of the level of human rights protection is a first step towards a more realistic appraisal of surveillance practices"[144]. Pur rimandando al successivo Capitolo per una ulteriore analisi di questo profilo, ciò che si vuole sin da ora evidenziare è come la sentenza *Tele2* non abbia risolto i dubbi interpretativi derivanti da tale posizione, che rimane dunque ancora aperta e dibattuta.

---

[141] "When it [the Court] summarily dismisses any interference with the essence of privacy and data protection rights, the Court unfortunately reverts to an out-dated perspective, according to which the collection of metadata is less sensitive simply because it does not concern the content of communications. This hierarchical and formalistic perception is increasingly contested. In certain instances, even a single communications event can reveal as much of someone's personal circumstances as the interception of the communications content. What is even more disturbing, the Directive [DRD] makes it possible to construct rich longitudinal metadata about a person's activities over an extended period. Six months of metadata from a mobile phone reveal the user's social network, location profile, commuting patterns and so on. The retention, use and abuse of metadata are thus liable to affect the essence of the right to privacy as much as the interception of communication content", M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, op. cit., p. 847. Ancora più esplicitamente Ojanen, che afferma: "the Court's reliance on the distinction between content and metadata can certainly be criticized as being orthodox and even obsolete. After all, the distinction between the content of the electronic communications and such metadata as traffic data and location data is rapidly fading away in a modern network environment. A lot of information, including sensitive information, about an individual can easily be revealed by monitoring the use of communications services through traffic data collection, storage and processing. Hence, the processing of metadata cannot any longer be invariably seen as falling with such 'peripheral areas' of privacy where limitations would be permissible more easily than in the context of the content of electronic communications", T. OJANEN, *Rights-based review of electronic surveillance after DRI and Schrems in the European Union*, op. cit., p. 24.

[142] Si fa riferimento ai par. 255-259 delle Conclusioni dell'Avvocato generale nonché al par. 99 della sentenza della Corte, che ha affermato: "tali dati [metadati] forniscono gli strumenti per stabilire il profilo delle persone interessate, informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni".

[143] M. BRKAN, *The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning,* in *German Law Journal*, 20, 2019, p. 873.

[144] D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, in *Israel Law Review*, 1, 2019, p. 54.

Restano infine notevoli incertezze quanto alle finalità e agli ambiti rispetto ai quali i principi e criteri delineati dalla CGUE debbono applicarsi: in particolare dubbi permangono con riferimento alle operazioni di conservazione e accesso a metadati effettuati per scopi di sicurezza nazionale da parte di agenzie di intelligence. Ai sensi del già richiamato art. 4 TUE, infatti, la sicurezza nazionale deve considerarsi competenza esclusiva degli Stati membri, al di fuori dell'ambito di applicazione del diritto dell'UE. Il rispetto dei principi sanciti dalla giurisprudenza della Corte di giustizia e delle condizioni di legittimità derivanti dalla Carta di Nizza sarebbe quindi obbligatorio e vincolante solo per le attività compiute dalle autorità di *law enforcement* per finalità di repressione e indagine di crimini gravi. Una applicazione estensiva dell'art. 15 Direttiva *e-Privacy* – e dei limiti che accompagnano la possibilità di derogare alla normativa generale – anche alle operazioni volte a garantire la sicurezza nazionale risulterebbe, ad opinione di alcuni studiosi, contraria alla limitazione dettata dall'art. 1, co. 3 della Direttiva *e-Privacy* stessa, ponendo problemi anche quanto al principio di attribuzione e della divisione delle competenze tra Stati membri e UE, "emphazising the fragility of the principle of conferral in an era of increasing judicial activism in Luxembourg. While both art. 6 TEU and Art. 51 of the Charter provide that the Charter shall not expand the competence of the Union, the judgement in *Tele2* leaves open to question the extent to which respect for this constitutional principle is always observed in practice. While the extension of competence in this way in the field of crime may be understood in light of the ill-fated legislative intervention at EU level through the DRD, what is perhaps of most concern – from the perspective of the principle of conferral – is that the same reasoning could justify the extension of EU competence into the field of national security"[145]. Certamente la rigida distinzione tra materia penale e misure che attengono il funzionamento del mercato interno, e dunque le problematiche relative alle competenze e al tipo di intervento dell'UE, sono venuti a mancare a seguito della entrata in vigore del Trattato di Lisbona e dell'abbandono di quella struttura a pilastri che aveva creato così tante incertezze quanto alle discipline, come quella della conservazione dei dati, che si trovavano "a cavallo" tra diverse aree. Nondimeno, anche in tale mutato assetto normativo la questione evidenziata apre a numerose e serie problematiche. Se, infatti, un divieto di conservazione generalizzata dovesse estendersi anche ad attività di intelligence, che utilizzano prevalentemente strumenti di *bulk retention*, ci si troverebbe dinnanzi al rischio di inficiare e paralizzare l'attività stessa di tali servizi. Ciò impone anche di addentrarsi in profonde e concrete riflessioni sul funzionamento e sugli strumenti adoperati dai diversi soggetti operanti nell'ambito della sicurezza e sintetizzabili in un unico interrogativo: è ancora possibile al giorno d'oggi distinguere tra attività svolte per finalità di sicurezza nazionale e quelle invece volte a scopi di sicurezza pubblica e, conseguentemente, sottrarre le prime dall'ambito di applicazione del diritto europeo? Viene infatti sempre più sottolineata la difficoltà di tracciare una netta e precisa distinzione tra i metodi impiegati da agenzie di intelligence e quelli invece proprie delle autorità di *law enforcement*: come anticipato nella Parte I e come si vedrà ampiamente nei Capitoli IV e V (in quest'ultimo con riferimento alla giurisprudenza della Corte EDU), i sistemi utilizzati per scopi securitari si assomigliano sempre più, rendendo complesso tracciare una linea di demarcazione sulla base della sola diversità dei soggetti che operano e delle tecniche impiegate. Nella sentenza *Tele2* i giudici parlano di conservazione finalizzata a contribuire alla lotta contro la criminalità grave o alla prevenzione di gravi rischi per la sicurezza pubblica (par. 111, *Tele2*); l'unico riferimento che viene promosso rispetto alla sicurezza nazionale è quello indicato al par. 119, nel quale la Corte ammette un accesso più ampio e meno targettizzato laddove sussista l'esigenza di proteggere interessi vitali della

[145] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, op. cit., p. 13. Ma anche Cameron ha affermato: "bulk retention of metadata is already a feature of a certain type of State body, namely signals intelligence agencies. It can therefore be envisaged that the judgement will be used as a tool to demand tighter control over signals intelligence agencies, even though EU States which have such agencies will insist that they clearly fall outside of EU competence by virtue of the exclusion of national security (art. 4(2) TEU)", I. CAMERON, *Balancing data protection and law enforcement needs*, op. cit.

sicurezza nazionale minacciati da attività di terrorismo: una maggiore flessibilità viene dunque riconosciuta in tali casi anche se unicamente per quanto attiene all'accesso e non anche alla conservazione. La Corte inoltre non ha mai avuto modo di raffrontarsi con sistemi che prevedano intercettazioni dirette da parte di autorità di *law enforcement* o di intelligence, rispetto ai quali ci si chiede dunque se i criteri stringenti indicati nelle pronunce sin qui esaminate siano da considerarsi applicabili. Come si vedrà nel Capitolo IV, proprio tali aspetti sono stati oggetto del rinvio pregiudiziale – ad oggi pendente – avanzato dal Regno Unito (*Privacy International* C-623/17), finalizzato a chiarire i limiti della giurisprudenza della CGUE in materia di conservazione e accesso per fini securitari e nel quale il giudice del rinvio non ha mancato di sottolineare le enormi conseguenze ed i pericoli che potrebbero derivare da una lettura eccessivamente estensiva dei requisiti delineati dai giudici di Lussemburgo anche ad ambiti di sicurezza nazionale, laddove ancora identificabili con chiarezza.

5.3. – Un dibattito acceso nonostante il duplice intervento della CGUE: una perdurante situazione di incertezza

In questa sintetica ricostruzione dei profili problematici emersi – anche – dalla sentenza *Tele2* e pur volendo rimandare ai capitoli successivi per analisi più approfondite di alcuni di essi, viene messo in luce come il dibattito, sul piano formale e sostanziale, in materia di conservazione ed accesso ai metadati per scopi securitari fosse – e sia – ancora acceso e ampio, nonostante il duplice intervento della Corte di giustizia.

Considerata questa premessa, alcune osservazioni generali possono essere tratte dalla analisi delle due sentenze esaminate in questo Capitolo, sia che le si consideri una importante conquista per la protezione dei diritti fondamentali, grazie alla loro portata restrittiva e maggiormente protettiva rispetto a pratiche di sorveglianza 'massiva' poste in essere dalle autorità pubbliche – anche sulla base di normative europee –, sia che le si ritenga, al contrario, eccessivamente impattanti sulla efficacia ed efficienza degli strumenti di lotta alla criminalità, stabilendo criteri troppo rigidi e difficilmente realizzabili nella pratica concreta da parte dei legislatori nazionali.

Senza dubbio la giurisprudenza sin qui analizzata in materia di *data retention* "shows a firm determination to rein in the state of exception and securitisation trends that infuse recent European anti-terrorism laws, and works to minimize their interference with important fundamental rights"[146]. L'UE quindi, mediante l'intervento della propria Corte, ha voluto fissare elevati standard di tutela dei diritti alla privacy e alla protezione dei dati, prendendo coscienza delle nuove minacce ed insidie derivanti dalle nuove tecnologie, inserendo quindi tali garanzie nello specifico contesto dell'era digitale e dei Big Data e, in particolare, del loro utilizzo sempre più ampio e sofisticato per finalità securitarie, dinnanzi alla minaccia costante e presente del terrorismo internazionale e dei crimini transnazionali[147]. Il

[146] M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland*, op. cit., p. 850. "The protection of fundamental rights should not depend on the political preferences of the day of a majoritarian body. We have seen that the Treaties underline the universal nature of these rights. However, practice shows that the actual state of a society determines what constitutes an intrusion. In the first decennium of this 21st century, we saw a relatively high legislative production for the protection of security relating to terrorist threats, post 9/11. These legislative measures were a reaction to threats that, also under the reasoning in Digital Rights Ireland and Seitlinger, may be proportionate, but exceeded the scope of the actual threat, by widening the purpose of the measure and by not containing a time limit", H. HIJIMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 116 TFEU*, Springer, 2016, p. 1319.

[147] Granger e Irion sottolineano come "there is a symbolic dimension to the fact that the strict scrutiny test was first applied to the right to privacy: 'the' human right in the information age" (M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland*, op. cit., p. 851), mettendo quindi in luce l'importanza dei diritti alla riservatezza e alla protezione dei dati nello specifico moderno contesto della società dell'informazione e della sempre più preponderante digitalizzazione.

bilanciamento promosso dai giudici di Lussemburgo trova coerente e decisa affermazione non solo rispetto alle scelte del legislatore europeo, come nella sentenza *DRI*, bensì anche con riferimento alle discipline adottate dagli Stati membri: "the Grand Chamber is increasingly building up a real and effective privacy shield to protect European values which are increasingly eroded by domestic legislation of Member States aiming to organize the fight against serious crime and terrorism"[148]. Proprio quest'ultimo approccio, riscontrato soprattutto nella sentenza *Tele2* nella quale i giudici di Lussemburgo forniscono un vero e proprio vademecum al legislatore nazionale, deve indurre ad una seria riflessione sul ruolo ricoperto dalla Corte di giustizia: da un lato, pur indicando quella che da più parti è stata definita una "detailed and demanding checklist that any data retention legislation, whether at national or EU level would satify", i giudici non si sono spinti – e per certi versi neppure avrebbero potuto farlo – a determinare nel dettaglio i concetti cui fa riferimento, quali ad esempio, come si è visto, il concetto di 'gravità del reato', la cui definizione da parte dei legislatori statali diviene però, in assenza di una specifica e chiara normativa europea in materia, un esercizio complesso della propria discrezionalità e passibile di risultare in soluzioni e approcci disomogenei che già in passato si erano problematicamente riscontrati; dall'altro un tale approccio incide sulle scelte e sul ruolo stesso tanto del legislatore europeo quanto di quello nazionale: come criticamente rilevato da alcuni commentatori, "in crafting a detailed code of this kind, the Court of Justice is arguably engaging in an excercise which would appear more legislative than judicial in its character, intervening in detailed matters of legislative and policy choice in a way that goes beyond what would appear necessary for the Court to reach its judgement. (..) The Court in effect constitutionalizes these detailed requirements. If such an approach was intended to serve as guidance for the legislature, this might be understandable. However, in the case of data retention, it appears to have had the contrary effect, inhibiting legislative action at EU and nation level"[149].

Nel determinare i criteri di necessità e proporzionalità sopra ampiamente analizzati, i giudici europei hanno certamente posto grande attenzione ai diritti alla privacy e alla protezione dei dati, anche laddove la loro compressione fosse motivata dall'interesse di garantire la sicurezza e di fornire strumenti efficaci alle autorità di *law enforcement* e di intelligence, dimostrando di "prendere davvero sul serio l'esigenza di tutelare un nuovo *digital right to privacy*, sforzandosi di adeguare alle caratteristiche tecniche del mondo dei *bit* quel *right to privacy* che Warren e Brandeis, per primi, nel 1890, avevano teorizzato"[150]. Pur stabilendo il carattere non assoluto dei diritti riconosciuti agli artt. 7 e 8 della Carta di Nizza, la giurisprudenza della Corte ha svolto un vaglio di proporzionalità e necessità attento e quanto mai rigido, tanto che alcuni commentatori hanno visto – più o meno criticamente – in tale posizione la volontà di riconoscere e attribuire ai diritti alla privacy il rango di "super-rights"[151].

---

[148] X. TRACOL, *The judgement of the Grand Chamber dated 21 December 2016 in the two joint Tele2Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level*, in *Comupter Law & Security Review*, 33, 2017, p. 552.

[149] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, op. cit., p. 17. In questo senso dunque le rigide condizioni previste dalla Corte nelle due pronunce analizzate hanno avuto l'effetto di "restringere uno spazio discrezionale – di autonomia procedurale per gli Stati membri – che la Direttiva del 2002 invece in origine dava per sotteso a tutti i casi in cui gli ordinamenti nazionali avessero introdotto eccezioni fondate su ragioni di pubblica sicurezza", F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa*, op. cit., p. 357.

[150] O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, 2015, p. 7.

[151] Come efficacemente riassunto da O'Leary, "these are not the first cases in which the ECJ had relied on the EU Charter to invalidate secondary EU law, but they have certainly become the most prominent. Indeed, it could be asked whether arts 7 and 8 of EU Charter have emerged as the most powerful and far-reaching EU Charter tools in the ECJ's post-Lisbon armament? No other EU Charter provisions, not even the defense rights enshrined in arts 47 and 48 which had been the subject of extensive case law via the EU general principles route pre-Lisbon, seem to have had an equivalent impact. Some commentators refer critically to the ECJ's elevation of these rights into 'super-rights' while others appear to applaud this nomenclature. The dividing line between the two camps appears

Al di là di queste considerazioni, sulle quali si tornerà più ampiamente anche nel Capitolo IV, a margine di una imprescindibile riflessione sui rinvii pregiudiziali pendenti, quello che le due importanti sentenze analizzate ben fotografano è come l'Unione europea abbia inizialmente affrontato la grande sfida del bilanciamento tra diritti fondamentali quali la riservatezza e la protezione dei dati da un lato e l'esigenza di garantire la sicurezza dall'altro: all'indomani delle rivelazioni di Snowden non solo gli Stati Uniti d'America ma anche l'UE è stata quindi chiamata a dare una risposta a tale complesso tema, nello specifico caso della disciplina della *data retention*. Complessità che emerge con grande chiarezza nelle efficaci e riassuntive parole dell'Avvocato generale nelle sue conclusioni alla controversia *Tele2*: Saugmandsgaard Øe infatti inizia le sue considerazioni richiamando la nota frase dell'autore James Madison, del 1788: "If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administred by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself". La "grande difficolta" richiamata da Madison, uno degli autori della Costituzione statunitense, può ben essere riscontrata nelle controversie di cui la CGUE si è dovuta occupare con riferimento alla disciplina della *data retention*: "da una parte, la conservazione dei dati relativi alle comunicazioni consente al governo di controllare i governati" (par. 2, Conclusioni), mediante la disponibilità di metadati che permettono di leggere il passato e dunque di avvalersi di dati prodotti da soggetti e relativi a momenti in cui tali utenti non potevano essere sospettati e collegati ad alcun reato grave; dall'altra parte, però, riprendendo la frase di Madison, risulta altrettanto fondamentale "obbligare il governo a controllare se stesso" e non solo i suoi consociati: ecco quindi che viene riconosciuta la necessità di stabilire normative, requisiti e condizioni appropriate al fine di limitare il potere di controllo delle autorità pubbliche a quanto necessario e proporzionato. Dinnanzi a tale difficoltà, è compito della Corte e dei giudici del rinvio definire un "punto di equilibrio tra l'obbligo incombente agli Stati membri di garantire la sicurezza delle persone che si trovano sul loro territorio e il rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati di carattere personale sanciti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE" (par. 5, Conclusioni).

Se però il precario punto di equilibrio, la cui determinazione è stata attribuita, nel silenzio del legislatore europeo, al giudice di Lussemburgo, non è stato con chiarezza individuato neppure nella sentenza *Tele2*, nella quale non sono stati risolti i profili problematici derivanti dalla disciplina della *data retention* e le numerose criticità, anche applicative, già emerse a seguito della sentenza *DRI*, la chiusura di questo Capitolo non può essere individuata in una perdurante situazione di incertezza e in un potenziale pericoloso proseguimento di una situazione di disomogeneità tra i vari Stati membri. Ecco quindi che Eurojust significamente rileva come "In this light, consideration of the development of a

to be the perspective or discipline from which one approaches the subject - data protection experts, national security experts, EU lawyers generally and fundamental rights specialists divide along different lines", S. O'LEARY, *Balancing rights in a digital age*, in *Irish Jurist*, 59, 2018, p. 87. Si pensi, ad esempio, a C. Kuner che in "*A super right to data protection? The Irish Facebok case and the future of EU data transfer regulation* (in *LSE Blog* del 24 giugno 2014, disponibile all'indirizzo https://blogs.lse.ac.uk/medialse/2014/06/24/a-super-right-to-data-protection-the-irish-facebook-case-the-future-of-eu-data-transfer-regulation/), si mostra estremamente critico rispetto all'approccio della CGUE verso la tutela del diritto alla privacy e protezione dei dati, ammonendo i giudici: "it is important that the CJEU not forget that, as it has stated in the past, data protection is not an absolute right, and must be considered in relation to its function in society". Di altro avviso è invece Scheinin che reputa appropriata, proporzionata e necessaria la valutazione della Corte nella sua giurisprudenza in materia di *data retention*, in M. SCHEININ, *Towards evidence-based discussion on surveillance*, in *European Constitutional Law Review*, 12, 2016, p. 347; Ojanen infine ritiene che il fatto che la posizione della Corte quanto alla incompatibilità con il diritto dell'UE di sistemi di conservazione o accesso generalizzato non produca quale effetto quello di "elevate privacy to a supreme fundamental right", ma che ciò sia, al contrario, una corretta applicazione dell'art. 52 della Carta di Nizza e della indicazione circa il contenuto essenziale dei diritti in esame (T. OJANEN, *Rights-based review of electronic surveillance after DRI and Schrems in the European Union*, op. cit., p. 16).

common understanding of the requirements resulting from the CJEU judgement, at an EU level, seems urgently required. It should thereafter be considered whether a common framework for data retention for the purpose of preventing and fighting crime would be beneficial"[152]. La richiesta di ulteriori riflessioni e il dibattito su questa difficile disciplina, anche dopo il forte intervento della CGUE, è dunque destinata a proseguire, come i prossimi Capitoli mostreranno.

[152] EUROJUST, *Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15*, op. cit., p. 13.

CAPITOLO III

L'EFFETTO DOMINO DELLA '*DATA RETENTION SAGA*' NELLA DIMENSIONE ESTERNA ALL'UE. IL PROBLEMA DEL TRASFERIMENTO E CONSERVAZIONE DI DATI OLTRE I CONFINI EUROPEI: DAL CASO *SCHREMS* AL PIÙ RECENTE *PARERE 1/15* IN MATERIA DI PNR

Come già anticipato nei precedenti Capitoli e come meglio si vedrà anche nel successivo, le profonde incertezze e le problematiche emerse nella sentenza *Tele2* sono da considerarsi tutt'altro che definitivamente risolte e superate; lo dimostra il fatto che, a poca distanza di tempo da tale pur rilevante decisione, la Corte di giustizia sia stata chiamata a pronunciarsi nuovamente in materia di *data retention,* sia nel caso *Ministerio Fiscal*, già conclusosi, che nei ben sei rinvii pregiudiziali ad oggi pendenti. Prima di analizzare questi rilevanti sviluppi, che restituiscono un'immagine complessa ed articolata della disciplina della raccolta, conservazione, accesso e trattamento di dati e metadati, non è possibile in questa sede ignorare un ulteriore ma imprescindibile aspetto legato alla tutela della riservatezza e alla protezione dei dati, che ha tenuto (e tiene tutt'ora) impegnati i giudici di Lussemburgo: il trasferimento di dati e metadati al di fuori dei confini dell'Unione europea.

In un mondo sempre più globalizzato e, al contempo, digitalizzato, il valore economico dei dati in formato elettronico – di cui si è già ampiamente parlato nel Capitolo I, Parte I – risiede proprio nella loro "volatilità" e "aterritorialità"[1], cioè nella loro intrinseca propensione e facilità ad essere trasferiti in qualsiasi parte del mondo, in qualsiasi momento; la ricchezza che deriva dai dati e, in particolare, dai Big Data, proviene proprio dal loro scambio tra diversi soggetti, tra chi li raccoglie e conserva e chi invece li elabora ed analizza per gli scopi più disparati[2].

Ecco allora che l'enorme rilevanza economica nonché la quotidianità ed automaticità di queste operazioni di 'movimentazione' di dati e metadati, non potevano che far sorgere questioni e problematiche giuridiche, affrontate da legislatori e giudici, nazionali ed europei; questi sono stati posti dinnanzi alla moderna esigenza di una tutela dei dati di tipo transfrontaliero, che sappia cioè travalicare i confini territoriali – nazionali o sovranazionali – mediante la predisposizione di specifiche regole volte a disciplinare il trasferimento di dati verso uno o più Stati terzi (nell'ottica della presente disamina, 'terzo' rispetto all'UE). In questo complesso contesto, il legislatore dell'Unione prima e i giudici poi, si sono dunque dovuti interrogare sul se e quali condizioni stabilire al fine di bilanciare l'interesse allo scambio di dati anche al di fuori dei confini europei da un lato e la tutela dei diritti alla riservatezza e alla protezione dei dati dall'altro, nonché, più genericamente, sul se e come garantire uno standard di tutela dei diritti degli utenti europei anche quando i dati non si trovino più ad essere sottoposti alla normativa europea o dei suoi Stati membri.

Tali questioni e decisioni, lungi dall'essere meramente teoriche, presentano evidenti e forti ripercussioni sul piano pratico ed operativo, considerando soprattutto che molte aziende operanti in diversi ambiti del settore digitale (Facebook, Apple, Google etc. ma anche aziende di più modeste dimensioni) hanno sede negli USA: sede alla quale le varie ramificazioni dislocate nel continente

[1] Sul punto si legga ampiamente: J. DASKAL, *The un-territoriality of data*, in *Yale Law Journal*, 125, 2015.

[2] Per alcune interessanti riflessioni sull'importanza dello scambio di dati sotto il profilo economico ma anche geopolitico, si rimanda a: M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, in *Rivista di Diritti Comparati*, 2, 2017.

europeo fanno capo ed alla quale trasferiscono i dati relativi agli utenti e clienti europei. Se il flusso di dati, come si è detto, è ormai parte integrante ed ineliminabile del funzionamento e del successo economico delle imprese nei più svariati settori, le operazioni di trasferimento dati non devono per questo rappresentare una rinuncia alla garanzia di un certo livello di riservatezza e sicurezza dei dati: per usare le parole della Commissione, "nell'era digitale, la promozione di standard elevati di protezione dei dati e la facilitazione del commercio internazionale devono necessariamente andare di pari passo"[3], a sottolineare sia la consapevolezza della inevitabilità e necessità di consentire il flusso di dati, che l'irrinunciabile esigenza – e dovere – di tutelare diritti fondamentali che non sono considerati dall'Unione 'merce di scambio'[4]. Nello stabilire quindi i criteri volti a consentire il trasferimento di dati personali verso Stati terzi, l'Unione ha inserito nel proprio apparato normativo – integrato e arricchito dalla giurisprudenza della Corte di Giustizia – disposizioni volte sì ad autorizzare il passaggio di dati oltre i confini europei, ma solo nel caso in cui ad essi venga garantito un livello elevato di protezione, come emerge con chiarezza dallo strumentario – composto da un'ampia gamma di meccanismi, dalle decisioni di adeguatezza ai codici di condotta – predisposto dalla Dir. 95/46/CE e ampliato ed implementato dal vigente GDPR[5].

Ben si può comprendere tuttavia quanto tale approccio, che stabilisce – o, forse meglio, impone normativamente – il rispetto di standard di tutela della privacy e di protezione dei dati al fine di consentire il flusso di dati verso Stati terzi, comporti delicatissime problematiche non solo di carattere giuridico – attinenti da un lato a possibili 'scontri' regolatori tra diversi modelli di garanzia del diritto alla riservatezza e dall'altro al punto di equilibrio, identificato in maniera diversa in differenti ordinamenti, tra garanzie costituzionali dei diritti fondamentali ed esigenze commerciali o securitarie del flusso di dati – ma anche di natura politica, di relazioni internazionali nonché economica[6].

Le possibili criticità sopra tratteggiate sono amplificate dal fatto che il trasferimento di dati non coinvolge solo soggetti privati (ad esempio un'azienda con sede in UE e la sua azienda-madre situata in USA) bensì anche autorità pubbliche di Stati terzi che possono divenire destinatarie o alle quali può essere comunque data la possibilità di trattare i dati provenienti dall'UE; ebbene, in questo panorama un ruolo fondamentale è stato assunto dalla Corte di giustizia dell'UE, che si è già pronunciata in casi attinenti ad entrambe le casistiche indicate: nella sentenza sul caso *Schrems*, i giudici di Lussemburgo hanno analizzato la conformità al diritto dell'UE – ed in particolare alla Carta di Nizza – della decisione di adeguatezza adottata dalla Commissione sulla base dei criteri del c.d. *Safe Harbour* e avente ad oggetto il trasferimento di dati, operato da soggetti privati, dall'UE agli USA; nel *Parere 1/15* in materia di PNR, invece, i giudici di Lussemburgo si sono interrogati sulla legittimità della bozza di accordo UE-Canada sul trasferimento dei dati di prenotazione aerea di cittadini europei raccolti dalle compagnie di volo ed inviati alle autorità pubbliche di *law enforcement* canadesi per scopi securitari.

Queste pronunce, accanto ad alcuni rilevanti rinvii pregiudiziali al momento pendenti, risultano particolarmente interessanti per una completa analisi della disciplina in materia di *data retention*:

---

[3] COMMISSIONE EUROPEA, *Comunicazione della Commissione al PE e al Consiglio: Scambio e protezione dei dati personali in un mondo globalizzato*, COM (2017) 7 final, 10 gennaio 2017.

[4] COMMISSIONE EUROPEA, *Comunicazione della Commissione al PE e al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni: Commercio per tutti. Verso una politica commerciale e di investimento più responsabile*, COM (2015) 497 final, 14 ottobre 2015.

[5] Come si avrà modo di sottolineare anche in seguito, "ponendo la regola secondo cui i dati personali non possono essere inviati al di fuori dell'EEA verso Paesi che non offrano adeguati livelli di tutela, si è in concreto fatto leva sulla dipendenza reciproca esistente fra imprese commerciali europee ed imprese dei Paesi terzi, in un contesto di economia dell'informazione", A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016, p. 241.

[6] Imporre determinate tutele e garanzie al fine di concedere il trasferimento di dati verso Stati terzi comporta infatti quale risultato l'adozione, da parte di soggetti privati quanto pubblici, di specifiche e spesso onerose *privacy policies*.

sebbene abbiano ad oggetto operazioni di trasferimento, conservazione e accesso ad una ampia categoria di dati – non solo quelli derivanti da telecomunicazioni elettroniche come nei casi esaminati nei precedenti Capitoli e in quelli che seguiranno –, in questi casi giurisprudenziali la Corte di Giustizia ha risposto comunque a questioni attinenti alla raccolta generalizzata di una mole ingente di dati, facendo, non a caso, ampio richiamo alle previe sentenze *DRI* o *Tele2*[7].

Lo studio della normativa e della giurisprudenza sul trasferimento di dati a Stati terzi nonché degli sviluppi in atto, permetterà, in ultima analisi, di svolgere due tipi di osservazioni: la prima orientata a riflettere sulle ripercussioni e sulle conseguenze delle pronunce in materia di trasferimento di dati rispetto alle problematiche ancora aperte in materia di *data retention*, con lo scopo di delineare quali sono i punti di contatto o di differenziazione presenti nelle decisioni analizzate in questo Capitolo rispetto alle precedenti sentenze *DRI* o *Tele2*; la seconda è volta a valutare la portata e l'impatto della normativa e della giurisprudenza dell'UE in materia di trasferimento dei dati – e dunque, per connessione, anche dell'intero filone giurisprudenziale relativo al versante interno della *data retention* – nella 'dimensione esterna' ovvero nel rapporto tra UE e Stati terzi, conseguentemente ragionando sul potenziale espansivo dei principi delineati dalla CGUE e sulla loro capacità di propagarsi in diverse direzioni[8]: la 'propagazione' del diritto dell'UE in materia di riservatezza e protezione dei dati anche al di fuori dei propri confini risulta particolarmente evidente, del resto, in un ambito, come quello digitale, che per sua natura presenta sfumati se non inesistenti confini territoriali; ambito nel quale proprio l'UE vuole promuovere i propri valori, spingendo verso un allineamento a livello internazionale agli standard dettati dalle proprie normative 'interne' a tutela della riservatezza e della protezione dei dati. Pur non essendo certamente questa la sede per avanzare sviluppate ed approfondite considerazioni in merito al complesso concetto di 'sovranità digitale', risulta chiaro come la normativa europea e la sua interpretazione giurisprudenziale vadano nella direzione di promuovere una convergenza delle normative dei Paesi terzi verso il livello di tutela dei dati delineato all'interno dell'Unione, la cui utilità ed efficacia meritano una specifica attenzione.

[7] Questa connessione tra le tematiche – e problematiche – affrontate dai giudici di Lussemburgo, permette di considerare i casi *Schrems* e il *Parere 1/15* come complementari rispetto alle previe decisioni *DRI* e *Tele2*: sul punto si veda S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, 3, 2016, p. 689.

[8] Come si è già anticipato nel Capitolo II, alcuni autori, tra cui E. CELESTE (in *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019) parlano di 'effetto domino' della giurisprudenza della CGUE in materia di *data retention*, ponendo attenzione alle conseguenze dell'applicazione dei principi identificati nel lungo filone giurisprudenziale inaugurato con la sentenza *DRI*, rispetto ad altre e differenti normative che pure disciplinano operazioni di conservazione, accesso e utilizzo di dati, pur di natura diversa da quelli derivanti dalle telecomunicazioni: si pensi ai già citati accordi internazionali esistenti tra UE e USA, aventi ad oggetto lo scambio di dati finanziari utilizzati per effettuare controlli sulle transazioni finanziarie dei terroristi (Terrorist Finance Tracking Program, tra cui l'*AGREEMENT between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program*, *GUUE* L 195 del 27 luglio 2010), o ancora alla Direttiva UE 2016/681 sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi. Si è avuto modo di vedere infatti come già all'indomani della sentenza *DRI* fossero emerse riflessioni lungimiranti sugli effetti di tale decisione rispetto al quadro normativo europeo esistente e agli accordi internazionali in materia di trasferimento dati vigenti tra UE e Stati terzi (si legga S. CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di diritto pubblico comunitario*, 3-4, 2015, p. 838), riflessioni che sono poi risultate ancor più attuali e ormai inevitabili a seguito delle decisioni *Schrems* e del *Parere 1/15*.

1. – La normativa europea in materia di trasferimento di dati verso Stati terzi

Il primo fondamentale passaggio per meglio comprendere il significato e la portata della sentenza *Schrems* e del *Parere 1/15* nonché dei rinvii pregiudiziali pendenti è inquadrare la disciplina normativa dell'UE in materia di trasferimento di dati diretti verso Stati terzi.

Per quanto attiene a questa specifica regolamentazione, merita sottolineare sin da ora come entrambi i casi giurisprudenziali decisi dalla Corte di Giustizia e ad oggi conclusi facciano riferimento alle previsioni contenute nella Dir. 95/46/CE. Questa, come si è già visto nella Parte I di questo elaborato, è stata sostituita dal GDPR: nel ricostruire la normativa europea rilevante si partirà quindi dalla Direttiva previgente, cui si farà riferimento nell'analisi giurisprudenziale, pur senza trascurare l'esame di alcuni importanti mutamenti introdotti dall'attuale Regolamento, che, oltre a dimostrarsi in linea con le considerazioni e i principi espressi dalla giurisprudenza CGUE in materia, non manca di rafforzare e migliorare anche alcuni punti deboli emersi dalle previe disposizioni normative.

La Direttiva 95/46/CE dedicava al trasferimento di dati personali verso Paesi terzi il Capo IV, che conteneva tuttavia una disciplina piuttosto scarna – solo due disposizioni e pochi Considerando – a differenza del Capo V del GDPR che invece riserva a questa materia ben 8 articoli e 19 Considerando, aggiungendo nuove modalità di trasferimento e meglio specificando, in alcuni casi, quanto già precedentemente contenuto nella Direttiva. Come pare evidente, la diversa e più ampia attenzione dedicata dal Regolamento è chiaro segnale della enorme rilevanza che nell'ultimo decennio lo scambio di dati ha assunto, grazie anche all'espansione dell'utilizzo di Internet e di nuove e sempre più avanzate tecnologie.

Analizzando il contenuto della normativa, ciò che emerge con forza sia dalla Direttiva che dal più recente Regolamento è il divieto generale di trasferimento dati verso un Paese terzo salvo alcune deroghe, espressamente previste: tra queste ultime, quella sicuramente più rilevante è la possibilità di "fuoriuscita" dei dati personali dal territorio UE nel caso in cui il Paese di destinazione garantisca un "livello di protezione adeguato" (art. 25 Dir. 95/46/CE ma anche art. 45 GDPR). Una tale scelta normativa, questa, dalla grande portata e impatto, che può essere compresa appieno solo se si considera il ragionamento svolto dal legislatore europeo: in una società "dell'informazione" in cui i dati e i flussi di dati diventano fonti dal valore economico inestimabile, la cui circolazione quindi non può essere del tutto bloccata, devono essere tenute in considerazione anche le conseguenze sul piano dei diritti fondamentali che da tali trasferimenti derivano; questo perché l''esportazione' di dati fuori dal territorio europeo ha prodotto, "nella maggior parte delle occasioni, la transizione delle informazioni da un'area giuridica ad elevato grado di protezione per il diritto alla riservatezza verso ordinamenti ove il *right of privacy* non è circondato dalle medesime garanzie"[9]. Per questo l'Unione ha imposto, quale condizione per il trasferimento di dati, che i Paesi destinatari garantiscano standard di tutela adeguati rispetto al modello europeo, diventando quest'ultimo pertanto l'unico punto di riferimento e di raffronto: è evidente la volontà dell'UE di garantire una certa continuità nel livello di tutela del diritto alla riservatezza e alla *data protection* anche quando i dati lasciano il territorio europeo[10], evitando così anche il verificarsi di pericolosi fenomeni di cd. *shopping regolatorio*[11].

[9] S. SICA, V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, op. cit., p. 138.

[10] Si legga al proposito il Considerando 101, GDPR: "L'aumento di flussi (di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali) ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. È opportuno però che, quando i dati personali sono trasferiti (..) il livello di tutela delle persone fisiche assicurato dall'Unione dal presente regolamento non sia compromesso".

[11] M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, op. cit., p. 2.

Non può negarsi tuttavia che il concetto di "adeguatezza" sia piuttosto vago e si presti a diverse interpretazioni[12]: sotto questo profilo la giurisprudenza della CGUE è venuta in soccorso, specificando e chiarendo il significato delle parole scelte dal legislatore. Nella sentenza *Schrems*, infatti, i giudici di Lussemburgo hanno affermato che il termine "adeguato" implica che "non possa esigersi che un Paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, come rilevato dall'Avvocato generale al paragrafo 141 delle sue conclusioni, l'espressione 'livello di protezione adeguato' deve essere intesa nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali *sostanzialmente equivalente* a quello garantito all'interno dell'Unione in forza della Direttiva 95/46, letta alla luce della Carta"[13]. In altre parole, il livello di tutela deve essere comparabile ma non identico a quello garantito in UE, mediante una "valutazione globale dei sistemi del Paese terzo, compresa la normativa sull'accesso ai dati personali da parte di pubbliche autorità preposte alle attività di contrasto, alla sicurezza personale o ad altro scopo d'interesse pubblico"[14]. Questa definizione ed interpretazione del concetto di adeguatezza – inserito, senza specifiche spiegazioni, nella Direttiva 95/46/CE – è stata chiaramente e pedissequamente recepita anche dal legislatore dell'UE all'interno del GDPR, nel Considerando 104[15].

Muovendo oltre la definizione, per analizzare l'aspetto più prettamente procedurale, il compito di valutare tale livello di adeguatezza era attribuito nella Dir. 95/46/CE sia alla Commissione che agli Stati membri, con l'unica differenza, in termini di efficacia, che la decisione della Commissione diveniva vincolante per tutti gli Stati membri (art. 25, Dir. 95/46/CE, co. 6). Nel caso in cui venisse rilevata la mancata adeguatezza del sistema di protezione dello Stato terzo, era conseguentemente impedito ogni trasferimento dati, insieme però all'obbligo della Commissione di avviare negoziati per superare la situazione di "inadeguatezza" (art. 25, co. 5)[16]. Le decisioni di adeguatezza, inoltre, potevano assumere carattere parziale cioè vertere su di uno specifico settore, su determinate categorie di dati (come nel caso

[12] L'art. 25, co. 2, Dir. 95/46/CE indica gli elementi e le disposizioni che devono essere considerati per valutare l'adeguatezza delle misure e delle tutele predisposte dallo Stato terzo: "L'adeguatezza del livello di protezione garantito da un Paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate".

[13] Par. 73, *Schrems*, enfasi aggiunta. La Commissione sul punto ha affermato che "il livello di adeguatezza non comporta necessariamente una duplicazione pedissequa delle norme dell'UE. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla riservatezza e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema estero in questione, nel suo insieme, offre il necessario livello elevato di protezione", COMMISSIONE EUROPEA, *Comunicazione della Commissione al Parlamento Europeo e al Consiglio. Scambio e protezione dei dati personali in mondo globalizzato*, COM (2017) 7 final, p. 7.

[14] COMMISSIONE EUROPEA, *Comunicazione della Commissione al PE e al Consiglio. Scambio e protezione dei dati personali in un mondo globalizzato*, op. cit, p. 7.

[15] Nel Regolamento attualmente vigente sono inoltre specificati con maggiore precisione i criteri determinanti l'adeguatezza; si fa riferimento in particolare all'art. 45, co. 2, che richiama quali elementi da valutare al fine di determinare la sostanziale equivalenza: lo stato di diritto; il rispetto dei diritti umani e libertà fondamentali, delle normative generali e settoriali, della giurisprudenza e dei diritti effettivi e azionabili; l'esistenza e l'effettività di una o più autorità di controllo indipendenti nel paese terzo; gli impegni internazionali assunti.

[16] Il successivo co. 6 esplicita proprio che la decisione di adeguatezza della Commissione può avvenire anche sulla base degli impegni internazionali assunti a seguito della negoziazione avviata con lo Stato terzo. La Commissione infatti spesso fonda la propria decisione sulla valutazione dell'adeguatezza dei principi e delle tutele contenute in specifici accordi, frutto molto spesso di lunghe trattative. Come si può ben immaginare e come non si mancherà di sottolineare anche in seguito, gli Stati extra-UE sono sovente restii a vedersi imporre o ad accettare, nella determinazione delle condizioni di accordo, livelli di tutela fortemente differenti da quelli previsti dal proprio ordinamento. La valutazione di adeguatezza inoltre non è stabilita una volta per tutte bensì, come indicato nel GDPR e suggerito nella sentenza *Schrems*, viene previsto un riesame periodico delle decisioni – almeno ogni quattro anni –, in modo da tenere adeguatamente in conto gli sviluppi nel frattempo intercorsi nel Paese terzo (art. 45, co. 3, GDPR).

dei PNR) oppure valere per una categoria particolare di soggetti (imprese, ad esempio): in questo caso la valutazione circa l'adeguatezza o meno delle tutele garantite dallo Stato terzo poteva essere fondata sulle condizioni ed i requisiti fissati da specifici accordi internazionali bilaterali, riguardanti appunto la precisa tipologia di dati da trasmettere o i soggetti coinvolti[17].

Questa breve analisi permette di cogliere una delle maggiori discontinuità della normativa vigente rispetto alla disciplina della Dir. 95/46/CE, da ravvisarsi nell'attribuzione esclusiva alla Commissione – e non più anche agli Stati membri – della facoltà di rilevare l'adeguatezza o meno della protezione garantita dallo Stato terzo[18]. Ma non solo: tale capacità valutativa, ora centralizzata, si estende non più unicamente all'adeguatezza garantita dagli Stati al di fuori dell'UE bensì anche dalle organizzazioni internazionali, oltre che riferirsi espressamente anche ai trasferimenti successivi di dati personali verso ulteriori organizzazioni o Stati terzi[19].

---

[17] Merita ricordare come, diversamente dalla decisione di adeguatezza, la conclusione da parte dell'UE di un accordo internazionale (che può costituire la base e dunque fissare le condizioni che permetteranno di considerare adeguate le tutele garantite dallo Stato terzo nell'ambito del trasferimento di dati extra-UE) implichi una procedura senz'altro complessa e articolata. Con l'entrata in vigore del Trattato di Lisbona, infatti, ai sensi degli artt. 218, 219 e 207 TFUE, vengono coinvolte nel procedimento tutte le Istituzioni europee, compreso il Parlamento, cui è attribuito un potere di veto nel caso di accordi vertenti su materie per le quali è prevista la procedura legislativa ordinaria. Prima del Trattato di Lisbona, invece, gli accordi internazionali vertenti su materie per le quali era prevista la procedura di co-decisione non richiedevano l'intervento del Parlamento (che aveva funzione meramente consultiva) bensì la sola ratifica del Consiglio, su proposta della Commissione. Per ulteriori approfondimenti su questo aspetto, che rappresenta un elemento necessario per comprendere le vicende giudiziarie legate agli accordi in materia di trasferimento di dati, si richiama, tra i tanti, P. EECKHOUT, *EU external relations law*, Oxford University Press, 2011; E. BARONCINI, *L'Unione europea e la procedura di conclusione degli accordi internazionali dopo il Trattato di Lisbona*, in *Cuadernos de Derecho Transnacional*, 1, 2013. Per approfondimenti invece sull'utilizzo di accordi internazionali nello specifico ambito del trasferimento di PNR, si rimanda a F. ROSSI DAL POZZO, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui "codici di prenotazione" (PNR)*, in *Rivista di diritto internazionale privato e processuale*, 4, 2016.

[18] "A differenza del vecchio art. 26 che disegna una sorta di 'parallelismo provvisorio di competenze' tra Commissione e Stati membri (..), nel nuovo articolo 45 scompare ogni riferimento agli Stati membri. La Commissione è dunque l'organo dell'Unione che emerge quale *dominus* incontrastato in materia di trasferimenti basati su una decisione di adeguatezza", M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, op. cit., p. 6.

[19] Si vuole sottolineare, per completezza, come sia la Dir. 95/46/CE che, in misura ancora maggiore e più puntuale, il GDPR, prevedono ulteriori deroghe al generale divieto di trasferimento di dati, anche in mancanza di una decisione di adeguatezza: l'art. 26 della Direttiva infatti elencava una serie di condizioni (consenso della persona interessata, trasferimento dati per esecuzione di un contratto, per salvaguardia di un interesse pubblico rilevante o necessario per constatare, esercitare o difendere un diritto per via giudiziaria o per salvaguardare l'interesse vitale della persona interessata) che consentivano agli Stati membri di disporre comunque il trasferimento di dati personali; l'autorizzazione della Commissione o dello Stato membro al trasferimento poteva anche giungere qualora il responsabile del trattamento presentasse "garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone", anche risultanti da clausole contrattuali appropriate (art. 26, co. 2). Questa disciplina è stata totalmente recepita nel GDPR (art. 49), che però aggiunge anche una ulteriore eccezione ovvero il caso di trasferimento dati non ripetitivo riguardante un numero limitato di interessati e necessario per il perseguimento di interessi legittimi del titolare del trattamento. Oltre a queste opzioni, il GDPR istituzionalizza anche altre modalità alternative di trasferimento dei dati, in assenza di decisioni di adeguatezza. L'art. 46 infatti stabilisce la possibilità di trasferimento nel caso in cui il titolare o il responsabile del trattamento forniscano "garanzie adeguate e gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi", che si sostanziano nella presenza di strumenti giuridicamente vincolanti, norme vincolanti d'impresa (art. 47), clausole tipo di protezione dei dati adottate da Commissione o autorità di controllo, codici di condotta e ancora clausole contrattuali (art. 46, co. 2, cd. *Standard Contractual Clauses*, che saranno oggetto poi di approfondimento e che sono al centro dell'attenzione della CGUE in un caso attualmente pendente) o, ancora, disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici. Per approfondimenti su tutti questi interessanti strumenti alternativi di trasferimento dei dati, si rimanda a M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, op. cit., ma anche P. PIRODDI, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo Regolamento generale sulla protezione dei dati*, in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015; più ampiamente: C. KUNER, *Transborder data flows and data privacy law*, Oxford University Press, 2013.

Al di là di queste importanti originalità e difformità rispetto alla disciplina precedente, anche nel GDPR viene comunque confermata la natura di atto di esecuzione della decisione di adeguatezza della Commissione[20]. Ed è proprio con riferimento a questa tipologia di decisione che la CGUE è stata chiamata più volte a pronunciarsi.

2. – La decisione di adeguatezza circa il trasferimento di dati dall'UE agli USA al vaglio della CGUE: il caso **Schrems** *e la mancanza di un 'approdo sicuro' oltreoceano*

2.1. – I principi sanciti nel c.d. **Safe Harbour** *e le rivelazioni di Snowden: la posizione espressa dalla Commissione*

Il primo intervento della CGUE avente ad oggetto una decisione di adeguatezza ha riguardato la decisione 520/2000 del 26 luglio 2000, con la quale la Commissione aveva ritenuto adeguate le tutele sancite dai requisiti e condizioni previste nell'accordo c.d. Approdo sicuro (o *Safe Harbour*), posto alla base – e quale precondizione – del trasferimento verso gli Stati Uniti di dati raccolti per fini commerciali da società aventi sede nel territorio UE. L'adeguatezza quindi era stata accertata dalla Commissione in maniera parziale: in assenza di una legislazione generale sulla protezione dei dati negli USA che consentisse di considerare tale ordinamento nel suo complesso come 'adeguato'[21], gli standard di protezione dei dati e di salvaguardia della riservatezza contenuti nell'Approdo sicuro erano stati ritenuti sufficienti ai fini di garantire una tutela adeguata rispetto a quella europea. Senza addentrarci in questa sede in una analisi puntuale del contenuto di questo accordo, merita sottolineare come l'Approdo sicuro stabilisse sette principi e 15 FAQ (redatte dalla *Federal Trade Commission*)[22] cui le aziende stabilite in USA erano tenute ad attenersi al fine di poter trasferire e quindi poi conservare, utilizzare, trattare e accedere ai dati provenienti dal continente europeo: l'adesione ed il rispetto dei requisiti individuati dall'Approdo sicuro aveva quindi carattere puramente volontario sebbene indispensabile per poter procedere al trasferimento oltreoceano. Coerentemente con questa impostazione, la conformità ai *Safe Harbour Principles* delle misure adottate dalle aziende non era vagliata in via preventiva da un organo europeo o statunitense bensì si fondava sulla autocertificazione delle aziende stesse, con un controllo

[20] "Si tratta generalmente di una serie di atti unilaterali adottati dalla Commissione e (talvolta) dalla Commissione e dagli Stati terzi, diretti a regolare il traffico transfrontaliero di dati. Con riferimento a quest'ultima ipotesi, tuttavia, è evidente, che tali atti, anche quando sottintendono obbligazioni sinallagmatiche tra Unione e Stati terzi, non possano in ogni caso essere considerati alla stregua di accordi in forma semplificata. Infatti, né l'Unione né gli Stati terzi, in alcuno degli atti menzionati [si fa riferimento alle decisioni di adeguatezza riguardanti Andorra, Argentina, Canada, Svizzera, Isole Faroe, Guernsey, Israele, Isola di Man, Isola di Jersey, Nuova Zelanda, Uruguay, USA (2000/520/EC e 2016/1250/EU), di cui si parlerà più avanti] hanno mai espresso la volontà di concludere un accordo internazionale", F. BORGIA, *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in *Il mercato unico digitale*, Numero Speciale 2017 della rivista *Diritto Mercato e Tecnologia*, 2017, p. 140.

[21] Per alcune riflessioni sul diverso livello di tutela della riservatezza e della protezione dei dati garantito oltreoceano negli USA, si rimanda a: J. WITHMAN, *The two Western culture of privacy: dignity versus liberty*, in *Yale Law Journal*, 113, 2004; P.M. SCHWARTZ, D. SOLOVE, *Reconciling personal information in the United States and European Union*, in *California Law Review*, 102, 2014.

[22] La Decisione n. 2000/520 della Commissione europea si componeva di diversi documenti, oltre ai Principi di Approdo sicuro: sono allegate infatti anche le FAQ, un documento circa "L'applicazione dell'Approdo sicuro", un ulteriore documento titolato "Tutela della riservatezza e risarcimento dei danni, autorizzazioni legali, fusioni, acquisizioni secondo la legge degli Stati Uniti" ed infine un insieme di comunicazioni intercorse tra Commissione europea e Autorità pubbliche statunitensi contenenti alcuni chiarimenti circa l'accordo e le sue condizioni. Per una approfondita analisi sul contenuto dell'accordo, si legga, tra gli altri: M. P. QUEK, *Personal data privacy protection in an age of globalization: the UE-USA Safe Harbour compromise*, in *Journal of European Public Policy*, 3, 2002; S. SICA, V. D'ANTONIO, *I Safe Harbour privacy principles: genesi, contenuti, criticità*, in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015.

meramente successivo da parte della *Federal Trade Commission*. Venivano però anche previste all'interno dell'accordo talune disposizioni di natura eccezionale in grado di consentire una deroga al rispetto di tali principi al fine di "soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti": in sostanza, per questi scopi, determinati in maniera estremamente ampia, le autorità pubbliche statunitensi avevano la possibilità di accedere ai dati provenienti dall'UE e conservati dalle aziende, senza essere vincolate al rispetto delle condizioni e delle garanzie indicate dall'accordo, che si applicavano dunque solo con riferimento ai soggetti privati. Nonostante queste deroghe rilevanti, che aprivano le porte ad ingerenze potenzialmente illimitate sui dati personali da parte delle autorità di intelligence o di *law enforcement* americane e nonostante l'assenza di una normativa statunitense specifica in materia di protezione dei dati e della vita privata che potesse fornire in tal caso una minima tutela, la Commissione aveva rinvenuto nelle garanzie previste nell'Approdo sicuro e nelle FAQ ad esso allegate un livello di tutela "adeguato".

Dopo le rivelazioni di Snowden, più volte ormai richiamate, che hanno messo in luce l'invasività e l'assenza di controlli e limitazioni ai meccanismi di sorveglianza massiva esercitata negli USA dalla NSA e dai servizi di intelligence nazionali, molti timori sono emersi nella società civile e nelle Istituzioni europee, preoccupate sempre di più per le sorti dei dati provenienti dall'Unione una volta attraversato l'Atlantico[23]: iniziavano infatti a sorgere dubbi sul fatto che le salvaguardie predisposte dall'Approdo

[23] In estrema sintesi e richiamando quanto già in parte analizzato nella Parte I, le rivelazioni di Snowden che hanno assunto maggiore impatto e che risulteranno centrali nel dibattito politico ma anche nelle scelte e valutazioni di legislatori e giudici dell'UE sono quelle attinenti ai programmi PRISM e Upstream ovvero *tools* di sorveglianza elettronica di massa che non riguardavano però comunicazioni 'wholly domestic' o tra cittadini statunitensi entrambi presenti sul territorio degli USA al momento della raccolta dei dati. Ne consegue che non sono escluse da controllo le comunicazioni tra un cittadino americano e un soggetto situato all'estero (riguardanti dunque soggetti americani connessi ad un target 'esterno') o quelle tra soggetti unicamente stranieri (su questo punto si legga l'interessante studio di Lubin sulla percezione di una maggiore accettabilità di sistemi di sorveglianza aventi come 'bersaglio' stranieri, in A. LUBIN, *'We only spy on foreigners': the myth of a universal right to privacy and the practice of foreign mass surveillance*, in *Chicago Journal of International Law*, 2, 2018). Il programma Upstream è certamente quello che ha destato maggiore preoccupazione e sgomento, oltre ad essere stato ritenuto fortemente problematico da un punto di vista giuridico e di rispetto dei diritti fondamentali: mediante tale programma, infatti, la NSA effettuava intercettazioni dirette (riguardanti sia il contenuto che i metadati) delle telecomunicazioni veicolate mediante le reti di telecomunicazione americane (la c.d. 'dorsale', ossia la rete di commutatori e cavi su cui 'viaggiano' le comunicazioni sia telefoniche che telematiche). La NSA dunque accedeva a determinate fasce di traffico dati ritenute di interesse per le operazioni di *Foreign Intelligence*; successivamente, attraverso l'uso di marcatori (cd. *selectors*), venivano 'scremate' ed individuate le comunicazioni da vagliare; "this system is designated to look for communications that either originate or end abroad but also sweeps in purely domestic communications because of its broad scope" (A. BUTLER, F. HIDVEGI, *From Snowden to Schrems: how the surveillance debate has impacted US-EU relations and the future of international data protection*, in *Seton Hall Journal of Diplomacy and International Relations*, Special Issue 2015/2016). Il programma PRISM invece era caratterizzato dall'accesso da parte dell'NSA ai dati conservati nelle banche dati dei fornitori di servizi telecomunicazioni (Google, Youtube, Facebook, Microsoft, Skype, Apple, Yahoo, etc.). Tali informazioni venivano poi trattenute per 5 anni in un database dell'NSA stessa e utilizzate mediante ricerche 'targetizzate' cioè svolte attraverso l'introduzione di target e obiettivi specifici: ciò, tuttavia, si traduceva nell'analisi di un numero estremamente ampio di dati correlati, considerando il fatto che le ricerche svolte includevano anche l'esame di comunicazioni di/con soggetti correlati ai target c.d. *contact chaining method*, identificativi di connessioni tra utenti. Questi programmi si fondavano sulla normativa *Patriot Act* del 2001, sul FISA (*Foreign Intelligence Surveillance Act*) *Amendments Act* del 2008 e sul controllo di un tribunale segreto ad hoc, il Tribunale FISA, istituito nel 2006. In particolare, grande rilievo, come si vedrà più avanti, assumeva la sezione 702 del FISA, in cui viene stabilito il potere del *Attorney General* e del Direttore della *National Intelligence* di autorizzare la sorveglianza di soggetti targetizzati, ritenuti presumibilmente al di fuori dagli USA, per acquisire informazioni utili per scopi di *foreign intelligence*. Una volta avviate tali procedure, non era necessario nessun ulteriore controllo da parte dei giudici, neppure per giustificare l'eventuale successivo ampliamento dei target stessi. La sezione 702 quindi è stata la base giuridica che ha consentito lo sviluppo dei programmi Upstream e PRISM e per tale ragione è stata indicata come una delle disposizioni più controverse del FISA. Merita preliminarmente sottolineare come la chiara invasività di questi strumenti di sorveglianza massiva e generalizzata, capaci di incidere profondamente sulla sfera privata di un numero elevatissimo di soggetti, sia stata accompagnata anche da critiche circa l'efficacia

sicuro fossero realmente sufficienti ed adeguate a garantire una effettiva protezione dei dati nel momento in cui essi venissero utilizzati (richiesti, conservati, trattati) da autorità pubbliche per finalità di sicurezza nazionale o interesse pubblico.

È proprio in questa situazione di tensione che è intervenuta inizialmente la Commissione, con una Comunicazione al Parlamento e al Consiglio (COM (2013) 846 final del 27 novembre 2013), emblematicamente intitolata "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA". Se inizialmente i *Safe Harbour Principles* erano stati accolti con entusiastica fiducia, tanto da spingere alcuni autori a ritenere l'innalzamento del livello di protezione dei dati trasferiti dall'UE agli USA come una conquista tutta europea, a testimonianza di un positivo *Brussels effect*[24], le dichiarazioni di Snowden svelavano le debolezze ed incertezze – se non addirittura le falle – di quello che non appariva più come un approdo realmente sicuro. La raccolta massiva e la conservazione sistematica ed indiscriminata di dati personali di diversa natura operati dai servizi di intelligence si estendevano infatti anche ai dati legittimamente trasferiti dall'UE agli Stati Uniti da imprese che correttamente rispettavano i principi dell'accordo *Safe Harbour* ma che venivano poi obbligate a cedere quegli stessi dati ad autorità pubbliche che, merita ricordarlo, non erano vincolate al rispetto delle medesime tutele e garanzie imposte ai soggetti privati dai principi dell'Approdo sicuro.

Con una interessante ricostruzione del sistema giuridico americano e ponendo particolare attenzione alle disposizioni che legittimano la presenza di sistemi di sorveglianza volti al controllo su larga scala di dati personali da parte di autorità pubbliche statunitensi, la Commissione rilevava la presenza di alcune carenze nelle tutele e garanzie apprestate da tale sistema, derivanti sia dalla ingerenza e dal possibile accesso ai dati da parte dei pubblici poteri[25], sia dalla "natura volontaria e dichiarativa del regime" che spesso dimostrava la sua intrinseca fragilità nella fase dei controlli, dai quali risultava il mancato effettivo rispetto delle regole da parte delle imprese partecipanti allo schema dell'Approdo sicuro. Pur arrivando a queste conclusioni, la Commissione reputava eccessivamente nocivo l'impatto che una abrogazione della decisione di adeguatezza avrebbe avuto rispetto all'interesse delle imprese,

---

e l'effettività dei programmi nel contribuire alla prevenzione e contrasto del terrorismo e di crimini gravi (si legga, in tal senso, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *Report on the telephone record program conducted under section 215 of the USA Patriot Act and on the operations of the foreign intelligence surveillance Court*, 23 gennaio 2014). Ampiamente e accuratamente sui programmi di sorveglianza di massa utilizzati dagli Stati Uniti ed emersi in occasione del *datagate*: C. BOWDEN, *The US Surveillance programmes and their impact on EU citizens' fundamental rights. Note to the European Parliament*, 2013; F. BIGNAMI, G. RESTA, *Transatlantic privacy regulation: conflict and cooperation*, in *Law and contemporary problems*, 4, 2015; L. P. VANONI, *Il IV emendamento della Costituzione americana tra terrorismo internazionale e datagate: security v. privacy*, in *Federalismi.it*, 1, 2015; C. COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa. A margine della sentenza "Safe Harbor" della Corte di Giustizia dell'Unione Europea*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016; S. MITSILEGAS, *Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime*, in *Columbia human rights law review*, 3, 2016; per un approfondimento sulle soluzioni e reazioni alle rivelazioni di Snowden negli USA, con particolare riferimento anche alla giurisprudenza in materia, si legga: R. A. MILLER (a cura di), *Privacy and power. A transatlantic dialogue in the shadow of the NSA affair*, Cambridge University Press, 2017; A. DIMITROVA, M. BRKAN, *Balancing national security and data protection: the role of EU and US Policy-Makers and Courts before and after the NSA affair*, in *Journal of Common Market Studies*, 4, 2018.

[24] A. BRADFORD, *The Brussels effect*, in *Northwestern University Law Review*, 1, 2012.

[25] "A causa dell'ampia entità dei programmi [di intelligence fondati sulla raccolta e il trattamento su larga scala di dati personali] può accadere che dati trasferiti nell'ambito di Approdo sicuro siano accessibili alle autorità americane e vengano ulteriormente trattati da queste al di là di quanto necessario e proporzionato alla protezione della sicurezza nazionale, come previsto dall'eccezione di cui alla decisione 2000/520. (..) L'accesso su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli USA da imprese certificate nell'ambito dell'Approdo sicuro solleva altri gravi problemi riguardanti la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati negli Stati Uniti", punti 7 e 8, COM (2013) 846 final, nella quale peraltro veniva sottolineato come questi meccanismi non fossero conosciuti o prevedibili all'epoca dell'adozione del regime di Approdo sicuro.

stanziate sia in UE che in USA, preferendo dunque come miglior soluzione percorribile, quella della apertura di un dialogo e di una discussione con le autorità americane, finalizzata a risolvere le carenze e le problematicità emerse.

Questo giudizio veniva peraltro confermato anche nella successiva Comunicazione della Commissione al PE e al Consiglio "sul funzionamento del regime 'Approdo sicuro' dal punto di vista dei cittadini dell'UE e delle società ivi stabilite"[26], nella quale venivano sottolineate ancora una volta le criticità che le eccezioni e deroghe comportavano rispetto ad un corretto ed efficiente funzionamento del sistema Approdo sicuro; in quel documento inoltre non si mancava di evidenziare come anche che i maggiori colossi dell'economia digitale (Microsoft, Google, Facebook, Apple, Yahoo!, Skype, YouTube, etc.), pur essendosi tutti autocertificati secondo l'accordo *Safe Harbour* e pur rispettandone i criteri, erano stati coinvolti nei programmi di sorveglianza di massa PRISM e Upstream, consentendo l'accesso ai dati provenienti dall'UE alle autorità statunitensi, proprio in virtù di quelle ampie deroghe previste dall'accordo UE-USA stesso[27].

2.2. – L'intervento della CGUE: la dichiarazione di invalidità della decisione di adeguatezza e l'influenza della previa pronuncia DRI

In questo delicato e complesso contesto si inserisce la vicenda *Schrems*, originata proprio dai timori del cittadino austriaco Maximillian Schrems, che si era rivolto, senza successo, all'autorità garante della protezione dei dati irlandese al fine di ottenere una pronuncia di divieto di trasferimento dei propri dati personali da Facebook Ireland a Facebook Inc. con sede negli USA. Tale richiesta era motivata dalla convinzione che, alla luce degli sviluppi e delle rivelazioni circa i meccanismi di *mass surveillance* americani, il livello di protezione dei dati negli USA non potesse essere considerato sufficiente a garantire una effettiva tutela della vita privata e della *data protection* da intromissioni generalizzate e indiscriminate. Il caso, giunto di fronte alla High Court irlandese, veniva inviato alla CGUE, tramite rinvio pregiudiziale: i giudici irlandesi, infatti, ritenendo che la decisione 520/2000 non rispettasse i diritti di cui agli artt. 7 e 8 della Carta di Nizza e neppure i principi derivanti dalla giurisprudenza della CGUE (richiamando la nota sentenza *DRI*), avanzavano dubbi circa l'interpretazione degli art. 25 e 28 della Dir. 95/46/CE che regolavano, come si è visto, il trasferimento di dati verso Paesi terzi.

I giudici di Lussemburgo dunque hanno emesso la sentenza di questo complesso e articolato caso il 6 ottobre 2015[28]. Quanto in questa sede interessa preliminarmente sottolineare è come la Corte, utilizzando il proprio potere di riformulare i quesiti, si sia occupata in questo rinvio anche della validità

[26] COMMISSIONE EUROPEA, *Comunicazione sul funzionamento del regime 'Approdo sicuro' dal punto di vista dei cittadini dell'UE e delle società ivi stabilite*, COM(2013) 847 final, 27 novembre 2013.

[27] Le raccomandazioni finali dunque stabilivano l'importanza del fatto che "l'eccezione per motivi di sicurezza nazionale prevista dalla decisione Approdo sicuro sia applicata solo in misura strettamente necessaria e proporzionata", COM (2013) 847 final.

[28] Si vuole preliminarmente sottolineare come né l'Avvocato generale Bot nelle sue Conclusioni, né la CGUE abbiano ritenuto di dover discutere o attestare l'esistenza di un reale danno o pregiudizio come elemento determinante per l'ammissibilità del ricorso. Come già stabilito nella sentenza *DRI* infatti, "per accertare l'esistenza di un'ingerenza nel diritto fondamentale al rispetto della vita privata, poco importa che le informazioni relative alla vita privata di cui trattasi abbiano o meno un carattere sensibile o che gli interessati abbiano o meno subito eventuali inconvenienti in seguito a tale ingerenza", par. 33. Di diverso avviso è stato invece il *Data Protection Commisioner* irlandese che ha per primo vagliato il ricorso di Schrems, ritenendolo inammissibile ("as frivolous or vexatious") per mancanza di prove circa un effettivo accesso da parte della NSA ai dati relativi al ricorrente, raccolti e trasferiti negli USA da Facebook Ireland. Su questo punto, che sarà oggetto, come si vedrà, di un diverso approccio della giurisprudenza della Corte EDU in materia, si legga ampiamente: M. TZANOU, *European Union regulation of transatlantic data transfers and online surveillance*, in *Human Rights Law Review*, 17, 2015.

della decisione 520/2000 della Commissione[29] e non solo dunque del quesito avanzato dai giudici irlandesi circa l'interpretazione degli artt. 25 e 28 della Dir. 95/46/CE aventi ad oggetto il ruolo delle autorità nazionali garanti della protezione dei dati nel campo del trasferimento dei dati al di fuori dell'UE[30].

Per quanto quest'ultimo aspetto, che pure è trattato per primo e che si rivela di estrema importanza per la efficiente e concreta futura tutela dei diritti dei cittadini europei[31], sia di estremo interesse, ciò che assume rilievo ai fini di questa trattazione è il ragionamento espresso dalla Corte rispetto alla validità della decisione di adeguatezza della Commissione: tale parte della pronuncia, infatti, presenta considerazioni specifiche in materia di *data retention* e di accesso indiscriminato e generalizzato ai dati personali. I giudici si sono concentrati pertanto sul contenuto dell'Approdo sicuro e delle sue disposizioni, in particolare su quelle di carattere eccezionale, già sopra richiamate, che consentivano alle autorità pubbliche di accedere ai dati trasferiti, senza sottostare alle regole e tutele previste dal *Safe Harbour*, per motivi principalmente riconducibili alla sicurezza nazionale (par. 82, *Schrems*). Riducendo dunque l'ambito di applicazione dei principi dell'accordo alle sole imprese americane autocertificate e non anche alle autorità pubbliche, ciò che ne derivava, secondo la CGUE, era l'affermazione della primazia delle esigenze di sicurezza nazionale, interesse pubblico e amministrazione della giustizia sul rispetto dell'accordo Approdo Sicuro e quindi sulla garanzia di un determinato standard di tutela della riservatezza e protezione dei dati valutato come adeguato dalle Istituzioni europee. I giudici di Lussemburgo così sono giunti alla conclusione che tale 'crepa' derogatoria nella regolamentazione del

[29] "In tali circostanze, in virtù delle constatazioni effettuate al punto da 60 a 63 della presente sentenza, e al fine di fornire una risposta completa a detto giudice, occorre verificare se tale decisione sia conforme ai requisiti risultanti da detta Direttiva, letta alla luce della Carta", par. 67, *Schrems*.

[30] Veniva chiesto in particolare se, sulla base della normativa indicata, le autorità di garanzia avessero l'obbligo di adeguarsi alla decisione della Commissione o se dovesse invece considerarsi sussistente in capo a tali autorità un potere autonomo di indagine e di messa in discussione della valutazione dell'organo europeo.

[31] L'effetto vincolante per gli Stati membri prodotto dalla decisione di adeguatezza emanata dalla Commissione ex art. 25, Dir. 95/46/CE è stato interpretato dall'Autorità garante irlandese come una privazione di discrezionalità e potere dei garanti nazionali, che non possono far altro se non rispettare le valutazioni della Commissione. Ciò viene in parte confermato dalla CGUE nella sentenza *Schrems* nel punto in cui afferma che i garanti nazionali non possono emanare decisioni contrarie a quelle adottate a livello europeo dalla Commissione stessa. I giudici di Lussemburgo però non si fermano a questa conclusione, che sembrerebbe negare ai cittadini la possibilità di denunciare, tramite lo scrutinio delle autorità garanti nazionali, violazioni dei propri diritti risultanti dal trasferimento di dati al di fuori del territorio dell'UE: pur non potendo infatti vietare o sospendere il trasferimento dati ritenuto inadeguato, la Corte afferma il dovere dei garanti nazionali di valutare comunque con diligenza le doglianze loro rivolte e "verificare, in piena indipendenza, se il trasferimento di tali dati rispetti i requisiti fissati" dalla Dir. 95/46/CE (par. 57, *Schrems*). Nel caso in cui dovesse considerare fondate le censure sollevate dal cittadino, l'autorità garante dovrebbe quindi avere la possibilità di promuovere azioni giudiziarie: "incombe al legislatore nazionale prevedere mezzi di ricorso che consentano all'autorità nazionale di controllo di cui trattasi di far valere le censure che essa reputa fondate dinanzi ai giudizi nazionali, affinché questi ultimi procedano, qualora condividano i dubbi di tale autorità in ordine alla validità della decisione della Commissione, ad un rinvio pregiudiziale inteso all'esame della validità di tale decisione" (par. 65, *Schrems*). Questa soluzione permetterebbe, secondo il ragionamento della Corte, di rispettare sia il diritto dei singoli di ottenere ascolto alle proprie doglianze, sia il principio di prevalenza del diritto UE e la competenza esclusiva della CGUE a dichiarare l'invalidità di un atto dell'Unione. Viene dunque attribuita facoltà alle autorità di garanzia di sollevare questioni di illegittimità dell'atto adottato dalla Commissione per via indiretta dinnanzi ai giudici nazionali, i quali poi, mediante rinvio pregiudiziale, attiveranno il ruolo esclusivo di controllo della CGUE. Tale rinvio però "dovrà possedere le caratteristiche alle quali la giurisprudenza UE subordina la ricevibilità di tali rinvii e in particolare essere una controversia reale tra più parti opposte tra loro. Ora, è proprio la sussistenza di questa condizione che potrebbe porre difficoltà. Nella ricostruzione della Corte, il predetto giudizio sembra in effetti volto non tanto a risolvere la controversia reale tra parti opposte, ma solo a effettuare il rinvio pregiudiziale di validità ai giudici UE al fine di preservare i principi di supremazia del diritto UE e il monopolio della Corte nel valutare la validità degli atti dell'Unione", S. CRESPI, *Il trasferimento dei dati personali UE negli Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la privacy*, op. cit., 702. Deve essere tuttavia precisato che ai sensi dell'art. 58, par. 1, lett. j del GDPR, alle autorità garanti nazionali è stato ora attribuito il potere di "ordinare la sospensione dei flussi di dati verso un destinatario in un paese terzo o un'organizzazione internazionale".

flusso di dati transfrontalieri comportasse una possibile ma significativa compressione dei diritti fondamentali dei soggetti cui i dati trasferiti oltreoceano appartenevano. La Commissione, nella sua decisione di adeguatezza, non aveva del resto menzionato né riconosciuto in nessun punto l'esistenza, all'interno dell'ordinamento statunitense, di tutele idonee a limitare tali probabili ingerenze perpetrate da soggetti pubblici. Questa assenza è poi stata confermata dalla Corte stessa che ha sottolineato come negli USA non fossero predisposte tutele giuridiche efficaci, richiamando peraltro quanto chiaramente affermato dalla Commissione stessa all'interno delle Comunicazioni sopra richiamate COM (2013) 846 e 847 final, a seguito del *datagate*.

Alla luce di questa analisi, si nota come anche in questa pronuncia vengano ribaditi i principi delineati nella precedente giurisprudenza della Corte di giustizia, in particolare nella sentenza *DRI*, questa volta però estesi ad un contesto diverso, quello della dimensione esterna, cioè del livello di tutela apprestato da uno Stato terzo ai dati provenienti dall'UE. Ciò che viene messo in discussione non è la legittimità dell'interesse "sicurezza nazionale", capace, entro certi limiti, di giustificare la compressione e l'interferenza nei diritti fondamentali; ciò che viene contestata è invece la natura incondizionata e generalizzata della conservazione, dell'accesso ed utilizzo di questi dati da parte delle pubbliche autorità statunitensi, operazioni prive di regole chiare, precise e prevedibili e non limitate a quanto strettamente necessario: qui è evidente la riproposizione di quella interpretazione del principio di necessità già affermato nella sentenza *DRI*. In particolare, ripercorrendo pedissequamente il test di proporzionalità delineato in materia di *data retention*, la Corte ha stabilito come non potesse ritenersi limitata "allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta" (par. 93, *Schrems*).

Un vaglio dettagliato di proporzionalità e stretta necessità delle misure predisposte dall'Approdo sicuro non si è tuttavia reso necessario ai fini della risoluzione del caso poiché la Corte ha ritenuto preliminarmente che "una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata *al contenuto* di comunicazioni elettroniche pregiudica il *contenuto essenziale* del diritto fondamentale al rispetto della vita privata" (par. 94, *Schrems*, enfasi aggiunta). I giudici di Lussemburgo inoltre hanno ritenuto violato non solo il nucleo essenziale del diritto alla vita privata[32] — ma anche quello ad una tutela giurisdizionale effettiva (art. 47, Carta di Nizza), indicando nell'assenza di rimedi e di un controllo giurisdizionale effettivo[33] nonché nella mancanza di misure volte a garantire la possibilità di rettifica o la cancellazione dei dati, elementi sufficienti a pregiudicare il contenuto essenziale del diritto stesso.

Questa specifica posizione della Corte assume particolare interesse poiché stabilisce una distinzione tra le intrusioni delle autorità di intelligence americane che coinvolgono il vero e proprio contenuto delle comunicazioni (come avvenuto con il programma Upstream) e le ingerenze che invece riguardano i meri metadati, come nella decisione *DRI*, che non sono state considerate idonee a pregiudicare il nucleo essenziale del diritto alla riservatezza e protezione dei dati (par. 39, *DRI*). Tale distinzione, dalla quale prenderanno le mosse alcune riflessioni di più ampio respiro all'interno delle conclusioni di questa analisi e che già era stata proposta nella previa sentenza del 2014, è stata il fattore determinante della rapida chiusura della questione e della brevità della decisione *Schrems*, diversamente da quanto

[32] Si vuole evidenziare sin da ora come non sia stata in questo caso considerata la violazione del nucleo essenziale del diritto alla protezione dei dati personali sancito dall'art. 8 della Carta di Nizza.

[33] Molto interessante sul punto è la precisazione della Corte al par. 95: "L'esistenza stessa di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto".

avvenuto nel caso *DRI*: in questo senso la Corte sembra accettare "the idea that fundamental rights must be understood as having a 'hard core' that should remain outside the scope of application of the balancing test"[34]. In altre parole, le considerazioni espresse dalla CGUE sulla lesione del nucleo essenziale dei diritti di cui agli art. 7 e 47 della Carta di Nizza bastano per ritenere la decisione di adeguatezza in violazione dei criteri indicati all'art. 25 della Dir. 95/46/CE, senza necessità di spingersi oltre ad analizzare la proporzionalità delle singole disposizioni dell'Approdo sicuro (par. 98, *Schrems*)[35]: nella decisione della Commissione infatti non veniva riconosciuta nella legislazione nazionale o negli impegni internazionali assunti dagli USA la garanzia di un livello di protezione adeguato dei diritti alla vita privata e protezione dei dati (par. 97, *Schrems*) e questa carenza, insieme alla mancanza di idonee tutele con riferimento alle attività e ai poteri delle autorità pubbliche, hanno fatto propendere per l'invalidità della Decisione[36].

Risulta chiaro, dalla ricostruzione della Corte, come le valutazioni circa l'adeguatezza delle tutele disposte dallo Stato terzo nel caso di trasferimento dati dall'UE non si debbano limitare a considerare i principi e le condizioni valide per i soggetti privati bensì anche le garanzie fornite dalle autorità pubbliche, ad esempio di *law enforcement* o intelligence, nel loro complesso: questo scrutinio è stato svolto dalla Corte nel caso *Schrems* ma è evidente che, in occasione di ulteriori decisioni di adeguatezza, sarà la Commissione stessa ad essere chiamata, sulla base dei parametri giurisprudenziali indicati dai giudici di Lussemburgo, a valutare anche questi aspetti così rilevanti ai fini di vagliare pienamente la sostanziale equivalenza delle garanzie predisposte dallo Stato ricevente[37].

---

[34] Così T. OJANEN, *Making the essence of fundamental rights real: the Court of Justice of the EU clarifies the structure of fundamental rights under the Charter*, in *European Constitutional Law Review*, 12, 2016, p. 325. Su questo punto l'autore equipara tale posizione della Corte con quella della Corte costituzionale tedesca nella sentenza BVerfGE 34, 238 (245) nella quale i giudici hanno negato la possibilità di effettuare un bilanciamento e applicare il principio di proporzionalità laddove l'ingerenza giunga colpire il nucleo essenziale del diritto, che rappresenta un limite invalicabile.

[35] Alcuni commentatori, quali Mantelero, hanno evidenziato come la *ratio* che ha mosso la decisione di adeguatezza risulti viziata alla base in quanto, diversamente da quanto espressamente previsto dalla Dir. 95/46/CE, manca una valutazione dell'adeguatezza delle tutele offerte dall'ordinamento statunitense considerato nella sua interezza e non solo limitatamente alle condizioni poste in essere dai principi dell'Approdo sicuro. Quella che è stata definita come una 'adeguatezza parziale', rappresenterebbe pertanto un *tertium genus* rispetto alle valutazioni indicate come necessarie dal legislatore europeo: "tali norme delineano infatti solamente due modalità volte a garantire un livello adeguato di protezione dei dati: l'accordo fra *data importer* e *data exporter* o l'esistenza nel Paese terzo di un ordinamento giuridico che offra tale livello di protezione", A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield* , op. cit., p. 241.

[36] Per una più ampia analisi di questa rilevante pronuncia, si legga, tra i molti: S. PEYROU, *La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques*, in *Journal de droit européen*, 2, 2015; P. FALLETTA, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c. DPC, C-362/14)*, in *Federalismi.it*, 24, 2015; F. LE DIVELEC, *Charte des droits fondamentaux – Protection des données personnelles – Safe Harbor (Sphére sécurité)*, in *Revue du droit de l'Union européenne*, 2, 2015; S. CARRERA, E. GUILD, *The end of Safe Harbor: what future for EU-US data transfers?*, in *Maastricht Journal of European and Comparative law*, 3, 2015; M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il diritto dell'informazione e dell'informatica*, 4, 2015; R. DE SIMONE, *Corte di giustizia dell'UE, Grande Sezione, sentenza 6 ottobre 2015, in causa C-362/14, Maximillian Schrems c. Data Protection Commissioner*, in *Rivista Italiana di diritto pubblico comunitario*, 4, 2015; X. TRACOL, *"Invalidator" strikes back: the harbour has never been* safe, in *Computer Law and Security Review*, 3, 2016; C. FOSSA', *Facebook nel mirino delle Corti: accanimento giurisprudenziale a cavallo del caso Schrems?*, in *Ricerche giuridiche*, 1, 2017.

[37] La necessità di estendere una valutazione dell'adeguatezza non solo alle disposizioni normative del Paese terzo attinenti al rapporto tra privati ma anche alle previsioni che riguardano le attività delle pubbliche autorità, è stata affermata peraltro dalla Commissione stessa, successivamente alla sentenza *Schrems*: "[Il riconoscimento del livello di adeguatezza] prevede una valutazione globale dei sistemi del Paese terzo, compresa la normativa sull'accesso ai dati personali da parte delle pubbliche autorità preposte alle attività di contrasto, alla sicurezza personale o ad altro scopo d'interesse pubblico", Comunicazione della Commissione al Parlamento Europeo e al Consiglio, *Scambio e protezione dei dati personali in mondo globalizzato*, COM (2017) 7 final, 7. Questo aspetto

3. – Dal Safe Harbour *al* Privacy Shield*: le implicazioni della sentenza* Schrems *e il complesso panorama attuale*

3.1. – Il Privacy Shield *e la pesante eredità della sentenza* Schrems

Inutile sottolineare il forte impatto che questa decisione ha comportato nel settore economico: le imprese stanziate nei territori dell'Unione europea si sono trovate a non poter più – legittimamente – inviare oltreoceano i dati raccolti, se non mediante la predisposizione di misure alternative[38], causando così una situazione di forte incertezza e stallo[39]. La necessità di addivenire presto ad una chiara via d'uscita da tale *empasse* è risultata da ambo le parti prioritaria, nell'interesse sia delle Autorità americane e delle aziende statunitensi così come di quelle europee e nella consapevolezza, più volta evidenziata,

peraltro emerge chiaramente dal nuovo dettato del GDPR che, all'art. 45, par. 3, lett. a, prevede espressamente che la Commissione debba considerare anche "la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali)".

[38] Le aziende aventi sede nel Continente europeo, in attesa di un nuovo accordo tra UE e USA e di una nuova decisione di adeguatezza, hanno potuto proseguire lo scambio di dati con gli Stati Uniti mediante il ricorso a strumenti alternativi predisposti dalla Dir. 95/46/CE e più sopra richiamati (clausole contrattuali tipo, etc.). Con riferimento ad essi, tuttavia, alcuni autori hanno sin da subito evidenziato perplessità circa la loro conformità alla Carta di Nizza ed al diritto dell'UE, ipotizzando la necessità di estendere ed applicare, anche a tali strumenti, i principi ed i requisiti individuati nella giurisprudenza della CGUE in *DRI* e *Schrems*. Sul punto si è interrogata, tra gli altri, S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo scudo UE/USA per la privacy*, op. cit., p. 711; ma anche la Commissione stessa in COM (2015) 566 final, p. 6. Come si vedrà nel prosieguo di questo Capitolo, tali quesiti, con particolare riferimento all'utilizzo di *Standard Contractual Clauses*, sono sfociati in un caso giudiziario rinviato dalla High Court irlandese alla Corte di giustizia ed attualmente pendente. Merita infine sottolineare come nella fase che ha preceduto l'approvazione di un nuovo accordo, sussistesse comunque, per le imprese americane che non garantivano un adeguato livello di tutela dei dati mediante gli strumenti alternativi indicati, il rischio di poter essere chiamate in causa di fronte ai giudici nazionali per rispondere dei danni provocati: "The remedy for the individual will be compensation and damages for loss and, depending on the national system, distress. A 2013 case from the UK where the breach was purely technical and there was no quantifiable loss to the individual still resulted in a compensation award of €1000 (Halliday v. Creation Consumer Finance Ltd [2013] All ER (D) 199 (Mar)", S. CARRERA, E. GUILD, *Safe Harbour or into the Storm? EU-US Data transfer after Schrems Judgement*, in *CEPD Liberty and Security in Europe Papers*, novembre 2015, disponibile all'indirizzo: https://www.ceps.eu/system/files/CEPS_LSE_85.pdf.

[39] È necessario precisare comunque come le conseguenze derivanti dalla decisione *Schrems* e dai principi in essa delineati non si siano manifestate solo con riferimento al trasferimento di dati verso gli USA: innanzitutto, la pronuncia analizzata ha determinato il bisogno di un intervento di modifica delle previe Decisioni di adeguatezza riguardanti "Paesi che sono strettamente integrati con l'UE e i suoi Stati membri (Svizzera, Andorra, Isole Faer Oer, Guernsey, Jersey, Isola di Man), importanti partner commerciali (Argentina, Canada, Israele) e i Paesi che hanno un ruolo di pioniere nell'elaborazione di leggi sulla protezione dei dati nella loro regione (Nuova Zelanda, Uruguay)" (COMMISSIONE EUROPEA, *Comunicazione: Scambio e protezione dei dati personali in mondo globalizzato*, COM(2017)7 final, p. 7). Queste decisioni, infatti, sono state riviste con la Decisione di esecuzione (UE) 2016/2295 della Commissione del 16 dicembre 2016, che ha modificato le previe Decisioni 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE e le decisioni di esecuzione 2012/484/UE, 2013/65/UE riguardanti l'adeguatezza della protezione dei dati personali da parte di taluni paesi, a norma dell'articolo 25, paragrafo 6, della Direttiva 95/46/CE del Parlamento europeo e del Consiglio. La pronuncia dei giudici di Lussemburgo oltretutto – e sorprendentemente – ha causato grande incertezza giuridica non solo nella disciplina del flusso dei dati tra USA e UE ma addirittura tra USA e Stati extra-UE che avevano concluso accordi con le autorità statunitensi sulla scorta del modello *Safe Harbour* e che, proprio alla luce della giurisprudenza della CGUE, hanno messo in discussione la proporzionalità e necessità di tali accordi e delle salvaguardie in esso sancite. La Svizzera, ad esempio, all'indomani della sentenza della CGUE, ha dichiarato non più applicabile l'accordo c.d. *Swiss-Harbour* per il trasferimento di dati Svizzera-USA e basato sui medesimi principi elaborati nell'accordo UE-USA, in quanto non compatibile con la normativa nazionale di protezione dei dati. Sul punto si richiama: S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo Sicuro allo Scudo UE/USA per la privacy,* op. cit, p. 706, ma anche O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'UE nel reasoning dei giudici di Lussemburgo*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield",* op. cit.

che un blocco del flusso di dati nell'economia dell'informazione attuale si traduce in ingenti perdite in termini di guadagno oltre che in un dannoso isolamento dal mercato globale. Questo spiega come in – relativamente – pochissimo tempo e con colloqui intensificati, l'UE e gli USA siano addivenuti ad un nuovo accordo denominato *Privacy Shield* (o 'Scudo per la privacy') e dunque ad una nuova decisione di adeguatezza della Commissione[40]. Tali più recenti condizioni regolanti il flusso dei dati UE-USA sono state certamente portatrici di rilevanti novità rispetto al previo assetto garantito dal meccanismo di Approdo sicuro, accogliendo ed attuando alcune osservazioni emerse sia dalle Comunicazioni della Commissione giunte all'indomani delle rivelazioni di Snowden, sia dalla decisione *Schrems*. Pur mantenendo il sistema di autocertificazione, che non era stato oggetto di critiche quantomeno da parte della Corte di giustizia, i controlli sul rispetto dei requisiti dello Scudo per la privacy sono stati rafforzati, rispondendo così a quella debolezza della fase di *enforcement* rilevata nel precedente Approdo sicuro[41]. Le novità riguardano anche, per la prima volta, il fronte delle attività delle autorità pubbliche e del loro accesso ai dati provenienti dall'UE, tra cui spiccano sia l'impegno, confermato in una dichiarazione delle autorità statunitensi stesse, di utilizzare i dati solo in casi eccezionali, sia la creazione della figura dell'Ombudsperson di nomina presidenziale ma indipendente rispetto ai servizi di intelligence, oltre all'introduzione di possibili rimedi previsti per i cittadini europei che ritengano illegittimo il trattamento dei propri dati e abbiano subito danni da esso.

Se è vero dunque che alcune rassicurazioni da parte delle autorità pubbliche sono espressamente contenute nel *Privacy Shield*, non possono comunque non evidenziarsi persistenti carenze e incongruità o quanto meno perplessità circa la conformità di tali disposizioni rispetto a quanto richiesto e fissato dalla Corte di giustizia nel caso *Schrems*: sebbene a seguito del *datagate* alcune modifiche siano state apportate al sistema normativo statunitense, permane in capo alle autorità *law enforcement* e intelligence una ampia possibilità di ottenere dalle aziende private con sede negli USA i dati, anche quelli relativi al contenuto delle telecomunicazioni, dei propri clienti e dunque anche di quei dati provenienti dall'UE. Questo potere delle pubbliche autorità si presenta senza dubbio maggiormente limitato rispetto alla vaga ed ampia dicitura che caratterizzava l'Approdo sicuro: ciò anche grazie al rimando ad alcune disposizioni statunitensi (ad esempio la *Presidential Policy Directive*, c.d. PPD-28, del 17 gennaio 2014 che regola raccolta e accesso ai dati da parte delle autorità di intelligence[42] o, ancora, il *Judicial Redress Act*[43]) che hanno circoscritto le operazioni di raccolta, conservazione e uso indiscriminato o

[40] Decisione di esecuzione COM (2016)1250, sull'adeguatezza della protezione offerta in ragione dello Scudo UE-USA per la privacy, 12 luglio 2016.

[41] Per approfondimenti sul contenuto di questo accordo, si rimanda più ampiamente a: S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo scudo UE/USA per la privacy*, op. cit.; G. VERMEULEN, *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities*, in G. VERMEULEN, E. LIEVENS (a cura di), *Data protection and privacy under pressure. Transatlantic tensions, EU serveillance and Big Data*, Maklu, 2017.

[42] Per una panoramica circa le modifiche normative che il Congresso si è apprestato, non senza difficoltà, ad approvare, a seguito delle rivelazioni di Snowden, si legga: A. BUTLER, F. HIDVEGI, *From Snowden to Schrems*, op. cit. In estrema sintesi (e come richiamato anche nell'analisi effettuata dalla Commissione all'interno della Decisione di esecuzione COM (2016)1250, Allegato VI), il PPD-28 è stato introdotto nel 2014 dal Presidente Obama e prevede in capo ai membri della Intelligence Community l'onere di implementare nuove misure e *policies* volte a rafforzare la tutela della privacy all'interno dei programmi di sorveglianza. Questa Directive è composta da sei sezioni, la prima delle quali fissa i principi che devono essere rispettati dall'intelligence nelle operazioni di raccolta dati ("executive branch authorization, purpose limitation, prohibition on collecting foreign private commercial information for competitive advantage, narrow tailoring of collection activities"). La seconda sezione invece impone che la raccolta dati *in bulk* sia limitata a sei scopi: combattere le minacce derivanti da attività di spionaggio, combattere il terrorismo, combattere la produzione e il commercio di armi di distruzione di massa, contrastare le minacce alla sicurezza informatica, le minacce alle forze armate o al personale militare e le minacce transnazionali inerenti una o più delle altre cinque finalità.

[43] Il *Judicial Redress Act*, approvato nel dicembre 2015, amplia anche ai cittadini stranieri le protezioni e garanzie giurisdizionali riconosciute in capo ai cittadini statunitensi (ad esempio il risarcimento dei danni da trattamento

generalizzato di dati relativi a soggetti non cittadini statunitensi solo a finalità specifiche ed ampliando parallelamente la possibilità di accesso a rimedi giudiziari.

Come alcuni autori hanno sottolineato[44], una lettura più approfondita di queste normative statunitensi e delle affermazioni della Commissione nella sua decisione di adeguatezza rivelano però l'utilizzo da parte del legislatore americano di formule ambigue o ampiamente discrezionali: il richiamato PPD-28 prevede infatti che la richiesta da parte delle autorità pubbliche di accedere ai dati – conservati da soggetti privati – debba essere "quanto più possibile mirata", favorendo, se disponibile, l'utilizzo di altre tipologie di informazioni o il ricorso ad alternative appropriate e fattibili, rispecchiando "la regola generale che impone di privilegiare la rilevazione mirata alla raccolta in blocco di dati. L'ODNI (Ufficio del direttore dell'intelligence nazionale statunitense) assicura in particolare che la raccolta di dati in blocco non si configura come raccolta in massa o indiscriminata e l'eccezione non fagocita la regola generale"[45]. La Commissione stessa, nella sua decisione, prosegue riconoscendo ed ammettendo che i servizi di intelligence necessitano, in talune circostanze, di procedere ad una raccolta di dati in blocco (*bulk collection*), pur limitandola ai soli casi in cui, "in base a considerazioni tecniche o operative, non risulti possibile procedere alla rilevazione mirata con il filtro di discriminanti, ossia di un identificatore associato a un obiettivo specifico (quale l'indirizzo di posta elettronica dell'obiettivo o il suo numero di telefono)"[46]. Queste rassicurazioni e condizioni restrittive e di tutela così ampiamente tracciate, fanno sorgere dubbi circa la loro conformità a quei criteri di proporzionalità e stretta necessità delineati dalla CGUE nella sua giurisprudenza; così come non paiono del tutto soddisfacenti le limitazioni all'accesso e trattamento di dati in blocco (*bulk*) che possono essere svolte per i soli scopi indicati in una lista di sei vaste finalità[47], anch'esse solo vagamente riportate dalla Commissione e comunque disciplinanti la sola fase di accesso e utilizzo dei dati e non i previ passaggi di raccolta e conservazione, che presentano dunque minori salvaguardie e restrizioni. Proprio questo aspetto, il concentrarsi cioè sui soli limiti posti alla fase di accesso, è stato sottolineato come critico e problematico da parte di alcuni commentatori[48]: sappiamo bene, infatti, sin dalla sentenza *DRI*, che secondo i giudici di Lussemburgo anche la mera conservazione di dati rappresenta *per se* una ingerenza nei diritti fondamentali che va pertanto limitata a quanto strettamente necessario, ancor prima delle operazioni di accesso, come peraltro confermato anche dalla sentenza *Schrems*[49]. Ritenere, al contrario, corretta ed accettabile una distinzione del livello di tutela richiesto a seconda delle due diverse fasi – richiesta e dunque raccolta e conservazione da un lato e accesso dall'altro – può far giungere alla conclusione che una raccolta e conservazione indiscriminata e generalizzata sia da considerarsi legittima nel caso in cui vi siano stringenti limitazioni e controlli nel successivo momento dell'accesso. Questa pare essere la lettura seguita dalla Commissione, che si focalizza più sulle garanzie in termini di utilizzo del dato da parte delle autorità

illecito). La portata garantista e innovatrice di questa misura viene comunque da molti autori largamente critica e ridimensionata poiché gli oneri per poter accedere a tali rimedi giudiziari risultano ancora estremamente pesanti, rendendo difficile la realizzazione di un effettivo accesso alla giustizia. Sul punto si legga: D. BENDER, *The Judicial Redress Act: A Path to Nowhere,* in *Privacy Advisor,* Issue 17, 2015.

[44] G. VERMEULEN, *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities,* op.cit., ma anche S. SICA, V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, op. cit., e A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, op. cit.

[45] Par. 71, Decisione di esecuzione COM (2016)1250.

[46] Par. 71, Decisione di esecuzione COM (2016)1250.

[47] Par. 65, Decisione di esecuzione COM (2016)1250.

[48] G. VERMEULEN, *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities,* op.cit., p. 65.

[49] "Non è limitata allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito", par. 93, *Schrems.*

pubbliche statunitensi anziché sulle limitazioni in materia di raccolta e conservazione: "Sebbene non formulati nei medesimi termini giuridici, nell'essenza detti requisiti [del *Privacy Shield*] rispecchiano i principi di necessità e di proporzionalità. È chiaramente privilegiata la rilevazione di dati mirata, mentre la raccolta in blocco è limitata alle situazioni (eccezionali) in cui motivi tecnici o operativi rendono impossibile la raccolta mirata. Anche nei casi in cui la raccolta in blocco è inevitabile, l'uso ulteriore, tramite l'accesso, dei dati così raccolti è rigorosamente limitato a precise finalità legittime di sicurezza nazionale"[50].

Quanto poi allo specifico regime della conservazione dei dati, esso viene considerato dalla Commissione proporzionato e legittimo, sebbene le condizioni di *data retention* siano delineate dalla normativa statunitense e dal *Privacy Shield* in maniera piuttosto generica e tutt'altro che ristretta: se la regola generale è che i dati siano conservati dalle autorità pubbliche per un massimo di cinque anni, è purtuttavia concessa una *data retention* più prolungata nell'interesse della sicurezza nazionale "in base a una considerazione di diritto o a una decisione esplicita del Direttore dell'Intelligence nazionale, maturata dopo un'attenta valutazione degli aspetti legati alla privacy e sentiti il responsabile della tutela delle libertà civili dell'ODNI e i responsabili della tutela della vita privata e delle libertà civili degli enti"[51]. Se è vero che nel caso *DRI* la Corte si riferiva ad una normativa europea riguardante la conservazione dei dati per scopi di sicurezza non necessariamente nazionale bensì pubblica e dunque riguardante l'attività di autorità di *law enforcement*[52], non si può non notare la discrepanza tra i criteri ed i principi individuati dalla CGUE in merito e quanto invece stabilito dalla normativa americana e ritenuto comunque adeguato dalla Commissione: in particolare resta piuttosto discusso e incerto se una forma di raccolta, conservazione e analisi così delineata assuma realmente natura limitata e se le restrizioni predisposte siano in grado di circoscriverne la portata e il carattere generalizzato.

Insomma i rilievi e sottolineature sino ad ora svolte hanno fatto sorgere, già all'indomani della adozione della decisione di adeguatezza della Commissione, forti perplessità circa la sua idoneità e capacità di superare il vaglio della Corte di giustizia[53]. Pur apportando delle modifiche innegabilmente

[50] Par. 76, Decisione di esecuzione COM (2016)1250.

[51] Par. 86, Decisione di esecuzione COM (2016)1250. È interessante sottolineare come in tale documento venga anche specificato che, con riferimento alle informazioni personali raccolte ai sensi della sezione 702 della FISA – già sopra analizzata –, "le procedure di minimizzazione dell'NSA, omologate dalla Corte FISA, prevedono che, in linea di principio, i metadati e i contenuti non scremati siano conservati al massimo per cinque anni per il programma PRISM e al massimo per due anni per il programma UPSTREAM. L'NSA rispetta questi limiti di archiviazione attraverso un processo automatizzato che cancella i dati raccolti al termine del rispettivo periodo di conservazione" (nota 94). Emergono quindi alcuni dubbi in merito alla natura realmente mirata, proporzionata e limitata allo stretto necessario di questa tipologia di conservazione, sulla base di quanto affermato dalla Corte di giustizia nella sua richiamata giurisprudenza. Per una lettura approfondita circa il funzionamento della controversa sezione 702 FISA e delle sue criticità: A. NOLAN, R. THOMPSON, E. LIU, *Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments*, Congressional Research Service, aprile 2014.

[52] Come si avrà modo di vedere, questo punto è ancora estremamente controverso e oggetto di un rinvio pregiudiziale attualmente pendente dinnanzi alla CGUE: C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e al.*

[53] Una posizione critica è infatti emersa dall'analisi svolta da numerosi autori, da quella più netta di Vermeulen, Terpan (vedi *infra*) e Mantelero, a quella più 'possibilista' ma comunque dubitativa di Crespi e Sica, che si sono da subito interrogati sulla conformità della decisione della Commissione ai criteri indicati dalla giurisprudenza europea. Anche Tracol, in *EU–U.S. Privacy Shield: The saga continues*, in *Computer Law and Security Review*, 32, 2016, ha sottolineato come nel nuovo accordo la Commissione abbia, ancora una volta, mancato di effettuare una valutazione del sistema normativo statunitense in materia di tutela della privacy e della protezione dei dati nel suo complesso, come invece richiesto dall'art. 25 Dir. 95/46 e ribadito nella sentenza *Schrems*: "The Commission has relied on letters from various authorities of the US government appended as annexes 1 to 7 to the decision and not on relevant US law. These letters may however not shield US law from the application of the findings made by the Grand Chamber in the Schrems judgment. The latter implies substantial changes to the US law. The legal system of the US has however not changed", p. 777. Tale visione è sostenuta anche da Terpan, che afferma: "One major shortcoming is that the adequacy decision as regards Privacy Shield, like its predecessor, does not meet the CJEU requirement that the Commission should make an evaluation of US rules and guarantees. As these

apprezzabili al precedente Approdo sicuro, introducendo e rafforzando non solo gli obblighi in capo alle imprese bensì anche quelli interessanti l'accesso da parte di autorità pubbliche, la decisione non pare fugare del tutto i dubbi circa il rispetto dei requisiti di stretta necessità e proporzionalità del trattamento di dati effettuato, anche per scopi securitari, negli USA, requisiti peraltro chiaramente ribaditi dalla Corte di giustizia anche nella successiva sentenza *Tele2*.

3.2. – L'adeguatezza del livello di protezione dei dati garantito dagli USA sulla base del Privacy Shield *sottoposta allo scrutinio dei giudici di Lussemburgo: una storia destinata a ripetersi?*

Tali quesiti e perplessità, già indicati non solo da studiosi ed esperti nel settore ma anche da autorità quali il Gruppo di lavoro Articolo 29[54], sono sfociati poi, come pronosticato e senza farsi a lungo attendere, in casi giudiziari promossi, a vario titolo, dinnanzi alla Corte di giustizia dell'UE: si fa riferimento a due differenti ricorsi di annullamento azionati rispettivamente dalle ONG *Digital Rights Ireland*[55] e *La Quadrature du Net*[56] insieme ad altre associazioni francesi; mentre il primo ricorso è stato dichiarato inammissibile con ordinanza del Tribunale, datata 22 novembre 2017[57], il secondo è attualmente pendente e vede i ricorrenti sostenere che il carattere generalizzato della raccolta e accesso ai dati autorizzata dalla normativa USA pregiudichi il contenuto essenziale del diritto fondamentale al rispetto della vita privata (art. 7, Carta di Nizza), con la conseguenza che le considerazioni della Commissione sul livello adeguato di tutela assicurato dal *Privacy Shield* siano da ritenersi erronee.

---

guarantees continue to be mostly based on declarations of intent, there are sufficient reasons to believe that the legality of the new regime is fragile", F. TERPAN, *EU-US data transfer from Safe Harbour to Privacy Shield: back to square one?*, in *European Papers*, 3, 2018, p. 1058. Forti perplessità sono state espresse anche con riferimento all'accesso ai rimedi giudiziari e alla efficacia della figura dell'Ombudsperson, sia perché la procedura per accedere al vaglio di quest'ultimo è estremamente lunga e complessa, sia perché anche al termine del procedimento non verrà comunque mai confermato l'assoggettamento del ricorrente ad operazioni di sorveglianza; ciò che verrà invece unicamente affermato è se il ricorso è stato "properly investigated" e se è stata o meno rispettata la normativa statunitense. Sul punto specifico, si legga: M. TZANOU, *European Union regulation of transatlantic data transfers and online surveillance*, op. cit. p. 563.

[54] Il Gruppo di lavoro Art. 29 ha vagliato la bozza di decisione di adeguatezza presentata dalla Commissione il 29 febbraio 2016 e ha espresso, ai sensi dell'art. 30 Dir. 95/46/CE, la propria opinione non vincolante (Opinion 01/2016 on the draft EU-US Privacy Shield adequacy decision, WP 238, 13 aprile 2016). In questo documento sono state messe in luce in particolare alcune criticità; tra le altre, è stato riconosciuto il fatto che la Directive PPD-28 "has not removed the possibility for the indiscriminate collection of personal data in bulk and that the scale of such collection possibilities remains unclear and potentially broad". Con riferimento dunque alla possibilità di raccolta e accesso di dati per motivi di sicurezza nazionale, il Gruppo di lavoro sottolinea come il fatto di provvedere ad un trattamento e uso dei dati di tipo targetizzato lasci però 'scoperta' e priva di specifiche tutele la fase della raccolta, che di conseguenza sembra poter assumere una natura massiva e generalizzata: "the targeted principles should apply to both the collection and the subsequent use of the data and cannot be limited to just the use". Anche i richiamati sei scopi per i quali è legittima una raccolta di dati generalizzata (*in bulk*) vengono ritenuti non sufficientemente ristretti e limitati a quanto necessario e proporzionato. Sebbene a seguito di questa Opinion la Commissione abbia modificato la bozza di decisione, recependo alcune delle segnalazioni del Gruppo di lavoro, quest'ultimo ha concluso, nella Press Release del 1 luglio 2016, che anche la versione finale della decisione presenta criticità di rilievo: in particolare, "the WP29 notes the committment of the ODNI not to conduct mass and indiscriminate collection of personal data. Nevertheless, it regrets the lack of concrete assurances that such practice does not take place".

[55] T-670/16 *Digital Rights Ireland v Commissione,* promossa il 16 settembre 2016.

[56] T-738/16 *La Quadrature du Net e altri c. Commissione*, promossa il 25 ottobre 2016.

[57] Il Tribunale ha infatti ritenuto insussistenti i requisiti di cui all'art. 263 TFEU, vista l'impossibilità di rinvenire in capo alla ricorrente un interesse nell'annullamento della misura contestata: "the applicant is a legal person and its official title does not identify any natural person, it cannot avail of the protection of personal data. The contested decision is thus incapable of breaching any right to protection of personal data of the applicant. The annulment of the contested decision, therefore, is not capable of having, in itself, legal consequences for the applicant or of procuring for it an advantage in that regard" (par. 26-28).

Una ulteriore disputa, sebbene solo tangenzialmente vertente sulla decisione di adeguatezza *Privacy Shield*, è stata azionata dall'*Irish Data Protection Commissioner* (DPC), sulla base di un ricorso promosso, ancora una volta, da Maximillian Schrems: in questo complesso caso, la High Court irlandese ha deciso di richiedere nuovamente l'intervento della Corte di giustizia[58]. Il rinvio ha ad oggetto principalmente l'accertamento dell'adeguatezza del livello di protezione ("sufficient safeguards") offerto dalle c.d. *Standard Contractual Clauses*[59] (d'ora in avanti SCC), mirando in particolare a determinare se il trasferimento di dati dall'UE agli USA, mediante l'uso di clausole contrattuali tipo, violi la Carta di Nizza[60]. Come evidente, il caso non concerne direttamente e specificamente la decisione di adeguatezza adottata sulla base delle condizioni del *Privacy Shield*; la CGUE è tuttavia chiamata a

[58] C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, promossa dalla High Court irlandese il 4 maggio 2018. Il caso dinnanzi alla High Court risulta essere in realtà una diretta conseguenza della decisione *Schrems*. A seguito di tale pronuncia, infatti, la Corte irlandese che aveva proposto il rinvio ai giudici di Lussemburgo aveva annullato la decisione precedentemente assunta dal Data Protection Commissioner (DPC) irlandese nei confronti delle pretese avanzate da Maximillian Schrems e aveva dunque rinviato il caso nuovamente all'Autorità garante affinché valutasse le rimostranze del ricorrente alla luce, questa volta, delle posizioni espresse dalla CGUE. Il DPC ha pertanto aperto un nuovo procedimento e ha richiesto al Sig. Schrems di riformulare il proprio ricorso sulla base anche della intervenuta invalidazione del *Safe Harbour*. In altre parole, l'originaria doglianza dell'attivista austriaco necessitava di essere riformulata, indicando una nuova base giuridica del trasferimento dati oltreoceano: non potendo più fondarsi sull'ormai invalidata decisione 2000/520/CE, Schrems individuava la fonte del flusso di dati tra la sede irlandese e quella americana di Facebook nell'accordo c.d. *Data transfer processing Agreement*, concluso tra le due aziende nel 2015 ed integrante le *Standard Contractual Clauses* indicate dalla Commissione nella Decisione 2010/87; il ricorrente sosteneva che tali clausole non fossero idonee a garantire alcun diritto di accesso alla giustizia negli USA e che, ancora una volta, il livello di protezione dei dati e della riservatezza offerto, anche dalle clausole contrattuali tipo, non potesse considerarsi sostanzialmente equivalente a quello europeo.

[59] Si veda sul punto quanto già illustrato in generale nella nota 19.

[60] La causa si riferisce nello specifico alla Decisione 2010/87/UE, come modificata dalla Decisione 2016/2297 (cd. *SCC decisions*), nella quale la Commissione aveva affermato l'adeguatezza del livello di protezione dei dati garantita da una serie di clausole predisposte all'interno della Decisione stessa. Il DPC irlandese ha effettuato investigazioni sulle garanzie offerte dalle SCCs utilizzate da Facebook per trasferire i dati oltreoceano, esprimendo, al termine di tale analisi, dubbi circa l'adeguatezza della protezione garantita in tale contesto rispetto agli standard europei. Applicando quanto stabilito nella sentenza *Schrems*, par. 65, il DPC ha ritenuto quindi di non potersi pronunciare sulle doglianze del ricorrente senza considerare la validità della Decisione della Commissione UE in materia di SCCs, valutazione che però risulta essere di pertinenza della High Court, alla quale dunque il DPC ha pertanto fatto ricorso e che è l'unica autorità deputata, qualora lo reputi necessario, a rinviare la questione alla CGUE. Le perplessità riscontrate dal DPC sono state poi confermate anche dalla High Court irlandese che ha vagliato il caso, utilizzando memorie presentate anche dal governo statunitense, e che ha infine chiesto l'intervento della CGUE. Il primo quesito del rinvio pregiudiziale è volto a stabilire se "In circumstances in which personal data is transferred by a private company from a European Union (EU) member state to a private company in a third country for a commercial purpose pursuant to and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter of Fundamental Rights of the European Union ('the Charter')) apply to the transfer of the data notwithstanding the provisions of Article 4(2) of TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive 95/46/EC ('the Directive') in relation to public security, defence and State security?". Ancora una volta dunque si propone alla CGUE il tema dell'utilizzo di dati per scopi securitari e, conseguentemente, i limiti di competenza dell'UE in materie, come quella della sicurezza nazionale, che sarebbero unicamente di competenza degli Stati membri (art. 4, co. 2 TEU). I giudici di Lussemburgo in questo rinvio pregiudiziale sono quindi nuovamente chiamati a valutare la conformità alla Carta di Nizza di una decisione della Commissione sul trasferimento dati verso Stati terzi, anche se questa volta nell'ambito delle SCCs. La delicatezza e le possibili ripercussioni del caso in esame risultano chiaramente dalle affermazioni di Facebook nel corso del processo dinnanzi alla Corte irlandese: "Were SCCs to be invalidated, the effect on trade would be immense. If data transfers were prohibited, the effect on EU service imports into the US per annum would be a decrease of between 16% and 24%" e del resto neppure Schrems è giunto a richiedere l'invalidazione delle SCCs, affermando che "the solution is not for the Court to invalidate SCCs but for the Data Protection Commissioner to enforce them".

valutare il livello di protezione dei dati garantito negli USA[61], tenendo presenti anche alcune considerazioni e informazioni elaborate dalla High Court irlandese circa il regime di conservazione, accesso e utilizzo di dati da parte delle autorità pubbliche o di intelligence statunitensi.

Ciò che la High Court irlandese ha scritto nella sua decisione di rinvio, a seguito di uno studio approfondito dell'apparato normativo statunitense (par. 29-30), risulta essere infatti di estrema rilevanza per l'impatto e la fermezza delle affermazioni contenute: pur non sconfessando la natura in parte 'targettizzata' di sistemi di sorveglianza quali Upstream, viene stabilito che "it is inherent in a targeted search that a large body of data is searched. There is a distinction between bulk searching and bulk aquisition, collection or retention. The evidence establishes that under Upstream there is a mass surveillance in the sense that there is mass searching of communications. The search is for targeted communications and in this sense it is not indiscriminate. The issue to determine is whether, in light of the definition of processing in the Directive and the evidence in relation to the operation of the PRISM and Upstream programmes authorized under s. 702 of FISA, there is mass indiscriminate processing of data by the US government agencies. The High Court concluded that this was so on the basis of the definition of 'processing' in the Directive" (par. 32-33). Questo passaggio è di estremo interesse per le distinzioni effettuate in primis tra le operazioni di ricerca/scandagliamento di dati e quelle di acquisizione, raccolta o conservazione nonché tra operazioni di natura generalizzata o indiscriminata. Quanto a quest'ultima differenziazione, la Corte irlandese sembra suggerire l'esistenza, nello specifico programma PRISM, di una ricerca generalizzata, in grado cioè di creare uno scenario di sorveglianza di massa, ma non indiscriminata grazie alla natura targettizzata della ricerca, che punta a trovare uno o una cerchia di obiettivi determinati. Pur giungendo a questa conclusione, il giudice irlandese sostiene che tutte le operazioni perpetrate dalle autorità statunitensi mediante i programmi PRISM e Upstream, si concretizzino, nel complesso, in un trattamento dei dati (così come definito nella Dir. 95/46) di natura massiva, che si pone dunque in contrasto con il diritto dell'UE e con i rilievi e l'interpretazione fornita dalla CGUE nella sua ampia giurisprudenza sul punto.

La Corte irlandese inoltre, con riferimento al diritto ad un rimedio giudiziario effettivo e ad un giudice imparziale (art. 47, Carta di Nizza), "concluded that despite the number of possible causes of action, it cannot be said that US law provides the right of every person to a judicial remedy for any breach of his data privacy by the intelligence agencies. Retrospective judicial remedies would likely be unavailing to victims of governmental overreaching in the conduct of surveillance for the purpose of national security. US law never requires the subject of surveillance to receive notification at any time of the surveillance (unless the subject is a defendant in a criminal or administrative action) (..). The experts on the law of the US accepted that most people never know that they have been the subject of surveillance and if they do not know that effectively they can never sue" (par. 35).

I giudici della High Court, sulla base dei rilievi richiamati, che tratteggiano un quadro complesso e che pare allontanarsi invero da quelle valutazioni effettuate dalla Commissione nella sua decisione di

[61] "The issue whether the protections afforded to EU citizens whose data is transferred to the US are protected as required by Union law following the adoption of the Privacy Shield Decision and the establishment of the Privacy Shield ombudsperson requires to be determined by the Court in order to determine the validity of the SSC decisions. For these reasons, questions eight and nine of the reference are referred to the Court" (par. 45, High Court, 2016 no. 4809 P.). In uno degli 11 complessi quesiti posti alla CGUE, il giudice irlandese ha chiesto inoltre espressamente se il livello di adeguatezza attestato dalla Commissione sulla base del *Privacy Shield* potesse essere ritenuto incidente anche sulla determinazione dell'adeguatezza di altri strumenti di trasferimento quali appunto, nel caso specifico, le SCCs: "For the purpose of Art. 25 (6) of the Directive, does Decision EU 2016/1250 ("the Privacy Shield Decision") constitute a finding of general application binding on data protection authorities and the Courts of the Member states to the effect that the US ensures an adequate level of protection within the meaning of Article 25(2) of the Directive by reason of its domestic law or of the international commitments it has entered into?" (quesito 9).

adeguatezza, hanno così rinviato ai giudici di Lussemburgo, presentando ben 11 quesiti[62] che spaziano dalla applicabilità del diritto dell'UE e delle tutele da esso sancite anche nel caso in cui i dati trasferiti vengano trattati nello Stato terzo per scopi di sicurezza nazionale (quesito n. 1); la conformità alla Carta di Nizza e al diritto europeo delle garanzie offerte dalle SCCs e dunque la validità stessa della decisione della Commissione 2010/87 (quesito n. 8); il rapporto tra tale decisione e quella di adeguatezza, basata sul regime *Privacy Shield* nonché, indirettamente, la validità di quest'ultima (quesito n. 6).

Come risulta chiaro da questa, pur succinta, ricostruzione delle vicende giudiziarie nonché dei numerosi quesiti posti all'attenzione della Corte di giustizia nel rinvio pregiudiziale sfociato nel caso C-311/18, *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems*, sono ancora molti gli interrogativi aperti e gli aspetti incerti relativi alla disciplina del trasferimento di dati personali verso Stati terzi ed, in particolare, verso gli USA. La delicatezza della attesissima pronuncia dei giudici di Lussemburgo risiede non solo nell'importanza e complessità delle questioni poste, nel loro potenziale impatto economico nonché nel campo delle relazioni internazionali e nella determinazione, come si dirà meglio nell'ultimo paragrafo, della posizione dell'UE nel dibattito globale circa la tutela della riservatezza e della protezione dei dati, ma anche nella dimensione interna all'Unione stessa: si fa riferimento cioè agli effetti che tale decisione potrà avere sui numerosi rinvii pregiudiziali pendenti in materia di trasferimento di dati e di *data retention* per scopi securitari. Come si vuole preliminarmente sottolineare, il caso in analisi si intreccia inscindibilmente sia con il già citato ricorso di annullamento, promosso da *La Quadrature du Net* avverso la decisione di adeguatezza in materia di trasferimento dati UE-USA[63], sia con i casi *Privacy International*, *La Quadrature du Net* e *Ordre des Barreaux Francophones*[64], anch'essi fortemente attesi ed osservati con grande attenzione soprattutto dai governi nazionali, aventi ad oggetto la disciplina della conservazione e accesso ai metadati per scopi securitari, di cui si è accennato nel previo Capitolo e che verranno dettagliatamente analizzati nel Capitolo IV. A questo scenario fatto di rimandi e di riflessi continui rispetto a casi pendenti, è da aggiungersi un ulteriore profilo di complessità, derivante dalla connessione delle questioni in esame con la giurisprudenza della Corte Europea dei Diritti dell'Uomo: come si dirà nel prossimo paragrafo, le pronunce ed i principi in materia di tutela della privacy dinnanzi a pratiche di raccolta, conservazione e accesso massivi (c.d. *bulk interception*), delineati dai giudici di Strasburgo, sono stati infatti individuati dall'Avvocato generale nelle sue Conclusioni depositate il 19 dicembre 2019 come criterio di raffronto per determinare la 'sostanziale equivalenza' del livello di protezione garantito dallo Stato terzo laddove non risulti applicabile il diritto dell'UE. Il riferimento a tale copiosa ed articolata giurisprudenza è reso ancor più difficile dai quesiti ad oggi ancora aperti dinnanzi alla Corte EDU stessa, come dimostrato dai fondamentali e rilevanti casi *Big Brother Watch* e *Centrum for Rattvisa* in materia di *mass surveillance* al momento oggetto di ricorso innanzi alla Grande Camera e che verranno analizzati nel Capitolo V[65].

---

[62] Si fa riferimento alla sentenza *The Data Protection Commissioner c. Facebbok Ireland Limited e Maximillian Schrems*, 4 maggio 2018, n. 4809/2016. Tale sentenza si presenta come estremamente articolata e composta non solo da ben 152 pagine bensì anche da un Annex contenente studi circa la normativa americana, le tutele da essa predisposte e il funzionamento dei sistemi di sorveglianza. Per una analisi del contenuto della pronuncia della High Court irlandese, si rinvia a R. CABAZZI, *Irish High Court e Corte di giustizia europea: un nuovo dialogo sul trasferimento di dati da Facebook Ireland a Facebook Inc.*, in *MediaLaws*, 1, 2018, p. 473. Si noti che Facebook Ireland Limited ha impugnato tale decisione della High Court dinnanzi alla Corte Suprema irlandese, che ha però respinto le istanze della ricorrente con sentenza del 31 maggio 2019, *The Data Protection Commissioner c. Facebook Ireland Limited and maximillian Schrems*, Appeal n. 2018/68.

[63] Non a caso l'udienza di questo caso, fissata agli inizi di luglio del 2019, è stata poi sospesa dalla Corte di giustizia per concentrarsi prima sulla risoluzione del rinvio qui in esame e ad esso connesso.

[64] C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e al.*; Cause riunite C-511/18 e C-512/18, *La Quadrature du Net e altri c. Premier Ministre e al.*; C-520/18, *Ordre des Barreaux Francophones e al. c. Conseil des Ministres*.

[65] *Centrum For Rattvisa c. Svezia*, ricorso n. 35252/08, deciso il 19 giugno 2018 e *Big Brother Watch e altri c. Regno Unito*, ricorsi n. 58170/13, 62322/14 e 24960/15, decisi il 13 settembre 2018, attualmente entrambi al vaglio della Grande Camera, dal febbraio 2019.

Le molteplici connessioni con altri casi pendenti di cruciale importanza sia sul fronte esterno del trasferimento dei dati che su quello interno della *data retention*, rendono dunque le questioni sottoposte alla CGUE estremamente articolate e profonde: le lunghe e tutt'altro che semplici Conclusioni dell'Avvocato generale Saugmandsgaard Øe ne sono il riflesso.

3.3. – Le Conclusioni dell'Avvocato generale nel rinvio pregiudiziale c.d. Schrems II*: dalle* Standard Contractual Clauses *al* Privacy Shield

Come anticipato, i quesiti posti dal giudice irlandese nel rinvio pregiudiziale hanno ad oggetto svariati aspetti e sfaccettature della disciplina del trasferimento dei dati. Volendosi concentrare, in questa sede, sulle questioni di maggior rilievo e sulle più importanti posizioni espresse dall'Avvocato generale, pare utile suddividere le Conclusioni in tre 'sezioni': la prima riguardante l'ambito di applicazione del diritto dell'UE nei casi di successivo trattamento per finalità di sicurezza nazionale dei dati trasferiti; la seconda attinente alle SCCs e alla validità della relativa decisione ed infine, la terza, nella quale vengono affrontati gli interrogativi circa la validità della decisione di adeguatezza riguardante il trasferimento dati UE-USA e, dunque, del regime di Scudo per la privacy ad essa connesso.

Partendo dunque dalla prima questione, Saugmandsgaard Øe chiarisce sin dall'inizio un punto di estrema importanza: al fine di determinare l'applicabilità del diritto dell'UE alle operazioni di *data transfer* a scopo commerciale, l'unico elemento da considerare è l'attività all'interno della quale il flusso di dati ha luogo, mentre lo scopo alla base di qualsiasi ulteriore trattamento dei dati trasferiti, anche da parte di pubbliche autorità del Paese di destinazione, risulta del tutto irrilevante (par. 105). In ogni caso, è lo stesso art. 45, c. 2 del GDPR a precisare che, nell'ambito della valutazione di adeguatezza del livello di protezione offerto nello Stato ricevente, la Commissione deve valutare anche le normative straniere inerenti alla tutela della sicurezza nazionale, portando a ritenere dunque che tali previsioni e l'eventuale trattamento dei dati per tale finalità non porti per sé stessa ad una esclusione dell'applicabilità del diritto dell'UE e non faccia rientrare l'utilizzo dei dati in quelle eccezioni espresse dagli art. 3, co. 2 della superata Dir. 95/46/CE e art. 2, co. 2 del vigente GDPR[66]. L'Avvocato generale conclude comunque sul punto ritenendo che il trasferimento dei dati oggetto di esame nel caso sottoposto alla CGUE faccia indubbiamente parte dello svolgimento di una attività commerciale, essendo così ad esso applicabile il diritto dell'UE e le normative in materia di privacy e *data transfer*, indipendentemente da ogni successivo utilizzo o trattamento, per qualsivoglia finalità.

Spostandoci poi al secondo ordine di quesiti affrontati nelle Conclusioni e dunque addentrandoci nello specifico ambito delle SCCs, viene innanzitutto chiarito il livello di protezione che questi strumenti debbono garantire. Ecco che l'Avvocato generale esprime preliminarmente una valutazione di non poco conto e dalle significative conseguenze: anche le clausole contrattuali tipo, così come le decisioni di adeguatezza, debbono garantire un livello di protezione dei dati e della riservatezza 'sostanzialmente equivalente' a quello europeo; usando le parole di Saugmandsgaard Øe "è irrilevante che il trasferimento sia fondato su una decisione di adeguatezza o su garanzie offerte dal titolare del trattamento, in particolare mediante clausole contrattuali. I requisiti per la tutela dei diritti fondamentali garantiti dalla Carta non fanno alcuna distinzione a seconda della base giuridica su cui si fonda un determinato trasferimento" (par. 117). Quello che invece differisce è la modalità con la quale la continuità del livello di tutela viene mantenuta: mentre la decisione di adeguatezza accerta lo standard di protezione garantito in un preciso Stato terzo – anche solo sulla base delle condizioni stabilite in uno specifico accordo – e, come si è già avuto modo di sottolineare, con valenza generale per tutti i trasferimenti dati verso di esso,

[66] Tali disposizioni escludono dal proprio ambito di applicazione il trattamento di dati "effettuato per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione" (art. 2, c. 2, GDPR), quali appunto la protezione della sicurezza nazionale, competenza riservata agli Stati membri dall'art. 4, c. 2 del TUE.

nel caso delle SCCs è invece l''esportatore' di dati che, mediante la predisposizione e il rispetto delle clausole contrattuali, assicura standard di protezione adeguati. La *ratio* sottostante alla previsione delle clausole tipo quale meccanismo alternativo di trasferimento dati è quindi proprio quella di sopperire e compensare alla assenza di una decisione di adeguatezza generale: la decisione 2010/87 della Commissione fissa pertanto le clausole tipo inseribili nei *data transfer agreements* al fine di garantire la sostanziale equivalenza della tutela dei diritti alla riservatezza e protezione dei dati, indipendentemente dal Paese di destinazione e dunque dal livello di protezione da esso garantito. Quest'ultima valutazione dello specifico Stato e delle garanzie offerte dal suo ordinamento diviene però fondamentale in un momento successivo alla previsione delle SCCs nei contratti tra esportatore e importatore di dati: gli obblighi derivanti dall'ordinamento del Paese terzo ricevente, infatti, potrebbero entrare in conflitto con le condizioni stabilite nelle clausole tipo ed impedirne quindi il rispetto da parte del *data importer*. Chiamato a valutare la conformità della decisione 2010/87 ai diritti sanciti nella Carta di Nizza, l'Avvocato generale ritiene, sulla base di tale premessa, che la validità della disposizione dipenda dalla sussistenza di meccanismi in grado di garantire una sospensione o un divieto del trasferimento laddove venga accertato che le SCCs non possono essere rispettate nell'ordinamento straniero di destinazione. In altre parole, il fatto che tali clausole siano vincolanti unicamente per i soggetti sottoscriventi il contratto di trasferimento non ne comporta automaticamente l'invalidità: l'adeguato livello di protezione dei diritti fondamentali infatti è garantita, secondo l'Avvocato generale, dal fatto che le SCCs previste nella decisione della Commissione, unitamente ai poteri attribuiti alle autorità di controllo degli Stati membri, individuino in capo a queste ultime e ai *data exporter* (e ai loro responsabili del trattamento) un obbligo di controllo circa la concreta possibilità di attuazione e rispetto delle clausole nel contesto dell'ordinamento dello Stato ricevente e, in caso contrario, il vincolo di provvedere a che il trasferimento non abbia luogo. Viene pertanto attribuito un dovere in capo in primis all'esportatore e, in caso di inerzia di quest'ultimo, alle autorità nazionali di controllo, con un intervento quindi suppletivo, di svolgere verifiche, di grande delicatezza e complessità, per ogni specifico trasferimento dati e dunque caso per caso: una forte responsabilizzazione – anche dei soggetti privati – che ha destato in realtà non poche perplessità sul fronte della concreta realizzabilità ed efficacia. Pur ammettendo di non poter ignorare tali dubbi e preoccupazioni[67], espresse anche dal DPC irlandese, l'Avvocato generale considera la Decisione 2010/87 valida sulla base della valutazione dei poteri assegnati dal GDPR (art. 58, c. 2) alle autorità di controllo e dei singoli responsabili del trattamento; insomma l'impossibilità di applicare le garanzie stabilite nel contratto di trasferimento, a causa degli eventuali obblighi di senso differente imposti dall'ordinamento dello Stato ricevente, non implica di per se l'incompatibilità del meccanismo alternativo delle SCCs rispetto alla Carta di Nizza poiché ad una potenziale situazione di inadeguatezza delle tutele sopperisce l'obbligo di sospensione o divieto del flusso dei dati (par. 158).

Giunto ad una tale conclusione, Saugmandsgaard Øe non ritiene necessario provvedere all'analisi e soluzione degli ulteriori quesiti promossi dal giudice del rinvio: la pronuncia sulla validità della decisione della Commissione in materia di SCCs, infatti, consente alla High Court irlandese e al DPC di risolvere il ricorso promosso da Schrems, senza il bisogno di valutare anche la decisione di adeguatezza sul trasferimento dati UE-USA e i connessi principi sanciti nel *Privacy Shield*. Tale questione, sollevata indirettamente dalla Corte irlandese, comunque fosse affrontata, non andrebbe ad incidere sulle considerazioni sino ad ora svolte in materia di clausole contrattuali tipo; sulla base delle osservazioni previamente svolte, una analisi *in concreto* dell'incompatibilità degli obblighi stabiliti dall'ordinamento statunitense con le tutele inserite nelle SCCs è compito precipuo di ogni singolo *data exporter* e, in caso di inerzia di questo, delle autorità nazionali di controllo: la Corte di giustizia, ad

[67] Il DPC irlandese mette anche in luce il rischio che, attribuendo una tale responsabilità alle singole autorità nazionali, si possa venire a creare un panorama frammentario di soluzioni differenti da Stato a Stato. Sul punto l'Avvocato generale ritiene che "il rischio di frammentazione degli approcci seguiti dalle diverse autorità di controllo è intrinseco al sistema di sorveglianza decentralizzata auspicato dal legislatore" (par. 155).

opinione dell'Avvocato generale, non dovrebbe quindi sostituirsi al DPC irlandese ed imbarcarsi in una valutazione definita 'precipitosa' e 'prematura'. Sebbene non venga negato che la valutazione dei sistemi di sorveglianza posti in essere dalle autorità di intelligence statunitensi sia elemento rilevante per la soluzione del ricorso dell'attivista austriaco che il DPC irlandese sarà chiamato a risolvere, viene pertanto sconsigliato alla Corte di giustizia "di pronunciarsi su tali questioni al solo scopo di aiutare il DPC a trattare tale denuncia, mentre non è necessario rispondere alle stesse per consentire al giudice del rinvio di risolvere la controversia nel procedimento principale. Poiché il procedimento di cui all'articolo 267 del TFUE instaura un dialogo tra giudici, la Corte non è chiamata a fornire chiarimenti unicamente al fine di assistere un'autorità amministrativa nell'ambito di una procedura sottostante a tale controversia. (..) Inoltre, pronunciandosi sulle problematiche sopra descritte, la Corte perturberebbe, a mio avviso, il normale corso del procedimento che si dovrà svolgere dopo la pronuncia della sua sentenza nella presente causa. Nell'ambito di tale procedimento, spetterà al DPC trattare la denuncia del sig. Schrems tenendo conto della risposta che la Corte fornirà relativamente all'undicesima questione pregiudiziale" (par. 178-180), senza considerare il fatto che una tale valutazione è già oggetto di una azione di annullamento pendente dinnanzi alla medesima Corte nel caso *La Quadrature du Net*, sopra richiamato[68].

Nonostante questa premessa, Saugmandsgaard Øe reputa comunque necessario sviluppare alcune riflessioni sulla decisione 2016/1250, nel caso in cui i giudici di Lussemburgo decidano di distanziarsi dall'approccio suggerito. Pur precisando sin da subito il carattere non esaustivo delle proprie considerazioni (par. 196), nonché stabilendo che l'esistenza di una decisione di adeguatezza non impedisce alle autorità di controllo nazionali di sospendere o vietare il trasferimento di dati effettuato sulla base delle SCCs, differenziando e distaccando così le due valutazioni (par. 194), l'Avvocato generale svolge una lunga e dettagliata analisi del sistema statunitense e, in particolare, dei programmi di sorveglianza Prism e Upstream, del loro funzionamento e delle fonti normative che li regolano, utilizzando le informazioni fornite, tra gli altri, dal governo statunitense e dalla articolata ricostruzione della High Court irlandese. Anche in questa sezione però sorge preliminarmente una questione connessa all'ambito di applicazione del diritto dell'UE, che condiziona poi tutta la successiva analisi: se infatti l'adeguatezza del livello di protezione assicurata in uno Stato terzo deve essere determinata sulla base di un raffronto tra regole e pratiche attuative proprie dello Stato terzo e livello di protezione garantito nell'UE, bisogna chiedersi quale sia innanzitutto il criterio da impiegare al fine di determinare le attività di trattamento dei dati alle quali è applicabile il diritto dell'UE, per poi stabilire quale sia il parametro di confronto e dunque i principi da valutare per attestare l'adeguatezza della protezione fornita da un ordinamento straniero. Sul punto, l'Avvocato generale stabilisce una considerazione determinante e passibile di avere un impatto anche sugli altri casi pendenti dinnanzi alla Corte di giustizia e aventi ad oggetto la dimensione interna della disciplina della *data retention*: il diritto dell'UE e i requisiti stabiliti dalla sua giurisprudenza non si applica alle attività di trattamento (conservazione, raccolta, accesso) dei dati per scopi securitari unicamente poste in essere dallo Stato e da autorità pubbliche, senza cioè il coinvolgimento di soggetti privati. Si rientra invece nel campo d'azione del diritto dell'UE nei casi in cui, sempre per scopi di sicurezza nazionale, venga richiesto dalle autorità pubbliche l'intervento e la collaborazione dei fornitori privati di servizi di telecomunicazione: questo alla luce del coinvolgimento di attività di trattamento dei dati da parte di operatori commerciali ed indipendentemente dalla sussistenza o meno di un obbligo generale in capo agli stessi di conservazione dei dati[69]. Seguendo

[68] L'Avvocato generale suggerisce poi che, nel caso in cui il DPC, anche in sede di riesame del ricorso avanzato da Schrems, reputasse essenziale ai fini della risoluzione della controversia una pronuncia della Corte di giustizia in materia di validità della decisione di adeguatezza riguardante il trasferimento dati UE-USA, allora sarebbe compito del DPC provvedere al trasferimento del caso alla High Court affinché questa, come avvenuto nella controversia in esame, predisponga un rinvio ai giudici di Lussemburgo (par. 180).

[69] Questo approccio, accolto dall'Avvocato generale, è ciò che emerge dai casi *Tele2* e *Ministerio Fiscal*, mentre differisce da una previa interpretazione della stessa Corte nella pronuncia cause riunite C-317/04 e C-138/04,

questo ragionamento e considerando che anche la mera 'messa a disposizione' di dati e metadati su richiesta di autorità pubbliche rientra nella definizione di trattamento dei dati, rappresentando dunque una attività svolta dai *service providers*, una tale attività e le disposizioni che la regolano rientrano nell'ambito di applicazione del diritto dell'UE e sono pertanto vincolate al rispetto delle normative in materia di tutela della riservatezza e protezione dei dati[70]. Chiarito questo generale principio, con riferimento al sistema statunitense di raccolta, conservazione e trattamento, per scopi securitari, dei dati personali, anche – ma non solo – provenienti dall'UE, l'Avvocato generale opera una distinzione: fanno parte della seconda categoria di attività sopra descritte, implicanti un trattamento svolto anche da soggetti privati, la Sezione 702 del *Foreign Intelligence Surveillance Act* (FISA). Questa normativa consente infatti alla NSA di emanare ordini diretti agli operatori dei servizi di telecomunicazione stanziati negli USA di effettuare ricerche tra i dati in loro possesso – mediante appositi *selectors* o *search criteria* – e di mettere le informazioni così ottenute a disposizione della autorità statunitensi. Questi ordini vengono preventivamente vagliati e approvati da una apposita Corte, la US *Foreign Intelligence Surveillance Court* (FISC), che non è chiamata però a svolgere valutazioni circa l'esistenza di una '*probable cause*' e di fondati sospetti a motivazione della sorveglianza e della raccolta di dati richiesta. Tale tipologia di attività, implicando l'intervento e il trattamento di dati da parte di *service providers*, rientra nell'ambito di applicazione del diritto dell'UE: il livello di adeguatezza delle tutele predisposte rispetto a tali misure deve essere quindi valutato alla luce della Carta di Nizza, del GDPR e dei criteri stabiliti dalla giurisprudenza della Corte di giustizia in materia ed è pertanto nello standard di garanzia previsto dall'Unione che deve essere individuato il parametro di raffronto da impiegare nella valutazione di adeguatezza. Ebbene, applicando al caso concreto tali considerazioni, l'Avvocato generale rileva come anche la mera messa a disposizione dei dati, nonché le operazioni di filtraggio e la conservazione effettuate dai *data importer* su richiesta delle autorità statunitensi rappresentino intrusioni ed interferenze nel diritto alla privacy e alla protezione dei dati; esse tuttavia non rappresentano, diversamente da quanto stabilito nella prima sentenza *Schrems*, una lesione dell'essenza del diritto alla vita privata. L'accesso ai dati effettuato dalle agenzie di intelligence, infatti, non può essere considerato 'generalizzato', essendo anzi targettizzato grazie alle previe operazioni di 'filtraggio' dei dati effettuate sulla base di appositi *search criteria*. Non mancano però di essere rilevate talune criticità nel sistema di sorveglianza statunitense, individuate innanzitutto nella carenza di chiarezza e precisione nel delimitare i confini del ricorso a tali mezzi di invasione della sfera privata, nonché nella insufficienza delle garanzie esistenti, incapaci di prevenire il rischio di abusi da parte delle autorità pubbliche. Sotto tali profili quindi Saugmandsgaard Øe esprime dubbi quanto alla idoneità delle normative statunitensi che regolano tali programmi di *surveillance* di assicurare un adeguato livello di tutela ai dati trasferiti dall'UE.

Nella prima categoria di attività di sorveglianza, quella cioè che comprende operazioni di trattamento dei dati che non implicano un intervento o azione di soggetti privati, bensì unicamente delle autorità pubbliche, rientrano invece gli *Executive Order 12333*. Questi ultimi autorizzano la NSA ad accedere direttamente ai cavi posti sotto l'Oceano Atlantico e attraverso i quali i dati vengono trasferiti dall'UE agli USA. Tali *Orders* non sono sottoposti ad un previo controllo giudiziario e non sono previsti neppure rimedi giurisdizionali successivi attivabili dai soggetti sorvegliati. L'unico limite posto a tali misure è quello stabilito dalla già richiamata PPD-28. Non essendo riconducibili all'ambito di applicazione del diritto dell'UE, quest'ultimo non può fungere da parametro nella valutazione dell'adeguatezza delle tutele predisposte: l'Avvocato generale quindi individua nella Convenzione Europea dei Diritti

Parlamento europeo c. Consiglio e Commissione, già esaminata. Per questo interessante confronto, rilevante anche in materia di *data retention*, sul fronte interno, si rimanda ai paragrafi 214-225.

[70] "Concludo che, secondo il ragionamento adottato dalla Corte nelle sentenze Tele2 Sverige e Ministerio Fiscal, il RGPD e, di conseguenza, la Carta si applicano a una normativa nazionale che impone a un fornitore di servizi di comunicazioni elettroniche di offrire il proprio contributo alle autorità responsabili della sicurezza nazionale, mettendo loro a disposizione i dati, eventualmente dopo averli filtrati, anche indipendentemente da qualsiasi obbligo giuridico di conservazione di tali dati" (par. 223).

dell'Uomo e nella giurisprudenza della Corte sita in Strasburgo il criterio da considerare nell'esame di adeguatezza di tali operazioni. Sotto questo profilo, l'analisi dell'Avvocato generale si basa su due premesse interessanti: innanzitutto sul fatto che "gli standard derivanti dagli articoli 7, 8 e 47 della Carta [di Nizza], come interpretati da questa Corte, sono per certi versi più rigorosi di quelli derivanti dall'articolo 8 della CEDU, secondo l'interpretazione datane dalla Corte europea dei diritti dell'uomo" (par. 251) e, secondariamente, che dinnanzi alla Corte di Strasburgo sono pendenti alcuni rilevanti casi, già evidenziati sopra – *Big Brother Watch* e *Centrum for Rattvisa* – nei quali i giudici dovranno riconfermare o riconsiderare alcuni dei principi sanciti nella sua giurisprudenza più recente. Tenendo conto di tali aspetti quindi Saugmandsgaard Øe ritiene da un lato che l'*Order 12333* non sia supportato da idonee tutele – considerate alla luce di quel criterio che la Corte Europea dei Diritti dell'Uomo definisce '*necessity in a democratic society*' – in grado di assicurare un adeguato livello di garanzia dei diritti fondamentali alla riservatezza e protezione dei dati e, dall'altro, che non sia regolato da una legge realmente prevedibile e conoscibile (criterio di '*foreseeability*').

L'ordinamento statunitense, unitamente alle tutele introdotte dal regime *Privacy Shield* (quali ad esempio l'istituzione della figura dell'Ombudsperson) non risulta infine, alla luce dell'analisi dettagliata dell'Avvocato generale, predisporre strumenti di accesso alla giustizia e rimedi capaci di garantire il diritto sancito all'art. 47 Carta di Nizza in maniera sostanzialmente equivalente a quanto stabilito nell'UE[71].

Pur tenendo conto della necessità di una certa flessibilità delle operazioni di accertamento del livello di protezione garantito da uno Stato terzo e dunque della sua adeguatezza, che deve dunque essere in grado di considerare anche le diverse tradizioni giuridiche e culturali che caratterizzano altri ordinamenti, l'Avvocato generale afferma comunque che il criterio della adeguatezza implichi "– a meno privarlo di sostanza – che talune garanzie minime e taluni requisiti generali di protezione dei diritti fondamentali derivanti dalla Carta e dalla CEDU trovino il loro equivalente nell'ordinamento giuridico del paese terzo di destinazione" (par. 249). Ebbene, sulla base di tale posizione e al termine della sua complessa disamina, l'Avvocato generale esprime infine dubbi quanto alla conformità della decisione di adeguatezza 2016/1250 agli articoli 7, 8 e 47 della Carta di Nizza e all'art. 8 della Convenzione Europea dei Diritti dell'Uomo: ciò par farlo propendere per l'invalidità della decisione stessa e dell'accordo *Privacy Shield*, pur avendo suggerito alla Corte di giustizia di non spingersi ad affrontare tale analisi.

3.4. – Alcune riflessioni a margine del rinvio **Schrems II** *alla luce delle Conclusioni dell'Avvocato generale: il forte intreccio con i numerosi rinvii pregiudiziali pendenti e l'incerto destino del trasferimento di dati verso gli USA*

Dai molteplici aspetti trattati dall'Avvocato generale e dalla complessità delle questioni giuridiche analizzate, è semplice comprendere come la Corte di giustizia si trovi dinnanzi ad un compito arduo, dalle delicate implicazioni sia sul piano economico che delle relazioni internazionali. L'esito finale di questa pronuncia ed i suoi effetti sono naturalmente ancora del tutto imprevedibili e del resto i giudici di Lussemburgo, in questioni attinenti alla tutela della privacy e protezione dei dati, non sono nuovi a

[71] Viene in tal sede criticata anche l'assenza di qualsiasi meccanismo di notifica ai soggetti sottoposti a misure di sorveglianza, anche quando la messa a conoscenza non costituisce più un pericolo per il raggiungimento dell'obiettivo securitario: tale mancanza infatti renderebbe l'accesso ai rimedi eccessivamente difficile (par. 322). Quanto all'Ombudsperson, l'Avvocato generale dichiara di dubitare dell'abilità di tale meccanismo di compensare le carenze riscontrate nell'ordinamento statunitense.

distanziarsi dall'approccio più cauto dell'Avvocato generale[72]. Senza dubbio, se la decisione della CGUE dovesse seguire le indicazioni emerse dalle Conclusioni sopra esaminate, lo scenario potrebbe essere maggiormente favorevole per i *data exporter*, che in tal caso non vedrebbero intaccata la validità né delle SCCs indicate dalla Commissione né, con riferimento allo specifico flusso di dati con gli USA, dell'importante strumento della decisione di adeguatezza e del regime *Privacy Shield*. Il condizionale però è quanto mai d'obbligo. Anche in questa più vantaggiosa ipotesi, la situazione derivante rimarrebbe aperta ed indefinita, passibile dei più disparati epiloghi: non bisogna infatti sottovalutare il fatto che, seguendo il ragionamento di Saugmandsgaard Øe, sia rimessa nelle mani di ciascun responsabile del trattamento – e, in caso di sua inerzia, alle autorità di controllo nazionali – il compito di effettuare valutazioni caso per caso circa la possibilità concreta di rispettare le clausole contrattuali dinnanzi agli obblighi stabiliti dall'ordinamento dello Stato ricevente. Non è quindi scontato e neppure certo che i singoli soggetti e le autorità preposte a tale vaglio, con riferimento allo specifico regime di trasferimento posto alla loro attenzione, possano giungere a ritenere attuabili le SCCs, ben potendo propendere invece per una sospensione o divieto del flusso di dati stesso. Nel caso dal quale il rinvio pregiudiziale ha preso origine, ad esempio, la posizione fortemente critica espressa dal DPC irlandese al termine della propria indagine iniziale non sembra poter far tirare un sospiro di sollievo a Facebook, viste le numerose perplessità e preoccupazioni mostrate avverso le imposizioni derivanti dal sistema di sorveglianza statunitense e la loro compatibilità con il rispetto delle clausole contrattuali tipo inserite nell'accordo di trasferimento tra l'azienda irlandese e quella americana. Questa posizione dell'Avvocato generale apre dunque a molteplici scenari e alla possibilità che si addivenga a soluzioni differenti a seconda dei diversi approcci delle autorità di controllo degli Stati membri dinnanzi all'ordinamento degli Stati terzi 'riceventi', che potrebbe peraltro variare nel corso del tempo.

Gli interrogativi che sorgono alla luce di queste considerazioni sono quindi numerosi: è da chiedersi innanzitutto se e come i responsabili del trattamento abbiano le forze, le capacità e l'interesse ad effettuare controlli così rilevanti quanto delicati, che implicano anche la conoscenza dell'ordinamento e dei vincoli normativi vigenti in ogni Stato ricevente. Queste valutazioni rimandano inevitabilmente alle critiche e perplessità emerse con riferimento alla posizione della CGUE nella nota sentenza *Google Spain* in materia di diritto all'oblio nonché nella più recente sentenza *Glawischnig-Piesczek*, sul controllo dei contenuti online[73]: attribuire un ruolo 'para-costituzionale' a soggetti privati è veramente una strada percorribile, soprattutto quando interessi economici così rilevanti sono in gioco? Certamente, nel caso in esame, l'immobilismo dei *data exporter* può essere compensato dall'intervento delle autorità di controllo. Anche con riferimento a queste ultime però ci si domanda se esse siano dotate dei mezzi necessari per effettuare complesse e costanti valutazioni caso per caso, potenzialmente onerose sotto il profilo del tempo, sforzi e personale richiesti nonché particolarmente delicate per i risvolti economici che una sospensione del flusso di dati comporterebbe; ciò anche considerando lo squilibrio e le disomogeneità che potrebbero venirsi a creare tra Stati membri a seconda dell'attivismo e delle decisioni delle diverse autorità nazionali, che potrebbero in ultima istanza portare ad uno spostamento dei *server* delle aziende negli Stati nei quali le autorità di controllo sono meno efficienti o effettuano un vaglio meno rigido. L'attribuzione di così ampi margini d'azione a soggetti privati o autorità di controllo e una loro forte responsabilizzazione sembra scontare pertanto, ad una prima analisi, alcuni limiti e difficoltà pratiche sul piano della possibile concreta attuazione, tanto che non è mancato chi ha rinvenuto nella posizione espressa dall'Avvocato generale un "*a head in the sand approach*"[74]. Infine merita rilevare

[72] Per esempio, si rimanda alla nota sentenza *DRI* nella quale, nonostante l'Avvocato generale avesse suggerito di modulare l'efficacia temporale della dichiarazione di invalidità della DRD, il giudice di Lussemburgo aveva invece optato per un approccio più netto, ritenendo la normativa invalida sin dal momento della sua entrata in vigore.

[73] C-131/12, *Google Spain SL e Google Inc. c. Agencia Espanola de Proteccion de Datos e Mario Costeja Gonzalez*; C-18/18, *Eva Glawischnig-Piesczek c. Facebook Ireland Limited*.

[74] L. WOODS, *The AG Opinion in Schrems II: Facebook, national security and data protection law*, in *EU Law Analysis*, 21 dicembre 2019.

come in un tale contesto assumano un ruolo di centrale importanza, per quanto non menzionati nelle Conclusioni, l'attenzione e la vigilanza continue dimostrate dai comuni utenti di servizi digitali, al fine di segnalare ed attivare meccanismi di controllo in caso di inerzia dei *data exporter* e delle autorità nazionali preposte. È innegabile infatti che, dinnanzi alle difficoltà attuative sopra evidenziate, potrebbe sopperire – in parte – un pubblico di utenti attivo ed informato. Anche sotto questo profilo, se una maggiore sensibilizzazione e, per certi versi anche responsabilizzazione, dell'utente i cui dati vengono trasferiti fuori dai confini europei è di grande rilievo, è altrettanto vero però che si rendono alla base necessarie adeguate conoscenze e competenze in materia: solo una approfondita consapevolezza dei meccanismi di raccolta, conservazione, trattamento e trasferimento dei dati adottati dal soggetto cui li cediamo, nonché del sistema giuridico dello Stato ricevente e dell'esistenza di possibili obblighi in capo ai *data exporter* tali da intaccare la corretta attuazione e rispetto delle SSCs previste, potrebbe consentire al singolo utente di promuovere ricorsi per la tutela dei propri diritti. Come risulta evidente ciò risulta tutt'altro che semplice da realizzare.

Le difficoltà pratiche e la situazione confusa che ne potrebbe derivare inducono dunque ad una lettura che vada al di là della mera affermazione di validità della decisione 2010/87/UE da parte dell'Avvocato generale: come sottolineato da alcuni commentatori[75], l'approccio emerso dalle Conclusioni non può essere considerato una vittoria a tutto tondo di Facebook o delle posizioni del governo statunitense, ben potendosi al contrario rivelare una vittoria di Pirro, nella quale i benefici si mostrano in conclusione assai limitati rispetto ai rischi corsi. Non è un caso se lo stesso Maximillian Schrems si è dichiarato nel complesso soddisfatto delle considerazioni di Saugmandsgaard Øe che, è bene ricordarlo, ha finito col mostrare conclusivamente forti perplessità rispetto alla validità della decisione di adeguatezza e del relativo regime di Scudo per la privacy UE-USA, pur affrettandosi a precisare che le proprie considerazioni non hanno carattere di completezza. Con riferimento a tale aspetto, se la Corte dovesse decidere di non seguire il ragionamento ed i suggerimenti dell'Avvocato generale ed addentrarsi nella valutazione di questa decisione, potrebbe riproporsi nuovamente quella situazione di confusione ed incertezza già descritta per la fase post-*Schrems*: laddove l'invalidità fosse nuovamente dichiarata, la storia si ripeterebbe e si renderebbe necessaria una nuova complessa fase di ri-negoziazione di principi e regole che disciplinino il trasferimento dati verso gli USA, accompagnati da una nuova decisione di adeguatezza. D'altra parte le considerazioni dell'Avvocato generale sulla inadeguatezza del livello di protezione dei dati e della riservatezza garantito dall'ordinamento statunitense e dall'accordo *Privacy Shield* paiono in linea con le criticità e problematiche sin da subito rilevate da parte della dottrina e da talune autorità europee e che sono state più sopra richiamate[76].

Oltre a questi aspetti è importante poi rilevare come, nell'affrontare la questione relativa ai confini applicativi del diritto dell'UE in materie connesse alla sicurezza nazionale, Saugmandsgaard Øe abbia fornito una chiave di lettura di grande importanza, pur non discostandosi dal passato e soprattutto da quanto affermato nelle sue Conclusioni nel caso *Ministerio Fiscal* del 2018, che verrà analizzato nel Capitolo IV. La posizione della CGUE sul punto sarà quindi determinante anche per i casi pendenti, sopra individuati, riguardanti la fondamentale quanto problematica disciplina della *data retention* per scopi securitari; la decisione finale inoltre potrà chiarire il rapporto tra il diritto europeo e la giurisprudenza della Corte Europea dei Diritti dell'Uomo in questa materia: nel caso in cui venisse

[75] C. KUNER, *International data transfers, standard contractual clauses and the Privacy Shield: the AG Opinion in Schrems II*, in *European Law Blog*, 7 gennaio 2020.

[76] Oltre agli autori sopra richiamati (Vermeulen, Crespi, Sica, Mantelero, Terpan), si legga anche quanto affermato da Brkan secondo cui, ponendo particolare attenzione al concetto di targetizzazione individuato come requisito da rispettare per azionare la Sezione 702 FISA, "in the past, the requirement of 'targeting' did not seem to prevent mass surveillance or blanket collection of content data which raised not only academic concerns, but also led to numerous challenges before U.S. Courts against this section of FISA", M. BRKAN, *The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning,* in *German Law Journal*, 20, 2019, p. 876.

confermata la funzione 'suppletiva' di quest'ultima rispetto alle attività di trattamento dei dati che fuoriescono dall'ambito di applicazione del diritto dell'UE, come suggerito dall'Avvocato generale, sarà poi interessante vedere se, alla luce delle altrettanto attese decisioni dei giudici di Strasburgo – in particolare nei casi *Big Brother Watch* e *Centrum for Rattvisa* – verrà confermata una interpretazione dei principi di necessità e proporzionalità meno stringente da parte della Corte Europea dei Diritti dell'Uomo rispetto alla Corte di giustizia – come sottolineato peraltro dall'Avvocato generale[77] – o se si potrà individuare un maggiore allineamento tra la giurisprudenza delle due Corti europee (sul punto si rimanda più ampiamente al Capitolo V).

In attesa degli importanti sviluppi giurisprudenziali sopra esaminati, ciò che fin da ora può essere rilevato e che emerge da questo importante rinvio pregiudiziale è come la posizione dei giudici irlandesi e, sotto determinati profili anche dell'Avvocato generale, rispetto all'adeguatezza delle salvaguardie garantite negli USA. sia in contrasto non solo con quanto stabilito dalla Commissione nella sua decisione di adeguatezza fondata sull'Accordo *Privacy Shield*, ma anche con quanto successivamente riaffermato dalla stessa Commissione nella *Relazione sul terzo riesame annuale del funzionamento dello Scudo UE-USA per la privacy* (COM(2019)495 final, del 23 ottobre 2019) nel quale viene sostanzialmente confermata l'adeguatezza delle tutele poste in campo dagli Stati Uniti e, nel complesso, la corretta ed efficace attuazione delle misure inserite nel *Privacy Shield*, pur con alcune criticità[78].

La complessità della questione e le incertezze circa lo standard di protezione disposto dall'ordinamento americano e dallo Scudo per la privacy, risultano chiare anche nella Risoluzione adottata dal Parlamento europeo nel 2018[79], che ha messo in luce molti dei punti problematici ancora aperti nell'ambito della disciplina del trasferimento dati UE-USA[80]; primo fra tutti il fatto che la ri-autorizzazione della controversa sezione 702 del FISA sia stata approvata dal Congresso statunitense nel 2018 senza considerare né i rilievi espressi dalla Commissione nelle sue Relazioni[81], né le

[77] Si rimanda sul punto anche a E. CELESTE, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, op. cit.; V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, Working Papers HSE, 2019, 1 ss.

[78] Ad esempio e solo brevemente, viene rilevata la carenza di efficaci controlli circa l'effettivo rispetto delle condizioni fissate nel *Privacy Shield* da parte delle compagnie che ne autocertificano la conformità (c.d. *false claims*, par. 2.1, p. 4), nonché la problematicità della concessione, da parte del *Department of Commerce*, di un "grace period" per le aziende che non abbiano ancora concluso il procedimento di ri-certificazione: durante questo periodo la compagnia rimane cioè nella lista delle aziende che rispettano i criteri definiti nel *Privacy Shield* ed è comunque autorizzata a ricevere dati provenienti dall'UE (par. 2.1, p. 3-4).

[79] Risoluzione del Parlamento europeo del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo Scudo UE-USA per la privacy (2018/2645 (RSP)).

[80] Alcuni profili critici indicati dal Parlamento sono, innanzitutto, individuati nella mancata estensione anche alla Sezione 702 FISA delle tutele disposte nel PPD-28 (par. 20-22), nonché nell'assenza di una chiara e specifica definizione di "sicurezza nazionale" nel meccanismo *Privacy Shield* che sia in grado di circoscrivere l'intervento delle autorità pubbliche e agenzie di intelligence americane (par. 20); vengono inoltre sottolineati "i persistenti ostacoli in materia di ricorso per i cittadini non statunitensi soggetti a una misura di sorveglianza basata sulla sezione 702 del FISA o sull'ordinanza esecutiva 12333 a causa dei requisiti procedurali di «legittimazione ad agire» quali attualmente interpretati dai tribunali statunitensi, in modo da consentire ai cittadini non statunitensi di adire i tribunali statunitensi contro le decisioni che li riguardano" (par. 25). Interessante è anche l'attento richiamo non solo al *Clarifying Overseas Use of Data* (c.d. CLOUD) *Act*, approvato il 23 marzo 2018 dal Congresso US, con cui viene concesso alle autorità di *law enforcement* di accedere più facilmente ai contenuti delle comunicazioni, anche nel caso in cui esse siano conservate al di fuori dai confini degli USA (lett. Q), ma anche al caso *Cambridge Analytica*, evidenziando come le gravi violazioni dei diritti alla privacy e alla protezione dei dati fossero state perpetrate da aziende certificate sulla base del sistema *Privacy Shield* e che avevano dunque beneficiato della Decisione di adeguatezza della Commissione quale base giuridica per il trasferimento e trattamento di dati personali provenienti dall'UE (lett. R). Al fine di meglio comprendere tale ultimo riferimento del Parlamento, si legga più ampiamente: E. ASSANTE, *Cosa ci può insegnare il caso Cambridge Analytica*, in *Federalismi.it*, 9, 2018; D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Anlaytica"*, in *Federalismi.it*, 20, 2018.

[81] Tra cui: COMMISSIONE EUROPEA, *Relazione della Commissione sul primo riesame annuale del funzionamento dello scudo UE-USA per la privacy*, COM(2017)611 final, 18 ottobre 2017; COMMISSIONE EUROPEA, *Relazione*

preoccupazioni manifestate nei pareri elaborati dal Gruppo di lavoro Art. 29[82]. Tutte questi richiami rimasti inascoltati dal Governo e dal Congresso americano, hanno indotto il Parlamento europeo nella richiamata Risoluzione a contestare il mancato avvio da parte della Commissione di nuovi negoziati – o quanto meno discussioni – circa il sistema di trasferimento dati con le autorità americane (par. 31-32), nonché a chiedere alla Commissione stessa di attivare tutte le misure necessarie affinché il *Privacy Shield* sia realmente e totalmente coerente e rispettoso dei principi affermati nel GDPR, nella Carta di Nizza e nella giurisprudenza della CGUE.

Pur rimandando al paragrafo finale di questo Capitolo per una riflessione generale in merito alla complessa questione del trasferimento dati oltre i confini dell'UE e alla efficacia dei criteri e strumenti adoperati dall'Unione stessa al fine di garantire un adeguato livello di protezione dei dati anche al di fuori del proprio territorio, è importante sottolineare preliminarmente come la storica decisione nel caso *Schrems* abbia dato vita ad un forte dibattito, ancora del tutto aperto, come i rinvii pregiudiziali pendenti sopra illustrati dimostrano; tale discussione vede in contrapposizione da un lato giudici nazionali (come la High Court irlandese), autorità indipendenti quali il Gruppo di lavoro Art. 29 e Istituzioni dell'UE quali il Parlamento, e dall'altro aziende e autorità pubbliche statunitensi insieme alla Commissione. Quest'ultima ha adottato una posizione certamente meno rigida quanto alla valutazione del criterio di adeguatezza, mediando tra esigenze di mercato e tutela dei diritti e giungendo a fissare nei principi delineati nel *Privacy Shield* "un compromesso volto a far fronte al vuoto creatosi in seguito all'annullamento della decisione della Commissione sull'adeguatezza del programma *Safe Harbour*"[83].

4. – Il trasferimento di PNR oltre i confini dell'UE: tra esigenze securitarie e garanzia della riservatezza e protezione dei dati

4.1. – Potenzialità e rischi derivanti dalla raccolta, conservazione, analisi e trattamento dei PNR: gli obblighi imposti agli operatori aerei da Stati terzi si scontrano con la necessità di garanzia degli standard di protezione dei dati stabiliti nell'UE

Il percorso giurisprudenziale della CGUE in materia di trasferimento dati verso Paesi terzi non risulta incentrato unicamente sui dati (contenuto e metadati) derivanti dalle comunicazioni elettroniche e trasferiti da soggetti privati al di fuori dei confini dell'UE; l'intervento dei giudici di Lussemburgo in materia, al contrario, vede una ulteriore importante tappa nel rilevante Parere avente ad oggetto la bozza di accordo tra UE e Canada riguardante la disciplina del trasferimento di Passenger Name Record (ovvero il codice di prenotazione dei passeggeri aviotrasportati, c.d. PNR)[84].

---

della Commissione sul secondo riesame annuale del funzionamento dello Scudo UE-USA per la privacy, COM(2018)860 final, 19 dicembre 2018.

[82] Tra cui si legga: GRUPPO DI LAVORO ART. 29, *EU-US Privacy Shield – First Annual Joint Review*, 17/EN WP 255, 28 novembre 2017 (disponibile solo in lingua inglese).

[83] A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, op. cit., p. 248. Lo stesso autore, nel citato contributo, ipotizza – in un momento antecedente alla adozione della Decisione di adeguatezza della Commissione sulla base del sistema *Privacy Shield* – che un nuovo accordo, certamente contestabile e sottoponibile al vaglio della CGUE, potrebbe essere letto "nell'ottica di una strategia dilatoria", portando la Commissione "a guadagnare un paio di anni e, considerata anche la congiuntura politica statunitense (elezioni presidenziali) e le trattative in corso sul fronte della Transatlantic Trade and Investment Partnership, questo potrebbe essere un tempo utile per conseguire una riforma dell'esistente quadro normativo statunitense in materia di *data protection* e di poteri delle forze di intelligence", p. 248.

[84] Può essere utile riportare la definizione fornita dalla *International Civil Aviation Organization* (ICAO), nelle sue *Guidelines on the PNR data* (2010): "A Passenger Name Record (PNR), in the air transport industry, is the generic name given to records created by aircraft operators or their authorized agents for each journey booked by or on behalf of any passenger. The data are used by operators for their own commercial and operational purposes in providing air transportation services". La definizione del legislatore europeo invece stabilisce che le

Gli operatori aerei, nel normale e corretto svolgimento delle proprie attività ed erogazione dei servizi, raccolgono e conservano nei sistemi automatizzati di controllo delle partenze un ampio numero di dati personali (i PNR appunto), rilasciati dai passeggeri al momento della prenotazione[85]. Soprattutto a seguito degli attentati del 2001 che hanno messo in luce la necessità di garantire maggiori controlli sui trasporti aerei[86], questa tipologia di informazioni ha assunto un'enorme importanza nel campo della prevenzione e della lotta al crimine grave, dal terrorismo alle attività criminali di natura transfrontaliera (tratta di esseri umani, traffico di sostanze stupefacenti, etc); l'utilizzo dei PNR è divenuto infatti strumento essenziale per effettuare, mediante lo sviluppo della tecnologia e l'implementazione di tecniche di intelligenza artificiale, analisi sistematiche dei dati di passeggeri di voli internazionali, prima dell'arrivo degli stessi nel luogo di destinazione: il grande valore aggiunto dell'esaminazione aggregata dei codici di prenotazione aerea deriva proprio dal fatto di consentire "l'identificazione di persone mai sospettate di reati di terrorismo o di reati gravi prima di tale valutazione, per cui è opportuno che le autorità competenti procedano a ulteriori verifiche. Usando i dati PNR è possibile far fronte alla minaccia di reati di terrorismo e reati gravi da una prospettiva diversa rispetto al trattamento di altre categorie di dati personali"[87]. In altre parole, ciò che viene reso possibile mediante il trasferimento e dunque la disponibilità dei PNR di tutti i passeggeri di voli aerei è da rilevarsi non solo in una analisi dei dati *ex post*, nel contesto cioè di una indagine già avviata, bensì anche una valutazione preventiva dei rischi di commissione dei reati, effettuata *ex ante*, adottando un approccio proattivo che permette un

---

informazioni relative al viaggio di ciascun passeggero comprendono "i dati necessari per il trattamento e il controllo delle prenotazioni a cura dei vettori aerei e di prenotazione interessati per ogni volo prenotato da qualunque persona o per suo conto, siano esse registrate in sistemi di prenotazione, in sistemi di controllo delle partenze utilizzato per la registrazione dei passeggeri sui voli, o in altri sistemi equivalenti con le stesse funzionalità" (Direttiva (UE) 2016/681 del Parlamento Europeo e del Consiglio Europeo del 27 aprile 2016 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, art. 3). Questi dati sono raccolti dalla compagnia aerea e da essa conservati nel *Computer Reservation System* (CRS), allo scopo di fornire ed erogare il servizio di volo. Come si avrà modo di vedere, i PNR contengono un elevato numero di informazioni: indirizzo, dati personali identificativi, forma di pagamento, itinerario di viaggio, numero di biglietto, informazioni relative al bagaglio ma anche alla frequenza dei viaggi (*frequent flyer information*); i PNR possono inoltre contenere o rivelare informazioni sensibili: esprimendo preferenze su un pasto o richiedendo la presenza di particolari strumenti o apparecchiature mediche a bordo (*Special Service Request* o *Special Service Information*), vengono indirettamente fornite informazioni circa la religione o lo stato di salute del passeggero che rientrano appunto nella categoria di dati sensibili o 'categoria particolare di dati personali', secondo la denominazione utilizzata dal GDPR.

[85] L'origine dell'utilizzo dei PNR per scopi di indagine e prevenzione di reati risale al 1996, con la creazione di un Sistema Computerizzato per Supportare il Monitoraggio del Passeggero (c.d. *Computer Assisted Passenger Pre-Screening System*, CAPPS). Per maggiori approfondimenti sulla storia e sul funzionamento dei sistemi di controllo basati sull'utilizzo dei PNR, si rimanda a: G. A. CANNETTI, *Passenger Name Records tra istanze di sicurezza globale e tutela dei dati personali*, in *I quaderni europei. Il diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, 63, 2014.

[86] "Gli attentati terroristici del 2001 negli Stati Uniti, il fallito attentato terroristico dell'agosto 2006 con cui si volevano far esplodere alcuni aerei in volo dal Regno Unito verso gli Stati Uniti e il tentativo di attentato su un volo da Amsterdam verso Detroit nel dicembre 2009 dimostrano che i terroristi sono in grado di preparare attentati contro voli internazionali in qualunque paese. Benché nel 2009 il fenomeno sia diminuito nell'UE, secondo la relazione 2010 di Europol sulla situazione e sulle tendenze del terrorismo nell'UE la minaccia terroristica rimane grave e reale. Poiché la maggior parte delle attività terroristiche ha carattere transnazionale e comporta viaggi internazionali, anche verso i campi di addestramento al di fuori dell'UE, è necessaria una maggior cooperazione tra le autorità di contrasto", Considerando (1), Proposta di Direttiva del Parlamento Europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi COM/2011/0032. L'importanza di un sistematico controllo dei voli internazionali è nuovamente tornata al centro del dibattito politico e normativo con l'affermarsi del sedicente Stato Islamico (IS): l'analisi dei PNR di cittadini europei che abbiano volato da e per la Siria o l'Iraq può consentire di identificare soggetti che abbiano raggiunto in quei luoghi campi di addestramento terroristici e che siano poi rientrati nell'UE per pianificare e attuare attentati.

[87] Dir. (UE) 2016/681, Considerando (7).

utilizzo in tempo reale dei dati, fornendo informazioni sui percorsi di viaggio di ogni passeggero ma anche creando connessioni tra una persona sconosciuta alle forze dell'ordine e un criminale noto[88].

Sulla base di queste enormi potenzialità, del tutto simili a quelle prima analizzate in materia di metadati derivanti dalle telecomunicazioni elettroniche, molti Stati hanno deciso di adottare normative che obbligano gli operatori aerei a fornire, a specifiche autorità di *law enforcement* o doganali, i PNR dei passeggeri per voli con destinazione o partenza o anche solo sorvolanti il proprio territorio nazionale. Gli Stati Uniti si sono per primi muniti di tale tipologia di legislazione, immediatamente dopo gli attacchi terroristici dell'11 settembre 2001[89], e sono stati seguiti in breve tempo da Regno Unito, Australia e Canada[90].

Come però già rilevato in merito alla conservazione di metadati relativi alle telecomunicazioni, anche- l'utilizzo dei PNR, pur per scopi securitari, non è privo di implicazioni negative per i diritti fondamentali: dopo la ricostruzione svolta nei Capitoli e nei paragrafi precedenti, è facile cogliere l'intrusività nella sfera privata rappresentata da operazioni di raccolta e accesso a simili dati, che hanno un impatto significativo sui diritti alla riservatezza e alla protezione dei dati. Sebbene infatti si possa pensare che i PNR, presi isolatamente, non siano in grado di ingerire nella vita privata del passeggero, anche in questo caso e come già evidenziato con riferimento ai metadati, una loro lettura aggregata e complessiva consente di rivelare "informazioni di viaggio complete, abitudini di viaggio, relazioni esistenti tra due o più persone nonché informazioni sulla situazione finanziaria dei passeggeri aerei, sulle loro abitudini alimentari o sul loro stato di salute, e potrebbero persino fornire informazioni sensibili su tali passeggeri" (par. 128, *Parere 1/15*). Vista tale capacità di ricostruire la vita di un soggetto, anche in questo ambito si ripropone dunque la sfida di predisporre norme sul trasferimento di tali informazioni capaci di prevedere specifici limiti alle operazioni di raccolta, conservazione e accesso ai dati PNR per finalità di prevenzione, accertamento e indagine, nonché di includere idonee tutele al fine di garantire il

[88] Usando le parole dell'Avvocato generale Paolo Mengozzi nelle sue Conclusioni a margine del *Parere 1/15*, che verrà poi approfonditamente analizzato, grazie all'analisi dei dati PNR si rende possibile l'utilizzo di "metodi relativi all'identificazione di passeggeri fino a quel momento sconosciuti ai servizi di polizia, in base a modelli comportamentali «preoccupanti» o che presentano un «interesse»" (Par. 164); in sostanza, mediante l'uso di sistemi di intelligenza artificiale e di analisi algoritmica, in grado di effettuare ricerche su una vastissima quantità di informazioni, vengono esaminati i dati forniti dai passeggeri alla luce di specifici criteri di valutazione prestabiliti dalle autorità di controllo: così facendo, si può giungere alla identificazione di sospetti "non noti" "ed effettuare confronti con varie banche dati di persone e oggetti ricercati", come rilevato nella Proposta di Direttiva sull'uso dei PNR a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi, Relazione della Commissione, 2011/0023 (COD) C7-0039/11). Sempre in questo documento, che pure è riferito alla successivamente adottata ed attualmente in vigore Direttiva PNR, di cui poi si dirà più ampiamente, viene affermato: "L'analisi dei dati PNR può dare indicazioni sulle rotte più usate dalla tratta di esseri umani o per il traffico di stupefacenti, che potranno poi essere incluse tra i criteri di valutazione. (..) Grazie alle informazioni sulla carta di credito contenute nei dati PNR le autorità di contrasto possono identificare e provare collegamenti tra una determinata persona e un criminale o un'organizzazione criminale noti. Uno Stato membro ha dato l'esempio di una vasta rete di tratta di esseri umani e traffico di stupefacenti in varie destinazioni europee facendoli inghiottire a persone a loro volta vittime della tratta. I criminali sono stati identificati perché dai dati PNR è emerso che compravano i biglietti con carte di credito rubate", p. 5. Merita tuttavia sottolineare sin da ora come la capacità dei sistemi di analisi dei PNR di contribuire alla prevenzione e lotta di crimini gravi non debba far pensare ad una loro indiscussa efficacia: in realtà proprio sul punto della utilità ed efficienza di tali sistemi di raccolta e controllo sono al momento aperti ampi dibattiti, di cui si darà rilievo nel prosieguo di questo Capitolo.

[89] US Aviation and Transportation Security Act of 2001, Public law 107-71, 19 novembre 2001.

[90] "The Australian Department of Immigration and Border Protection is responsible for undertaking the risk assessment and clearance of all passengers arriving into and departing Australia. As part of its intelligence led approach to Australia's border protection, under section 64af Customs Act 1901, the Department is authorized to access PNR data from all international air service operators flying to and from Australia. In Canada since 2005 the Canadian Border Services Agency has collected PNR data under section 107.1, Customs Act 1985 with data protection of passengers' information provided under the Protection of Passenger Information Regulations 2005", D. LOWE, *The European Union's Passenger Name Record Data Directive 2016/681: is it fit for purpose?*, in *International Criminal Law Review*, 16, 2016, p. 859.

rispetto della riservatezza e la protezione dei dati: in altre parole, una regolamentazione che abbia ad oggetto lo scambio di PNR tra operatori aerei e autorità pubbliche nazionali per scopi securitari dovrà stabilire un corretto bilanciamento tra esigenze di controllo e prevenzione del crimine grave da un lato e tutela dei diritti fondamentali dall'altro. La complessità di una tale disciplina inoltre è ulteriormente accresciuta dal carattere transfrontaliero del flusso di dati PNR e dal differente standard di salvaguardia della privacy e *data protection* offerto dagli Stati terzi riceventi.

Tali rilevanti problematiche sono del resto risultate evidenti sin dalla già richiamata prima normativa in materia di PNR adottata dagli USA: tale disposizione prevedeva l'obbligo in capo ai vettori aerei operanti viaggi da e per gli USA, di fornire ad apposite autorità[91] i PNR dei propri passeggeri, dunque anche di quelli relativi a voli da e per l'UE. Tale imposizione risultava in netta incompatibilità con la normativa europea, in particolare con quanto stabilito dall'allora Dir. 95/46/CE, che imponeva, come già ampiamente rilevato nei precedenti paragrafi, il divieto generale di trasferimento di dati provenienti dall'UE se non in presenza di una decisione di adeguatezza (o altre misure alternative di cui agli artt. 25 e ss.). Non essendo presente a quel tempo nessuna decisione di quel tipo né alcun accordo adottato dalla Commissione e specificamente riferito al trasferimento di PNR negli USA, i vettori aerei si erano dunque trovati a dover affrontare un problema di estrema complessità, dovendo scegliere se rispettare la legislazione degli USA, violando il divieto di trasferimento dati stabilito a livello dell'UE o, viceversa, rifiutare di trasmettere i dati alle autorità americane rischiando di perdere le proprie rotte da e verso gli Stati Uniti[92]. Di fronte a questa situazione così problematica, diventava dunque sempre più urgente il raggiungimento di un accordo USA-UE in materia di PNR che stabilisse condizioni e tutele specifiche per i dati trasferiti oltreoceano, in grado di garantire un livello adeguato di protezione e di permettere l'adozione di una decisione di adeguatezza da parte della Commissione (o dai singoli Stati Membri, cui la Direttiva all'epoca attribuiva tale facoltà)[93].

Da questa esigenza ha dunque avuto origine il primo accordo USA-UE in materia di PNR, sulla base del quale la Commissione aveva adottato la decisione di esecuzione 2004/535/CE del 14 maggio 2004[94]. Tale disposizione non ha avuto tuttavia vita facile, a dimostrazione della complessità delle sfide legate alla regolamentazione di questo delicato ambito e dei molteplici dubbi relativi alla conformità al diritto dell'UE che questa tipologia di accordi sollevava e tutt'ora solleva. Il 30 maggio 2006, infatti, la CGUE, nella causa C-317/04 e C-138/04 *Parlamento europeo c. Consiglio e Commissione*, ha annullato la richiamata decisione di adeguatezza; in questo caso tuttavia, diversamente da quanto avvenuto nel più recente Parere, i giudici non si erano addentrati nella valutazione del contenuto delle previsioni

[91] Individuate, secondo quanto disposto dall'Homeland Security Act of 2002, Public Law 107-29 del 25 novembre 2002, nel *Department of Homeland Security* (DHS) e nel *US Customs and Border Protection* (CBP).

[92] A. VEDASCHI, G. M. NOBERASCO, *From DRD to PRN: looking for a new balance between privacy and security*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and trans-Atlantic relations*, Bloomsbury, 2015.

[93] In realtà sussiste ancora una certa confusione e dibattito circa la necessità di una decisione di adeguatezza laddove vi sia già la presenza di un accordo internazionale relativo e disciplinante il trasferimento di dati tra UE e Stato terzo. Questa mancanza di chiarezza emerge anche nel *Parere 1/15* in materia di trasferimento di PNR: mentre l'Avvocato generale infatti afferma che "l'oggetto dell'accordo previsto non può essere principalmente assimilato a una decisione di adeguatezza" (par. 93), l'art. 5 della bozza di accordo stesso fa espressamente riferimento alla garanzia offerta dalle sue disposizioni di un livello adeguato di protezione. Come evidenziato anche da Kuner, "The relationship between adequacy decisions and international agreements as a legal basis for data transfers requires clarification by the Court", C. KUNER, *International agreements, data protection and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, in *Common Market Law Review*, 3, 2018, p. 21.

[94] COMMISSIONE EUROPEA, *Decisione relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States' Bureau of Customs and Border Protection*, 2004/535/CE, 14 maggio 2004. Il 17 maggio 2004 il Consiglio ha quindi adottato la decisione 2004/496/CE di approvazione dell'accordo negoziato dalla Commissione in materia di trasferimento di PNR tra UE e USA.

normative (dunque della necessità e proporzionalità delle misure adottate): al contrario, è risultata determinante ai fini della risoluzione del caso, ancor prima di giungere a considerazioni di merito, la carenza di una corretta base giuridica[95]. Partendo da questo presupposto, i giudici di Lussemburgo non hanno proceduto oltre nella propria analisi: non troviamo pertanto in questa decisione indicazioni o suggerimenti contenutistici per la conclusione di ulteriori accordi, che sarebbero stati certamente utili per la Commissione nelle future operazioni di negoziazione con Stati terzi o nelle operazioni di valutazione dell'adeguatezza. Si dovrà quindi attendere il *Parere 1/15* per un'analisi 'sostanziale' della conformità di un accordo in materia di PNR con il diritto dell'UE ed in particolare con la Carta di Nizza.

[95] Pur non essendo questa la sede per dilungarci su tale discussa pronuncia, il tema affrontato e risolto in una breve e sintetica decisione della Corte è utile per sviluppare alcune ulteriori riflessioni circa l'evoluzione apportata dal Trattato in Lisbona – anche – in materia di PNR. Nel caso in esame, che è già stato oggetto di analisi nel Capitolo II, i giudici di Lussemburgo hanno considerato la Decisione della Commissione erroneamente fondata sull'art. 95 CE: l'atto sottoposto a scrutinio, secondo la CGUE, non aveva ad oggetto un trattamento dei dati volto alla prestazione di un servizio bensì un trattamento avente quale oggetto la pubblica sicurezza e le attività dello Stato terzo in materia di diritto penale. Ai sensi dell'art. 3, par. 2, la Direttiva 95/46 precisava che sono esclusi dal proprio ambito di applicazione i dati correlati allo svolgimento di attività proprie degli Stati o delle autorità statali estranee ai settori di attività dei singoli. Ne derivava quindi che non solo la Direttiva madre non poteva essere applicata ma che, conseguentemente, l'art. 95 CE non risultava costituire base giuridica corretta della Decisione: essa, infatti, "non avrebbe né per oggetto né per contenuto l'instaurazione e il funzionamento del mercato interno contribuendo all'eliminazione di ostacoli alla libera prestazione dei servizi e non conterrebbe disposizioni volte alla realizzazione di tale scopo. Infatti, la sua finalità sarebbe piuttosto quella di legittimare il trattamento di dati personali imposto dalla legislazione statunitense. Del resto, l'art. 95 CE non potrebbe costituire il fondamento della competenza della Comunità a concludere l'accordo, giacché questo riguarda trattamenti di dati esclusi dall'ambito di applicazione della Direttiva" (par. 63). La Corte dunque concludeva sbrigativamente affermando che la Comunità europea non aveva competenza per concludere l'accordo, che avrebbe dovuto quindi essere fondato sul Terzo Pilastro (quello di cooperazione di polizia e giudiziaria in materia penale) anziché sul Primo. Le maggiori critiche avanzate dalla dottrina a tale sentenza erano legate al fatto che stabilendo una distinzione tra raccolta di dati da parte dei soggetto privati (vettori aerei) ed utilizzo (accesso e trattamento) successivo di tali informazioni da parte di autorità di *law enforcement* per scopi securitari, quest'ultimo indicato come vera finalità dell'accordo in oggetto, la Corte giungeva ad escludere di fatto la materia del trasferimento dei dati verso Stati terzi per obiettivi securitari dall'ambito di applicazione della Dir. 95/46/CE; così facendo le Istituzioni europee in sede negoziazione con il Paese terzo avrebbero quindi potuto approvare un accordo senza dover in alcun modo tenere in considerazione i principi e le disposizioni dell'UE in materia di protezione dei dati. Tale decisione inoltre pone alcuni dubbi e perplessità rispetto alla successiva sentenza C-301/06 vertente, come si è visto, sulla correttezza della base giuridica della DRD, esaminata nel Capitolo II: in quel caso infatti, lo si ricorda, il governo irlandese aveva proprio presentato ricorso di annullamento basandosi sul ragionamento della CGUE nella sentenza qui analizzata, la cui distinzione tra raccolta da parte di soggetti privati e successivo accesso da parte di autorità pubbliche ben poteva essere riproposta con riferimento alla DRD, facendo giungere alla conclusione che anche tale Direttiva avrebbe dovuto essere adottata sulla base del Terzo Pilastro. La CGUE invece, sorprendentemente, come già ampiamente visto, ha ritenuto corretta la base giuridica della DRD individuata nell'art. 95 CE (sul punto, oltre a rimandare a quanto già scritto nel precedente Capitolo, si legga: F. MARIATTE, *La sécurité intérieure des États-Unis ne relève pas des compétences externes des Communautés*, in *Révue Europe*, 7, 2006, étude 8). Questo interessante punto, relativo alla distinzione tra i momenti di raccolta e di accesso e conseguentemente all'ambito di applicazione del diritto dell'UE, ripropone dunque quelle riflessioni già avanzate nella parte inerente alle vicende giudiziarie della DRD e che rimangono ancora ampiamente discusse, mentre la specifica problematica attinente alla divisione in Pilastri e dunque alla corretta individuazione della base giuridica di atti, quale quello esaminato, che per natura risultavano inter-Pilastro, sia stata superata dall'entrata in vigore del Trattato di Lisbona (incidendo anche sul fatto che non solo la DG Home ma anche la DG Justice sono ora coinvolte nel procedimento di negoziazione di accordi in materia di trasferimento dati). Per una lettura approfondita della sentenza *Parlamento europeo c. Consiglio e Commissione* si rimanda comunque a: G. TIBERI, *L'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura elettronica dei passeggeri aerei al vaglio della Corte di giustizia*, in *Quaderni costituzionali*, 2006; E. PEDILARCO, *Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione europea-Stati Uniti sul trasferimento dei dati dei passeggeri aerei*, in *Diritto Pubblico Comparato ed Europeo*, 2006; M. MENDEZ, *Passenger Name Record Agreement*, in *European Constitutional Law Review*, 3, 2007, ma anche F. ROSSI DAL POZZO, *Servizi di trasporto aereo e diritti dei singoli nella disciplina comunitaria*, Giuffré, 2008 e E. LEHNER, *Democrazia e tutela dei dati personali nell'UE: l'evoluzione nella negoziazione sul PNR dopo il Trattato di Lisbona*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli Editore, 2013.

Nonostante questa prima travagliata vicenda giurisprudenziale, premonitrice sia del destino tutt'altro che felice di questa disciplina sia del ruolo sempre più preponderante svolto dalla CGUE in materia, l'UE ha successivamente concluso non solo un nuovo accordo con gli USA[96] ma anche altri accordi – e

[96] Un secondo accordo tra USA e UE è stato approvato il 16 ottobre 2006 (decisione del Consiglio 2006/729/PESC/GAI, c.d. *interim agreement*, dalla natura temporanea), sostituito da un ulteriore accordo il 23 luglio 2007 a seguito di nuovi negoziati (decisione del Consiglio 2007/551/PESC/GAI). Nel 2011, su indicazione anche del Parlamento europeo che, con risoluzione del 5 maggio 2010 aveva sottolineato la necessità di rinegoziare l'accordo con gli USA, si è giunti alla versione, attualmente ancora in vigore, approvata nell'aprile 2012 da Parlamento e Consiglio. Per interessanti approfondimenti sulla evoluzione delle tutele inserite nei diversi accordi, si rimanda a M. BOTTA, M. VIOLA DE AZEVEDO CUNHA, *La protezione dei dati personali nelle relazioni tra UE e USA, le negoziazioni sul trasferimento dei PNR*, in *Il Diritto dell'Informazione e dell'Informatica*, 2, 2010. Pur non essendo possibile esaminare nel dettaglio tutte le disposizioni dell'ultimo e vigente accordo, si vogliono tuttavia brevemente qui riassumere alcuni dei punti essenziali che regolano gli scambi dei codici di prenotazione tra Stati Uniti e UE, che risulteranno indispensabili inoltre per svolgere alcune considerazioni conclusive sulle conseguenze 'espansive' del *Parere 1/15* anche rispetto a questo atto. Il nuovo accordo, infatti, descritto dall'allora Commissario UE per gli Affari Interni Cecilia Malmstrom, come contenente "solide garanzie per la privacy dei cittadini europei ma al tempo stesso efficace in termini di sicurezza dell'UE e degli USA" (Comunicato Stampo della Commissione Europea IP/11/1368), ha apportato alcune modifiche migliorative rispetto al testo precedente. Innanzitutto vengono più precisamente e dettagliatamente individuati gli scopi per i quali le autorità di *law enforcement* statunitensi possono accedere ai PNR inviati dai vettori aerei: prevenzione, accertamento, indagine e azione penale per reati di terrorismo o transnazionali che prevedano pene detentive non inferiori a 3 anni, escludendo quindi i reati minori. Viene inoltre stabilita l'impossibilità per le autorità statunitensi di adottare decisioni che causino effetti negativi per l'interessato – e dunque ne comprimano i diritti – sulla sola base di un trattamento automatizzato di dati. Sono infine previste alcune tutele particolari con riferimento ai dati sensibili che, purtuttavia, restano oggetto di trasmissione e conservazione. L'aspetto che appare maggiormente problematico, vista l'ampiezza del dettato normativo di alcune disposizioni, è la disciplina in materia di conservazione dei PNR: essa viene fissata ad un periodo massimo complessivo di 15 anni per i reati di terrorismo e di 10 anni invece per i reati gravi di natura transnazionale. La particolarità della disciplina risiede nella specifica scansione temporale, secondo cui le autorità americane (*Department of Homeland Security*, DHS) conservano i PNR in una banca dati "attiva" per un massimo di 5 anni, mentre già dopo 6 mesi dalla ricezione alcune informazioni inserite all'interno del PNR devono essere parzialmente anonimizzate e l'accesso al database è limitato ad un ristretto numero di soggetti autorizzati (art. 8, co. 1). Trascorsi i cinque anni, i dati non vengono cancellati bensì trasferiti e conservati, fino al decorrere massimo di tempo sopra indicato, all'interno di un database c.d. "inattivo" o "dormiente" che richiede procedure di vigilanza e di approvazione per l'accesso molto più rigorose rispetto a quelle regolanti la prima banca dati. È importante sottolineare come, anche al termine di questo periodo, i dati vengano totalmente anonimizzati ma mai distrutti. Una rilevante eccezione a quanto sin qui delineato è rappresentata dal fatto che nel caso in cui un PNR sia stato utilizzato nel corso di investigazioni criminali, lo stesso non subirà la parziale anonimizzazione e l'invio alla banca dati "dormiente" fino a quando le operazioni investigative non saranno concluse, con evidente dilatazione dei termini temporali di conservazione e accesso. Quanto alla supervisione esercitata dal *Privacy Officer* del DHS (art. 14 dell'accordo), essa non garantisce uno scrutinio da parte di un soggetto indipendente: tale Officer infatti è parte della struttura organizzativa del DHS. Emerge già da questa prima generale analisi quanto le disposizioni previste nell'accordo, contenenti previsioni e definizioni estremamente generali e dalla vasta portata (si veda ad esempio la disposizione di grande ampiezza che permette l'uso dei PNR al fine di "prevent serious threat and for the protection of vital interests"), abbiano quale effetto quello di attribuire un notevole margine di discrezionalità alle autorità statunitensi nel disporre ed accedere ai PNR, senza previ interventi e autorizzazioni da parte di autorità giudiziarie o amministrative indipendenti. Per quanto venga attribuita al cittadino europeo cui il dato appartiene la possibilità di richiedere la correzione o l'accesso ai dati o ancora promuovere azioni giudiziarie dinnanzi a giudici statunitensi, il controllo sui dati che può essere concretamente esercitato dai passeggeri è da considerarsi limitato. Per una approfondita analisi dell'Accordo, si legga, tra gli altri: M. SPATTI, *Il trasferimento dei dati relativi ai PNR: gli accordi UE con Austria e USA*, in *Diritto del commercio internazionale*, 3, 2013.

le relative decisioni adeguatezza – molto simili con Canada (nel 2006 e scaduto nel 2009)[97] e Australia (nel 2012)[98].

4.2. – Il Parere 1/15 della CGUE sulla la bozza di accordo Canada-UE in materia di trasferimento di PNR

4.2.1. – I motivi che hanno spinto il Parlamento europeo a richiedere il parere preventivo della CGUE e l'analisi dettagliata svolta dai giudici di Lussemburgo: un vademecum per la Commissione

La ricostruzione svolta nel precedente paragrafo ha messo in luce la cornice estremamente complessa all'interno della quale i negoziati per un nuovo accordo Canada-UE in materia di PNR hanno avuto luogo. In tale contesto, reso ancor più delicato in un momento in cui l'attenzione per la tutela della vita privata e la protezione dei dati era estremamente alta dopo le rivelazioni di Snowden e a seguito della significativa pronuncia della CGUE in materia di *data retention*[99], il Parlamento europeo decideva di rivolgersi, il 30 gennaio 2015, ai giudici di Lussemburgo e di chiedere il loro previo intervento al fine di verificare la compatibilità rispetto all'*acquis communautaire* – comprensivo della Carta dei Diritti Fondamentali dell'Unione Europea – della bozza di nuovo accordo Canada-UE predisposta dalla Commissione e approvata dal Consiglio[100]. L'art. 218 co. 11 TFUE infatti ha attribuito al Parlamento europeo, al Consiglio, alla Commissione e a ciascuno Stato membro, la possibilità di ottenere un parere a carattere preventivo da parte della Corte di Giustizia "circa la compatibilità di un accordo previsto con

[97] La Commissione con decisione 2006/253/CE aveva dichiarato l'adeguatezza del livello di protezione dei PNR trasferiti all'Agenzia dei servizi di frontiera canadese sulla base degli impegni che il Consiglio e le autorità dello Stato terzo avevano adottato e che erano state approvate dalla decisione 2006/230/CE relativa alla conclusione di un accordo tra CE e governo canadese sul trattamento dei dati PNR. Tale accordo, peraltro modificato e revisionato da Commissione e Canada nel 2008, è scaduto il 22 settembre 2009 e nel 2010 sono stati dunque avviati nuovi negoziati che hanno portato alla firma da parte del Consiglio del testo dell'accordo il 25 giugno 2014; tale versione finale è stata inviata dal Consiglio al Parlamento il 7 luglio 2014 per approvazione. Come vedremo, proprio tale bozza sarà oggetto dell'attenzione della CGUE nel più volte richiamato *Parere 1/15*.

[98] L'ultimo accordo è stato adottato con decisione del Consiglio 2012/380/UE, 22 settembre 2011.

[99] Non bisogna infatti dimenticare che al momento del rinvio alla Corte, si era ancora in attesa della pronuncia sulla validità della decisione di adeguatezza in merito al trasferimento di dati verso gli USA nel caso *Schrems*. Il Parere della Corte inoltre poteva risultare anche particolarmente utile per gli Stati membri che erano stati chiamati ad attuare nel proprio ordinamento interno, entro il 25 maggio 2018, la Direttiva UE 681/2016 in materia di PNR – di cui si è già accennato e di cui si dirà più ampiamente nel prosieguo di questo Capitolo – che prevedeva una disciplina armonizzata in materia di raccolta, conservazione e accesso ai PNR nel territorio dell'UE (dei voli da e per l'UE e, in maniera solo opzionale, anche per i PNR relativi a voli infra-UE) per scopi di lotta alla criminalità e garanzia della sicurezza: le valutazioni della CGUE avrebbero potuto fornire delle importanti linea guida anche per i legislatori nazionali nell'adozione delle normative interne di trasposizione della Direttiva europea.

[100] Le motivazioni che hanno spinto il Parlamento a svolgere tale richiesta derivavano dalla considerazione "dei seri dubbi espressi dal GEPD in particolare nel suo parere del 30 settembre 2013, e della giurisprudenza derivante dalla sentenza dell'8 aprile 2014, Digital Rights Ireland e a. (C-293/12 e C-594/12, EU:C:2014:238)", che portavano a ritenere "che vi sia un'incertezza del diritto quanto alla compatibilità dell'accordo previsto con l'articolo 16 TFUE nonché con l'articolo 7, l'articolo 8 e l'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea", Par. 35, *Parere 1/15.*

i trattati"[101]; questa facoltà, assolutamente utile e dai positivi risvolti[102], prevede tuttavia una conseguenza tutt'altro che trascurabile in caso di parere negativo: quest'ultimo infatti ha l'effetto di impedire l'entrata in vigore dell'accordo così come stabilito, imponendo o l'approvazione di modifiche al testo posto al vaglio dei giudici o la revisione dei trattati. Come ben si può comprendere, dunque, una tale richiesta di intervento preventivo della CGUE non deve essere considerata con leggerezza poiché può avere risvolti di forte impatto, obbligando, nella più logica delle conseguenze, ad una rinegoziazione delle condizioni dell'accordo, facendo così sorgere notevoli problemi sotto il profilo dei rapporti con gli Stati terzi nonché in termini di ritardi ed incertezze provocati da una riapertura delle trattative. È interessante alla luce di questo aspetto e preliminarmente all'analisi del contenuto del Parere chiedersi pertanto per quale motivo il Parlamento abbia ritenuto opportuno correre un simile rischio: alcuni autori[103] hanno letto in questa posizione la volontà del Parlamento di "scaricare" sulla Corte il peso di una decisione di estrema delicatezza in un frangente storico-politico e giudiziario, come si è visto sopra, fortemente complesso.

La Corte così incaricata di sciogliere tale nodo, il 26 luglio 2017 ha espresso, nel *Parere 1/15*, una valutazione negativa della bozza di accordo sottoposta alla sua attenzione, affermando l'incompatibilità del testo negoziato con gli articoli 7, 8, 21 e 52 comma 1 della Carta di Nizza. Ma i giudici non si sono limitati ad esprimere questa posizione: similmente a quanto avvenuto anche nelle sentenze *DRI* e *Tele2*

[101] Come poi meglio specificato dalla Corte, "devono pertanto poter essere esaminate nell'ambito della procedura prevista all'articolo 218, paragrafo 11, TFUE tutte le questioni tali da generare dubbi sulla validità sostanziale o formale dell'accordo in relazione ai trattati. Il giudizio sulla compatibilità di un accordo con i trattati può dipendere a tale riguardo, in particolare, non solo da disposizioni che riguardino la competenza, la procedura o l'organizzazione istituzionale dell'Unione, ma anche da disposizioni di diritto sostanziale [v., in tal senso, per quanto riguarda l'articolo 300, paragrafo 6, CE, parere 1/08 (Accordi che modificano gli elenchi di impegni specifici ai sensi del GATS), del 30 novembre 2009, EU:C:2009:739, punto 108 e giurisprudenza ivi citata]. Lo stesso vale anche per una questione relativa alla compatibilità di un accordo internazionale con l'articolo 6, paragrafo 1, primo comma, TUE e, di conseguenza, con le garanzie sancite dalla Carta, la quale ha lo stesso valore giuridico dei trattati", par. 70, *Parere 1/15*.

[102] Come già rilevato dalla Corte nel Parere 1/09, non vi è dubbio che tale procedimento *ex ante* "mira a prevenire le complicazioni che deriverebbero da controversie giudiziarie riguardanti la compatibilità con i Trattati di accordi internazionali che impegnino l'Unione. Infatti, la pronuncia di un giudice che constati eventualmente, successivamente alla conclusione di un accordo internazionale che impegni l'Unione, che quest'ultimo sia incompatibile con le disposizioni dei Trattati, alla luce o del suo contenuto o della procedura adottata per la sua conclusione, non mancherebbe di far sorgere serie difficoltà non solo a livello interno dell'Unione, ma anche su quello delle relazioni internazionali, e rischierebbe di danneggiare tutti gli interessati, ivi compresi gli Stati terzi", Parere 1/09 della CGUE, 8 marzo 2011, par. 47-48. Si legga anche, in questo senso, X. TRACOL: "The procedure of prior opinion thus has a double preventive function, *i.e* . (1) at the EU level, it avoids concluding an international agreement that would affect the treaties; (2) at the international level, it avoids involving the liability of the EU after the act concluding the agreement has been invalidated or after its invalidity has been found which would have consequences in the EU legal order but not at the international level", in *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada*, in *Computer Law and Security Review*, 4, 2018, p. 839.

[103] Si legga sul punto A. VEDASCHI, *Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement*, in *International Data Privacy Law*, 2, 2018, e della stessa autrice anche A. VEDASCHI, G. M. NOBERASCO, *From DRD to PRN: looking for a new balance between privacy and security*, op. cit., nel quale viene affermato altresì che: "While seemingly giving up its 'responibility to decide' to a judicial body, in fact the EP made a reasonable choice" (p. 87); X. TRACOL, in *Opinion 1/15 of the Grand Chamber date 26 July 2017*, op. cit. riflette anche sul fatto che, nel silenzio dell'art. 218, co. 11 TFUE, che nulla dice in merito alle tempistiche entro le quali è possibile richiedere il parere della CGUE, la richiesta avanzata dal Parlamento sia da considerarsi tardiva, essendo proposta in un momento in cui l'accordo già era stato siglato dal Consiglio e dal Canada e dunque in un contesto temporale estremamente avanzato, con l'effetto peraltro di rendere difficili e ancora più lunghi i nuovi negoziati con lo Stato terzo (p. 840). Mendez invece esprime grande apprezzamento per la decisione del Parlamento di azionare il meccanismo del previo parere, ritenendo che "we should be grateful for the presence of the opinion procedure which not only allows for review to take place, but allows it to take place in an arguably less charged political setting than would be the case if we were to allow exclusively ex post review", in M. MENDEZ, *Opinion 1/15: the Court of Justice meets PNR data (again!),* in *European Papers*, 3, 2017, p. 812.

– quest'ultima intercorsa nelle more del giudizio in esame –, il Parere indica una serie molto precisa e dettagliata di condizioni e requisiti che l'accordo rinegoziato dovrà possedere per poter essere considerato compatibile con il diritto dell'UE[104]. Come già avvenuto in passato, dunque, la Corte ha effettuato una analisi estremamente tecnica e precisa, prendendo in esame ogni singola disposizione della bozza e fornendo, infine, linee guida e potenziali soluzioni per consentire di bilanciare la tutela dei diritti fondamentali senza rinunciare alla garanzia della sicurezza, posta alla base della adozione del sistema di scambio di dati PNR. L'analisi della pronuncia dei giudici, che ora verrà svolta, permetterà di giungere ad alcune considerazioni critiche e ragionate sul reale ed effettivo equilibrio che questo bilanciamento ha stabilito.

Procedendo con ordine, la Corte è stata innanzitutto chiamata a rispondere in merito all'individuazione della corretta base giuridica dell'accordo (o meglio della decisione del Consiglio): i giudici di Lussemburgo individuano le fondamenta dell'atto non solo nell'art. 87(2)a del TFUE in materia di cooperazione di polizia e giudiziaria, bensì anche nell'art. 16 TFUE sulla garanzia del diritto alla protezione dei dati personali[105]. La determinazione della base giuridica appropriata è un aspetto tutt'altro che meramente procedurale o tecnico e che, al contrario, permette di anticipare alcune riflessioni di carattere sostanziale: questo aspetto preliminare insomma è tutt'altro che secondario rispetto alle valutazioni circa la compatibilità dell'accordo con le disposizioni della Carta di Nizza. La duplicità dello scopo dell'accordo, individuato da un lato nella garanzia della pubblica sicurezza e dall'altro nella protezione dei dati – mediante cioè la predisposizione di un sistema di norme volte a proteggere i dati personali, che il Canada si impegna a rispettare nel trattamento dei PNR –, rivela non solo i due interessi e diritti che i giudici dovranno valutare nelle operazioni di bilanciamento ma anche il fatto che non sia individuabile la prevalenza di un interesse o diritto sull'altro, neppure sotto il profilo della base giuridica[106].

---

[104] Si vuole infatti sin da ora far notare come alcuni autori abbiano parlato di un approccio para-legislativo del giudice di Lussemburgo "che esalta la dimensione costruttiva dell'attività del giudice, laddove non si limita ad invalidare (o censurare) le norme che è chiamato a vagliare, ma nell'intento di concretizzare principi espressi dalla pregressa giurisprudenza tenda a riscriverne di nuove, anche con il piglio tipico del comitato di tecnica legislativa", A. VEDASCHI, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione Europea*, in *Giurisprudenza Costituzionale*, 4, 2017, p. 1925; sul punto anche H. HIJMANS, *PNR Agreement EU-Canada scrutinised: CJEU gives very precise guidance to negotiators*, in *European Data Protection Law Review*, 3, 2017.

[105] Interessante notare come la Corte precisi: "In tali circostanze, il fatto che i dati PNR siano inizialmente raccolti da vettori aerei a fini commerciali e non da un'autorità competente nel settore della prevenzione o dell'individuazione dei reati e delle relative indagini non può, contrariamente a quanto sostiene il Parlamento, ostare a che l'articolo 87, paragrafo 2, lettera a), TFUE costituisca altresì una base giuridica adeguata della decisione del Consiglio relativa alla conclusione dell'accordo previsto". In questo senso sembra affievolirsi quella distinzione individuata nella previa decisione in merito all'accordo PNR con gli USA, nella quale invece, come già rilevato, veniva effettuata una distinzione forte tra le operazioni svolte da privati e quelle poste in essere da autorità pubbliche, determinando anche effetti con riferimento alla normativa applicabile. Viene invece esclusa come base giuridica l'art. 82, par. 1, co. 2, lett. d TFUE, poiché l'accordo non prevede in alcun modo una facilitazione della cooperazione tra autorità giudiziarie in relazione all'azione penale e all'esecuzione delle decisioni (par. 102-103).

[106] Di rilievo sul punto è l'affermazione dell'Avvocato generale nelle sue Conclusioni: "A conti fatti, ritengo che questi due obiettivi e queste due componenti dell'accordo previsto *siano inscindibilmente connessi, senza che uno sia secondario e indiretto rispetto all'altro*", par. 81, enfasi aggiunta. Per una lettura approfondita di tali Conclusioni, si veda: F. COUDERT, *The legitimacy of bulk transfers of PNR data to law enforcement authorities under the strict scrutiny of AG Mengozzi*, in *EDPL*, 4, 2016. Sotto il profilo della base giuridica inoltre si deve riscontrare come, anche in relazione a quanto già illustrato precedentemente circa l'impatto del Trattato di Lisbona, "The ruling in Opinion 1/15 thus marks a complete departure from the limited EC-US PNR ruling in 2006. It illustrates the impact of the Lisbon Treaty, its consolidation of the former First and Third Pillars of the Maastricht Treaty, and the strength that the new Treaty provides to the Court", C. DOCKSEY, *Opinion 1/15: privacy and security, finding the balance*, in *Maastricht Journal of European and Comparative Law*, 6, 2017, p. 771.

La seconda parte del lungo Parere è poi dedicata al merito dell'accordo, che viene affrontato, come si è avuto modo di vedere, per la prima volta dalla CGUE. L'analisi dei giudici dunque ha inizio con l'individuazione dei diritti fondamentali interessati ovverosia quelli previsti agli artt. 7 e 8 della Carta di Nizza, riconoscendo rispetto ad essi la sussistenza di una interferenza; come già ampiamente affermato nei casi sopra esaminati, i diritti alla vita privata e alla protezione dei dati non sono tuttavia assoluti e anzi vanno considerati in relazione alla loro funzione nella società (par. 136, *Parere 1/15*): la loro compressione dunque può essere considerata legittima nel caso in cui superi il vaglio di proporzionalità e sussistano i requisiti fissati nell'art. 52 della Carta di Nizza stessa (previsione per legge, rispetto dell'essenza dei diritti, principio di proporzionalità – fondato sui concetti di stretta necessità e interesse generale). Utilizzando le concise parole della Corte, "per soddisfare tale requisito, la normativa di cui trattasi, che comporta l'ingerenza, deve prevedere norme chiare e precise che disciplinino la portata e l'applicazione della misura considerata e fissino un minimo di requisiti, di modo che le persone i cui dati sono stati trasferiti dispongano di garanzie sufficienti e tali da permettere di proteggere efficacemente i dati personali contro i rischi di abuso. Essa deve in particolare indicare in quali circostanze e a quali condizioni una misura che prevede il trattamento di siffatti dati possa essere adottata, garantendo così che l'ingerenza sia limitata allo stretto necessario" (par. 141, *Parere 1/15*). Dopo aver affermato che le ingerenze sono basate su di un atto normativo, giustificate dalla sussistenza di un interesse generale (quello alla sicurezza e alla prevenzione e repressione dei reati gravi)[107] nonché tali da non pregiudicare il contenuto essenziale dei diritti fondamentali, i giudici hanno valutato in maniera estremamente rapida l'idoneità del sistema di trasferimento, conservazione e accesso ai PNR rispetto al raggiungimento dell'obiettivo dell'accordo stesso, cioè quello di garanzia della sicurezza (par. 152-153, , *Parere 1/15*), principalmente basandosi sui dati forniti dalle autorità canadesi nel corso del processo[108]: tale approccio è stato tuttavia da taluni[109] giudicato discutibile e sotto alcuni profili persino deficitario.

[107] Addirittura la Corte ritiene che: "Del resto, la protezione della sicurezza pubblica contribuisce altresì alla tutela dei diritti e delle libertà altrui. A tale proposito, l'articolo 6 della Carta enuncia il diritto di ogni persona non solo alla libertà, ma anche alla sicurezza", par. 149, *Parere 1/15*.

[108] Si fa riferimento ai dati e alle informazioni fornite dall'Agenzia dei servizi di frontiera canadese e riprese dalla Commissione nelle osservazioni rese nel corso del processo, secondo cui "il trattamento dei dati PNR aveva permesso, tra gli altri risultati, l'arresto di 178 persone tra i 28 milioni di viaggiatori che avevano effettuato un volo tra l'Unione e il Canada durante il periodo dal mese di aprile 2014 al mese di marzo 2015", arrivando così alla conclusione che "in tali circostanze, il trasferimento dei dati PNR verso il Canada e i trattamenti ulteriori degli stessi possono essere considerati idonei a garantire la realizzazione dell'obiettivo, relativo alla protezione della sicurezza e dell'incolumità pubbliche, perseguito dall'accordo previsto" par. 152-153, *Parere 1/15*.

[109] Il GEPD, ad esempio, nella propria Opinion on the Proposal for Council decisions on the conclusion and signature of the Agreement between Canada and the EU on the transfer and processing of PNR data, del 30 settembre 2013, aveva espresso perplessità circa la reale utilità di tale meccanismo e la sua concreta idoneità a contribuire alla sicurezza pubblica. Del resto anche il Parlamento europeo, richiedendo l'intervento della Corte, si era interrogato sulla idoneità della misura, sottolineando come Consiglio e Commissione non avessero dimostrato, sulla base di elementi obiettivi, la necessità effettiva della conclusione dell'Accordo ai sensi dell'art. 52, co. 1 della Carta di Nizza (par. 40, *Parere 1/15*). Tale aspetto è peraltro emerso anche in occasione della proposta di Direttiva europea in materia di conservazione e trattamento di PNR, cui si è già accennato e di cui si parlerà più avanti. Ciò che anche tale occasione è stato evidenziato è come "Mancava, e manca tuttora, anche nelle argomentazioni del più convincente sostenitore di una Direttiva sull'utilizzo dei dati PNR, la dimostrazione dei vantaggi che detta normativa possa apportare; quali sarebbero le informazioni aggiuntive tali da giustificare la burocrazia, i costi e il grado di intrusione del nuovo sistema. Inoltre, non è chiaro perché sia stato escluso a priori un approccio più selettivo, che limitasse la portata delle misure di controllo ad alcuni Paesi, ad alcune categorie di voli, ad alcune categorie di passeggeri, o ad un arco temporale definito. Tali interrogativi sono stati sollevati da tutti gli oppositori della Proposta del 2011; tra costoro vanno però distinte le posizioni più estreme di chi vede nei dati PNR un vero e proprio passo in avanti verso la sorveglianza globale (E. BROUWER, *Ignoring Dissent and Legality. The EU's Proposal to Share the Personal Information of All Passengers*, in *CEPS Paper in Liberty and Security in Europe* 2011) e quelle più moderate di chi (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Twelve Operational Fundamental Rights Considerations for Law Enforcement When Processing Passenger Name*

Verificata dunque la sussistenza dei primi tre requisiti di cui all'art. 52, la Corte ha applicato il test di proporzionalità inteso *stricto sensu*, entrando nel dettaglio di ogni singola disposizione della bozza di accordo, facendo emergere tutti i punti critici o le previsioni normative che, per come formulate e per il loro contenuto, non sono considerate in grado di garantire il superamento del vaglio di proporzionalità.

Record (PNR) Data, gennaio 2015), pur avversando la normativa in parola, ne riconosce alcuni aspetti positivi, proponendo soluzioni di compromesso che assicurino allo stesso tempo la tutela dei diritti fondamentali e la sicurezza delle persone. I servizi di sicurezza nazionali, peraltro, sostengono all'unisono la necessità di un sistema europeo di scambio dei dati dei passeggeri" F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella Direttiva PNR?*, in *Diritti Umani e Diritto Internazionale*, 1, 2017, p. 224. Sul punto, Tracol in particolare rileva che "PNR data have not permitted to identify any terrorist although one of the two stated purposes of the agreement is to combat terrorism. The Grand Chamber has however not questioned or challenged the compliance of processing mass PNR data with the principle of proportionality. It considered that such processing was appropriate in light of the objective of ensuring public security even though the latter notion is undefined in EU law", in *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the Eu and Canada*, op. cit., p. 836. Ciò che l'autore mette in rilievo e che si vuole qui chiarire è che l'oggetto della critica mossa non è – e non potrebbe essere – individuato nella mancanza di una valutazione circa l'opportunità del sistema di trasferimento PNR negoziato e dunque della conclusione di un accordo su tale oggetto. Alla CGUE infatti non è attribuito il potere e la funzione di spingersi a considerazioni o valutazioni circa l'opportunità delle misure legislative o degli accordi internazionali adottati, essendo questa funzione unica prerogativa del legislatore europeo. In altre parole, la Corte può intervenire valutando la legittimità della normativa adottata rispetto ai Trattati e alla Carta di Nizza; in questo contesto i giudici possono pertanto svolgere il test di proporzionalità che prevede anche, nella valutazione della stretta necessità della misura adottata, una considerazione sulla idoneità delle disposizioni rispetto al raggiungimento del fine stabilito, e, successivamente, sulla esistenza di misure meno invasive dei diritti fondamentali ugualmente in grado di garantire il raggiungimento dello scopo fissato. Proprio su questo aspetto, Tracol ritiene il vaglio della Corte eccessivamente sbrigativo (par. 152-153). Sul punto invece è maggiormente attento l'Avvocato generale Mengozzi, che nelle sue già più volte richiamate Conclusioni ritiene che "non è sufficiente immaginare, in astratto, misure alternative meno restrittive dei diritti fondamentali delle persone. Occorre altresì, a mio avviso, che tali misure presentino garanzie di efficacia analoghe a quelle di cui si prevede l'istituzione nell'ambito della finalità di lotta contro i reati di terrorismo e contro la criminalità transnazionale grave. Non sono state portate a conoscenza della Corte, nel presente procedimento, altre misure che, limitando il numero di persone i cui dati PNR siano sottoposti a un trattamento automatizzato da parte della competente autorità canadese, possa conseguire, con analoga efficacia, lo scopo di pubblica sicurezza perseguito dalle parti contraenti", par. 244. Interessante è chiedersi se, in questo caso, la Corte avrebbe potuto avanzare una richiesta di informazioni e la produzione di ulteriori documenti ai sensi dell'art. 64 del Regolamento di procedura della Corte di giustizia. Del resto quest'ultimo aspetto circa l'utilizzo o meno dei poteri istruttori dei giudici di Lussemburgo è stato discusso anche con riferimento, più ampiamente, alla valutazione del diritto straniero, come avvenuto nei casi *Schrems* e nel *Parere 1/15*, nei quali grande rilievo ai fini della decisione della Corte hanno assunto l'ordinamento statunitense e quello canadese, con particolare attenzione alle disposizioni normative da tali ordinamenti predisposti in materia di protezione dei dati e della privacy nonché di accesso ai dati personali da parte di autorità pubbliche di *law enforcement* o di intelligence. Sotto tale profilo, alcuni autori hanno criticato la mancata decisione della Corte di richiedere uno studio da parte di esperti della normativa straniera, coinvolgendo accademici o esponenti della società civile, al fine di interpretare il più correttamente possibile il diritto dello Stato terzo (potere che i giudici avrebbero peraltro potuto attivare con ancor meno restrizioni nell'ambito del *Parere*). Sul punto si legga Tracol che, nel contributo sopra richiamato, ricorda come la decisione della Corte richiedesse una valutazione della normativa canadese per comprendere le condizioni del trattamento dei dati dei passeggeri e dunque i rischi o le carenze rispetto alla tutela garantita nell'Unione. Ebbene l'autore ritiene "regrettable that the Grand Chamber has not exercised its discretion in commissioning an expert's report to assist it in correctly interpreting Canadian law (..). It [the Gran Chamber] relied only on the submissions of both Council and Commission to that effect", p. 840. Dello stesso avviso è anche Kuner: "The Court's Opinion procedure allows the use of expert opinions and further investigation in a way that is not permissible in preliminary reference proceedings. Interpreting foreign law and practice poses daunting problems of evidence-gathering and interpretation, and the Court could in the future consider gathering evidence from academic experts, civil society groups, and others with an expert knowledge of foreign law. In Opinion 1/15, it would have seemed useful to consult Canadian experts regarding issues involving Canadian law, rather than relying mainly on web sites and evidence presented by the EU institutions. It would also be helpful if the Court would abandon the fiction that it never has to evaluate foreign legal standards in its cases", in C. KUNER, *International agreements, data protection and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, op. cit., p. 22.

Punto di partenza è la disposizione recante la definizione di PNR, che viene considerata dai giudici non contenente elementi chiari e precisi[110] per la determinazione dei dati da trasferire. Di grande rilievo e di estrema problematicità è poi l'art. 8 della bozza di accordo che stabilisce come nella categoria dei PNR possano anche rientrare dati sensibili, pur essendo questi sottoposti a specifiche salvaguardie da parte delle autorità canadesi: i giudici affermano con forza l'assenza di stretta proporzionalità tra il trasferimento di dati sensibili e la finalità di prevenire e contrastare il terrorismo o altri gravi crimini transfrontalieri. Richiamando l'esempio positivo della Direttiva UE 2016/681 in materia di PNR – su cui si rifletterà in seguito –, che esclude e proibisce *tout court* il trasferimento, conservazione e accesso ai dati sensibili, viene quindi con forza affermato come gli artt. 7, 8, 21 e 52 della Carta di Nizza precludano la possibilità di adottare disposizioni concernenti il trasferimento di detta categoria di dati.

Un'ulteriore criticità emerge con riferimento all'analisi automatizzata dei dati PNR prima che il passeggero cui il dato afferisce arrivi sul suolo canadese[111]: questa tipologia di controllo è fondata sull'uso di strumenti di analisi automatizzata, che trattano i dati sulla base di modelli e criteri prestabiliti nonché mediante controlli incrociati con diverse banche dati. Secondo i giudici di Lussemburgo la previsione che esclude la possibilità di prendere decisioni che danneggino in modo significativo il passeggero solo sulla base del trattamento automatizzato dei PNR, come previsto dall'art. 15 della bozza di accordo, non risulta sufficiente a garantire il rispetto del principio di stretta necessità: manca infatti una disposizione che imponga l'utilizzo di modelli e criteri prestabiliti che siano specifici ed affidabili, oltre ad essere privi di qualsiasi carattere discriminatorio. Il margine di errore, insito nell'utilizzo stesso di sistemi automatizzati – quel *bias* di cui si è ampiamente parlato nel Capitolo I, Parte I – deve poi essere scongiurato mediante la disposizione di un riesame individuale effettuato senza l'impiego di strumenti automatizzati. Sotto questo ulteriore profilo dunque le tutele apprestate dalla bozza di accordo mostrano i propri limiti e non superano il test di proporzionalità, rendendo necessaria una rinegoziazione delle condizioni del trasferimento e trattamento dei dati verso il Canada.

Mentre le norme che individuano e descrivono le finalità del trattamento dei dati PNR da parte delle autorità canadesi vengono ritenute solo in parte chiare, precise e limitate allo stretto necessario[112], anche l'individuazione delle autorità competenti a ricevere i dati è ritenuta parzialmente vaga e non sufficientemente chiara poiché vengono indicate genericamente, quali possibili destinatari dei dati, "altre autorità governative canadesi" o addirittura autorità situate in Stati terzi[113]. L'accordo peraltro viene considerato eccedente lo stretto necessario nella parte in cui prevede la possibilità da parte delle autorità canadesi di comunicare informazioni a soggetti privati (par. 216-217, *Parere 1/15*).

---

[110] In particolare l'utilizzo di termini quali "etc." viene criticato aspramente dalla Corte in quanto "non determina a sufficienza la portata dei dati da trasferire" (par. 157, *Parere 1/15*) e questo nonostante la definizione riportata nell'accordo corrisponda a quanto contenuto nell'Allegato 1 delle Linee Guida ICAO.

[111] Occorre precisare un aspetto tecnico: la trasmissione dei dati in questione si fonda sul metodo c.d. "push", che richiede cioè un ruolo attivo dei vettori aerei, tenuti ad inviare i PNR presso specifici database delle autorità nazionali richiedenti, debitamente individuate dalla legge del Paese terzo o dagli accordi internazionali. Questo metodo differisce dai sistemi c.d. "pull" che sono invece basati su un accesso diretto delle autorità nazionali ai database-PNR delle compagnie aeree.

[112] Salvo quanto stabilito all'art. 3, co. 5, lettere a) e b) che vengono considerate troppo vaghe e generiche (par. 181, *Parere 1/15*).

[113] In questo senso si nota come la bozza di accordo attribuisca alle autorità canadesi un ampio margine di discrezionalità nel valutare se il livello di protezione dei dati e della vita privata nel Paese terzo sia equivalente o meno a quanto garantito nell'accordo. I giudici di Lussemburgo nel parere chiariscono, riprendendo quanto affermato nella sentenza *Schrems*, la necessità che la sostanziale equivalenza del livello di protezione sia accertata da un accordo tra UE e Paese terzo o da una decisione di adeguatezza della Commissione, cosicché "tale requisito vale anche nel caso della comunicazione dei dati PNR dal Canada verso altri paesi terzi, di cui all'articolo 19 dell'accordo previsto, al fine di evitare che il livello di protezione previsto da tale accordo possa essere eluso da trasferimenti di dati personali verso paesi terzi e di assicurare la continuità del livello di protezione offerto dal diritto dell'Unione" (par. 214, *Parere 1/15*).

4.2.2. – La valutazione della proporzionalità delle operazioni di invio, conservazione e accesso ai PNR stabilite nella bozza di accordo: una differenziazione a seconda dei momenti del viaggio del passeggero

L'aspetto sicuramente più delicato ed interessante dell'analisi della CGUE è però quello attinente alla determinazione delle condizioni per una legittima conservazione dei PNR da parte delle autorità canadesi: la Corte, rilevando come la bozza di accordo non riconosca alcuna differenziazione nella disciplina della *retention* e trattamento dei dati a seconda dei diversi momenti del viaggio (prima della partenza, durante la permanenza in Canada e successivamente all'uscita dal territorio canadese), afferma come, a seconda della distinzione temporale, la necessità di trattenimento/conservazione dei PNR e dunque la proporzionalità o meno dell'ingerenza nei diritti fondamentali debbano essere diversamente modulate. Ecco dunque che, partendo dalla fase antecedente all'arrivo dei passeggeri in Canada, i giudici di Lussemburgo giungono a sostenere la legittimità del meccanismo di invio sistematico e generalizzato dei PNR mediante un ragionamento di grande rilevanza: nonostante l'invio e la prima analisi automatizzata dei dati avvengano "indipendentemente da qualsiasi elemento obiettivo che consenta di ritenere che i passeggeri possano rappresentare un rischio per la sicurezza pubblica in Canada" (par. 186, *Parere 1/15*), i giudici di Lussemburgo ne riconoscono il rispetto del criterio di stretta necessità poiché "la conservazione e l'uso a tal fine non possono, per loro stessa natura, essere limitati a una cerchia determinata di passeggeri aerei né essere oggetto di una previa autorizzazione di un giudice o di un ente amministrativo indipendente" (par. 197, *Parere 1/15*). Anche durante il soggiorno i dati PNR possono essere conservati in maniera generalizzata purché le operazioni di accesso vengano svolte solo in presenza di condizioni sostanziali e procedurali basate su criteri oggettivi.

In questa prima parte dell'analisi del sistema PNR con particolare riferimento alla disciplina della conservazione dei dati stessi nella fase 'pre' arrivo e durante il soggiorno del passeggero, quindi, ciò che emerge è l'accettazione del meccanismo stesso oggetto della bozza di accordo, che prevede cioè un flusso e una conservazione dei dati di tipo generalizzato ed indiscriminato, riguardando indifferentemente tutti i passeggeri di voli diretti da e per il Canada. In questo modo la CGUE ammette, solo nella fase precedente all'arrivo e durante il soggiorno, una forma di *retention* sistematica e slegata da quei caratteri di 'oggettività' che richiederebbero invece una conservazione targettizzata e limitata dunque a taluni soggetti appartenenti a determinati gruppi sociali o provenienti da specifiche aree geografiche. Questa posizione, sulla quale si discuterà più ampiamente nel prosieguo di questo Capitolo, potrebbe essere letta[114] come contrastante rispetto a quanto affermato nelle sentenze *DRI* e *Tele2*, nelle quali la Corte ha espressamente e chiaramente ritenuto illegittime e non conformi alla Carta di Nizza forme generalizzate ed indiscriminate di conservazione dei dati provenienti dalla totalità della popolazione e riguardanti i metadati di tutti i mezzi di telecomunicazione[115]. L'Avvocato generale

[114] In effetti alcune critiche sono state mosse alla Corte per aver di fatto accettato la legittimità di programmi di scambio PNR, pur ammettendo specifiche salvaguardie e tutele. Mendez sul punto ritiene però che: "Perhaps this is the most that can have realistically been expected, given the rapid and growing deployment of PNR schemes, including crucially within the EU itself, especially in light of access to PNR data becoming a central aspect of the US's counter terrorism strategy since 11 September 2001", *Opinion 1/15: the Court of Justice meets PNR data (again!)*, op. cit., p. 813.

[115] Del resto il GEPD nella sua *Opinion 5/2015*, seppur vertente sulla proposta di Direttiva europea in materia di PNR, ha ribadito con forza come "the non-targeted and bulk collection and processing of the PNR scheme amount to a measure of general surveillance" (par. 63), suggerendo che l'unico utilizzo dei PNR conforme ai principi di proporzionalità debba ravvisarsi nell'uso dei PNR "on a case-by-case basis but only in case of a serious and concrete threat established by more specific indicators", non mancando di sottolineare come "there is no information available to the effect that the necessity and proportionality of the measures proposed have been adequately demonstrated" (par. 64). Più in generale, già nella *Opinion 7/2010 on the European Commission's Communication on the global approach to transfers of PNR data to third countries* (12 novembre 2010), lo stesso GEPD aveva chiarito la propria posizione, affermando: "the usefulness of large-scale profiling on the basis of

Mengozzi nelle sue Conclusioni, cogliendo la delicatezza di queste considerazioni, ha espressamente toccato questo punto, effettuando una distinzione tra il sistema PNR e quello oggetto dei precedenti giudizi: viene rilevato innanzitutto come i codici di prenotazione dei voli e le informazioni in esse contenute, pur essendo certamente invasivi della sfera personale del passeggero, lo siano in misura minore rispetto alla *retention* della totalità dei metadati provenienti dalle telecomunicazioni, provocando quindi una ingerenza meno ampia rispetto a quella prevista dalla Direttiva 2006/24 e dall'art. 15 Direttiva *e-Privacy*[116]. Partendo da questa premessa comunque l'Avvocato ammette che la "natura indifferenziata e generalizzata [del sistema di raccolta e conservazione PNR] suscita interrogativi" (par. 240) che tuttavia non comportano l'incompatibilità del meccanismo con il diritto dell'UE. "L'interesse stesso dei regimi PNR è di garantire la trasmissione massiccia di dati che consenta alle autorità competenti di identificare, mediante strumenti di trattamento automatizzato e di scenari o di criteri prestabiliti, individui fino a quel momento sconosciuti ai servizi di polizia" (par. 241): come a dire quindi che la generalizzazione costituisce parte integrante e necessaria della *ratio* del sistema di trasferimento di PNR, che non avrebbe ragione di esistere se fosse diversamente limitato *ratione personae*; ogni tentativo di targetizzare i soggetti interessati dalla trasmissione e conservazione dei dati avrebbe come esito quello di minare l'efficacia stessa della misura, pregiudicando il conseguimento effettivo del suo obiettivo, oltre al rischio che un regime mirato, sulla base dei criteri indicati ad esempio nelle sentenze *DRI* e *Tele2*, rappresenti una forma di discriminazione vietata (par. 243)[117]. Insomma sulla base di queste valutazioni, l'Avvocato generale, seguito poi dalla Corte stessa, ha precisato quanto il *Parere 1/15* abbia ad oggetto un sistema di trasferimento dati che differisce, sotto vari profili, da quello di conservazione generalizzata ed indiscriminata di cui alla Direttiva 26/2004 e come non debba vedersi in tale decisione della Corte una posizione difforme dal filone giurisprudenziale precedente; al contrario, il Parere rappresenta una conferma di tutti quei principi e criteri individuati nelle previe decisioni, che saranno applicati nello scrutinio circa la conformità al diritto dell'UE delle misure della bozza di accordo riguardanti la conservazione e il trattamento di dati PNR durante il soggiorno in Canada e successivamente alla partenza del passeggero dallo Stato terzo. Proprio con riguardo alla conservazione dei dati dei passeggeri dopo che questi ultimi abbiano lasciato il Canada, i giudici di Lussemburgo osservano come "i passeggeri aerei che hanno lasciato il Canada sono stati, di norma, oggetto di controlli all'entrata e all'uscita da tale Paese. Parimenti, i loro dati PNR sono stati verificati prima del loro arrivo in Canada e, eventualmente, durante il loro soggiorno nonché all'uscita da tale Paese terzo. In dette circostanze, si deve ritenere che tali passeggeri non presentino, in linea di principio, un rischio in materia di terrorismo o di reati gravi di natura transnazionale" (par. 204, *Parere 1/15*). Questa premesse rendono pertanto necessaria la presenza di elementi obiettivi che determinino l'esigenza di trattenere il dato e che siano idonei a far ritenere sussistente un rischio più elevato nei confronti di questo soggetto rispetto alle altre persone che mai hanno volato in Canada e rispetto alle quali quindi le autorità non posseggono

passengers' data must be questioned thoroughly, based on both scientific elements and recent studies. On the contrary, recent studies tend to establish the counter-productive character of such screening, especially in relation to the fight against terrorism", p. 4.

[116] Sul punto si legga anche L. WOODS, *Trasnferring personal data outside the EU: clarification from the ECJ?*, in *EU Law Analysis*, 4 agosto 2017, la quale ritiene appunto che l'accettazione del sistema di trasferimento di dati PNR possa essere dovuta proprio alla diversa natura dei dati oggetto di trattamento: quello che è certo è che comunque la Corte, a differenza dell'Avvocato generale, non spiega nulla in merito a tale posizione.

[117] Così si legga F. COUDERT, *The legitimacy of bulk transfers of PNR data to law enforcement authorities under the strict scrutiny of AG Mengozzi*, op. cit., p. 600. L'Avvocato generale prosegue poi affermando: "Inoltre, contrariamente alle persone i cui dati formavano oggetto del trattamento di cui alla Direttiva 2006/24, tutte quelle cui si riferiva l'accordo previsto prendono volontariamente un mezzo di trasporto internazionale diretto o proveniente da un paese terzo, mezzo di trasporto che è esso stesso, purtroppo in modo ricorrente, veicolo o vittima di atti di terrorismo o di reati gravi di natura transnazionale, il che necessita dell'adozione di misure che garantiscano un livello di sicurezza elevato di tutti i passeggeri.", par. 242.

i PNR[118]. La mancata presenza di tali elementi oggettivi in grado di legare l'obiettivo di lotta al terrorismo e crimini gravi al soggetto 'in uscita', rende ingiustificata e sproporzionata una archiviazione continua e prolungata dei PNR, determinandosi così per la Corte una illegittimità della bozza di accordo anche sotto questo profilo[119].

Ecco quindi che, legittimato il sistema di invio generalizzato, di analisi automatizzata preventiva e di conservazione durante il soggiorno – che altrimenti, se considerato incompatibile con l'*acquis communautaire*, avrebbe reso superflua qualsiasi ulteriore valutazione della Corte, rendendo altresì impossibile la predisposizione di un qualsiasi accordo sul tema –, i giudici hanno spostato poi l'attenzione sulla disciplina dell'accesso ai dati, distinguendo anche in tal caso la propria analisi a seconda dei diversi frangenti temporali.

Esaminando quindi l'accesso da parte delle autorità di *law enforcement* ai dati dei passeggeri aviotrasportati durante il loro soggiorno, con riferimento cioè a soggetti già ammessi all'ingresso nel territorio canadese e che hanno superato il 'controllo' automatizzato preventivo, viene rilevata la necessità di istituire un legame tra l'accesso al dato e una determinata indagine: debbono pertanto essere individuate esigenze nuove che giustifichino tale ulteriore ingerenza nella sfera privata e che perciò debbono subentrare in un momento successivo all'ingresso nel Paese. In questo caso, la Corte ha pertanto ribadito e riconfermato i criteri già individuati nelle sue previe pronunce, in particolare nella *Tele2*: servono norme precise che dettino condizioni sostanziali e procedurali e che si fondino su elementi oggettivi "per definire le circostanze e le condizioni alle quali le autorità canadesi contemplate dall'accordo previsto siano autorizzate a farne uso" (par. 200, *Parere 1/15*). Vengono richieste inoltre precise ed ulteriori tutele, una di carattere preventivo e alcune da attuarsi invece successivamente al trattamento del dato: quanto al primo dei due profili, salvo casi di particolare urgenza, l'accesso e l'uso dei codici di prenotazione deve essere subordinato ad un controllo preventivo effettuato da un giudice o da un soggetto amministrativo che gode del carattere di indipendenza[120]. Quanto al secondo profilo, i giudici di Lussemburgo evidenziano la necessità di garantire il diritto d'informazione del passeggero nonché quello di accesso e rettifica, ritenendo imprescindibile l'obbligo di notifica contenente indicazioni circa l'uso effettuato dei dati o la comunicazione degli stessi ad altre autorità pubbliche o private (par. 218 ss, *Parere 1/15*). La carenza di tali tutele nella bozza di accordo in esame ne rendono il testo incompatibile con il diritto dell'UE poiché l'assenza delle indicate garanzie rende la possibile ingerenza delle autorità pubbliche non limitata allo stretto necessario.

Merita solo da ultimo rilevare come la Corte abbia individuato una ulteriore carenza nella bozza di accordo nella parte in cui non viene garantito in modo sufficientemente chiaro e preciso che l'autorità

---

[118] Con riferimento a questo passaggio viene rilevato da alcuni autori, tra cui Tracol, come la Corte non abbia specificato con grande precisione cosa intenda per 'criteri oggettivi' e quindi in quali casi tali elementi siano sufficienti per determinare una connessione tra un soggetto e l'obiettivo di prevenzione e repressione di crimini gravi: "The Grand Chamber has not specified the cases where objective evidence is identified from which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime. It has not specified either the standard of proof applicable to the possible interference to be drawn, such as the only reasonable inference available from circumstantial evidence in criminal law. (..) In any case, the Gran Chamber did not require that air passengers whose PNR data may be stored after their departure from Canada should have the legal status of suspects subjects to a police or criminal investigation", X. TRACOL, *Opinion 1/15 of the Grand Chamber date 26 July 2017*, op. cit., p. 838.

[119] Anche nel caso in cui siano ritenuti sussistenti elementi oggettivi tali da consentire la conservazione dei PNR anche successivamente alla partenza del soggetto dal Canada, la Corte ritiene necessaria la previsione di tutele e garanzie per il possibile utilizzo e accesso ai dati stessi, che dovranno quindi godere delle stesse protezioni previste nel caso di accesso ai dati di passeggeri durante la permanenza di questi ultimi.

[120] Ai par. 202 e 203 la Corte richiama dunque per analogia quei criteri indicati già nelle sentenze *DRI* e *Tele2*. Con riferimento a tale aspetto, la Corte va al di là di quanto richiesto dall'Avvocato generale, che riteneva sufficiente il solo "un controllo giurisdizionale effettivo a posteriori delle decisioni o delle misure riguardanti l'accesso ai suoi dati PNR", par. 272.

canadese deputata alla sorveglianza del rispetto dell'accordo stesso sia una autorità indipendente (par. 230).

Per tutte le ragioni sopra didascalicamente enunciate, la Corte giunge ad affermare l'incompatibilità della bozza di accordo con gli articoli 7, 8 e 52 della Carta di Nizza, fornendo però, similmente a quanto fatto nella sentenza *Tele2*, un vero e proprio vademecum di criteri e requisiti da rispettare che fungono da cartina di tornasole per la Commissione nelle operazioni future di negoziazione di accordi.

4.3 – Una ricognizione delle più significative implicazioni del **Parere 1/15** *fuori e dentro i confini dell'UE*

4.3.1. – La necessaria rinegoziazione dell'accordo con il Canada e le ripercussioni rispetto alle negoziazioni in atto con altri Stati terzi

Il preciso ed articolato elenco di criteri e condizioni indicato dalla Corte nella sua pronuncia in materia di PNR non può che far sorgere, innanzitutto, alcune perplessità quanto alla sua reale e concreta attuazione nel contesto delle relazioni internazionali: vi sono infatti dubbi circa la possibilità che un accordo che rispetti tutte le condizioni indicate dai giudici di Lussemburgo sia effettivamente negoziabile ed "accettabile" da uno Stato terzo; inoltre alcuni autori si sono anche chiesti se la posizione espressa nel Parere non determini, nei fatti, una forte discontinuità e incongruenza tra quanto affermato preliminarmente ed in linea generale dalla Corte nella parte in cui viene stabilita l'ammissibilità, *per se*, del sistema di trasferimento sistematico di PNR e quanto successivamente richiesto in termini di condizioni e criteri necessari al fine di rendere l'accordo – e dunque il flusso di dati – conforme al diritto dell'UE e, in particolare, alla Carta di Nizza[121].

Da queste prime incertezze circa la reale portata del *Parere 1/15* e in maniera funzionale a quanto si svilupperà più ampiamente nel successivo paragrafo, si diramano una serie di considerazioni circa l'impatto della pronuncia esaminata rispetto: a) alla necessaria rinegoziazione dell'accordo con il Canada e alle negoziazioni al momento in atto con altri Stati terzi (Messico e Giappone); b) agli accordi in materia di PNR attualmente in vigore con altri Stati terzi (USA e Australia); c) alla Direttiva europea 2016/681 in materia di PNR.

Iniziando dunque ad analizzare il primo profilo, è utile sottolineare come a seguito dell'autorizzazione del Consiglio, ricevuta dalla Commissione nel dicembre 2017, nel giugno 2018 nuovi negoziati siano stati avviati con il Canada, che si sono poi conclusi, in tempi relativamente brevi, nel luglio 2019: "sebbene il Canada abbia fatto presente il proprio obbligo di esame giuridico, le parti si sono impegnate, fatto salvo tale esame, a concludere l'accordo quanto prima riconoscendone il ruolo fondamentale per rafforzare la sicurezza e garantire al tempo stesso la tutela della vita privata e la protezione dei dati personali"[122]. Tali considerazioni assumono ancor più rilievo se si pensa che, durante

[121] A. VEDASCHI, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di Giustizia dell'Unione Europea*, op. cit., 1927, che afferma sul punto come: "la legittimità di tale operazione resta meramente teorica, poiché il legislatore, a giudizio della Corte, non ha ancora trovato, sul piano pratico, una realizzazione compatibile con la Carta dei diritti". Pur ammettendo quindi in linea generale la legittimità del sistema di scambio di PNR, la Corte stabilisce talmente tante condizioni da rendere nella pratica quasi impossibile delineare un accordo che le rispetti e racchiuda tutte. Questa riflessione ben può essere estesa più genericamente poi anche all'intera regolamentazione del trasferimento di dati transfrontaliero: se sia possibile cioè, come si rifletterà *infra*, imporre l'alto livello di tutela delineato dalla giurisprudenza della CGUE sin dalla sentenza *DRI* anche, come stabilito in *Schrems* e nel parere in oggetto, al di fuori dei confini europei in contesti ordinamentali differenti da quello del vecchio continente e in un panorama di interdipendenza economica che rende difficile per l'UE assumere una posizione netta ed impedire *in toto* e per un tempo indefinito il flusso di dati.

[122] Ciò emerge dalla Proposta di Decisione del Consiglio relativa alla posizione da adottare a nome dell'Unione europea in sede di Consiglio dell'Organizzazione per l'aviazione civile internazionale in merito alla revisione

le procedure di rinegoziazione e in assenza di un nuovo accordo, i vettori aerei hanno comunque continuato a trasferire i dati dei propri passeggeri alle autorità canadesi: il trattamento dei dati continua ad essere regolato, al momento, da un "Committment" elaborato della *Border Service Agency* canadese che altro non è se non un allegato alla decisione della Commissione 2006/253/EC, cioè la prima decisione sull'adeguato livello di protezione offerto dai PNR trasferiti in Canada. Il citato documento, ormai datato, presenta un livello di garanzia del diritto alla protezione dei dati e alla riservatezza di gran lunga inferiore a quanto previsto nella bozza di accordo[123]: questa situazione, per quanto temporanea, deve pertanto far riflettere sull'urgenza di trovare un accordo in tempi rapidi, tenendo tuttavia in considerazione che più elevato è lo standard di tutela che la Corte (o le altre Istituzioni europee) fissa, più i negoziati saranno lunghi, complessi e dagli incerti risvolti. Come si dirà anche nelle considerazioni dell'ultimo paragrafo, se da un lato la Corte di giustizia vuole porsi quale baluardo a difesa della riservatezza e della protezione dei dati, fissando l'asticella delle garanzie ad un livello particolarmente alto, dall'altro essa deve necessariamente fare i conti con Stati terzi che possono mostrarsi riluttanti ad approvare accordi che impongono condizioni di trattamento dei dati restrittive e stringenti, in grado di avere peraltro un forte impatto sull'ordinamento interno dello Stato stesso e sulle sue politiche di salvaguardia della sicurezza[124]. In mancanza di un punto di equilibrio tra questi due poli opposti e nella impossibilità di creare un dialogo proficuo con lo Stato terzo ricevente i dati, si andrebbe a generare un vuoto regolatorio, come accaduto nel caso del trasferimento dati PNR verso il Canada ma più ampiamente anche a seguito della decisione *Schrems* (pur essendo presenti in quel caso soluzioni alternative volte a garantire il flusso di dati). Tale situazione di 'stallo' e di indeterminatezza, anche in termini temporali – considerando la lunghezza ed imprevedibilità dei negoziati nonché l'incertezza circa il raggiungimento di un nuovo accordo – espone pertanto i dati degli utenti o dei passeggeri europei a seri rischi in termini di garanzie e tutele: ciò spinge dunque a chiedersi in ultima analisi se un accordo imperfetto e perfezionabile non sia in realtà comunque più apprezzabile e maggiormente garantista rispetto all'assenza totale di accordi. Su questo punto, le Istituzioni dell'UE dovranno necessariamente riflettere e confrontarsi, viste le posizioni divergenti che spesso Commissione, Consiglio, Parlamento e Corte esprimono in materia e che abbisognano dunque di un serio confronto e di maggiore coordinamento, anche e soprattutto con riferimento ai negoziati al momento in corso con Messico e Giappone[125]; alcuni di essi, iniziati in tempi lontani, hanno visto una battuta d'arresto forte ed inevitabile in occasione del *Parere 1/15*. Inoltre, a seguito di tale decisione e dell'incerta sorte degli Accordi elaborati dalla Commissione, molti Stati terzi, come numerosi autori non hanno mancato di segnalare[126], potrebbero in futuro mostrarsi riluttanti o dubbiosi ad avviare trattative con l'UE in materia di

dell'allegato 9 ("Facilitazioni"), capo 9, della convenzione relativa all'aviazione civile internazionale per quanto riguarda gli standard e le pratiche raccomandate sui dati del codice di prenotazione, COM(2019)416 final, del 13 settembre 2019. Ad oggi comunque l'accordo negoziato con il Canada nel 2019 è ancora in attesa di riesame giuridico e approvazione politica da parte del Canada.

[123] Per una analisi delle tutele predisposte dal *Committment* attualmente utilizzato per il trasferimento dei dati PNR verso il Canada, si legga, ancora una volta: X. TRACOL, *Opinion 1/15 of the Grand Chamber*, op. cit., p. 841.

[124] Non si è mancato di notare infatti come l'accettazione da parte di uno Stato terzo degli standard di tutela europei e la loro garanzia all'interno dell'ordinamento nazionale possa comportare la necessità di modifiche dell'assetto normativo, adeguandolo mediante la previsione di particolari disposizioni: si pensi a figure quali l'Ombudsperson richiesto ed introdotto dal *Privacy Shield* nel contesto Statunitense o ancora alla predisposizione di controlli e garanzie da parte di organi indipendenti che non sempre sono originariamente e normalmente previsti nell'ordinamento dello Stato terzo ricevente i dati dall'UE.

[125] Mentre il 18 febbraio 2020 la Commissione è stata autorizzata dal Consiglio ad avviare negoziati con il Giappone finalizzati alla conclusione di un accordo in materia di trasferimento di dati PNR, i negoziati con il Messico, iniziati nel 2015, sono ora in una fase di stallo.

[126] C. KUNER, *Reality and illusion in EU data transfer regulation post-Schrems*, in *German Law Journal*, 18, 2017. Mendez invece sottolinea come "It always seemed inevitable that there would be a considerable degree of second-guessing involved because we were dealing with an agreement negotiated prior to key jurisprudential developments", in *Opinion 1/15: the Court of Justice meets PNR data (again!)*, op. cit., p. 812.

trasferimento di dati: come il caso *Schrems* e il *Parere 1/15* insegnano, anche una decisione di adeguatezza – e dunque l'accordo già concluso su cui essa si basa – può essere suscettibile di invalidazione, mentre l'accordo può addirittura risultare 'bloccato', in fase ancora preliminare, dal vaglio effettuato dalla CGUE su richiesta ex art. 218, co. 11 TFUE, acuendo così un senso di incertezza e provvisorietà che può costituire un concreto deterrente all'avvio di negoziazioni, già per sé lunghe e complesse. Se è certamente vero, tuttavia, che l'interesse e la necessità ad avere in essere accordi con l'UE, sia in materia di PNR che di trasferimento di dati, assumono carattere prioritario per tutti gli Stati che si trovano ad avere significativi contatti con il vecchio continente e che sono pertanto incentivati, sotto tale profilo, ad avviare procedure di negoziazione, permangono comunque forti dubbi sul se e come la Commissione e il Consiglio, nello svolgimento del loro operato, possano riuscire ad attuare concretamente quanto stabilito dalla giurisprudenza della CGUE e ad imporre efficacemente negli accordi pattuiti i criteri da quest'ultima delineati, in modo da rendere le relative decisioni di adeguatezza più solide e resistenti al vaglio eventuale – ma ultimamente piuttosto frequente – dei giudici di Lussemburgo.

4.3.2. – Le conseguenze del Parere 1/15 *sugli Accordi in materia di PNR al momento vigenti*

Simili riflessioni sulle conseguenze del *Parere 1/5* devono necessariamente essere svolte anche rispetto agli accordi in materia di PNR attualmente in vigore, quali quello con gli USA e quello con l'Australia, sopra richiamati[127]: bisogna chiedersi cioè se tali disposizioni, e le relative e connesse decisioni di adeguatezza, possano superare illese il controllo della Corte. L'esercizio che può essere compiuto al fine di rispondere a tale quesito, è quello di applicare lo stesso test di proporzionalità utilizzato dai giudici di Lussemburgo nel vaglio della bozza di accordo col Canada anche agli accordi esistenti, e di rileggere quindi questi ultimi alla luce dei criteri e principi fissati dalla giurisprudenza in materia.

Ciò che emerge da questo esame è innanzitutto la somiglianza di molte delle disposizioni contenute nell'accordo PNR con gli USA e con l'Australia rispetto a quelle inserite nella bozza esaminata dalla CGUE; ne deriva una prima criticità sotto il profilo formale, relativamente alla base giuridica: mentre entrambi gli accordi già in vigore infatti individuano nell'art. 82, co. 1, lett. d, (cooperazione tra autorità giudiziarie in relazione all'azione penale e all'esecuzione delle decisioni) il proprio fondamento, i giudici di Lussemburgo, nel *Parere 1/15*, hanno espressamente escluso la correttezza di tale disposizione quale base giuridica: certamente "While finding that the wrong legal basis was used for the Draft Agreement does not by itself invalidate other international agreements, it does have implications for them, should they ever come before the Court"[128].

Ponendo ora particolare attenzione, per semplicità espositiva e di analisi, all'accordo con gli USA, può essere immediatamente rilevato come la definizione di PNR sia esattamente identica in tutti i testi degli accordi, fondati sul richiamo delle Linee Guida ICAO. Sotto questo profilo quindi sembra logico presumere che le stesse carenze in termini di chiarezza e precisione nella identificazione dei dati da trasferire rilevate nel Parere ben potrebbero essere allo stesso modo riproposte anche con riferimento all'accordo con gli USA. Analizzando poi gli scopi indicati a giustificazione dell'accesso ai dati da parte di autorità di *law enforcement* del Paese terzo, si può notare come il testo dell'accordo UE-USA

[127] Si veda in particolare la nota 96, nella quale è illustrato brevemente il contenuto dell'accordo vigente con gli USA.

[128] C. KUNER, *International agreements, data protection and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, op. cit., p. 14.

contenga disposizioni che, confrontate a quelle della bozza di accordo con il Canada, appaiono molto meno precise, chiare e circostanziate, portando quindi a ritenerle non limitate allo stretto necessario[129].

Altri profili problematici emergono sia con riferimento al trattamento di dati sensibili[130] sia alla mancata differenziazione delle modalità di conservazione e accesso ai PNR a seconda della scansione temporale, come evidenziata dalla Corte nel *Parere 1/15*. Non può non essere poi rilevato come alcune disposizioni dell'accordo esistente garantiscano un livello di tutela della privacy e della protezione dei dati addirittura inferiore rispetto a quanto previsto nella bozza di accordo con il Canada: basti pensare al fatto che i dati PNR negli USA non vengono mai distrutti, neppure al termine del periodo di conservazione nella banca dati dormiente. Per quanto venga previsto l'obbligo di anonimizzazione dei dati, in modo da impedire qualsiasi possibilità di ripersonalizzarli, è chiaro come questa misura abbia un impatto invasivo sui diritti fondamentali dei passeggeri oltre quanto strettamente necessario: se nel *Parere 1/15* i giudici di Lussemburgo hanno chiarito la necessità di limitare la conservazione dei PNR dopo la partenza del passeggero ai soli casi in cui sussistano elementi oggettivi idonei a comprovare rischi in termini di lotta al terrorismo o reati gravi di natura transnazionale, una conservazione illimitata dei dati PNR, pur se anonimizzati, sembra a maggior ragione non poter superare indenne il test di proporzionalità della Corte. Il medesimo ragionamento può essere esteso alle disposizioni che nell'accordo vigente con gli USA regolano la possibilità, da parte delle autorità statunitensi, di trasferire

[129] L'art. 4 co. 2 dell'accordo UE-USA vigente, stabilisce che "I PNR possono essere usati e trattati caso per caso se necessario in vista di una minaccia grave e per salvaguardare gli interessi vitali di una persona o se disposto dall'autorità giurisdizionale"; la bozza di accordo UE-Canada esaminata dalla CGUE invece prevedeva che: "In circostanze eccezionali l'autorità canadese competente può trattare i dati PNR, se necessario, per salvaguardare l'interesse vitale di una persona, come in caso di rischio di morte o lesione grave oppure rischio grave per la salute pubblica, in particolare secondo quanto previsto da norme internazionalmente riconosciute. Il Canada inoltre può trattare i dati PNR, caso per caso, al fine di a) garantire il controllo o la responsabilità della pubblica amministrazione, oppure b) conformarsi ad una citazione in giudizio, un mandato di arresto o un ordine emesso da un'autorità giudiziaria" (art. 3, co. 4 e 5). Si può notare dunque come la norma inserita nella bozza risulti molto più chiara e precisa (usando i termini della Corte) rispetto a quanto previsto dall'accordo con gli Stati Uniti. L'art. 4, co. 5 peraltro è stato considerato dai giudici della Corte come troppo vago e generico per soddisfare i requisiti di chiarezza e precisione imposti e come non limitato a quanto strettamente necessario per conseguire l'obiettivo perseguito (par. 181). Viene da chiedersi quindi se le disposizioni attualmente vigenti per il trasferimento di PNR con gli Stati Uniti non siano destinate allo stesso giudizio.

[130] L'art. 8 della bozza di accordo con il Canada e l'art. 6 dell'accordo vigente con gli USA sono molto simili tra loro, prevedendo entrambi la possibilità di trasferimento di dati sensibili, pur con l'adozione di specifiche tutele: entrambi infatti stabiliscono che il trattamento di tale speciale categoria di dati personali deve essere valutato caso per caso in circostanze eccezionali di pericolo per la vita di una persona o di rischio di grave lesione dei diritti fondamentali; entrambi prevedono che tali dati siano cancellati (entro 15 giorni nella bozza di accordo con il Canada mentre l'accordo vigente con gli USA prevede un termine di 30 giorni dalla ricezione dei dati). La posizione della Corte in merito è stata tuttavia, come si è già sottolineato, estremamente chiara e netta: "(..) Qualsiasi misura basata sul postulato secondo cui una o più caratteristiche figuranti all'art. 2, lett. e), dell'accordo previsto potrebbero, di per sé stesse e indipendentemente dal comportamento individuale del viaggiatore interessato, essere rilevanti rispetto alla finalità dei trattamenti dei dati PNR, ossia la lotta al terrorismo e ai reati gravi di natura transnazionale, violerebbe i diritti garantiti agli articoli 7 e 8 della Carta, letti in combinato disposto con l'art. 21 della stessa. In considerazione del rischio di un trattamento di dati contrario all'art. 21 della Carta, un trasferimento dei dati sensibili verso il Canada richiederebbe una giustificazione precisa e particolarmente solida, vertente su motivi diversi dalla protezione della sicurezza pubblica contro il terrorismo e i reati gravi di natura transnazionale. Orbene, nella fattispecie, una siffatta giustificazione manca. (..) Alla luce delle valutazioni figuranti ai due punti precedenti, occorre constatare che gli articoli 7, 8 e 21 nonché l'art. 52, par. 1, della Carta ostano sia al trasferimento dei dati sensibili verso il Canada sia alla disciplina negoziata dall'Unione con tale Stato terzo delle condizioni relative all'uso e alla conservazione di siffatti dati da parte della autorità del medesimo Stato terzo" (par. 164-167, *Parere 1/15*). Pare chiaro dunque che l'art. 6 dell'accordo con gli USA non rispetti i criteri stabiliti dalla giurisprudenza della Corte, prevedendo misure simili, se non persino più problematiche di quelle della cassata bozza di accordo con il Canada: tale disposizione infatti stabilisce addirittura la conservazione dei dati sensibili "per il periodo prescritto dalla legislazione statunitense ai fini di un'indagine, azione penale o esecuzione specifica" (art. 6, par. 10), estendendo ulteriormente i limiti temporali di *retention* di tale delicatissima categoria di dati.

i PNR ad ulteriori Stati terzi: anche in questo caso infatti le previsioni della bozza di accordo con il Canada, ritenute eccedenti i limiti di quanto strettamente necessario, risultano maggiormente tutelanti[131].

Da questa breve analisi è possibile comprendere come molti aspetti della attuale disciplina che regola il trasferimento dei PNR in USA – e similmente quella riguardante lo scambio di dati con l'Australia – non risultino sufficientemente chiari, precisi e limitati allo stretto necessario alla luce dei requisiti e dei principi fissati dalla CGUE: la gran parte delle criticità rilevate nella bozza di accordo con il Canada ben potrebbero essere individuate anche nell'accordo vigente con gli Stati Uniti, con il risultato di poter portare ad una dichiarazione di invalidità dell'accordo e della connessa decisione di adeguatezza. Essendo ormai ampiamente decorsi i termini di annullamento, la validità di questi risalenti accordi e delle decisioni relative potrebbe essere portata alla valutazione della Corte mediante rinvio pregiudiziale[132] da parte di una Corte nazionale e, in tale caso, si è propensi ad affermare che l'esito del vaglio dei giudici di Lussemburgo sarebbe negativo: una "traslazione" dei principi affermati con riferimento alla bozza di accordo UE-Canada all'analisi degli accordi vigenti potrebbe pregiudicare e minacciare dunque la sussistenza di questi ultimi[133]. Si può discutere certamente sul fatto che la CGUE si sia pronunciata in merito al trasferimento dei dati PNR in un contesto del tutto particolare e che cioè, dovendo decidere su una bozza di accordo e in via preventiva, la Corte stessa si sia sentita meno vincolata e dotata di maggiore 'spazio di manovra', trovandosi dinnanzi ad un accordo non ancora vigente e potendo dunque prendere una decisione che non avrebbe avuto l'effetto immediato e diretto di modificare la situazione esistente; ciò potrebbe far presumere che, nel caso in cui i giudici europei

[131] Sul punto l'accordo con gli USA, all'art. 17, stabilisce che: "Gli Stati Uniti possono trasferire i PNR alle autorità governative competenti di paesi terzi solo ai sensi di disposizioni conformi al presente accordo e solo previo accertamento che l'uso previsto dal destinatario è in linea con tali disposizioni. Salvo in casi di emergenza, i trasferimenti successivi sono effettuati in conformità di intese esplicite che contemplano disposizioni a tutela dei dati personali analoghe a quelle applicate dal DHS ai PNR secondo il presente accordo. I PNR sono scambiati solo nei casi oggetto di esame o di indagine"; è chiaramente evidente la differenza con la disciplina predisposta all'art. 19 della bozza di accordo che prima di tutto affermava: "Il Canada provvede affinché l'autorità canadese competente non comunichi i dati PNR ad autorità governative di paesi diversi dagli Stati membri dell'UE, a meno che non siano rispettate le seguenti condizioni: a) le mansioni svolte dalle autorità governative a cui sono comunicati i dati PNR sono direttamente connesse all'ambito di applicazione dell'art. 3; b) i dati PNR sono comunicati solo caso per caso; c) i dati PNR sono comunicati solo se necessario ai fini stabiliti dall'art. 3; è comunicato solo il numero minimo necessario di dati PNR; e) l'autorità canadese competente ha accertato che: l'autorità straniera che riceve i dati PNR applica norme di protezione equivalenti a quelle disposte dal presente accordo, conformemente agli accordi e alle intese che contengono dette norme, oppure l'autorità straniera applica le norme di protezione dei dati PNR concordate con l'Unione europea".

[132] Nel caso C-266/16, *The Queen, Western Sahara Campaign Uk v Commissioners for Her Majesty's Revenue and Customs and Secretary of State for Environment, Food and Rural Affairs*, la CGUE è stata chiamata a decidere, mediante rinvio pregiudiziale, sulla validità dell'accordo di partenariato nel settore della pesca, concluso tra CE e Regno del Marocco, approvato e attuato dal Reg. (CE) 746/2006 e da successive decisioni adottate dal Consiglio. In quel caso, la CGUE ha affermato con chiarezza che: "La Corte è competente, sia nell'ambito di un ricorso per annullamento sia in quello di una domanda di pronuncia pregiudiziale, a valutare se un accordo internazionale concluso dall'UE sia compatibile con i trattati (v. in tal senso, parere 1/75 (Accordo OCSE – Norma sulle spese locali), dell'11 novembre 1975, EU:C:1975:145, p. 1361) e con le norme di diritto internazionale che, conformemente agli stessi, vincolano l'Unione. (..) Pertanto, occorre ritenere che, nell'ipotesi in cui, come nel caso di specie, alla Corte sia deferita una domanda di pronuncia pregiudiziale vertente sulla validità di un accordo internazionale concluso dall'Unione, tale domanda debba essere intesa come riferita all'atto con il quale l'Unione ha concluso un tale accordo (v. per analogia, sentenze del 9 agosto 1994, Francia/Commissione, C-327/91, EU:C:1994:305, punto 17 e del 3 settembre 2008, Kadi e Al Barakaat International Foundation/Consiglio e Commissione, C-402/05 P e C-415/05 P, EU:C:2008:461, punti 286 e 289). In considerazione degli obblighi dell'Unione esposti ai punti 46 e 47 della presente sentenza, il controllo di validità che la Corte può essere indotta ad operare in un contesto del genere può nondimeno vertere sulla legittimità di tale atto alla luce del contenuto stesso dell'accordo internazionale in questione" (par. 48-50).

[133] Sul punto tra gli altri X. TRACOL, *Opinion 1/15 of the Grand Chamber date 26 July 2017*, op. cit, ma anche MENDEZ che afferma con chiarezza come: "there is no difficulty in establishing that the two existing PNR agreements do not meet the privacy and data protection standards outlined in Opinion 1/15", in *Opinion 1/15: the Court of Justice meets PNR data (again!)*, op. cit., p. 816.

fossero chiamati a valutare la conformità di accordi già in vigore, l'approccio potrebbe essere più flessibile e maggiormente cauto. È tuttavia da sottolineare come, di fronte alla giurisprudenza europea sino ad ora analizzata, che non ha mancato di assumere decisioni dal forte impatto quali la sentenza *DRI* sul fronte interno e la pronuncia *Schrems* sul fronte esterno, risulti difficile sostenere che i principi fissati nel *Parere 1/15*, richiamanti la previa giurisprudenza, possano essere messi da parte in occasione del vaglio di un accordo, seppure già vigente, come quello con gli USA.

Resta comunque oggetto di dibattito e di riflessione la possibilità ed opportunità di utilizzare i criteri delineati dalla Corte quali linee guida per la stesura di un modello di accordo da sottoporre a tutti gli Stati terzi che dovessero decidere di intraprendere iniziative in tal senso con l'UE: ciò potrebbe anche indurre le Istituzioni europee a considerare l'adozione di una strategia unitaria e globale, che superi cioè l'approccio bilaterale sino ad ora seguito; in questo senso, l'idea di definire standard a livello internazionale di protezione dei dati e di tutela della riservatezza può certamente rappresentare una soluzione alle problematiche che attualmente l'UE sta affrontando[134]. Sembra andare in questa direzione la 'Decisione del Consiglio, relativa alla posizione da adottare a nome dell'Unione europea in sede di Consiglio dell'Organizzazione per l'aviazione civile internazionale in merito alla revisione dell'allegato 9 ("Facilitazioni"), capo 9, della convenzione relativa all'aviazione civile internazionale per quanto riguarda gli standard e le pratiche raccomandate sui dati del codice di prenotazione'[135], nella quale si vuole promuovere, mediante l'adozione di una posizione unitaria degli Stati membri in sede di ICAO, una seria discussione a livello internazionale sugli standard di protezione dei dati in materia di PNR in modo che essi siano compatibili con la giurisprudenza della Corte e con la normativa dell'UE in materia.

4.3.3. – L'impatto del **Parere 1/15** *entro i confini dell'UE: la legittimità della Direttiva 2016/681 in materia di PNR e i rinvii pregiudiziali pendenti*

Giungendo infine all'analisi del terzo profilo, quello cioè relativo alla già più volte richiamata Direttiva (UE) 2016/681, si vuole mettere in evidenza come la posizione della Corte nel Parere in esame induca a riflettere non solo sulle conseguenze e sugli impatti potenziali rispetto agli accordi e alle decisioni di adeguatezza vigenti con Stati terzi ma anche sulla normativa europea stessa in materia di raccolta, conservazione e accesso ai dati PNR nel territorio dell'Unione. Se alcune disposizioni della Direttiva vengono infatti addirittura elogiate dai giudici di Lussemburgo, che ne citano il contenuto quale esempio positivo e modello cui ispirarsi[136], altre tuttavia non mancano di destare alcune

[134] Sul punto si legga anche il documento del Consiglio n. 10838/15: *Passenger Name Record (PNR) data to third countries: a global approach?*, nel quale il Consiglio riflette sulle possibili alternative a disposizione per ovviare alle difficoltà incontrate nel predisporre accordi bilaterali con Stati terzi, considerata la complessità delle trattative nonché il tempo e le risorse da investire in esse. Prestando particolare attenzione alla opzione di un accordo-modello, predisposto dalla Commissione, il Consiglio ne sottolinea però anche i limiti: "The model agreement can therefore be a model to be followed by the Commission that would streamline work, but it cannot be a "one-size-fits all solution". Regardless of the political prerogatives of the EU institutions to demand that the terms of an agreement be tailored to the specific (political, legal or other) situation of a third country, it is moreover doubtful that all third countries which are demanding PNR data from EU airline companies would be willing to enter into an agreement with the European Union under exactly the same terms. Thus a model agreement would have an indicative nature only. The model agreement would also have to be in line with the standards set in a future EU PNR Directive". Tale posizione del Consiglio riprende una previa Comunicazione della Commissione (13954/10 (COM(2010) 492 final) on the global approach to transfers of Passenger Name Record (PNR) data to third countries, accolta positivamente dal Gruppo di lavoro Art. 29 (622/10/EN WP 178), che criticava però, alla base, l'assunto della necessità reale e dunque della utilità di un sistema di trasferimento dati PNR per scopi securitari.

[135] Decisione (UE) 2019/2107 del 28 novembre 2019.

[136] Si richiama in questo senso il riferimento svolto dalla Corte alla disciplina in materia di dati sensibili contenuta nella Direttiva (UE) 2016/681 (*Parere 1/15*, par. 166).

perplessità. Pur non volendo in questa sede entrare nel dettaglio di tutte le misure contenute nella normativa europea[137], è necessario delinearne alcuni dei punti più rilevanti.

La Direttiva ha ad oggetto il trasferimento di PNR verso uno o più Stati membri ad opera delle compagnie aeree, relativamente ai passeggeri di voli internazionali da e per l'UE: sono quindi esclusi dalla regolamentazione in esame i voli meramente infra-UE, che possono però essere sottoposti anch'essi agli obblighi e alla disciplina enucleata nella Direttiva sulla base di una decisione, eventuale e discrezionale, adottata da ciascuno Stato membro nella propria normativa interna di recepimento. La Direttiva, adottata nel 2016 ma che ha previsto un termine di tempo più ampio, scaduto il 25 maggio 2018, per l'attuazione a livello nazionale[138], impone agli Stati membri di istituire delle *Passenger Information Unit* (PIU) incaricate della conservazione e trattamento dei PNR, del loro trasferimento alle competenti autorità nazionali di *law enforcement* nonché dello scambio di informazioni con altri Stati membri e con Europol, mentre sono attribuiti significativi poteri di controllo alle Autorità nazionali garanti della protezione dei dati. Anche la Direttiva comunque prevede un lungo periodo di conservazione dei dati, della durata di 5 anni, al termine del quale viene prevista la cancellazione, stabilendo però una prima procedura di anonimizzazione da effettuarsi dopo sei mesi dalla raccolta; deve essere sin da subito evidenziato come, anche nella normativa dell'UE, non siano previste differenziazioni quando alla disciplina della conservazione e accesso sulla base della scansione temporale ovvero a seconda che ci si riferisca a momenti precedenti, durante o successivi all'arrivo del volo nel territorio di uno Stato membro. Proprio quest'ultimo sembra essere l'aspetto maggiormente problematico di tale disciplina: se infatti, a seguito del *Parere 1/15* può ormai definirsi accettato il meccanismo di trasferimento generalizzato di PNR e di una loro analisi automatizzata precedente all'arrivo del passeggero, senza che sia presente in capo ad esso alcun sospetto o connessione con attività criminose – operazioni queste ritenute *per se* non eccedenti i limiti dello stretto necessario –, deve essere tuttavia considerata cruciale la predisposizione di criteri che impongano la sussistenza di elementi oggettivi tali da rendere giustificata e proporzionata la conservazione di dati e l'accesso agli stessi anche durante e dopo la permanenza del passeggero entro i confini dell'UE. Se dunque vi sono molti punti rispetto ai quali il legislatore europeo ha dimostrato di tenere in considerazione i rilievi emersi dalla giurisprudenza della CGUE – che al momento dell'adozione della Direttiva erano rappresentati dalla sentenza *DRI* e dal caso *Schrems* –, ad esempio vietando la raccolta e l'utilizzo di dati sensibili, o predisponendo una anonimizzazione e una successiva cancellazione dei dati (art. 9) o ancora imponendo un intervento umano dinnanzi ai risultati di analisi automatizzate (art. 12), non possono essere ignorate tuttavia anche talune carenze sotto il profilo della base giuridica[139] nonché della proporzionalità e stretta necessità della conservazione dei PNR, che fanno inevitabilmente dubitare circa la legittimità della Direttiva e della sua capacità di resistere indenne al vaglio della Corte[140].

---

[137] Per una analisi approfondita si rimanda a E. SAULNIER-CASSIA, *La Directive (UE) 2016/681: miscellanies sur l'utilisation des données des données des dossier passagers dans l'Unione Européenne du PNR eurpéen*, in C. CHEVALLIER GOVERS, *L'èchange des données dans l'Espace de liberté, de sécurité et de Justice de l'Unione Européenne*, Mare & Martin, 2017.

[138] Per uno studio dettagliato del delicato quanto lungo iter legislativo che ha portato all'approvazione della Direttiva, la cui prima proposta risale al 2007 e che ha poi avuto forte spinta 'propulsiva' a seguito della nuova ondata di attentati terroristici registratasi nel 2015, si legga F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella Direttiva PNR?*, op. cit. Nella ricostruzione dell'autore vengono bene messe in luce le perplessità e ritrosie del Parlamento nell'accettare una forma di raccolta indiscriminata e generalizzata di dati personali, la cui necessità e i cui vantaggi erano e sono tuttora poco chiari e solo genericamente indicati.

[139] Anche in questo caso infatti si sottolinea come la base giuridica della Direttiva sia stata individuata negli art. 82 e 87 TFEU, il che fa sorgere alcuni dubbi quanto alla correttezza della scelta dell'art. 82 alla luce delle osservazioni della CGUE nel *Parere 1/15*, che, come più volte richiamato, ne ha affermato l'erroneità.

[140] Di tale opinione, tra i molti, E. CARPANELLI, N. LAZZERINI, *PNR: problems not resolved? The EU PNR conundrum, after Opinion 1/15 of the CJEU*, in *Air and Space Law*, 42, 2017; C. GRAZIANI, *PNR EU-Canada, la Corte di giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali,* in *DPCE Online*, 4,

Alla luce di queste considerazioni, alcune ONG nonché taluni cittadini europei, si sono attivati dinnanzi alle Corti statali per contestare la legittimità della normativa interna adottata in attuazione della Direttiva in materia di PNR, con l'obiettivo ultimo di ottenere dai giudici nazionali un rinvio pregiudiziale alla CGUE in grado di condurre ad una valutazione della compatibilità della Direttiva PNR qui esaminata rispetto al diritto dell'UE e alla Carta di Nizza[141]. Queste azioni si sono dimostrate efficaci: due sono infatti i rinvii pregiudiziali al momento pendenti dinnanzi alla CGUE ed aventi ad oggetto proprio la Direttiva 2016/681, il primo su rinvio della Corte costituzionale belga (C-817/19, *Lingue des droits humains c. Conseil des Ministres*, promosso il 31 ottobre 2019) e il secondo azionato invece dal Tribunale circoscrizionale di Colonia, il 20 gennaio 2020 (C-148/20, *AC c. Deutsche Lufthansa AG*).

Sebbene con riferimento alla controversia sorta dinnanzi ai giudici costituzionali belgi verrà dedicato ampio spazio nel Capitolo II, Parte III di questo elaborato, nel quale ci si concentrerà anche sull'analisi della legge nazionale belga di trasposizione della Direttiva PNR, si vogliono in questa sede brevemente riportare alcune considerazioni svolte dalla Corte del rinvio: quest'ultima, su ricorso per annullamento[142] presentato dalla ONG Ligue des droits humains avverso la *Loi du 25 décembre 2016, relative au traitement des données des passegers*, ha messo in evidenza infatti significative problematiche circa la compatibilità rispetto alla Carta di Nizza della disciplina nazionale in materia di trasferimento, raccolta, conservazione e accesso ai PNR e dunque della stessa disciplina dell'UE. Ricostruendo con grande attenzione la giurisprudenza della CGUE, a partire dalla sentenza *DRI* sino al *Parere 1/15*, la Corte costituzionale belga ha rinvenuto numerosi parallelismi tra quanto affermato dai giudici di Lussemburgo con riferimento alla bozza di accordo UE-Canada e quanto contenuto nella Direttiva PNR: così, ad esempio, i criteri di chiarezza e precisione quanto alla definizione di codici di prenotazione e alle informazioni comprese, delineati dalla CGUE nel *Parere 1/15*, vengono ritenuti applicabili e trasponibili anche al caso di specie. Proprio sulla base di tali parallelismi e similitudini, nonché vagliando i punti critici già individuati dai giudici di Lussemburgo nel noto Parere, la Corte costituzionale ha reputato necessario rinviare alla Corte di giustizia, affinché questa determini se la definizione proposta dal legislatore dell'UE, e ripresa dalla normativa nazionale belga, possa considerarsi limitata allo stretto necessario. Quello definitorio tuttavia non è l'unico aspetto rimesso alla valutazione dei giudici di Lussemburgo: di grande rilievo infatti è il quesito n. 4, con il quale vengono promosse quelle questioni

---

2017, ma anche M. ZALNIERIUTE, *Developing a European standard for international data trasnfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *The modern law review*, 6, 2018; X. TRACOL, *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada*, op. cit. Interessante sul punto è notare come, già prima del *Parere 1/15*, fosse aperta una accesa discussione circa la legittimità della Direttiva in materia di PNR, letta alla luce delle sentenze *DRI* e *Schrems*: posizioni discordanti si rinvenivano tra chi, come Di Matteo (in *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella Direttiva PNR?*, op. cit.) rinveniva la mancata conformità della normativa rispetto al diritto dell'UE (anche se l'autore fondava la propria argomentazione principalmente sulla natura indiscriminata del trasferimento, conservazione e trattamento dei dati e delle carenze in termini di necessità e proporzionalità del sistema di trasferimento PNR *per se*, aspetto che pare ormai superato e validato dal *Parere 1/15* della CGUE), e di chi invece considerava la Direttiva del tutto legittima e le sue disposizioni proporzionate e limitate allo stresso necessario (D. LOWE, *The European Union's passenger name record data Directive 2016/681: is it fit for the purpose?*, op. cit.).

[141] Sul punto si legga S. RODA, *Shortcomings of the PNR Directive in light of Opinion 1/15 of the Court of Justice of the European Union*, in *European data protection law review*, 6, 2020.

[142] Si vuole solo preliminarmente ricordare come la Corte costituzionale belga sia deputata ad effettuare, oltre ad un controllo di costituzionalità di tipo concreto mediante rinvio di una questione pregiudiziale, anche un controllo astratto mediante ricorso per annullamento. Quest'ultimo può essere promosso dal Consiglio dei ministri, dagli organi esecutivi delle Regioni e delle Comunità, dal Presidente dell'Assemblea legislativa (nazionale, regionale o comunitaria) nonché, a seguito di riforma intervenuta nel 1988, anche da persone fisiche e giuridiche. Il termine temporale per la presentazione del ricorso è di sei mesi dalla pubblicazione della normativa da impugnare. Sul punto si rimanda comunque più ampiamente al Capitolo II, Parte III, dedicato proprio all'analisi della disciplina normativa belga e alle vicende giurisprudenziali in materia di *data retention*.

già sottolineate nella lettura critica sopra svolta e cioè se un sistema di raccolta, trasferimento e trattamento generalizzato di PNR, che riguarda tutti i passeggeri che si servono di un determinato mezzo di trasporto a prescindere da elementi obiettivi che consentano di creare una connessione tra il soggetto cui i dati si riferiscono e un rischio per la sicurezza pubblica, sia da ritenersi compatibile agli artt. 7, 8 e 52 della Carta di Nizza. In altre parole, ripercorrendo quanto affermato nelle pronunce *DRI* e *Tele2*, i giudici belgi chiedono se i principi e requisiti, sanciti in tali storiche decisioni con riferimento alla *bulk retention* di metadati, siano applicabili e trasponibili anche ai regimi di trasferimento e trattamento parimenti generalizzato ed indiscriminato avente ad oggetto i PNR, quale quello disposto dalla Direttiva PNR. Altro elemento di criticità viene rilevato nell'utilizzo di sistemi di controllo preventivo – in un momento antecedente all'arrivo del passeggero nel territorio dello Stato membro – dei PNR su base automatizzata, mediante il raffronto del codice di prenotazione con informazioni contenute in banche dati e l'utilizzo di criteri di valutazione prestabiliti dall'UIP nazionale. Vista la delicatezza di tali operazioni e la mancanza di specifiche indicazioni a livello europeo quanto al contenuto di tali controlli sistematici, in grado di prevenire fenomeni di *bias* degli strumenti automatizzati – che possono anche risultare in pratiche discriminatorie –, viene chiesto alla CGUE di determinare se l'analisi preliminare dei PNR, così come prevista dalla Direttiva, risulti limitata a quanto strettamente necessario nonché accompagnata da disposizioni chiare e precise. Anche quanto alla durata della conservazione dei PNR, infine, vengono messi in evidenza i rischi che una *retention* significativamente protratta nel tempo in banche dati dall'ampia portata può comportare (ad esempio il pericolo di c.d. *function creep*, già richiamato nel Capitolo I, Parte I) rispetto ai diritti alla vita privata e alla protezione dei dati, anche in considerazione dell'assenza di qualsiasi distinzione, basata su elementi oggettivi, tra i passeggeri interessati, a secondo del fatto cioè che il controllo preliminare abbia o meno individuato una connessione tra l'utente ed una minaccia per la sicurezza.

Il secondo rinvio, sopra citato, promosso dai giudici tedeschi[143], presenta aspetti di forte somiglianza con il rinvio della Corte costituzionale belga appena analizzato: anche in tale caso, infatti, viene chiesto l'intervento della CGUE al fine di determinare la compatibilità della Direttiva PNR rispetto agli artt. 7 e 8 della Carta di Nizza, in particolare sotto quattro differenti profili; il primo attiene alla definizione di PNR, rispetto alla quale i giudici del rinvio esprimono, similmente ai colleghi belgi, dubbi quanto ai caratteri di certezza, chiarezza e precisione; il secondo quesito invece, ben più delicato, ha ad oggetto la proporzionalità della Direttiva stessa e del sistema di trasferimento di PNR, alla luce della assenza di una differenziazione oggettiva nelle operazioni di raccolta dei codici di prenotazione: la normativa dell'UE infatti prevede la raccolta e conservazione di tutti i codici di prenotazione, indipendentemente da valutazioni quanto al livello di rischio concreto presente nel Paese di partenza del volo o alla pericolosità della passeggero, così che non solo non vengono specificati criteri oggettivi in grado di stabilire un nesso tra conservazione e finalità perseguite ma neppure vengono previste norme chiare sulle condizioni giuridiche che governano la fase di *matching* cioè di confronto tra i PNR e le banche dati o la scelta e le caratteristiche degli indicatori impiegati per il primo controllo automatizzato. I dubbi quanto alla proporzionalità delle misure disposte nella Direttiva PNR inoltre si estendono anche alla durata della conservazione dei codici di prenotazione e alla disciplina relativa al trasferimento di PNR da parte degli Stati membri verso Stati terzi.

Come ben si comprende, dunque, entrambi i rinvii pongono in discussione le basi stesse e la compatibilità dello strumento del trasferimento, raccolta, conservazione e accesso ai codici di

[143] La controversia dinnanzi al Tribunale circoscrizionale di Colonia ha avuto origine da una azione inibitoria promossa dal ricorrente AC avverso la compagnia aerea Lufthansa: l'obiettivo del ricorrente era quello di impedire al vettore aereo di trasferire i propri dati PNR all'ufficio federale tedesco della polizia, sulla base della ritenuta incompatibilità con il diritto dell'UE e la Carta di Nizza della normativa tedesca in materia di trattamento dei dati dei passeggeri aviotrasportati (*Gesetz uber die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie EU 2016/681* del 10 giugno 2017), adottata in attuazione alla Direttiva PNR.

prenotazione, basando i dubbi e le perplessità sottoposte alla CGUE proprio sui principi e requisiti affermati sia nelle sentenze in materia di *data retention* che nel *Parere 1/15*. Gli ampi richiami a tali pronunce da parte dei giudici del rinvio sono pertanto significativi quanto alle difficoltà applicative ed interpretative riscontrate da legislatori e Corti nazionali, che affondano le radici in quelle criticità e – più o meno apparenti – divergenze che emergono dalla giurisprudenza della CGUE in tale complesso ambito.

Si vuole infine sottolineare come, anche dinnanzi ai rinvii pendenti, la Commissione europea abbia promosso un approccio piuttosto cauto: l'art. 19 della Direttiva PNR prevede l'onere in capo alla Commissione stessa di procedere al riesame di tutti gli elementi della normativa, entro due anni dalla sua entrata in vigore, e di predisporre una relazione al Parlamento e al Consiglio sul punto. Sin dal 2019, in risposta ad una interpellanza parlamentare posta proprio in merito alla Direttiva PNR, il Commissario Avramopoulos aveva affermato che: "The review of the PNR Directive is currently under preparation and will provide an opportunity to look into all the issues relevant for the implementation of the directive by Member States. Any potential subsequent Commission proposal for a revision of the PNR legal framework would be preceded by a thorough assessment. This assessment would look into all the relevant aspects, including the applicable EC law and relevant rulings of the European Court of Justice on fundamental rights to data protection and privacy, as well as the principles of subsidiarity and proportionality"[144]. Nella successiva relazione predisposta dalla Commissione[145], quest'ultima ha poi concluso con l'affermare non solo che la Direttiva "contribuisce positivamente al suo obiettivo principale che consiste nel garantire l'istituzione di sistemi PNR efficaci negli Stati membri come strumento per combattere il terrorismo e i reati gravi", ma anche che "non debba essere proposta alcuna modifica", neppure alle luce delle criticità rilevate dai giudici nazionali nei rinvii analizzati. Con riferimento a questi ultimi, tuttavia, la Commissione ha aggiunto però che una eventuale decisione di "revisione [della Direttiva PNR] si baserà anche sull'esito della domanda di pronuncia pregiudiziale attualmente pendente dinanzi alla Corte di giustizia" (p. 13). Con tale ultima precisazione, dunque, la Commissione ha riconosciuto il potenziale impatto che l'intervento dei giudici di Lussemburgo potrebbe avere rispetto alla validità e legittimità della Direttiva stessa, e ha preso atto della necessità di attendere l'esito dei delicati rinvii sopra esaminati per disporre ulteriori interventi e modifiche alla disciplina esistente.

5. – Le ripercussioni della giurisprudenza della CGUE in materia di trasferimento dati verso gli Stati terzi sulla disciplina della **data retention** *nel contesto interno all'UE e gli effetti nella 'dimensione esterna' all'UE*

Come risulta dalla ricostruzione del quadro normativo e giurisprudenziale sino ad ora svolta, gli sviluppi attesi nel prossimo futuro sono molteplici ed interessano sia l'intervento delle Istituzioni europee (con riferimento ad esempio a possibili modifiche della Direttiva in materia di PNR o ancora ai processi di negoziazione di nuovi accordi o all'adozione di decisioni di adeguatezza), che della Corte, chiamata a pronunciarsi su rilevanti e delicate questioni, la cui risoluzione avrà certamente un forte impatto non solo nella dimensione interna europea bensì anche in quella esterna, delle relazioni internazionali.

[144] Risposta E-002461/2019(ASW) fornita dalla Commissione (Comm. Avramopoulos) al Parlamento europeo il 29 ottobre 2019.

[145] COMMISSIONE EUROPEA, *Relazione sul riesame della Direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*, COM(2020)305 final, luglio 2020.

Se è dunque difficile al momento prevedere tutti gli scenari che potranno aprirsi nei prossimi anni, risulta tuttavia necessario svolgere alcune osservazioni che, per quanto non definitive, cercano di elaborare utili spunti di riflessione seguendo due principali tematiche, tutte strettamente connesse tra loro: la prima è volta a tratteggiare le connessioni e le possibili ripercussioni delle pronunce in materia di trasferimento dei dati rispetto alla problematica ancora del tutto attuale ed aperta della *data retention* nel contesto europeo interno; la seconda pone particolare attenzione invece agli effetti della giurisprudenza europea in materia di protezione dei dati e di tutela della riservatezza nella dimensione 'esterna' all'UE stessa, valutando quindi le incidenze e le conseguenze prodotte nelle relazioni con gli Stati terzi e negli Stati terzi stessi, per interrogarsi sulla efficacia ma anche sulle persistenti criticità dell'approccio europeo sul fronte esterno.

5.1 – Dalle sentenze DRI *e* Tele2 *alla decisione* Schrems *e al* Parere 1/15*, tra punti di contatto e obbligate distinzioni*

Partendo dunque con il primo ordine di osservazioni, gli effetti e i legami tra la decisione *Schrems* e il *Parere 1/15* da un lato e la *DRI* e *Tele2* dall'altro, sono molteplici ed emergono non solo per il costante richiamo dei principi delineati in tali ultime sentenze nella giurisprudenza successiva della CGUE: pur con le dovute distinzioni, che non mancheranno di essere sottolineate, tutte queste quattro pronunce riguardano forme di sorveglianza generalizzata, perpetrata mediante misure normative che prevedono la raccolta, conservazione e accesso ad una grande mole di dati (sia con riferimento al contenuto, sia ai soli metadati); le quattro decisioni mostrano tutte elementi e riflessioni capaci di integrarsi tra loro, ad esempio creando un distinzione più chiara, per quanto ancora critica sotto certi profili, tra 'compromissione' del nucleo essenziale dei diritti alla privacy e alla protezione dei dati e lesioni gravi ma non idonee ad incidere sull'essenza dei diritti richiamati; una integrazione che si riscontra anche tra i principi e criteri delineati nella dimensione interna dell'azione del diritto dell'UE e quella esterna, che si mostrano dunque fortemente intrecciate e i cui effetti si propagano l'una nella direzione dell'altra.

5.1.1. – La lesione dell'essenza dei diritti fondamentali: dubbi e perplessità sulla lettura promossa dalla CGUE

Quando al profilo, già anticipato, afferente alla essenza dei diritti fondamentali, è evidente come prima delle sentenze *DRI* e *Schrems* non fosse affatto chiaro cosa si dovesse intendere per nucleo essenziale dei diritti di cui agli artt. 7 e 8 della Carta di Nizza e quali situazioni fattuali ne determinassero la lesione. In questo senso le due pronunce richiamate si completano a vicenda, mostrando chiaramente il punto di vista della CGUE, che pure non è esente da criticità. La visione proposta dai giudici di Lussemburgo è quella che crea una simmetria tra ingerenza nel contenuto delle comunicazioni e lesione dell'essenza del diritto: tale connessione, delineata in primis nella decisione *DRI*, è stata poi meglio esemplificata ed applicata nel caso *Schrems* nel quale proprio l'ingerenza in maniera indiscriminata e generalizzata[146] nel contenuto dei dati provenienti dall'UE da parte delle autorità pubbliche statunitensi ha determinato la lesione del contenuto essenziale del diritto alla riservatezza (e, come si dirà meglio *infra*, solo di questo diritto e non anche di quella alla protezione dei dati). Tale visione conferma peraltro

[146] "For the sake of avoiding misunderstandings, it should be emphasized that the access of public authorities to the content of electronic data as such does not trigger the essential core of privacy: it is only if there is indiscriminate blanket access by the public authorities to the content of electronic communications that a violation of the essence of the right to privacy can be found", T. OJANEN, *Making the essence of fundamental right real: the Court of Justice of the EU clarifies the structure of fundamental rights under the Charter*, op. cit., p. 327.

la struttura del ragionamento e dello scrutinio operato dai giudici di Lussemburgo che vede prima la valutazione circa la presenza di una compromissione dell'essenza del diritto e poi, solo in caso di esito negativo, una attuazione del test di proporzionalità; ciò ha portato pertanto ad affermare che una misura normativa che rispetti l'essenza del diritto fondamentale non è necessariamente ed automaticamente rispettosa del principio di proporzionalità, come mostrato prima nel caso *DRI* e successivamente nel caso *Tele2*[147].

Questa coerenza e complementarietà delle pronunce richiamate può apparire, ad un primo sguardo, idonea a determinare una distinzione del tutto chiara, logica e convincente circa quali misure pregiudichino o meno il contenuto essenziale dei diritti fondamentali alla privacy e protezione dei dati. Se si leggono tuttavia con maggiore attenzione le sentenze richiamate, emergono alcune fragilità e perplessità, sia da un punto di vista 'formale' che da un punto di vista 'sostanziale' e concreto. Sotto il primo aspetto, non viene innanzitutto mai chiarito dalla Corte cosa debba intendersi per 'contenuto essenziale': "it has been ambiguous as to whether the essence of fundamental rights under article 52 co 1 referes to the common and universal essence of a fundamental right or whether it can have a different meaning in each particular case"[148], potendosi quindi ritenere che una valutazione della lesione del nucleo essenziale basata sulla distinzione tra 'coinvolgimento' o meno del contenuto della comunicazione sia eccessivamente superficiale e semplicistica nonché troppo connessa al caso specifico, senza così che vengano fornite coordinate utili al legislatore per comprendere la *ratio* e il significato più ampio ed astratto di 'essenza' del diritto in analisi. Sotto il profilo 'sostanziale' si deve notare invece come la Corte nel *Parere 1/15* paia discostarsi dal criterio contenuto-metadato per verificare l'impatto sul nucleo essenziale dei diritti in gioco: nel Parere, infatti, i giudici ritengono che la bozza di accordo UE-Canada in materia di PNR non pregiudichi il nucleo essenziale del diritto di cui all'art. 7 della Carta di Nizza in quanto "anche se i dati PNR possono, eventualmente, rivelare informazioni molto precise sulla vita privata di una persona, la natura di dette informazioni è limitata ad alcuni aspetti di tale vita privata, relativi in particolare ai viaggi aerei tra il Canada e l'Unione", mentre con riferimento al diritto di cui all'art. 8 della Carta, il contenuto essenziale non risulta leso poiché l'accordo circoscrive le finalità di trattamento e stabilisce norme destinate a garantire "la sicurezza, la riservatezza e l'integrità di tali dati, nonché a tutelare dagli accessi e dai trattamenti illegali" (par. 150, *Parere 1/15*). Questa lettura sembra suggerire nuovi criteri di valutazione utili a determinare l'ingerenza o meno nell'essenza del diritto: questa volta infatti le considerazioni dei giudici si fondano sulla conformità al principio di *purpose limitation* e dunque sulla predisposizione o meno di specifiche e dettagliate finalità del trattamento, nonché sulla previsione di misure idonee a garantire la sicurezza del dato[149]. Ciò sembra suggerire che "in order to determine whether a measure compromises the essence of a fundamental right, one must not only examine the intensity, but also the extent, of the limitation at issue. A measure that limits the exercise of certain aspects of a fundamental right, leaving others untouched, or that only applies in a specific set of circumstances regarding the individual conduct of the person concerned, is not such as to compromise the essence of that fundamental right"[150]. Viene

[147] K. LENAERTS, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, in *German Law Journal*, 20, 2019, p. 781.

[148] M. TZANOU, *European Union regulation of transatlantic data transfers and online surveillance*, op. cit., p. 558. Della stessa opinione si legga anche: V. PFISTERER, *The Right to Privacy—A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, in *German Law Journal*, 20, 2019, che afferma: "the Court should move beyond what was stated and implied in the Digital Rights and Schrems cases and provide a more in-depth rationale as to why the measures in dispute compromise the respective essence of the right to privacy and right to protection of personal data", p. 733. Similmente sul punto: C. KUNER, *International agreements, data protection and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, op. cit.

[149] Così M. BRKAN, *The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning*, op. cit, p. 880.

[150] K. LENAERTS, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, op. cit., p. 782.

delineata quindi una interpretazione della 'essenza' del diritto fondamentale e dei criteri per determinarla, differente da caso a caso, mancando dunque, ancora una volta, una visione o una definizione che permetta di comprendere il concetto di 'nucleo essenziale' in maniera univoca.

Sempre sotto il profilo sostanziale, poi, non può non rilevarsi una certa contraddittorietà nella giurisprudenza della Corte che individua nella distinzione tra lesività del contenuto e del metadato l'elemento chiave per determinare l'ingerenza o meno nell'essenza del diritto: come si è già anticipato nel Capitolo II, tale criterio, che vede nella raccolta e accesso ai contenuti un maggiore ed inaccettabile pericolo per la vita privata degli individui, è da considerarsi ormai obsoleto se si ammette che anche i metadati sono in grado di fornire, se letti in maniera aggregata e vista la capacità delle nuove tecnologie di produrli in quantità elevatissima, una ampia panoramica della vita privata di un soggetto, delle sue abitudini e stili di vita, del tutto paragonabile a quanto è possibile scoprire mediante l'accesso al contenuto delle comunicazioni stesse[151]. Questa lettura sembra peraltro essere accettata dalla stessa Corte nella già analizzata sentenza *Tele2* quando afferma: "In particolare, tali dati (i metadati) forniscono gli strumenti per stabilire – come ha rilevato l'avvocato generale ai paragrafi 253, 254 e da 257 a 259 delle sue conclusioni – il profilo delle persone interessate, informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni" (par. 99, *Tele2*). In questo caso dunque i giudici di Lussemburgo sembrano equiparare l'ingerenza provocata dalla conservazione e trattamento di una grande mole di metadati a quella provocata dall'accesso, conservazione e utilizzo dei contenuti: una tale conclusione porterebbe a ritenere dunque sussistente, anche nel caso in cui si tratti di meri metadati, una lesione del nucleo essenziale del diritto alla vita privata. Questa logica conseguenza viene tuttavia smentita nel momento in cui la Corte, come si è analizzato e già rilevato nel Capitolo II, ritiene di escludere, sia nella sentenza *DRI* che nel caso *Tele2*, la presenza di una lesione del nucleo essenziale.

Una ulteriore criticità della giurisprudenza analizzata sul punto risiede infine nel mancato chiarimento di una distinzione tra lesione del nucleo essenziale del diritto alla riservatezza e di quello alla protezione dei dati: non può essere infatti ignorato come la sentenza *Schrems* faccia riferimento al solo diritto di cui all'art. 7 (oltre alla lesione del nucleo essenziale dell'art. 47, che è già stato richiamato). Questo aspetto, tutt'altro che formale, rivela una problematica, sottesa a tutte le pronunce sino ad ora oggetto di analisi, che risiede nella confusione e nella mancata chiara distinzione tra diritto alla vita privata e diritto alla protezione dei dati che, per quanto strettamente connessi, presentano distinzioni e peculiarità già evidenziate nel Capitolo I, Parte I[152].

---

[151] Indicativa in tal senso è l'affermazione di M. Hayden, ex Direttore della NSA e della CIA (richiamata da Ojanen, in *Making the essence of fundamental rights real: the Court of Justice of the EU clarifies the structure of fundamental rights under the Charter*, op. cit., p. 328) che ha statuito: "we kill people based on metadata. If you have enough metadata, you don't really need content"; ma si legga sul punto anche: D. COLE, *We kill people based on metadata*, in *The New York Review of Books*, 10 maggio 2014. Questa lettura, che attribuisce enorme rilevanza ai metadati, emerge anche dalla più recente giurisprudenza della Corte EDU nel caso *Big Brother Watch* che sarà oggetto di approfondita analisi nel prosieguo di questo lavoro. Merita essere qui preliminarmente sottolineato come la Corte EDU non abbia adottato un ragionamento che vede prima la valutazione della sussistenza di una lesione del nucleo essenziale e solo in caso negativo il vaglio di proporzionalità: nella propria giurisprudenza, infatti, la Corte di Strasburgo, anche nel caso di raccolta, conservazione e accesso indiscriminati al contenuto di comunicazioni, ha provveduto egualmente ad applicare il test di proporzionalità, come verrà analizzato in seguito. Questo è sottolineato non solo da Ojanen, nel contributo sopra richiamato, bensì anche da K. LENAERTS, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, op. cit., p. 788.

[152] "In the Schrems and Tele2 cases – and in contrast to the approach taken in the Digital Rights and PNR cases – the Court merged its analysis of the interference of the relevant measures with the right to privacy and the right to protection of personal data in a way that disallows the reader to discern the criteria governing, or relevant to, each one of the rights and how they unfold in the case at hand. (..) Seventeen years after the proclamation of the CFREU, the relationship between the right to privacy – Article 7 CFREU – and the right to protection of personal data – Article 8 CFREU – is still unclear. The recent landmark decisions contribute to the longstanding confusion about the distinction between the right to data protection and privacy", V. PFISTERER, *The Right to Privacy—A*

5.1.2. – Il sistema di trasferimento generalizzato e analisi automatizzata di PNR e la **bulk data retention** *di metadati a confronto*

Spostandosi dal discorso inerente all'essenza dei diritti fondamentali, per muover verso l'analisi delle ulteriori convergenze o divergenze e dei legami sussistenti tra le sentenze *DRI* e *Tele2* in materia di *data retention* e quelle in ambito di trasferimento dati al di fuori dei confini dell'UE, è necessario riprendere quanto già anticipato nei precedenti paragrafi: bisogna cioè riflettere sul come e se l'ammissione della conformità al diritto dell'UE di un sistema di raccolta, trasferimento e trattamento generalizzato e indiscriminato di dati PNR, come affermata nel *Parere 1/15*, abbia ripercussioni in materia di raccolta, trasferimento e trattamento generalizzato ed indiscriminato di metadati derivanti dalle telecomunicazioni elettroniche sul piano interno. Ci si deve interrogare, in altre parole, sulla portata della dichiarata tollerabilità di una forma di sorveglianza massiva (pur assistita necessariamente da una serie di garanzie e tutele molto rigorose) relativa alla totalità dei dati inerenti i passeggeri di voli aerei (sia da e per il Canada ma anche nella dimensione interna europea, sulla base della Direttiva in materia di PNR) e se tale presa di posizione possa essere letta come una 'rimodulazione' della previa giurisprudenza in materia di *data retention* nella quale era stata stabilita invece in maniera chiara l'incompatibilità con il diritto dell'UE, e con la Carta di Nizza in particolare, di sistemi di conservazione e accesso indiscriminato e generalizzato (c.d. *bulk data retention*).

Ripercorrendo le argomentazioni della Corte nel *Parere 1/15*, unitamente alle Conclusioni dell'Avvocato generale, si nota come venga affermata la necessità che "nel momento in cui le tecnologie moderne consentono alle pubbliche amministrazioni, in nome della lotta al terrorismo e alla criminalità transnazionale grave, di sviluppare metodi estremamente sofisticati di sorveglianza della vita privata degli individui e di analisi dei loro dati personali, la Corte si assicuri che le misure progettate, sia pure sotto forma di accordi internazionali previsti, riflettano un contemperamento equilibrato tra la preoccupazione legittima di preservare la sicurezza pubblica e quella, non meno fondamentale, che chiunque possa godere di un livello elevato di protezione della sua vita privata e dei propri dati" (Conclusioni Avvocato generale, par. 8). Del resto questa visione, poi confermata dalla Corte, accoglie i rilievi dei governi estone, francese, britannico e della Commissione stessa, che hanno ritenuto il carattere generalizzato ed indiscriminato dei sistemi di trasferimento e trattamento dei codici di prenotazione un elemento essenziale, intrinsecamente ed inscindibilmente radicato nella natura stessa del meccanismo di controllo del PNR che dunque non può essere messo in discussione a meno di negare il funzionamento e la sussistenza del meccanismo stesso: "se fosse autorizzata soltanto la trasmissione dei dati PNR riguardanti le persone già segnalate come costituenti un rischio per la sicurezza, l'obbiettivo di prevenzione non potrebbe essere così raggiunto" (par. 58, *Parere 1/15*). In altre parole viene abbracciata dalla Corte la teoria secondo la quale "In order for the suspect to emerge, everyone must be subject to surveillance"[153], accettando un sistema, come quello dei PNR, che ha come primario scopo quello di permettere di individuare soggetti potenzialmente pericolosi e prima non noti alle autorità di *law enforcement* (par. 187-197, *Parere 1/15*).

Ebbene questo non può che richiamare alla mente quanto trattato nei casi *DRI* e *Tele2*, nei quali in discussione era proprio il sistema di conservazione generalizzata ed indiscriminata di metadati relativi alle comunicazioni elettroniche, che, anche in quel caso e similmente al sistema PNR, aveva quale scopo quello di mettere a disposizione delle autorità pubbliche informazioni relative a soggetti prima sconosciuti alle forze dell'ordine, per consentire un intervento fondato e reso possibile da una conservazione *ex ante* dei dati. Proprio questo sistema è stato, come ben noto, 'bocciato' dalla Corte,

Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy, op. cit., p. 726; ma anche C. KUNER, *Reality and illusion in EU data transfer regulation post-Schrems*, op. cit.

[153] M. ANDREJEVIC, *Surveillance in the Big Data era*, in K. PIMPLE (a cura di), *Emerging pervasive information and communication technologies*, Springer, 2014, p. 55.

che ha proposto, quale soluzione – pur ampiamente criticata – conforme al diritto dell'UE e rispondente al principio di proporzionalità, una conservazione dei dati mirata sulla base della individuazione di uno specifico gruppo di soggetti o di una area geografica (par. 59, *DRI*) ed un successivo accesso mirato e fondato su elementi obiettivi che colleghino un dato ad un sospetto o ad una indagine. Anche nei casi *DRI e Tele2* tuttavia una delle argomentazioni sostenute dai governi intervenuti a favore della utilità e proporzionalità dei sistemi di *bulk data retention* era proprio fondata sul fatto che una limitazione e targettizzazione della conservazione dei metadati avrebbe compromesso l'efficacia del sistema stesso di *retention* che, per risultare utile a fini preventivi e di repressione dei reati gravi, abbisogna di essere necessariamente generalizzata ed indiscriminata.

Questa discrasia o quantomeno allontanamento della posizione espressa dalla Corte nelle sue diverse pronunce deve far riflettere, anche alla luce del fatto che nel *Parere 1/15* i richiami alla previa giurisprudenza, in particolare alla storica pronuncia sulla DRD, sono numerosi e costanti, quasi a sottolineare, al contrario, una uniformità e coerenza tra le argomentazioni proposte[154]. La spiegazione a questa – più o meno apparente – divergenza interpretativa può basarsi su due ordini di argomentazioni, opposte tra loro: si può ritenere che la Corte nell'ultimo Parere abbia voluto optare per uno 'smussamento' di quel divieto di conservazione indiscriminata e generalizzata così forte operato nella previa giurisprudenza, ammettendo sistemi di *bulk data retention* dei dati a fini di prevenzione e repressione di reati gravi, oppure si può ritenere che quanto affermato nel Parere non possa essere esteso anche a meccanismi di conservazione massiva riferiti alla totalità dei metadati derivanti dalla totalità dei sistemi di comunicazione elettronica e riguardanti la totalità della popolazione, poiché le differenze oggettive e fattuali dei diversi casi non consentono di individuare possibili parallelismi.

Partendo da quest'ultima interpretazione, sostenuta, come si è già visto, dall'Avvocato generale nelle sue Conclusioni[155], si può notare come essa si fondi sugli elementi di differenziazione ed in particolare sulla differente estensione dell'ingerenza in termini di persone coinvolte e di 'qualità' dei dati trasmessi che caratterizzano i due diversi filoni giurisprudenziali: nel caso del sistema di trasferimento di PNR infatti i soggetti interessati sono 'solo' i passeggeri di voli aerei da e verso il Canada[156] e i dati sono solamente quelli riferiti ai codici di prenotazioni che, per quanto idonei a tratteggiare i contorni della vita privata di un soggetto, non paiono fornire il medesimo grado di informazioni deducibili dall'analisi dei metadati derivanti dalla totalità delle telecomunicazioni dallo stesso svolte. L'ambito di incisività dunque del sistema di conservazione e accesso ai PNR risulta più ristretto di quello oggetto di analisi nei casi *DRI* e *Tele2*[157].

---

[154] Come non manca di sottolineare l'Avvocato generale: "L'esame di tale questione beneficia indubbiamente dei preziosi insegnamenti derivanti dalle sentenze dell'8 aprile 2014, Digital Rights Ireland e a., nonché del 6 ottobre 2015, Schrems. Come sarà spiegato in termini più ampi, ritengo che si debba proprio seguire la via tracciata da tali sentenze e sottoporre l'accordo previsto a un rigoroso controllo del rispetto degli obblighi posti dagli articoli 7, 8 e dall'articolo 52, paragrafo 1, della Carta", par. 7.

[155] Queste posizioni non sono poi state riprese dalla Corte, che è giunta però alle medesime conclusioni sul punto riprendendo solo in parte le affermazioni di Mengozzi, senza riproporre cioè la distinzione da questi esplicitata rispetto ai casi di *data retention* riferiti alle telecomunicazioni elettroniche.

[156] Si ricordino sul punto le già richiamate affermazioni dell'Avvocato generale: "Inoltre, contrariamente alle persone i cui dati formavano oggetto del trattamento di cui alla Direttiva 2006/24, tutte quelle cui si riferiva l'accordo previsto prendono volontariamente un mezzo di trasporto internazionale diretto o proveniente da un paese terzo, mezzo di trasporto che è esso stesso, purtroppo in modo ricorrente, veicolo o vittima di atti di terrorismo o di reati gravi di natura transnazionale, il che necessita dell'adozione di misure che garantiscano un livello di sicurezza elevato di tutti i passeggeri" (par. 242), a dimostrazione della sussistenza di una relazione 'oggettiva', ma solo vaga ed estremamente ampia, tra la raccolta, conservazione e trattamento dei dati da un lato e rischio probabile di un pericolo per la sicurezza dei passeggeri nonché, più in generale, della sicurezza pubblica e nazionale.

[157] Sul punto si legga P. VOGIATZOGLOU, *Mass surveillance, predictive policing and the implementation of the CJEU and the ECtHR requirement of objectivity*, in *European Journal of Law and Technology*, 1, 2019, che afferma: "this last ruling [*Parere 1/15*] is claimed to be more restricted in its effect than rulings concerning, for

Del resto anche la scansione temporale (mancante nella bozza di accordo e determinante l'incompatibilità dello stesso rispetto al diritto dell'UE) delineata nel Parere e ritenuta fondamentale per la legittimità del regime di trasferimento PNR stesso, non è altrettanto facilmente applicabile e 'traslabile' nei casi di conservazione dei metadati relativi alle telecomunicazioni: è – e se sì, come – possibile determinare un momento oltre il quale la conservazione di metadati non può più essere considerata legittima, similmente a quanto delineato nel Parere con riferimento alla partenza del soggetto dal Canada? In altre parole, nel sistema PNR è più ragionevole e semplice affermare che sia legittimo e proporzionato raccogliere e conservare i dati dei passeggeri prima del loro arrivo, determinando nel momento della ripartenza il punto 'temporale' in cui tale conservazione non si rende più giustificabile in assenza di debiti elementi oggettivi che ne legittimino il trattenimento; non è però altrettanto possibile o quanto meno immediato identificare un momento di discrimine di tale tipo rispetto ad un sistema generalizzato di conservazione quale quello previsto dalla DRD o dalla facoltà attribuita agli Stati membri sulla base dell'art. 15 Direttiva *e-Privacy*. Ciò risulta difficile anche alla luce di quanto stabilito dalla Corte nella sentenza *DRI* nel punto in cui cioè si afferma l'illegittimità della durata di conservazione fissata dalla DRD "senza che venga precisato che la determinazione della durata di conservazione debba basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario" (par. 64). Il contesto entro cui il *Parere 1/15* si inserisce, inoltre, coinvolgendo uno Stato terzo e il suo sistema di controlli ai confini, è fortemente diverso da quello meramente interno all'UE che si ravvisa nei casi *DRI* e *Tele2*, sebbene non possa mancarsi di rilevare come anche all'interno dell'Unione stessa, con la Direttiva 2016/681, si sia istituito un sistema di raccolta, conservazione e trattamento dei codici di prenotazione simile, anche se non identico, a quello previsto con gli Stati terzi.

Se tale linea interpretativa impedisce dunque di ravvisare nella decisione della Corte in materia di PNR un impatto diretto rispetto alla disciplina della *data retention*, vi sono tuttavia punti di contatto tra i due sistemi di conservazione e trattamento dei dati, rispetto ai quali è possibile individuare alcune incongruenze – o per lo meno argomentazioni poco chiare o poco motivate – tra le posizioni dei giudici di Lussemburgo. Innanzitutto, nel caso del sistema PNR, il trasferimento, conservazione e trattamento generalizzato dei dati relativi ai passeggeri in arrivo in Canada vengono considerati legittimi e limitati a quanto strettamente necessario per il raggiungimento dell'obiettivo 'sicurezza': "per quanto riguarda la conservazione dei dati PNR e il loro uso fino all'uscita dei passeggeri aerei dal Canada, va rilevato che tali attività consentono, in particolare, di facilitare i controlli di sicurezza nonché i controlli alle frontiere. La loro conservazione e il loro uso a tal fine non possono, per loro stessa natura, essere limitati a una cerchia determinata di passeggeri aerei né essere oggetto di una previa autorizzazione di un giudice o di un ente amministrativo indipendente. Pertanto, e conformemente alle valutazioni figuranti ai punti da 186 a 188 del presente parere, si deve ritenere che, fintantoché i passeggeri aerei si trovano in Canada o in partenza da tale paese terzo, sussiste il rapporto necessario tra tali dati e l'obiettivo perseguito da detto accordo, cosicché esso non eccede i limiti dello stretto necessario per il solo fatto che consente la conservazione e l'uso sistematici dei dati PNR di tutti tali passeggeri" (par. 197, *Parere 1/15*). Alla luce di queste affermazioni, e sempre tenendo conto della peculiarità dei soggetti coinvolti, dei dati oggetto di trattamento e del contesto riguardante uno Stato terzo, viene da chiedersi comunque se non sia possibile applicare il medesimo ragionamento della Corte anche ai sistemi di *data retention* generalizzata ed indiscriminata relativo ai metadati derivanti da telecomunicazioni. Se si accoglie la posizione di chi contrasta, come si è visto nel Capitolo relativo alle pronunce *DRI* e *Tele2*, la reale possibilità ed efficacia di una conservazione targettizzata e di chi rinviene in quest'ultima forti ed

instance, electronic communications data, due to the nature, narrow scope and limited amount of PNR data in relation to the latter. It, thus, argued that a wider rationale would not be similarly applicable to a vast category of personal data like electronic communications data", p. 9.

insuperabili problematiche rispetto al diritto alla non discriminazione[158], diviene chiaro come anche una *retention* generalizzata dei metadati relativi a telecomunicazioni per finalità di prevenzione e contrasto di reati gravi non possa che essere ritenuta parimenti legittima e limitata a quanto strettamente necessario purché ovviamente accompagnata, come stabilito dalla Corte nel Parere richiamato, da idonee tutele relative alla fase di accesso e utilizzo di tali dati. Conseguentemente poi bisognerebbe chiedersi se, anche per i sistemi di *data retention* quali quello previsto dalla invalidata DRD, possa essere affermato che una forma di conservazione mirata ne inficerebbe lo stesso funzionamento, utilità, nonché l'intrinseco scopo e natura, col risultato di far salvo dunque il carattere generalizzato ed indiscriminato, spostando le tutele del criterio oggettivo solo in un secondo momento e cioè alla fase dell'utilizzo/accesso. Del resto la conservazione nel sistema di trasferimento di PNR viene garantita anche durante tutto il periodo di soggiorno del viaggiatore, in un momento cioè in cui, a seguito dei controlli in entrata, mediante sistemi di analisi automatizzate e algoritmiche dei dati, non era stata rilevata alcuna problematicità o sospetto in capo al soggetto entrante nel territorio nazionale; una conservazione che è purtuttavia legittimata sulla base della considerazione secondo cui "durante il soggiorno dei passeggeri aerei in Canada e indipendentemente dal risultato dell'analisi automatizzata dei dati PNR effettuata prima del loro arrivo in tale paese terzo, possono presentarsi situazioni nelle quali l'autorità canadese competente disponga di indicazioni, raccolte durante tale soggiorno, per le quali l'uso dei loro dati potrebbe rivelarsi necessario al fine di combattere il terrorismo e i reati gravi di natura transnazionale" (par. 199, *Parere 1/15*). Tale posizione, che ritiene la *retention* dei codici di prenotazione giustificata alla luce di una mera ipotetica ed eventuale necessità di accesso successivo ai dati, rimane alquanto dubbia o quantomeno poco motivata, soprattutto alla luce delle previe pronunce della Corte di giustizia che hanno invece ampiamente affermato l'illegittimità di sistemi generalizzati di *data retention*, ritenendo la conservazione di metadati – per quanto di differente natura ed estensione rispetto a quella avente ad oggetto i PNR, come già ampiamente rimarcato – *per se* una interferenza nei diritti alla vita privata e alla protezione dei dati, che deve pertanto essere proporzionata e debitamente fondata su criteri oggettivi che ne dimostrino la stretta necessità. Questa lettura critica della decisione dei giudici di Lussemburgo ed i dubbi che il *Parere* ha fatto sorgere rispetto all'interpretazione della giurisprudenza precedente, viene messa in luce anche dalla richiesta di chiarimenti promossa dalla Corte costituzionale belga mediante rinvio pregiudiziale alla CGUE[159], attualmente pendente: esso, come si vedrà nel Capitolo IV, mira proprio a chiarire se una conservazione targettizzata ed un accesso mirato e limitato da specifiche garanzie, siano condizioni di legittimità da intendersi come necessariamente presenti cumulativamente o se invece possano essere lette ed attuate disgiuntamente poiché la tutela nella fase dell'utilizzo del

[158] Con riferimento alla difficoltà di applicare concretamente i criteri indicati dalla CGUE in *DRI* e *Tele2*, che si riferiscono cioè ad una conservazione targettizzata, si richiama quanto indicato da EUROPOL (in *Proportionate data retention for law enforcement purposes*, WK9957/2017) che afferma l'impossibilità di attuare una *targeted data retention* dal momento che "the potential relevance amongst data and the purposes pursued cannot be foreseen in advance", come riportato da P. VOGIATZOGLOU, *Mass surveillance, predictive policing and the implementation of the CJEU and the ECtHR requirement of objectivity*, op. cit. L'autrice nello stesso contributo pone inoltre attenzione all'aspetto, già evidenziato, della possibile portata discriminatoria di criteri di targettizzazione basati sull'individuazione di un determinato gruppo di soggetti o area geografica: tale approccio può portare ad effetti perversi e distorsivi nel caso in cui divenga elemento determinante nella configurazione dell'algoritmo e del sistema automatizzato di analisi dei dati, producendo potenzialmente un meccanismo caratterizzato da *bias*. "Therefore, seemingly objective and lawful, under the discussed case law, criteria such as geographical location, that may be utilised to define the personal data to be transferred from the private sector to security actors for the purpose of carrying out predictive policing methods, may lead to biased results. The issue has only been lightly touched upon by the CJEU in its ruling on the EU-Canada PNR Agreement, where the Court stated that the pre-established models, criteria and databases should be non-discriminatory. Besides the lack of analysis of this topic, this single-sentenced reference to non-discrimination law may also prove inadequate for the protection of citizens' fundamental rights in this context of big data analytics and predictive policing methods", p. 13.

[159] Domanda di pronuncia pregiudiziale proposta dalla Cour constitutionnelle (Belgio) il 2 agosto 2018, Causa C-520/18.

dato è sufficiente a limitare allo stretto necessario l'ingerenza di una conservazione generalizzata, come pare avvenire per i sistemi di trasferimento di PNR verso Stati terzi, pur con tutte le distinzioni necessarie del caso.

In questo contesto, insieme alle attese pronunce dei giudici di Lussemburgo attinenti direttamente alla disciplina della *data retention* per scopi securitari e all'applicazione e ai limiti dei requisiti indicati nella pronuncia *Tele2*, anche la posizione che la Corte di giustizia esprimerà con riferimento ai rinvii pregiudiziali sopra esaminati aventi ad oggetto la compatibilità con la Carta di Nizza e il diritto dell'UE della Direttiva PNR, avranno un impatto significativo. In queste controversie, infatti, i giudici sono chiamati ancora una volta a vagliare sistemi di raccolta, conservazione e trattamento generalizzato che, pur riguardando solo i passeggeri di voli aerei e i dati PNR e non l'intera popolazione, colpiscono comunque tutte le persone che si servono di un mezzo di trasporto determinato, senza che sussista alcun elemento oggettivo che consenta di collegare la conservazione dei dati di un passeggero con un determinato rischio per la sicurezza. Le considerazioni e le riflessioni che la CGUE porrà in essere in tale ambito potranno dunque chiarire ed assumere utilità al fine di meglio comprendere le distinzioni o le similitudini rispetto alla disciplina e ai requisiti fissati in materia di *data retention* di metadati derivanti da telecomunicazioni.

Capire e determinare con precisione l'estensione dei principi sanciti nel *Parere 1/15* e determinarne la portata al di fuori dello specifico contesto dei sistemi transfrontalieri di invio di dati PNR, assume grande rilevanza dunque anche rispetto ad altre misure europee che parimenti prevedono forme di raccolta, conservazione e accesso massivi, sebbene aventi ad oggetto tipologie diverse di dati: si fa riferimento non solo ai sistemi di *data retention* di metadati di telecomunicazioni bensì anche, a titolo di esempio, al sistema Entry/Exit (c.d. SEE), istituito con Regolamento UE 2017/2226, che crea una banca dati centrale informatizzata di dati biometrici ed alfanumerici finalizzata a gestire le frontiere esterne all'Unione e a prevenire l'immigrazione irregolare[160].

5.1.3. – Il possibile impatto della decisione Schrems *e del* Parere 1/15 *rispetto a forme di sorveglianza massiva del contenuto delle telecomunicazioni operate da agenzie di intelligence per scopi di sicurezza nazionale*

Le riflessioni sulla possibile estensione nella dimensione interna dell'UE dei principi delineati nelle pronunce sino ad ora analizzate non possono poi ignorare anche il portato della sentenza *Schrems* e dell'affermazione, in essa contenuta, della lesività del nucleo essenziale del diritto alla riservatezza di sistemi che prevedano una raccolta, conservazione e trattamento indiscriminato e generalizzato di dati riguardanti il contenuto di comunicazioni elettroniche, pur per finalità di tutela della sicurezza. Ebbene i principi e criteri stabiliti dai giudici nella sentenza *Schrems*, se applicati pedissequamente nel contesto

[160] Si leggano sul punto le riflessioni di M. COLE, T. QUINTEL, *Legal opinion (commissioned by The Greens in the EU Parliament): Data Retention under the Proposal for an EU Entry/Exit System (EES) Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union*, ottobre 2017 (disponibile all'indirizzo: http://orbilu.uni.lu/bitstream/10993/35446/1/Legal%20Opinion.PDF), nelle quali si afferma conclusivamente che: "In sum, the analysis above shows clearly that the conclusions to be drawn from Opinion 1/15 in combination with the previous case law of the CJEU are that the principles developed therein also impact the admissibility and design of an EES and connected data collection and retention. Irrespective of the politically questionable signal if EU legislative bodies would agree on an instrument that does not fully meet the requirements for an international agreement as set by the Court in view of the protection of EU citizens, because it concerns Third Country Nationals, the proposal for the Regulation establishing the EES should in its current form be reconsidered, in order to avoid potential difficulties in a later review of the instrument by the CJEU. This review would certainly build on the established case law about data retention schemes and therefore likely result in the finding of a violation of fundamental rights standards", p. 37.

interno all'UE, potrebbero portare a considerare non conformi al diritto dell'UE meccanismi di controllo, intercettazione e sorveglianza massiva ed indiscriminata del contenuto delle telecomunicazioni posti in essere non da autorità di *law enforcement* bensì da agenzie e servizi di intelligence. Certamente, come già sottolineato nelle osservazioni a margine dei casi *DRI* e *Tele2*, nel panorama interno all'UE una limitazione ulteriore e un aggiuntivo elemento di complessità sono dati dal principio di attribuzione e dall'art. 4, co. 2, TFUE che esplicita, lo si ripete, che "la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro". Se, per tali ragioni però si giungesse a ritenere non applicabili ad operazioni svolte da autorità di intelligence per scopi di sicurezza nazionale i criteri delineati nel filone giurisprudenziale sino a qui studiato, dalla *DRI* a *Schrems*, si arriverebbe al paradosso di imporre un livello di tutela elevato nei confronti dello Stato terzo anche per il trattamento di dati da questo effettuato per finalità di garanzia della sicurezza nazionale, ma di non imporre tale medesimo standard di tutela della protezione dei dati anche all'interno del territorio dell'Unione e degli Stati membri[161]. Queste osservazioni, circa la difficoltà di determinare una chiara linea di demarcazione tra attività in capo a soggetti privati, ad autorità di *law enforcement* o ancora, ad agenzie di intelligence, legate alla divisione di competenze tra UE e Stati membri nel delicato ambito della *data retention*, sono già state preliminarmente svolte nel Capitolo II e verranno più ampiamente sviluppate nel Capitolo IV: in questa sede è sufficiente richiamare come tali questioni risultino al momento ancora del tutto aperte, come evidenziato dal pendente rinvio pregiudiziale promosso dal Regno Unito[162] volto proprio a chiedere alla CGUE un chiarimento sulla portata espansiva dei criteri e delle condizioni indicate nelle sue storiche pronunce, da *DRI* a *Tele2*, alle attività volte alla tutela della sicurezza nazionale.

Ciò che infine si vuol mettere in evidenza, prima di passare all'analisi del secondo ordine di conclusioni, è la problematicità relativa alla corretta identificazione della base giuridica di accordi che abbiano ad oggetto il trasferimento di dati all'estero ma che, più in generale, concerne anche gli atti dell'UE che riguardino sistemi di conservazione e trattamento di dati. Come emerso nel *Parere 1/15* ma anche nella previa decisione, già richiamata, avente ad oggetto l'accordo di trasferimento PNR tra USA e UE (per quanto in quel caso ci si trovasse ancora in fase pre-Trattato di Lisbona), risulta chiaro come la difficoltà nel determinare questo aspetto, formale ma di estremo rilievo sostanziale, sia dovuta alla divergenza tra la finalità primaria per la quale i dati vengono raccolti e in un primo momento conservati – operazioni effettuate cioè da soggetti privati a mero scopo commerciale e di fornitura di un servizio – e l'ulteriore scopo di conservazione, trattamento e accesso al dato che risponde invece ad esigenze di sicurezza, prevenzione e repressione di reati gravi ad opera di autorità pubbliche. Questa differenziazione e distanza tra gli scopi comporta una necessaria mediazione tra interessi securitari ed esigenze di tutela dei cittadini e dei loro diritti alla riservatezza e alla protezione dei dati, imponendo altresì di riflettere sulle competenze dell'Unione e degli Stati membri in un ambito complesso, nel quale si devono disciplinare attività dei privati e funzionamento del mercato da un lato e attività delle pubbliche autorità dall'altro. Tali esigenze di regolamentazione, che certamente emergono con maggior forza nei casi *DRI* e *Tele2*, possono ben essere rinvenute anche nelle pronunce *Schrems* e *Parere 1/15* nelle quali le attività delle aziende con sede in UE e dei vettori aerei privati si intrecciano con le attività e gli obblighi imposti da autorità pubbliche, benché in tal caso di Stati terzi.

[161] Sul punto e solo preliminarmente si rimanda a S. CRESPI, *The applicability of Schrems principles to the Member States: national security and data protection within the EU context*, in *European Law Review*, 43, 2018.
[162] Domanda di pronuncia pregiudiziale proposta dall'Investigatory Powers Tribunal, Londra (Regno Unito) del 31 ottobre 2017, C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e al.*

5.2. – La giurisprudenza della CGUE e le reazioni di Istituzioni europee e Stati terzi: la disciplina dell'UE in materia di trasferimento dei dati al di fuori dei confini dell'UE come strumento vincente per l'affermazione di un più elevato standard globale di tutela della riservatezza e protezione dei dati?

Se si porge ora attenzione al secondo profilo da analizzare, che si propone di riflettere sull'approccio di tutela della privacy e della protezione dei dati adottato dall'UE nella sua azione verso l'esterno, allo scopo di metterne in rilievo le conseguenze, i risultati nonché le criticità, non si può che iniziare col prendere atto di quanto le disposizioni della Dir. 95/46 prima e del GDPR ora, unitamente alla giurisprudenza della Corte nei casi *Schrems* e *Parere 1/15*, abbiano ormai delineato requisiti, criteri e principi in materia di trasferimento dati verso Stati terzi di grande impatto e fortemente virati all'affermazione di un elevato standard di tutela dei diritti fondamentali.

Ciò ha comportato non pochi problemi, come si è anticipato, sul fronte delle relazioni internazionali, considerando appunto che "the specificity of the debate on EU-US transfer of data is that it cannot be considered as purely "internal". Although the Schrems ruling has to be complied with at European level, it is not merely an EU political issue. On the contrary, external relations and EU politics are intertwined, and external factors, including the position of the United States, need to be addressed"[163]; queste affermazioni, sebbene svolte nell'ambito del caso *Schrems*, ben possono essere estese a tutti gli accordi e le decisioni aventi ad oggetto la più ampia materia del trasferimento dati al di fuori dell'UE.

In questo contesto di estrema complessità, è da rilevare innanzitutto come l'approccio dell'UE sia stato letto dalle stesse Istituzioni europee e dalla dottrina in maniera estremamente differente: la Commissione, ad esempio, nonostante la piena consapevolezza delle debolezze e criticità del meccanismo *Safe Harbour*, soprattutto dopo le rivelazioni di Snowden[164], ha preferito lavorare a stretto contatto con le Istituzioni americane al fine di rivedere i principi di "Approdo sicuro" ed incentivare una loro migliore, corretta e concreta attuazione da parte delle aziende e delle autorità pubbliche statunitensi, anziché mettere in discussione la validità della decisione di adeguatezza stessa[165]; ciò anche considerando, come sottolineato dalla High Court irlandese nel suo rinvio pregiudiziale nel caso *Schrems*, l'estrema difficoltà del legislatore statunitense di adattare l'ordinamento interno ad un livello di protezione dei dati e della privacy molto distante dalla propria tradizionale concezione e tutela di tali diritti fondamentali[166]. L'approccio della Commissione tuttavia, come noto, si è scontrato con quello

---

[163] F. TERPAN, *EU-US data transfer from Safe Harbour to Privacy Shield: back to square one?*, op. cit., p. 1047.

[164] Come ben dimostrato dalle affermazioni contenute nella Comunicazione al Parlamento e al Consiglio COM (2013) 846 final, del 27 novembre 2013.

[165] "In August 2013, Viviane Reding, Vice-President of the Commission, called for a review of the Safe Harbour by the year-end, calling the Safe Harbour 'a loophole' that 'may not be so safe after all'. The EC issued out a series of recommendations to improve the content of the Safe Harbour in December 2013. This included a close monitoring of the use of the exceptions contained in the Decision, the provision of information to individuals about potential further transfers to US intelligence services, and the recognition of individuals' rights to access, rectify and delete their data, as well as the right to redress in the context of US surveillance programmes. Discussions were reopened but soon stall. The attempt to elaborate a political solution reached a dead end.", F. COUDERT, *Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for Data Protection Authorities,* in *European Law Blog*, ottobre 2015, disponibile all'indirizzo: https://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/

[166] Sul punto si richiama, oltre agli autori già citati, anche: I. TOURKOCHORITI, *The Transatlantic Flow Of Data And The National Security Exception In The European Data Privacy Regulation: In Search For Legal Protection Against Surveillance*, in *University of Pennsylvania Journal of International Law*, 3, 2015; W. B. WRAY, *A European approach to the United States Constitutional privacy*, in *Craighton International and Comparative Law Review*, 51, 2015; F. BIGNAMI, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Study for the LIBE Committee, 2015; L.P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of the Eu and US constitutional systems*¸ in L. VIOLINI, A. BARAGGIA (a cura di), *The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and non-Judicial Actors*, Elgar Publish, 2018.

della CGUE che, investita del caso, ha assunto una posizione netta e decisa in merito, optando per la dichiarazione dell'invalidità con effetto *ex tunc*, senza peraltro decidere per una modulazione nel tempo della sentenza, scelta che avrebbe consentito di limitarne l'impatto per le imprese.

Anche la dottrina si è interrogata sul significato più sostanziale della normativa dell'UE in materia di trasferimento dei dati e sull'interpretazione fornitane dalla Corte nelle sue pronunce, giungendo a risultati differenti: da un lato vi è chi considera lodevole la presa di posizione dei giudici di Lussemburgo, che ha dimostrato di non voler sacrificare la tutela dei diritti fondamentali dinnanzi sia ai forti interessi del settore privato, dettati dalla interdipendenza economica con Stati quali gli USA e dall'elevato valore di mercato dei dati, sia ad una crescente 'securitarizzazione' delle normative in "times of stress"[167], tese a garantire una prioritaria protezione della sicurezza dei consociati a discapito della salvaguardia dei diritti[168]; dall'altro lato vi è invece chi ritiene lo scrutinio adottato dalla CGUE eccessivamente rigido, col risultato di produrre una oggettiva impossibilità o quantomeno una concreta e seria difficoltà di attuazione, nelle relazioni con Stati terzi, dei principi stabiliti[169]. Secondo tale lettura, quindi, la tutela della continuità degli standard europei di riservatezza e protezione dei dati si tradurrebbe, in realtà, in una discutibile valutazione unilaterale effettuata dalla Corte del sistema giuridico straniero; nella sentenza *Schrems* i giudici di Lussemburgo hanno specificato che il termine 'adeguatezza' non deve essere interpretato nel senso di 'eguaglianza', non rilevando dunque ai fini di tale valutazione il fatto che gli strumenti normativi usati da Paesi terzi siano differenti da quelli europei e adottando altresì quello che è stato definito una sorta di *self-restraint "*così ponendo le basi, concettualmente, per una sostanziale insindacabilità delle soluzioni normative adottate in ordinamenti diversi da quello dell'Unione europea"; se ciò pare corretto, è altrettanto vero però che la Corte è poi entrata "eccome nel merito degli strumenti normativi che assicurano la protezione dei dati personali nell'ordinamento (..) E lo fa con un approccio che è inedito, almeno per quanto riguarda le decisioni che più direttamente vertono in materia di diritti fondamentali, e non di libertà economiche: con uno sguardo pragmatico e un'attenzione particolare per il soddisfacimento dell'obiettivo di tutela sotteso alle misure in questione", manipolando così, secondo taluni autori, il più flessibile significato del termine

[167] Come mette in luce Zalnieriute, del resto, "a great deal of far-reaching 'pro-security' legislation and numerous data-sharing agreements were implemented without any serious democratic debate during the decade following 9/11, and only some received a post factum attention by raising suspicions about their constitutional legitimacy in the US and EU"; in tale contesto dunque, secondo l'autore, è da leggere positivamente la posizione della CGUE: "at least the CJEU will no longer accept the rules of the game for data-sharing modelled around security interests in the previous decades", in *Developing a European standard for international data transfers after Snowden: Opinion 1/15 on the EU-Canada PNR agreement*, op. cit., p. 1055-1056.

[168] Mendez ad esempio ritiene che "we should praise it for seeking to ensure that privacy and data protection standards in the Charter are taken seriously and that, despite the very real threat of terrorism and serious crime, international agreements cannot simply be used in a manner that rides roughshod over these fundamental rights", in *Opinion 1/15: the Court of justice meets PNR data (again!)*, op. cit., p. 811.

[169] Si legga in questo senso la veemente critica rivolta alla Corte da R. EPSTEIN, voce proveniente dall'altra parte dell'Oceano e che restituisce una visione molto distante da quella europea, fondata sulla convinzione che la giurisprudenza europea sia errata sotto il profilo sostanziale della valutazione della ingerenza nei diritti fondamentali rappresentata dal sistema statunitense (ed in particolare di cosa debba intendersi per sorveglianza di massa e quando essa rappresenti una lesione sproporzionata del diritto alla riservatezza) ma anche nella interpretazione del termine stesso di adeguatezza: "It was therefore incorrect, in my view, for the European Court of Justice to take the position that the American statutory framework had to offer protection 'essentially equivalent' to that supplied under exacting European standards, which started from the assumption that the privacy right in data—apparently even that which has been previously publicly posted on Facebook—was a fundamental interest deserving the highest protection". Ciò che viene poi fortemente condannato dall'autore è il peso attribuito dalla Corte alle rivelazioni di Snowden, fondando su di esse il vaglio di adeguatezza e rifiutando di "look closely at the general agreement by which data passed from the EU to the United States. It takes years to put into place successful complex systems of data transmission. It takes only one errant complaint and a dubious decision of the European Court of Justice to rip it all apart", R. EPSTEIN, *The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European Constitutional Law Review*, 12, 2016, p. 339.

"sostanziale equivalenza"[170]. Questa lettura interpretativa dell'approccio della CGUE si distanzia quindi dalle parole del Presidente della CGUE, Koen Lenaerts che, in merito alla decisione del caso *Schrems*, ha affermato: "We are not judging the US system here, we are judging the requirements of EU law in terms of the conditions to trasfer data to third countries"[171], a sottolineare come la decisione della Corte sia solo frutto della necessità di rispettare e attuare i principi e "l'identità costituzionale" dell'Unione Europea, da individuarsi principalmente nel rispetto dei diritti fondamentali e dello Stato di diritto[172].

Da questo scenario articolato, composto da differenti visioni ed interpretazioni della disciplina normativa e dell'intervento della CGUE, emerge come anche le valutazioni circa l'efficacia del sistema di trasferimento dati al di fuori dei confini europei siano discordanti: senza dubbio la finalità ultima del diritto dell'UE è quella di predisporre tutele in grado di scongiurare i pericoli derivanti da un trasferimento dati verso quelli che potrebbero essere definiti, parafrasando la terminologia usata in ambito fiscale, "paradisi dei dati" cioè verso Paesi terzi in cui la normativa in materia di privacy e *data protection* risulta essere più blanda e meno garantista; pratica questa che risulterebbe non solo in una compressione dei diritti fondamentali riconosciuti dall'Unione Europea, ma anche, in ultimo, in una distorsione nell'ambito della concorrenza e competizione tra aziende, a discapito di quelle che attuano rigorose *policies* in materia di privacy e protezione dei dati rispettose di elevati standard di tutela ma che impongono anche costi ed investimenti maggiori (in termini di gestione, di controllo, di strumentazione, di formazione). Se una tale visione è da tutti condivisa, ciò che viene però discussa è la modalità con la quale l'UE sta cercando di garantire il raggiungimento di tale obiettivo nonché la sua efficacia ed opportunità. Vi è infatti chi riscontra nell'approccio dell'UE il tentativo di far leva sul valore economico sempre maggiore dei dati e dell'indispensabile trasferimento e scambio degli stessi per creare un canale attraverso cui imporre unilateralmente agli Stati terzi il proprio livello di tutela, nella 'esaltante illusione' di poter proteggere i propri valori e i diritti dei propri cittadini anche oltre i confini, basandosi su forzature unilaterali[173] e su un modello di 'imperialismo normativo'[174]: "The [Schrems] judgment thus lays bare the internal contradictions of the regulation of data transfers under EU law, and shows how its unilateral application cannot provide complete protection for data transfers to Third Countries"[175]. Secondo tale visione, un approccio fondato sui criteri dell'adeguatezza non sarebbe quindi funzionale ed efficace nel produrre un reale e tangibile impatto nello Stato terzo[176]. Ciò sarebbe

---

[170] O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo,* op. cit., p. 87.

[171] Presidente della CGUE, *Public Opinion, Safe Harbour, Antitrust*, in *The Wall Street Journal*, 14 ottobre 2015; sul punto si legga anche l'Avvocato generale Mengozzi nelle sue Conclusioni, in particolare al par. 163.

[172] Queste affermazioni inducono peraltro a riflettere, come si è già richiamato nei precedenti paragrafi, sull'importanza sempre maggiore che la conoscenza di normative straniere sta assumendo, a causa della forte interconnessione tra ordinamenti dovuta sia alle nuove tecnologie e alla natura immateriale e a-territoriale di Internet e dei dati, sia al fenomeno della globalizzazione. In questo contesto alcuni autori (C. KUNER, *Reality and illusion in EU data transfer regulation post-Schrems*, op. cit.) ritengono necessaria sia una accuratezza maggiore nella ricostruzione delle normative di un Paese terzo, che dovrebbe fondarsi su fonti accademiche o su documentazioni fornite da soggetti imparziali ed esperti, sia una rafforzata trasparenza e chiarezza da parte della Corte circa le fonti e le motivazioni che hanno portato ad una determinata interpretazione della normativa straniera, spingendosi a pensare anche alla necessità di riconsiderare i poteri istruttori della Corte stessa.

[173] Usa questo termine L. ZAGATO, *Il trasferimento di dati personali verso Stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*, in *Diritto del commercio internazionale*, 2, 2008, giungendo però alla conclusione, opposta rispetto a quella sin qui delineata, che tale modello di imposizione unilaterale sia cioè da considerarsi vincente ed efficace.

[174] Espressione mutuata da M. LEFFI, *I trasferimenti di dati terzi nel nuovo Regolamento UE*, op. cit., p. 17.

[175] C. KUNER, *Reality and Illusion in the EU data transfer regulation post Schrems*, op. cit., p. 910.

[176] Come sottolineato anche all'Avvocato generale Mengozzi nelle sue Conclusioni: "Tuttavia, occorre tener presente che il progetto di accordo di cui la Corte è investita è la conseguenza di un negoziato internazionale con un paese terzo il quale, in mancanza di un accordo soddisfacente, potrà rinunciare alla conclusione dell'accordo previsto e preferirà, come avviene attualmente, l'applicazione unilaterale del suo regime PNR ai vettori aerei stabiliti nell'Unione e che garantiscono collegamenti con il Canada", par. 7. Ciò mette in evidenza come livelli

dimostrato dalla stessa 'cedevolezza' dei principi affermati nelle pronunce della Corte, non tradottisi poi in accordi o decisioni realmente in grado portare ad un incremento nella garanzia dei diritti e pertanto invalidate dalla Corte stessa nelle proprie decisioni. L'incapacità della Commissione stessa di giungere ad accordi che attuino i principi delineati dalla giurisprudenza europea è il sintomo sia di quanto discordanti siano le azioni delle varie Istituzioni dell'UE, sia di quanto il sistema di garanzia del trasferimento dati "si riveli più debole di quanto ora appare, incapace in concreto di difendere nella sostanza i confini del proprio standard di tutela in un mondo globale e interconnesso"[177]. La garanzia offerta quindi dalla disciplina normativa europea sarebbe di carattere prettamente formale e non sostanziale, caratterizzata da declamazioni di alti livelli di protezione e da una prassi che ad essi non corrisponde, scontrandosi peraltro con la necessità, nella realtà dei rapporti internazionali, di scendere a compromessi e di smorzare quella – da taluni ritenuta illusoria – garanzia extraterritoriale di protezione dei dati e della riservatezza, delineata dalla normativa dell'UE ed, ancor più, dalla Corte[178]. Il modello promosso risulterebbe quindi solo apparentemente vincente, scontrandosi anche con i forti limiti del controverso strumento della 'decisione di adeguatezza', criticato per la lunga procedura che esso richiede e per la mancanza di trasparenza nelle valutazioni, ben potendo essere soggetta a possibili forte influenze politiche ed economiche in grado di inficiare le considerazioni della Commissione[179]. Le problematiche relative ai principi che l'UE vorrebbe garantire ai dati in uscita dall'Europa sono anche rinvenute nel rischio di un atteggiamento 'ipocrita', come è stato definito[180], delle Istituzioni europee che impongono e pretendono nelle relazioni con Stati terzi livelli di tutela che non sono però spesso rispettati e garantiti efficacemente e concretamente nel contesto interno all'Unione stessa[181].

Certamente alcune delle obiezioni al modello utilizzato dall'UE che sopra sono emerse risultano fondate e in parte confermate nei fatti[182] e senza dubbio una maggiore coerenza nell'azione delle

troppo elevati e irraggiungibili di tutela, che comportano complicazioni e possibili insormontabili dissensi nello Stato terzo parte della negoziazione, possano portare ad uno stallo che può tradursi o in un pericoloso 'embargo' per il trasferimento di dati (questa opzione tuttavia pare ormai impossibile, in una società datizzata e globalizzata, fondata sulla interdipendenza economica) o nell'applicazione unilaterale della normativa straniera. Questa problematica si pone anche con riferimento alle rinegoziazioni di accordi già esistenti, per i quali può essere complesso, se non rischioso e controproducente, imporre una posizione netta e non 'trattabile' allo Stato terzo.

[177] A. MANTELERO, *I flussi di dati transfrontalieri*, op. cit., p. 262.

[178] In questo senso S. Crespi che, con riferimento ad un possibile giudizio della Corte avente ad oggetto la compatibilità del *Privacy Shield* con i principi stabiliti dal diritto dell'UE, afferma: "L'esito del giudizio UE dipenderà poi dall'intensità del sindacato dei giudici dell'Unione quanto alle condizioni e ai limiti applicabili in caso di accesso della autorità USA ai dati UE per motivi di sicurezza nazionale. Un giudizio di compatibilità sembra in effetti più plausibile qualora la Corte concentri la propria analisi sulla solidità della motivazione della decisione di adeguatezza e sull'assenza di errori manifesti o di contraddizioni, così come fatto in Schrems. L'esito della controversia pare invece più incerto qualora tale controllo si spinga fino a sindacare il contenuto del diritto straniero, valutando se il diritto USA garantisca sufficienti garanzie alla luce dei criteri UE di proporzionalità e necessità. L'uso di tale metodo interpretativo esporrebbe tuttavia la giurisprudenza UE a critiche di espansione extraterritoriale", S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'Approdo sicuro allo Scudo UE/USA per la privacy*, op. cit., p. 713.

[179] C. KUNER, *The Internet and the global reach of EU law*, in M. CREMONA, J. SCOTT (a cura di), *EU law beyond EU borders. The extraterritorial reach of EU law*, Oxford University Press, 2019, p. 137. Se è vero infatti, come afferma la Commissione (COM (2017) 7 final), che la compatibilità dei livelli di tutela facilita non solo i flussi di dati a scopi commerciali ma anche la cooperazione tra autorità pubbliche, ciò può riverberarsi sulle scelte delle Istituzioni stesse di privilegiare le trattative sull'adeguatezza con partner commerciali chiave.

[180] C. KUNER, *Reality and Illusion*, op. cit., p. 898.

[181] La ipocrisia può essere ravvisata anche sotto un altro profilo: "When a legal system strives for its standards to be accepted as universal values, it is inevitably engaged in a hegemonic struggle in which it seeks to have its own special interests identified with the general interest", C. KUNER, *The Internet and the global reach of EU law*, op. cit., p. 137.

[182] Se si pensa alle criticità riscontrate nel – forse – frettoloso accordo *Privacy Shield* o ancora ai dubbi circa la conformità della Direttiva in materia di PNR al diritto dell'UE, emerge come i rigidi standard enunciati dalla Corte non siano poi stati seguiti da una coerente azione delle altre Istituzioni europee, né sul fronte esterno né su quello interno.

Istituzioni europee è fondamentale per individuare una linea di azione esterna che non risulti continuamente sconfessata da successivi o preventivi interventi della Corte, avendo peraltro forti ripercussioni, come si è visto, sul piano delle relazioni internazionali e della affidabilità dell'UE nelle sue negoziazioni[183].

È purtuttavia vero che nel modello adottato dall'Unione, volto a regolare il trasferimento dei dati fuori dai confini, può essere individuata non tanto la volontà di "esportare" e imporre il modello normativo europeo ai legislatori stranieri, bensì quello di esercitare una positiva influenza nel contesto internazionale, per la costruzione di un "regime internazionale di tutela della vita privata e delle informazioni di natura personale"[184]. In questo senso, e non in quello di imperialismo normativo europeo, può essere letto l'art. 50 del GDPR in materia di cooperazione internazionale per la protezione di dati personali, che prevede in capo alla Commissione e alle autorità di controllo nazionali il compito di sviluppare meccanismi di collaborazione con Stati terzi o con organizzazioni internazionali volti a facilitare una efficace applicazione di elevati standard di protezione dei dati e a prestare assistenza a livello internazionale: "la nuova previsione normativa potrebbe incarnare uno Zeitgeist europeo in una materia ancora in bilico fra resistenza ad ogni cedimento sul piano della tutela del diritto, e volontà di aprire strade nuove, che comunque non facciano della protezione dei dati un ostacolo insormontabile allo sviluppo"[185].

In questo senso e a tale scopo può essere affermato che l'UE ha saputo utilizzare efficacemente la protezione dei dati e la tutela della vita privata nel trasferimento di dati oltre i confini europei come mezzo e strumento per affermare l'Unione stessa come una "the fortress of digital privacy"[186] nel panorama internazionale, trasformando, mediante il meccanismo dell'adeguatezza, i propri standard di tutela in "*de facto* standard"[187] internazionali a garanzia dei diritti fondamentali sanciti dagli artt. 7 e 8 della Carta. Un tale approccio ha avuto effetti espansivi positivi in altri ordinamenti, sotto il profilo delle scelte adottate sia dai soggetti privati che dalle autorità pubbliche. Con riferimento ai soggetti privati, ed in primis alle aziende operanti nel settore digitale, aventi sede fuori dal territorio europeo ma riceventi dati dall'UE, molte di esse hanno o stanno allineando le proprie *policies* in materia di tutela della vita privata e protezione dei dati a quanto indicato dalla normativa e giurisprudenza europea, reputando tale

[183] Il rischio è infatti quello di creare una situazione di 'isolamento' dell'UE, data dalla difficoltà da parte degli Stati terzi di negoziare accordi conformi agli standard europei o dalla reticenza e diffidenza degli Stati terzi stessi che, pur interessati ad attivare lunghi e costosi procedimenti di negoziazione, potrebbero essere scoraggiati, come già si è detto, dal timore dell'instabilità dell'accordo ottenuto e della relativa decisione di adeguatezza, che potrebbero essere invalidati dalla Corte. Di fronte a questa consapevolezza e vedendo nel raggiungimento di un accordo internazionale che fissi livelli globali di tutela della privacy e di protezione dei dati l'unica possibile soluzione per ovviare ai pericoli insiti nella sussistenza di differenti standard di garanzia nazionale, alcuni autori, come Reidenberg, ritengono che l'UE debba rassegnarsi ad accettare l'idea che il proprio livello di tutela non venga adottato in Stati terzi (J. REIDENBERG, *The transparent citizen,* in *Loyola University Chicago Law Journal*, 47, 2015, p. 437).

[184] "L'Unione può svolgere un ruolo chiave e di guida, valorizzando siffatto modello [frutto dei principi delineati nella giurisprudenza della CGUE e nella normativa GDPR] nell'ambito di fora internazionali, nella prospettiva della costruzione di un regime internazionale di tutela della vita privata e delle informazioni personali, sia che si scelga la strada della conclusione di un trattato internazionale, sia che gli Stati stabiliscano un modello giuridico internazionale sulla falsariga del modello UNCITRAL", M. NINO: *Le prospettive internazionali ed europee della tutela della privacy*, op. cit., p. 785.

[185] M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, op. cit., p. 17.

[186] F. FABBRINI, *The EU Charter of Fundamental Rights and the rights to data privacy: the EU Court of Justice as a Human Rights Court*, in S. DE VRIES et al. (a cura di), *The EU Charter of Fundamental Rights as a binding instrument: five years old and growing*, Bloomsbury, 2015, p. 261; W. B. WRAY, *A European approach to the United States Constitutional privacy*, Craighton International and Comparative Law Review, 2015, p. 51; L. P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of the EU and US constitutional systems*, op. cit.

[187] M. BRKAN, *The unstoppable expansion of the EU fundamental right to data protection. little shop of horrors?*, in *Maastricht Journal of European and Comparative Law*, 5, 2016.

scelta più conveniente e meno rischiosa – per quanto almeno inizialmente più onerosa –, al fine ultimo di evitare di perdere la possibilità di ottenere dati provenienti dall'Unione e quindi subire un forte svantaggio competitivo ed economico[188]. Oltre a predisporre politiche interne o ad utilizzare strumenti alternativi volti a dimostrare l'adeguatezza delle tutele disposte, in caso di assenza di una decisione di adeguatezza della Commissione, i soggetti privati possono utilmente fare leva sui legislatori nazionali degli Stati terzi affinché approvino normative di tutela e garanzia della riservatezza e protezione dei dati capaci di consentire un maggior riavvicinamento agli standard europei[189].

L'impatto della normativa e giurisprudenza dell'UE in materia di trasferimento dati si riverbera però anche sulle scelte legislative di Stati terzi o dei loro giudici[190]: basti pensare al recente esempio dello Stato della California che, in assenza di una normativa federale in materia di protezione dei dati, ha adottato nel 2018 il *California Consumer Privacy Act* (CCPA), chiaramente ispirato alla disciplina del GDPR[191], a dimostrazione di quanto l'assetto normativo europeo e le condizioni fissate per il trasferimento dei dati abbiano, in alcuni casi, incentivato gli Stati terzi ad incrementare o migliorare le proprie normative in materia; è quello che Bradford ha definito *Brussels effect*, considerando "the unprecedented and deeply underestimated global power that the European Union is exercising through its legal institutions and standards, and how it successfully exports that influence to the rest of the world" e che si esplica anche attraverso le azioni esterne dell'UE sino ad ora descritte nell'ambito della tutela della privacy e protezione dei dati[192]. Questo approccio dunque può essere iscritto "con coerenza all'interno della dinamica di competizione regolatoria (..), dove ai ripetuti fenomeni di violazione transfrontaliera dei diritti fondamentali – resi possibili dallo sviluppo delle tecnologie dell'informazione e della comunicazione – corrispondono puntualmente meccanismi di reazione a carattere

---

[188] "Multinational corporations have adjusted their global data management systems to reduce their compliance costs with multiple regulatory regimes", A. BRADFORD, *The Brussels effect*, op. cit., p. 25. Ma si pensi anche, a titolo di esempio, al fatto che una grande multinazionale statunitense quale Microsoft abbia promosso "una causa contro il governo americano a difesa della extraterritorialità dei dati contenuti sui propri server situati in Europa, iniziativa che ha goduto dell'appoggio di molte imprese del settore ICT", e che è volta a sottrarre i dati all'accesso e controllo da parte delle autorità pubbliche statunitensi, così A. MANTELERO, *I flussi di dati transfrontalieri*, op. cit., p. 259. Oppure ancora: "In the short term, organisations may consider keeping personal data in the EU and avoiding transfers to the US. Some US companies offer cloud customers the option to store personal data in Europe so that it is not sent for storage elsewhere. For instance, Amazon announced on 6 November 2015 that it would be building data centres in the UK in 2016. A few days later, the CEO of Microsoft, Satya Nadella, also announced that Microsoft was opening data centres in the UK for the first time. The new data centres will enable UK users of Microsoft's cloud services, Azure and Office 365, to keep their data within Europe at all times. Companies that provide cloud services within the EU and rely on data centres in the US may invest in data centres within the EU provided they sign contracts with European companies only. European based cloud providers that ensure compliance with EU law could thus benefit from the situation", X. TRACOL, *"Invalidator" strikes back: the harbour has never been safe*, op. cit. Sin dal 2000 non si era mancato di sottolineare come i principi *Safe Harbour* avessero contribuito ad innalzare gli standard di protezione dei dati di tutela della riservatezza negli USA: sul punto si legga G. SHAFFER, *Globalization and social protection: the impact of EU and International Rules in the ratcheting up of US data privacy standards*, in *Yale Journal of International Law*, 25, 2000.

[189] Si legga ampiamente sul punto UNCTAD, *Data protection regulations and international data flows: implications for trade and development*, 2016.

[190] Nella sentenza destinata a divenire una pietra miliare della giurisprudenza Indiana, *Puttaswamy v. Union of India* – di cui si è già parlato nel Capitolo I, Parte I – la Corte Suprema indiana ha più volte richiamato la giurisprudenza dell'UE in materia di *data retention*, giungendo ad affermare per la prima volta in India che '[p]rivacy is the constitutional core of human dignity' e ammonendo il legislatore federale dell'esigenza di porre in essere un regime normativo unitario di tutela della privacy e protezione dei dati.

[191] L'atto è entrato in vigore nel gennaio 2020: alcune disposizioni di questo testo normativo sono molto simili a quanto disposto nel GDPR, garantendo quindi alti livelli di protezione, tanto da far ritenere questa normativa come quella maggiormente garantista in materia di privacy e *data protection* in tutti gli Stati Uniti. Sono incluse previsioni circa il diritto di accesso, il diritto di *opt-out*, il diritto di azione in caso di *data-breach*, sanzioni amministrative, diritto all'oblio (tale diritto presenta però notevoli differenze rispetto alla versione europea, facendo emergere quell'innegabile distanza insita nelle peculiarità dei diversi ordinamenti).

[192] Utilizzando il termine impiegato da A. BRADFORD, *The Brussels effect*, op. cit., p. 1.

dichiaratamente 'nazionalistico'. Tale termine non è impiegato in un'accezione dispregiativa, bensì per denotare l'impronta tipicamente 'locale' del modello di disciplina (e di bilanciamento degli interessi) che si intende proteggere, a fronte dei rischi di aggiramento derivanti dall'utilizzo delle tecnologie informatiche e dalla de-localizzazione dei dati su server remoti"[193]. Ecco dunque che in questa ottica, l'azione dell'UE si è positivamente riflessa sugli Stati terzi, sia mediante lo strumento della decisione di adeguatezza, utilizzato quale moderna forma di 'gunboat diplomacy'[194] per indurre ad una modifica nel Paese terzo del proprio livello di tutela (o, talvolta, per portare alla introduzione, per la prima volta, di disposizioni in materia)[195], sia attraverso azioni promosse a livello delle organizzazioni internazionali[196], incoraggiando ad esempio l'adesione alla Convenzione del Consiglio d'Europa n. 108, esaminata nel Capitolo I, Parte I.

[193] G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio,* in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016, p. 45.

[194] M. TZANOU, *European Union regulation of transatlantic data transfers and online* surveillance, op. cit., p. 552.

[195] Secondo Mitsilegas, proprio l'utilizzo del meccanismo di adeguatezza, ha prodotto, quale risultato, che "a system of generalized pre-emptive surveillance which has been imposed unilaterally by the US as an emergency post-9/11 response, potentially becomes normalised via EU action on a global scale, notwithstanding the persistent concerns with regard to the compatibility of such a system with European human rights law", V. MITSILEGAS, *The value of privacy in an era of security: embedding constitutional limits on preemptive surveillance*, in *International Political Sociology*, 1, 2014, p. 105.

[196] Adottando, ad esempio, come si è visto, in sede dell'ICAO, una posizione unitaria di tutti gli Stati membri, finalizzata a promuovere una modifica a livello internazionale degli standard in materia di PNR che vada nella direzione di una maggiore garanzia dei diritti fondamentali (COM(2019) 416 final).

CAPITOLO IV

I PIÙ RECENTI SVILUPPI IN MATERIA DI *DATA RETENTION*: UNA STRADA ANCORA LUNGA PER IL LEGISLATORE E IL GIUDICE EUROPEO

Nei capitoli precedenti e, in particolare, al termine del Capitolo II, sono stati messi in rilievo i quesiti e gli aspetti problematici ancora aperti in materia di *data retention* e accesso ai metadati derivanti da telecomunicazioni elettroniche: come si è avuto modo di vedere, molte delle criticità legate a questa delicata disciplina sono rimaste irrisolte e permangono sino ad oggi, nonostante i numerosi interventi della Corte di giustizia dell'UE – nonché di Corti e legislatori nazionali – che hanno cercato di determinare quel necessario punto di equilibrio tra l'utilizzo di tali strumenti di lotta alla criminalità grave e il rispetto dei diritti fondamentali. Questo arduo compito è stato reso ancor più complicato dall'assordante silenzio del legislatore europeo che, a seguito della sentenza *DRI*, non è più intervenuto a colmare il vuoto normativo creatosi dalla invalidazione della DRD e neppure a chiarimento dei vaghi criteri indicati dal dettato normativo dell'art. 15 Direttiva *e-Privacy*. Anche da questo atteggiamento, risulta evidente la complessità di regolamentare un ambito, quello della conservazione e accesso ai metadati, estremamente insidioso e rispetto al quale gli Stati membri, benché in diversa misura e con differenti approcci, hanno incontrato serie difficoltà, soprattutto nell'incorporare nella disciplina normativa nazionale i dettami della giurisprudenza europea senza compromettere l'utilità ed efficacia della *data retention* stessa e del successivo utilizzo dei metadati. Se tale articolata situazione era già emersa con chiarezza nella sentenza *Tele2* e nelle osservazioni indicate dagli Stati intervenuti nel procedimento, essa viene ribadita anche – e con maggior forza – nei più recenti rinvii pregiudiziali, attualmente pendenti, oltre che nel dibattito instauratosi in seno al Consiglio e alla Commissione, volto a valutare l'opportunità di un nuovo intervento del legislatore europeo in materia.

Obiettivo di questo Capitolo dunque è quello di fotografare la situazione attuale nel contesto dell'UE, sia sotto il profilo giurisprudenziale che legislativo, partendo dall'analisi della decisione *Ministerio Fiscal*, primo frutto di quelle criticità e lacune rimaste aperte dalla sentenza *Tele2*, per arrivare poi allo studio dei ben sei rinvii pregiudiziali al momento pendenti – due dei quali saranno oggetto di attenzione anche nella Parte III –, con lo scopo ultimo di comprendere rispetto a quali profili critici ed incerti la CGUE sia stata nuovamente chiamata a pronunciarsi e quali siano invece i punti fermi che dalla giurisprudenza europea sin qui analizzata possono essere individuati, non solo nell'ambito della disciplina della *data retention* bensì anche con riferimento alle connessioni e agli intrecci con le pronunce attinenti al trasferimento di dati verso Stati terzi, esaminate nel previo Capitolo. Una tale analisi permetterà di meglio comprendere le difficoltà presenti sul tavolo del legislatore dell'UE e le soluzioni o approcci presentati dai diversi attori che operano nel panorama europeo.

1. – L'art. 15 Direttiva e-Privacy *nuovamente sottoposto all'intervento chiarificatore della CGUE: la sentenza* Ministerio Fiscal *e i requisiti dell'accesso ai metadati conservati*

Successivamente alla sentenza *Tele2*, il primo caso che sottopone nuovamente alla Corte di giustizia dell'UE una questione attinente alla disciplina della *data retention* e dell'accesso ai metadati per scopi securitari è da rinvenirsi nel rinvio pregiudiziale *Ministerio Fiscal*, conclusosi con la pronuncia del 2

ottobre 2018[1]. Viene dunque, ancora una volta, offerta ai giudici di Lussemburgo l'occasione per fornire una interpretazione dell'art. 15 della Direttiva 2002/58, chiarendo così quei dibattuti requisiti faticosamente fissati nella previa giurisprudenza europea.

Nella specifica controversia che si vuole in questa sede analizzare, tuttavia, i dubbi del giudice del rinvio si sono principalmente concentrati, anziché sul profilo della conservazione, su quello altrettanto complesso dell'accesso ai metadati, ed in particolare, sul fondamentale ma dubbio criterio della 'gravità dei reati'.

Ricostruendo brevemente la questione pregiudiziale, essa trae origine da un caso di rapina ai danni di un cittadino spagnolo, il signor Sierra, che in quella occasione subiva anche il furto del proprio cellulare. Per risalire all'autore del reato, la polizia giudiziaria spagnola decideva di seguire proprio le tracce del telefono: al fine di attivare una SIM e dunque aprire una utenza presso un fornitore di servizi di telecomunicazione, è necessario fornire al *service provider*, oltre alle informazioni relative alla propria identità, anche il codice relativo all'identificatore internazionale di apparecchiature mobili, c.d. codice IMEI, che identifica il dispositivo sul quale si intende attivare l'utenza stessa. La polizia pertanto decideva di ingiungere a tutte le maggiori compagnie telefoniche di verificare nei propri database, contenenti i dati di attivazione di SIM, se vi fosse una utenza aperta utilizzando il codice IMEI del dispositivo rubato. Così facendo, la polizia avrebbe potuto risalire al numero telefonico e all'identità del soggetto che aveva attivato l'utenza sul telefono oggetto di furto e che poteva essere, presumibilmente, l'autore stesso del furto o comunque una persona a conoscenza di informazioni utili alle indagini. Dinnanzi a tale linea investigativa proposta dagli agenti, però, il giudice istruttore si era rifiutato di emanare l'ingiunzione necessaria rivolta ai fornitori di servizi di telefonia: la legge spagnola n. 25/2007[2] stabiliva infatti la possibilità di accesso e comunicazione dei dati conservati dagli operatori di telecomunicazioni solo in caso di reati gravi che, ai sensi del codice penale nazionale, risultavano essere solo quelli puniti con detenzione superiore a cinque anni. Poiché il furto non rientrava nella definizione data dall'ordinamento spagnolo di reato grave, la richiesta di accesso ai dati veniva respinta il 5 maggio 2015. Il pubblico ministero, dinnanzi a tale diniego, proponeva appello di fronte alla *Audiencia Provincial de Tarragona* (Corte provinciale di Tarragona). Quest'ultima rilevava l'esistenza di una ulteriore fonte normativa di riferimento, applicabile al caso in esame ed approvata in un momento successivo al provvedimento impugnato: la legge organica n. 13/2015[3]. Tale normativa incideva sulle modalità di determinazione del concetto di "gravità" del reato, stabilendo – diversamente dalla disposizione della legge n. 25/2007 cui il giudice istruttore aveva fatto riferimento – due criteri alternativi: uno materiale, identificato nella rilevanza criminosa della condotta e nella grave lesione dei beni giuridici, e uno formale, meramente basato sulla durata della pena che doveva essere maggiore di tre anni. Ebbene, quest'ultimo criterio, che disponeva un termine temporale inferiore a quello indicato nella normativa del 2007 e che avrebbe avuto quale esito quello di portare al superamento della soglia di gravità la maggior parte dei reati previsti dall'ordinamento spagnolo, faceva sorgere in capo al giudice dell'appello un dubbio di conformità della normativa nazionale rispetto alla tutela dei diritti fondamentali sanciti dalla Carta di Nizza e ai principi enucleati della Corte di Giustizia nella pronuncia *Digital Rights Ireland*[4]. Di fronte a tali dubbi, il giudice spagnolo sottoponeva dunque alla Corte di

[1] 2 ottobre 2018, C-207/16, *Ministerio Fiscal*; domanda di rinvio pregiudiziale promossa dall'*Audiencia Provincial de Tarragona*, con decisione del 6 aprile 2016.

[2] *Ley 25/2007 de conservación de datos relativos a las comunicaciones elecrtónicas y a la redes publicas de comunicaciones*, 18 ottobre 2007. Tale normativa trasponeva nel diritto nazionale la Direttiva 2006/24/CE.

[3] *Ley Organica 13/2015 de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantias procesales y la regulación de las medidas de investigación tecnológica*, 5 ottobre 2015.

[4] Merita sin da ora ricordare che il criterio di 'gravità' come elemento necessario e limitativo della disciplina della conservazione e dell'accesso ai metadati era espressamente inserito nella Direttiva 2006/24, laddove veniva fatto esplicito riferimento al fatto che la *data retention* dovesse essere limitata, nel suo scopo, alla repressione di reati gravi, la cui definizione veniva però lasciata a ciascun legislatore nazionale, come ben messo in luce nel Capitolo

Giustizia due questioni pregiudiziali, chiedendo in primis se la soglia di gravità potesse essere "individuata prendendo in considerazione unicamente la pena irrogabile per il reato oggetto di indagine o se sia inoltre necessario rilevare nella condotta criminosa particolari livelli di lesività nei confronti dei beni giuridici individuali e/o collettivi" (par. 25) e dunque se sia sufficiente utilizzare per la determinazione della gravità un criterio meramente formale o se sia necessario il rispetto, contestualmente, anche di un criterio materiale; in secundis, nel caso in cui la determinazione della gravità del reato sulla sola base della durata della pena fosse risultata conforme ai principi costituzionali dell'Unione "applicati dalla CGUE nell'ambito della sentenza *DRI*", il giudice del rinvio richiedeva di indicare quale dovesse essere tale soglia temporale e se essa fosse compatibile con il limite di tre anni di reclusione indicato dalla discussa normativa spagnola.

Il rinvio pregiudiziale descritto, proposto nell'aprile 2016, era stato sospeso dalla CGUE in attesa della sentenza relativa al caso *Tele2* che avrebbe potuto, potenzialmente, già rispondere ai quesiti posti dal giudice spagnolo. A seguito di tale decisione, tuttavia, il giudice del rinvio aveva mantenuto ferme le proprie domande, ritenendo che "sebbene detta pronuncia [*Tele2*] fornisse esempi di reati gravi, non definiva in modo sufficientemente chiaro il contenuto sostanziale della nozione di gravità del reato che può servire da criterio di valutazione della giustificazione di una misura d'ingerenza"[5]; il caso quindi veniva ripreso dinnanzi alla CGUE il 16 febbraio 2017. Impossibile non rilevare, sin da questo primo aspetto sottolineato dal giudice spagnolo a motivazione della necessità di proseguire con il rinvio promosso, come anche a seguito della sentenza *Tele2* fossero comunque rimasti rilevanti dubbi ed incertezze relativamente ai limiti fissati dall'art. 15 Direttiva *e-Privacy* e all'interpretazione di essi fornita dalla giurisprudenza sino ad ora analizzata.

1.1. – La riconducibilità della disciplina dell'accesso all'ambito di applicazione della Direttiva e-Privacy *tra conferma dell'orientamento emerso dalla previa giurisprudenza e persistenti dubbi*

Nel caso *Ministerio Fiscal* la Corte, con una decisione relativamente breve, ha fornito una prima risposta alle perplessità e criticità emerse sin dalla sentenza *DRI* in materia di conservazione ed accesso ai metadati, partendo innanzitutto dalle eccezioni di incompetenza della Corte di giustizia sollevate dal governo spagnolo e condivise anche dal Regno Unito. Questi ultimi ritenevano infatti che la domanda di accesso ai dati, promossa da autorità nazionali di *law enforcement* avverso i fornitori di servizi di comunicazione elettronica, rientrasse nell'esercizio dello *ius puniendi*, ricompreso nel novero delle attività escluse dalla disciplina della Direttiva 2002/58, ai sensi del suo art. 1, co. 3, già richiamato nei precedenti Capitoli: si riproponeva quindi quell'aspetto così problematico e ancora discusso relativo all'ambito di applicazione della Direttiva *e-Privacy* nonché, conseguentemente, ai confini tra competenze dell'Unione europea e degli Stati membri in questo specifico ambito. Tale punto, lo si vuole ricordare, è tutt'altro che meramente formale: da esso discende la possibilità o meno di applicare il diritto dell'UE e dunque la Carta di Nizza, nonché la possibilità di pronunciarsi da parte della Corte di giustizia; stabilire pertanto che la disciplina dell'accesso ai metadati per scopi di lotta alla criminalità grave non può considerarsi rientrante nell'ambito di applicazione della Direttiva 2002/58 significherebbe escludere anche l'applicazione dei criteri e dei requisiti individuati dalla giurisprudenza europea, in particolare nelle sentenze *DRI* e *Tele2*.

I. Il dato letterale dell'art. 15 dir. 2002/58/CE, invece, non qualifica in alcun modo il carattere del reato: è stata la Corte di giustizia, nella sentenza *Tele2*, a mutuare il criterio di "gravità" della DRD trasponendolo nell'ambito della interpretazione dell'art. 15 ed identificandolo come uno dei criteri in grado di giustificare e rendere proporzionata la conservazione dei dati e l'accesso agli stessi per scopi investigativi.

[5] Conclusioni dell'Avvocato generale Henrik Saugmandsgaard Øe, 3 maggio 2018, par. 27.

I giudici di Lussemburgo hanno sciolto questo delicato e rilevante primo nodo con grande velocità, ripercorrendo e riproponendo, come si vedrà non senza problemi, lo stesso ragionamento seguito nella pronuncia *Tele2*: le normative nazionali adottate sulla base della deroga sancita dall'art. 15 Direttiva *e-Privacy* vengono per questo stesso fatto "attirate" nell'ambito di applicazione della Direttiva, anche nel caso in cui "rimandino ad attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati" (par. 34) e persino quando le finalità perseguite dalle leggi interne coincidano sostanzialmente con quelle indicate nel citato art. 1, co. 3. L'art. 15 è deputato infatti a stabilire le condizioni di legittimità delle norme nazionali adottate in materia di conservazione dei dati e questo basta a permette di ricomprendere queste ultime nel campo d'azione della Direttiva stessa e, più ampiamente, del diritto dell'UE.

Sempre con un breve paragrafo e sempre – sbrigativamente – richiamando le conclusioni adottate sul tema nella pronuncia *Tele2*, i giudici di Lussemburgo hanno risolto anche l'ulteriore aspetto critico attinente alla propria competenza, ovverosia quello della riconducibilità all'ambito di applicazione della Direttiva 2002/58 delle operazioni di accesso: la Corte, infatti, aveva già in passato affermato come rientrassero nell'ambito di applicazione della Direttiva *e-Privacy* non solo le norme in materia di *data retention* ma anche quelle riguardanti l'accesso delle autorità statali di *law enforcement* ai dati conservati dai fornitori di servizi di comunicazioni elettroniche (par. 35). Ciò sulla base del fatto che le operazioni di accesso, al pari di quelle di conservazione, prevedono un trattamento dei dati da parte degli operatori dei servizi di telecomunicazione[6] e sono pertanto da considerarsi come attività di attori privati e non attività proprie degli Stati. La legge n. 25/2007 spagnola, ad esempio, consentendo alla polizia, sulla base di una previa autorizzazione giudiziaria, di obbligare i fornitori a mettere a disposizione i dati conservati, richiede di fatto ai *service providers* di svolgere un trattamento dei dati stessi, diverso ed ulteriore da quello di conservazione (par. 38)[7].

Anche il fatto che i dati per i quali viene richiesto l'accesso siano limitati ai numeri di telefono e dunque alle SIM attivate utilizzando uno specifico codice IMEI nonché a nome, cognome ed indirizzo degli utenti cui la SIM appartiene, non può portare a ritenere che la normativa spagnola richiamata non rientri nell'ambito di applicazione della Direttiva 2002/58: il governo spagnolo, danese, irlandese, lettone, del Regno Unito e la Commissione avevano sostenuto che i dati relativi all'identità dell'utente non potessero rientrare nella nozione di "dati relativi al traffico" così come definita dall'art. 2 della Direttiva stessa[8]. Sul punto la Corte, così come l'Avvocato generale, hanno invece concluso che, sebbene tali informazioni non riguardino il 'traffico' propriamente detto, esse non di meno rientrano tra i dati necessari per la fornitura di un servizio e per la fatturazione e pertanto nelle categorie di dati rispetto alle quali la Direttiva *e-Privacy* è applicabile[9]. La Corte con grande chiarezza ha stabilito che

[6] Con riferimento al fatto che anche le operazioni di accesso ai dati conservati possano essere ricondotte alla definizione di 'trattamento del dato', la Corte richiama quanto già affermato nel noto *Parere 1/15* in materia di PNR, di cui si è ampiamente parlato nel Capitolo III e nel quale i giudici avevano ribadito come l'accesso costituisse una forma di trattamento del dato, rappresentando una ingerenza distinta e autonoma rispetto alla conservazione (par. 51).

[7] Sul punto si leggano similmente anche le Conclusioni dell'Avvocato Generale al par. 46.

[8] L'art. 2, co. 2, lett. b) definisce 'dati relativi al traffico' "qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione".

[9] La Corte e l'Avvocato generale inoltre sul punto richiamano il Considerando 15 della Direttiva *e-Privacy*, nel quale viene espresso come i dati relativi al traffico comprendano anche il nome e l'indirizzo della persona che utilizza un collegamento al fine di effettuare una comunicazione, oltre ai dati relativi alla comunicazione in sé e per sé (par. 42). L'Avvocato generale similmente, con riferimento al Considerando 15, parla di una "concezione elastica della normazione di comunicazione, includendovi segnatamente un indirizzo fornito da chi emette la comunicazione" (par. 55). Questo profilo specifico è tutt'altro che residuale o scontato: "This is an important aspect of the judgment, because it requires subscriber data (the name and the IMEI address of the mobile device) to be protected in the same way as traffic data, even though they do not form part of an electronic communication. In consequence, access to such data falls within the safeguards of the ePrivacy Directive, and these safeguards cannot be circumvented by creating a separate category of subscriber data. This has important consequences for

tale Direttiva copre qualsiasi trattamento di dati personali nell'ambito della fornitura di servizi di comunicazione elettronica e che la nozione di dati relativi al traffico comprende "qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione" (par. 41)[10].

Con riferimento a questi primi aspetti esaminati e risolti dalla Corte, emerge subito come nulla di nuovo venga affermato rispetto alle previe sentenze, alle quali anzi i giudici attingono a piene mani, richiamando i nodi più rilevanti che avevano già permesso, nella sentenza *Tele2* in particolare, di ricondurre le normative nazionali 'eccezionali' e 'derogatorie', adottate sulla base dell'art. 15, all'ambito di applicazione della Direttiva 2002/58 non solo nella parte in cui esse disciplinavano la conservazione dei dati, ma anche con riferimento alla regolamentazione dell'accesso ai dati stessi[11]. Viene pertanto ribadito il superamento, indubbiamente influenzato anche dal nuovo assetto dettato dal Trattato di Lisbona, di quella rigida distinzione tra disciplina della *data retention* e dell'accesso che, in un primo momento, era stata abbracciata dalla Corte e che l'aveva portata a far salva la DRD e la sua base giuridica nella sentenza *Irlanda c. Parlamento e Consiglio*; viene, in altre parole, riconfermata la "concezione unitaria che considera i due momenti della "conservazione" e dell'"accesso" come espressione di un atto invero complessivamente unitario"[12], fornendo così una interpretazione da alcuni autori[13] ritenuta 'estensiva' dell'art. 15, già proposta sin dalla *Tele2*. Non bisogna però pensare che, alla luce dell'ampio richiamo alla giurisprudenza precedente, la questione sollevata dal governo spagnolo fosse di semplice e scontata soluzione: in realtà l'interpretazione della Corte, già all'epoca della pronuncia *Tele2*, non aveva mancato, come si è visto nel Capitolo II, di sollevare serie perplessità nella dottrina e nei governi nazionali[14]. La lettura proposta dai giudici di Lussemburgo in *Ministerio Fiscal* dunque porta inevitabilmente alla riproposizione delle medesime criticità e dubbi, in assenza di ulteriori elementi chiarificatori. Ed è proprio sotto questo profilo che merita di essere sottolineata la posizione dell'Avvocato generale nelle sue Conclusioni che, pur non essendo stata ripresa dalla Corte, aggiunge un ulteriore spunto di riflessione. L'Avvocato generale infatti afferma la necessità di distinguere da una parte i dati personali trattati "*direttamente* nell'ambito delle attività – di natura sovrana – dello Stato in un settore rientrante nel diritto penale e, dall'altra, quelli trattati nell'ambito delle attività – di natura

---

pending legislation.", così C. DOCKSEY, *Ministerio Fiscal: holding the line on ePrivacy*, in *Maastricht Journal of European and Comparative Law*, 4, 2019, p. 592.

[10] L. Woods peraltro rileva, in un primo commento, come questa ricostruzione della CGUE sia contraria alla sentenza *Liberty* della *Divisional Court* inglese, che sul punto aveva rifiutato di rinviare la questione al giudice europeo (*Liberty v. Secretary of State for the Home Department*, 2018 EWHAC 975). In quella pronuncia infatti la Corte d'oltremanica confermava la tesi del Governo del Regno Unito – espressa anche nel caso *Ministerio Fiscal* – secondo cui gli "entity data", ovvero quei dati relativi all'identificazione dell'utente, non possono essere ritenuti rientranti nell'ambito di applicazione della Direttiva *e-Privacy* e che, conseguentemente, non si possono ad essi applicare i criteri individuati dalla sentenza *Tele2*. La posizione della Corte di giustizia, che ha invece sostenuto la tesi contraria, potrebbe dunque avere implicazioni anche sulla giurisprudenza inglese in materia e sulla interpretazione fornita dai giudici del Regno Unito. Sul punto più approfonditamente: L. WOODS, *Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers*, in *EU Law Analysis*, 4 ottobre 2018, http://eulawanalysis.blogspot.com/2018/10/mobile-phone-theft-and-eu-eprivacy-law.html.

[11] "Rientra del pari nel suddetto ambito di applicazione (della Dir. 2002/58/CE) una misura legislativa riguardante, come nel procedimento principale, l'accesso delle autorità nazionali ai dati conservati dai fornitori di servizi di comunicazione elettronica. Infatti, la tutela della riservatezza delle comunicazioni elettroniche e dei dati relativi al traffico afferenti alle stesse, garantita dall'art. 5, par. 1, della Direttiva 2002/58, si applica alle misure adottate da tutti i soggetti diversi dagli utenti, indipendentemente dal fatto che si tratti di persone o di entità private oppure di entità statali" (par. 76-77, *Tele2*).

[12] O. POLLICINO, M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 9 gennaio 2017, p. 5.

[13] D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* op. cit.

[14] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, in *ERA Forum*, Springer, 2018; ma anche L. WOODS, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber),* in *EU Law Analysis*, 21 dicembre 2016, http://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html.

commerciale – di un fornitore di servizi di comunicazione elettronica che sono *successivamente* utilizzati dalle autorità statali competenti" (par. 47). Riferendosi dunque ad attività "sovrane" dello Stato come a quelle che si "riferiscono alle funzioni riservate allo Stato o ai suoi apparati, che esso non può delegare ad enti privati, in particolare, quelle relative alla giustizia, alla polizia o alle forze armate" (nota 43), l'Avvocato generale ritiene tra di esse rientranti il trattamento dei dati da parte di "autorità di polizia o giudiziarie al fine di ricercare gli autori di reati, ad esempio i dati raccolti e analizzati durante un'intercettazione di conversazioni telefoniche effettuata da agenti di polizia su richiesta di un giudice istruttore" (nota 44). Sulla base di questo ragionamento, e sebbene l'Avvocato non si spinga a portare a conclusione con chiarezza le conseguenze della differenziazione proposta, la prima tipologia di trattamento e accesso ai dati esulerebbe dall'ambito di applicazione della Direttiva *e-Privacy*, rientrando nella esclusione di cui all'art. 1, co. 3, mentre la seconda, avendo alla base un trattamento operato da fornitori di servizi privati, ne sarebbe invece ricompresa. Del resto è lo stesso Avvocato a sottolineare come nella pronuncia in esame non si intendano affrontare questioni, pur in parte sollevate dal governo spagnolo, circa l'interpretazione dell'art. 1, co. 3 Direttiva 2002/58 e dunque dei limiti di applicazione del diritto dell'UE. Questo per due ordini di ragioni: innanzitutto perché "alla Corte è stata recentemente sottoposta una domanda di pronuncia pregiudiziale vertente, in particolare, sull'interpretazione dell'art. 1, par. 3, della Direttiva 2002/58 nel contesto dell'utilizzo, da parte dei servizi di sicurezza e di informazione di uno Stato membro [agenzie di intelligence] di dati che devono essere loro trasmessi in massa da tali fornitori" (par. 47). Viene fatto riferimento in questo caso al rinvio pregiudiziale *Privacy International* promosso dal Regno Unito, di cui si parlerà nel prossimo paragrafo, nel quale l'attenzione viene posta proprio sulla estensione dei "requisiti *Tele2*" stabiliti dalla CGUE anche agli ambiti di azione degli Stati membri riconducibili più propriamente alla sicurezza nazionale e dunque a quelle attività indicate all'art. 1, co. 3 della Direttiva stessa. Il secondo motivo è da individuarsi nella distinzione dei fatti e delle ingerenze nei diritti fondamentali posti alla base del rinvio pregiudiziale in esame e quelli invece caratterizzanti il pendente rinvio *Privacy International*: nel caso concreto da cui *Ministerio Fiscal* origina, infatti, non si riscontra, diversamente dalla disciplina oggetto del rinvio del Regno Unito, una trasmissione di dati massiva e generalizzata bensì solamente un accesso mirato, ristretto cioè a quei soli dati circa il numero di utenza – e l'identità dell'utente associato – attivato utilizzando lo specifico codice IMEI del telefono rubato. Secondo l'Avvocato generale quindi la diversità indicata e la riconducibilità del trattamento oggetto del rinvio in esame a quello operato dai fornitori privati rende inutile e non necessario, nel caso in esame, risolvere la più complessa questione oggetto invece del rinvio *Privacy International*. Ciò che risulta chiaro, in ogni caso, anche dalla posizione e dal ragionamento espresso dall'Avvocato generale, è la complessità e delicatezza di tale punto e le conseguenze che ne derivano. Da un lato, ricomprendere le attività riguardanti l'accesso all'interno dell'ambito di applicazione della Direttiva *e-Privacy* permette alla Corte di pronunciarsi sul punto e di estendere il bilanciamento con i diritti fondamentali anche sul fronte di una operazione certamente invasiva nei diritti alla riservatezza e alla protezione dei dati, quale l'accesso. Dall'altro, pare altrettanto vero che il confine tra le attività ricomprese nella Direttiva e quelle invece escluse risulta estremamente sottile ed incerto, tanto da spingere il Regno Unito a promuovere un apposito rinvio sul tema.

1.2. – La determinazione del binomio 'gravità dell'ingerenza-gravità del reato': una importante precisazione dei giudici di Lussemburgo

Dopo aver trattato ed analizzato le questioni maggiormente 'formali' preliminarmente affrontate dalla Corte, si vogliono ora esaminare i punti sostanziali riguardanti più specificamente i quesiti promossi dal giudice del rinvio attinenti al rilevante criterio di 'gravità' del reato. Quello che viene immediatamente svolto dai giudici di Lussemburgo è una riformulazione della prima domanda

pregiudiziale proposta dal giudice spagnolo. Essa infatti viene fatta precedere dall'introduzione di un passaggio preliminare aggiuntivo, individuato dalla Corte: prima di stabilire quali elementi (materiali o formali) debbano essere utilizzati per determinare il carattere di 'gravità' del reato, è necessario innanzitutto valutare se l'ingerenza rispetto ai diritti fondamentali, rappresentata dall'accesso a determinati dati, sia tale da richiedere, al fine di essere giustificata e legittima, la gravità del crimine perseguito. Solo dopo aver risposto a tale quesito si potranno individuare i criteri che definiscono la gravità del reato, rispondendo così agli interrogativi posti dal giudice spagnolo[15].

Seguendo questa riformulazione[16], la Corte specifica poi preventivamente che non saranno oggetto di valutazione e resteranno quindi esclusi dal suo vaglio sia la conformità al diritto dell'Unione della disciplina della conservazione dei dati[17], sia ogni altro criterio di accesso ai dati individuato dalla previa giurisprudenza europea e diverso da quello di gravità del reato.

Concentrandosi dunque su quest'ultimo e pur premettendo che l'art. 15, come già sottolineato nei precedenti Capitoli, si limita a parlare di lotta ai crimini in generale senza alcuna ulteriore accezione di 'gravità', i giudici risolvono la questione di merito riformulata richiamando e meglio specificando quel rapporto consequenziale tra obiettivo perseguito e gravità dell'ingerenza già affermato nella pronuncia *Tele2*. In altre parole, sulla base del principio di proporzionalità, solo la lotta alla criminalità connotata dal carattere di gravità legittima una ingerenza grave nei diritti alla riservatezza e alla protezione dei dati. Ne deriva, ragionando a contrario, che, qualora l'ingerenza non sia grave, non sarà neppure necessaria, ai fini della legittimità dell'accesso stesso, la presenza di un reato grave. Ecco dunque che per comprendere se sia richiesta la natura grave del reato si dovrà svolgere una previa valutazione circa la natura grave o meno dell'ingerenza: nel caso *Tele2* la Corte aveva ritenuto sussistente una ingerenza grave rispetto ai diritti fondamentali poiché l'accesso aveva ad oggetto una mole indiscriminata di dati che "considerati nel loro insieme, consentono di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione" (par. 99, *Tele2*); nel caso in esame invece, come sottolineano i giudici, l'accesso avrebbe avuto ad oggetto non solo un ristretto numero di dati – quelli riferibili all'utenza telefonica attivata usando il codice IMEI del telefono rubato – ma anche una ristretta tipologia di dati cioè solo quelli che "mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e se del caso, l'indirizzo" (par. 48), dati peraltro ristretti ad

[15] "Con le sue due questioni (..) il giudice del rinvio chiede, in sostanza, se l'articolo 15, par. 1, della Direttiva 2002/58, letto alla luce degli articoli 7 e 8 della Carta, debba essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e se del caso l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta, che presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave e, in caso affermativo, sulla base di quali criteri dovrebbe essere valutata la gravità dell'infrazione in questione", par. 48.

[16] "Da una giurisprudenza costante risulta che, al fine di fornire al giudice del rinvio una risposta utile che gli consenta di dirimere la controversia di cui è stato investito, spetta alla Corte, se necessario, riformulare le questioni che le sono sottoposte", nota 83 delle Conclusioni dell'Avvocato generale, ma si veda anche il par. 87 della decisione della Corte.

[17] "Osservo che (..) le questioni pregiudiziali sollevate nella presente causa si caratterizzano per il fatto di vertere non già sulle condizioni della *conservazione* di dati personali nel settore delle comunicazioni elettroniche, bensì sulle modalità dell'*accesso* delle autorità nazionali a tali dati conservati dai fornitori di servizi operanti in tale settore. (..) Nel caso di specie, sembra che i dati personali a cui le autorità di polizia chiedono di accedere, ai fini investigativi, abbiano potuto essere archiviati dagli operatori di telefonia mobile in esecuzione di un obbligo derivante dalla legge spagnola (..) e la conformità dell'archiviazione dei dati alle prescrizioni del diritto dell'Unione non è messa in discussione nel procedimento principale" (par. 38 e 40, Conclusioni dell'Avvocato generale). Viene rimessa dunque al giudice del rinvio la valutazione della conformità della conservazione dei dati (e quindi della normativa nazionale che la disciplina) rispetto alle condizioni indicate dall'art. 15, Direttiva 2002/58.

uno specifico e limitato periodo di tempo di dodici giorni (par. 59)[18]. Ne deriva che l'accesso – che si può quasi definire un "*accesso targettizzato*" e mirato quanto alla quantità, tipologia dei dati e arco temporale coperto dall'accesso – rappresenta sì una ingerenza nei diritti fondamentali di cui agli artt. 7 e 8 della Carta di Nizza[19] ma non costituisce una ingerenza di tipo grave.

Giunti a tale conclusione ed applicando quel principio di proporzionalità prima individuato, che lega gravità dell'ingerenza a gravità del reato, la Corte è giunta a ritenere che l'intrusione 'lieve' rilevata nel caso specifico in esame non richieda, per essere giustificata, la lotta ad un crimine grave (par. 63). L'Avvocato generale, seguito poi dai giudici stessi, ha stabilito quindi che "nell'ipotesi di un'ingerenza non grave, si deve ritornare al principio di base risultante dal testo di tale disposizione [l'art. 15, dir 58/2002], vale a dire che qualsiasi tipo di 'reato' è idoneo a giustificare una siffatta ingerenza" (par. 89, Conclusioni dell'Avvocato generale).

Alla luce di queste considerazioni, ed avendo appurato che in casi di accesso ai dati quali quello sottoposto alla sua attenzione, non si rende necessaria la finalità di lotta alla criminalità grave, la Corte conclude così la sua pronuncia e non procede ulteriormente alla determinazione dei criteri volti a stabilire la natura 'grave' o meno del reato; mediante la riformulazione effettuata e il vaglio preventivo svolto circa la sussistenza di una grave ingerenza, la questione pregiudiziale dunque è stata risolta senza che di fatto si sia risposto ai quesiti posti dal giudice del rinvio.

Nonostante questo e per quanto la Corte di giustizia abbia concluso la propria decisione in poche pagine, la pronuncia non è certo da ritenersi priva di profili interessanti e di molteplici spunti di riflessione, soprattutto se si procede nello sforzo di leggerla all'interno del più ampio contesto post-*Tele2*: un tale tipo di analisi infatti permette di vedere come i dubbi e le perplessità avanzate dalla Corte spagnola siano retaggio ed eredità della previa giurisprudenza europea, dubbi e perplessità che peraltro permangono anche a seguito di questa nuova decisione e che verranno riproposti in particolare nel rinvio pregiudiziale al momento pendente e promosso dalla *Riigikohus*, la Corte Suprema estone, di cui si parlerà nel prossimo paragrafo.

Prima di addentrarsi in una analisi critica della pronuncia, è però certamente importante sgombrare sin da subito il campo da possibili letture eccessivamente estensive e, per certi versi, fuorvianti. Dopo una prima veloce analisi della sentenza si potrebbe cioè essere portati a vedere nella posizione della Corte una sorta di "revirement", di passo indietro, rispetto a quanto emerso dalle previe sentenze con riferimento alla importanza che era stata attribuita allo stringente requisito di gravità del reato: in altre parole, si potrebbe ritenere che la necessaria sussistenza di tale elemento sia valutata in questa pronuncia in maniera più blanda e che l'effetto possa quindi essere quello di restringere l'elenco rigoroso dei criteri

[18] "Questi dati non permettono di conoscere né la data, né l'ora, né la durata, né i destinatari delle comunicazioni effettuate con la o le carte SIM in questione, né i luoghi in cui dette comunicazioni sono avvenute o la frequenza di esse con talune persone nel corso di un determinato periodo. Questi dati non permettono quindi di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione" (par. 60). Qui è evidente come la particolare e specifica natura dei dati richiesti dalle autorità spagnole porti i giudici a conclusioni differenti rispetto a quelle indicate nel caso *Tele2*. Sul punto anche l'Avvocato generale ha precisato, nelle proprie Conclusioni che "il numero delle persone potenzialmente interessate dalla misura controversa non è illimitato, bensì ristretto. Inoltre, tali persone sono non già tutti i detentori di una carta SIM, bensì individui aventi un profilo molto particolare, poiché si tratta di coloro che hanno utilizzato il telefono rubato dopo la sua sottrazione, o persino che ne sono ancora in possesso, e che possono essere quindi legittimamente sospettati di essere autori del reato o di essere in relazione con questi ultimi" (par. 34); e ancora, significativamente "il procedimento principale riguarda dati personali la cui trasmissione è richiesta non già in maniera generalizzata e indifferenziata, bensì in modo mirato quanto alle persone e limitato quanto alla durata" (par. 37).

[19] Sia la Corte che l'Avvocato generale hanno riconosciuto la sussistenza di una forma di ingerenza nei diritti alla riservatezza e alla protezione dei dati, derivante dal solo fatto che vengano poste in essere attività di accesso ai dati e di comunicazione degli stessi ad un terzo, ritenendo comunque poco rilevanti, ai fini della individuazione della esistenza di una ingerenza, elementi quali la natura sensibile o meno del dato o di inconvenienti per l'interessato derivanti da tali operazioni (par. 76-77 delle Conclusioni dell'Avvocato e similmente par. 51 della sentenza della Corte).

indicati nella *Tele2* con riferimento alla disciplina dell'accesso[20]. Questa erronea interpretazione viene però smentita, con grande chiarezza, dalla Corte ma soprattutto dall'Avvocato generale che nelle sue conclusioni afferma proprio sul punto "che la controversia oggetto del procedimento principale presenta notevoli peculiarità, che la distinguono, in particolare, dal contesto delle cause che hanno dato luogo alle decisioni *Digital Rights Ireland* e *Tele2*" (par. 32). Il caso di un accesso limitato nella sua estensione, nella sua dimensione temporale e nella tipologia dei dati richiesti, quale quello in esame[21], non può che differire fortemente dall'accesso generalizzato ed indifferenziato, riferito ad un ventaglio ben più ampio di dati (tutti i metadati prodotti dai servizi di telecomunicazione) che caratterizzava invece le vicende giurisprudenziali precedenti. La portata del ragionamento della Corte in *Ministerio Fiscal*, dunque, deve essere considerata con riferimento a casi, come quello analizzato, in cui l'accesso è ristretto, ben definito e non permette di trarre conclusioni sulla vita privata dei soggetti interessati[22]. L'Avvocato generale Saugmandsgaard Øe con grande realismo e concretezza, ha avvertito dunque che "occorre evitare di adottare una concezione troppo ampia dei requisiti stabiliti dalla Corte in tali due pronunce [*Digital Rights* e *Tele2*], al fine di non ostacolare, in ogni caso non eccessivamente, la possibilità degli Stati membri di derogare al regime stabilito dalla Direttiva 2002/58, ad essi concessa dall'Articolo 15, par. 1, di quest'ultima, nei casi in cui le intrusioni nella vita privata in questione abbiano nel contempo una finalità legittima e una portata ridotta, come quelle che possono essere causate nel caso di specie dalla richiesta del servizio di polizia giudiziaria" (par. 90): solo quindi con riferimento agli specifici casi di ingerenza non grave e finalità legittima può essere coerentemente e proporzionalmente 'calibrato' e ridotto il criterio indicato dalla giurisprudenza europea della gravità del reato.

Tenendo in considerazione questa premessa, utile a circoscrive il ragionamento dei giudici di Lussemburgo, pare importante porre attenzione all'effetto della riformulazione operata dalla Corte rispetto alle questioni pregiudiziali poste dal giudice spagnolo. Tale intervento di riscrittura porta infatti

[20] "Con la sentenza in commento la Corte sembra a primo impatto cambiare orientamento, in quanto potrebbe portare il lettore a ritenere che non sia più necessario il criterio, tanto sottolineato in precedenza, della gravità del reato per giustificare l'accesso ai dati conservati", D. DEL VESCOVO, *L'accesso delle autorità pubbliche a dati personali di natura meramente identificativa non costituisce ingerenza grave nei diritti fondamentali degli interessati*, in *Amministrativamente – Rivista di diritto amministrativo*, 11-12, 2018, p. 12.

[21] Lo si coglie bene dalle affermazioni conclusive della Corte secondo cui "l'art. 15 della Direttiva 2002/58, letto alla luce degli artt. 7 e 8 della Carta, deve essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con telefono cellulare rubato, come il cognome, il nome e, se del caso, l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi (..) che non presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione, ricerca, accertamento e perseguimento dei reati alla lotta contro la criminalità grave" (par. 63). Viene quindi espressamente e con attenzione precisato il peculiare caso entro cui il ragionamento della Corte si inserisce e i dati specifici e i limiti particolari che caratterizzano le attività di accesso poste all'attenzione dei giudici europei.

[22] "Il numero delle persone potenzialmente interessate dalla misura controversa non è illimitato, bensì ristretto. Inoltre tali persone sono non già tutti i detentori di una carta SIM, bensì individuo aventi un profilo molto particolare, poiché si tratta di coloro che hanno utilizzato il telefono rubato dopo la sua sottrazione, o persino che ne sono ancora in possesso, e che possono essere quindi legittimamente sospettati di essere gli autori del reato o di essere in relazione con questi ultimi. Per di più i dati oggetto della richiesta consistono non già in qualsiasi tipo di dati personali detenuti dai fornitori di servizi di comunicazione elettronica, bensì soltanto in quelli relativi all'identità civile degli individui summenzionati, vale a dire (..) dati che possono anche essere qualificati 'di contatto'. (..) Pertanto, l'obiettivo qui perseguito è, a mio avviso, quello di raccogliere informazioni che non riguardano né un'ubicazione né comunicazioni in quanto tali, bensì persone fisiche ricercate per aver potuto utilizzare un servizio di comunicazione elettronica mediante il telefono rubato, anche se tali persone non hanno effettuato in concreto una telefonata" (par. 34-36, Conclusioni dell'Avvocato generale). E ancora "gli effetti potenzialmente nocivi per le persone interessate dalla richiesta di accesso in questione sono nel contempo moderati e circoscritti. Infatti, essendone previsto l'utilizzo nello specifico ambito di una misura di indagine, i dati richiesti non sono destinati ad essere divulgati al pubblico. Inoltre, la facoltà di accesso offerta alle autorità di polizia è circondata da garanzie procedurali" (par. 85).

la Corte ad esimersi, secondo alcuni autori con una scelta "tattica"[23], dal prendere una posizione sulla ben più rilevante e complessa questione della individuazione dei criteri determinanti la gravità del reato. Di fatto, se questa ultima determinazione era quanto chiesto dal giudice del rinvio, possiamo affermare che al termine della lettura della decisione non si riescono a trovare posizioni della Corte in merito: rispondendo, seppur con un ragionamento logico e coerente, alla domanda derivante dalla riformulazione dei quesiti, era infatti divenuto irrilevante ai fini della soluzione del caso la determinazione degli importanti criteri cui il giudice del rinvio aveva fatto riferimento[24]. Quello che viene analizzato, in conclusione, pare essere non tanto la gravità in sé del reato o i criteri utili a definirla,

[23] L. WOODS, *Mobile phone theft and EU e-privacy law: the CJEU clarifies police powers*, op. cit. Della stessa opinione Tracol, che afferma: "through its re-phrasing of the questions posed by the referring Court, the Grand Chamber carefully avoided and quite notably sidestepped the tricky issues of defining the notion of serious crime and determining whether it is an autonomous concept of EU law", X. TRACOL, *Ministerio Fiscal: access of public authorities to personal data retained by providers of electronic communications services*, in *European Data protection Law Review*, 1, 2019, p. 134.

[24] Senza dubbio la precisazione della necessità di un vaglio preventivo circa la sussistenza della gravità dell'ingerenza rispetto alla gravità del reato (necessità che non emergeva in maniera chiara dalla decisione *Tele2*) assume un rilievo importante; nonostante questo, resta innegabile come la CGUE, così facendo, non sia giunta a fornire una definizione di reato grave e dei criteri necessari per individuarlo. Merita comunque sottolineare come l'Avvocato generale, nelle sue Conclusioni, spinga la propria analisi e valutazioni attinenti anche ai criteri di determinazione della gravità del reato. Questo perché l'Avvocato ha proposto le proprie considerazioni anche per il caso in cui la Corte avesse ritenuto necessario fornire una vera e propria definizione di "reato grave", cosa che, come si è visto, non è avvenuta. Pare utile mettere in luce, in questa sede, i punti salienti individuati dall'Avvocato: innanzitutto, sulla base della giurisprudenza *DRI* e *Tele2*, quella di reato grave non può essere considerata una nozione autonoma del diritto dell'Unione (par. 93-101); tale determinazione spetterebbe dunque agli Stati membri e non alla Corte. Alla luce però della disomogeneità delle soluzioni normative e definitorie nazionali, l'Avvocato è comunque portato a considerare che la definizione di gravità non dovrebbe basarsi meramente sull'entità della pena e dunque su un criterio formale. Con una limitazione di fondo: richiamando la necessità di una interpretazione restrittiva dell'art. 15 stesso, da considerarsi come deroga e non come regola, anche la nozione di "reato grave" dovrebbe essere intesa restrittivamente e in modo non eccessivamente ampio da parte degli Stati membri. Ancora in subordine, se la Corte avesse invece ritenuto la nozione di 'reato grave' come autonoma, la pronuncia dei giudici di Lussemburgo avrebbe dovuto spingersi a valutare anche i criteri che consentono di stabilire la gravità. In quel caso, l'Avvocato ha ritenuto necessario fondare la definizione di gravità su una pluralità di criteri, quali – a titolo esemplificativo e non esaustivo – il contesto nel quale si colloca il reato asserito (dolo, recidiva, aggravanti), l'importanza degli interessi della società lesi dall'autore del reato, la natura e/o entità dei danni subiti dalla vittima, le pene applicabili in generale nello Stato membro interessato (par. 105). Muovendo poi alla considerazione della seconda questione pregiudiziale, viene sottolineato come tale quesito avrebbe dovuto trovare risposta solo nel caso in cui la Corte avesse basato la nozione di gravità esclusivamente sul criterio formale e quindi sul *quantum* della pena. La seconda domanda pregiudiziale infatti ha ad oggetto l'individuazione della soglia minima di pena richiesta per attribuire la qualifica di gravità ad un reato e, in particolare, se la soglia individuata dal legislatore spagnolo in 3 anni di reclusione possa essere considerata conforme al diritto dell'Unione (par. 108). Se è vero che una tale soglia di pena non può essere determinata in modo uniforme su tutto il territorio dell'UE e che ciascuno Stato membro ha la facoltà di determinarla autonomamente, viene ripreso quel principio, già più volte affermato, secondo cui l'utilizzo della deroga prevista all'art. 15 deve rimanere una eccezione ed avere quindi una interpretazione restrittiva. Partendo da questa considerazione, l'Avvocato è giunto ad affermare che nell'esercizio di tale facoltà esclusiva degli Stati questi non possano fissare una soglia "ad un livello talmente basso, rispetto al *quantum* abituale delle pene applicabili in tale Stato, che le eccezioni al divieto di conservare e di utilizzare i dati personali previste da tale articolo 15, co. 1, sarebbero trasformate in principi" anziché in eccezioni (par. 114). L'Avvocato ammonisce comunque la Corte circa i rischi derivanti dalla determinazione giurisprudenziale di una simile soglia: "poiché una determinazione richiede una valutazione complessa e potenzialmente soggetta a evoluzione, occorre a mio avviso restare prudenti a questo proposito e riservare tale operazione alla valutazione del legislatore dell'Unione, nella sfera delle competenze conferite a quest'ultima, o alla valutazione del legislatore di ciascuno Stato membro, entro i limiti dei requisiti derivanti dal diritto dell'Unione" (par. 117). Senza dunque arrivare a stabilire un quantitativo temporale specifico, l'Avvocato generale giunge alla conclusione che, nell'ipotesi in cui la Corte, contrariamente a quanto suggerito, ritenesse la pena irrogabile l'unico criterio da considerare per la determinazione della gravità del reato, gli Stati membri devono essere ritenuti liberi di fissare il livello minimo della pena, a condizione che siano rispettati i requisiti risultanti dal diritto dell'Unione e, in particolare, quello secondo cui le ingerenze nei diritti fondamentali devono restare eccezionali e rispettare il principio di proporzionalità (par. 121).

bensì il suo rapporto con la gravità dell'ingerenza nei diritti fondamentali; si può quasi affermare, quindi, che i giudici si siano piuttosto pronunciati sulla determinazione della gravità dell'ingerenza e della sua relazione consequenziale con la necessaria gravità del reato. In questo senso, pur chiarendo i punti sopra esposti, tale mancanza non permette alla pronuncia di fungere da guida ulteriore per un legislatore nazionale che appariva – e appare tutt'ora – non poco disorientato dinnanzi alle molteplici difficoltà applicative e dubbi che erano emersi dalla previa giurisprudenza europea[25]. In questo contesto, inoltre, non bisogna dimenticare come la pronuncia *Ministerio Fiscal* lasci da parte ogni questione relativa alla legittimità della disciplina sulla *data retention*. Se questo è certamente motivato dall'esigenza di rimanere nei limiti del *petitum*, non si può non rilevare come una tale visione possa risultare in realtà limitata, vedendo la disciplina dei due momenti della conservazione e dell'accesso come slegata e priva di influenza dell'una sull'altra. In realtà infatti una conservazione del dato è prerequisito fondamentale per poter procedere successivamente ad un accesso e sarebbe del tutto impossibile parlare di accesso mirato o meno, se prima alla base non vi fosse una qualche forma di conservazione. A tal proposito, quanto al rapporto conservazione/accesso, alcuni autori si sono interrogati sul possibile impatto della sentenza *Ministerio Fiscal* rispetto ai criteri relativi alla *data retention* fissati, in particolare, dalla sentenza *Tele2*: "according to paragraphs 108-111 of the Tele2 judgement, targeted data retention requirements for the purpose of fighting serious crime are compatible with EU law. Moreover, it would be natural to read par. 115 of the Tele2 as always limiting the access to such retained data to cases involving serious crime because targeted data retention requirement in itself constitutes a serious interference with fundamental rights that can only be justified by the objective of fighting serious crime. Allowing access to the retained data in cases not involving serious crime would arguably undermine the purpose limitation at the retention stage"[26]. In altre parole, risulta poco chiaro come sia possibile conciliare la legittimazione di un accesso a talune tipologie di metadati anche per reati non gravi, laddove ovviamente l'ingerenza non sia grave, con il fatto che tale accesso, sulla base di quanto affermato nella *Tele2*, deve comunque fondarsi sui dati conservati mediante una *data retention* targettizzata e giustificata solo se finalizzata alla lotta alla criminalità grave.

Fornire una risposta su questi punti – risposta ormai sempre più delegata al solo intervento della CGUE – così come sulle molteplici criticità interpretative dei requisiti fissati nelle sentenze sino a qui analizzate, risulta ormai di fondamentale importanza: se con la pronuncia *Ministerio Fiscal* i giudici di Lussemburgo non hanno risolto gli interrogativi emersi nell'era post-*Tele2* relativamente alla gravità del reato come requisito per l'accesso ai dati[27], pur avendo chiarito taluni aspetti di rilievo e slegando

[25] Secondo Celeste, il fatto che i giudici non abbiano potuto spingersi a vagliare alcuni aspetti di grande rilievo quali la legittimità della disciplina sulla conservazione dei dati spagnola o gli elementi che determinano il carattere di gravità di un reato, dovendosi attenere al *petitum*, è diretto derivato delle caratteristiche del funzionamento della giustizia a livello dell'Unione europea. In questo senso, però, per l'autore, "the very architecture of the European judicial system, which does not allow the Court of Justice to go beyond the questions referred by national courts and prevents it from quashing national legislation, slows down ad fragments the effective application of the data retention principles within the member states. This situation increases the state of uncertainty at national level, amplifies national divergences, and ultimately appears to be in contrast with the proactive approach that the Court adopted so far in the data retention saga", E. CELESTE, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019.

[26] L. WOODS, *Mobile phone theft and EU e-privacy law: the CJEU clarifies police powers*, op. cit.

[27] Tale era l'auspicio di alcuni autori: non a caso Artemiou sceglieva emblematicamente e forse provocatoriamente di titolare il proprio commento alle Conclusioni dell'Avvocato generale nel caso *Ministerio Fiscal*: "The way out of Digital Rights Ireland" (E. ARTEMIOU, *The way out of Digital Rights Ireland*, in *CiTiP Blog*, University of Leuven, 19 giugno 2018). In tale contributo, l'autrice intravedeva l'occasione per la Corte di poter indicare alle autorità nazionali un modo legittimo per accedere ai dati conservati dai fornitori di servizi di comunicazione, fornendo criteri chiari e concretamente realizzabili: "In conclusion, it is safe to say that the Court of Justice of the European Union has raised the bar in terms of protection of personal data, to a point where it seemed impossible to process such data for prosecution purposes lawfully. This is a unique opportunity to illustrate practically if the

da tale criterio 'rafforzato' alcune tipologie di indagini limitate a particolari dati, è da individuarsi nei sei rinvii pregiudiziali al momento pendenti l'occasione per la Corte di chiarire i dilemmi ancora aperti e di fornire nuove ed attese indicazioni e principi nella difficile sfida rappresentata dall'esigenza di bilanciamento tra interessi securitari e tutela dei diritti fondamentali.

2. – La situazione attuale: una analisi dei rinvii pregiudiziali pendenti e delle posizioni espresse dagli Avvocati generali in merito, quale riflesso delle complesse criticità ancora irrisolte

2.1. – I rinvii pregiudiziali promossi dai giudici inglesi, francesi e belgi e le Conclusioni dell'Avvocato generale: la regolamentazione della **data retention** *tra efficacia e tutela dei diritti fondamentali*

2.1.1. – Le posizioni espresse dai Governi nazionali e dai giudici del rinvio e il tentativo di promuovere una lettura 'pragmatica' dei criteri restrittivi individuati dalla giurisprudenza della CGUE

Come ben emerso dalla analisi della sentenza *Ministerio Fiscal*, ancora molte sono le questioni irrisolte e le significative perplessità e difficoltà applicative dei criteri individuati dalla giurisprudenza dell'UE in materia di conservazione ed accesso ai metadati per scopi securitari. Questi dubbi rilevanti e sostanziali, unitamente alla fondamentale importanza rivestita dalla disciplina della *data retention*, sono sfociati in ben sei rinvii pregiudiziali, susseguitisi a partire dal 2017 sino al più recente risalente al marzo 2020 e ad oggi ancora sottoposti all'analisi della Corte di giustizia: si tratta dei rinvii promossi dall'Investigatory Powers Tribunal del Regno Unito[28], dal Conseil d'État (Consiglio di Stato) francese[29], dalla Cour constitutionnelle (Corte costituzionale) belga[30], dalla Riigikohus (Corte Suprema) estone[31] e, più recentemente, dalla Bundesverwaltunsgericht (Corte amministrativa federale) tedesca[32] e dalla Supreme Court irlandese[33].

Le normative nazionali di riferimento e le vicende giurisprudenziali attinenti ai rinvii provenienti dalla Corte costituzionale belga e dall'Investigatory Power Tribunal del Regno Unito saranno oggetto di più ampia analisi nella Parte III di questo lavoro, allo scopo di mettere in luce il complesso dibattito, le peculiarità e il differente approccio adottato in questi due ordinamenti. Ciò che si vuole invece in questa sede esaminare approfonditamente sono innanzitutto i quesiti e le questioni poste alla base delle diverse cause pendenti dinnanzi alla CGUE: pur nelle loro differenti sfumature, tutte presentano infatti quale comune denominatore l'interpretazione dell'art. 15 della Direttiva *e-Privacy* e tutte richiedono ai giudici di Lussemburgo un chiarimento e un maggiore approfondimento quanto ai criteri delineati nella previa giurisprudenza in materia. Tutti i Governi degli Stati membri dai quali i rinvii provengono, inoltre, hanno espresso forte preoccupazione – quando non vera e propria 'resistenza' – verso una integrale e letterale attuazione dei requisiti affermati nelle sentenze da *DRI* a *Tele2*, sino a *Ministerio*

police can request access to personal data retained by telecommunication service providers for the purposes of criminal investigation but should without a doubt be framed carefully by the Court".

[28] C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e al.*, depositato il 31 ottobre 2017.

[29] Cause riunite C-511/18 e C-512/18, *French Data Network, La Quadrature du Net e a. c. Premier ministre, Garde des Sceaux, Ministre de la Justice*, depositato il 3 agosto 2018.

[30] C-520/18, *Ordre des barreaux francophones et germanophone e al. c. Conseil des ministres*, depositato il 2 agosto 2018.

[31] C-746/18, *H. K. c. Prokuratuur*, depositato il 29 novembre 2018.

[32] C-793/19, *SpaceNet AG c. Repubblica federale di Germania*, depositato il 29 ottobre 2019.

[33] C-140/20, *G. D. c. Commissioner of the Garda Siochana e al.*, depositato il 25 marzo 2020.

Fiscal, sia sotto il profilo della disciplina della *data retention*, sia sotto quella del successivo ed eventuale accesso ai metadati conservati: ad avviso dei Governi, nonché di alcune delle Corti del rinvio, le salvaguardie e limitazioni indicate dalla CGUE "hanno l'effetto di privare [gli Stati membri] di uno strumento che essi ritengono imprescindibile per la salvaguardia della sicurezza nazionale e la lotta contro la criminalità e il terrorismo", tanto che "alcuni di detti Stati membri chiedono di invertire o temperare la giurisprudenza in parola"[34]. Tutti i rinvii quindi mettono in luce e rappresentano, con profili molto simili tra loro, quelle problematicità attuative che erano con forza scaturite dalla sentenza *Tele2*, facendo leva su quei dubbi, mai sciolti, circa i limiti e confini di applicabilità della Direttiva *e-Privacy*, l'estensione dei c.d. 'criteri *Tele2*' anche all'ambito della sicurezza nazionale, la disciplina dell'accesso da parte di autorità di *law enforcement*, la compatibilità di una conservazione generalizzata alla Carta di Nizza, le conseguenze di una dichiarazione di incompatibilità della normativa nazionale soprattutto con riferimento alle prove utilizzate in procedimenti penali e fondate sull'utilizzo di metadati raccolti sulla base di un obbligo di *bulk data retention*, nonché i criteri che devono essere valutati per determinare la gravità dell'ingerenza nei diritti fondamentali e la gravità del reato. Tutti questi aspetti ricorrenti, sebbene in diversa misura, nei sei rinvii pregiudiziali pendenti, consentono di creare tra questi ultimi un forte legame: non deve dunque stupire come sia individuabile nei rinvii stessi un continuo richiamo alle altre cause pendenti, così come non sorprende neppure la scelta di Campos Campos Sanchez-Bordona, Avvocato generale nei rinvii promossi dalle Corti di Regno Unito, Francia e Belgio, di pubblicare le proprie Conclusioni il medesimo giorno per tutte le tre cause, operando un intreccio di rimandi ai diversi testi presentati. Per tali motivi, pare pertanto utile analizzare insieme la 'triade' richiamata, per esaminare invece successivamente il rinvio estone, incentrato sulla disciplina dell'accesso ai metadati e le relative Conclusioni dell'Avvocato generale Giovanni Pitruzzella del 21 gennaio 2020 – anch'esse ricche di richiami agli altri rinvii pendenti. Infine verranno presentati i più recenti quesiti pregiudiziali promossi dai giudici di Germania e Irlanda, per i quali ancora non sono state depositate Conclusioni ma che meritano di essere vagliati viste le importanti questioni poste e le posizioni di rilievo espresse dagli stessi giudici del rinvio.

Prendendo avvio dalla più risalente delle tre cause che si vogliono per prime studiare, l'Investigatory Power Tribunal[35] del Regno Unito (d'ora in avanti IPT) era stato investito del ricorso della ONG Privacy International che riteneva l'acquisizione ed utilizzo in massa di metadati da parte delle *UK Security and Intelligence Agencies* (ovvero le agenzie di sicurezza ed intelligence del Regno Unito, d'ora in avanti SIA) incompatibili con il diritto dell'Unione europea. Le SIA ricevevano infatti dagli operatori di servizi di telecomunicazione i dati di traffico e ubicazione (ovverosia i metadati) relativi alle comunicazioni dei propri utenti per finalità di spionaggio, lotta al terrorismo, alla proliferazione di armi nucleari e contrasto avverso minacce gravi alla pubblica sicurezza[36]. In tale controversia, l'IPT rilevava come simili operazioni fossero conformi al diritto interno e alla CEDU mentre dubbi sorgevano quanto alla

[34] Conclusioni dell'Avvocato generale M. Campos Sanchez-Bordona del 15 gennaio 2020, nelle cause riunite C-511/18 e C-512/18 ma anche nella Conclusioni del medesimo Avvocato generale nelle cause C-520/18 e C-623/17, tutte pubblicate nella medesima data.

[35] Si rimanda sin da ora al Capitolo I, Parte III per una approfondita analisi delle funzioni di tale autorità.

[36] Tali operazioni sono regolate da disposizioni contenute nel *Telecommunications Act* del 1984, nel *Data Retention and Investigatory Powers Act* del 2014 e nel *Regulation of Investigatory Powers Act* del 2000. Come evidenziato da Celeste, "in the specific case of the UK, access and use of traffic data by public security and national security authorities are regulated by two distinct pieces of legislation and entail two slightly different procedures. For public security purposes, telecommunications operators retain traffic data and allow, when necessary, relevant authorities to access them; while, in the field of national security, telecommunications operators are required to transfer all traffic data to the competent authorities, which will then be responsible for the retention of such information. In other words, telecommunications providers do not retain traffic data for national security purposes, but directly transfer such data to the competent authorities. However, apart from these differences, the model of bulk retention and access of traffic data is essentially the same", E. CELESTE, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, op. cit.

compatibilità con i criteri indicati dalla giurisprudenza della CGUE ed in particolare dalla sentenza *Tele2*. Nel rimettere la questione ai giudici di Lussemburgo però la Corte inglese metteva subito in rilievo come "un aspetto fondamentale dell'utilizzo di tali dati da parte delle SIA consiste nel rilevare minacce alla sicurezza nazionale precedentemente ignote, attraverso tecniche di raccolta non mirate che si basano sull'aggregazione di dati in unico luogo (..). Il fornitore di una rete di comunicazioni elettroniche non è successivamente tenuto a trattenere tali dati oltre il periodo previsto per esigenze aziendali, che vengono quindi conservati unicamente dalla Stato (attraverso le SIA)"; alla luce di tali pratiche e della finalità perseguite dalle operazioni di trasferimento e conservazione generalizzata dei metadati, veniva ribadito con chiarezza e decisione dai giudici come "l'imposizione delle prescrizioni specificate nella sentenza *Tele2*, ove applicabili, vanificherebbe le misure adottate dalle SIA per proteggere la sicurezza nazionale, *mettendo perciò a rischio la sicurezza del Regno Unito*"[37] (enfasi aggiunta). Emergeva dunque con forza quella resistenza e opposizione – già messa in evidenza nei previ paragrafi e Capitoli – ad una attuazione estensiva delle salvaguardie e limitazioni previste dalla giurisprudenza dell'UE che, qualora attuate anche nell'ambito di azione della agenzie di intelligence, avrebbero avuto quale risultato quello di neutralizzare totalmente l'utilità dello strumento della *data retention* stessa, intesa come mezzo imprescindibile e prezioso per la garanzia della sicurezza nazionale[38]. Ecco perché il giudice del rinvio ha espressamente citato, a rafforzamento della propria posizione, gli artt. 4 TUE e 1, co. 3 della Direttiva *e-Privacy*, chiedendo quindi se, tenuto conto di tali disposizioni, l'obbligo imposto ai *service providers* di fornire e trasferire metadati in massa alle SIA dovesse considerarsi rientrante nell'ambito di applicazione del diritto dell'UE e della Direttiva *e-Privacy* e, in caso affermativo, entro quali limiti dovessero essere applicati i requisiti indicati dalla CGUE nella previa giurisprudenza in materia. La modalità e riflessioni contenute nei quesiti del rinvio sembrano quindi richiedere ai giudici di Lussemburgo una sorta di 'modulazione' della portata e delle tutele stabilite dalla c.d. *data retention saga* almeno nei casi in cui conservazione e accesso siano volti a garantire la sicurezza nazionale.

Del tutto similmente anche il Consiglio di Stato francese, nel rinvio promosso, ha richiamato l'art. 4 TUE, specificando come la garanzia della sicurezza nazionale e le misure da adottarsi per tutelare il diritto stesso alla sicurezza previsto all'art. 6 della Carta di Nizza siano unicamente responsabilità degli Stati membri. Da questa premessa, il giudice francese ha chiesto alla CGUE se un obbligo di conservazione generalizzata ed indifferenziata, adottato sulla base dell'art. 15 Direttiva *e-Privacy*, possa essere ritenuto una ingerenza giustificata "in un contesto caratterizzato da minacce gravi e persistenti alla sicurezza nazionale e in particolare dal rischio terroristico"[39].

Anche il rinvio della Corte costituzionale belga infine pare invitare la Corte di giustizia a leggere il medesimo art. 15 in combinato disposto con il diritto alla sicurezza di cui all'art. 6 della Carta di Nizza, chiedendo se da una tale interpretazione debba ricavarsi l'incompatibilità con il diritto dell'UE di una normativa nazionale che preveda in capo agli operatori di servizi di telecomunicazione un obbligo generale di conservazione dei metadati per finalità di lotta alla criminalità grave ma anche di garanzia della sicurezza nazionale, difesa del territorio, sicurezza pubblica e perseguimento di fatti diversi da quelli di criminalità grave o ancora di realizzazione di un altro obiettivo tra quelli indicati nell'art. 23 GDPR, anche nel caso in cui tale normativa sia accompagnata da garanzie adeguate quanto alle condizioni di conservazione e accesso ai metadati stessi. Ciò che sembra proporsi dunque è una lettura

[37] Par. 20, Conclusioni Avvocato generale, *Privacy International*.

[38] Il IPT parla addirittura di "esigenza fondamentale delle SIA di utilizzare tecniche di acquisizione di massa e di trattamento automatizzato".

[39] Il giudice del rinvio poi ha promosso altri due quesiti, di minor rilievo ai fini della presente analisi: uno riguarda la necessità di prevedere un obbligo di informazione degli interessati circa le procedure di raccolta dei dati di connessione; l'altro invece la legittimità e compatibilità col diritto dell'UE di forme di raccolta in tempo reale di dati sul traffico e sull'ubicazione di persone determinate, forme che non impongono però uno specifico obbligo di conservazione dei dati stessi.

'globale' dei requisiti emersi dalla sentenza *Tele2*, che non vede cioè nella sola *bulk data retention* un elemento di incompatibilità con la Carta di Nizza bensì ritiene necessario valutare la normativa nel complesso e non unicamente con riferimento alla disciplina della conservazione: l'insieme di tutele e salvaguardie predisposte per la fase di conservazione e accesso ai metadati potrebbe pertanto compensare e legittimare la maggiore ingerenza nella sfera privata legata ad una conservazione di tipo generalizzato. La peculiarità poi del rinvio proveniente dalla Corte belga è da individuarsi nell'ulteriore quesito posto che, come vedremo, risulta essere estremamente simile a quello promosso dalla Corte Suprema irlandese: i giudici belgi infatti si chiedono se sia possibile prorogare gli effetti di una normativa nazionale dichiarata incompatibile con il diritto dell'Unione europea, "al fine di evitare una situazione di incertezza giuridica e di permettere che i dati raccolti e conservati in precedenza possano ancora essere utilizzati per il raggiungimento degli obiettivi previsti dalla legge".

Come è ben possibile notare dalla ricostruzione delle questioni poste alla CGUE nei tre rinvii pregiudiziali qui considerati, l'attenzione dei giudici nazionali è tutta incentrata sulla possibilità di 'smussare' quella posizione enunciata nella sentenza *Tele2* di incompatibilità di qualsiasi forma di conservazione generalizzata ed indiscriminata dei metadati che aveva portato a forti critiche da parte di diverse autorità (da Europol alle autorità di *law enforcement* nazionali stesse), nonché ad un tentativo di 'defensive reaction' da parte dei Governi e dei legislatori nazionali, già messi in rilievo nel Capitolo II.

Del resto, nel corso dell'udienza pubblica tenutasi il 9 settembre 2019, unitamente per tutte i tre rinvii richiamati, questa richiesta è ben emersa non solo dalle posizioni espresse dagli Stati membri intervenuti bensì anche – e sorprendentemente – dallo stesso Garante europeo per la protezione dei dati (GEPD). Nelle *Pleading notes* di quest'ultimo si legge infatti come "in the specific context of retention of electronic communications data, it might not be possible to identify in advance those data subjects (or categories of data subjects) whose information may at some point in the future become part of a criminal investigation, for example victims of serious crime" (p. 11). Anche il GEPD dunque riconosce il problematico aspetto legato alla *data retention* che mal si presta, per sua natura e salvo una rinuncia sostanziale delle proprie potenzialità, ad una preventiva limitazione: così, se una forma generalizzata di conservazione dei dati non può essere considerata conforme al diritto dell'UE, una tipologia legittima di *data retention* "limited yet effective" viene essere identificata laddove la conservazione sia circoscritta a specifiche categorie di dati e siano presenti rafforzate salvaguardie attinenti all'accesso ai dati medesimi. Quanto al primo aspetto, dunque, il GEPD richiede di ridurre il volume di dati da conservare, attribuendo al legislatore nazionale il compito di indicarne una lista esauriente all'interno di una apposita normativa sulla *data retention*, nella quale venga inoltre determinato il periodo di conservazione prevendendo una differenziazione a seconda della categoria di dati interessati. Basandosi poi sulla concezione secondo cui "conditions for data retention must always be considered together with conditions for subsequent access", il GEPD sottolinea l'importanza sia di una autorizzazione preventiva da parte di una autorità giudiziaria o amministrativa indipendente, che di una forte limitazione dei soggetti cui può essere autorizzato l'accesso ai dati nonché di un significativo controllo *ex post*, richiedendo infine "a period review of the suitability and effectiveness of the data retention and access system, based on objective and reliable information. A high degree of transparency, including about the practical implementation and outcomes, is essential for the legitimacy of any data retention scheme in a democratic society" (p. 12). Anche il GEPD quindi pare rendersi conto della complessità della situazione e delle difficoltà 'pratiche' legate alla richiesta di una targettizzazione preventiva della conservazione, non sempre concretamente possibile e realizzabile.

Una valutazione simile è stata richiamata e sintetizzata dallo stesso Avvocato generale nelle sue Conclusioni alla causa promossa dalla Corte costituzionale belga, punto al quale anche le Conclusioni degli altri rinvii rimandano; qui, dopo una sintesi dei principi e dei criteri affermati nelle sentenze *Tele2* e *Ministerio Fiscal*, Campos Campos Sanchez-Bordona ricostruisce le critiche, "velate o esplicite", mosse avverso tale giurisprudenza, sin dalla pronuncia *DRI*: "la maggioranza degli Stati membri che

hanno presentato osservazioni invitano la Corte a chiarire, temperare o addirittura riconsiderare vari aspetti della sua giurisprudenza in materia (..). Sarebbero sufficienti norme rigorose sull'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica, che possano compensare, in qualche modo, la gravità dell'ingerenza che la conservazione generalizzata e indifferenziata di tali dati comporta" (par. 70-71).

2.1.2 – La posizione dell'Avvocato generale Campos Sanchez-Bordona nelle sue Conclusioni: significative conferme e qualche compromesso

2.1.2.1. – Il rifiuto di forme di conservazione generalizzata ed indiscriminata e la proposta di una 'terza via' intermedia tra **bulk** *e* **targeted**

Ebbene, di fronte alle posizioni espresse dai Governi di numerosi Stati membri, volte a far salva la preziosa *blanket* o *bulk data retention* e a bocciare come irrealizzabile e discriminatoria una forma di conservazione targettizzata, l'Avvocato generale ha affermato invece con forza e decisione come i principi assunti dalla CGUE nelle previe sentenze debbano essere confermati, non ritenendo condivisibile il binomio "conservazione più ampia in cambio di un accesso più limitato" (par. 75, Conclusioni alla causa promossa dalla Corte costituzionale belga)[40]. L'unica via alternativa percorribile viene individuata in una forma di conservazione limitata (*conservation limitée*) dei metadati; per giungere a tale conclusione, l'Avvocato generale ha riconosciuto innanzitutto, con un ragionamento di grande rilievo, che i giudici di Lussemburgo da un lato non hanno mai censurato in sé la possibilità di adottare regimi di conservazione dei dati per scopi securitari, mentre dall'altro ciò che hanno escluso è la proporzionalità e legittimità di una conservazione indifferenziata estesa a qualsiasi tipologia di metadati prodotti dalle telecomunicazioni; inoltre Campos Sanchez-Bordona ammette, con realismo, che la conservazione targettizzata o mirata (*conservation ciblée*) proposta dalla Corte, ovvero quella mirata per zone geografiche o categorie di persone specifiche, comporta significative criticità applicative: "l'identificazione di un gruppo di potenziali aggressori sarebbe probabilmente insufficiente qualora essi utilizzassero tecniche di anonimizzazione o falsificassero la loro identità. La scelta di tali gruppi inoltre potrebbe portare ad introdurre un regime di sospetto generalizzato su alcuni segmenti della popolazione ed essere qualificata come discriminatoria, a seconda dell'algoritmo utilizzato. La selezione in base a criteri geografici solleva gli stessi problemi e ne aggiunge altri, come osservato in udienza dal Garante europeo della protezione dei dati, in quanto potrebbe stigmatizzare determinate aree" (par. 88). È una ammissione importante questa, che avvalora quelle critiche e quelle serie difficoltà emerse dalle posizioni espresse dagli Stati membri stessi, ammissione accompagnata poi da una ulteriore affermazione significativa: "potrebbe esservi una certa contraddizione tra il carattere preventivo della conservazione riguardante un pubblico specifico o un'area geografica determinata e il fatto che non si conoscano in anticipo gli autori dei reati, né il luogo e il momento della loro commissione" (par. 89). Posto dunque che una conservazione generalizzata è da escludere in maniera assoluta e che una *data retention* targettizzata presenta parimenti criticità rilevanti, l'Avvocato cerca di 'smussare' le problematiche derivanti dalla previa giurisprudenza proponendo una lettura più ampia della *data retention* ammessa dalla CGUE, giungendo dunque ad una sorta di 'terza via': la conservazione targettizzata non è da considerarsi l'unica forma che i giudici europei ritengono compatibile con il diritto dell'UE; anzi, vi sono altre possibili strade da esplorare, che si basano su diversi criteri di 'limitazione' della conservazione, differenti da quelli proposti per la *targeted data retention* (o *conservation ciblée*):

[40] "La conservazione e l'accesso ai dati costituiscono due tipi diversi di ingerenza. (..) Ciascuna di tali ingerenze deve essere giustificata separatamente, mediante un esame specifico alla luce dell'obiettivo perseguito.", par. 75.

la riduzione delle categorie dei dati da conservare, la pseudonimizzazione, la fissazione di periodi di conservazione limitati e diversificati per ciascuna categoria di dati e, in base all'utilità presunta, l'esclusione di determinate categorie di fornitori di servizi di telecomunicazione, le autorizzazioni alla conservazione rinnovabili, l'obbligo di conservare i metadati entro i confini dell'UE e l'affidamento ad autorità amministrative indipendenti il controllo sistematico e costante della qualità ed efficacia delle salvaguardie poste in essere dai fornitori per scongiurare il rischio di abusi (par. 92)[41]. Tutti questi criteri possono essere impiegati per creare forme di conservazione legittime in quanto non *mirate* sulla base dei soggetti e delle aree geografiche bensì *limitate*: in questo caso i termini impiegati non sono di poco rilievo perché in essi è possibile leggere una differenza non più solo tra conservazione generalizzata e mirata (cioè tra *bulk* e *targeted,* o *généralisée* e *ciblée*) bensì anche tra conservazione mirata e limitata (ovvero tra *targeted* e *restricted* o tra *ciblée* e *limitée*). Questa distinzione, come si vedrà ampiamente nel successivo paragrafo attinente alle azioni intraprese sul fronte normativo europeo, è stata promossa negli studi elaborati da Europol e dal Consiglio stesso con riferimento alle possibili soluzioni legislative da adottare in materia di conservazione dei metadati. Ed è proprio a tale lettura che pare ispirarsi la posizione dell'Avvocato generale, sotto questo profilo in linea con quanto proposto da autorità di *law enforcement* e operanti nell'ambito della sicurezza e lotta alla criminalità.

Campos Sanchez-Bordona sembra dunque aprire a possibili ulteriori forme di conservazione, differenti da quelle promosse dalla CGUE stessa, giungendo in conclusione ad attribuire agli Stati membri o alle Istituzioni europee il compito di valutare e scegliere quale soluzione adottare mediante una normativa apposita, pur sempre rinunciando "a qualsiasi tentativo di imporre una conservazione generalizzata e indifferenziata" (par. 95). In assenza di una disciplina unitaria europea, quindi, la CGUE non può assumere il compito di sopperire a tale mancanza assumendo funzione normativa o puntualizzando minuziosamente le soluzioni da adottare: spetta a legislatori nazionali o europeo, "una volta fissati i limiti che, secondo la Corte, derivano dalla Carta, collocare il cursore nella posizione giusta per conseguire un equilibrio fra la tutela della sicurezza e i diritti fondamentali protetti dalla Carta" (par. 100). Questa visione deriva da un più ampio e strutturato ragionamento dell'Avvocato generale, secondo cui necessario punto di partenza per qualsiasi riflessione in materia deve essere individuato nella ammissione che limitare la quantità di dati conservati può incidere negativamente sulla efficacia ed efficienza della lotta alla criminalità: muovendo da tale considerazione, la compressione, imposta dalla giurisprudenza della CGUE, delle potenzialità che l'uso dei metadati rappresenta deve essere vista come un "tributo che i poteri pubblici devono pagare quando si impongono l'obbligo di salvaguardare i diritti fondamentali" (par. 102). Per questo motivo, pur ribadendo con sincerità e consapevolezza la difficoltà legislativa che questa limitazione e la determinazione di una conservazione limitata comportano, gli Stati membri non possono addurre tale complessità regolatoria come giustificazione per l'adozione di una conservazione generalizzata (par. 104). Quest'ultima deve restare un'eccezione, così che solo la

[41] Sotto questo profilo, merita sottolineare come l'Avvocato generale concordi con la posizione espressa dal GEPD, secondo cui più sono le categorie di dati conservate e più lungo è il periodo di conservazione, tanto più semplice sarà determinare il profilo di un individuo e la sua vita privata (par. 98); vi è inoltre una significativa presa di coscienza circa la difficoltà di determinare un confine ed una distinzione tra alcuni metadati e il contenuto delle comunicazioni stesse, come peraltro ampiamente sottolineato dal GEPD nel corso dell'udienza pubblica. Sulla base di tali considerazioni l'Avvocato quindi propone una forma di conservazione *limitata* mediante una restrizione ai dati strettamente indispensabili e necessari per il perseguimento dell'obiettivo securitario, solo di determinati fornitori di servizi e modulando la durata di conservazione sulla base della categoria dei dati interessati. Viene poi specificato come i sistemi di autorizzazione della conservazione potrebbero basarsi "su valutazioni periodiche delle minacce in ciascuno Stato membro. (..) Siffatte autorizzazioni potrebbero essere concesse da un giudice o da un'autorità amministrativa indipendente e comporterebbero una revisione periodica degli elementi indispensabili di tale conservazione", nota 75.

minaccia imminente o un rischio straordinario possono consentire una conservazione – e un accesso – dei metadati più ampia e pur sempre garantendo specifiche salvaguardie[42].

Alla luce di tutte queste importanti considerazioni sulla disciplina della conservazione dei metadati, l'Avvocato generale giunge a ritenere, rispondendo alla questione posta dalla Corte costituzionale belga, che l'art. 15 della Direttiva *e-Privacy* debba essere letto nel senso di precludere ai legislatori nazionali la possibilità di adottare normative che instaurino un regime di conservazione generalizzato ed indiscriminato, a nulla rilevando il fatto che le finalità siano anche quelle di sicurezza nazionale o che l'accesso sia soggetto a specifiche garanzie. Il fatto dunque che nella normativa belga siano previste forti salvaguardie nella fase di accesso, che la conservazione sia limitata ai metadati e non al contenuto delle comunicazioni, che vi siano obblighi stringenti in termini di sicurezza dei dati, i quali vengono conservati per 12 mesi unicamente nel territorio europeo e poi distrutti, non possono compensare il carattere comunque generalizzato della *data retention*, applicata peraltro in modo permanente e continuato. Ciò rende dunque la disciplina nazionale così caratterizzata, incompatibile con la Carta di Nizza e il diritto dell'UE. Il legislatore belga dunque, a parere dell'Avvocato generale, dovrà adottare altre soluzioni normative, quale quella sopra riportata di una conservazione in forma *limitata*.

2.1.2.2. – La conferma della incompatibilità con la Carta di Nizza di una bulk data retention *anche nel caso in cui la finalità perseguita sia la garanzia della sicurezza nazionale (salvo situazioni propriamente eccezionali)*

A nulla rileva neppure il richiamo all'art. 6 della Carta di Nizza o ancora allo specifico scopo di tutela della sicurezza nazionale effettuato da tutte le tre Corti del rinvio, belga, francese ed inglese: come emerge chiaramente nelle Conclusioni relative al rinvio francese, l'Avvocato generale ritiene che non sia possibile rimettere in discussione o temperare l'affermata incompatibilità con il diritto dell'UE di una *bulk data retention* neppure quando essa sia utilizzata in un contesto caratterizzato da "minacce gravi e persistenti alla sicurezza nazionale e in particolare dal rischio terroristico" (rinvio pregiudiziale Conseil d'Etat). Nonostante tutti i Governi degli Stati membri intervenuti nel procedimento abbiano messo in luce con forza come i requisiti imposti dai giudici di Lussemburgo a partire dalla sentenza *DRI*, se applicati letteralmente, abbiano come esito quello di privare i servizi di intelligence della possibilità di accedere a dati fondamentali per la difesa dello Stato, Campos Sanchez-Bordona ribadisce la necessità di quel 'tributo' che gli Stati devono riconoscere al fine di tutelare i diritti fondamentali. Nelle Conclusioni richiamate l'Avvocato generale utilizza termini ancora più forti e decisi per esprimere tale concetto: "la lotta contro il terrorismo non deve essere impostata solo pensando alla sua efficacia. Da ciò deriva la sua difficoltà, ma anche la sua grandezza quando i suoi mezzi e metodi rispettano i requisiti dello Stato di diritto, che significa anzitutto assoggettamento del potere e della forza ai limiti del diritto e, in particolare, a un ordinamento giuridico che trova nella difesa dei diritti fondamentali la ragione e

[42] Interessante notare come l'Avvocato generale al par. 107 affermi che "dall'esame comparato dei regimi normativi che disciplinano le situazioni costituzionali di emergenza risulta che non è impossibile delimitare le situazioni di fatto idonee a determinare l'applicazione di un regime normativo particolare, stabilendo quale autorità possa adottare tale decisione, a quali condizioni e sotto quale controllo". Per tale motivo, una *bulk data retention* risulta giustificata e proporzionata solo "in situazioni propriamente *eccezionali*, caratterizzate da una minaccia imminente o da un rischio di natura straordinaria tali da giustificare la dichiarazione ufficiale dello stato di emergenza in uno Stato membro": in tale caso è possibile che "la legislazione nazionale preveda, per un periodo limitato, la possibilità di imporre un obbligo di conservazione dei dati tanto ampio e generale quanto si ritenga necessario", par. 104. Tale casistica, come ben si comprende, risulta essere estremamente ristretta e, appunto, eccezionale nonché difficile da determinare in maniera univoca (quando una minaccia può dirsi imminente? E quando il rischio è di natura straordinaria?).

il fine della sua esistenza" (par. 130)[43]. Sulla base di queste importanti considerazioni, viene riaffermato come le uniche forme di conservazioni ammissibili siano quella mirata – già proposta dalla CGUE sin dalla sentenza *DRI* – o quella limitata, delineata nelle Conclusioni alla causa C-520/18 e che è stata più sopra esaminata.

Quanto poi all'art. 6 della Carta, viene precisato come tale riferimento normativo sia del tutto fuorviante: questa disposizione, infatti, secondo la lettura proposta nelle Conclusioni, è volta a tutelare la sicurezza personale, intesa come diritto alla libertà fisica di ciascun individuo da arresto o detenzione arbitraria e dunque come affermazione del principio secondo cui nessuno può essere privato della propria libertà se non sulla base di condizioni e procedure stabilite dalla legge; in questo senso quindi l'art. 6 non si riferisce alla sicurezza pubblica e non impone un obbligo "positivo" in capo all'Unione o agli Stati membri di adottare misure volte a tutelare la sicurezza delle persone da atti criminosi (par. 96).

Sebbene dunque questa interpretazione e richiamo all'art. 6 debbano essere scartati, l'Avvocato non si esime dal ribadire l'importanza e centralità della garanzia della sicurezza per l'UE e per la CGUE stessa: quest'ultima in particolare ha sempre mostrato di tenere in considerazione, nella propria giurisprudenza, la necessità degli Stati membri e delle Istituzioni europee di tutelare la sicurezza pubblica e nazionale[44], soprattutto nella lotta al terrorismo, intendendo la sicurezza come "consustanziale alla stessa esistenza e sopravvivenza di una democrazia, il che giustifica il fatto che se ne tenga pienamente conto nell'ambito della valutazione della proporzionalità" (par. 102) delle misure legislative nazionali adottate. Pur riconoscendo che "si potrebbe approfittare dell'opportunità offerta dai presenti rinvii pregiudiziali per proporre più chiaramente la ricerca di un equilibrio tra, da un lato, il diritto alla sicurezza e, dall'altro, il diritto alla vita privata e il diritto alla protezione dei dati personali", evitando così le critiche secondo le quali la Corte di giustizia favorirebbe i secondi a scapito del primo (par. 101), l'Avvocato giunge comunque alla conclusione che la giurisprudenza europea abbia già opportunamente valutato, nelle proprie decisioni, la minaccia terroristica e l'importanza dei mezzi preposti a combatterla efficacemente e che non ci sia dunque bisogno di ridimensionare o modificare i criteri indicati dalla sentenza *Tele2* laddove la conservazione sia finalizzata alla garanzia della sicurezza nazionale, anche mediante l'attività di autorità di intelligence. Ecco quindi che, similmente a quanto affermato nel rinvio pregiudiziale promosso dalla Corte costituzionale belga, anche in quello derivante dal Consiglio di Stato francese, l'Avvocato stabilisce che l'art. 15 della Direttiva *e-Privacy* osta a che

[43] Sul punto, debbono essere riportate, per la loro forza ed incisività, le parole dell'Avvocato generale: "Se si abbandonasse semplicemente alla mera efficacia, lo Stato di diritto perderebbe la qualità che lo contraddistingue e potrebbe diventare esso stesso, in casi estremi, una minaccia per il cittadino. Nulla potrebbe assicurare che, dotando il potere pubblico di strumenti esorbitanti per il perseguimento dei reati, mediante i quali esso potesse ignorare o svuotare di contenuto i diritti fondamentali, la sua azione incontrollata e totalmente libera non si risolverebbe in definitiva in un pregiudizio per la libertà di tutti. L'efficacia del potere pubblico, ripeto, trova una barriera insuperabile nei diritti fondamentali dei cittadini", par. 131-132. "Seppur difficile, non è impossibile determinare con precisione e sulla base di criteri oggettivi sia le categorie di dati la cui conservazione è considerata imprescindibile, sia la cerchia degli interessati. Certamente la soluzione più pratica ed efficace sarebbe la conservazione generale e indifferenziata di tutti i dati che possono essere raccolti dai fornitori di servizi di comunicazione elettronica, ma ho già rilevato che *la questione non può essere risolta in termini di efficacia pratica, bensì di efficacia giuridica e nel contesto di uno Stato di diritto*", par. 135, enfasi aggiunta.

[44] L'Avvocato generale infatti afferma con decisione, con riferimento alla lotta al terrorismo, come essa sia, "letteralmente vitale per lo Stato e il suo successo costituisce un obiettivo di interesse generale irrinunciabile per uno Stato di diritto", par. 128. L'Avvocato generale comunque non si spinge a cercare di fornire una definizione chiara di sicurezza nazionale e della sua distinzione rispetto alla sicurezza pubblica: quanto emerge è come alla prima tipologia vada ricondotta certamente l'attività delle agenzie di intelligence impegnate nella lotta al terrorismo; nella seconda invece paiono rientrare le attività di lotta alla criminalità. Per un approfondimento su questi termini, è utile rimandare alle considerazioni svolte nel Capitolo I, Parte I; in quel contesto, infatti, così come brevemente anche nel Capitolo II, Parte II, è stata messa in luce tanto la difficoltà definitoria quanto i contorni ormai sfumati che distinguono le attività volte alla garanzia della sicurezza nazionale e quelle finalizzate alla tutela della sicurezza pubblica, anche a causa dell'impiego, in entrambi i casi, di mezzi tecnologici sempre più sofisticati ed invasivi della sfera privata.

una normativa nazionale, anche in un contesto di gravi minacce alla sicurezza nazionale, imponga una conservazione generalizzata ed indifferenziata di tutti i metadati derivanti da telecomunicazioni elettroniche.

2.1.2.3. – La determinazione dell'ambito di applicazione della Direttiva e-Privacy *e gli effetti di una dichiarazione di incompatibilità di una normativa nazionale in materia di* data retention

Queste stesse considerazioni vengono impiegate e testualmente riportate dall'Avvocato Campos Sanchez-Bordona nelle sue Conclusioni alla causa C-623/17 promossa dal IPT del Regno Unito. In questo caso i giudici del rinvio si chiedevano se la finalità di garanzia della sicurezza nazionale dovesse portare ad escludere dall'ambito di applicazione della Direttiva 2002/58 la normativa nazionale sulla conservazione dei metadati e sulla trasmissione degli stessi alle agenzie di intelligence. Il chiaro e significativo ragionamento dell'Avvocato generale, sopra analizzato, lo porta, ancora una volta, ad escludere qualsiasi rilevanza del richiamo al concetto di sicurezza nazionale: le tecniche di acquisizione e trasferimento di metadati in massa alle autorità di intelligence, indipendentemente dalla finalità cui esse sono preposte, prevedono comunque un previo trattamento di dati da parte dei fornitori di servizi di telecomunicazione e questo basta per far considerare tali operazioni rientranti nell'ambito di applicazione della Direttiva *e-Privacy*.

L'Avvocato generale, riprendendo peraltro quella distinzione che già era stata effettuata dal collega Saugmandsgaard Øe nella causa *Ministerio Fiscal*, ha precisato che mentre le attività delle SIA "potrebbero collocarsi al di fuori del diritto dell'Unione qualora non riguardassero gli operatori di comunicazioni elettroniche" (par. 32) – ad esempio laddove esse provvedessero direttamente alla intercettazione e conservazione dei metadati tratti dalle comunicazioni elettroniche –, quando si parla invece di conservazione e successiva trasmissione da parte degli operatori privati allora si deve considerare questa disciplina come rientrante nel diritto dell'UE. Ecco perché i criteri delineati nella giurisprudenza europea vengono confermati nella sostanza, senza bisogno di alcun temperamento, e debbono quindi essere applicati anche rispetto a misure quali quelle indicate dai giudici del rinvio inglesi: pur prevedendo una conservazione diretta da parte delle SIA stesse, il sistema analizzato dal IPT si fondava comunque sul trasferimento – e pertanto sul trattamento – dei dati da parte degli operatori privati e non su di una 'intercettazione' diretta operata dalle autorità statali; ed ecco anche perché l'Avvocato generale ha concluso col ritenere che le tecniche di acquisizione massiva e di trasferimento automatizzato dei metadati alle SIA, che presuppongono una forma di conservazione indifferenziata e generalizzata dei metadati da parte dei *service providers*, non possono essere considerate compatibili con il diritto dell'Unione europea. A nulla quindi sono servite quelle puntualizzazioni forti e monitorie dei giudici del IPT, che avvertivano circa le conseguenze potenzialmente disastrose derivanti dall'applicazione dei 'requisiti *Tele2*' alle misure adottate dalle SIA, individuate addirittura nella vanificazione delle attività di intelligence stesse e dunque dal venirsi a creare di una situazione di serio rischio per la sicurezza del Regno Unito.

Questo punto, del resto, si scontra con l'annosa questione dalla determinazione dell'ambito di applicazione della Direttiva 2002/58: come si è visto nei previ paragrafi e Capitoli, con riferimento a settori relativi alla difesa della sicurezza nazionale si è registrato il tentativo di molti Stati membri di 'portare al di fuori' del diritto dell'UE questo specifico campo d'azione, con ragionamenti ed osservazioni che sono state, sin dalla sentenza *DRI*, al centro di un ampio dibattito. Non stupisce pertanto che non solo nel rinvio del IPT bensì anche in quello promosso dal Consiglio di Stato francese la medesima questione fosse stata riproposta addirittura mediante il richiamo alla tanto discussa sentenza del 2006, C-317/04, *Parlamento c. Consiglio e Commissione*, già richiamata nei Capitoli II e III e attinente alla Decisione del Consiglio relativa all'accordo tra Comunità europea e USA sul trattamento

e trasferimento dei dati PNR. Il rinvio a quella pronuncia, come si ricorderà, era già stato utilizzato per giustificare la teoria di cui taluni Stati membri si erano fatti portatori sin dalla adozione della DRD, secondo cui normative nazionali riguardanti la conservazione dei metadati per finalità di sicurezza nazionale non avrebbero potuto essere considerate rientranti nell'ambito di applicazione del diritto dell'UE.

L'Avvocato generale nelle sue Conclusioni alle cause riunite C- 511/18 e C-512/18 reputa opportuno chiarire nuovamente i dubbi riproposti su tale punto, analizzando la sentenza *Parlamento c. Consiglio e Commissione* e comparandola a quanto affermato nelle sentenze *Tele2* e *Ministerio Fiscal*, escludendo infine qualsiasi discordanza tra le posizioni espresse dalla Corte e dunque qualsiasi diversità di approccio che possa avvalorare la lettura proposta dagli Stati membri. Nella pronuncia del 2006 infatti i giudici di Lussemburgo avevano escluso dall'ambito di applicazione del diritto dell'UE, e della Direttiva 95/46 in particolare, il richiamato accordo in materia di PNR poiché, sebbene il trasferimento di dati costituisse un trattamento svolto da vettori aerei, dunque da attori privati nell'ambito delle loro attività economiche, esso non era finalizzato ad una prestazione di servizi bensì solo alla salvaguardia della sicurezza pubblica nello Stato terzo. Nello specifico contesto della cooperazione tra UE e USA, e dunque in un ambito internazionale, doveva prevalere la dimensione statale dell'attività regolata dall'accordo, cioè quella del trattamento dei dati trasferiti per scopi di repressione dei reati, piuttosto che il trattamento operato dai soggetti privati. Inoltre, la clausola di esclusione della Direttiva 95/46 estrometteva dalla disciplina di quest'ultima i trattamenti aventi ad oggetto la sicurezza dello Stato: da tale dettato normativo si deduce come tale esclusione dovesse essere identificata sulla base dello scopo del trattamento, indipendentemente dal soggetto deputato a compierlo; per questo le operazioni di trasferimento ricadevano in tale esclusione e non rientravano nell'ambito di applicazione del diritto europeo. La clausola di esclusione inserita nella Direttiva *e-Privacy*, all'art. 1, co. 3, invece, estrometteva le attività dirette a tutelare la sicurezza dello Stato, intendendo espressamente per tali attività quelle svolte dallo Stato e dalle autorità statali e dunque estranee ai settori di operatività dei singoli. Viene pertanto identificata una netta distinzione tra le due clausole di esclusione, quella inserita nella previgente Direttiva sulla protezione dei dati e quella invece nella Direttiva 2002/58 cui i rinvii si riferiscono. Per questo motivo e proprio in ragione di questa differenza sostanziale, la pronuncia del 2006 aveva portato ad un esito differente rispetto alla decisione *Tele2*: nessun cambiamento di orientamento può essere ravvisato nella giurisprudenza della Corte e la sentenza *Parlamento c. Consiglio e Commissione* non può essere in alcun modo richiamata in casi in cui sono la Direttiva *e-Privacy* e la sua diversa clausola di esclusione a venire in gioco.

Liberato il campo quindi da ogni parallelismo con la citata sentenza, l'Avvocato chiarisce poi anche una ulteriore possibile fonte di confusione derivante dalla Direttiva 2002/58 stessa: il termine sicurezza nazionale (o sicurezza dello Stato) viene ivi richiamato sia nella clausola di esclusione indicata all'art. 1, co. 3 che in quella di limitazione dell'art. 15 della medesima Direttiva. Ebbene proprio tale distinzione risulta determinante: la 'sicurezza nazionale' di cui all'art. 1, co. 3 deve essere intesa come riferita a quelle attività autonomamente svolte dai poteri pubblici, senza la collaborazione di soggetti privati e quindi senza l'imposizione di obblighi in capo ad essi (par. 79). In sintesi quindi, debbono essere rispettate le competenze degli Stati membri nell'ambito della sicurezza nazionale "allorché essi le esercitino in modo diretto e con i propri mezzi. Viceversa, allorché, anche per questi stessi motivi di sicurezza nazionale, sia richiesta la collaborazione di privati, ai quali vengono imposti determinati obblighi, tale circostanza comporta l'ingresso in un ambito disciplinato dal diritto dell'Unione" (par. 85).

Anche sotto il profilo dell'ambito di applicazione della normativa europea quindi non emerge alcuna novità: la giurisprudenza della CGUE viene confermata e vengono semplicemente suggerite alcune vie interpretative "per affinarne il contenuto" (par. 92). Quella esclusione così auspicata e più o meno velatamente suggerita negli stessi quesiti dei rinvii pregiudiziali, volta a lasciare interamente agli Stati

membri – e dunque libera dai vincoli stabiliti nella *Tele2* – la delicata e determinante disciplina della *data retention* laddove ad essere interessata fosse la sicurezza nazionale, non è stata dunque accolta dall'Avvocato generale. Quest'ultimo, pur consapevole delle difficoltà applicative in tale ambito e pur proponendo come legittima una forma di conservazione *limitata*, meno rigida rispetto a quella *mirata* suggerita dalla Corte di giustizia, non è giunto a consentire quella riconsiderazione e restrizione dei requisiti dettati nelle previe pronunce. Nessuna marcia indietro quindi, bensì un piccolo passo verso una forma di conservazione 'intermedia' che possa meglio conciliare, in una soluzione di compromesso, le esigenze di efficacia delle autorità nazionali e la tutela dei diritti fondamentali.

Le medesime considerazioni possono poi essere svolte anche con riferimento alla disciplina dell'accesso ai dati, rispetto alla quale l'Avvocato ritiene adeguati i requisiti già indicati nelle sentenze *Tele2* e *Ministerio Fiscal*: spetterà dunque al giudice del rinvio e in generale al giudice nazionale analizzare nel dettaglio le condizioni di accesso previste per le diverse autorità statali (ad esempio la normativa belga considerata nella causa C-520/18 prevede criteri differenti a seconda che l'accesso venga effettuato da parte di autorità di *law enforcement*, giudiziarie, di intelligence o ancora autorità di servizi di emergenza). Campos Sanchez-Bordona tuttavia non manca di ribadire l'importanza dei requisiti dell'informazione obbligatoria all'interessato in caso di accesso consentito ai propri metadati, qualora tale notifica non comprometta le indagini in corso[45], o ancora quello della gravità dei reati tale da giustificare l'accesso ai dati e dunque la sussistenza di un chiaro nesso tra intensità dell'ingerenza e gravità del crimine oggetto di indagine (par. 142).

La natura 'compromissoria' della posizione dell'Avvocato generale emerge infine con estrema evidenza nell'analisi del quesito finale, posto dalla Corte costituzionale belga nella causa C-520/18, circa la possibilità di mantenere provvisoriamente gli effetti di una normativa nazionale sulla conservazione dei dati trovata incompatibile con il diritto dell'UE. Questo aspetto riveste una importanza centrale rispetto alla garanzia sia della certezza del diritto che della possibilità di utilizzare i metadati raccolti e conservati per scopi securitari nonostante la dichiarazione di incompatibilità della legislazione di riferimento, con evidenti e chiari effetti per i procedimenti penali che proprio sull'analisi e sulle informazioni fornite dai metadati conservati si fondano. L'Avvocato generale, ben consapevole delle conseguenze anche devastanti che potrebbero scaturire dalla risposta a tale delicato quesito, ha richiamato la giurisprudenza europea nel caso *Inter-Environnement Wallonie e Terre wallonne* del 28 febbraio 2012, causa C-41/11, poi confermata anche nella sentenza del 2019, C-411/17 *Inter-Environnement Wallonie e Bond Beter Leefmiliue Vlaanderen*: in queste controversie era stato concesso ad un giudice nazionale, dinnanzi ad una esigenza imperativa legata alla protezione ambientale, di mantenere in via eccezionale gli effetti di un atto statale annullato per contrasto con una norma di livello europeo. Tale giurisprudenza è stata ritenuta applicabile anche in altri settori del diritto dell'Unione e non solo alle questioni ambientali, purché si faccia riferimento ad ambiti che rappresentano obiettivi essenziali dell'Unione, rivestendo quindi carattere trasversale e fondamentale. Ebbene, la costituzione di uno spazio di sicurezza, il mantenimento dell'ordine pubblico e la tutela della sicurezza nazionale sono ritenuti dall'Avvocato obiettivi trasversali e fondamentali dell'Unione stessa, in quanto il loro raggiungimento "costituisce condizione necessaria per l'istituzione di un quadro normativo idoneo a garantire l'effettivo godimento dei diritti e delle libertà fondamentali" (par. 149). Sulla base di tali considerazioni, anche ragioni imperative nell'ambito della tutela della sicurezza possono autorizzare il giudice del rinvio a mantenere, in via provvisoria, alcuni effetti della legge controversa e dichiarata non

[45] Nelle Conclusioni relative al rinvio pregiudiziale promosso dal Consiglio di Stato francese, poi, l'Avvocato si addentra ancora maggiormente nel dettaglio con riferimento a tale requisito: il giudice del rinvio infatti chiede se tale obbligo di informazione sia da considerarsi vincolante in tutti i casi. La risposta proposta è affermativa: "l'accesso al giudice per la tutela dei propri diritti deve essere effettivo per tutti, il che implica che chi abbia subito un trattamento dei propri dati personali deve poter contestare giudizialmente la legittimità di tale trattamento e, di conseguenza, deve essere informato della sua esistenza. (..) La difesa dei suoi diritti non può dipendere dalla circostanza che egli venga a conoscenza di tale trattamento tramite terzi o con i propri mezzi", par. 151-153.

compatibile con il diritto dell'UE: la proroga dovrebbe essere concessa per evitare il crearsi di ripercussioni deleterie e gravi sulla sicurezza pubblica e dello Stato, che non potrebbero essere con altri mezzi evitate e che comporterebbero la perdita per le autorità nazionali di un valido strumento di garanzia della sicurezza nazionale (par. 153); tale proroga tuttavia deve essere considerata possibile solo limitatamente al lasso di tempo strettamente necessario affinché il legislatore ponga rimedio alla situazione, mediante l'approvazione di una normativa conforme al diritto dell'UE. Risulta sotto tale profilo interessante sottolineare come l'Avvocato generale abbia ritenuto questa soluzione percorribile ed auspicabile considerando da un lato le difficoltà riscontrate e denunciate dagli Stati membri stessi nell'adeguamento dell'ordinamento nazionale ai requisiti stabiliti dalla CGUE nella sentenza *Tele2*, nonché, dall'altro, valutando positivamente l'atteggiamento del legislatore belga, nello specifico caso, che aveva già in passato manifestato la propria volontà di adeguarsi alla giurisprudenza europea, modificando, all'indomani della sentenza *DRI*, la propria normativa nazionale in materia di conservazione dei metadati (par. 154). In questo modo quindi l'Avvocato propende per affidare ai giudici nazionali la valutazione e determinazione dell'impatto e delle conseguenze derivanti dall'annullamento di una normativa interna disciplinante la *data retention*, dando così la possibilità di limitare ed arginare le rischiose derive che ne potrebbero derivare[46].

2.1.2.4. – Una sostanziale riaffermazione dei criteri indicati dalla giurisprudenza della CGUE: gli scenari aperti dalle Conclusioni dell'Avvocato generale

Prima di analizzare gli altri rinvii pregiudiziali promossi, la sintesi delle tre Conclusioni dell'Avvocato Campos Sanchez-Bordona sino ad ora svolta ci consente di muovere alcune riflessioni: innanzitutto, se la Corte dovesse seguire le considerazioni proposte, i criteri delineati nella sentenza *Tele2* resterebbero sostanzialmente invariati e confermati. Le preoccupazioni espresse dagli Stati membri – talvolta condivise dai giudici del rinvio – e il loro timore di vedere fortemente limitata l'efficacia di uno strumento così importante per la garanzia della sicurezza, non solo pubblica ma anche nazionale, quale appunto la conservazione generalizzata dei metadati, resterebbero in gran parte senza soluzione. I requisiti fissati dalla giurisprudenza europea, pur nella loro riconosciuta complessità, risulterebbero idonei ed applicabili anche a normative che mirano ad affrontare minacce gravi alla sicurezza, quali il terrorismo. Solo in casi eccezionali, di pericolo imminente o rischio straordinario, diventerebbe possibile imporre un obbligo di conservazione più ampio, benché per un periodo di tempo limitato e accompagnato da idonee garanzie giurisdizionali. Anche sul fronte dei criteri attinenti all'accesso e alla determinazione dell'ambito di applicazione della Direttiva 2002/58 e della relativa interpretazione fornita dalla CGUE, non vi sarebbero grandi innovazioni, essendo confermata quella visione, promossa già nel caso *Ministerio Fiscal* nelle Conclusioni dell'Avvocato generale, che mira ad escludere dal diritto dell'Unione europea solo le attività per scopi securitari poste in essere direttamente dalle autorità pubbliche statali, senza il coinvolgimento di soggetti privati: è questa dunque, e non la finalità perseguita, la distinzione determinante. Sulla base di queste considerazioni, le normative belga, francese e inglese, tutte fondate su una forma di conservazione generalizzata ed indiscriminata – sebbene

[46] Questa posizione dell'Avvocato generale si pone in contrasto con quanto invece sostenuto dalla Commissione, intervenuta nel processo dinnanzi alla CGUE: essa infatti riteneva che solo la Corte di giustizia dell'UE avrebbe potuto, in casi eccezionali e per esigenze di certezza del diritto, "concedere una sospensione provvisoria dell'effetto di disapplicazione esercitato da una norma di diritto dell'Unione rispetto a norme di diritto interno con esso in contrasto" (par. 145), poiché ammettere il contrario vorrebbe dire pregiudicare l'applicazione uniforme del diritto europeo. Nel caso specifico in esame, siccome nella sentenza *DRI* e *Tele2* la Corte non aveva in alcun modo limitato gli effetti nel tempo della propria interpretazione della DRD e dell'art. 15 Direttiva *e-Privacy*, non si sarebbe potuto concedere nessuna modulazione degli effetti rispetto ad una normativa nazionale in contrasto col diritto dell'UE.

con diverse sfumature, alcune delle quali verranno ampiamente messe in luce nella Parte III di questo lavoro –, non risulterebbero dunque compatibili con il diritto dell'UE e con l'interpretazione fornita dalla Corte di giustizia circa l'art. 15 della Direttiva 2002/58.

Ancora una volta, però, come già sottolineato nel Capitolo II nell'analisi sia della sentenza *DRI* che *Tele2*, ogni considerazione quanto all'efficacia della *data retention* viene lasciata a margine delle valutazioni svolte dall'Avvocato generale: il fatto che una conservazione generalizzata rappresenti realmente uno strumento utile ed efficace per prevenire e contrastare la criminalità grave viene infatti ritenuta questione assodata e difficilmente contestabile, pur in mancanza di analisi, fondate su dati e fatti, e di considerazioni specifiche capaci di avvalorare questa tesi. Sul punto, Campos Sanchez-Bordona giunge ad affermare che "in ogni caso, la determinazione di tali tecniche di indagine e la valutazione della loro efficacia rientrano nel margine di discrezionalità degli Stati membri" (nota 69), quasi a voler escludere il bisogno di una riflessione sulla idoneità ed adeguatezza dello strumento impiegato al raggiungimento della finalità perseguita, che pure dovrebbe rientrare in quel vaglio di necessità richiesto dall'art. 52 della Carta di Nizza.

Ciò che infine emerge chiaramente è la forte attenzione e rilievo mostrati rispetto alla disciplina della conservazione, prima ancora che a quella dell'accesso: nelle Conclusioni relative alla causa C-520/18 l'Avvocato generale sostiene come "le considerazioni relative all'accesso delle autorità ai dati passino in secondo piano quando, per i motivi già illustrati, è la stessa conservazione generalizzata e indifferenziata di tali dati la ragione principale per cui la normativa nazionale sulla quale verte la presente domanda di pronuncia pregiudiziale non risulta conforme al diritto dell'Unione", (par. 143).

2.2. – Le Conclusioni dell'Avvocato generale Pitruzzella nel rinvio pregiudiziale **H.K. c. Prokuratuur***: la disciplina dell'accesso, la gravità del reato e il controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente*

Diversamente dai rinvii sino ad ora esaminati, maggiore attenzione alle condizioni e ai requisiti riguardanti l'accesso ai metadati conservati viene invece prestata nel rinvio pregiudiziale *H.K. c. Prokuratuur*, relativamente al quale sono state pubblicate le Conclusioni dell'Avvocato generale Pitruzzella, pochi giorni dopo quelle di Campos Sanchez-Bordona. Nel rinvio promosso dalla Corte suprema estone e riguardante, ancora una volta, l'interpretazione dell'art. 15 Direttiva *e-Privacy*, viene chiesto infatti se tra i criteri da valutare per determinare la gravità dell'ingerenza nei diritti fondamentali rientrino sia la tipologia e la quantità di dati rispetto ai quali viene effettuato l'accesso, che la durata del periodo per il quale l'accesso stesso viene richiesto. Ulteriore quesito attiene poi ad uno dei criteri di accesso fissati dalla pronuncia *Tele2* ovvero il controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente: i giudici del rinvio si chiedono in particolare se tale condizione possa essere legittimamente assolta laddove il controllo venga effettuato da un pubblico ministero che dirige il procedimento istruttorio ma che, sulla base della normativa nazionale, dovrà poi anche rappresentare la pubblica accusa nel corso del procedimento giudiziario eventualmente avviato.

Ponendo interamente l'attenzione sulla regolamentazione dell'accesso, l'Avvocato generale risolve con grande velocità – e richiamando interamente la giurisprudenza precedente, da *Tele2* a *Ministerio Fiscal* – sia la questione riguardante l'ambito di applicazione della Direttiva 2002/58, sia quella sulla conservazione dei metadati: le disposizioni attinenti all'accesso vengono considerate rientranti nell'ambito di applicazione del diritto dell'UE, respingendosi quindi le obiezioni di alcuni Stati membri che, come in passato, avevano sostenuto di poter escludere la regolamentazione dell'utilizzo dei metadati da parte delle autorità statali dalla disciplina europea. Pitruzzella ha poi ripreso pedissequamente quanto già evidenziato nella pronuncia *Ministerio Fiscal* che presenta diverse similitudini con il rinvio promosso: come in quel contesto, infatti, le questioni formulate dal giudice

estone non vogliono determinare se i dati cui si fa riferimento siano stati conservati conformemente alla disciplina europea, bensì solo a stabilire la compatibilità al diritto dell'UE delle condizioni di accesso (par. 51). Viene pertanto lasciata al giudice nazionale ogni valutazione circa la legittimità della normativa in materia di conservazione dei metadati per scopi securitari. Questo è motivato, oltre che da ragioni legate al *petitum* e dunque alla necessità di rispondere a quanto formulato nei quesiti del rinvio, anche da motivi sostanziali: secondo l'Avvocato generale, la Corte, sin dalla pronuncia *Tele2*, ha dimostrato di considerare la conservazione e l'accesso come due ingerenze distinte (par. 57).

Ripercorrendo e confermando quelli che vengono definiti gli 'insegnamenti' delle previe pronunce in materia, l'Avvocato generale inizia a rispondere ai quesiti posti fornendo alcune generali indicazioni necessarie ad individuare quali criteri consentano di stabilire la gravità di una ingerenza: quest'ultima diviene 'grave' laddove l'accesso consenta alle autorità nazionali di trarre conclusioni precise sulla vita privata dei soggetti ai quali i dati si riferiscono. "Orbene, per poter delineare il preciso ritratto di una persona, è necessario non soltanto che l'accesso riguardi più categorie di dati, come i dati identificativi, relativi al traffico e i dati relativi all'ubicazione, ma anche che tale accesso abbia ad oggetto un periodo abbastanza lungo da poter rivelare con sufficiente precisione gli aspetti principali della vita di una persona. (..) Deve parimenti essere preso in considerazione il cumulo di varie domande di accesso relative a una sola persona, anche se esse concernono periodi brevi" (par. 82-83)[47]. Ecco allora che la categoria dei dati, la quantità e varietà degli stessi e la durata del periodo di accesso vengono individuati come criteri fondamentali per determinare la gravità dell'ingerenza e, conseguentemente, secondo il ragionamento espresso in *Ministerio Fiscal*, la necessaria sussistenza di un reato di carattere grave.

Proprio con riferimento a quest'ultimo punto, l'Avvocato afferma, come già in precedenza era stato statuito da Saugmandsgaard Øe, che la qualifica di reato grave deve essere lasciata alla discrezionalità degli Stati membri, anche in considerazione del fatto che, a seconda dei diversi sistemi giuridici, il medesimo reato può essere punito più o meno severamente. Mentre nella sentenza *Ministerio Fiscal* la Corte non aveva preso posizione sulla questione della determinazione della gravità del reato, di fatto non rispondendo a quanto richiesto concretamente dal giudice del rinvio, nel caso in esame però Pitruzzella fornisce preziose indicazioni sul punto: il criterio per accertare la gravità del reato non può essere individuato solo nella tipologia della pena bensì è necessario prendere in considerazione anche "la natura dei reati, il danno che causano alla società, il pregiudizio che arrecano ai beni giuridici e i loro effetti complessivi sull'ordinamento giuridico nazionale nonché sui valori di una società democratica. Anche il contesto storico, economico e sociale specifico di ciascuno Stato membro svolge un ruolo in proposito" (par. 93). Inoltre, se certamente non è sempre possibile determinare con precisione il grado di gravità di un reato al momento della richiesta di autorizzazione dell'accesso, che può anche avvenire in una fase precoce delle indagini, è altrettanto vero che tale incertezza non può far venire meno la necessità di specificare, "sulla base di un sospetto avvalorato da elementi obiettivi", per quale reato l'accesso venga richiesto. "Pertanto una domanda di accesso non può avere per scopo l'esame, nell'arco di un dato periodo, di tutti i fatti e gesti di una persona, in vista della ricerca di eventuali reati" (par. 96), escludendo quindi la legittimità di una pratica di accesso e ricerca 'generalizzata' ed esplorativa; conseguentemente, se nell'arco dell'indagine emergessero nuovi fatti, tali da rendere necessario l'accesso ad ulteriori dati, dovrà essere richiesta un ulteriore ed apposita autorizzazione.

[47] "La valutazione del grado dell'ingerenza nei diritti fondamentali derivante dall'accesso delle autorità nazionali competenti ai dati personali conservati risulta da un esame concreto delle circostanze proprie di ciascun caso di specie", par. 85. Ad esempio nel caso oggetto di rinvio, il Procuratore distrettuale di Viru aveva autorizzato diversi accessi, relativi ad una durata di un giorno, un mese e un anno, riguardanti due numeri di telefono appartenenti ad un solo soggetto, H. K., indagata di vari reati, dal furto alla violenza. Tali dati erano volti a dimostrare, grazie all'indicazione dei ripetitori telefonici agganciati in un determinato giorno, che H. K. era autrice del furto di cui era sospettata. Si era però posta, rispetto a tali accessi ai metadati, la questione circa la loro ammissibilità e la loro compatibilità con la giurisprudenza europea in materia. Da tale dubbio ha avuto origine il rinvio pregiudiziale in esame.

Dopo aver fornito indicazioni volte a determinare la gravità dell'ingerenza e la gravità del reato, l'Avvocato generale precisa quello che anche il governo estone definisce "il criterio dell'assoluta necessità": una ulteriore valutazione da effettuare deve infatti essere finalizzata a stabilire quali dati si rendano davvero necessari "per il buon esito del procedimento penale e senza i quali non sarebbe possibile, nel contesto di un determinato procedimento, consentire di far emergere la verità o catturare un presunto delinquente o criminale" (par. 94).

Definite queste fondamentali coordinate, che ampliano e precisano quanto già espresso dalla sentenza *Ministerio Fiscal*, l'Avvocato esamina l'ulteriore quesito posto dal giudice estone, quello cioè riguardante la determinazione della natura indipendente dell'autorità preposta al controllo preventivo all'accesso. In primis viene stabilito, mediante l'analisi della giurisprudenza europea in materia, cosa debba intendersi per 'indipendenza': per potersi dire 'indipendente' un'autorità deve poter svolgere le proprie funzioni senza subire influenze esterne, né dirette né indirette, ed essere al di sopra di qualsiasi sospetto di parzialità (par. 103), cioè soddisfare un requisito di obiettività nell'ambito del controllo effettuato. Sulla base di tale definizione, che comprende al suo interno anche il concetto di imparzialità, dovrà essere valutata la natura del pubblico ministero: dovrà in particolare determinarsi se quest'ultimo, nelle attività volte ad autorizzare l'accesso ai metadati, possa ingenerare dubbi legittimi quanto "all'impermeabilità dei procuratori rispetto ad elementi esterni e alla loro neutralità", alla luce della duplice funzione da essi svolta di direzione del procedimento istruttorio e di parte del procedimento giudiziario quale pubblica accusa nel caso in cui venga esercitata l'azione penale.

Su tale punto delicato, e pur riconoscendo l'esistenza di garanzie nella normativa estone, l'Avvocato generale ritiene che proprio la particolarità e duplicità della natura e delle funzioni esercitate dal pubblico ministero facciano sorgere un legittimo dubbio sulla indipendenza di tale autorità e sulla sua capacità di esercitare un controllo preventivo neutro ed obiettivo sul carattere proporzionato dell'accesso ai dati (par. 118): la circostanza per la quale l'autorità tenuta a tale importante controllo sia al contempo quella che può perseguire e poi rappresentare la pubblica accusa, finisce con l'indebolire le garanzie di imparzialità e far insorgere nelle persone coinvolte la percezione che il pubblico ministero abbia un interesse a concedere un ampio accesso ai loro dati. In conclusione, dunque, il requisito del controllo indipendente non può ritenersi soddisfatto in casi di cumulo di competenze nella persona del pubblico ministero, come nel caso esaminato. Secondo la Commissione, "la situazione potrebbe essere differente se l'organizzazione amministrativa interna del pubblico ministero fosse tale da far sì che il procuratore che deve pronunciarsi sulla domanda di accesso non svolga alcun ruolo nel procedimento istruttorio e nelle fasi successive del procedimento penale, inclusa la pubblica accusa" (par. 125). Questa interessante lettura della Commissione, condivisa da Pitruzzella nella sua sostanza, non può essere tuttavia considerata applicabile al caso estone nel quale l'organizzazione gerarchica della procura non consentirebbe, se non difficilmente, di porre rimedio ai dubbi derivanti dal cumulo di compiti in capo al pubblico ministero stesso. L'Avvocato generale comunque conclude sostenendo che "al fine di rispettare l'autonomia procedurale degli Stati membri, la Corte non dovrebbe intromettersi ulteriormente nell'organizzazione generale dell'amministrazione della giustizia negli Stati membri e neppure nell'organizzazione interna delle procure. Compete agli Stati membri predisporre gli strumenti idonei a garantire che il controllo preliminare all'accesso ai dati conservati assicuri un giusto equilibrio tra gli interessi connessi all'efficacia dell'indagine penale e il diritto alla protezione dei dati delle persone interessate da tale accesso" (par. 127).

Pitruzzella aggiunge poi un ulteriore e rilevante tassello a questa riflessione sulla disciplina dell'accesso ai metadati, sostenendo che la mancanza di un controllo preventivo non possa essere compensata da un controllo giurisdizionale effettuato *ex post*, cioè successivamente all'autorizzazione dell'accesso. Sotto questo profilo quindi l'Avvocato respinge quella posizione, espressa invece dalla Corte EDU nella sentenza *Szabo* – di cui si parlerà ampiamente nel successivo Capitolo V – che ha ammesso, a determinate condizioni, la legittimità di un mancato controllo preventivo laddove un

controllo giurisdizionale successivo venga garantito. Una lettura complessiva delle tutele poste in essere, che porta a ritenere compensate talune carenze se sopperite da altre garanzie, viene respinta dall'Avvocato generale con riferimento alla disciplina dell'accesso, similmente a quanto era stato già affermato più genericamente anche da Sanchez-Bordone che negava la possibilità che la generalità della conservazione potesse essere compensata da maggiori tutele nella fase di accesso.

In conclusione, anche in questo rinvio pregiudiziale vengono sostanzialmente confermati i requisiti e i criteri già indicati nelle previe sentenze alle quali però, con specifico riferimento alla fase dell'accesso, vengono forniti importanti chiarimenti quanto alla valutazione della gravità della ingerenza e del reato e della indipendenza della autorità deputata al controllo preventivo. Si addiviene così ad un arricchimento dei requisiti, pur in coerenza con quanto era già stato in passato stabilito.

2.3. – I rinvii pregiudiziali promossi dalle Corti tedesca e irlandese: una conferma dei dubbi e delle criticità derivanti dalla giurisprudenza della CGUE in materia di data retention

La disamina di questo paragrafo, dedicato agli sviluppi giurisprudenziali più recenti, non può infine che chiudersi con l'analisi degli ulteriori due rinvii pregiudiziali più recentemente promossi dai giudici di Germania e Irlanda e riguardanti alcuni specifici aspetti della disciplina della *data retention* e dell'accesso, taluni in parte già presenti e sottolineati nei casi sin qui esaminati.

Innanzitutto, il rinvio promosso dalla Corte amministrativa federale tedesca presenta elementi di forte interesse: l'art. 113b del *Telekommunikationsgesetz* (c.d. TKG), ovvero la normativa tedesca che prevede un obbligo di conservazione dei metadati in capo ai fornitori di servizi di telecomunicazione per scopi securitari, è stato modificato dalla legge del 10 dicembre 2015, come reazione sia alla sentenza *DRI* che alla previa decisione del Tribunale costituzionale federale del 2010, di cui si è ampiamente parlato nel Capitolo II e che aveva dichiarato l'incostituzionalità della previa legislazione in materia di *data retention*. La normativa modificata, e tuttora vigente, ha cercato di integrare i principi e requisiti fissati dalla giurisprudenza nazionale e sovranazionale in materia, pur senza però rinunciare ad una forma di conservazione generalizzata, cioè non ristretta sulla base di un indizio in grado di creare un collegamento tra un soggetto – o un gruppo di soggetti – ed un reato grave. Proprio per questo aspetto, considerato in contrasto con la normativa dell'Unione e soprattutto con la giurisprudenza della CGUE, la fornitrice di servizi di telecomunicazione SpaceNet AG aveva promosso azione avverso il Tribunale amministrativo federale che, in primo grado, aveva ritenuto la ricorrente non obbligata a memorizzare i metadati; dinnanzi a questa pronuncia, dai prorompenti e rischiosi effetti, capace di incidere fortemente sull'efficacia dello strumento della *data retention* per scopi securitari, la Repubblica federale tedesca ha proposto ricorso di annullamento: per risolvere tale delicata questione, il giudice amministrativo tuttavia ha ritenuto imprescindibile determinare se la normativa nazionale fosse compatibile con il diritto dell'Unione e, per giungere a tale valutazione, si rendeva necessario un chiarimento da parte della CGUE sull'interpretazione dell'art. 15 della Direttiva *e-Privacy*. Per giungere a tale conclusione, la Corte tedesca ha svolto un interessante ed approfondito esame della giurisprudenza europea: se la sentenza *Tele2* deve essere interpretata nel senso che una conservazione generalizzata è sempre, in tutte le circostanze e per sua stessa natura, incompatibile con il diritto dell'Unione, allora egualmente incompatibile dovrebbe essere considerata una normativa nazionale che preveda un obbligo di *data retention* senza alcuna limitazione personale, territoriale o temporale. Il giudice del rinvio, tuttavia, ha sollevato alcuni dubbi quanto a questa rigida lettura, in particolare chiedendosi se debba risultare non conforme alla Carta di Nizza e ai requisiti stabiliti dalla CGUE anche una normativa, come quella tedesca, che, pur prevedendo una conservazione ampia e non fondata su un indizio di connessione ad una minaccia per la sicurezza pubblica o nazionale, stabilisce precisi e dettagliati limiti e ampie garanzie; sono state infatti richiamate sul punto (a) le disposizioni specifiche sulla durata della *data retention*,

estremamente ridotta e differenziata a seconda della categoria dei dati (quattro settimane per i dati relativi all'ubicazione e dieci settimane per tutte le altre tipologie) nonché l'esclusione dalla conservazione del contenuto delle comunicazioni, dei dati relativi alle pagine Internet visitate, dei collegamenti effettuati a linee Internet in ambito sociale e religioso nonché dei dati sul traffico di soggetti tenuti al segreto professionale; (b) l'esistenza di rigorose e severe restrizioni attinenti non solo alla sicurezza dei dati conservati ma anche all'accesso, ammesso solo per finalità di lotta contro i reati gravi o prevenzione di un pericolo concreto per la vita, l'integrità fisica o la libertà di una persona, la salvaguardia dello Stato o di un Land. Tutte queste salvaguardie e limiti riducono considerevolmente l'invasività della conservazione stessa e il rischio di profilazione delle persone cui i metadati si riferiscono e dunque l'ingerenza nei loro diritti fondamentali. I giudici del rinvio, sulla base di tali considerazione, suggeriscono pertanto una interpretazione dell'art. 15 della Direttiva *e-Privacy* che non escluda a priori la compatibilità col diritto dell'UE di qualsiasi forma di conservazione ingiustificata – cioè non targettizzata[48] –; questo anche perché "il concetto alla base della conservazione dei dati non è conciliabile con la richiesta formulata dalla Corte di distinguere, nei dati oggetto di memorizzazione, in base alle persone, ai periodi e alle aree geografiche" (par. 25, *Sintesi della domanda di pronuncia pregiudiziale ai sensi dell'art. 98, par. 1, del Regolamento di procedura della CGUE*). Una lettura eccessivamente rigida della giurisprudenza dei giudici di Lussemburgo porterebbe inoltre ad una notevole restrizione del margine di discrezionalità ed autonomia lasciato ai legislatori nazionali nell'ambito della tutela della sicurezza, ai sensi dell'art. 4, co. 2, TUE. Quello che viene posto in luce dunque è la necessità di trovare un equilibrio tra il rispetto dei diritti fondamentali e l'obbligo degli Stati membri di garantire il diritto alla sicurezza dei propri cittadini. L'analisi svolta dai giudici del rinvio li porta in conclusione ad affermare che "non può desumersi dalla giurisprudenza della Corte [di giustizia dell'UE] il fatto che ai legislatori nazionali non sia più concessa la possibilità, sulla base di una valutazione globale, di introdurre la conservazione ingiustificata dei dati, eventualmente integrata da rigorose norme di accesso, al fine di tener conto dello specifico potenziale di rischio associato ai nuovi mezzi di telecomunicazione" (par. 27). Da qui dunque le ragioni del rinvio alla CGUE, rinvio che ancora una volta, come già accaduto per gli altri già analizzati, sembra suggerire una modulazione e 'affievolimento' dei requisiti stabiliti nelle previe pronunce, ritenuti incompatibili con la finalità stessa dello strumento della conservazione dei metadati.

Particolarmente interessante è notare l'attenzione posta dalla Corte amministrativa federale non solo verso le sentenze dei giudici di Lussemburgo bensì anche verso quelle della Corte EDU. Sul primo fronte, viene espressamente richiamato il *Parere 1/15*, che il Governo tedesco ha citato a sostegno della tesi secondo cui una conservazione ingiustificata, quindi priva di una connessione con un reato, non possa per sé stessa essere considerata incompatibile con il diritto dell'UE. Il giudice del rinvio invece, con lucidità e mostrando una profonda conoscenza della materia, ha sottolineato come nel Parere riguardante la bozza di accordo di trasferimento di PNR dall'UE al Canada la CGUE abbia sì ammesso la legittimità dell'invio di dati indipendentemente dalla presenza di elementi oggettivi che stabiliscano un legame tra i passeggeri e un pericolo per la sicurezza pubblica canadese, ma abbia anche statuito come tale trattamento non costituisca una forma di conservazione ingiustificata. La memorizzazione dei codici di prenotazione, dunque di una specifica categoria di dati, è legata esclusivamente ai controlli effettuati alle frontiere e la conservazione di tali dati deve venir meno nel momento in cui il passeggero lascia il territorio canadese, a meno che non sussistano elementi oggettivi tali da dimostrare la presenza

[48] Con tale termine si intende evidenziare come la conservazione non sia del tutto definibile come generalizzata, poiché, come si è visto, alcune categorie di metadati vengono escluse dalla disciplina della *data retention*. Nonostante il fatto di non interessare tutti i dati di tutte le comunicazioni, la conservazione resta comunque priva di quegli elementi e criteri oggettivi che permettono, anche solo indirettamente, di collegare la conservazione dei metadati di un soggetto – o di un gruppo di soggetti – alla minaccia di reati gravi e pertanto non può essere considerata targettizzata.

di ulteriori rischi per la sicurezza. Ogni parallelismo tra tale Parere e la posizione espressa dalla Corte in materia di *data retention* viene quindi esclusa in ragione delle differenze sostanziali che connotano il trasferimento di PNR, pur per finalità securitarie: la stessa Corte tedesca non sembra dunque accogliere quelle riflessioni e critiche, analizzate nel Capitolo III, che vedevano nel *Parere 1/15* possibili conseguenze e incidenze anche rispetto alla disciplina della *data retention* 'interna' all'UE.

Quanto al secondo profilo indicato, quello cioè del richiamo alla giurisprudenza della Corte EDU, il giudice del rinvio pare suggerire di valutare con attenzione la corrispondenza della posizione espressa dalla CGUE con le più recenti pronunce dei giudici di Strasburgo che, in particolare nella sentenza *Centrum For Rattvisa*, sembrano ammettere la compatibilità con l'art. 8 della Convenzione EDU di forme di sorveglianza massiva relative però, è bene precisarlo subito, a metadati derivanti da comunicazioni transfrontaliere (*Signal Intelligence*) e non tra soggetti presenti unicamente nel territorio di uno Stato membro. Nonostante questa diversità, anche rilevante, dei dati e dei soggetti coinvolti dalle attività di sorveglianza, i giudici tedeschi evidenziano la discrezionalità più ampia lasciata dalla Corte EDU ai singoli Stati membri di porre in essere sistemi volti a combattere le grandi minacce che colpiscono ormai da tempo il contesto europeo, in primis il terrorismo internazionale. Sebbene ci si concentrerà su questi aspetti nel Capitolo V, pare rilevante notare come anche i giudici nazionali guardino sempre più spesso alla giurisprudenza della Corte EDU degli ultimi decenni relativa a sistemi di sorveglianza massiva, prestando attenzione anche alla concordanza o meno tra l'approccio delle due Corti europee in materia.

Anche il rinvio più recente promosso dalla Corte Suprema irlandese è incentrato sulla disciplina della conservazione e, ancora una volta, sui dubbi quanto alla incompatibilità, per sua stessa natura, di un regime generale o universale di conservazione dei metadati con il diritto dell'Unione anche quando (a) esso preveda rigorose limitazioni e salvaguardie sulla sicurezza dei dati e sulla fase di accesso; (b) la *data retention* sia finalizzata alla garanzia della sicurezza nazionale; (c) la conservazione sia indispensabile e strettamente necessaria al raggiungimento dell'obiettivo di lotta contro reati gravi. Il giudice irlandese inoltre pone, similmente a quanto già svolto dalla Corte costituzionale belga nel suo rinvio, la questione relativa agli effetti nel tempo di una dichiarazione di incompatibilità con il diritto dell'UE della normativa nazionale sulla conservazione dei dati e alla possibilità di limitarne le conseguenze laddove una mancata modulazione temporale sia tale da portare ad un serio disordine e ad un danno all'interesse pubblico. Proprio quest'ultimo aspetto è di estrema delicatezza per i giudici nazionali, anche in considerazione dello specifico caso concreto dal quale il rinvio origina: il signor Graham Dwyer, accusato dell'omicidio di una donna sulla base delle informazioni dedotte dai metadati telefonici conservati dalle compagnie di telecomunicazione, ha ritenuto inammissibili le prove addotte a suo carico ed ha promosso un procedimento civile nel quale ha contestato la legittimità della legge irlandese, il *Communications Data Retention Act* del 2011, adottata in attuazione della DRD. A seguito dell'accoglimento del ricorso da parte della High Court nel 2018, lo Stato ha impugnato tale decisione dinnanzi alla Supreme Court, che ha ritenuto fondamentale ottenere un chiarimento da parte della CGUE circa la corretta interpretazione dell'art. 15 Direttiva *e-Privacy*. Mentre Dwyer ha sostenuto l'incompatibilità con il diritto dell'UE di una forma di conservazione generalizzata, indipendentemente dalle garanzie previste nella fase di accesso, lo Stato irlandese invece ha affermato, come già altri Stati membri hanno fatto, la necessità di un approccio 'globale' di valutazione del regime giuridico sulla *data retention* e comunque sostenendo che qualsiasi decisione sulla validità e legittimità della normativa stessa debba avere valenza solo per il futuro, per evitare conseguenze disastrose e significative per le indagini e i processi penali in corso, così come per quelli già conclusi. Le incertezze su tale posizione e sulla giurisprudenza della CGUE hanno ancora una volta reso necessario ed imprescindibile l'intervento dei giudici di Lussemburgo.

Sebbene le questioni promosse siano del tutto simili a quelle oggetto dei previ rinvii pregiudiziali analizzati, la decisione della Corte Suprema irlandese assume grande rilievo per le affermazioni forti ed

estremamente concrete che sembra volgere alla CGUE: viene innanzitutto posta grande enfasi sui dati e sulle considerazioni riportate da alcuni esperti ascoltati dalla High Court, tra cui l'ex *UK Independent Reviewer of Terrorism Legislation*, da cui emerge l'importanza e l'utilità della conservazione generalizzata e dell'analisi dei metadati nella lotta alla criminalità grave e al terrorismo nonché l'insostituibilità, nella maggioranza dei casi, di questo strumento[49]. In questo contesto e sulla base di tali studi, non solo il c.d. sistema 'quick-freeze' ma anche la conservazione targettizzata vengono considerate inefficaci, scarsamente utili e potenzialmente discriminatori, mentre "l'obiettivo della conservazione dei dati con mezzi minori rispetto a quelli di un regime generale di conservazione dei dati, fatte salve le necessarie garanzie, è impraticabile e gli obiettivi di prevenzione, indagine, accertamento e perseguimento di reati gravi sarebbero notevolmente compromessi in assenza di un regime generale di conservazione"[50].

Da queste significative affermazioni, la Corte Suprema specifica due aspetti e valutazioni di estremo rilievo: innanzitutto, la sensazione di sorveglianza costante, di cui la CGUE ha parlato nelle sue pronunce sin dalla sentenza *DRI* quale conseguenza di forme di conservazione generalizzata, deve essere valutata in maniera diversa a seconda dello Stato membro: "the precise extent to which such matters may have such an effect on citizens may well vary from Member State to Member State, not least because of the different experiences within Member States of pervasive scrutiny on the part of police authorities" (par. 6.17); inoltre "significant regard would have to be attributed to the fact that many serious crimes against vulnerable people are most unlikely, on the undisputed evidence, to be capable of successful prosecution in the absence of a system of universal retention. In that context, I would consider that considerable weight must be attached to the undoubted rights of the victims of such crime, which rights will be impaired to a very significant degree indeed if it should prove impossible to detect or successfully prosecute the perpetrators of crimes against them. I would suggest that the rights of such persons need to be kept very much in mind in determining any appropriate balance" (par. 6.18)[51], evidenziando dunque l'importanza di considerare, nel bilanciamento tra diversi diritti e interessi, anche i diritti delle vittime di reati e non solo quelli della collettività che si troverebbe sottoposta a misure di *bulk data retention*.

Come ben si comprende dalla ricostruzione effettuata, le questioni toccate dai due più recenti rinvii richiamano quelle già affrontate dagli Avvocati generali Campos Sanchez-Bordona e Pitruzzella nella loro Conclusioni del gennaio 2020: ne consegue che alcuni degli interrogativi posti dai giudici irlandesi

[49] Viene riportata una analisi statistica elaborata dalla Germania, presentata alla Commissione europea nel 2013, secondo cui "in 44,5% of the cases involving requests for retained traffic data, there were no other means of conducting the investigation", par. 4.3 della sentenza n. 2019/18 della Supreme Court, nel caso *Graham Dwyer v. The Commissioner of An Garda Siochana, the Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General*, del 24 febbraio 2020. Al successivo par. 4.4. si legge come "the expert witnesses also gave evidence that they considered that there were no equally effective alternatives to a universal regime of data retention. The 'quick-freeze' system, under which preservation orders relating to particular individuals can be served on service providers after those individuals came under suspicion, would have limited efficacy in the context of the investigation of crime, as the majority of data regarding the suspect's conduct prior to their identification would be unavailable. (..) Further, this system would be of no utility in identifying persons who are unknown to law enforcement authorities at the time of the offence".

[50] Par. 8 della Sintesi della domanda di pronuncia pregiudiziale ai sensi dell'art. 98, par. 1, del Regolamento di procedura della CGUE, che riprende quanto affermato dalla Corte Suprema al par. 5.5 della pronuncia richiamata nella precedente nota.

[51] Merita infine sottolineare come, nel corso del procedimento, siano sorti anche dubbi quanto alla compatibilità della disciplina irlandese dell'accesso ai metadati rispetto al diritto dell'Unione e, in particolare, ai requisiti posti dalla giurisprudenza della CGUE, soprattutto con riferimento al criterio della indipendenza dell'autorità preposta al controllo preventivo. Su questo punto, sebbene il giudice irlandese stesso consideri la normativa, a suo giudizio, non conforme a quanto statuito nella sentenza *Tele2*, nondimeno viene ravvisata la necessità di rinviare alla CGUE la determinazione dei criteri da considerare per valutare se il regime di accesso ai metadati sia sufficientemente robusto e preveda un vaglio preventivo sufficientemente indipendente.

e tedeschi potrebbero già trovare risposta utile nelle sentenze della CGUE relative ai più risalenti rinvii; si pensi ad esempio alla possibilità di modulare nel tempo gli effetti delle dichiarazioni di incompatibilità di normative nazionali in materia di conservazione dei dati rispetto al diritto dell'UE, tematica già promossa nel rinvio della Corte costituzionale belga.

La posizione della Corte di giustizia su tutte queste cause comunque sarà certamente di grande rilievo e aiuterà a meglio chiarire la giurisprudenza precedente e a comprendere se e come le difficoltà applicative rilevate in tutti questi anni dalle autorità degli Stati membri porteranno ad una modulazione dei requisiti sanciti nella sentenza *Tele2* o se invece verranno mantenuti fermi i principi stabiliti, prevedendo però qualche possibile via interpretativa più flessibile, come la conservazione *limitata*, anziché *mirata*, promossa dall'Avvocato generale. Quel che senza dubbio emerge dall'esame sino ad ora svolto è come diversi giudici nazionali abbiano evidenziato, ed in parte condiviso, l'importanza di strumenti di conservazione generalizzata e le gravi conseguenze che potrebbero derivare da una esclusione definitiva e totale di tale forma di *data retention*. Dinnanzi a quesiti così specifici, che ribadiscono e rappresentano con lampante chiarezza la confusione o quantomeno la diversità di approcci ed interpretazioni possibili a seguito della pronuncia *Tele2*, pare che la Corte di giustizia non possa più esimersi dal prendere una netta e decisa posizione, che chiarisca in maniera definitiva una questione che ormai si protrae da più di un decennio e che necessita di trovare una risposta certa e univoca.

3. – L'assordante silenzio del legislatore europeo dopo la sentenza DRI e il rinnovato dibattito attuale

3.1. – La posizione espressa dal Consiglio e l'affidamento alla Commissione del compito di avviare iniziative e studi volti a determinare l'opportunità di una nuova normativa dell'UE in materia di data retention

La ricostruzione delle problematiche e delle sfide attuali riguardanti la disciplina europea in materia di *data retention* non potrebbe tuttavia dirsi completa senza una analisi del dibattito presente – o, come vedremo, per lo più assente – sul piano normativo. Sotto questo profilo, è del tutto evidente come, a seguito della sentenza *DRI*, il legislatore dell'UE non sia più intervenuto in alcun modo per reintrodurre un obbligo di conservazione dei dati per scopi securitari: il vuoto venutosi a creare dopo l'invalidazione della DRD non è mai stato colmato da un apposito atto e neppure la scarna e generica disposizione dell'art. 15 Direttiva *e-Privacy*, così discussa e al centro di tanti dubbi e perplessità interpretative, è mai stata in alcun modo modificata o integrata. Dinnanzi al forte attivismo della CGUE pare poi ancor più assordante il silenzio del legislatore dell'UE, che solo negli ultimi anni sta lentamente e faticosamente cercando di superare la lunga fase di immobilismo, riaprendo quantomeno un dibattito in materia.

Questo difficile tentativo di interrogarsi sui possibili sviluppi normativi e sulla necessità stessa di stabilire una disciplina a livello europeo sulla *data retention* e sull'accesso ai metadati per scopi securitari, ha ad oggi portato solamente ad una vaga presa di posizione del Consiglio nel documento *Conclusioni sulla conservazione dei dati per finalità di lotta contro la criminalità* (n. 9663/19) del 27 maggio 2019. Tale breve elaborato contiene una sorta di ricostruzione riassuntiva di tutti gli studi e le valutazioni svolte dal Consiglio in occasione di svariati incontri con diversi soggetti esperti del settore (da Europol alle autorità di *law enforcement* degli Stati membri), ponendosi così come punto finale – benché non risolutivo o determinante – di quel processo di riflessione avviato sin dall'aprile 2017, dopo l'ulteriore e significativo intervento dei giudici di Lussemburgo con la sentenza *Tele2*. All'esito di tale processo di riflessione viene con estrema chiarezza sottolineata, più volte, l'importanza di assicurare la "disponibilità dei dati per combattere efficacemente le gravi forme di criminalità, comprese il

terrorismo" (par. 5)[52]: del resto già nelle Conclusioni del 23 giugno 2017 e in quelle del 18 ottobre 2018, la direzione indicata dal Consiglio era quella di "adottare misure tese a fornire alle autorità di contrasto degli Stati membri e ad Europol risorse adeguate per far fronte alle nuove sfide derivanti dagli sviluppi tecnologici e dall'evoluzione del panorama delle minacce alla sicurezza" (par. 5). Sebbene venga affermata l'utilità di ricorrere ad imprescindibili obblighi di conservazione dei metadati derivanti da servizi di telecomunicazione, il Consiglio rileva anche la necessità di predisporre discipline che risultino proporzionate e trasparenti, in grado di offrire "garanzie sufficienti per i diritti fondamentali sanciti dalla Carta, in particolare i diritti alla riservatezza, alla protezione dei dati personali, alla non discriminazione e alla presunzione di innocenza" (par. 3), così come interpretati dalle sentenze *DRI* e *Tele2* della CGUE e così come verranno chiariti nei rinvii pregiudiziali pendenti che vengono espressamente richiamati dal Consiglio come meritevoli di grande attenzione.

Emerge quindi con forza dalle considerazioni e dalla fotografia fornita dal Consiglio la profonda conoscenza delle criticità e delle questioni ancora sospese legate alle zone grigie lasciate dal vigente assetto normativo e, in particolare, dall'art. 15 Direttiva *e-Privacy*, nonché la necessità di trovare una soluzione alla assenza di un regime di *data retention* a livello dell'UE e alla conseguente frammentarietà e disomogeneità delle discipline nazionali in materia. In questo contesto però il legislatore europeo dimostra anche di essere consapevole dell'estrema difficoltà di un intervento normativo di tale tipo: ciò richiederebbe infatti di trovare un punto di equilibrio tra spinte opposte, provenienti da un lato dai limiti fissati dalla giurisprudenza della Corte di giustizia sin qui esaminata e, dall'altro lato, dai Governi e dalle forze di *law enforcement* degli Stati membri che vorrebbero al contrario ampliare le maglie di azione in materia di conservazione dei dati a livello nazionale e garantire una disponibilità di informazioni ampia ed efficace. Anche la Commissione speciale sul terrorismo del Parlamento europeo ha rilevato come l'importanza "di un regime adeguato di conservazione dei dati sia stata costantemente sollevata durante i lavori della Commissione stessa. I relatori ritengono necessario prevedere un regime dell'UE in materia di conservazione dei dati che sia in linea con i requisiti derivanti dalla giurisprudenza della Corte di giustizia, tenendo conto nel contempo delle esigenze delle autorità competenti e delle specificità del settore della lotta al terrorismo" (par. 9). Condividendo tale veduta e ribadendo come non sia possibile rinunciare ad una disciplina sulla *data retention* tanto a livello nazionale quanto dell'UE, il Consiglio affida in conclusione alla Commissione il compito di avviare iniziative per raccogliere informazioni sulle esigenze della autorità interessate degli Stati membri, di procedere a consultazioni e di predisporre uno studio "approfondito sulle possibili soluzioni per conservare i dati, compresa la valutazione di una futura iniziativa legislativa", tenendo conto inoltre dell'evoluzione della giurisprudenza della Corte di giustizia.

È interessante notare come il Consiglio chiami la Commissione a valutare anche "i concetti di conservazione dei dati *generale, mirata e limitata* (interferenza di primo livello) e il concetto di accesso mirato ai dati conservati (interferenza di secondo livello), nonché ad esaminare in che misura l'effetto cumulativo di forti garanzie e possibili limitazioni a entrambi i livelli di interferenza possa contribuire ad attenuare l'impatto complessivo della conservazione dei dati sulla protezione dei diritti fondamentali sanciti dalla Carta, garantendo nel contempo l'efficacia delle indagini, in particolare quando si assicura che è consentito accedere solo a dati specifici necessari a una particolare indagine" (par. 2, Conclusioni, enfasi aggiunta). In questa indicazione viene fornita una possibile lettura della giurisprudenza della CGUE, peraltro per certi versi simile a quella suggerita da alcune Corti nazionali nei rinvii pregiudiziali pendenti promossi e dall'Avvocato generale Campos Sanchez-Bordona nelle Conclusioni sopra esaminate. Innanzitutto il Consiglio pare proporre una forma di valutazione 'cumulativa' delle garanzie previste sia per quanto attiene alla disciplina della *data retention* che per quella dell'accesso: questa

[52] Tale scopo è peraltro inteso come "obiettivo di interesse generale finalizzato a mantenere la sicurezza pubblica e provvedere alla sicurezza delle persone quale presupposto per garantire i diritti fondamentali", par. 3.

lettura unitaria potrebbe rappresentare una strada utile per giungere a legittimare anche forme di conservazione di carattere non necessariamente targettizzato. Inoltre, rilevante e tutt'altro che casuale è il richiamo a tre diverse tipologie di conservazione: generale, mirata e limitata (ovvero *general*, *targeted* e *restricted* nella versione inglese). Mentre la distinzione tra generalizzata e targettizzata era stata individuata dalla giurisprudenza della CGUE stessa, la conservazione 'limitata' è una tipologia coniata da Europol: nel documento, solo in parte pubblicamente accessibile, WK 9957/2017 del 21 settembre 2017 dal titolo "Proportionate data retention for law enforcement purposes", emerge come la *data retention* non debba diventare uno strumento eccezionale rispetto al divieto di conservazione quanto piuttosto debba puntare ad avere natura proporzionata: sotto tale profilo, "not only targeted data retention, but also restricted data retention is compliant with the Charter according to *DRI* and *Tele2*". La conservazione limitata (o *restricted*) così identificata è basata solo su dati assolutamente ed oggettivamente necessari per la salvaguardia della sicurezza ed è inoltre ristretta a certi tipi di *providers* e di servizi individuati sulla base di un "link" cioè di una connessione tra conservazione dei dati e obiettivo da raggiungere. Mentre una forma di *data retention* targettizzata, ovvero limitata a specifici periodi di tempo, luoghi e gruppi di persone, come indicato dalla CGUE, difficilmente riuscirebbe a rispondere ai bisogni concreti delle autorità di *law enforcement*, pur essendo certamente meno intrusiva di una *restricted data retention*, quest'ultima, sebbene più invasiva, risulterebbe, a parere di Europol, maggiormente efficace e al contempo limitata a quanto necessario e, per quanto possibile, fondata su esigenze concrete e precise di repressione della criminalità e pertanto conforme alla Carta di Nizza e alle indicazioni della giurisprudenza europea[53]. Ad esempio, rispetto ad una conservazione generalizzata, una *restricted data retention* escluderebbe dalla conservazione i piccoli fornitori di servizi internet così come i metadati di soggetti le cui attività sono coperte da segreto professionale. In questo senso, "the initial retention of data has to be restricted in order to be compliant with the Charter. Such restriction can be achieved through exclusion of data not even potentially relevant. To compensate the strong interference as regards retention, the data access must be strictly targeted" (p. 20). Ciò che Europol in conclusione ha proposto è una lettura della giurisprudenza della CGUE[54] nel senso di non rifiutare totalmente qualsiasi forma di *data retention* che non sia targettizzata, escludendo da un lato forme di conservazione generalizzata "pura", ma consentendo dall'altro forme di conservazione più ampie di quella *targeted*, cui siano però applicate apposite limitazioni e che siano fatte seguire da un accesso targettizzato, rispondente a tutti i criteri indicati nella sentenza *Tele2*[55].

Tale idea di conservazione *limitata* tuttavia ha trovato la ferma opposizione e critica di numerose ONG attive nell'ambito della tutela dei dati e della riservatezza, che hanno individuato in questa

[53] Sul punto si può leggere P. VOGIATZOGLOU, *Data Retention tales: the Council of the EU strikes back*, in *CiTiP Law Blog*, luglio 2019.

[54] Interessante notare come Europol parli di "forgotten part of *DRI*" riferendosi alla parte di tale storica pronuncia nella quale viene riconosciuto come obiettivo di interesse generale la lotta al terrorismo internazionale per mantenere la pace e la sicurezza, nonché il richiamo all'art. 6 della Carta di Nizza che riconosce espressamente il diritto di ogni soggetto non solo alla libertà ma anche alla sicurezza. Secondo Europol dunque non può essere dimenticata una parte così rilevante, che pur viene riconosciuta dalla CGUE e che deve essere tenuta in debita considerazione dalle Istituzioni europee e nazionali.

[55] Anche nel documento del Consiglio n. 14319/18 del 23 novembre 2018, titolato "Conservazione dei dati. Stato dei lavori", viene ribadita la lettura della giurisprudenza europea presentata nella relazione di Europol. Vengono inoltre forniti alcuni suggerimenti su come interpretare i criteri che determinano la natura 'limitata' della conservazione dei dati con riferimento alle categorie di dati, ai periodi di conservazione, alla limitazione territoriale all'interno dell'UE, alla necessità di ricorrere a modalità cifrate o pseudonimizzazione nonché alla cancellazione dei dati alla fine del periodo di conservazione. Il confronto con gli Stati membri e l'analisi delle soluzioni normative da essi adottati nonché le possibilità di concrete di giungere a tali limitazioni senza compromettere l'efficacia ed utilità dello strumento, traggono origine dalla interpretazione della sentenza *Tele2* secondo cui una conservazione è limitata allo stretto necessario – e dunque non generalizzata ed indifferenziata – laddove risulti ristretta sotto il profilo delle categorie di dati, dei mezzi di comunicazione interessati, delle persone i cui dati sono soggetti a conservazione e alla durata della stessa.

soluzione una lettura erronea della giurisprudenza della Corte di giustizia: una *data retention* quale quella proposta da Europol e sostenuta dai Governi degli Stati membri nonché dalle autorità di *law enforcement*, infatti, risulterebbe comunque coprire la quasi totalità della popolazione e si troverebbe dunque in contrasto con quella che è stata individuata invece dai giudici di Lussemburgo come unica forma legittima di conservazione dei metadati, ovvero quella targettizzata. Secondo il ragionamento di Europol, la legittimità di una *restricted data retention* farebbe leva sul par. 112 della sentenza *Tele2*: quando i giudici parlano di conservazione generalizzata e indifferenziata si riferiscono a quelle tipologie di conservazione che riguardano contemporaneamente tutti i dati relativi al traffico e i dati relativi all'ubicazione, riferiti a tutti gli abbonati e utenti iscritti riguardanti tutti i mezzi di comunicazione elettronica; ebbene laddove la *data retention* fosse limitata a specifiche categorie di dati o particolari mezzi di comunicazione o categorie di utenti, ciò basterebbe a ritenere una conservazione siffatta come non generalizzata ma limitata e quindi legittima. La ONG EDRI, tuttavia, ha sottolineato come l'enunciato richiamato non possa intendersi come legittimante una forma di conservazione, quale quella proposta da Europol, che sarebbe comunque estremamente ampia e peraltro contraria a quanto più volte affermato dalla CGUE, non solo in *DRI* e *Tele2* ma anche in *Schrems* e nel *Parere 1/15* in materia di PNR: in tutte le pronunce richiamate, infatti, viene costantemente ribadita la necessaria sussistenza di un criterio oggettivo che metta in rapporto i dati da conservare con l'obiettivo perseguito. Per questo l'opzione di una *restricted data retention* non viene ritenuta dalle ONG richiamate una soluzione percorribile e conforme ai parametri indicati nella giurisprudenza europea[56].

Come si è visto nel previo paragrafo, l'Avvocato generale Campos Sanchez-Bordona ha espressamente fatto riferimento a questa posizione del Consiglio e di Europol nelle proprie Conclusioni, proponendo e quindi avvallando questa lettura come legittima soluzione di compromesso tra le diverse esigenze in gioco. Bisognerà pertanto prestare grande attenzione agli sviluppi dei rinvii analizzati per osservare se la CGUE accoglierà la visione proposta. Contemporaneamente sarà interessante e di fondamentale importanza verificare se tali stesse indicazioni del Consiglio saranno o meno seguite nella elaborazione e studio di una possibile normativa europea in materia da parte della Commissione. A quest'ultima spetterà più in generale il compito di valutare se sia opportuno e necessario elaborare un nuovo testo normativo *ad hoc* o una modifica dell'assetto legislativo vigente che sappia considerare e conciliare sia le esigenze espresse da Europol e da molti degli Stati membri coinvolti nelle varie occasioni di confronto e indagine, sia i principi e criteri individuati dalla Corte di giustizia.

Sino ad ora, la Commissione ha avviato vari incontri con ONG e rappresentanti della società civile, autorità – europea e nazionale – garanti della protezione dei dati, Stati membri e agenzie europee operative nell'ambito sia della tutela dei diritti fondamentali che della sicurezza pubblica. Sebbene a margine dell'incontro tenutosi il 6 giugno 2019, la Commissione, come riportato dalla partecipante EDRI, abbia affermato che non ci sono "clear next stages in the process", pare comunque particolarmente utile, al fine comprendere la direzione degli studi e delle valutazioni promosse dalla Commissione stessa, il questionario indirizzato dalla DG Home ai partecipanti dell'incontro citato[57]. In tale documento infatti vengono poste alcune rilevanti questioni, a partire dalla determinazione dell'impatto sui diritti fondamentali degli individui provocato da normative esistenti in materia di *data retention*, chiedendo anche la disponibilità di studi analitici e documentati sulle implicazioni per gli individui, sul volume di dati conservati dai diversi Stati membri ma anche sull'efficacia e sull'utilità

[56] Sul punto, si legga EDRI, *EU Member States plan to ignore EU Court data retention rulings*, 2017 e EDRI, *EU Member States willing to retain illegal data retention*, 2019, disponibili agli indirizzi: https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/ e https://edri.org/eu-member-states-willing-to-retain-illegal-data-retention/ .

[57] Tali dichiarazioni e il documento richiamato sono reperibili all'indirizzo: https://edri.org/data-retention-eu-commission-inconclusive-about-potential-new-legislation/ .

concreta della disponibilità di dati e sui risultati di tale pratica rispetto alla lotta alla criminalità[58]. Particolare attenzione è poi dedicata alla comprensione di come un regime di conservazione dei metadati possa essere compatibile con il rispetto dei diritti fondamentali, domandando quali siano i rischi di una *targeted retention*, in particolare con riferimento al diritto alla non discriminazione, e come i "targeting criteria" dovrebbero essere determinati; ma anche chiedendo quali criteri debbano essere posti alla base della individuazione di una legittima e corretta durata di conservazione, delle autorità autorizzate all'accesso ai dati, degli obiettivi e scopi che consentono l'accesso, delle salvaguardie da porre in essere per minimizzare i rischi di *data breaches*, ponendo in rilievo le procedure di autorizzazione *ex ante*, la notifica ai soggetti interessati, i rimedi e la supervisione *ex post*. Infine la Commissione chiede – e si chiede, ritenendo dunque fondamentale la comprensione e definizione di tale aspetto – se "are there any alternatives to data retention that could be equally effective in fighting crime and be more respectful of fundamental rights?" (pag. 2). Come ben emerge da tali numerosi e articolati quesiti, la complessità dei punti ancora da definire e chiarire, molti dei quali sono già stati ampiamenti posti all'attenzione della Corte di giustizia, rappresenta una enorme sfida per il legislatore europeo che si trova ora a dover comprendere se e come intervenire in una materia tanto delicata e che impone la considerazione di molteplici interessi e diritti.

3.2. – La proposta di un nuovo Regolamento che sostituisca la Direttiva e-Privacy*: una occasione da cogliere?*

Oltre all'intervento e alla valutazione assegnata alla Commissione da parte del Consiglio, una ulteriore soluzione che possa andare nella direzione di stabilire una disciplina in materia di *data retention* più chiara ed aggiornata, capace di tener conto di tutti i rilievi giurisprudenziali intervenuti e del dibattito politico-istituzionale sviluppatosi a livello dell'UE e nazionale, è stata rinvenuta da Europol nella proposta di *Regolamento relativo al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche* (COM(2017)0010) del 10 gennaio 2017); con riferimento ad essa, infatti, Europol afferma: "there is an essential need to incorporate data retention rules for law enforcement purposes into the upcoming ePrivacy Regulation". Tale proposta, al momento ancora al vaglio del legislatore dell'UE, andrebbe ad abrogare la Direttiva 2002/58/CE e dunque anche il tanto controverso e confuso art. 15: per tale motivo, questo Regolamento ben potrebbe rappresentare la giusta occasione per prendere posizione sul tema della conservazione e accesso ai metadati per scopi securitari e fornire una disciplina omogenea in tutto il territorio europeo, in modo da definire più chiaramente quel tanto auspicato e complesso bilanciamento tra esigenze securitarie e criteri definiti nella giurisprudenza europea.

Nonostante la scelta dello strumento normativo sia certamente significativa, ricadendo cioè su di un regolamento e non più su di una Direttiva, optando quindi per un atto direttamente applicabile negli Stati membri e limitativo della discrezionalità dei legislatori nazionali[59], è da sottolineare come il testo nella

[58] Ad esempio: "Are there any analyses regarding the investigative or judicial outcome of using the data? Are there any evaluations, reports, statistics or studies on the subject available? What are the cross-border implications of data retention laws? Would an EU-wide data retention regime bring any added value?".

[59] La proposta di Regolamento inoltre presenta grandi innovazioni e mira ad ammodernare il testo del 2002 e a renderlo maggiormente rispondente alle nuove sfide di mercato ed in ambito privatistico che l'avanzamento tecnologico nel campo delle comunicazioni elettroniche ha portato con sé. Lo scopo è quello di predisporre un nuovo assetto normativo efficiente, in grado di favorire il progresso nel settore imprenditoriale, regolando il flusso ed il trasferimento di dati, nel rispetto di determinati standard di riservatezza, estesi, come nella normativa attualmente in vigore, non solo ai contenuti ma anche ai metadati prodotti dalla comunicazione. Molte sono le novità che questo Regolamento vorrebbe introdurre: prima fra tutti l'estensione dell'applicazione delle regole sulla *e-privacy* anche ai nuovi operatori delle telecomunicazioni, i cosiddetti *Over The Top* (OTT) quali Google, Facebook, Whatsapp. La significativa rilevanza e i sostanziali mutamenti proposti hanno creato un forte dibattito

sua ultima versione resa disponibile dal Consiglio nel febbraio 2020[60] contenga solo generiche disposizioni in materia di *data retention*: queste non solo non contribuirebbero a chiarire i limiti di tale strumento, ma anzi le condizioni in esse disposte verrebbero delineate in maniera molto ampia e ancora potenzialmente foriera di diverse interpretazioni ed applicazioni.

Prima di giungere all'analisi di tali previsioni nella loro più recente forma (per quanto ancora non definitiva), merita però sottolineare il mutamento e l'evoluzione che hanno interessato nel corso del tempo la normativa proposta: nella versione iniziale infatti il regolamento avrebbe dovuto mantenere "l'essenza dell'articolo 15 della Direttiva sulla vita privata elettronica, allineandosi con il testo specifico dell'articolo 23 del GDPR, che disciplina i motivi per i quali gli Stati membri possono restringere l'ambito di applicazione dei diritti e degli obblighi in articoli specifici della Direttiva sulla vita privata elettronica. Gli Stati membri sono pertanto liberi di mantenere o creare quadri di riferimento nazionali in materia di conservazione dei dati che prevedano fra l'altro misure di conservazione mirate, purché essi siano conformi al diritto dell'Unione e tengano conto della giurisprudenza della Corte di giustizia sull'interpretazione della Direttiva sulla vita privata elettronica e della Carta dei diritti fondamentali" (par. 1.3)[61]. Ecco quindi che, mentre l'art. 5 del proposto Regolamento, nella sua prima stesura, prevedeva quale regola generale il divieto di conservazione dei dati delle comunicazioni elettroniche e dunque l'obbligo di cancellazione da parte del fornitore del servizio di comunicazione del contenuto delle comunicazioni e dei metadati quando non più necessari per trasmettere la comunicazione stessa, l'art. 11 stabiliva alcune possibili eccezioni tra cui appunto la possibilità da parte dell'Unione o di uno Stato membro di limitare, mediante una normativa, gli obblighi di cui agli artt. 5-8, qualora "siffatta limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e costituisca una misura necessaria, appropriata e proporzionata in una società democratica intesa a salvaguardare uno o più interessi pubblici ai sensi dell'art. 23, par. 1, lettere da a) a e) del Reg. (UE) 2016/679". Il richiamo a tale ultimo Regolamento, meglio noto come GDPR, rimanda alla disposizione dell'art. 23 che consente l'adozione di limitazioni rispetto ad alcuni obblighi e diritti previsti dalla normativa stessa (negli artt. 5, 34 e da 12 a 22, quali i diritti sull'informazione e comunicazione agli interessati, il diritto d'accesso, di rettifica, di cancellazione, di limitazione del trattamento, alla portabilità dei dati, di opposizione) laddove tali eccezioni rispettino comunque l'essenza dei diritti e delle libertà fondamentali e risultino necessarie e proporzionate in una società democratica per salvaguardare, secondo quanto richiamato dall'art. 11

---

in seno al Consiglio, tanto che quest'ultimo si è dovuto arrendere alla impossibilità di addivenire ad un testo definitivo entro maggio 2018: il termine della procedura di predisposizione ed approvazione di questo importante tassello normativo era stato infatti originariamente, e molto ambiziosamente, pensato per coincidere con l'inizio dell'applicazione del pacchetto di riforme in materia di trattamento e protezione dei dati. La volontà del legislatore europeo era quella di allineare le normative in materia e garantire, con una più o meno simultanea applicazione, un complesso di regole completo ed integrato, capace di far fronte a quelle criticità riscontrate a partire dal nuovo millennio. La proposta di Regolamento invece è ancora oggi in fase di vaglio. Per approfondimenti, si legga: G. BUTTARELLI, *The Commission proposal for a Regulation on e-Privacy: why do we need a Regulation dedicated to e-Privacy in the European Union*, in *European Data Protection Law Review*, 3, 2017.

[60] *Proposal for a Regulation of the EP and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC*, n. 5979/20, 21 febbraio 2020. Altro documento (n. 6543/20 del 6 marzo 2020) che riporta alcune modifiche al testo della proposta non rileva ai fini di questa indagine poiché non comporta interventi rispetto alla disciplina della *data retention* mentre l'esito delle ultime discussioni sulla proposta effettuate dal Consiglio non sono al momento pubblicamente disponibili (il doc. 8204/20 del 3 giugno 2020 è infatti riservato).

[61] "Laddove il trattamento dei dati delle comunicazioni elettroniche da parte dei fornitori di servizi di comunicazione elettronica rientra nell'ambito di applicazione del presente regolamento, questo dovrebbe prevedere la possibilità che l'Unione o gli Stati membri, a determinate condizioni, possano limitare i diritti e gli obblighi, qualora tale restrizione costituisca una misura necessaria e proporzionata all'interno di una società democratica per la salvaguardia di specifici interessi pubblici, compresa la sicurezza nazionale, la difesa, la sicurezza pubblica nonché la prevenzione, la ricerca, l'accertamento o il perseguimento dei reati o l'esecuzione di sanzioni penali, compresa la salvaguardia e la prevenzione delle minacce alla sicurezza pubblica e ad altri obiettivi di rilievo di interesse pubblico generale dell'Unione o di uno Stato membro", Considerando 26.

GDPR e dunque per quanto in questa sede interessa: a) la sicurezza nazionale, b) la difesa, c) la sicurezza pubblica, d) la prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica, e) altri importanti obiettivi di interesse pubblico generale dell'Unione o di uno Stato membro, in particolare un rilevante interesse economico o finanziario dell'Unione o di uno Stato membro, anche in materia monetaria, di bilancio e tributaria, di sanità pubblica e sicurezza sociale.

Le proposte intervenute nel corso del dibattito sulla bozza del Regolamento svoltosi in seno al Consiglio sono state ampie ed hanno interessato anche il citato art. 11. Come dichiarato dal Consiglio stesso nel *Progress Report* pubblicato il 27 novembre 2019 (n. 14447/19), "while the issue of data retention is primarily discussed in another formation (Friends of Presidency on Data Retention under the Justice and Home Affairs Council) delegations consistently underlined the need to ensure that the approach taken in the ePrivacy Regulation does not negatively impact on any potential solution that may eventually be found on data retention. Since many delegations believed that relying only on the mechanism under article 11 would not be sufficient, the Presidency introduced modifications to that effect also in the related provisions (articles 2, 6 and 7)". Ecco dunque che mentre prima l'art. 6 sul trattamento consentito dei dati delle comunicazioni elettroniche non stabiliva direttamente la possibilità di conservazione dei metadati per finalità securitarie, ora invece ne contiene un espresso riferimento: "providers of electronic communications networks and services shall be permitted to process electronic communications data only if: (..) lett. d) it is necessary for compliance with a legal obligation to which the provider is subject laid down by Union or Member State law, which respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security" (art. 6, co. 1). L'art. 7 poi si occupa della conservazione e cancellazione dei metadati, riconfermando l'obbligo di cancellazione o anonimizzazione da parte dei fornitori di servizi, qualora tali dati non siano più necessari per il trattamento di cui all'art. 6, co. 1, tra cui dunque anche per gli analizzati scopi securitari. Il comma 4 del medesimo articolo prevede inoltre che "Union or Member state law may provide that the electronic communications metadata is retained to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period that is no longer than the period set out in this Article". Le modifiche promosse vanno dunque nella direzione di ricalcare l'esistente art. 15 della Direttiva *e-Privacy*, richiamando generici rinvii all'art. 23 GDPR, nonché a concetti ampi quali proporzionalità e necessità. Anche le finalità che legittimano la conservazione restano ampie: nelle parole scelte nelle ultime versioni, si parla addirittura di 'criminal offences', mantenendo quindi quella criticata mancanza di specificazione riguardo alla natura dei crimini che, dalla giurisprudenza della CGUE e solo da essa, viene individuata come 'criminalità grave'. Non paiono pertanto essere stati presi in considerazione con attenzione ed integrati nel testo normativo quei requisiti tanto discussi emersi dalle sentenze sino ad ora esaminate e che non hanno ottenuto alcun chiarimento o specificazione nel testo normativo proposto. Per questo motivo, sebbene con riferimento alla originaria versione inizialmente avanzata, alcuni autori non hanno mancato di muovere critiche al legislatore: "Non ci appare che questa formula di salvaguardia sia efficace quanto potrebbe essere l'adozione di un atto di armonizzazione delle legislazioni nazionali che fissi il periodo massimo ammissibile di conservazione dei dati, le procedure di accesso delle autorità pubbliche, le garanzie di controllo, ecc. È evidente che se il legislatore europeo si limitasse alla semplice indicazione dei criteri in parola segnerebbe un regresso nella tutela sostanziale dei diritti fondamentali. Soprattutto ci sembra che la scelta del legislatore dell'Unione di non sostituire la Direttiva *data retention* manifesti la volontà

degli Stati membri di ridurre il preteso 'attivismo giudiziario' della Corte di giustizia"[62]. Anche la già richiamata EDRI, insieme ad altre ONG, ha manifestato timore e preoccupazione rispetto alla proposta attualmente al vaglio del Consiglio, rinvenendo in essa quelle ampie maglie di discrezionalità lasciate ai legislatori nazionali che potrebbero portare la *data retention*, "fatta uscire dalla porta" da parte dei giudici di Lussemburgo, a "rientrare dalla finestra", vanificando o comunque limitando l'apporto fondamentale alla tutela dei diritti garantito negli ultimi decenni dalla giurisprudenza europea.

Se certamente bisognerà attendere le sopra analizzate valutazioni della Commissione, chiamata a considerare anche l'opportunità di un intervento *ad hoc* in materia che possa riempire il vuoto normativo lasciato dalla Direttiva 2006/24/CE[63], pare certa la mancata volontà – al momento – del Consiglio, forse risentendo anche della posizione di forte resistenza mostrata dai Governi nazionali, di fissare nel Regolamento proposto più rigide e precise condizioni valide per le normative in materia di conservazione dei metadati per finalità securitarie. Questo anche a causa della complessità della materia e dei fortissimi impatti che essa presenta sulle competenze degli Stati membri in materia penale: non è un caso che nel *Progress Report*, sopra richiamato, il Consiglio abbia riconosciuto la *data retention* come uno dei punti maggiormente problematici della proposta, rispetto al quale è particolarmente difficile trovare una soluzione di compromesso. Tale materia quindi sta contribuendo, insieme ad altri aspetti delicati – tra cui la capacità di tale Regolamento di disicplinare e rispondere alle esigenze poste da nuove tecnologie quali l'*Internet of Things* o le *machine-to-machine communications*, e ancora la determinazione del ruolo del Comitato europeo per la protezione dei dati –, a rallentare l'approvazione del testo finale del Regolamento.

Nel frattempo, l'assenza reiterata di una armonizzazione delle normative nazionali in materia di *data retention* comporta inevitabilmente il perdurare di un panorama frammentario all'interno dell'Unione, che continua e continuerà a dare adito a diverse interpretazioni ed attuazioni nonché a dubbi di conformità e rispetto dei diritti fondamentali, portando dunque all'intervento di giudici nazionali e, come si è visto, in sempre più casi, ad un rinvio alla Corte di giustizia dell'UE. Come già avvenuto in passato, i criteri e principi indicati da quest'ultima saranno poi, a loro volta, recepiti e inclusi negli ordinamenti nazionali in maniera differente, alimentando un circolo vizioso di interventi continui da parte di attori diversi. Se si concorda con chi sostiene che "forse proprio l'inerzia del legislatore e la constatata obsolescenza della normativa in vigore hanno indotto la Corte di Giustizia a compiere sforzi ulteriori, valorizzando il patrimonio della Carta"[64], neppure nella posizione attuale del legislatore europeo sembra possibile intravedere un mutamento in tempi rapidi di questa complessa situazione sul fronte legislativo.

---

[62] G. CAGGIANO, Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione, in MediaLaws, 2, 2018, p. 16.

[63] La *Digital Rights Ireland* era stata vista da alcuni autori come una grande occasione per il legislatore sovranazionale di riordinare la controversa materia della *data retention* e dell'accesso dei metadati relativi alle comunicazioni elettroniche, raccolti e usati per finalità di sicurezza. Per questo era stato auspicato un nuovo intervento normativo sovranazionale che armonizzasse le misure nazionali in questo ambito, seguendo i parametri indicati dalla CGUE: "an EU instrument that harmonizes *data retention* regimes and thus indirectly ensures comparable data protection standards within the region would be the most appropriate solution to balance potentially conflicting interest: enhancing security and safeguarding data privacy rights", F. GALLI, *Digital Rights Ireland as on opportunity to foster a desirable approximation of data retention provisions,* in *Maastricht Journal of European and Comparative Law*, 3, 2016. Questo auspicio è stato sinora disatteso e pare continuerà ad esserlo.

[64] M. BASSINI, *La Corte di giustizia e la conservazione dei dati. Spunti di una rilettura 'postuma'*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, in corso di pubblicazione.

4. – Uno sguardo alle sfide per il futuro: un provvisorio bilancio della 'data retention saga' e dei giudizi ad oggi pendenti

L'analisi svolta nei paragrafi precedenti, che fotografa la situazione attuale sia sotto il profilo giurisprudenziale, dei numerosi rinvii pregiudiziali pendenti dinnanzi alla CGUE, che sotto quello legislativo, con le varie proposte sul tavolo delle diverse istituzioni europee, aiuta a comprendere la complessità delle numerose sfide che dovranno essere affrontate in futuro. Le scelte del legislatore sovranazionale e quelle dei giudici di Lussemburgo saranno certamente decisive per chiarire i limiti e l'applicabilità dei requisiti sanciti dalla giurisprudenza europea e che da lungo tempo cercano una definizione. "I regret to say that the task now facing this Court [in questo caso la High Court] is far from easy in view of the fact that the preliminary ruling from the CJEU is lacking in clarity": queste sono le parole utilizzate dal giudice inglese Lord Lloyd-Jones all'indomani della sentenza *Tele2*[65]; e se si pensa che questa affermazione risulta ancora del tutto attuale nonostante siano trascorsi ormai quattro anni dalla storica pronuncia della CGUE, ciò basta per far riflettere su quanto i dubbi e le criticità applicative, evidenziate in questo Capitolo e nei Capitoli precedenti, fatichino ancora a trovare una risposta finale.

Dinnanzi a tale quadro, si possono appieno comprendere i continui richiami di numerose ONG, molte delle quali sono state protagoniste attive dei rinvii pregiudiziali attualmente pendenti, che da un lato premono affinché le Istituzioni europee proseguano un dibattito sempre più rapido ed inclusivo circa la necessità di una nuova e chiara disciplina normativa a livello dell'UE in materia di *data retention*, e dall'altro spronano la Commissione ad assumere una posizione decisa avverso gli Stati membri che ancora mantengono legislazioni nazionali in evidente contrasto con i requisiti e principi delineati dalla giurisprudenza della CGUE, suggerendo anche l'opportunità di avviare procedure di infrazione. Le spinte in queste due direzioni si uniscono poi all'esigenza di maggiore trasparenza volta a consentire ai cittadini tutti di avere accesso a studi e documenti preparatori dei lavori delle Istituzioni europee, soprattutto del Consiglio, favorendo chiarezza e un proficuo scambio di dati e informazioni; proprio su quest'ultimo punto vi è la richiesta sempre maggiore di analisi ampie, capaci di comprendere il panorama normativo di tutti gli Stati membri dell'UE e di tratteggiare le caratteristiche fondamentali delle legislazioni interne e delle soluzioni adottate nell'ambito della disciplina della conservazione e accesso ai metadati per scopi securitari, che permettano di vagliare, in ultima istanza, lo stato dell'arte e il livello di concreta attuazione e applicazione dei criteri indicati nella *Tele2* e di come essi abbiano, nelle diverse realtà statuali, influito sulle scelte legislative e giurisprudenziali nazionali. Sul piano sostanziale poi le maggiori critiche mosse dalla società civile e dalle ONG attive nell'ambito della tutela dei diritti fondamentali alla privacy e protezione dei dati sono quelle che individuano nelle più recenti esternazioni del Consiglio e di Europol, così come nella prassi di molti Stati membri, la volontà forte di non abbandonare lo strumento della conservazione generalizzata ed indiscriminata, peraltro senza fornire prove e dimostrazioni attendibili e provenienti da fonti indipendenti circa la necessità, utilità ed efficacia di tale strumento[66].

Su questa linea si inseriscono anche le domande ed interrogazioni poste in seno al Parlamento europeo e che, similmente a quanto evidenziato dalle ONG e dalla società civile, mirano a chiedere un intervento più chiaro e deciso da parte della Commissione: si fa riferimento alla interrogazione E-000389/2020 del 23 gennaio 2020, con la quale viene evidenziato come, mentre le Conclusioni dell'Avvocato generale Campos Sanchez-Bordona nei rinvii pendenti sopra analizzati hanno mostrato come le normative di Francia, Belgio e Regno Unito, prevedendo una *bulk data retention*, non possano

[65] *Secretary of State for the Home Department c. Watson et al.*, 2018, EWCA Civ 70, par. 7.

[66] Si legga in questo senso la lettera, firmata da numerose ONG, tra cui le note EDRI, Digital Rights Ireland, La Quadrature di Net e Privacy International, che è stata inviata il 22 luglio 2019 alla Presidente della Commissione europea Von der Leyen, reperibile all'indirizzo https://edri.org/files/Dataretention/20190719-DR_letter_EC_edri.pdf

essere considerate compatibili con il diritto dell'Unione e con i principi sanciti dalla giurisprudenza europea, la Commissione non sia mai intervenuta avverso gli Stati membri che hanno erroneamente interpretato e trasposto l'art. 15 della Direttiva *e-Privacy*[67]. A tali quesiti, così diretti e volti ad ingenerare una reazione forte della Commissione, la risposta di quest'ultima è stata poco incisiva: "The Commission is monitoring developments at the Court of Justice of the EU on a number of legal frameworks and will assess the need for further action once the judgments in the relevant pending cases are delivered"[68].

Per una presa di posizione a livello dell'UE quindi pare necessario attendere sia gli esiti dei rinvii pregiudiziali pendenti che i possibili sviluppi sul fronte legislativo. La situazione risulta pertanto essere ancora del tutto in divenire e in attesa di una determinazione nei suoi punti fondamentali: i prossimi passi saranno decisivi per comprendere il destino, nell'Unione europea, della *data retention* come strumento di lotta alla criminalità.

In questo contesto, di grande rilievo sarà certamente la posizione che la Corte di giustizia vorrà tenere, chiarendo e confermando il precedente approccio, eliminando le zone grigie e i dubbi applicativi oppure proponendo una lettura attenuata dei principi stabiliti, conformemente alle richieste degli Stati membri, delle autorità di *law enforcement* e di talune autorità a livello europeo stesso (Europol ad esempio). Ma altrettanto determinante sarà l'applicazione ed attuazione concreta, sia nel contesto nazionale che in quello europeo, di quanto i giudici di Lussemburgo affermeranno; ciò per evitare che, successivamente alle attese pronunce della CGUE nelle sei cause pendenti, il silenzio delle Istituzioni dell'Unione e l'immobilismo degli Stati membri portino *de facto* al riproporsi della situazione attuale, nella quale le perplessità sorte all'indomani della sentenza *Tele2* hanno creato un forte stallo – dovuto in parte anche alla resistenza opposta da talune autorità statali – che ha visto, in taluni casi, come unica via d'uscita per sbloccare l'incertezza attuativa quella di promuovere rinvii pregiudiziali e dunque richiedere un intervento chiarificatore della Corte di giustizia.

I pericoli di una mancata applicazione concreta di quanto indicato dalla CGUE sono emersi con evidenza nella frammentarietà delle reazioni dei diversi Stati membri ma anche delle Istituzioni europee stesse a seguito della pronuncia *Tele2*: è del resto indicativo il fatto che il Consiglio, nel più recente documento, sopra analizzato, sulle Conclusioni in materia di *data retention*, non abbia seguito pedissequamente le indicazioni fornite dai giudici di Lussemburgo sulla conservazione targettizzata o mirata, bensì abbia promosso la posizione suggerita da Europol attinente ad una forma *limitata* di conservazione; una sorta di soluzione di compromesso, che, come si è sottolineato, è stata anche abbracciata dall'Avvocato generale Campos Sanchez-Bordona nelle Conclusioni ai rinvii di Belgio, Francia e Regno Unito: pur mantenendo fermo il divieto di una *bulk data retention* nonché confermando le strette condizioni attinenti all'accesso, viene proposto di non considerare la conservazione mirata come unica soluzione legittima e compatibile con il diritto dell'Unione europea. Questa possibile lettura, che imporrebbe comunque seri e drastici mutamenti nell'assetto normativo vigente in molti – se non tutti – Stati membri che ancora attuano forme di conservazione generalizzata, potrebbe purtuttavia essere maggiormente accettata e forse più facilmente applicata nel contesto nazionale. Sotto questo profilo, non manca chi proprio nel *Parere 1/15* in materia di trasferimento dei PNR ritrova conferma di questo approccio. Se si esclude infatti la visione di chi individua nella legittimazione di questa specifica forma di *data transfer* – che riguarda tutti i codici di prenotazione di tutti i passeggeri aerei, senza che sussista alcun criterio oggettivo che porti ad individuare un preciso collegamento tra un soggetto e una minaccia per la sicurezza –una più ampia legittimazione di forme di conservazione generalizzata, ciò che emerge

[67] In tale interrogazione viene espressamente chiesto "When will the Commission give a full and detailed overview of the state of play of implementation of the ePrivacy Directive in each Member State? When will it launch infringement proceedings against those Member States that have breached the provisions of the ePrivacy Directive?".

[68] Questa è la risposta fornita dalla Commissione il 29 aprile 2020.

dal Parere richiamato è, al contrario, una riaffermazione della incompatibilità di forme di *bulk data retention*. Il trasferimento e trattamento avente ad oggetto dati PNR infatti sono di per sé operazioni già selettive e limitate, riguardando solo, in questo caso, talune specifiche tipologie di dati, i codici di prenotazione appunto, la cui capacità di fornire una profilazione precisa della vita privata di un individuo è ridotta rispetto a quella dei metadati derivanti da telecomunicazioni; i giudici hanno ribadito che elementi da considerare per determinare la proporzionalità e necessità della ingerenza nella sfera privata sono da individuarsi nella quantità dei dati stessi, nelle caratteristiche e tempistiche della conservazione, nella esclusione dei dati sensibili, nella conservazione solo per il periodo di soggiorno e nella cancellazione successiva al momento della partenza[69]. In questo senso e sulla base di tali valutazioni quindi si può ammettere una *data retention* 'ristretta' quale quella riguardante i PNR, che mantiene comunque un margine di efficacia più ampio rispetto alla mera conservazione targettizzata, che tante critiche e perplessità ha sollevato. Merita tuttavia precisare come una tale lettura potrà essere confermata o sconfessata dall'esito dei rinvii pregiudiziali promossi dai giudici belgi e tedeschi[70], già analizzati nel Capitolo III e che attengono alla legittimità e proporzionalità della Direttiva 2016/681 in materia di PNR, letta alla luce degli artt. 7, 8 e 52 della Carta di Nizza. Sotto questo profilo la posizione della CGUE sarà dirimente per comprendere se un tipo di conservazione e accesso a dati sul modello di quanto proposto dalla normativa europea con riferimento ai codici di prenotazione dei passeggeri sia compatibile con il diritto dell'UE e con l'interpretazione di esso fornita dalla CGUE nelle sue pronunce in materia di *data retention* nonché nel *Parere 1/15*.

Certamente, insieme ai limiti della conservazione che necessitano ancora di essere con chiarezza determinati e in attesa della pronuncia della Corte che potrebbe fornire indicazioni utili per comprendere se una conservazione dei dati *limitata* possa essere legittima, un ulteriore nodo centrale da sciogliere, che potrebbe portare a reazioni fortemente avverse da parte degli Stati membri, è quello della delimitazione dell'ambito di applicazione dell'art. 15 della Direttiva *e-Privacy* e dunque della espansione dei criteri indicati dalla giurisprudenza europea anche alle normative che regolano le attività delle agenzie di intelligence operanti nell'ambito della garanzia della sicurezza nazionale. La lettura fornita dalla Corte in *Tele2* ha trovato conferma e, in un certo senso, ulteriore sviluppo anche nelle più recenti Conclusioni dell'Avvocato generale Saugmandsgaard Øe in *Ministerio Fiscal* e di Campos Sanchez-Bordona nei tre rinvii pendenti richiamati: laddove vi sia un trattamento di dati da parte di un soggetto privato, la normativa di riferimento rientra all'interno dell'ambito di applicazione della Direttiva *e-Privacy* e del diritto dell'UE. Resta invece unicamente appannaggio degli Stati membri la regolamentazione di attività delle autorità di *law enforcement* o di intelligence che non comportano un intervento dei fornitori privati, ad esempio quando siano le autorità stesse ad effettuare direttamente intercettazioni, raccolta e conservazione di metadati.

Questa lettura, che ha il merito di includere e dunque sottoporre al diritto dell'Unione e al rispetto della Carta di Nizza talune operazioni di trattamento rivolte alla finalità di sicurezza nazionale, comporta alcuni pregi e talune problematiche, alcune delle quali sono già emerse nei Capitoli precedenti. Innanzitutto una distinzione fondata sui soggetti coinvolti e operanti e non sulla finalità perseguita

[69] Una lettura di questo tipo, che cioè prende esempio dai criteri e dalla posizione espressa dalla CGUE nel *Parere 1/15* per interpretare quanto affermato nella sentenza *Tele2* sul fronte interno al territorio UE, viene fornita da Coudert, che sottolinea come le tutele, le salvaguardie e i limiti posti dalla Corte con riferimento al trasferimento dati verso il Canada siano sufficienti e necessari per permettere di considerare la *data retention* conforme a quei requisiti stabiliti nella sentenza *Tele2* e nel diritto dell'Unione in generale. Valutazioni di questo tipo consentono di far salva la potenzialità della conservazione dei dati, senza che ciò comprometta in maniera sproporzionata i diritti fondamentali, riconosciuti nel contesto europeo. F. COUDERT, *In the aftermath of Tele2 and Opinion 1/15: when are data retention measures legitimate?*, in *CiTiP Blog*, University of Leuven, 21 novembre 2017, https://www.law.kuleuven.be/citip/blog/in-the-aftermath-of-tele2-and-opinion-115-when-are-data-retention-measures-legitimate/.

[70] Si rimanda sul punto, più ampiamente, all'analisi fornita nel Capitolo III.

permette certamente di eliminare le criticità derivanti dalla difficile definizione di 'sicurezza nazionale' intesa come differente rispetto alla 'sicurezza pubblica'. Il diritto dell'Unione europea, pur richiamando in molteplici normative il concetto di sicurezza nelle sue diverse accezioni di pubblica e 'dello Stato' o nazionale (si fa riferimento ad esempio alla nota Direttiva *e-Privacy*, al GDPR, alla Direttiva 2016/681 in materia di PNR, alla Direttiva 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali), non prevede tuttavia delle chiare definizioni di tali termini. Proprio sul fronte definitorio, sia la dottrina[71] che la giurisprudenza della CGUE hanno riscontrato difficoltà, come evidenziato nel Capitolo I, Parte I. La Corte in particolare ha molto spesso utilizzato indifferentemente o quanto meno ha affiancato i due termini: nella pronuncia *Promusicae c. Telefonica*[72], i giudici di Lussemburgo hanno affermato che "la sicurezza nazionale, la difesa e la sicurezza pubblica, costituiscono attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei singoli" (par. 51). L'Unione europea stessa, soprattutto a seguito del Trattato di Lisbona e del superamento della rigida separazione in Pilastri, ha rafforzato, sia nel Titolo V TUE che nell'art. 83 TFUE, le proprie competenze nell'ambito della sicurezza e della determinazione di "norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni", tra cui anche la lotta al terrorismo. Questo ha portato alcuni autori a pensare che la 'sicurezza nazionale', da considerarsi esclusa dall'ambito di applicazione del diritto dell'UE ai sensi dell'art. 4, co. 2, TUE, sia rimasta ormai un ambito residuale che riguarda quelle minacce strettamente relegate entro i confini dello Stato membro, mentre la 'sicurezza pubblica' debba intendersi come un concetto più ampio, che riguarda i pericoli che hanno valenza e dimensione europea o quantomeno transnazionale[73]. Come si nota comunque la distinzione tra le due nozioni di sicurezza resta estremamente labile e flessibile e la lettura proposta dagli Avvocati generali di determinare l'applicabilità o meno del diritto dell'UE distaccandosi da una teorica individuazione dei confini tra sicurezza pubblica e nazionale, può rappresentare una utile soluzione.

D'altro lato però non può non tenersi conto come, soprattutto nel contesto moderno caratterizzato da sempre più sofisticate tecnologie, anche la determinazione di una differenziazione delle operazioni a seconda dei soggetti coinvolti può essere alquanto complessa: "the heightened capacity for wide-scale data harvesting by the intelligence services of the Member States, including by gaining access to data initially collected by private operators for commercial reasons, has blurred the dividing line and increased the potential for interference between activities seeking to guarantee national security and contiguous areas governed by EU law, such as for instance the protection of privacy"[74]. Sotto questo profilo, se ormai è stata superata la teoria secondo cui il mero richiamo alla sicurezza nazionale dovrebbe di per sé escludere l'applicabilità del diritto dell'Unione[75] – e di conseguenza, è bene ricordarlo, anche del rispetto dei diritti dettati nella Carta di Nizza –, è altrettanto vero che l'interpretazione della Corte e degli Avvocati generali porterebbe alla conseguenza che qualsiasi normativa che, per qualsiasi scopo securitario, comporti un intervento di operatori privati, debba necessariamente essere sottoposta al diritto

[71] Per una utile e completa ricostruzione delle posizioni espresse dalla dottrina, si rimanda a P. VOGIATZOGLOU, S. FANTIN, *National and public security within and beyond the Police Directive*, in A. VEDDER, J. SCHROERS, C. DUCUING, P. VALCKE (a cura di), *Security and Law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Intersentia, 2019, pp. 27-62.

[72] 28 gennaio 2008, C-275/06, *Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU*.

[73] Così A. DIMOTROVA, M. BRKAN, *Balancing national security and data protection: the role of EU and US policy-makers and Courts before and after the NSA affair*, in *Journal of Common Market Studies*, 4, 2018, p. 751.

[74] S. CRESPI, *The applicability of Schrems principles to the Member States: national security and data protection within the EU context*, in *European Law Review*, 5, 2018, p. 678.

[75] La stessa CGUE in 4 giugno 2013, C-300/11, *ZZ c. Secretary of State*, ha affermato come "sebbene spetti agli Stati membri decidere le misure idonee a garantire la loro sicurezza interna ed esterna, la mera circostanza che una decisione riguardi la sicurezza dello Stato non può comportare l'inapplicabilità del diritto dell'Unione", par. 38.

dell'Unione e al rispetto dei principi di proporzionalità e necessità di cui all'art. 52 della Carta di Nizza come interpretati, con riferimento alla raccolta di metadati, dalla CGUE nelle sentenze sino a qui analizzate[76]. Del resto questa lettura "espansiva", che finirebbe col sottoporre gran parte delle attività poste in essere da agenzie di intelligence ai c.d. 'criteri *Tele2*', pone innegabili rischi e pericoli collaterali: gli Stati membri potrebbero in futuro privilegiare l'impiego di strumenti di indagine mediante raccolta e conservazione di dati che non prevedano l'intervento di attori privati, in modo da avere così minori vincoli, soprattutto quanto al ricorso a forme di conservazione generalizzata ed indiscriminata. Inoltre non bisogna dimenticare che l'Avvocato generale Campos Sanchez-Bordona stesso, così come già brevemente statuito dai giudici nella sentenza *Tele2*, ha accennato alla possibilità di utilizzare forme di *bulk data retention* in casi di comprovata e incombente emergenza e per periodi ben determinati: anche questa eccezione, formulata in maniera piuttosto ampia, lascia potenzialmente spazio a diverse interpretazioni e dunque a pericolose derive o al rischio di abusi.

Ecco quindi che alla luce di queste considerazioni emergono i limiti delle soluzioni proposte: è chiaro che le riflessioni sulle competenze e sui limiti dell'intervento del diritto dell'Unione europea sono strettamente interrelati con le peculiarità delle operazioni e della disciplina cui si fa riferimento, quella della conservazione di metadati e del successivo accesso da parte di autorità pubbliche statali, che coinvolgono diversi soggetti e che impattano sia sull'attività di operatori privati che sulla efficacia delle attività dei singoli Stati membri nella garanzia della sicurezza dei propri cittadini[77]. La complessità delle tecnologie impiegata contribuisce a sfumare ancora più i confini tra attività poste in essere, finalità perseguite e soggetti coinvolti, così come la delicatezza dei diritti e degli interessi in gioco rendono la questione preliminare della determinazione dell'ambito di applicazione del diritto dell'Unione e in particolare, per quanto qui interessa, dell'art. 15 Direttiva *e-Privacy*, un punto focale sul quale, soprattutto nei rinvii pregiudiziali promossi da Regno Unito, Francia e Belgio, la CGUE dovrà dare una risposta pressoché definitiva, per quanto, come si è visto, nessuna scelta o delimitazione del campo sia scevra da conseguenze di grande rilievo.

Un ulteriore profilo di complessità e di necessaria riflessione, che si somma a quanto già evidenziato, è quello relativo alla giurisprudenza della Corte EDU: anche questa Corte infatti si è occupata, ormai da lungo tempo, di controversie attinenti a normative nazionali in materia di sorveglianza, adottate per

---

[76] Anderson, British Independent Reviewer of Terrorism Legislation ha affermato sul punto come: "national security remains the sole responsibility of each Member State: but subject to that, any UK legislation governing interception or communications data is likely to have to comply with the EU Charter because it would constitute a derogation from EU directives in the field", in D. ANDERSON, *A Question of* Trust, 2015, disponibile all'indirizzo: *ht*tps://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

[77] Altro punto sul quale riflettere con attenzione deriva dalla posizione espressa dalla CGUE nella sentenza *Schrems* e nel *Parere 1/15*: se si escludesse l'applicazione dei c.d. criteri *Tele2* alle attività di conservazione e trattamento dei dati svolti dagli Stati membri per finalità di sicurezza nazionale, si giungerebbe al paradosso di stabilire criteri più rigidi per quanto riguarda il fronte esterno, cioè il trasferimento dei dati verso Stati terzi per scopi securitari, mentre il medesimo ambito verrebbe invece lasciato alla discrezionalità degli Stati membri sul fronte interno. Ciò creerebbe quella che già nel Capitolo III è stata definita come una posizione ipocrita dell'Unione europea che impone a Stati extra-UE elevati livelli di tutela della riservatezza e della protezione dei dati e che esclude invece l'applicazione dei medesimi criteri agli Stati membri sulla base del principio di attribuzione dei poteri e della ripartizione di competenze tra Stati e UE. "The unclear delineation and definition of "national security" can produce confusion about the standards that should apply to Member State activities. There is an urgent need for limitation or clarification of the meaning of the term in the context of data protection rights. (..) It is hypocritical for EU policymakers and the CJEU to concern themselves with the standards of data protection for intelligence surveillance outside the EU, when the standards of data protection for intelligence surveillance outside the EU, when the standards that apply in the EU seem lacking in many respects. (..) In a moral and political sense, the legitimacy of EU fundamental rights protection is undermined if the EU is viewed as holding third countries to standards that it is not willing to abide by itself. It would enhance the legitimacy of the EU law in the eyes of third countries if national security was clearly brought within the ambit of EU fundamental rights law", C. KUNER, *Reality and Illusion in EU data transfer regulation post* Schrems, in *German Law Journal*, 4, 2018, p. 889.

finalità securitarie e determinanti l'intervento di diverse autorità statali, di *law enforcement* o di intelligence, nonché l'impiego di diversi strumenti di intrusione nella vita privata, con o senza l'apporto di operatori privati del settore delle telecomunicazioni. Benché si rimandi sin da ora al Capitolo V per una analisi approfondita di tale giurisprudenza e della sua evoluzione nel corso del tempo, oltre che per un raffronto con la posizione della CGUE pur con tutti i necessari distinguo derivanti dal diverso contesto entro cui le due Corti operano, pare sin da ora utile sottolineare come alcune divergenze stiano emergendo negli ultimi casi sottoposti alla Corte sita in Strasburgo; quest'ultima pare ammettere sistemi di sorveglianza massiva e generalizzata, anche senza richiedere, quantomeno nel più recente approccio, la sussistenza di un 'ragionevole sospetto' tra intrusione nella sfera privata e minaccia per la sicurezza e pare inoltre sfumare o limitare anche altri criteri determinati dalla CGUE e, in precedenza, dalla Corte EDU stessa quali ad esempio la notifica ai soggetti interessati dall'accesso ai dati o la previa autorizzazione e controllo delle operazioni di accesso da parte di una autorità indipendente. Benché le normative esaminate siano differenti, così come alcuni dei criteri siano diversamente intesi e un parallelismo non possa sempre essere individuato, è comunque importante riflettere su come le scelte della Corte EDU possano incidere sulla giurisprudenza della Corte di giustizia dell'UE e sul se e come i giudici di Lussemburgo terranno conto delle più recenti evoluzioni della giurisprudenza della Corte EDU.

Un ulteriore punto sul quale la CGUE dovrà porre attenzione nelle pronunce attese rispetto ai rinvii pregiudiziali esaminati è quello, già emerso soprattutto nella critica mossa da alcune ONG, della valutazione sulla reale efficacia, utilità ed adeguatezza della conservazione dei metadati a raggiungere l'obiettivo preposto e alla inesistenza di mezzi alternativi, meno invasivi ma egualmente efficaci. È questo un profilo sino ad ora poco indagato e discusso, rispetto al quale i giudici del rinvio così come la CGUE hanno solo sbrigativamente risposto, per lo più basandosi su studi o affermazioni rilasciate da autorità di *law enforcement* nel corso dei procedimenti. Del resto è lo stesso Avvocato generale Saugmandsgaard Ø, nelle sue Conclusioni al caso *Tele2*, ad affermare come "diversi studi portati all'attenzione della Corte rimettono in discussione la necessità di tale tipo di obbligo ai fini della lotta contro i reati gravi", pur giungendo poi a concludere che "ammesso che altre misure possano essere altrettanto efficaci nella lotta contro i reati gravi, ai giudici del rinvio spetterà l'ulteriore compito di determinare se queste ultime siano meno lesive dei diritti fondamentali in questione" (par. 209-210). Alcuni commentatori tuttavia hanno criticato tale approccio ritenendo che la CGUE nei casi *DRI* e *Tele2* "did not base its ruling on evidence relating to the effectiveness of the instrument of the data retention. The ruling is rather based on a theoretical reasoning that data retention genuinely satisfies an objective of general interest"[78]. Queste considerazioni peraltro divengono di estrema utilità non solo per i giudici bensì anche con riferimento al dibattito sul piano legislativo e alle scelte che le Istituzioni europee stanno vagliando quanto alla necessità di una apposita legislazione in questo ambito. L'assenza di simili valutazioni sul profilo della utilità dello strumento della conservazione generalizzata porta al rischio che "far too many governments are in fact pursuing maximalist surveillance agendas without proper evidence-based assessment of the actual benefits of what is proposed, without an honest cost efficiency analysis and without real privacy impact assessment", potendosi così individuare nella mancanza di una seria discussione su questo cruciale aspetto la vera "tragedy of the current surveillance debate"[79]. Quello

[78] H. HIJIMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 16 TFEU*, Springer, 2016.

[79] M. SCHEININ, *Towards evidence-based discussion on surveillance: a rejoinder to Richard A. Epstein*, in *European Constitutional Law Review*, 12, 2016, p. 344. Dello stesso avviso anche D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, in *Israel Law Review*, 1, 2019, pp. 31-60. Sul punto, si richiama anche quanto sottolineato, sin dal 2014, dal Commissioner for Human Rights del Consiglio d'Europa, che nel *Issue Paper: the rule of law on the Internet and in the wider digital world*, 2014, ha affermato: "What is more, extensive research has failed to show any significant positive effect on clear-up rates for crime, and especially not for terrorism-related crime, as a result of compulsory

che molti autori invocano è una riflessione 'evidence-based' sulla *data retention*, che sia fondata su studi concreti circa la efficacia e la necessità di tale misura: se da un lato vi sono studiosi che vedono nelle limitazioni imposte dalla CGUE un pericolo significativo per il funzionamento corretto delle attività di intelligence e in generale per la prevenzione e lotta di reati gravi che trovano nella conservazione generalizzata uno strumento fondamentale[80], altri invece rilevano l'assenza di prove e dati che stabiliscano la reale portata e potenzialità, nella concreta operatività, dell'avere a disposizione una quantità sconfinata di metadati. Se per trovare un ago – una informazione utile per prevenire o combattere un crimine – in un pagliaio – di dati – serve necessariamente un pagliaio, ciò che viene criticato è il fatto che un pagliaio troppo ampio rischi di rendere eccessivamente complessa la ricerca dell'ago stesso: con riferimento agli attentati di Parigi del 2015, Scheinin afferma come le autorità di intelligence e *law enforcement* avessero riscontrato proprio nelle troppe piste da seguire un ostacolo alla efficacia delle proprie attività: "The fact that the attack came as a surprise demonstrates a failure of intelligence coordination internally in France and in Belgium, and between those two neighbouring EU countries. More broadly, it demonstrates a failure of the collect-it-all mentality, whereby any unmonitored modalities of communication are seen as an unknown security threat worth any investment of money, personnel and political influence – often to the detriment of taking action in respect of known security threats, such as individuals already suspected of preparing acts of terrorism"[81]. Un ulteriore spunto di riflessione emerge anche dai rinvii pregiudiziali pendenti, in particolare da quelli promossi dalla Corte costituzionale belga e dalla Corte suprema irlandese, nei quali viene messo in evidenza come i regimi di conservazione generalizzata dei dati non tutelino solo la sicurezza pubblica e nazionale e l'efficienza delle operazioni delle pubbliche attività in tale ambito bensì anche i diritti fondamentali delle vittime di reati, aiutando nello svolgimento delle indagini, così come a favore di soggetti scomparsi e di minori nella lotta a reati quali la pedopornografia online. Tutti questi soggetti e i diritti di cui essi sono titolari possono trovare, secondo tali posizioni, un enorme vantaggio e beneficio dall'utilizzo dei dati conservati.

Quello che rileva, comunque, è quanto una valutazione sulla efficacia della misura risulti indispensabile precondizione per poter svolgere un corretto bilanciamento dei diversi interessi e diritti in gioco, ricordando che, come il Gruppo di Lavoro Art. 29 aveva messo in evidenza, "not everything that is technically feasible or might prove to be useful for the purpose of fighting serious crime is

---

data retention. Civil society has strongly and convincingly argued for the replacement of suspicionless data retention by data preservation (also referred to as quick-freeze of data), making it possible for law-enforcement agencies to obtain an order requiring e-communications companies and the like to retain the communications data of people when there are factual indications that it may be helpful to the prevention, investigation or prosecution of crimes, with urgent procedures allowing for the imposition of such a measure without delay in appropriate cases, subject to ex post facto authorization", p. 264.

[80] Di questo avviso R. A. EPSTEIN, *The ECJ's fatal imbalance: its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European constitutional law review*, 12, 2016, pp. 330-340. Egli sostiene che "it is surely the case that the ability to trace connections among various parties does allow the government to build up profiles against individual persons—which is of course exactly why the data is collected. If it can be said that piecing together disconnected bits of information allows the government to spy on innocent people, then it should be conceded that the same techniques allow the government to spy on individuals who do pose a threat to the security of other individuals. It seems very odd to say that a technique that is effective in committing privacy violations against ordinary citizens is of no use in tracking terrorists. And given the complete breakdown of intelligence with respect to the perpetrators of the terrorist acts in Paris, it seems that this concern should be greater today than it was at the time of the 6 October decision. What was true at that time, and is still true today, is that an invasion of privacy is small potatoes in comparison with the loss of life and limb", p. 333. In risposta alla posizione critica e avversa di Scheinin, lo stesso Epstein definisce la giurisprudenza della CGUE come fondata su di una "exaggerated and misconceived notion of individual privacy", in *The deepening EU blindness on privacy: a pointed response to Professor Martin Scheinin*, in *European Constitutional Law Review*, 12, 2016, p. 352.

[81] M. SCHEININ, *Towards evidence-based discussion on surveillance: a rejoinder to Richard A. Epstein*, op. cit., p. 347.

desirable or can be considered as a necessary measure in a democratic society"[82] e dunque una corretta valutazione della proporzionalità e necessità delle misure è operazione di fondamentale importanza.

Questa analisi dei numerosi punti ancora problematici e delicati e degli incerti e complessi possibili sviluppi futuri mette in evidenza come la disciplina della *data retention* e del successivo accesso per scopi securitari imponga una riflessione ben più ampia di quella strettamente limitata alla determinazione delle singole condizioni e requisiti, aprendo a significative considerazioni su svariati profili cruciali attinenti al ruolo della CGUE, all'ambito di applicazione del diritto dell'Unione europea e al rapporto tra istituzioni europee e Stati membri.

[82] GRUPPO DI LAVORO ART. 29, *Opinion 9/2004 on the draft framework decision on the storage or data processed and retained for the purpose of providing electronic public communications services*, 2004.

CAPITOLO V

L'EVOLUZIONE DELLA GIURISPRUDENZA DELLA CORTE EUROPEA DEI DIRITTI DELL'UOMO IN MATERIA DI RACCOLTA, INTERCETTAZIONE, CONSERVAZIONE E ACCESSO A DATI E METADATI PER SCOPI SECURITARI

L'esistenza di sistemi di – concreta o potenziale – sorveglianza di massa, resi possibili mediante l'utilizzo sempre più massiccio da parte delle autorità pubbliche di strumenti di raccolta, conservazione e accesso a dati e metadati, non è stata oggetto di scrutinio della sola Corte di giustizia dell'UE. Anche la Corte europea dei diritti dell'uomo, infatti, è stata chiamata a pronunciarsi in merito alla conformità rispetto alla Convenzione Europea dei Diritti dell'Uomo (CEDU) di normative nazionali disciplinanti misure di sorveglianza utilizzate sia da autorità di *law enforcement* per finalità di prevenzione e repressione di crimini gravi, sia da agenzie di intelligence al fine di tutelare la sicurezza nazionale. Entrambe le Corti europee dunque si sono dovute confrontare con complesse controversie riguardanti la legittimità e proporzionalità dell'ingerenza dello Stato nella sfera privata per scopi securitari e la conseguente individuazione di limiti e salvaguardie necessari ad una efficace tutela della riservatezza e della protezione dei dati.

Sebbene sia stata già evidenziata nei Capitoli precedenti la posizione avanguardista assunta negli ultimi decenni dalla Corte di giustizia dell'UE con le sue storiche e determinanti pronunce in materia, è innegabile come la Corte EDU vanti una casistica di ben più lontana origine: risalgono infatti a oltre 40 anni fa le prime decisioni aventi ad oggetto la tutela dell'art. 8 CEDU dinnanzi a forme di sorveglianza massiva o segreta, a partire dalla sentenza *Klass*[1]. La rilevanza di tale ampia giurisprudenza – spesso richiamata dai giudici di Lussemburgo nonché da numerose Corti nazionali – non può essere ignorata nella presente ricostruzione: si rende quindi necessario dedicare un apposito, per quanto contenuto, spazio all'esame di alcune delle più recenti e significative pronunce della Corte EDU in ambito di conservazione e accesso ai dati per scopi securitari, al fine di fornire una panoramica quanto più completa possibile della tematica sino ad ora analizzata e di sviluppare, in conclusione, alcune riflessioni di raffronto tra i diversi approcci impiegati dai due giudici europei. Sotto questo ultimo profilo, non può mancarsi di sottolineare preliminarmente quanto un confronto acritico o astratto, che sottovaluta o trascura cioè i differenti contesti entro cui le Corti operano, rischi di risultare del tutto fuorviante ed erroneo. La CGUE infatti opera in un contesto differente, quello dell'Unione europea, all'interno del quale è chiamata ad utilizzare quali parametri dei propri giudizi non solo la Carta di Nizza e dunque la conformità di una normativa o di un atto rispetto ai diritti fondamentali riconosciuti, bensì anche la compatibilità rispetto ai Trattati e al diritto dell'UE. Inoltre, la CGUE deve considerare la struttura ed il funzionamento dell'UE e i limiti che derivano dal principio di attribuzione e dal riparto delle competenze tra UE e Stati membri; tale aspetto diviene di estrema delicatezza nell'ambito in esame: secondo l'interpretazione già evidenziata nei Capitoli II e IV e sino ad ora avvallata dai giudici di Lussemburgo

[1] *Klass e altri c. Germania*, ricorso n. 5029/71, deciso il 6 settembre 1978. Come ricordato anche da O'Leary, "it is clear that the origins and underpinnings of ECJ data protection case law remain located in the ECHR. The terms of recent ECJ judgements, the EU Charter and the accompanying explanations support this. In addition, recent judgements of the ECtHR on mass surveillance and other UK, French, German, Austrian and Swedish cases now pending mean that this is not territory which is exclusively focused on the EU's harmonized data protection regime and on the interpretative standards set by the ECJ when interpreting the latter.", S. O'LEARY, *Balancing rights in a digital age*, in *Irish Jurist*, 59, 2018, p. 82.

– per quanto sul punto sia ancora attesa una posizione definitiva, con riferimento in particolare al rinvio pendente *Privacy International* –, non rientrano nell'ambito di applicazione del diritto dell'UE le attività di sorveglianza effettuate mediante raccolta, conservazione e accesso a dati e metadati per scopi securitari qualora esse siano poste in essere direttamente dalle autorità pubbliche nazionali, senza che obblighi o azioni siano stabilite e previste a carico di operatori privati. La Corte EDU, invece, ha la possibilità di svolgere uno scrutinio più ampio, potendo decidere ad esempio sulla compatibilità alla Convenzione di attività interamente svolte da autorità statali (ad esempio operazioni di *Foreign Intelligence* operate dai servizi segreti mediante accesso diretto ai mezzi di telecomunicazione), pur scontando maggiori limiti in termini di concreta efficacia ed effettività delle decisioni. Diversamente dalla CGUE che deve considerare una pluralità di parametri, però, l'unico parametro di riferimento dei giudici di Strasburgo è rappresentato dalla Convenzione EDU stessa e dunque dai diritti fondamentali enunciati.

Le diversità riscontrabili nello scrutinio svolto dalle due Corti europee risiedono inoltre nel differente dettato normativo delle due Carte di riferimento poste a tutela dei diritti fondamentali: come già sottolineato nel Capitolo I, Parte I, l'art. 8 della CEDU riconosce il diritto di ogni persona al rispetto della vita privata e familiare, del proprio domicilio e della propria corrispondenza (art. 8, co. 1), senza che trovi però apposito e autonomo spazio il diritto alla protezione dei dati[2], riconosciuto invece espressamente all'art. 8 della Carta di Nizza; mentre in quest'ultima poi le limitazioni ai diritti e libertà riconosciuti debbono rispettare le condizioni fissate dal più volte richiamato art. 52 al fine di essere considerate legittime, nella CEDU è l'art. 8 co. 2 stesso ad enunciare direttamente la natura relativa e non assoluta del diritto alla riservatezza, fissando gli specifici requisiti di legittimità[3].

Tutte queste differenziazioni 'sistematiche' si riflettono ovviamente sulla natura ed estensione delle questioni poste all'attenzione delle due Corti nonché sul ragionamento e sul metodo di analisi utilizzati: se dunque alcune sovrapposizioni sono rinvenibili nei casi affrontati, come emerge anche dal richiamo dell'una alla giurisprudenza dell'altra, un perfetto parallelismo e trasposizione delle conclusioni dei giudici di Strasburgo rispetto a quelle adottate dai 'colleghi' di Lussemburgo non è effettuabile.

Nonostante questa necessaria premessa, che vuole indurre quindi ad osservare con cautela la giurisprudenza in esame, invitando a coglierne le importanti differenze fattuali e di contesto, l'esperienza della Corte EDU ed il percorso evolutivo da essa seguito meritano grande attenzione per le considerazioni proposte e i rilevanti riflessi ed influenze che potrebbero avere, in futuro, sull'approccio della CGUE.

---

[2] Merita sottolineare come, certamente, nel momento in cui la Convenzione EDU è stata redatta non fosse possibile pensare ad un diritto alla protezione dei dati inteso nella sua accezione attuale di diritto al 'controllo' delle e sulle informazioni, la cui esigenza è stata fortemente sentita solo a seguito della massiva digitalizzazione e la cui affermazione si è registrata anche e soprattutto in ragione dell'avanzamento tecnologico che ha portato alla produzione massiva di dati. Una interpretazione dell'art. 8 CEDU come previsione volta a garantire non solo il diritto alla riservatezza bensì anche il diritto alla protezione dei dati emerge tuttavia dalla giurisprudenza della Corte EDU stessa, che fa più o meno implicitamente riferimento a tale diritto in numerosi casi aventi ad oggetto violazioni dell'art. 8. Per ulteriori approfondimenti sul tema si rimanda al Capitolo I, Parte I.

[3] "Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui", art. 8, co. 2, CEDU. Come vedremo, la Corte EDU nella sua giurisprudenza ha definito e chiarito la portata dei criteri indicati in tale disposizione, da rinvenirsi appunto: a) nella previsione di misure limitative del diritto alla vita privata all'interno di una legge nazionale; b) nella presenza di uno scopo legittimo (rispetto al quale il dettato normativo prevede alcuni esempi) ed infine c) nella necessità della ingerenza nel contesto di una società democratica. Per una preliminare analisi dell'art. 8 CEDU, si rimanda, oltre alla bibliografia richiamata nel Capitolo I, Parte I, a P. BREYER, *Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR*, in *European Law Journal*, 3, 2005.

Questo capitolo dunque svolgerà una sintetica ricostruzione di alcune delle decisioni maggiormente significative pronunciate dai giudici di Strasburgo in materia: pur potendosi rinvenire sin dagli anni '80, come si è già anticipato, casi concernenti misure di sorveglianza quali intercettazioni e controllo della corrispondenza[4], è parso più appropriato ed adeguato ai fini della presente disamina, concentrare l'analisi su alcuni casi più recenti, nello specifico *Roman Zakharov c. Russia*[5], *Szabo e Vissy c. Ungheria*[6], *Centrum For Rattvisa c. Svezia*[7] e *Big Brother Watch e altri c. Regno Unito*[8], per due ordini di ragioni. Innanzitutto perché tali decisioni, adottate in tempi più recenti, hanno permesso alla Corte EDU di confrontarsi con sistemi fondati sulle c.d. *surveillance technologies* e dunque su meccanismi tecnologicamente all'avanguardia e sofisticati, che utilizzano principalmente forme di controllo operate su dati e metadati derivanti da servizi di telecomunicazioni; secondariamente perché le quattro pronunce selezionate consentiranno di tracciare con maggiore chiarezza lo sviluppo nel tempo della posizione della Corte in tale ambito e di cogliere le problematiche ancora aperte, al momento poste al vaglio della Grande Camera nei ricorsi pendenti. Solo al termine di questa ricostruzione e pur tenendo conto delle diversità sopra evidenziate, sarà possibile riflettere sulla esistenza o meno di una tutela giurisprudenziale 'europea', intesa in senso lato, uniforme e convergente in materia di riservatezza e protezione dei dati personali dinnanzi a pratiche sempre più diffuse di sorveglianza massiva.

1. – Da Zakharov *a* Big Brother Watch*: l'evoluzione della giurisprudenza della Corte EDU in materia di sorveglianza di massa*

Le quattro sentenze scelte, la cui analisi occuperà questo ed il prossimo paragrafo, sono state riunite in due gruppi, *Zakharov* e *Szabo* da un lato e *Centrum For Rattvisa* e *Big Brother Watch* dall'altro. Questa decisione non trova le sue ragioni solamente nel criterio cronologico bensì anche in valutazioni di tipo sostanziale: nelle pronunce inserite nel medesimo gruppo, infatti, è possibile individuare una posizione ed un approccio pressoché coerente della Corte, mentre una certa evoluzione – se non, come vedremo, per alcuni commentatori addirittura una vera e propria inversione di marcia[9] – può essere riscontrata tra i due raggruppamenti di sentenze nonché tra il primo blocco e la giurisprudenza precedente, cui si farà incidentalmente richiamo. Prendendo dunque abbrivio dalla sentenza *Zakharov*, verranno poi esaminate le ulteriori decisioni e posti in evidenza gli elementi di discordanza o di convergenza, per poi analizzare conclusivamente i possibili scenari futuri e le questioni aperte dalle ultime discusse sentenze, avverso le quali è stato richiesto l'intervento della Grande Camera.

Anche con riferimento a questa ricostruzione deve comunque essere posto preliminarmente in evidenza come le lesioni dei diritti fondamentali denunciate dai ricorrenti nei quattro casi derivino da normative nazionali anche molto diverse tra loro, aventi ad oggetto misure di sorveglianza poste in essere da autorità differenti, per finalità differenti, sebbene tutte riconducibili alla tutela della sicurezza, nonché riguardanti destinatari diversi – talvolta stranieri, talaltra cittadini – ed inserite in ordinamenti

[4] Si pensi al caso *Klass e altri c. Germania*, sopra citato o ancora a *Weber e Saravia c. Germania*, ricorso n. 54934/00, deciso il 29 giugno 2006, *Liberty e altri c. Regno Unito*, ricorso n. 58243/00, deciso il 1 luglio 2008 e *Kennedy c. Regno Unito*, ricorso n. 26839/05, deciso il 18 maggio 2010. Questi casi, che non verranno esaminati nel dettaglio in questa sede, saranno comunque spesso richiamati nell'analisi delle quattro decisioni oggetto di più ampia ricostruzione in questo Capitolo.

[5] *Roman Zakharov c. Russia*, ricorso n. 47143/06, deciso il 4 dicembre 2015.

[6] *Szabo e Vissy c. Ungheria*, ricorso n. 37138/14, deciso il 12 gennaio 2016.

[7] *Centrum For Rattvisa c. Svezia*, ricorso n. 35252/08, deciso il 19 giugno 2018, attualmente al vaglio della Grande Camera, dal febbraio 2019, su ricorso di Centrum For Rattvisa.

[8] *Big Brother Watch e altri c. Regno Unito*, ricorsi n. 58170/13, 62322/14 e 24960/15, decisi il 13 settembre 2018, attualmente al vaglio della Grande Camera, dal febbraio 2019, su ricorso di Big Brother Watch e altri ricorrenti.

[9] Tra gli altri, come si dirà più ampiamente in seguito, V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, Working Papers HSE, 2019.

dotati di legislazioni a tutela della protezione dei dati e della riservatezza molto dissimili. Queste diverse condizioni fattuali non possono, come si vedrà, non essere tenute in debita considerazione quando ci si appresterà a comparare le conclusioni cui la Corte EDU è giunta nelle sue diverse decisioni: ciò al fine di scongiurare il rischio di una lettura deviante, che astragga eccessivamente dalle peculiarità del caso concreto.

1.1. – La sentenza Zakharov*: la riconosciuta violazione dell'art. 8 CEDU e la determinazione di stringenti requisiti in materia di sorveglianza*

Venendo pertanto all'analisi della prima pronuncia, la sentenza *Zakharov* originava dalle rimostranze del caporedattore di una casa editrice russa nonché membro apicale di una ONG avente quale missione quella di monitorare il livello di libertà ed autonomia della stampa nazionale; questi, dopo aver esperito senza successo i previsti rimedi giudiziari interni[10], adiva la Corte EDU, ritenendo il controllo segreto delle proprie comunicazioni telefoniche, perpetrato dai servizi di polizia russi, ingiustificatamente lesivo del diritto alla riservatezza di cui all'art. 8 CEDU. L'Ordine n. 70 del Ministero delle Comunicazioni russo, infatti, permetteva l'installazione di dispositivi volti a consentire operazioni dirette di intercettazione di comunicazioni da parte di autorità di *law enforcement*, anche in assenza di previa autorizzazione e controllo da parte di una autorità giudiziaria.

Prima di vagliare nel merito la sussistenza dei tre criteri indicati all'art. 8, co. 2 CEDU, la Corte si è dovuta innanzitutto pronunciare su una questione preliminare, tutt'altro che meramente formale: la determinazione dello status di vittima del ricorrente e, conseguentemente, l'ammissibilità del ricorso stesso.

La regola generale di ammissibilità prevede che le decisioni della Corte EDU non possano avere ad oggetto l'analisi di una normativa *in abstracto*[11] bensì debbono essere volte unicamente a determinare se l'applicazione concreta di una legge abbia dato vita ad una violazione dei diritti riconosciuti nella CEDU. La peculiare natura segreta dei sistemi di controllo e sorveglianza tuttavia renderebbe nella maggior parte dei casi impossibile per l'individuo dimostrare di essere stato concretamente assoggettato a forme di controllo e di aver quindi subìto una lesione dei propri diritti: una rigida attuazione della regola di ammissibilità così come indicata avrebbe l'effetto di far divenire *de facto* incontestabili gli strumenti di sorveglianza segreta e massiva, ponendoli al di fuori della supervisione della Corte EDU[12]. Per questi motivi e per scongiurare tale serio rischio, i giudici europei, sin dalla più risalente sentenza *Klass*, avevano pertanto rivisto la condizione generale di ammissibilità del ricorso, concedendo al ricorrente, in via eccezionale e previo il rispetto di taluni requisiti, di assumere lo status di vittima senza dover provare di essere 'directly affected' da una determinata disposizione normativa. Ebbene, se sulla correttezza e necessità di tale circostanza eccezionale non sorgevano dubbi, tanto da essere ripresa a confermata anche nella sentenza in esame, perplessità significative si erano invece venute a creare quanto ai requisiti richiesti al fine riconoscere al ricorrente lo status di vittima: la giurisprudenza della

[10] Il ricorrente aveva già promosso istanze di fronte alla 'District Court' e successivamente alla 'City Court' di San Pietroburgo. In entrambi questi casi i giudici avevano entrambe i ricorsi di Zakharov sia per la mancanza di prove circa la reale e concreta lesione del diritto alla riservatezza del ricorrente, sia perché le contestate operazioni di invio dei dati da parte degli operatori di telecomunicazioni erano basate e regolate da una legge nazionale considerata sufficientemente prevedibile e consultabile. Per maggiori approfondimenti sulle decisioni delle Corti nazionali russe nel caso Zakharov, si rimanda a: M. COLE, A. VANDENDRIESSCHE, *From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabo/Vissy in Strasbourg: what the ECtHR made of the deep pass by the CJEU in the recent cases on mass surveillance*, in *European Data Protection Law Review*, 1, 2016, ma anche P. DE HERT, P. C. BOCOS, *Case of Roman Zakharov v. Russia: the Strasbourg follow up to the Luxembourg Court's Schrems judgement*, in *Strasbourg Observers*, 23 dicembre 2015.

[11] Par. 164, *Zakharov*.

[12] Par. 124, *Kennedy*; par. 169, *Zakharov*.

Corte EDU sul punto aveva conosciuto infatti un avvicendamento di due differenti approcci; secondo il primo, il criterio richiesto era da individuarsi nella c.d. "reasonable likelihood", cioè nella necessaria sussistenza di una ragionevole probabilità che le informazioni o comunicazioni personali del ricorrente fossero state oggetto di raccolta e conservazione da parte di *security services*[13]; la seconda linea interpretativa riteneva invece la mera esistenza di normative relative alla sorveglianza delle telecomunicazioni una condizione *per se* sufficiente a comprovare una ingerenza nel diritto alla riservatezza del ricorrente[14]. Abbracciando quest'ultimo approccio, ritenuto maggiormente coerente allo scopo ultimo di rendere sottoponibile al vaglio della Corte le normative in materia di sorveglianza, i giudici nella sentenza *Zakharov* si sono spinti anche a chiarire le ulteriori condizioni di ammissibilità imposte: nel caso di provata sussistenza di legislazioni aventi ad oggetto sistemi di controllo deve essere inoltre ragionevolmente possibile ritenere che il ricorrente sia stato sottoposto a sorveglianza – o perché appartenente ad un gruppo/categoria di individui oggetto della normativa al vaglio o perché la normativa è idonea a colpire indifferentemente tutti gli utenti di servizi di telecomunicazione – e non devono sussistere efficaci rimedi giudiziari a livello nazionale; per verificare questo punto, la Corte non dovrà però limitarsi a vagliare la mera esistenza *sulla carta* dei rimedi ma a considerare anzi la loro concreta efficacia: "where the domestic system does not afford an effective remedy to the person who suspects that he was subjected to secret surveillance, widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified" (par. 171, *Zakharov*).

L'individuazione in maniera precisa di queste specifiche e fondamentali condizioni di ammissibilità e il chiarimento della corretta interpretazione tra le diverse letture proposte dalla previa giurisprudenza rappresentano senza dubbio elementi di grande rilievo. La sentenza in esame, già in questa fase preliminare, ha pertanto il merito di aver appianato le divergenti posizioni emerse in precedenza e di aver fornito una univoca linea interpretativa che verrà peraltro mantenuta e confermata anche in tutte le successive sentenze in materia.

Applicando allo specifico caso in esame i requisiti sopra stabiliti, la Corte da un lato ha considerato adeguatamente comprovata la sussistenza di una normativa in materia di sorveglianza segreta[15] che, essendo volta a consentire le intercettazioni di tutti gli utenti di servizi di telefonia mobile russi, è certamente in grado di colpire anche il ricorrente, e dall'altro ha reputato inefficaci i rimedi predisposti sul piano nazionale (par. 178). Affermando quindi la presenza di tutti i requisiti necessari e, pertanto, riconoscendo lo status di vittima del ricorrente e l'ammissibilità del ricorso, la Corte ha poi proseguito il suo vaglio analizzando la legislazione russa alla luce dei criteri espressi nel già più volte richiamato art. 8, co. 2, CEDU: anche sotto questo profilo i giudici hanno fornito una lettura puntuale e chiarificatrice, che non ha mancato di porsi, in certi punti, in discontinuità rispetto alla previa giurisprudenza.

I giudici hanno dovuto valutare in primis la presenza di uno scopo legittimo, di una finalità cioè idonea a giustificare l'ingerenza in un diritto fondamentale: essa viene identificata, come del resto sostenuto dalle parti stesse, nella tutela della sicurezza (nazionale, ma non solo). Pur riconoscendo un certo 'margine di apprezzamento' in capo allo Stato quanto alla determinazione dei mezzi da porre in campo per raggiunge tale scopo, la Corte già in questo punto iniziale ha proposto una affermazione di estrema rilevanza: "this margin (of appreciation) is subject to European supervision embracing both legislation and decisions applying it. In view of *the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it*, the

[13] Approccio utilizzato ad esempio nella sentenza *Esbester c. Regno Unito*, ricorso n. 5029/71, deciso il 6 settembre 1978.

[14] Questa linea interpretativa era stata affermata nelle già richiamate sentenze *Klass* e *Kennedy*.

[15] Normativa peraltro non generalmente pubblica e dunque, diversamente da quanto sostenuto dalle Corti nazionali russe, non accessibile da parte di qualsiasi cittadino, se non mediante la consultazione di specifici database online (par. 180).

Court must be satisfied that there are adequate and effective guarantees against abuse" (par. 232, enfasi aggiunta). Da questa forte dichiarazione, emerge chiaramente la consapevolezza della pericolosità rappresentata dai sistemi di sorveglianza per la sussistenza della democrazia e dello stato di diritto, una consapevolezza che induce la Corte, nel suo vaglio delle normative nazionali, a porre particolare attenzione alle tutele e garanzie previste, che debbono essere in grado di limitare la discrezionalità del potere pubblico ed il rischio di abusi nell'impiego di tali insidiose misure.

È proprio partendo da questo fondamentale assunto che i giudici muovono poi a vagliare quella che viene definita "the quality of law", che implica non solo la presenza di una base normativa accessibile e prevedibile – carattere della "foreseeability" – ma anche che il sistema di sorveglianza così regolato risulti necessario in una società democratica, contenendo adeguate salvaguardie (par. 237). Questi criteri di prevedibilità e necessità, che erano stati già genericamente individuati anche nella giurisprudenza precedente, abbisognavano però di una univoca e puntuale interpretazione, che fosse specificamente adeguata e ritagliata sul peculiare ambito delle normative in materia di sorveglianza massiva. In un tale contesto, ad esempio, il requisito di 'sufficiente prevedibilità' della normativa, sopra richiamato, non poteva essere inteso nel senso di consentire ad ogni cittadino di determinare esattamente il momento di avvio delle intercettazioni delle proprie comunicazioni da parte delle autorità pubbliche: una siffatta interpretazione avrebbe comportato uno svilimento totale della misura di controllo stesso e della sua utilità. Ecco perché la Corte ha provveduto ad elaborare una lettura di tale criterio che fosse rigida ma al contempo compatibile con il funzionamento del sistema di sorveglianza, stabilendo così che la 'prevedibilità' impone in capo al legislatore nazionale l'onere di predisporre chiare e dettagliate regole sulle intercettazioni, in grado di limitare i possibili rischi di abusi e di arbitrarietà[16]. Con riferimento a questo criterio, così interpretato, i giudici europei non hanno trovato nella normativa russa e nell'Ordine n. 70 disposizioni sufficientemente dettagliate volte a regolare l'avvio di intercettazioni segrete[17]: "It leaves the authorities an almost unlimited degree of discretion in determining which events or acts constitute such a threat and whether that threat is serious enough to justify secret surveillance, thereby creating possibilities for abuse" (par. 248). La normativa russa prevedeva, infatti, la possibilità di utilizzare lo strumento di sorveglianza delle comunicazioni non solo per finalità di prevenzione e repressione di crimini di media severità, gravi o eccezionalmente gravi (già di per se un elenco estremamente vasto di fattispecie), ma anche per contrastare eventi o attività in grado di mettere in pericolo la "sicurezza nazionale, militare, economica o ecologica": tali scopi, non meglio definiti o specificati, aprivano ad un uso pressoché sconfinato e genericamente determinato dello strumento delle intercettazioni.

La Corte, dichiarata quindi l'assenza del requisito della 'prevedibilità', si è poi dedicata ad uno studio puntuale e meticoloso degli aspetti preminenti della normativa in esame, alla luce dei già collaudati requisiti del caso *Weber*[18], valutando la procedura autorizzativa prevista per l'adozione delle misure di

[16] Non viene pertanto richiesta la predisposizione di una lista completa delle condotte per le quali un soggetto può essere sottoposto a sorveglianza, nella consapevolezza che le minacce alla sicurezza nazionale possono essere estremamente varie e difficili da definire in anticipo (come già rilevato nella pronuncia *Kennedy*). Tuttavia, per evitare che una simile 'flessibilità' della normativa sfoci nella attribuzione di un potere ed una discrezionalità illimitati nelle mani del legislatore o degli organi dell'esecutivo, viene ritenuto necessario che la legge indichi con precisione e chiarezza le modalità di esercizio di tale potere, fissando così dei limiti capaci di garantire un sufficiente margine di prevedibilità.

[17] La normativa, infatti, utilizzava espressioni generiche quali "a person who may have information about a criminal offence", "a person who may have information relevant to the criminal case", o "events or activities endangering Russia's national, military, economic or ecological security".

[18] I programmi di sorveglianza devono stabilire condizioni minime di salvaguardia e garanzia, quali la definizione della natura dei reati che possono dare luogo ad intercettazione; la determinazione delle persone che possono essere sottoposte ad intercettazione; i limiti di durata delle operazioni di raccolta dati; la disciplina della procedura di esame, trattazione e conservazione dei dati; le salvaguardie che devono essere messe in campo per il trasferimento di dati ad altri soggetti; le circostanze sulla base delle quali i dati possono o devono essere distrutti. Questa sentenza

sorveglianza, il procedimento di notifica e la disponibilità di rimedi a livello nazionale. Al termine di tale dettagliata disamina, la normativa russa viene nuovamente trovata priva di quelle adeguate ed efficaci garanzie contro i rischi di abusi che si rendono ancor più necessarie con riferimento a sistemi di sorveglianza, come quello analizzato, che prevedono l'accesso diretto da parte delle autorità pubbliche a tutte le comunicazioni telefoniche, relative alla totalità degli utenti. Tale incapacità della legislazione di fornire le garanzie necessarie in una società democratica ha fatto quindi concludere i giudici per la sussistenza di una violazione dell'art. 8 CEDU. Pur non potendo ripercorrere in questa sede tutte le criticità individuate nella lunga pronuncia, si vogliono tuttavia sottolineare alcuni rilievi della Corte, che rivestiranno particolare importanza al fine di meglio comprendere l'evoluzione della giurisprudenza nei casi successivamente decisi. Ebbene i giudici di Strasburgo hanno posto particolare attenzione alle disposizioni volte a disciplinare le tempistiche e le modalità delle intercettazioni nonché la conservazione e le procedure di cancellazione e distruzione dei dati raccolti. Sotto il profilo della *data retention*, veniva stabilito dalla normativa russa un termine massimo di conservazione di sei mesi di tutte le informazioni intercettate, indipendentemente dal fatto che esse fossero di una qualche rilevanza per il raggiungimento degli obiettivi posti alla base delle operazioni di raccolta stesse: la Corte ha ritenuto, con una affermazione di grande rilievo, che "the automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8. At the same time, it deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained (compare *Klass and Others*, cited above, § 52, and *Kennedy*, cited above, § 162)" (par. 255, *Zakharov*). La disciplina in materia di conservazione prevedeva poi una *retention* oltre il termine di sei mesi per i dati appartenenti a soggetti successivamente sottoposti ad indagine e processo: anche con riferimento a queste disposizioni la Corte EDU ha rinvenuto forti criticità in termini di chiarezza e prevedibilità della normativa nella parte in cui veniva attribuita al giudice una illimitata discrezionalità quanto al se e quando disporre la distruzione delle intercettazioni, ben potendo anche optare per una conservazione protratta oltre il termine del processo a carico dell'indagato (par. 256).

Anche la previa autorizzazione da parte di una autorità giudiziaria è risultata, a seguito del vaglio della Corte, una misura inefficace ed estremamente limitata nella sua pratica attuazione, soprattutto alla luce del fatto che i giudici nazionali non erano chiamati ad effettuare un controllo circa la sussistenza di un "ragionevole sospetto"[19] quale giustificazione dell'ingerenza nella sfera privata. Diversamente dalle precedenti decisioni *Weber* e *Liberty*, che non prendevano in considerazione tale aspetto, la Corte per la

---

risulta di estrema importanza proprio perché vengono in essa fissati con chiarezza i requisiti e criteri rilevanti al fine della valutazione di conformità alla CEDU di una normativa nazionale in materia di sorveglianza di massa. Le linee guida ed indicazioni elaborate in questa pronuncia sono infatti state ampiamente utilizzate e richiamate nelle successive decisioni, da *Liberty* a *Zakharov*, da *Szabo* fino alle più recenti *Centrum For Rattvisa* e *Big Brother Watch*, nelle quali, non a caso, i ricorrenti hanno invocato una modifica ed un ripensamento di tali criteri ritenuti ormai vetusti e, per certi versi, superati dalle sempre più complesse sfide frutto del progresso tecnologico. Sul punto si rimanda comunque sin da ora a F. DUBUISSON, *La Cour européenne des droits de l'homme et la surveillance de masse*, in *Revue Trimestrelle des droits de l'homme*, 108, 2016.

[19] La Corte EDU ha sottolineato come nei procedimenti autorizzativi i giudici russi non abbiano mai effettuato un vaglio sostanziale delle richieste, basato cioè sulla sussistenza di criteri quali il ragionevole sospetto o il rispetto dei principi di necessità e proporzionalità: "It transpires from the analytical notes issued by District Courts that interception requests are often not accompanied by any supporting materials, that the judges of these District Courts never request the interception agency to submit such materials and that a mere reference to the existence of information about a criminal offence or activities endangering national, military, economic or ecological security is considered to be sufficient for the authorisation to be granted. An interception request is rejected only if it is not signed by a competent person, contains no reference to the offence in connection with which interception is to be ordered, or concerns a criminal offence in respect of which interception is not permitted under domestic law" (par. 263). Per una più ampia lettura di questa pronuncia e dei numerosi rilievi in essa contenuti, si rimanda anche a M. PALMISANO, *The surveillance cold war: recent decisions of the ECtHR and their application to mass surveillance in the USA and Russia*, in *Journal of International Law*, 2, 2017.

prima volta ha specificato in questa pronuncia la necessità del criterio del *reasonable suspicion*; esso infatti risulta determinante ai fini di limitare l'ampiezza dell'autorizzazione – e dunque, conseguentemente, dell'intercettazione stessa – concessa dall'organo giudiziario. Laddove il vaglio preventivo dei giudici non sia basato su informazioni relative allo specifico soggetto da intercettare e neppure sulla durata della sorveglianza, ne deriva inevitabilmente che la misura autorizzata avrà una ampia estensione, non potendo essere circoscritta a specifici soggetti o categorie di individui ma al contrario potendo riguardare tutte le comunicazioni telefoniche interessanti un'area territoriale e una fascia temporale anche estremamente vaste. Questa mancata specificità del procedimento autorizzativo e delle informazioni messe a disposizione dalle autorità richiedenti e sottoposte al controllo dei giudici, si traduce necessariamente in una ampia discrezionalità delle autorità pubbliche nella determinazione dei modi e tempi delle intercettazioni, con ciò limitando, se non addirittura svilendo, l'efficacia della tutela rappresentata dallo strumento della previa autorizzazione[20].

La normativa russa inoltre è stata considerata carente anche con riferimento alla fase dei controlli *ex post*: non solo tale delicata funzione veniva assegnata ad una pluralità di soggetti privi del requisito fondamentale dell'indipendenza dal potere esecutivo, ma il procedimento stesso di revisione successiva è stato ritenuto nel complesso lacunoso e, in taluni casi, difficilmente attivabile. Ciò diviene evidente se si considera che le intercettazioni effettuate nell'ambito delle operazioni di *counter-intelligence* – volte cioè a proteggere i programmi di intelligence di un'agenzia nazionale da attacchi perpetrati da agenzie di intelligence straniere – potevano essere oggetto di controllo successivo solo a seguito di un ricorso azionato da chiunque lamentasse una lesione dei propri diritti. Considerato però che non era previsto alcun meccanismo di notifica a beneficio dei cittadini, finalizzato a metterli al corrente di essere stati sottoposti ad intercettazione, risultava di fatto del tutto impossibile promuovere azioni avverso tali sistemi di sorveglianza[21]. Pur specificando l'impossibilità di provvedere, in talune occasioni, a notifica senza che ciò metta a rischio l'utilità e il successo stesso della misura di controllo posta in essere, i giudici di Strasburgo hanno evidenziato come l'obbligo di informazione non sia *per se* fondamentale ma possa divenirlo laddove rappresenti una precondizione essenziale per attivare i rimedi giudiziari. In altre parole, viene affermato lo stretto legame intercorrente tra la notifica e la reale e concreta possibilità di accesso a forme di controllo *ex post*: "in Russia persons whose communications have been intercepted are not notified of this fact at any point or under any circumstances. It follows that, unless criminal proceedings have been opened against the interception subject and the intercepted data have been used in evidence, or unless there has been a leak, the person concerned is unlikely ever to find out that his communications have been intercepted" (par. 289); l'assenza di notifica quindi, sempre letta congiuntamente alla capacità di azionare controlli dinnanzi alle autorità giudiziarie, non solo impedisce di prendere coscienza della invasione subìta nella sfera privata, ma non consente neppure all'individuo che ritenga di essere stato sottoposto ad intercettazioni di provare, come richiesto dalla legge, l'esistenza di una interferenza nei propri diritti personali. Questo circolo vizioso si traduce dunque in una considerevole compromissione, nei fatti, del corretto e concreto funzionamento di un sistema di tutele delle prerogative individuali e dei principi dello stato di diritto.

In conclusione la Grande Camera, pur non condannando *per se* la creazione di sistemi di sorveglianza per scopi securitari, considera sussistente una violazione dell'art. 8 CEDU, ribadendo non solo la necessità di cornici normative capaci di garantire idonee salvaguardie volte a limitare l'invasione della sfera privata a quanto necessario e proporzionato in una società democratica, ma anche aggiungendo e chiarendo alcuni fondamentali requisiti, da quello di un previo controllo giudiziario, fondato su elementi,

[20] Sul punto si legga anche V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroad*, op. cit., p. 6.

[21] Sull'importanza della notifica come fondamentale strumento di salvaguardia nei sistemi di sorveglianza, si legga: P. DE HERT, F. BOEHM, *Notification, an important safeguard against the improper use of surveillance finally recognized in case law and EU law*, in *European Journal of Law and Technology*, 3, 2012.

quali il ragionevole sospetto, capaci di circoscrivere le dimensioni delle misure di sorveglianza, fino alla concreta predisposizione di effettivi ed efficaci rimedi *ex post*.

1.2. – La normativa anti-terrorismo ungherese al vaglio dei giudici di Strasburgo: la decisione **Szabo**

In continuità con quanto affermato in *Zakharov* e coerentemente alla linea interpretativa in essa individuata, è possibile collocare la sentenza *Szabo* con la quale la Corte EDU è stata nuovamente chiamata a confrontarsi con complesse misure di sorveglianza segreta per fini securitari, pronunciandosi in questa occasione sulla normativa ungherese anti-terrorismo. Quest'ultima[22] prevedeva la possibilità, da parte della c.d. *Anti-Terrorism Task Force*, di attuare forme di controllo diretto della corrispondenza privata, di sorveglianza di soggetti target, di conservazione e accesso al contenuto di telecomunicazioni e di perquisizioni segrete del domicilio, limitatamente a due scopi: prevenzione di attacchi terroristici e protezione della sicurezza nazionale da un lato e salvataggio di cittadini ungheresi catturati all'estero in zone di guerra o da terroristi dall'altro. Tali operazioni potevano essere autorizzate dal Ministero della Giustizia per un periodo – prorogabile – di 90 giorni e solo nei casi in cui non risultasse possibile ottenere diversamente e con mezzi meno invasivi le medesime informazioni.

Dopo aver esperito tutti i gradi di giudizio interni[23], due membri di una ONG ungherese si sono rivolti alla Corte EDU la quale, richiamando ampiamente i principi individuati nella previa decisione *Zakharov*, ha innanzitutto determinato l'ammissibilità del ricorso[24]. I giudici, ribadendo la forte invasività delle misure di sorveglianza rispetto al diritto tutelato dall'art. 8 CEDU[25], sono passati poi alla valutazione dei requisiti "accordance with the law" e "necessity", già ampiamente affermati nella sua previa giurisprudenza in materia. Ritenendo indiscussa sia la sussistenza di una base normativa accessibile e conoscibile, sia la legittimità dello scopo cui le disposizioni erano preposte (sicurezza nazionale e prevenzione di disordini), aspetto peraltro non contestato da nessuna delle parti, ciò che ha invece maggiormente impegnato i giudici è stata l'analisi della necessità delle misure in esame in una società democratica. Utilizzando i criteri individuati nella sentenza *Weber* e nella *Zakharov*, la Corte ha nuovamente posto grande attenzione alla 'foreseeability' e dunque alla prevedibilità della normativa, mediante la predisposizione di indicazioni chiare e precise degli scopi e delle modalità di esercizio delle

[22] Section 7/E (3) del Police Act, n. XXXIV del 1994 ed emendato nel 2011, connesso al National Security Act n. CXXV del 1995 (occorre precisare come in questa sede vengano impiegati i termini tradotti in lingue inglese nella versione utilizzata dai giudici di Strasburgo).

[23] Di particolare interesse è la pronuncia della Corte costituzionale ungherese (18 novembre 2013) che, pur ribadendo la necessità di accompagnare l'adozione di misure di sorveglianza con motivazioni esaustive, ha ritenuto conclusivamente e complessivamente legittima la più ampia invasività nella sfera privata causata da strumenti di sorveglianza volti a tutelare la sicurezza nazionale: secondo il ragionamento dei giudici costituzionali, tali misure, per loro natura e proprio in considerazione della vitale finalità cui sono preposte, non sempre possono essere fondate e motivate sulla base di sospetti ragionevoli e delimitate alla prevenzione e contrasto di un crimine specifico.

[24] La Corte EDU, infatti, ha riconosciuto lo status di vittime dei ricorrenti valutando i due criteri già affermati nella precedente pronuncia: innanzitutto i giudici hanno stabilito che, sulla base della normativa ungherese, qualunque cittadino risultava potenzialmente assoggettabile a misure di sorveglianza in quanto utente di sistemi di telecomunicazione (par. 38); quanto poi alla sussistenza di efficaci rimedi a livello nazionale, il sistema ungherese non consentiva a coloro che avessero ritenuto di essere sottoposti ad intercettazioni la possibilità di presentare ricorso ad una autorità indipendente. Nulla di innovativo dunque deve essere rilevato con riferimento a questo profilo iniziale, rispetto al quale i giudici hanno ricalcato e applicato i principi già definiti nel caso *Zakharov*.

[25] Particolarmente interessante è l'affermazione della Corte che, in tema di misure di sorveglianza segreta, ribadisce: "this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence" (par. 53, *Szabo*).

attività di sorveglianza poste in essere[26]. Sulla base di questa lettura del criterio di prevedibilità, la normativa esaminata non offriva, nel suo complesso, sufficienti salvaguardie a protezione dei diritti fondamentali: ogni cittadino ungherese era infatti potenzialmente assoggettabile a sorveglianza poiché la legge non prevedeva alcuna delimitazione dei soggetti (o delle specifiche categorie di soggetti) sottoponibili a controllo, senza dunque richiedere l'esistenza di un *individual suspect*. Sebbene vi fosse una disposizione nella normativa ungherese che obbligava le autorità pubbliche ad individuare "either by name or as a range of persons" coloro che dovevano essere interessati da intercettazioni o simili misure, i giudici di Strasburgo non hanno mancato di evidenziare i limiti e le criticità di tale espressione, talmente ampia da poter includere chiunque, aprendo potenzialmente le porte ad una sorveglianza illimitata ed estesa ad un amplissimo numero di destinatari. A ciò si aggiunga il fatto che non era neppure stabilito il dovere in capo alla *Task force* di dimostrare la concreta o presunta relazione tra le persone – o il gruppo di persone – da sottoporre a sorveglianza da un lato e la prevenzione di minacce terroristiche dall'altro. Ed ecco che la Corte, sul punto, ha proposto una lettura di grande rilievo, fortemente concreta ma al contempo consapevole dell'esigenza di bilanciare le finalità securitarie con la tutela e protezione dei diritti: una lettura che ben può essere considerata una sorta di sunto dell'approccio dei giudici dinnanzi al tema controverso e complesso dell'utilizzo di sistemi di sorveglianza di massa quale risposta alla emergenza 'normalizzata' del terrorismo internazionale. Lasciando quindi parlare la Corte stessa: "For the Court, it is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents. The techniques applied in such monitoring operations have demonstrated a remarkable progress in recent years and reached a level of sophistication which is hardly conceivable for the average citizen, especially when automated and systemic data collection is technically possible and becomes widespread. *In the face of this progress the Court must scrutinise the question as to whether the development of surveillance methods resulting in masses of data collected has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights*" (par. 68, enfasi aggiunta)[27]. Sulla base di questo approccio i giudici sono così giunti ad affermare che, benché distinti, il criterio di 'necessità per una società democratica' e quello di 'stretta necessità' sono da considerarsi fortemente interrelati: le misure di sorveglianza segreta risultano conformi alla CEDU e dunque 'necessarie in una società democratica' solo se *strettamente necessarie* al reperimento di informazioni vitali per la salvaguardia delle istituzioni democratiche stesse. È alla luce di questa interpretazione che sono state quindi vagliate le disposizioni della normativa ungherese, trovata carente sotto il profilo della possibilità incontrollata ed illimitata di proroga del periodo di intercettazione e della assenza di una previa supervisione da parte di autorità giudiziarie in grado di valutare la sussistenza di un legittimo scopo, unitamente al rispetto del requisito di stretta necessità. Pur affermando come, in linea generale, una autorizzazione *ex ante* ad opera di una autorità giudiziaria o quasi-giudiziaria non sia da considerarsi obbligatoria in assoluto, ben potendo

[26] In particolare è stato riaffermato come, nello specifico contesto delle misure di sorveglianza segreta, tale requisito non possa tradursi né in una completa e sconfinata arbitrarietà in capo alle autorità pubbliche, né nella predisposizione di norme eccessivamente dettagliate, che sconterebbero il limite di una sproporzionata rigidità dinnanzi a circostanze ed esigenze fattuali in rapido mutamento e difficilmente prevedibili.

[27] La Corte poi prosegue: "These data often compile further information about the conditions in which the primary elements intercepted by the authorities were created, such as the time and place of, as well as the equipment used for, the creation of computer files, digital photographs, electronic and text messages and the like. Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information" (par. 68, *Szabo*).

essere controbilanciata da un estensivo controllo giudiziario *post factum*, la Corte ha ritenuto invece tale controllo preventivo assolutamente necessario con riferimento a specifiche circostanze, ad esempio nel caso di sorveglianza segreta riguardante i *media*: in tale circostanza, l'ingerenza ed incidenza nei diritti di libertà di espressione, diritto di informazione e, in ultima analisi, sulla democraticità della società stessa, sono tali da richiedere un innalzamento del livello delle tutele e delle salvaguardie. Accanto a tali lacune, è stata poi rilevata dai giudici anche la mancanza di un debito controllo sulle attività di sorveglianza effettuato *a posteriori* da una autorità indipendente, indipendenza che non viene riscontrata nel Ministro della Giustizia, deputato a tale controllo secondo quanto previsto dalla normativa ungherese: questo vaglio viene riconosciuto come necessario sia nei casi di intercettazioni targettizzate sia in quelli di supervisione generalizzata, nonché rispetto a misure di sorveglianza adottate in situazioni e per ragioni di particolare emergenza. La sentenza poi prosegue ponendo attenzione ad una ulteriore salvaguardia di fondamentale importanza, individuata nella notifica agli individui interessati da controllo: ribadendo il già affermato stretto legame tra notifica ed efficacia dei rimedi, la Corte ha condannato l'assenza di qualsiasi forma di comunicazione ai cittadini sottoposti a misure di sorveglianza, mancante anche nel momento in cui una tale conoscenza non sia più in grado di compromettere lo svolgimento delle operazioni di sorveglianza stesse e il raggiungimento dello scopo da esse perseguito. Rilevate tutte queste gravi carenze nella normativa ungherese, è stata infine dichiarata la sussistenza di una violazione dell'art. 8 CEDU.

1.3. – Primi mutamenti nell'orientamento della Corte EDU: le sentenze del 'primo gruppo' tra rigidi criteri di 'necessità in una società democratica' e alcune divergenze

Con queste due pronunce, che hanno portato allo stesso negativo esito per entrambe le normative sottoposte al vaglio della Corte, sono stati tracciati con chiarezza e – in gran parte – coerenza alcuni principi di grande rilievo, da rinvenirsi sinteticamente a) nella determinazione dei criteri volti a riconoscere ad un soggetto lo status di vittima e quindi l'ammissibilità del ricorso; b) nel riconoscimento della salvaguardia della sicurezza nazionale ma anche della prevenzione e repressione di crimini (quanto meno nel caso russo, anche di non grave entità) quali scopi legittimi giustificanti misure di sorveglianza; c) nella accettazione di forme di sorveglianza segreta – che non vengono negate *tout court* – purché esse siano accompagnate da debite salvaguardie e garanzie dei diritti fondamentali; d) nella necessità di controlli *ex ante* e/o *ex post* (a seconda della lesività e dell'ingerenza nel diritto colpito), che debbono assumere carattere effettivo ed efficace e non meramente illusorio e teorico (così *Zakharov*, par. 288); e) nell'indipendenza dell'autorità preposta ai controlli; f) nella previsione di forme di notifica laddove ciò sia essenziale per consentire un concreto accesso ai rimedi giudiziari da parte del soggetto interessato[28].

Accanto a tutti questi elementi comuni, non possono però essere taciute anche alcune differenze tra l'interpretazione fornita dalla Grande Camera nel caso *Zakharov* e quella della Quarta Camera nel caso *Szabo*. Una prima divergenza, rilevata e criticata anche nella *Concurring Opinion* del giudice Pinto De Albuquerque con riferimento alla pronuncia *Szabo*, attiene al criterio del 'sospetto' inteso quale elemento giustificante l'ingerenza della sorveglianza nella vita privata di un soggetto o di una categoria

[28] Tale approccio è stato peraltro richiamato nella sentenza *Barbulescu c. Romania*, ricorso n. 61496/08, deciso prima dalla Quarta Camera (12 gennaio 2016) e poi dalla Grande Camera (5 settembre 2017). Come ben affermato nella *Concurring Opinion* del giudice Pinto de Albuquerque, seppure con riferimento allo specific caso della sorveglianza nei luoghi di lavoro: "Unconsented collection, access and analysis of the emplyee's communications, including metadata, may be permitted only exceptionally, with judicial authorisation, since employees suspected of policy breaches in disciplinary or civil proceedings must not be treated less fairly than presumed offenders in criminal procedure. Only targeted surveillance in respect of well-founded suspicions of policy violations admissible, with general, unrestricted monitoring being manifestly excessive snooping on employees", par. 13.

di soggetti. Mentre nella sentenza *Zakharov*, infatti, i giudici hanno parlato di *reasonable suspicion*, nella successiva pronuncia la Quarta Camera utilizza la locuzione *individual suspicion*: nonostante tale requisito venga quindi affermato e richiesto in entrambe le decisioni, l'entità del 'sospetto' passa da quello basato sulla ragionevolezza (*reasonable* appunto) ad un sospetto 'individuale', dai contorni non meglio chiariti e che il giudice Pinto De Albuquerque per questo definisce "vague, anodyne, unqualified" (par. 35), sottolineandone il potenziale pericoloso impatto rispetto ai criteri della previa autorizzazione e del controllo giudiziario *ex post*. Il rischio infatti è che, con tale abbassamento del 'livello di sospetto' richiesto, non più necessariamente ragionevole, "it will suffice to launch the heavy artillery of State mass surveillance on citizens, with the evident risk of the judge becoming a mere rubber-stamper of the governmental social-control strategy" (par. 35), con la conseguenza che "a ubiquitous 'individual suspicion' equates to overall suspicion, i.e., to the irrelevance of the suspicion test at all" (par. 35). Sulla base della interpretazione emersa dalla *Concurring Opinion*, la Corte giungerebbe a depotenziare il criterio stesso del sospetto e del legame tra ingerenza e scopo perseguito, ammettendo *volenti nolenti* una forma generalizzata di 'strategic surveillance', in contrasto con la posizione adottata della Grande Camera nella pronuncia *Zakharov* che, imponendo la sussistenza di un ragionevole sospetto, limitava *de facto* la generalità ed estensione della sorveglianza.

Oltre a questo aspetto, una ulteriore difformità tra le due pronunce può essere rilevata nel diverso test effettuato nel caso *Szabo*, nel quale viene richiamato il concetto di stretta necessità: nella *Concurring Opinion* sopra richiamata, il giudice Pinto De Albuquerque non manca di criticare da un lato l'assenza di coerenza tra la richiesta di un test di stretta necessità e il criterio ambiguo e ampio dell'*individual suspicion*[29], e dall'altro la definizione fornita di 'stretta necessità', per la quale è sufficiente che la sorveglianza persegua lo scopo di "safeguarding of democratic institutions and the acquiring of vital intelligence in an individual operation"[30]. Questa accezione ed interpretazione di 'stretta necessità' infatti risulta meno rigida e maggiormente ampia rispetto ai criteri delineati dalla Grande Camera in *Zakharov*, che parlava di valutazione della 'accordance with the law' e 'necessity requirements' (par. 230-236). I giudici della Quarta Camera inoltre non chiariscono in cosa il test di stretta necessità, così vagamente definito, si sostanzi e neppure se esso integri una considerazione circa l'impossibilità da parte delle autorità di raggiungere il medesimo scopo con misure meno intrusive della sfera privata. Merita però sottolineare come il ricorso a tale test di 'stretta necessità', diversamente da quanto espresso dal giudice Pinto De Albuquerque, sia stato al contrario apprezzato da taluni commentatori che hanno visto in esso una ulteriore limitazione, più chiara ed estesa, del margine di apprezzamento e discrezionalità lasciato a ciascuno Stato: "Le critère de stricte nécessité interviendra donc tant pour apprécier la légalité de la mesure en son principe qu'au regard des «garde-fous » qui l'entourent"[31].

Al di là di questi rilievi e nonostante le diversità rispetto alla pronuncia *Zakharov*, il giudizio della Quarta Camera non è stato comunque impugnato dai ricorrenti e non è stato pertanto ritenuto necessario fornire alla Grande Camera la possibilità di chiarire i due punti maggiormente criticati e dubbi ovvero il contenuto del criterio di stretta necessità o la portata del sospetto richiesto.

Quel che è incontestabile è il fatto che la Corte, in entrambe le pronunce esaminate, abbia vagliato le misure di sorveglianza adottate dai diversi Stati partendo dalla consapevolezza e dal dato concreto

[29] "It does not match the looser criterion for the degree of suspicion of involvement in the offences or activities being monitored. It is logically inconsistent that the same judgment imposes a 'strict necessity' test for the determination of the surveillance measure, but at the same time accepts a very loose criterion for the degree of suspicion of involvement in the offences or activities being monitored, as demonstrated above. It is logically incoherent to criticise the overly broad text of the Hungarian law when it refers to the 'persons concerned identified as a range of persons' and yet to accept the linguistically vague and legally imprecise 'individual suspicion' test to ground the applicability of a surveillance measure", par. 20, Concurring Opinion, *Szabo*.

[30] Par. 21, Concurring Opinion, *Szabo*.

[31] F. DUBUISSON, *La Cour européenne des droits de l'homme et la surveillance de masse*, in *Revue Trimestrelle des droits de l'homme*, op. cit., p. 883.

che vede un utilizzo sempre più espansivo di queste tecniche dinnanzi alla minaccia 'normalizzata' del terrorismo, considerandole dunque non di per sé illegittime nella loro natura bensì accettandone l'esistenza "under exceptional conditions" (par. 80, *Szabo*) e purché accompagnate da un quadro normativo di garanzie complesso ed articolato, capace di salvaguardare i diritti fondamentali. Sulla base dei requisiti richiesti (tra cui l'esistenza di un sospetto che giustifichi l'intercettazione, una autorizzazione a priori e/o a posteriori a seconda della ingerenza, l'obbligo di notifica, il rispetto del principio di stretta necessità, un controllo successivo da parte di un'autorità indipendente) pare che la Corte sia giunta, *de facto*, ad escludere la possibilità di sistemi di sorveglianza di massa generalizzata ed indiscriminata, imponendo condizioni stringenti che, nei fatti appunto, limitano l'ampiezza della sorveglianza e del controllo possibili; del resto i giudici di Strasburgo già nella richiamata sentenza *Kennedy* avevano escluso la sussistenza di una violazione dell'art. 8 CEDU da parte di sistemi di sorveglianza proprio grazie al fatto che la normativa analizzata in quella sede non autorizzava una raccolta indiscriminata di un vasto numero di comunicazioni. Nel caso *Szabo* è stato poi ribadito come "the Court considers that, in the absence of specific rules to that effect or any submissions to the contrary, it cannot be ruled out that the broad-based provisions of the National Security Act can be taken to enable so-called strategic, large-scale interception, which is a matter of serious concern" (par. 69). È indicativo sul punto anche il continuo ed ampio richiamo alla decisione *Schrems* della CGUE o ad alcune dichiarazioni espresse dalle Istituzioni dell'UE, quali la Risoluzione del 12 marzo 2014 del Parlamento Europeo, già citata nel Capitolo III e riferita ai programmi di sorveglianza utilizzati dalla NSA statunitense, nonché a documenti quali il Report del 2013 elaborato dallo Special Rapporteur ONU per la promozione e protezione del diritto alla libertà di opinione ed espressione, nel quale viene più volte ribadita la condanna di forme di sorveglianza indiscriminata[32]. Certo, diversamente dalla CGUE che in *Schrems* aveva affermato chiaramente come forme di accesso indiscriminato al contenuto di comunicazioni elettroniche andassero a ledere il contenuto essenziale del diritto alla riservatezza e come non potesse essere considerata limitata allo stretto necessario una normativa che consentiva una conservazione generalizzata ed indiscriminata, la Corte EDU non è giunta ad una simile netta presa di posizione[33], imponendo però requisiti e criteri che nei fatti imbrigliano fortemente il margine di apprezzamento degli Stati e la loro possibilità di adottare sistemi di sorveglianza totalmente indiscriminata, optando per misure di controllo più limitate e motivate da un legame concreto tra sorveglianza e obiettivo perseguito.

[32] Interessante è il richiamo alla citata Risoluzione, nella quale, come riportato al Par. 25, il Parlamento europeo "Condemns the vast and systemic blanket collection of the personal data of innocent people, often including intimate personal information; emphasises that the systems of indiscriminate mass surveillance by intelligence services constitute a serious interference with the fundamental rights of citizens; *stresses that privacy is not a luxury right, but is the foundation stone of a free and democratic society*" (enfasi aggiunta).

[33] Come già anticipato e come si vedrà più ampiamente nei prossimi paragrafi, il parallelo tra le pronunce della Corte EDU e quelle della CGUE deve sempre essere svolto con grande attenzione e tenendo conto delle peculiarità specifiche che contraddistinguono i due casi e la differente posizione delle due Corti; certamente quanto trattato nel caso *Schrems*, avente ad oggetto l'adeguatezza del sistema di tutele della privacy e protezione dei dati fornite dall'ordinamento statunitense, soprattutto a fronte delle svelate operazioni di sorveglianza di massa perpetrate dalla NSA è ciò che più si avvicina a quanto analizzato dalla Corte EDU nelle normative russe e ungherese: tutti questi sistemi, infatti, prevedono intercettazioni aventi ad oggetto anche il contenuto delle comunicazioni, diversamente dai casi *DRI* o *Tele2* che concernono invece i soli metadati. Le operazioni disciplinate dalle normative russe e ungherese, tuttavia, sono svolte prettamente per scopi di tutela della sicurezza nazionale, direttamente dalle autorità di intelligence, diversamente dai casi affrontati dalla CGUE che si concentrano principalmente sulle finalità di prevenzione e repressione di crimini gravi e su sistemi di sorveglianza che prevedono l'intervento di soggetti privati e l'accesso a informazioni da questi raccolte e conservate per finalità diverse da quelle securitarie.

1.4. – Un cambio di paradigma? Le più recenti pronunce Centrum For Rattvisa *e* Big Brother Watch

1.4.1. – Il caso Centrum For Rattvisa *e la compatibilità rispetto alla Convenzione EDU delle operazioni di* Foreign Intelligence*: la peculiare normativa svedese*

Successivamente alle due decisioni sopra analizzate, la Corte EDU è stata chiamata a pronunciarsi su sistemi di *bulk interception*, dunque di raccolta ed intercettazione generalizzata di dati effettuata direttamente da autorità di intelligence per finalità esclusive di sicurezza nazionale: le due rilevanti sentenze, adottate a pochi mesi di distanza l'una dall'altra, *Centrum For Rattvisa* e *Big Brother Watch* hanno investito rispettivamente la Terza e la Prima Camera e, come anticipato, sono state entrambe oggetto di ricorsi innanzi alla Grande Camera, al momento pendenti.

Partendo dunque con l'analisi della prima di questo secondo gruppo di sentenze, delle quali si evidenzieranno poi i punti di contatto nonché le divergenze rispetto alle pronunce sino ad ora esaminate, il caso portato dinnanzi alla Corte dalla ONG svedese Centrum For Rattvisa, dopo aver esperito senza successo i ricorsi innanzi alle Corti nazionali, aveva ad oggetto la normativa svedese in materia di *Signals Intelligence*. Quest'ultima rappresenta una delle tipologie di operazioni messe in campo nell'ambito delle attività di *Foreign Intelligence*[34] per finalità di tutela della sicurezza nazionale e consiste nella intercettazione, trattamento, controllo e analisi di 'segnali' (riguardanti dunque sia i metadati che i contenuti delle comunicazioni) derivanti dalle telecomunicazioni e diretti o provenienti dall'estero[35]: vengono pertanto esclusi dall'ambito di applicazione della normativa in esame sia operazioni di raccolta di intelligence (informazioni) per scopi di *law enforcement* e sicurezza pubblica[36], che la sorveglianza di comunicazioni svolte unicamente tra cittadini svedesi, all'interno del territorio nazionale[37]. Più nel dettaglio, tale sistema comporta che ogni comunicazione che oltrepassi in entrata o

[34] "Foreign intelligence is, according to the Foreign Intelligence Act (*Lagen om försvarsunderrättelseverksamhet*; 2000:130), conducted in support of Swedish foreign, defense and security policy, and in order to identify external threats to the country" (par. 8, *Centrum for Rattvisa*).

[35] Il termine di 'foreign' intelligence fa riferimento alle operazioni di intelligence riguardanti segnali elettronici che oltrepassano il confine nazionale, escludendo quindi le misure relative a comunicazioni avvenute tra soggetti che si trovano unicamente nel territorio svedese. Pare opportuno comunque sin da ora sottolineare la problematicità di una tale concezione: come da più parti rilevato, la determinazione del confine tra sorveglianza 'esterna' e servizi di intelligence interni è piuttosto complessa e la possibilità di addivenire ad una netta distinzione risulta estremamente affievolita se non addirittura superata soprattutto alla luce di fenomeni di terrorismo internazionale: "With the development of digital communications, national borders (i.e. the indications of what is foreign and what is national) are more difficult to identify. Furthermore, national security threats are not only posed by states, but also by terrorist groups and organised crime networks", FRA (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume I: Member States' legal framework*, 2017, p. 13.

[36] Come si avrà modo di vedere nel paragrafo successivo e come già anticipato anche nei Capitoli precedenti, la distinzione tra sicurezza pubblica e attività di *law enforcement* da un lato e sicurezza nazionale dall'altro non appare più così chiara e definibile come in passato; si pensi che la normativa svedese in esame prevede: "authorities that conduct foreign intelligence may support authorities dealing with law enforcement or crime prevention", sfumando dunque ulteriormente i confini tra le due attività e gli strumenti utilizzati.

[37] Come è già stato ribadito, affinché tale sorveglianza rientri nella categoria di 'Foreign Intelligence', è necessaria la sussistenza di un elemento di 'estraneità' rispetto alla dimensione interamente nazionale, da individuarsi appunto nella natura transfrontaliera delle comunicazioni soggette a controllo. Per una definizione generale di 'Signals Intelligence' si rimanda invece alla Corte EDU stessa, che nella pronuncia in esame ha affermato: "Signals intelligence can be defined as intercepting, processing, analysing and reporting intelligence from electronic signals. These signals may be processed to text, images and sound. The intelligence collected through these procedures may concern both the content of a communication and its associated communications data (the data describing, for instance, how, when and between which addresses the electronic communication is conducted). The intelligence may be intercepted over the airways – usually from radio links and satellites – and from cables. Whether a signal is transmitted over the airways or through cables is controlled by the communications service

uscita il confine nazionale venga automaticamente captata e trasferita ad un punto di raccolta, nel quale però le informazioni non sono immagazzinate nella loro totalità bensì solamente vagliate e trattate: al termine di tale preliminare operazione, svolta sulla base di specifici criteri, solo una parte limitata delle informazioni intercettate sarà oggetto di trasferimento all'autorità di intelligence preposta (*Försvarets radioanstalt*, d'ora in avanti FRA) per ulteriore conservazione e analisi. Tutte queste attività debbono essere fondate e disciplinate da istruzioni e ordini dettagliati emanati dal Governo, da suoi uffici o dalle Forze Armate; con riferimento a tali atti, il 'Signals Intelligence Act' (*Lagen om signalspaning i försvarsunderrättelseverksamhet*; 2008:717, emendato da ultimo nel 2016) conteneva un preciso e specifico elenco di elementi ed informazioni da inserire necessariamente negli ordini di intercettazione: l'obiettivo da perseguire[38], le motivazioni circa la necessità di reperire informazioni e di attivare operazioni di sorveglianza, specificando che "a detailed tasking directive determines the direction of the intelligence activities and may concern a certain phenomenon or situation, but it may not solely target a specific natural person"; quest'ultimo aspetto risulta essere di grande rilevanza e si rivelerà determinante nello scrutinio della Corte. Diversamente dalle normative russe e ungherese oggetto delle precedenti sentenze, la normativa svedese stabiliva inoltre in capo al FRA l'obbligo di chiedere una preventiva autorizzazione ad una apposita Corte denominata Foreign Intelligence Court (*Försvarsunderrättelsedomstolen*): "the application shall contain the mission request that the FRA has received, with information on the relevant detailed tasking directive and the need for the intelligence sought. Also, the signal carriers to which the FRA requires access have to be specified, along with the search terms or categories of search terms that will be used. Finally, the application must state the duration for which the permit is requested"; la richiesta, così tratteggiata, risultava quindi comprensiva delle indicazione dei *service providers* rispetto ai quali l'accesso alle comunicazioni viene riferito, motivazione, durata, criteri di ricerca e selezione (di cui si parlerà a breve), assumendo dunque caratteri molto specifici e determinati e consentendo così alla Corte di svolgere un vaglio puntuale e approfondito, diversamente da quanto rilevato nei casi *Zakharov* e *Szabo* in cui la mancanza di complete informazioni a disposizione dei giudici nazionali nella fase autorizzativa inficiava l'utilità e l'efficacia stessa del preventivo controllo giudiziale. La normativa svedese inoltre prevedeva espressamente in capo all'autorità giudiziaria designata il compito di accertare, prima di dare il proprio assenso, che lo scopo perseguito dalle misure di *Signal Intelligence* non potesse essere ottenuto con mezzi meno invasivi, richiedendo quindi un vaglio di necessità in senso stretto. Infine, "if granted, the permit shall specify the mission for which signals intelligence may be conducted, the signal carriers to which the FRA will have access, the search terms or categories of search terms that may be used, the duration of the permit and other conditions necessary to limit the interference with personal integrity" (sezione 5a); le operazioni di sorveglianza, superato il vaglio preventivo, potevano pertanto essere effettuate solo entro i precisi limiti dell'autorizzazione della Corte e con una durata (non superiore comunque a sei mesi), scopo e soggetti – o categoria di soggetti sottoposti – ben predefiniti. Venivano inoltre stabilite chiare norme circa la distruzione dei dati raccolti (che potevano essere conservati comunque per un tempo massimo di un anno) nonché circa la creazione di un apposito organo di controllo, il *Foreign Intelligence Inspectorate*, deputato alla supervisione delle attività poste in essere dalla FRA mentre il vaglio delle sole e specifiche operazioni di trattamento dei dati era attribuita all'Autorità garante della protezione dei dati svedese. Sin da questa breve analisi emergono molteplici punti di differenziazione e di distanza tra questa normativa e quelle precedentemente analizzate.

providers. A great majority of the traffic relevant for signals intelligence is cable-based. The term "signal carriers" refers to the medium used for transmitting one or more signals. Unless indicated in the following, the regulation of Swedish signals intelligence does not distinguish between the content of communications and their communications data or between airborne and cable-based traffic" (par. 7, *Centrum for Rattvisa*).

[38] La finalità in ultima istanza doveva comunque essere sempre e solo quella di contrastare fenomeni di terrorismo o altri crimini gravi internazionali in grado di minacciare interessi nazionali essenziali.

Seguendo comunque il ragionamento della Corte EDU, quest'ultima si è occupata inizialmente delle questioni inerenti lo status di vittima dei ricorrenti e l'esistenza di una interferenza nel diritto di cui all'art. 8 CEDU. Sotto questi profili nulla di nuovo è stato affermato dai giudici di Strasburgo, che hanno richiamato nuovamente sul punto la sentenza *Zakharov* (approccio confermato, come si è visto, anche nella pronuncia *Szabo*): l'ubiquità del regime di sorveglianza, che può potenzialmente colpire qualsiasi utente di comunicazioni elettroniche, senza che nulla gli sia comunicato, nonché l'assenza di rimedi a livello nazionale che permettano di dare risposta alle specifiche rimostranze dei singoli, giustificano una eccezionale valutazione della Corte *in abstracto*. L'esistenza poi di una normativa in materia di intercettazioni, di carattere potenzialmente generalizzato, fa ritenere di per sé sussistente una interferenza rispetto al diritto alla riservatezza.

Venendo poi al vaglio sostanziale della normativa, riprendendo ampiamente i requisiti stabiliti nella previa giurisprudenza, è stata ribadita la necessità di limitare il margine di apprezzamento in materia di tutela della sicurezza nazionale riconosciuto agli Stati, imponendo il rispetto di salvaguardie minime da individuarsi nella accessibilità della legge, nella determinazione chiara di finalità e durata delle intercettazioni, nella previsione di procedure autorizzative nonché di procedure specifiche relative all'accesso, conservazione, utilizzo, diffusione e distruzione dei dati intercettati, oltre alla predisposizione di misure di supervisione e di notifica ai soggetti interessati da sorveglianza, unitamente alla messa a disposizione di rimedi giudiziari.

Ritenendo la normativa accessibile, punto sul quale peraltro le parti hanno concordato, la Corte si è concentrata sulle finalità per le quali l'ingerenza nella sfera privata è concessa e, pur riscontrando alcune criticità – ad esempio il dettato normativo eccessivamente ampio o generico nell'elencazione degli scopi –, i giudici hanno ritenuto le disposizioni, considerate nel loro complesso, adeguate[39]. Questo tipo di valutazione, che ricorre spesso nel corso del giudizio e che punta a valutare la regolamentazione nella sua totalità e nel livello di tutela complessivamente garantito, ha destato non poche perplessità, come si vedrà in seguito, soprattutto con riferimento alle misure attinenti ai metadati. Rispetto a questi ultimi e, in particolare, alle disposizioni che ne disciplinano raccolta, trattamento e conservazione, viene infatti riconosciuto un livello di precisione e chiarezza inferiore a quanto previsto per le operazioni di intercettazione del contenuto delle comunicazioni: purtuttavia la Corte ha affermato che tale regolamentazione, dai più ampi contorni e meno specificamente delimitata dalla legge, sia comunque necessaria al corretto funzionamento delle operazioni di intelligence e che la previsione di controlli successivi sia tale da poter ritenere sufficientemente delimitate e correttamente individuate le condizioni di raccolta dei metadati. In altre parole, pur essendo evidenziata una certa lacunosità, la disciplina in materia di metadati risulta proporzionata ed adeguata grazie ad una lettura alla luce della normativa e delle tutele apprestate nel loro complesso. Anche con riferimento alla durata delle intercettazioni, i giudici hanno considerato accettabile e non irragionevole concedere un certo margine di discrezionalità alle autorità, persino sotto il profilo della possibilità di proroga – che era stata invece oggetto di decisa critica nelle sentenze *Szabo* e *Zakharov* – purché accompagnata da adeguate salvaguardie: esaminando infatti le circostanze che dovrebbero portare a fissare un termine finale delle intercettazioni quanto più possibile preciso, la Corte ha ammesso l'assenza di disposizioni chiare nella normativa svedese (par.

[39] Ad esempio in questo caso la Corte considera positivamente il fatto che le operazioni di *Signals Intelligence* possano riguardare solo le comunicazioni che travalicano il confine svedese e che non possano quindi coinvolgere, se non incidentalmente, comunicazioni riguardanti soggetti situati unicamente in Svezia (par. 121 e 122, *Centrum for Rattvisa*); ciò pare presupporre che una sorveglianza come quella descritta, potenzialmente coinvolgente in misura maggiore soggetti stranieri, possa ritenersi più accettabile e 'legittima' rispetto alla raccolta massiva di comunicazioni riguardanti la sola dimensione interna e nazionale. Su tale linea interpretativa, così come sulle problematiche ad esso relative, si rimanda più ampiamente ai rilievi svolti nel successivo paragrafo.

129)[40]; eppure, anche in questo caso, considerando le disposizioni nel loro complesso e tenendo conto che il rinnovo dei termini deve essere sottoposto al vaglio della Corte nazionale preposta, i giudici europei sono infine giunti ad una valutazione positiva della normativa in esame come legittima e conforme ai requisiti di cui all'art. 8 CEDU.

Alla medesima conclusione la Corte è arrivata inoltre nell'analisi della disciplina riguardante la previa autorizzazione giudiziaria: pur ritenendo che un controllo preventivo svolto da un organo giudiziario – per sua natura in grado di meglio garantire il carattere di imparzialità – sia da preferirsi, una autorizzazione di tale tipo "is not an absolute requirement *per se*, because where there is extensive subsequent judicial oversight, this may counterbalance the shortcomings of the authorisation" (par. 133). Dunque il fatto che la *Foreign Intelligence Court* non sia un organo giudiziario (solo il Presidente è un giudice mentre i restanti membri sono nominati dal Governo), non rappresenta *per se* un limite all'efficacia del controllo stesso, così come tale sistema non viene neppure ritenuto carente sotto il profilo della trasparenza: sul punto e con affermazioni di grande rilievo, la Corte ha anzi riconosciuto come legittimo il fatto che, vista la necessaria segretezza delle operazioni di *Signals Intelligence*, anche nella procedura di previa autorizzazione alcune informazioni, concernenti gli aspetti maggiormente delicati delle attività di intelligence svolte, non vengano messe a disposizione dell'autorità di controllo. In conclusione, ancora una volta, la Corte ritiene il sistema di previa autorizzazione, nel suo compresso, sufficientemente garantista nonostante alcune carenze.

1.4.1.1. – Il trasferimento di dati e la notifica ai soggetti interessati: la conferma di un approccio fondato su una lettura 'globale' della normativa, considerata nel suo complesso

Similmente a quanto affermato con riferimento alle procedure di accesso, conservazione, uso e distruzione dei dati raccolti, viene considerata adeguata anche la disciplina concernente la trasmissione di dati ad autorità terze, ad esempio verso altre autorità nazionali e non: "given the context – the collection of intelligence on foreign circumstances that may have an impact on Swedish national security and other essential national interests as well as the country's participation in international security operations – it is evident that there must be a possibility of exchanging intelligence collected with international partners" (par. 150); viene conseguentemente assegnata una ampia discrezionalità quanto al trasferimento di informazioni, nonostante venga rilevato come la legge individui solo vagamente le autorità alle quali i dati potrebbero essere trasferiti, senza richiedere peraltro alle stesse di rispettare e garantire un determinato livello di tutela e di salvaguardie: un'autorità straniera potrebbe dunque disporre un livello di protezione dei dati inferiore a quello stabilito in Svezia senza che ciò osti comunque al trasferimento. Anche con riferimento a tale profilo riconosciuto problematico e carente in termini di tutela apprestata, però, la Corte ha considerato, nuovamente, la normativa nella sua complessità, ritenendo le mancanze in termini di garanzie imposte al trasferimento ad altri soggetti sufficientemente controbilanciate dai controlli e dalla supervisione *ex post* predisposta dalla legge stessa[41]. Come a dire

[40] In particolare: "There is no provision obliging the FRA, the authorities mandated to issue detailed tasking directives or the Foreign Intelligence Court to cancel a signals intelligence mission if the conditions for it have ceased to exist or the measures themselves are no longer necessary", par. 129, *Centrum for Rattvisa*.

[41] Si potrebbe tuttavia obiettare che le supervisioni e i controlli *ex post* garantiti dalla normativa in esame difficilmente possono fornire tutele quanto al trattamento di dati operato dagli Stati terzi riceventi le informazioni dalle autorità svedesi. Un approccio che sembra distanziarsi da quello della Corte di Giustizia dell'UE che si è occupata ampiamente della tutela dei dati anche una volta varcati i confini europei: basti pensare al fatto che uno dei motivi di criticità riscontrati nella bozza di accordo con il Canada in materia di trasferimento di dati PNR (*Parere 1*/15) era proprio incentrato sulla possibilità, attribuita alle autorità canadesi, di trasferire dati ad autorità terze, anche al di fuori del Canada. Lo stesso dicasi anche per la sentenza *Tele2*, nella quale uno dei punti di contrasto con la Carta di Nizza è stato proprio identificato nella mancata predisposizione di un obbligo di conservazione dei dati nel territorio europeo. Sul punto Vogiatzoglou ha affermato: "The European Court of

che la fase successiva maggiormente garantista è in grado di sopperire alle lacune della fase di intercettazione e di condivisione stessa delle informazioni.

Altro punto altamente controverso è quello riguardante l'obbligo di notifica, con riferimento al quale i giudici svolgono una analisi piuttosto pratica e concreta, per certi versi apprezzabile ma in alcuni punti contrastante con quanto sostenuto nella previa giurisprudenza: non solo viene affermato come non in tutti i casi sia possibile provvedere ad una successiva notifica, ma anche che "activity or danger against which a particular series of surveillance measures is directed may continue for years, even decades, after the suspension of those measures. Subsequent notification to each individual affected by a suspended measure might well jeopardise the long-term purpose that originally prompted the surveillance. Furthermore, such notification might serve to reveal the working methods and fields of operation of the intelligence services and even possibly to identify their agents" (par. 164); il fatto quindi che, considerando la possibile sussistenza di tali rischi, non sia stabilito alcun obbligo di notifica, anche in un momento successivo alla cessazione delle operazioni di intercettazione, non deve *per se* portare a ritenere la normativa in contrasto col requisito di "necessità in una società democratica"; in altre parole viene affermato che solo nel momento in cui una notifica possa essere effettuata senza porre a repentaglio lo scopo e l'utilità stesse delle operazioni di intercettazione, vi è allora e solamente in quel caso l'obbligo di portarla a compimento. Come si avrà modo di vedere in seguito, questo approccio, seguito anche nella sentenza *Big Brother Watch*, rappresenta uno dei motivi che hanno portato i ricorrenti a presentare ricorso innanzi alla Grande Camera: ammettere ampie e discrezionali eccezioni all'obbligo di notifica – quale appunto un generico riferimento al potenziale pericolo legato alla rivelazione dei metodi di indagine utilizzati – finirebbe, secondo i ricorrenti, con lo svilire e rendere del tutto inutile il requisito stesso, che risulterebbe svuotato della propria obbligatorietà. La Corte, nel proprio ragionamento, ha ancora una volta giustificato tale limitazione ritenendo sussistenti sufficienti tutele e salvaguardie nella fase successiva dei rimedi disponibili: ribadito il legame intrinseco tra notifica e rimedi, che rendono la prima necessaria proprio al fine di consentire l'intervento dei giudici, la Corte è giunta alla conclusione che se i rimedi sono adeguati e l'accesso ad essi è comunque garantito anche in assenza di una notifica, allora anche le problematiche e i limiti riguardanti tale requisito possono ritenersi accettabili. Viene così richiamato il ben più risalente caso *Kennedy,* nel quale l'assenza dell'obbligo di notifica era comunque stata ritenuta compatibile con la CEDU proprio in quanto la possibilità di attivare successivi rimedi non risultava dipendente e connessa alla previa notifica; ebbene, la Corte ha ritenuto di poter applicare questa valutazione anche nella controversia attinente alla normativa svedese, sulla base della quale la possibilità lasciata a ciascun individuo di attivare l'intervento del *Foreign Intelligence Inspectorate* (FII) risulta slegata ed indipendente dalla avvenuta comunicazione al singolo di essere stato sottoposto a sorveglianza. Da ciò tuttavia deriva che il vaglio così attivato assume necessariamente carattere generale, non riguardando una specifica situazione o diritto di un particolare soggetto, con la conseguenza che i poteri dell'*Inspectorate* non si sostanziano nella possibilità di attribuire un risarcimento dei danni al ricorrente. Anche sotto questo ultimo profilo, che rappresenta certamente un limite alla tutela del diritto del singolo, la Corte ha mostrato di volgere lo sguardo alla normativa svedese nel suo complesso, ritenendo sufficiente e compensativa la presenza di ulteriori rimedi, da attivarsi dinnanzi al *Chancellor of Justice* o ad altre Corti nazionali, capaci di addivenire ad una dichiarazione risarcitoria.

Human Rights seems reluctant to get involved in matters of Intelligence Sharing, an approach which could be justified by the implication of international law", P. VOGIATZOGLOU, *Centrum For Rattvisa v. Sweden: bulk interception communications by Intelligence Services in Sweden does not violate the right to privacy*, in *European Data Protection Law Review*, 4, 2018, p. 566. Sullo specifico punto riguardante le operazioni di *Intelligence Sharing* la Corte si è poi però per la prima volta pronunciata nella sentenza *Big Brother Watch*, di cui si parlerà dettagliatamente.

In tale contesto, anche l'attribuzione al singolo della possibilità di richiedere direttamente al FRA notizie circa le proprie comunicazioni sottoposte ad intercettazione, riscontra un limite nella previsione della possibilità, da parte delle autorità di intelligence, di esprimere un legittimo rifiuto laddove le relative operazioni siano secretate: questa ampia discrezionalità, capace di incidere concretamente sulla efficacia del rimedio, non è stata considerata di una gravità tale da costituire una violazione dell'art. 8 CEDU. Il fatto che, ancora una volta, nel complesso, la normativa svedese abbia stabilito molteplici ulteriori rimedi di natura generale (la possibilità di adire il *Parliamentary Ombudsmen* e il *Chancellor of Justice*, ad esempio) è stato ritenuto una salvaguardia sufficiente: "In the Court's view, the aggregate of remedies, although not providing a full and public response to the objections raised by a complainant, must be considered sufficient in the present context, which involves an abstract challenge to the signals intelligence regime itself and does not concern a complaint against a particular intelligence measure" (par. 178).

Conclusivamente, quindi, la Corte è tornata a riaffermare l'ampiezza del margine di apprezzamento lasciato agli Stati nella valutazione del tipo di regime di sorveglianza da adottare (part. 179), mentre maggiori restrizioni sono state poste quanto alla disciplina e alle condizioni di funzionamento del regime scelto. Nel momento poi in cui i giudici di Strasburgo vengono chiamati ad operare una valutazione circa la compatibilità rispetto alla CEDU della normativa che regola il sistema di controllo e intercettazione prescelto, "the Court has had regard to the relevant legislation and the other information available in order to assess whether, on the whole, there are sufficient minimum safeguards in place to protect the public from abuse. *While the above assessment has disclosed some areas where there is scope for improvement, the Court is of the opinion that the system reveals no significant shortcomings in its structure and operation*" (par. 180, enfasi aggiunta): nel complesso quindi non viene rilevata alcuna violazione dell'art. 8 CEDU.

Sebbene questa pronuncia non possa ormai essere letta disgiuntamente dalla *Big Brother Watch*, pubblicata solo a distanza di qualche mese, pare opportuno svolgere alcuni rilievi preliminari: innanzitutto è da criticare e respingere una lettura che vede in questa pronuncia una netta e totale rottura con la precedente giurisprudenza della Corte e che vi riscontra, per la prima volta, una legittimazione ed accettazione generale dei sistemi di sorveglianza di massa. I giudici di Strasburgo, infatti, come emerso dalle previe analisi, non hanno mai condannato *per se* i regimi di raccolta massiva di dati e metadati, neppure nelle più recenti sentenze *Zakharov* e *Szabo*: ciò che, in quei casi, era stato dichiarato in violazione della CEDU era la carenza di salvaguardie e garanzie in grado di rendere 'necessaria in una società democratica' l'ingerenza nella vita privata dei consociati. Ciò che risulta però corretto ed innegabile è che i criteri indicati nella previa giurisprudenza – in particolare quello richiedente la sussistenza di un sospetto (*reasonable* o *individual*) e dunque di un legame tra l'intercettazione ed un determinato crimine, nonché quello di una successiva notifica e soprattutto di rimedi specifici in grado di permettere forme di controllo *ex post* – rendevano, nei fatti, estremamente difficile predisporre forme di sorveglianza indiscriminata e generalizzata[42]. Sotto questo profilo, i requisiti emersi nelle sentenze del 'primo gruppo' sopra esaminate appaiono invece mitigati nella pronuncia *Centrum for Rattvisa*, che non svolge alcun riferimento alla necessità di un sospetto e che non ritiene necessaria neppure la notifica laddove il sistema di rimedi successivo sia comunque azionabile anche senza la prova da parte del ricorrente di essere stato sottoposto a sorveglianza, prova per la quale la notifica sarebbe precondizione

[42] Con riferimento a quanto statuito nelle sentenze *Zakharov* e *Szabo*, Celeste afferma: "Although the Strasbourg Court was never explicit on this point, its strong condemnation of national surveillance systems that do not specifically identify the categories of persons which could be potentially targeted led one to think that bulk interceptions or other large-scale collections of data could not be considered admissible under the Convention", E. CELESTE, *The Court of Justice and the ban on bulk Data Retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019, p. 153.

necessaria[43]. La Corte giunge a queste conclusioni provvedendo ad una analisi della normativa nel suo complesso, considerando determinate carenze come accettabili e compensate dalla presenza di norme esaustive sotto altri profili. Per questi motivi, e principalmente nell''annacquamento' dei criteri sopra sottolineati, alcuni autori[44] hanno dunque rinvenuto nella sentenza *Centrum For Rattvisa* un abbassamento del livello di tutela previamente stabilito, pur dinnanzi ad un innegabile maggior livello di protezione e completezza garantito dalla normativa svedese rispetto a quelle russa e ungherese, oggetto delle previe pronunce.

Accanto a queste considerazioni, alcune necessarie riflessioni emergono anche con riferimento alle finalità delle normative analizzate: mentre nei casi precedenti le disposizioni riguardavano operazioni di *law enforcement* (per quanto, come si è già detto, non sia spesso semplice tracciare un chiaro confine con le operazioni di intelligence 'pura', viste anche le disposizioni normative estremamente vaghe ed ampie nella loro formulazione), la disciplina svedese ha invece ad oggetto operazioni di *Foreign Intelligence* che quindi hanno come finalità esclusivamente la tutela della sicurezza nazionale e che non coinvolgono – o quantomeno non dovrebbero coinvolgere – comunicazioni unicamente interne al territorio svedese. Proprio rilevando questo aspetto, emerge una certa perplessità nel continuo riferimento della Corte al caso *Zakharov*, che riguardava primariamente attività di polizia, e non di intelligence, e che era finalizzata ad una più ampia categoria di applicazioni (non solo *national security* ma anche "public safety, the prevention of crime and the protection of the economic well-being of the country"): ciò potrebbe anche portare a pensare che, salvo alcune differenze, gli stessi standard di tutela e garanzia possano quindi essere applicati sia alle operazioni poste in essere da agenzie di intelligence, sia a quelle poste in essere da autorità di *law enforcement*.

In estrema sintesi, dunque, pur volendosi distaccare da letture affrettate o estremizzanti, in questa pronuncia sono certamente riscontrabili diversi aspetti innovativi rispetto al passato, da individuarsi anche e soprattutto in un allontanamento, o quanto meno un affievolimento, dei criteri richiesti nelle sentenze *Zakharov* e *Szabo*: l'approccio maggiormente concreto della Corte nel vaglio della normativa svedese la porta a considerare sia le esigenze 'fattuali' necessarie ad un utile ed efficace funzionamento dei sistemi di sorveglianza, sia ad analizzare le disposizioni e il sistema di tutele approntato nel suo complesso, compensando eventuali carenze o eccessive generalizzazioni con salvaguardie successive più puntuali, efficaci ed accessibili. Questo scostamento da un controllo estremamente puntuale delle singole disposizioni e dai criteri individuati come necessari nelle previe sentenze, è – non a caso – alla base di quelle perplessità ed incertezze che da un lato hanno portato le ricorrenti ad adire la Grande Camera e dall'altro caratterizzano anche la quasi contemporanea sentenza *Big Brother Watch*.

[43] Come messo in luce da alcuni commentatori, tra cui Vogiatzoglou, sebbene venga data la possibilità di accedere a rimedi anche in assenza di una prova circa l'ingerenza nella sfera personale subita dal ricorrente – dal che la Corte fa derivare l'accettabilità della carenza di notifica, che in un sistema siffatto non si ripercuote dunque sul diritto di accesso alla giustizia – e nonostante le normative in materia di sorveglianza siano ora per la maggior parte accessibili pubblicamente, è innegabile tuttavia come solo gli individui realmente consapevoli dell'esistenza di pratiche di sorveglianza massive potranno decidere di attivarsi dinnanzi alle autorità competenti. Se si pensa infatti alla scarsa conoscenza della estensione ed invasività di strumenti di sorveglianza prima delle rivelazioni di Snowden, è facile comprendere come una tale consapevolezza sia da ritenersi tutt'altro che scontata.

[44] P. VOGIATZOGLOU, *Centrum For Rattvisa v. Sweden: bulk interception communications by Intelligence Services in Sweden does not violate the right to privacy*, op. cit.; A. LUBIN, *Legitimising foreign mass surveillance in the European Court of Human Rights*, in *Just Security*, 2 agosto 2018.

1.4.2. – La complessa pronuncia Big Brother Watch, le conseguenze delle rivelazioni di Snowden, gli strumenti di Foreign Intelligence *e di* Intelligence Sharing*: una vittoria di Pirro*

1.4.2.1. – L'incompatibilità di taluni importanti requisiti stabiliti nella previa giurisprudenza CEDU rispetto a forme di bulk interception*: una prima importante inversione di tendenza?*

Esaminando ora proprio quest'ultima articolata e – per certi versi – storica decisione della Corte EDU, bisogna innanzitutto sottolineare come il fondamento e vero motore propulsivo del ricorso di ben 16 ONG inglesi[45], tra cui appunto la Big Brother Watch, sia rappresentato dalle rivelazioni di Edward Snowden, dalle quali, come si è già avuto modo di vedere nei precedenti Capitoli, è emersa l'esistenza di compositi ed estesi sistemi di sorveglianza massiva e di *intelligence sharing* predisposti – anche – dal Regno Unito. Proprio all'analisi di questi meccanismi la Corte dedica una parte sostanziosa della sua lunga pronuncia, dando quindi conto della grande complessità del contesto normativo ed operativo entro cui i giudici hanno dovuto muoversi: sono presi in considerazione sia il meccanismo di *Foreign Intelligence* denominato TEMPORA[46], posto in essere da una delle agenzie di intelligence inglesi denominata *Government Communications Headquarters* (d'ora in avanti GCHQ), sia la normativa di riferimento sulla intercettazione generalizzata di comunicazioni, la *Regulation Investigatory Powers Act* del 2000 (d'ora in avanti RIPA), nonché i meccanismi di *Intelligence Sharing* e dunque di trasferimento dei dati e delle informazioni intercettate dalle agenzie del Regno Unito ad altre autorità di intelligence straniere; a tutto questo si aggiunge una disamina dei meccanismi di intelligence americani quali i già citati PRISM e UPSTREAM[47]. Una tale ampia ricognizione si è resa necessaria per l'ampiezza dei tre quesiti richiesti dai ricorrenti e riguardanti (a) la conformità rispetto agli artt. 8 e 10 della CEDU dei sistemi di *Foreign Intelligence*, aventi ad oggetto informazioni che fuoriescono dai confini nazionali (in entrata o in uscita) e basati su intercettazioni generalizzate disciplinate dalla Sezione 8 (4) RIPA; ma anche la compatibilità alla CEDU (b) delle operazioni di *Intelligence Sharing* (in particolare sotto il profilo dei dati ottenuti ed utilizzati dalle agenzie inglesi provenienti dai sistemi di sorveglianza statunitensi Upstream e Prism) e (c) delle operazioni di acquisizione dei metadati (*Communication data*) richiesti ai *service providers* e regolate dal Capitolo II RIPA.

Partendo dunque dall'ammissibilità del ricorso, la Corte ha avuto occasione, come già in *Centrum For Rattvisa*, di riaffermare, senza innovazioni sul punto, i criteri individuati in *Zakharov* e *Szabo*, circa la possibilità, nei peculiari casi aventi ad oggetto normative sulla sorveglianza segreta, di effettuare un vaglio *in abstracto* purché il ricorrente possa ritenersi presumibilmente colpito dalla normativa in esame, pur non avendone le prove, e considerando la disponibilità di rimedi efficaci a livello nazionale. Ecco che sotto quest'ultimo aspetto, l'intervento della Corte assume notevole rilievo per la particolarità del suo approccio: i giudici di Strasburgo infatti hanno esaminato il vaglio effettuato dall'*Investigatory*

[45] Merita rilevare come, mentre alcune ONG hanno direttamente adito la Corte EDU, altre 10 invece abbiano promosso ricorso dinnanzi all'apposito *Investigatory Power Tribunal* (IPT), di cui si è già accennato nei previ Capitoli e di cui si parlerà più ampiamente nella Parte III di questo elaborato. Sugli esiti del vaglio del giudice inglese in tali controversie nazionali, al termine delle quali le 10 ricorrenti indicate hanno poi adito la Corte EDU, si rimanda più ampiamente a: B. VAN DER SLOOT, E. KOSTA, *Big Brother Watch and others v. UK: lessons from the latest Strasbourg ruling on bulk surveillance*, in *European Data Protection Law Review*, 2, 2019.

[46] Un sistema di sorveglianza che consentiva alla GCHQ di intercettare enormi quantità di informazioni direttamente dai cavi di fibra-ottica installati nel mare.

[47] Nonostante questi due meccanismi di sorveglianza utilizzati dal governo USA siano già stati descritti nel Capitolo III, è bene comunque riprendere quanto evidenziato dalla Corte EDU sul punto: mentre il programma PRISM permette l'ottenimento di informazioni raccolte e conservate dagli *Internet Service Providers*, il programma UPSTREAM consente invece la raccolta di dati (contenuto e metadati) derivanti da comunicazioni elettroniche captate direttamente dai cavi in fibra-ottica utilizzati dai *Communication Service Providers*. Dalle rivelazioni di Snowden è emerso come il Regno Unito (la GCHQ in particolare) richiedesse ed acquisisse informazioni dalle autorità di intelligence statunitensi, ottenute mediante il sistema PRISM.

Power Tribunal (d'ora in avanti IPT), unico organo deputato a decidere sui casi di supposta violazione dei diritti fondamentali ad opera di agenzie di intelligence, e hanno concluso per l'efficacia del rimedio, garantito da giudici di alta formazione, ai quali vengono forniti pieni poteri di giudizio anche mediante la possibilità di accesso a importanti documenti 'below the waterline', cioè secretati, che consentono pertanto al Tribunale di effettuare un controllo completo. Se si fosse fermata qui nella sua analisi, la Corte avrebbe dovuto però dichiarare l'inammissibilità di quelle ricorrenti, tra le 16 ONG, che avevano direttamente adito l'organo sovranazionale senza prima promuovere giudizio innanzi al IPT. I giudici europei tuttavia non sono giunti a tale dichiarazione di inammissibilità, spingendosi oltre il dato oggettivo e considerando il contesto temporale entro il quale i ricorsi hanno avuto origine: a quel tempo, infatti, in un precedente giurisprudenziale della Corte EDU stessa, la già richiamata sentenza *Kennedy*, era stata dichiarata l'inefficacia del vaglio del IPT; le parti ricorrenti dunque avevano fatto affidamento su tale valutazione dei medesimi giudici europei ed avevano quindi reputato opportuno e legittimo adire direttamente la Corte EDU, proprio alla luce della dichiarata inefficacia del rimedio nazionale. Nonostante dunque la Corte abbia, nella sentenza in esame, oggettivamente riconosciuto che, a seguito di vari interventi normativi succedutisi proprio dopo la sentenza *Kennedy*, il rimedio garantito dall'apposito tribunale inglese fosse da considerarsi efficace e dunque da esperirsi necessariamente prima di adire la Corte europea quale criterio di ammissibilità, nondimeno i giudici hanno preso in considerazione un fattore meramente soggettivo, legato cioè alla *percezione* dell'efficacia del rimedio da parte del ricorrente, al tempo del ricorso stesso. In questo caso la percezione di alcune ONG è stata ritenuta ragionevole e giustificabile in quanto fondata su quanto statuito dalla Corte EDU stessa nei suoi precedenti giurisprudenziali: per tale ragione il ricorso è stato dichiarato ammissibile anche per le organizzazione che non avevano prima esperito i rimedi interni[48]. Indiscutibilmente questa posizione, del tutto singolare, della Corte EDU poggia sulle peculiarità della vicenda in esame e pare quindi difficile che una tale situazione possa ripetersi e che si possa replicare una valutazione di tipo 'soggettivo' quale quella qui proposta; è altrettanto vero però che questa argomentazione apre le porte ad incerte interpretazioni, anche e soprattutto da parte dei ricorrenti, sul criterio di efficacia dei rimedi, che potrebbe quindi potenzialmente essere valutato sulla base di mere considerazioni e 'percezioni' laddove precedenti giurisprudenziali creino una certa confusione o divergenti possibili interpretazioni.

Dopo aver chiarito, pur con i rilievi indicati, tale preliminare ed importante questione, i giudici hanno preso in esame la prima delle violazioni dell'art. 8 CEDU denunciate dai ricorrenti cioè quella riguardante il regime di *bulk interception* posto in essere sulla base della Sezione 8(4) del RIPA, prendendo avvio dalla rapida ricostruzione dei requisiti da considerare: innanzitutto l'ingerenza nel diritto alla vita privata deve essere fondata sulla legge e quest'ultima deve essere rispettosa dei principi propri dello stato di diritto, accessibile, prevedibile ed infine necessaria per una società democratica, da valutarsi sulla base della sussistenza delle sei salvaguardie minime individuate nella sentenza *Weber*, più volte richiamate, oltre alla presenza di meccanismi di supervisione, di strumenti di notifica e di rimedi *ex post*.

Addentrandosi in questa analisi, ciò che la Corte da subito ha affermato è di prorompente impatto: evidenziando i progressi tecnologici e la maggiore pervasività dei sistemi di sorveglianza odierni, i ricorrenti avevano infatti chiesto ai giudici di aggiornare le sei salvaguardie minime stabilite nella ormai risalente pronuncia *Weber*, aggiungere all'elenco dei requisiti di legittimità necessari anche ulteriori criteri obbligatori quali la prova oggettiva della sussistenza di un ragionevole sospetto, la preventiva autorizzazione giudiziaria e la successiva notifica al soggetto sottoposto a sorveglianza, come emersi nella sentenza *Zakharov*. I ricorrenti poi miravano ad ottenere una dichiarazione di incompatibilità con la CEDU delle forme di *bulk interception*, per loro stessa natura, rinvenendo nella sorveglianza

[48] Di diverso avviso sul punto sono stati invece i giudici Pardalos e Eicke, nella loro *Joint Partly Dissenting and Partly Concurring Opinion*, che hanno messo in rilievo come la valutazione della Corte debba essere esclusivamente oggettiva e dunque basata sulla efficacia concreta, e non percepita e soggettiva, del rimedio.

targettizzata l'unica forma proporzionata ed accettabile. Ebbene la Corte, con grande risolutezza ha respinto *in toto* tali istanze: da un lato viene considerata erronea la tesi secondo cui una *bulk interception* rappresenta automaticamente una intrusione maggiore nella sfera privata rispetto ad una *targeted interception*, e dall'altro viene affermato come le ulteriori salvaguardie proposte dai ricorrenti, per quanto importanti, non possano entrare nel novero delle salvaguardie minime richieste.

Quanto al primo profilo, merita sin da ora precisare come i giudici di Strasburgo abbiano ritenuto che una sorveglianza mirata comporti certamente una limitazione delle intercettazioni effettuate e dunque dei soggetti colpiti ma che essa porti altrettanto sicuramente ad una analisi e vaglio di tutte le comunicazioni raccolte, con un grado di invasività ed intrusione nella sfera privata maggiore. Al contrario, in un sistema di sorveglianza generalizzata la discrezionalità nella raccolta dei dati sarà ampia e dunque i soggetti interessati saranno molto più numerosi ma la quantità di comunicazioni sottoposte a successivo accesso, controllo ed analisi sarà invece più limitata e non riguarderà la totalità di quanto intercettato, grazie all'applicazione di criteri più restrittivi e selettivi al momento di primo esame e 'scrematura' dei dati raccolti. Queste argomentazioni, che catturano immediatamente l'attenzione per la loro portata e impatto, hanno posto non pochi dubbi sia per il loro distaccarsi dalle previe sentenze della Corte stessa, che avevano visto nella forma di sorveglianza targettizzata una misura da preferirsi a quella generalizzata, sia per quanto successivamente affermato nella medesima decisione, nella parte in cui cioè i giudici hanno ritenuto legittima e necessaria l'adozione di misure di controllo generalizzato solo nel momento in cui non fosse possibile adoperare efficacemente il mezzo meno invasivo della intercettazione targettizzata (par. 343)[49]. Sebbene quest'ultima affermazione paia essere riferita al *targeted warrant* che il RIPA richiede nel caso in cui siano coinvolti nelle operazioni di intercettazione soggetti che si trovino unicamente nel territorio inglese (e dunque quando non vi sia un elemento di 'estraneità' tale da consentire di applicare le normative in materia di *Foreign Intelligence*)[50], non può comunque essere negato come appaia difficile conciliare tale statuizione con quella che invece non rinviene necessariamente una minore invasività nella sorveglianza di tipo mirato[51]. Questo profilo problematico deve sin da subito far riflettere, soprattutto con riferimento a quanto stabilito nelle previe sentenze *Zakharov* e *Szabo*, nelle quali invece proprio l'assenza di una intercettazione mirata e targettizzata, nonché la mancata previsione della necessaria sussistenza di un sospetto ragionevole erano stati elementi determinanti, come si è visto, per stabilire la non conformità delle normative esaminate rispetto alla CEDU.

Questi iniziali aspetti quindi appaiono come un primo momento di distanza tra la previa giurisprudenza e il secondo gruppo di pronunce in analisi: se nella *Centrum For Rattvisa* la questione del 'sospetto' quale requisito di proporzionalità e necessità non era neppure stata affrontata, nella *Big Brother Watch* la Corte pare avere un approccio di contrapposizione col passato, soprattutto se si

[49] "The intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant" (par. 343, *Big Brother Watch*).

[50] Ci si deve chiedere tuttavia se abbia senso ritenere questo criterio (quello cioè che impone di ricorrere a misure di *bulk interception* solo laddove lo stesso obiettivo perseguito non possa essere diversamente ottenuto con misure di sorveglianza targettizzata) applicabile alle sole operazioni di intelligence di natura meramente 'interna' e non anche alle attività rientranti nella definizione di *Foreign Intelligence*: questo infatti si tradurrebbe nel riconoscimento di un minor livello di tutela alle comunicazioni che travalicano il confine nazionale rispetto alle comunicazioni interne.

[51] Tale lettura della Corte, secondo cui "the exclusion of communications of individuals known currently to be in the British Islands is, in the opinion of the Court, an important safeguard, since persons of interest to the intelligence services who are known to be in the British Islands could be subject to a targeted warrant under section 8(1) of RIPA", è risultata piuttosto oscura, come già rilevato anche in occasione della sentenza *Centrum for Rattvisa*: su quale base un maggior livello di tutela previsto per le comunicazioni interne deve essere visto come una apprezzabile e importante salvaguardia? Le comunicazioni 'esterne' possono, per questa stessa caratteristica di 'estraneità', risultare giustificatamente meno protette? Il ragionamento della Corte su questi punti non presenta ulteriori argomentazioni che permettano di comprendere le motivazioni alla base di una tale considerazione.

prosegue nella lettura della sentenza, nella quale addirittura viene affermato come "requiring objective evidence of reasonable suspicion in relation to the persons for whom data is being sought and the subsequent notification of the surveillance subject would be inconsistent with the Court's acknowledgment that the operation of a bulk interception regime in principle falls within a State's margin of appreciation. *Bulk interception is by definition untargeted, and to require "reasonable suspicion" would render the operation of such a scheme impossible*. *Similarly, the requirement of "subsequent notification" assumes the existence of clearly defined surveillance targets, which is simply not the case in a bulk interception regime*" (par. 317, enfasi aggiunta). Una posizione quindi di grande importanza e rilievo, che in sostanza ridimensiona enormemente i due requisiti di sospetto e notifica che risultano, sulla base di una analisi fortemente concreta ed 'operativa', inconciliabili, per loro natura, con sistemi di sorveglianza di massa e intercettazione generalizzata. È interessante sin da ora notare come proprio tale punto sia stato fermamente criticato da Centrum for Rattvisa, Big Brother Watch ed altre ONG, nelle loro richieste di rinvio alla Grande Camera: tutti i ricorrenti sono concordi nell'affermare la possibilità di utilizzare forme egualmente efficaci ma meno invasive di sorveglianza nonché la compatibilità con sistemi di *bulk interception* dei requisiti sopra indicati di 'reasonable suspicion'[52] e notifica[53].

Quanto invece alla previa autorizzazione giudiziaria, per quanto *per se* compatibile con l'effettivo funzionamento di un sistema di intercettazioni generalizzate e pur essendo riconosciuta come importante salvaguardia contro l'abuso o uso arbitrario dei meccanismi di sorveglianza (una *best practice*), essa non può essere considerata necessaria ed obbligatoria[54]; sotto questo profilo la Corte svolge una valutazione ampia, di sistema, che, discostandosi da quanto effettuato in *Zakharov*, non si basa sulla considerazione della natura ed efficacia dell'autorizzazione, del contenuto della stessa e della capacità dell'autorità di previo controllo di conoscere nel dettaglio le condizioni e motivazioni della intercettazione da autorizzare (argomentazioni queste che peraltro aveva portato i giudici ad affermare la necessità di un *reasonable suspicion*). Diversamente da ciò, infatti, quello che viene valutato è la sussistenza di un adeguato sistema di rimedi e supervisione successivi alla intercettazione stessa nonché la possibilità dei soggetti che ritengano di essere stati illegittimamente sottoposti a sorveglianza di attivare meccanismi di rimedio. Quindi la Corte ripropone le considerazioni che già erano state determinanti in *Centrum For Rattvisa* e richiama l'ancor più risalente decisione *Kennedy*, stabilendo che la presenza di efficaci controlli *ex post* è capace di sopperire all'assenza di controlli *ex ante*. Nel caso in esame avente ad oggetto la normativa inglese, come già accennato, la possibilità di adire il IPT, anche in assenza di specifiche prove o di notifica circa l'avvenuta sorveglianza, è stata valutata una

[52] "The Applicant submits that the minimum safeguards governing bulk interception should contain a requirement of reasonable suspicion, at least in situations where personalised search terms or other such indicators are used in order to single out or target specific individuals as part of a broader bulk interception activity. The use of search terms directly relating to a specific individual has serious privacy implications. Failing to apply the same threshold for use as applies to targeted interception risks creating a dangerous lacuna in the protection afforded by the Convention, and opens up the possibility for personalised bulk interception searches being used as a work-around method for targeting individuals" (par. 31, *Request for referral to the Grand Chamber*, Centrum for Rattvisa).

[53] Con riferimento a tale criterio, la ricorrente Big Brother Watch, nella propria *Request for referral*, ha richiamato le argomentazioni e i dati presentati da 10 ONG e volti a dimostrare come altri ordinamenti abbiano predisposto normative in materia di sorveglianza segreta inclusive della garanzia di notifica agli interessati. Queste disposizioni dimostrerebbero dunque che tale requisito non è affatto incompatibile con sistemi di *bulk interception* e che non necessariamente esso incide negativamente sull'efficacia e sul funzionamento delle operazioni di sorveglianza stesse (par. 25).

[54] Sul punto: "While the Court considers judicial authorisation to be highly desirable and, in its absence, will generally require a non-judicial authority to be independent of the executive, in the present case, in view of the pre-authorisation scrutiny of warrant applications, the extensive post-authorisation scrutiny provided by the (independent) Commissioner's office and the IPT, and the imminent changes to the impugned regime, it would accept that the authorisation of section 8(4) warrants by the Secretary of State does not, in and of itself, give rise to a breach of Article 8 of the Convention" (par. 381, *Big Brother Watch*).

tutela ed un rimedio sufficiente ed adeguato[55]. Ciò che la Corte oltretutto consiglia di considerare è "the actual operation of the system of interception, including the checks and balances on the exercise of power, and the existence or absence of any evidence of actual abuse" (par. 382), come a dire che il dato normativo, carente sotto determinati profili, può essere accettato e dichiarato compatibile con la CEDU laddove, nei fatti e mediante una valutazione concreta della sua applicazione e funzionamento, non ci siano prove che lo stesso abbia portato a condotte illegittime o ad abusi[56].

1.4.2.2. – La carenza di efficaci garanzie anche con riferimento ai 'related communication data' *e la mancanza di adeguate tutele nella fase di 'selezione' dei dati da sottoporre ad analisi, conservazione e trattamento: due violazioni dell'art. 8 Convenzione EDU*

Proseguendo nell'analisi della normativa inglese poi la Corte, come consueto, ha iniziato a vagliare la sussistenza dei sei requisiti minimi di salvaguardia delineati nella decisione *Weber*: sotto questo profilo è interessante notare come, con riferimento alla determinazione dello scopo e delle finalità della sorveglianza, ancora una volta i giudici mostrano di non fare tanto riferimento al dettato normativo quanto più alle chiarificazioni fornite del *Interception of Communications Commissioner*; quest'ultimo infatti ha spiegato il significato "in pratice" da attribuire al termine generico "sicurezza nazionale", intesa come giustificante "surveillance of activities which threatened the safety or well-being of the State and activities which were intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means. It therefore found the term to be sufficiently clear" (par. 333). Si vuole tuttavia preliminarmente notare come un tale significato non appaia in realtà per nulla circoscritto, soprattutto se si richiama alla memoria lo scrutinio puntuale e dettagliato delle disposizioni normative e delle definizioni in esse inserite effettuato in *Zakharov* e *Szabo*.

---

[55] La Corte si spinge addirittura oltre (par. 319), sottolineando sia come il rischio di abusi nell'utilizzo di meccanismi di sorveglianza non possa mai essere, in ogni caso, del tutto eliminato, sia come, anche in sistemi nei quali una previa autorizzazione giudiziaria era prevista, quale quello russo esaminato nella pronuncia *Zakharov*, gli abusi e le inefficienze non fossero comunque scongiurate. Questa argomentazione pare criticabile: affermare l'impossibilità di limitare del tutto i rischi non è appare motivo sufficientemente valido per ritenere non necessaria una misura che, per quanto certamente non perfetta e risolutiva di tutte le criticità, sicuramente può contribuire a ridurre il pericolo di abusi. Il fatto poi che le normative esaminate in altri casi posti all'attenzione della Corte non avessero disposto una disciplina efficace del controllo preventivo non sembra ragione condivisibile per escludere la possibile efficacia della misura stessa; a ciò si aggiunga come nel caso *Zakharov* il sistema analizzato fosse stato dichiarato inadeguato non solo per la carenza di efficacia del sistema di previo controllo ma anche e soprattutto per l'assenza del requisito di *reasonable suspicion*.

[56] Utilizzando questo approccio, la Corte è giunta ad affermare, con riferimento alla previa autorizzazione giudiziaria, che: "In the present case there is no evidence to suggest that the Secretary of State was authorising warrants without due and proper consideration. Furthermore, the IPT has extensive jurisdiction to examine any complaint of unlawful interception: unlike in many other countries, its jurisdiction does not depend on notification of the interception to its subject (see paragraph 124 above), which means that any person who believes that he or she has been subject to secret surveillance may make an application to it (see paragraph 318 above). Its members must hold or have held high judicial office or be a qualified lawyer of at least ten years' standing. In any case, the Court notes that under the new Investigatory Powers Act 2016 warrants will have to be approved by judicial commissioners following their authorisation by the Secretary of State. Although this new procedure has not yet been implemented, the Investigatory Powers Commissioner and the deputy Investigatory Powers Commissioner have been appointed" (par. 382, *Big Brother Watch*). Con riferimento a questa posizione della Corte, T. CHRISTAKIS (*A fragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch Judgement*, in *European Law blog*, 20 settembre 2018), afferma: "For the Court, then, substance prevails over form. But we might lose in terms of legal certainty and predictability: it is one thing to lay down a clear procedural condition that States should respect and then check of course whether it works effectively as in the *Zakharov* case", criticando quindi una visione che si fonda eccessivamente sulla presunta – e non sempre provata e argomentata – analisi dei fatti e dei risultati prodotti dalla normativa esaminata e non tanto su ciò che il dettato normativo prevede e potrebbe dunque portare quale esito nella sua concreta applicazione.

Anche la categoria dei soggetti da sottoporre a sorveglianza è, per ammissione della Corte stessa, estremamente ampia: "Section 8(4) only permits the Secretary of State to issue a warrant for the interception of external communications, which in principle excludes communications where both of the parties are in the British Islands. Although there has been some confusion about the application of the terms "external communications" and "internal communications" to modern forms of communications" (par. 336). Ma ecco che sul punto nuovamente la Corte adotta un approccio 'concreto' e basato sulle dichiarazioni e sui dati forniti dal Governo circa la realizzazione e attuazione, nella pratica, del sistema di sorveglianza: "That being said, it is clear that the targeted bearers [ovvero i canali di comunicazione dai quali intercettare i dati] are not chosen at random. They are selected because they are believed to be the most likely to carry external communications of intelligence interest (paragraph 6.7 of the IC Code, at paragraph 90 above and the Annual Report of the Interception of Communications Commissioner for 2016). *Therefore, while anyone could potentially have their communications intercepted under the section 8(4) regime, it is clear that the intelligence services are neither intercepting everyone's communications, nor exercising an unfettered discretion to intercept whatever communications they wish*. In practice, one of the grounds set out in section 5(3) of RIPA must be satisfied, bulk interception must be proportionate to the aim sought to be achieved" (par. 337, enfasi aggiunta)[57]. Una tale affermazione risulta tuttavia piuttosto criptica: su quale base si deve ritenere che i servizi di intelligence non intercettino la totalità delle 'external communications', evitando di esercitare quindi in maniera pienamente discrezionale il proprio potere? Risulta piuttosto difficile comprendere su quali elementi si possa fondare tale assunto, soprattutto se si prendono in considerazione l'ampiezza del dettato normativo in materia e l'assenza di un criterio oggettivo (quale il sospetto ragionevole) capace di legare l'assoggettamento a misure di sorveglianza con una minaccia alla sicurezza nazionale. La Corte sembra basare la propria posizione sulla presunzione, non approfonditamente argomentata, secondo cui un sistema di *bulk interception* debba consentire, per sua stessa natura, alle autorità ampia discrezionalità nella determinazione delle comunicazioni da intercettare e dei dati e metadati da raccogliere, discrezionalità che, in quanto tale, non è ritenuta incompatibile con l'art. 8 CEDU. Ed ecco che, pur riconoscendo l'ingerenza nella sfera privata rappresentata dalle intercettazioni, dalla raccolta nonché dalle operazioni di 'filtraggio' delle comunicazioni[58], ciò che i giudici hanno ritenuto indispensabile e sufficiente è l'esistenza di rigorose salvaguardie nella fase di selezione delle comunicazioni da trasmettere poi ad apposite autorità che le passeranno al vaglio. In altre parole si potrebbe dire che se una maggiore generalizzazione può essere concessa – e dunque ritenuta legittima e proporzionata – nella fase di intercettazione e raccolta, anche nella forma di una *bulk interception*, deve poi però sussistere una rigida struttura a 'imbuto', che vada a scremare, sulla base di criteri oggettivi e predeterminati, le informazioni da sottoporre successivamente ad analisi e accesso[59]. Ed è proprio su questo fronte che la Corte riscontra la prima carenza della

[57] Al par. 347 la Corte ribadisce nuovamente l'adozione e propensione per un vaglio concreto sull'attuazione della normativa più che sul dettato legislativo stesso: "there is no evidence to suggest that the intelligence services are abusing their powers – on the contrary, the Interception of Communications Commissioner observed that the selection procedure was carefully and conscientiously undertaken by analysts".

[58] Questa affermazione è di non poco conto: viene infatti chiaramente riconosciuto che anche un sistema che prevede una rapida (quasi in tempo reale) cancellazione o esclusione dei dati raccolti giudicati non rilevanti, rappresenta una ingerenza nel diritto alla vita privata. Anche le sole operazioni di raccolta e scansione dei dati mediante specifici criteri o indicatori (operazione di 'filtering') vengono quindi *per se* identificate come invasive della privacy, indipendentemente dal fatto che i dati vengano successivamente sottoposti ad accesso e a specifica analisi.

[59] È interessante notare infatti sul punto come la Corte, per argomentare il proprio ragionamento, abbia diviso in differenti fasi le operazioni di sorveglianza: "1. The interception of a small percentage of Internet bearers, selected as being those most likely to carry external communications of intelligence value. 2. The filtering and automatic discarding (in near real-time) of a significant percentage of intercepted communications, being the traffic least likely to be of intelligence value. 3. The application of simple and complex search criteria (by computer) to the

normativa inglese: le salvaguardie che regolano la selezione dei materiali intercettati non sono considerate dai giudici sufficientemente robuste da prevenire abusi, così come risulta problematica l'assenza di un controllo indipendente sulla individuazione e determinazione dei 'selectors', cioè dei criteri di ricerca usati per filtrare le comunicazioni intercettate (par. 347). Queste criticità sono poi accompagnate da un secondo aspetto della normativa, anch'esso trovato in violazione dell'art. 8 CEDU: la disciplina dei c.d. *related communications data*[60]; questi ultimi infatti non vengono sottoposti alle tutele e salvaguardie predisposte dalla Section 16[61], che si riferisce solo alle informazioni riguardanti il contenuto delle comunicazioni. Conseguentemente i *related communications data*, anche quelli riguardanti comunicazioni meramente interne incidentalmente intercettate, possono essere vagliati e analizzati senza alcuna restrizione. Rispetto a questa disciplina dunque la Corte esprime una posizione di grande rilievo, fortemente simile a quanto già in precedenza assunto dalla CGUE: l'acquisizione di *related communications data* non è necessariamente meno intrusiva dell'ottenimento del contenuto di dati. Quest'ultimo infatti può essere criptato e, anche se reso leggibile, può comunque non rivelare elementi di particolare importanza, mentre i metadati possono disvelare identità e geolocalizzazione del destinatario e del mittente di una comunicazione o il tipo di strumento utilizzato per la trasmissione dei dati. Inoltre, "in bulk, the degree of intrusion is magnified, since the patterns that will emerge could be capable of painting an intimate picture of a person through the mapping of social networks, location tracking, Internet browsing tracking, mapping of communication patterns, and insight into who a person interacted with" (par. 356). Impossibile non rilevare la somiglianza e convergenza con quanto indicato dai giudici di Lussemburgo sin dalla sentenza *DRI*: questa è però la prima volta in cui la Corte EDU pone nero su bianco tale constatazione di grandissima importanza. Certo i giudici non giungono a richiedere – o almeno non espressamente – che le stesse identiche salvaguardie previste per i 'content data' siano da applicare anche ai metadati[62], ma ciò che viene sicuramente specificata è la necessità di predisporre salvaguardie idonee anche per questa tipologia di informazioni.

---

remaining communications, with those that match the relevant selectors being retained and those that do not being discarded. 4. The examination of some (if not all) of the retained material by an analyst", par. 329.

[60] Questi dati si riferiscono ai c.d. *traffic data* che includono "information identifying the location of equipment when a communication is, has been or may be made or received (such as the location of a mobile phone); information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication; routing information identifying equipment through which a communication is or has been transmitted (for example, dynamic IP address allocation, file transfer logs and e-mail headers (other than the subject line of an e-mail, which is classified as content)); web browsing information to the extent that only a host machine, server, domain name or IP address is disclosed (in other words, website addresses and Uniform Resource Locators ("URLs") up to the first slash are communications data, but after the first slash content); records of correspondence checks comprising details of traffic data from postal items in transmission to a specific address, and online tracking of communications (including postal items and parcels)" (par. 353, *Big Brother Watch*). Come ben si comprende, la quantità di informazioni riguardanti la vita privata di un soggetto che possono essere carpite da tali dati è veramente significativa. La Corte non manca infatti di sottolineare quanto i 'related communications data' rappresentino una significativa e considerevole risorsa per i servizi di intelligence: "It can be analysed quickly to find patterns that reflect particular online behaviors associated with activities such as a terrorist attack and to illuminate the networks and associations of persons involved in such attacks, making it invaluable in fast-moving operations; and, unlike much data relating to content, it is not generally encrypted" (p. 353). Essi sono inoltre utilizzati anche per stabilire se il soggetto coinvolto in una comunicazione si trovi o meno nel Regno Unito.

[61] Si fa riferimento cioè al già richiamato previo vaglio del Segretario di Stato circa la necessità dell'intercettazione e alla presenza di elementi di estraneità delle comunicazioni da sottoporre a intercettazione.

[62] "In any event, it is not necessary for the Court to decide whether the six minimum requirements apply to the interception of communications data since, save for the section 16 safeguards, the section 8(4) regime treats intercepted content and related communications data in the same way. It will therefore focus its attention on whether the justification provided by the Government for exempting related communications data from this safeguard is proportionate to the legitimate aim pursued; that is, ensuring the effectiveness of that safeguard in respect of content" (par. 352, *Big Brother Watch*). Nelle conclusioni poi i giudici si limitano ad affermare: "While the Court does not suggest that related communications data should only be accessible for the purposes of

Questi due aspetti ora analizzati – la carenza di efficaci garanzie per la raccolta, trattamento e accesso ai 'related communication data' e l'assenza di controllo e tutele adeguate nella fase di 'selezione' dei dati da sottoporre a scrutinio – sono gli unici due elementi critici rilevati nella Sezione 8(4) del RIPA e rappresentano dunque i soli due motivi per i quali la normativa analizzata non è stata ritenuta compatibile con l'art. 8 CEDU.

Nessun rilievo invece è stato sollevato con riguardo alle condizioni di conservazione, esame e utilizzo dei dati[63] e neppure alla disciplina attinente all'invio delle informazioni intercettate ad autorità terze, quest'ultime da intendersi sia soggetti diversi rispetto a quelli abilitati normalmente ad attività di *Foreign Intelligence*, sia autorità situate oltre i confini del Regno Unito. Quest'ultima posizione in realtà appare problematica: l'invio a soggetti terzi infatti è reso possibile, sulla base del RIPA, nel caso in cui ciò si renda necessario o anche solo qualora sia possibile che diventi necessario ('is likely to become necessary') allo scopo di "facilitating the carrying out of any of the interception functions of the Secretary of State; for facilitating the carrying out of any functions of the Interception of Communications Commissioner or of the IPT; to ensure that a person conducting a criminal prosecution has the information he needs to determine what is required of him by his duty to secure the fairness of the prosecution; or for the performance of any duty imposed on any person under public records legislation". Le finalità elencate dunque sono estremamente ampie e la disciplina pare fondata su una terminologia piuttosto vaga: "likely to become necessary" è espressione che lascia un rilevante margine di discrezionalità ai servizi di intelligence; purtuttavia la Corte ha ritenuto che, nel complesso, la regolamentazione prevista dal RIPA predisponga adeguate tutele, in particolare grazie alla previsione che impone ai servizi di intelligence, una volta svelata o condivisa l'informazione con autorità appartenenti ad uno Stato diverso dal Regno Unito, di assicurare che tali autorità terze destinatarie garantiscano le salvaguardie necessarie al trattamento dei dati e assicurino che l'informazione venga ulteriormente divulgata o conservata solo nella misura strettamente necessaria. Appare legittimo tuttavia interrogarsi su come realmente le agenzie di intelligence inglesi possano imporre a soggetti terzi di rispettare tali principi e salvaguardie e di quali strumenti di controllo dispongano rispetto all'utilizzo dei dati condivisi effettuato dalle autorità straniere riceventi: possono continuare a tenerne traccia? Possono valutare e avere notizie circa l'uso dell'informazione una volta inviata a soggetti terzi? Possono richiederne la distruzione nel caso in cui non considerino limitato allo stretto necessario il trattamento del dato? Su questi aspetti la Corte non pare interrogarsi[64].

Piuttosto sbrigativa può apparire inoltre l'analisi della proporzionalità di un sistema di *bulk interception*: anche in questo caso infatti i giudici sembrano fondare il proprio convincimento su dati fattuali ed analisi predisposte da autorità inglesi: "the Independent Reviewer of Terrorism Legislation, examined a great deal of closed material and concluded that bulk interception was an

---

determining whether or not an individual is in the British Islands, since to do so would be to require the application of stricter standards to related communications data than apply to content, *there should nevertheless be sufficient safeguards in place to ensure that the exemption of related communications data from the requirements of section 16 of RIPA is limited to the extent necessary to determine whether an individual is, for the time being, in the British Islands*" (par. 357, enfasi aggiunta).

[63] Di particolare rilievo peraltro sono le considerazioni in merito alla conservazione e cancellazione delle informazioni intercettate: la Corte rileva non solo come ogni agenzia impegnata in attività di *Foreign Intelligence* abbia una diversa percezione di ciò che deve essere identificato come un 'appropriate retention period' ma anche come gli specifici periodi di conservazione non siano resi pubblici. Nonostante questi rilievi critici, che evidenziano l'indeterminatezza delle disposizioni normative in materia e della loro attuazione, i giudici concludono per la conformità della disciplina nel suo complesso, basandosi sul fatto che sussiste comunque un termine massimo di conservazione di due anni e che, sulla base del Report annuale 2016 del *Interception of Communications Commissioner*, tale periodo nella pratica attuazione non supera la durata di un anno.

[64] B. VAN DER SLOOT, E. KOSTA, *Big Brother Watch and others v. UK: lessons from the latest Strasbourg ruling on bulk surveillance*, op. cit., che sottolineano anche un altro aspetto problematico, rimasto senza risposta: "What is left unaddressed is the question of oversight over such cross-border sharing of data: who is responsible for authorizing such transfers and who is auditing the conditions for it?", p. 261.

essential capability: first, because terrorists, criminals and hostile foreign intelligence services had become increasingly sophisticated at evading detection by traditional means; and secondly, because the nature of the global Internet meant that the route a particular communication would travel had become hugely unpredictable" (par. 384), riprendendo peraltro la conclusione di questa indagine che propende per l'inesistenza di mezzi alternativi capaci di sostituire in maniera sufficiente ed efficiente il sistema di intercettazione generalizzata. Citando anche il Report della Commissione di Venezia[65], la Corte considera ragionevole affidarsi a queste valutazioni, fino a sostenere: "It is clear that bulk interception is a valuable means to achieve the legitimate aims pursued, particularly given the current threat level from both global terrorism and serious crime" (par. 386). Questo punto è di non poco rilevo: se si ricordano le considerazioni svolte già con riferimento al *Parere 1/15* della CGUE in materia di PNR, si nota come, tanto in quel caso quanto in quello ora in esame, le valutazione di entrambe le Corti europee risultino piuttosto sbrigative – dedicando alla questione solo brevi paragrafi – e non approfonditamente argomentate, basate cioè sulla assunta correttezza di studi, indagini e valutazioni predisposte da autorità, peraltro più o meno indipendenti dal potere esecutivo, e fondate solo parzialmente su dati empirici documentati.

Un simile approccio della Corte EDU è da riscontrarsi peraltro anche con riferimento ai sistemi di *Intelligence Sharing* cioè ai meccanismi di richiesta e utilizzo di informazioni e dati derivanti da servizi di intelligence stranieri: "the Court has considered it legitimate for Contracting States to take a firm stand against those who contribute to terrorist acts. Due to the nature of global terrorism, and in particular the complexity of global terror networks, the Court accepts that taking such a stand – and thus preventing the perpetration of violent acts endangering the lives of innocent people – requires a flow of information between the security services of many countries in all parts of the world" (par. 446). I giudici però, accanto ad una chiara affermazione dell'importanza di sistemi di condivisione e scambio di dati, si sono mostrati altrettanto consapevoli dei pericoli che tali operazioni comportano, potendo in particolare essere utilizzate come escamotage per aggirare facilmente gli obblighi di salvaguardia ed i limiti imposti dal rispetto della CEDU e delineati dalla giurisprudenza della Corte EDU stessa, mediante la richiesta e l'ottenimento di informazioni da servizi di intelligence stranieri non sottoposti al rispetto delle medesime condizioni o livelli di garanzia europei. Per far fronte a tali rischi concreti, i giudici hanno ritenuto necessaria e sufficiente la predisposizione di una normativa nazionale che indichi in maniera chiara e precisa le circostanze per le quali il Regno Unito è legittimato a servirsi di intercettazioni di provenienza straniera. Una tale normativa, nel caso in esame, non può essere individuata nel RIPA bensì deve essere cercata nel *British-US Communication Intelligence Agreement* del 1946, che autorizza lo scambio di informazioni USA-UK, nel *Security Services Act* del 1989 e nel *Intelligence Services Act* del 1994, che consentono l'invio e la richiesta di dati limitatamente a quanto necessario al raggiungimento degli scopi per i quali i servizi di intelligence sono stati istituiti, nonché nell'ambito di qualsiasi procedimento penale. A giudizio della Corte, tali disposizioni della normativa inglese, benché sparse in diverse fonte, indicano con sufficiente chiarezza le procedure da seguire per la richiesta di intercettazioni e, imponendo che il materiale trasferito da intelligence straniere venga vagliato e filtrato sulla base dei medesimi criteri stabiliti per i dati raccolti direttamente dalle intelligence nazionali, non sono considerate sussistenti violazioni dell'art. 8 CEDU. Per la prima volta quindi i giudici di Strasburgo si sono pronunciati e hanno legittimato un sistema transfrontaliero di scambio e condivisione di dati, non solo ritenendolo necessario e proporzionato alla garanzia della sicurezza nazionale ma anche considerando adeguate le tutele previste. È innegabile però come l'attenzione della

[65] *Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies*, 2015, nel quale la Commissione riconosce il valore intrinseco della sorveglianza generalizzata per scopi securitari. Questi sistemi infatti rendono possibile l'attuazione di un approccio proattivo da parte della autorità di intelligence, in grado cioè di prevenire pericoli non determinati o conosciuti anziché investigare su crimini già compiuti. Su questo specifico punto si tornerà in seguito.

Corte nello svolgimento di tali considerazioni si sia concentrata solo sulla disciplina prevista per la fase di selezione ed utilizzo dei dati trasferiti e non sulla disciplina concernente la raccolta dei dati stessi da parte dell'intelligence straniera. Ciò deve indurre ad alcune valutazioni critiche: escludendo qualsiasi controllo sull'operato delle autorità di intelligence di Paesi terzi, in questo caso statunitensi, per la Corte EDU ciò che avviene nella fase di raccolta al di fuori dei confini del Regno Unito non rientra nella responsabilità dello Stato ricevente stesso[66]: possono dunque essere sottoposte a valutazione solo la legittimità e proporzionalità del regime regolatorio relativo alla richiesta e ottenimento dei dati e alla loro successiva memorizzazione, esame ed utilizzo (par. 421). Un tale approccio è stato da alcuni commentatori fortemente criticato come passibile di aprire un notevole gap nella tutela dei diritti fondamentali[67]. La scelta di ignorare ed escludere da qualsiasi controllo la fase precedente alla ricezione delle comunicazioni pare poi ancora più discutibile alla luce dei rilievi operati dalla CGUE nel caso *Schrems*, nel quale è stata messa in evidenza l'inadeguatezza, rispetto al diritto dell'UE, del livello di protezione dei dati e di rispetto della privacy predisposto dall'ordinamento americano con riferimento proprio ai programmi di sorveglianza PRISM e Upstream[68]. I dubbi derivanti – anche ma non solo – da questa discussa posizione della Corte sono alla base della richiesta, avanzata dai ricorrenti, di porre le questioni emerse dalla sentenza in esame all'attenzione della Grande Camera: una delle pretese avanzate da Big Brother Watch e da altre ONG è infatti che, laddove si intenda richiedere ed utilizzare dati raccolti da agenzie di intelligence straniere, a queste vengano applicate le medesime salvaguardie previste per le operazioni di *bulk interception* effettuate dalle agenzie nazionali inglesi[69].

L'ultimo punto di questa lunga ed articolata pronuncia, sul quale si vuole porre l'attenzione, riguarda la terza e finale domanda dei ricorrenti concernente la compatibilità con l'art. 8 CEDU del Capitolo II RIPA che disciplina l'ottenimento di metadati raccolti e conservati dai *service providers*. Ebbene con riferimento a tale questione, che la Corte risolve piuttosto velocemente, viene effettuato un vasto richiamo alla giurisprudenza CGUE: attingendo ampiamente proprio alle sentenze *DRI* e *Tele2*, i giudici di Strasburgo rilevano la somiglianza del caso in esame con quanto già vagliato dai colleghi di Lussemburgo. Diversamente dagli altri quesiti sino ad ora analizzati, quest'ultimo punto non riguarda infatti intercettazioni generalizzate effettuate direttamente dai servizi di *Foreign Intelligence* e riguardanti i contenuti e metadati di comunicazioni che fuoriescono dai confini nazionali e raccolti

[66] "Although the impugned regime concerns intercepted communications, the interference under consideration in this case does not lie in the interception itself, which did not, in any event, occur within the United Kingdom's jurisdiction, and was not attributable to that State under international law. As the communications are being intercepted by foreign intelligence agencies, their interception could only engage the responsibility of the respondent State if it was exercising authority or control over those agencies" (par. 420, *Big Brother Watch*). Da alcuni autori (V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, op. cit.) viene quindi rilevato come anche ai sensi dell'art. 1 CEDU, riguardante la competenza della Corte stessa, quest'ultima non possa giudicare sulla fase della intercettazione operata dalle agenzie di intelligence statunitensi, essendo operazioni e condotte che non solo non rientrano nella giurisdizione del Regno Unito ma non sono neppure a tale Stato attribuibili sulla base dell'art. 8 dei *Draft Articles on Responsibility of States for Internationally Wrongful Acts*. Per maggiori approfondimenti su tale complesso tema, si rimanda anche a C. M. RYNGAERT, N. VAN EIJK, *International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees*, in *International data privacy law*, 1, 2019.

[67] V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, op. cit. Un tale approccio della Corte, facendo salve le pratiche di *Intelligence Sharing*, rende impossibile, per un soggetto le cui conversazioni siano state raccolte da agenzie di intelligence statunitense e poi inviate ed utilizzate dalle agenzie inglesi, di poter disporre di alcun rimedio in caso di violazione dell'8 CEDU intervenuta nella sola fase di raccolta all'estero dei dati.

[68] Si rimanda al Capitolo III per una più ricostruzione di tale pronuncia.

[69] Merita sin da ora evidenziare come anche i giudici Koskelo e Turkovic nella loro già richiamata *Joined Partly Concurring Partly Dissenting Opinion*, abbiano rilevato che "the shortcomings referred to in the context of the section 8(4) regime [quindi quelli riferiti alle salvaguardie relative alle operazioni di *Foreign Intelligence*] also attach to the intelligence-sharing regime. I therefore conclude that the safeguards have not been adequate and that there has been a violation of Article 8 in respect of this regime also", par. 33.

utilizzando i mezzi di trasmissione dei *Communication Service Providers*; si tratta, al contrario, di normative che disciplinano la richiesta, avanzata da pubbliche autorità, di acquisizione di metadati (*Communication data*) raccolti e conservati da compagnie di telecomunicazione private. Viene quindi effettuata una utile distinzione tra metodi investigativi che prevedono, ad esempio, un accesso ai dati riguardanti la posizione geografica di un soggetto in un dato momento del passato e sistemi di sorveglianza che monitorano invece gli spostamenti di un soggetto (quali quelli oggetto del caso *Ben Faiza*[70]), permettendo di geolocalizzarlo in tempo reale (par. 462). La CGUE, occupandosi della prima tipologia di raccolta e analisi dei metadati, si era pronunciata anche sulla disciplina riguardante l'accesso ai dati conservati, stabilendo, come già ampiamente esaminato nei precedenti Capitoli, che tali operazioni debbono essere limitate a quanto strettamente necessario per il raggiungimento dell'obiettivo e debbono altresì essere accompagnate, tra gli altri, da un previo controllo di una Corte o di una autorità amministrativa indipendente e solo al fine di contrastare un crimine grave. Sulla base di tali rilievi, che avevano comportato la dichiarazione di incompatibilità di normative nazionali, quali la Parte IV dell'*Investigatory Powers Act* (IPA), con il diritto dell'UE e la Carta di Nizza in particolare, la legislazione inglese era stata soggetta a modifiche, intervenute il 1 novembre 2018. La Corte EDU, dunque, di fronte alla medesima questione posta in passato già ai giudici di Lussemburgo, ha di fatto trasposto le conclusioni della Corte di giustizia alle disposizioni oggetto della sua analisi (Capitolo II RIPA)[71] e ha rilevato come queste ultime non solo non limitino ai soli casi di reati gravi l'accesso ai metadati conservati dai servizi di telecomunicazioni ma non prevedano neppure alcun previo controllo da parte di una autorità indipendente. Prendendo quindi atto che il Regno Unito, essendo (al momento della pronuncia) membro dell'UE, avrebbe dovuto sottostare al principio di primazia del diritto dll'UE in caso di contrasto tra il primo e la normativa nazionale, a parere della Corte EDU le disposizioni in esame, interpretate alla luce della recente giurisprudenza della CGUE, non potevano essere considerate conformi all'art. 8 CEDU[72].

[70] *Ben Faiza v. France*, ricorso n. 31446/12, deciso il 8 febbraio 2018.

[71] Quanto in questa sede è importante sottolineare preliminarmente è che i giudici di Strasburgo, nel caso *Big Brother Watch*, non hanno analizzato la normativa attualmente vigente (*Investigatory Powers Act*, IPA), dovendo attenersi alla disciplina prevista e applicata al momento del ricorso (il RIPA, appunto). Pare utile ricordare sin da ora che il RIPA e il successivo DRIPA sono state sostituite nel 2016 dal IPA, anch'esso modificato nel 2018 a seguito della pronuncia *Tele2* della CGUE e della conseguente successiva decisione della High Court: tali innovazioni e modifiche saranno oggetto di più ampia disamina nella Parte III del presente elaborato, che si concentrerà nello specifico sul sistema inglese di conservazione e accesso a dati per scopi securitari.

[72] Per completezza espositiva, si vuole infine solo velocemente menzionare un ulteriore aspetto innovativo della più recente sentenza in esame: per la prima volta la Corte EDU si è infatti pronunciata sulla compatibilità di un sistema di sorveglianza rispetto al diritto alla libertà di espressione, tutelato dall'art. 10 CEDU; rispetto ad esso, i giudici di Strasburgo hanno rinvenuto una violazione della Convenzione nella parte in cui la normativa inglese non tutela espressamente e specificamente la confidenzialità delle informazioni reperite ed utilizzate dai giornalisti. La protezione della confidenzialità infatti viene individuata come elemento fondamentale ed imprescindibile per la garanzia di un reale godimento ed esercizio del diritto di libertà di stampa e deve essere tutelata non solo sotto il profilo dell'accesso alle fonti delle informazioni giornalistiche ma anche in ogni caso in cui vengano effettuate operazioni di raccolta, conservazione, trattamento e accesso ai dati (sia concernenti i contenuti sia i soli metadati) riguardanti i giornalisti stessi. Con riferimento alla Section 8(4) DRIPA, la Corte EDU ha infatti affermato: "In the Article 10 context, it is of particular concern that there are no requirements – at least, no "above the waterline" requirements – either circumscribing the intelligence services' power to search for confidential journalistic or other material (for example, by using a journalist's email address as a selector), or requiring analysts, in selecting material for examination, to give any particular consideration to whether such material is or may be involved. Consequently, it would appear that analysts could search and examine without restriction both the content and the related communications data of these intercepted communications" (par. 493). Mentre con riguardo al Capitolo II DRIPA: "they [le disposizioni riguardanti appunto i metadata] do not, therefore, apply in every case where there is a request for the communications data of a journalist, or where such collateral intrusion is likely. Furthermore, in cases concerning access to a journalist's communications data there are no special provisions restricting access to the purpose of combating "serious crime". Consequently, the Court considers that the regime cannot be "in accordance with the law" for the purpose of the Article 10 complaint" (par. 499).

1.5. – Una posizione controversa in attesa di chiarimento: il 'secondo gruppo' di sentenze e la distanza rispetto al livello di garanzie precedentemente affermato

Ecco quindi che, muovendo ad alcune considerazioni finali, dalla lettura di queste due più recenti pronunce e dagli aspetti già sottolineati di divergenza o allontanamento rispetto alla linea giurisprudenziale precedente, emerge un quadro fortemente complesso che, se non vuole essere definito di totale rottura con il passato, quantomeno deve essere visto come una sua possibile evoluzione. Non è mancato dunque chi, dinnanzi a questi considerevoli mutamenti, ha criticato l'approccio delle due Camere della Corte: "sul ricorso in sé ad un sistema di sorveglianza elettronica di massa la Corte EDU sfoggia una posizione assai più deferente nei confronti delle scelte legislative degli Stati contraenti la CEDU, che pare segnare un cambio di paradigma rispetto non solo alla sopra richiamata giurisprudenza della Corte di giustizia ma della stessa Corte EDU se letta alla luce anche di recenti suoi precedenti"[73]. Le ultime decisioni analizzate infatti fanno propendere per una accettazione, invero poco argomentata, di sistemi di sorveglianza e intercettazione generalizzata, considerati ormai ordinari ed inevitabili strumenti di contrasto al terrorismo globale e ai crimini gravi, senza che questa conclusione – non necessariamente erronea – sia però accompagnata da una seria riflessione sulla proporzionalità e stretta necessità di tali misure e dunque sia sulla loro reale efficacia rispetto agli obiettivi, sia sulla possibilità di individuare strumenti alternativi egualmente efficienti, meno invasivi della sfera personale e più compatibili con le fondamenta stesse delle nostre democrazie. Per quanto sia da considerarsi assolutamente positivo il tentativo della Corte di richiamare dati concreti e considerazioni svolte da soggetti terzi (Commissione di Venezia, *UK Independent Reviewer of Terrorism Legislation*), il vaglio dei giudici pare spesso ancora troppo sbrigativo su un punto estremamente centrale e delicato: una maggiore attenzione e argomentazione su questi profili non deve portare necessariamente ad un giudizio opposto rispetto a quanto affermato in queste due ultime sentenze ma avrebbe certamente il merito, anche in tal caso, di rafforzare e rendere complete le valutazioni della Corte, stabilendo criteri e requisiti maggiormente chiari, coerenti e comprensibili per i legislatori nazionali. Sul punto è interessante vedere come la ricorrente Big Brother Watch, nella richiesta di rinvio alla Grande Camera, abbia fortemente criticato il vaglio sbrigativo della Corte in termini di proporzionalità e necessità delle misure di *bulk interception*: "The Chamber erred in its uncritical adoption of the position of the Government's Independent Reviewer and its focus on a partial selection of materials supportive of that position to the exclusion of the concerns expressed by many international bodies as to mass surveillance" (par. 22)[74].

Dal controverso e criticato approccio più 'sintetico' dei giudici in queste due pronunce, che non paiono mettere approfonditamente in discussione necessità e proporzionalità di sistemi di controllo generalizzato, emerge di conseguenza come il margine di apprezzamento degli Stati quanto alla scelta del tipo di sistema di sorveglianza da adottare non venga messo in discussione mentre ciò che può essere oggetto di scrutinio è la sussistenza o meno di idonee garanzie e salvaguardie nella disciplina di tali meccanismi di intercettazione e controllo. Ed è proprio e specificamente sotto questo profilo che si può individuare la maggiore distanza del secondo gruppo di sentenze esaminate rispetto alle previe decisioni

[73] G. TIBERI, *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?*, in *Quaderni costituzionali*, 4, 2018, p. 932.

[74] Sul profilo della stretta necessità e sulla possibilità dunque di utilizzare misure meno invasive dei diritti dell'individuo ed egualmente efficaci, la ricorrente afferma: "The UK's purported justifications for bulk interception do not hold water. The discovery of new targets through bulk interception is disproportionate in circumstances where those targets are highly likely to be discovered through the alternative use of appropriate discriminators following extraction, i.e. at stage (iii) above. As the Chamber noted, "[t]he intelligence services should not be permitted to obtain via a bulk warrant what they could obtain via a targeted warrant" (§343). The Applicants submit that a bulk interception regime of this nature cannot, therefore, be proportionate: the bulk collection and storage of data and communications of a substantial segment of the European population, the majority of whom are of no interest to the intelligence agencies, is plainly disproportionate" (par. 20-21, *Request for referral to the Grand Chamber*).

Zakharov e *Szabo* che, imponendo quali requisiti la previa autorizzazione, la sussistenza di un sospetto e la garanzia di una notifica al soggetto interessato, limitavano, nei fatti, forme generalizzate di raccolta di dati. La Corte in *Big Brother Watch* pare allontanarsi con grande chiarezza dalla richiesta di inserire tali requisiti tra quelli obbligatori, rifiutando di aggiornare i criteri delineati nella sentenza *Weber* con una scelta che è stata criticata non solo dai ricorrenti ma anche dai giudici Koskelo e Turkovic nella loro *Joined Partly Dissenting and Partly Concurring Opinion*. I due giudici infatti hanno ritenuto che ciò che viene definito, con una significativa espressione, il 'sea change' frutto dello sviluppo tecnologico non possa non essere tenuto in debita considerazione dalla Corte: "the factual context in which "exploratory" or "strategic" secret surveillance operates is dramatically different from the circumstances that still prevailed a couple of decades ago, when the *Weber* application was lodged, let alone four decades ago, when *Klass and Others* was decided. *In the light of such changes, it is problematic and troubling to approach the question of the necessary safeguards against abuse simply by applying standards that were considered sufficient under significantly or even essentially different factual circumstances*" (par. 13, enfasi aggiunta)[75].

Ulteriori critiche e discordanti visioni emergono peraltro anche rispetto a quell'approccio della Corte (sottolineato più volte non solo in *Big Brother Watch* ma anche in *Centrum For Rattvisa*) che tende a considerare la normativa nel complesso e che porta quindi a compensare, ad esempio, carenze di tutele e salvaguardie nella fase *ex ante* con la sussistenza di tutele adeguate nella fase *ex post*. Questo tipo di ragionamento viene da un lato contestato nella *Joint Partly Dissenting and Partly Concurring Opinion* di Koskelo e Turkovic, che sul punto sostengono: "While the safeguards *ex post* that are provided for in the UK legislation and practice appear to set a good model in this domain, this does not in my view suffice to remedy the fact that the authorisation and implementation of the surveillance are wholly in the hands of the executive authorities, without any independent control *ex ante"* (par. 26); dall'altro lato, invece, i giudici Pardalos e Eicke, nella loro *Partly Dissenting and Partly Concurring Opinion* non solo hanno ritenuto questo approccio corretto ma addirittura troppo poco applicato dalla Corte, individuando come maggiormente opportuna la posizione adottata in *Centrum For Rattvisa*: in tale decisione, infatti, pur evidenziando aree critiche e passibili di miglioramenti, la Corte aveva infine escluso, proprio alla luce di un vaglio complessivo della normativa svedese, qualsiasi violazione dell'art. 8 CEDU; al medesimo risultato, a parere dei giudici Pardalos e Eicke, sarebbe dunque dovuta arrivare la Corte anche nel caso *Big Brother Watch*.

Se è invece stato positivamente accolto, in maniera pressoché unanime[76], il riconoscimento da parte della Corte circa la forte invasività delle operazioni di intercettazione, raccolta e accesso ai metadati – capaci, se letti in maniera aggregata, di delineare un quadro preciso della vita dell'individuo –, non è tuttavia chiaro se rispetto ad essi la normativa nazionale debba applicare le stesse identiche garanzie

[75] Interessante, anche per la sensibilità con la quale tali giudici leggono le recenti evoluzioni storico-politiche-giuridiche, è quanto affermato al par. 15: "There is yet another "sea change" calling for heightened attention in the assessment of the necessary standards in the context of secret surveillance of communications. It is the degradation of respect for democratic standards and the rule of law of which there is increasing evidence in a number of States. While I am not suggesting that the present respondent State is a case in point in this regard, the Convention standards must nevertheless be considered in the light of the fact that such developments testify to the actual or potential fragility of safeguards, institutional arrangements and the underlying assumptions that in ideal circumstances might appear adequate in order to minimise the risks of abuse. In fact, the same threats that are invoked to justify secret surveillance may also serve to reinforce tendencies toward a weakening of the checks and balances which underpin adherence to the rule of law and democratic governance".

[76] Molti individuano in questa posizione della Corte EDU, che peraltro si avvicina fortemente a quanto affermato dalla CGUE, il punto decisivo "per il quale la presente pronuncia si candida ad essere un *leading case* per la tutela dei diritti fondamentali nell'era di Internet e degli algoritmi che lo governano", G. TIBERI, *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?*, op. cit., p. 933.

predisposte per i 'content data'[77]: quel che è certo comunque è l'innalzamento del livello di tutela previsto e la necessaria inclusione, anche con riferimento ai metadati, di un insieme di salvaguardie minime.

In conclusione, nonostante le prime entusiastiche reazioni dinnanzi alla condanna del Regno Unito per violazione dell'art. 8 CEDU, una lettura più attenta della sentenza *Big Brother Watch*, anche alla luce delle criticità sopra indicate, deve indurre a ridimensionare l'esaltazione iniziale e a riconoscere la decisione della Corte come una 'vittoria di Pirro'[78]. Se sotto taluni profili, e sempre tenendo in debita considerazione la diversità delle normative poste all'attenzione della Corte[79], è individuabile un certo 'paradigm shift' rispetto non solo al precedente approccio della Corte EDU stessa ma anche, per taluni aspetti, alle pronunce della CGUE[80], alcuni autori sono giunti addirittura a chiedersi se in tale approccio non debba piuttosto ravvisarsi anche il rischio di un 'two-speed control'[81] della Corte che cioè attua per i Paesi dell'Europa dell'Est un controllo più rigido e fortemente fondato sull'analisi della singola disposizione piuttosto che sulla valutazione d'insieme della normativa stessa, e adotta invece per gli Stati dell'Europa occidentale un vaglio più flessibile, che tiene in considerazione le tutele del sistema normativo e di accesso ai rimedi giudiziari nel loro complesso, sulla base della presunzione secondo cui tali sistemi democratici sono da tali da costituire, per natura, una barriera a possibili abusi.

Pur non volendo condividere letture 'estremizzanti', certamente sarà di grande interesse e rilievo osservare gli sviluppi delle due ultime pronunce analizzate: essendo entrambe sottoposte al giudizio della Grande Camera, per gli aspetti critici che sono stati via via individuati nel corso dell'analisi, si avrà modo di vedere se quest'ultima ricomporrà la 'frammentazione' – più o meno profonda a seconda delle interpretazioni – che si è venuta a creare nella giurisprudenza della Corte EDU, o se verrà confermata invece la lettura innovativa più recente, con determinanti risvolti soprattutto con riferimento alla individuazione dei requisiti minimi di salvaguardia richiesti[82].

---

[77] La Corte infatti si è limitata ad affermare l'incompatibilità della normativa inglese alla CEDU nella parte in cui esclude totalmente l'applicazione delle tutele di cui alla Section 16 ai metadata ma non specifica se tutte le garanzie previste in tale normativa debbano necessariamente essere applicate, allo stesso modo e al medesimo livello, anche ai *communications data*. Sul punto Rusinova afferma: "It weeks too early to mark an end of the endeavours to acknowledge the collection of metadata as not less intrusive, than the interception of the content of communications", V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, op. cit., p. 14.

[78] L. WOODS, *Analysis of the ECtHR judgement in Big Brother Watch (Part 1 and 2)*, in *EU Analysis Blog*, 16 settembre 2018; ma anche: T. CHRISTAKIS, *A fragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch Judgement*, op. cit e M. MILANOVIC, *ECtHR Judgement in Big Brother Watch v. UK*, in *EJIL Talk*, 17 settembre 2018.

[79] Non bisogna infatti farsi influenzare da letture eccessivamente generalizzatrici: è necessario contestualizzare le conclusioni cui la Corte giunge allo specifico quadro normativo sottoposto alla sua attenzione. Come già sottolineato è innegabile come le normative svedese e inglese presentino tutele e salvaguardie maggiormente robuste ed ampie rispetto alle discipline contenute nella legislazione russa e ungherese.

[80] "Until not long ago, the case law of the Strasbourg Court seemed to have followed the Court of Justice's 'deep pass' with regard to the balancing of digital privacy and national security measures", E. CELESTE, *The Court of Justice and the ban on bulk Data Retention: expansive potential and future scenarios*, op. cit., p. 153.

[81] T. CHRISTAKIS, *A fragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch Judgement*, op. cit.

[82] Per una analisi delle richieste dei ricorrenti dinnanzi alla Grande Camera sia in *Centrum* che nel caso *BBW*, si rimanda a quanto si dirà in seguito, nonché, più approfonditamente, a M. AZARMI, *European Court of Human Rights to reexamine bulk collection*, in *European Union Security & Surveillance*, 4 marzo 2019.

2. – Problematiche ancora aperte: i motivi del rinvio alla Grande Camera nei casi **Centrum For Rattvisa** *e* **Big Brother Watch** *e il contributo della sentenza* **Catt c. Regno Unito**

Come si è avuto modo di sottolineare già nel corso dei previ paragrafi, le questioni che la Corte EDU è stata chiamata, nel corso dei decenni, ad affrontare in materia di sorveglianza di massa sono molteplici, a partire dai casi *Weber* o *Klass,* sino a giungere alle più recenti pronunce che si inseriscono in un contesto caratterizzato dall'uso delle moderne tecnologie e, dunque, da nuove e complesse sfide; alcune di queste sembrano ormai aver ricevuto una risposta chiara e confermata nel tempo, altre invece rimangono ancora aperte, mentre il progresso tecnico e la concreta attuazione di innovativi e sofisticati strumenti di sorveglianza impongono di ripensare ad alcune distinzioni 'classiche', di cui giudici e legislatori si sono per decenni serviti. In quest'ultima categoria rientra certamente la classificazione tra sistemi di *bulk interception* per finalità di sicurezza nazionale poste in essere da autorità di intelligence e strumenti di *interception* (targettizzata o generalizzata) per finalità di repressione di crimini gravi ad opera di autorità di *law enforcement*. Questa distinzione, le cui conseguenze emergono con maggior evidenza nell'ambito del diritto dell'UE[83] ma che assumono tuttavia importante rilievo anche nella giurisprudenza della Corte EDU, porta a riflettere con rinnovata attenzione sui diversi concetti, già brevemente accennati, di *strategic surveillance* e *surveillance* per scopi di *law enforcement*. Una prima definizione, proposta dalla Commissione di Venezia, è quella che afferma: "Strategic surveillance thus differs in a number of ways from surveillance in law enforcement or more traditional internal security operations. It does not necessarily start with a suspicion against a particular person or persons. It can instead be proactive: finding a danger rather than investigating a known danger. Herein lay both the value it can have for security operations, and the risk it can pose for individual rights. Prosecution is not the main purpose of gathering intelligence. The intelligence is, however, stored and used in a number of ways which can affect human rights"[84]. Se questa osservazione è certamente meritevole di rilievo, non può tuttavia ignorarsi come non solo le minacce globali e ramificate del terrorismo internazionale ma anche il carattere sempre più transfrontaliero dei crimini gravi (traffico di droga, traffico di esseri umani, traffico di armi) rendano sempre più difficile applicare con chiarezza la differenziazione proposta. Il confine infatti tra le attività di intelligence, volte preminentemente alla tutela della sicurezza nazionale, e le misure poste in essere dalle autorità di *law enforcement* è in realtà ormai molto sfumato: "law enforcement authorities turn to tackling external threats and adopt intelligence type of strategies and techniques in fighting crime and increasingly cooperate with intelligence services. (..) The so called 'intelligence – led policing' allows for police to employ more invasive, secret-service type of powers, while also resorting to these technologies of surveillance for the prevention of crime that are more sophisticated than ever"[85]. A dimostrazione di quanto gli strumenti di sorveglianza e raccolta

[83] Come già ampiamente analizzato nei Capitoli precedenti, infatti, la questione assume grande importanza nel contesto dell'Unione europea, diventando un punto di rilievo nella determinazione del confine tra le competenze dell'UE stessa e quelle degli Stati membri.

[84] *Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies*, 2015, p. 12.

[85] P. VOGIATZOGLOU, *Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity*, in *European Journal of Law and Technology*, 1, 2019, p. 3; sul punto si legga anche A. ZAVRSNIK, *Blurring the line between law enforcement and intelligence: sharpening the gaze of surveillance?*, in *Journal of contemporary european research*, 1, 2013. Interessante vedere come lo sviluppo tecnologico, la raccolta di dati massiva ed i moderni strumenti di intelligenza artificiale stiano permettendo un utilizzo sempre più estensivo di sistemi di *pre-emptive policing*, intesa quale "Application of analytical, particularly quantitative, techniques in order to identify likely targets for police intervention and prevent crime or solve past crimes by making statistical predictions", bloccando – mediante tecniche di *Big Data analytics* (tra cui *data mining*) – la possibilità che un crimine venga compiuto. Per un maggiore approfondimento si veda anche: R. VAN BRAKEL, P. DE HERT, *Policing surveillance and law in a pre-crime society: understanding the consequences of technology based strategies*, Cahiers Politiestudies Jaargag, 3, 2011; W. L. PERRY ET AL., *Predictive policing. The role of*

generalizzata delle telecomunicazioni elettroniche siano ormai ampiamente utilizzati anche dalle autorità di *law enforcement*, è sufficiente richiamare i dati dell'*Annual Report of the Interception of Communications Commissioner* del 2016, riportati nella sentenza *Big Brother Watch*, con riferimento allo specifico caso del Regno Unito e all'impiego di metadata per scopi securitari: "According to the report, police forces and law enforcement agencies were responsible for acquiring ninety-three percent of the total number of items of data in 2016, six percent was acquired by intelligence services and the remaining one percent was acquired by other public authorities, including local authorities. (..) With regard to the purpose of the request, eighty-three percent of the items of data were acquired for the purpose of preventing or detecting crime or preventing disorder; eleven percent were acquired for the purpose of preventing death or injury or damage to a person's mental health, or of mitigating any injury or damage to a person's physical or mental health; and six percent were acquired in the interests of national security" (par. 189 - 190)[86]. Questa sempre maggiore difficoltà di determinare una chiara differenziazione dei sistemi di sorveglianza che sia fondata sui soggetti che li impiegano e sugli scopi perseguiti, si riverbera anche nelle salvaguardie e nelle tutele richieste dalla Corte EDU stessa: con riferimento ad esempio al caso *Centrum For Rattvisa*, avente ad oggetto esclusivamente operazioni di *Foreign Intelligence*, viene ampiamente richiamata la pronuncia *Zakharov* che riguardava invece intercettazioni primariamente poste in essere da autorità di *law enforcement* per finalità legate prevalentemente alla prevenzione e repressione di crimini[87]. Come anticipato, ciò dovrebbe dunque far ritenere che, salvo eccezioni espressamente previste, i requisiti e principi affermati dalla Corte EDU nella sua giurisprudenza possano valere con riferimento a tutti i sistemi di sorveglianza, indipendentemente dall'autorità che li utilizza e dalla finalità cui essi sono preposti. Già nella sentenza *Liberty*, del resto, i giudici avevano affermato: "It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses. However, the *Weber and Saravia* case was itself concerned with generalised "strategic monitoring", rather than the monitoring of individuals. The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other" (par. 63). Tali considerazioni risultano sicuramente di grande rilevanza anche rispetto alla giurisprudenza della CGUE, la quale, come si è ampiamente detto, è ora chiamata a pronunciarsi in numerosi rinvii che affrontano la questione di una possibile distinzione tra sicurezza pubblica e nazionale e tra requisiti e salvaguardie da porre in essere.

Un'altra problematica distinzione da considerare, non ancora del tutto chiarita dalla Corte EDU e oggetto di attenzione in particolare nelle sentenze *Centrum For Rattvisa* e *Big Brother Watch*, è quella

---

crime forecasting in law enforcement operations, Rand Corporation, 2013; F. COUDERT, *Precrime police is not for 2054, it's for now: how to regulate data intensive policing?*, Submission to the Amsterdam Privacy Conference, 2015. Una sempre maggiore consapevolezza e conoscenza della complessità delle sfide poste dalle nuove tecniche di sorveglianza, prevenzione e repressione dei crimini deve indurre ad una riflessione seria da parte del mondo del diritto, legislatori e giudici, che sia in grado di considerare la profondità dei rischi tecnici (di *bias* algoritmico, di pregiudizio derivante dalla scelta di alcune aree geografiche o fasce di popolazione da assoggettare a sorveglianza mirata, come già ampiamente visto nei Capitoli precedenti), e che valuti dunque la possibilità di adottare disposizioni o decisioni che tengano conto della diversa necessità di tutele, e dunque di salvaguardie e parametri, a seconda che si consideri il momento di *preventive* e *predictive processing* o quello invece successivo di repressione e indagine. Sul punto si richiama anche la Data Retention Directive, analizzata nei Capitoli I e II: benché tale Direttiva disciplinasse la conservazione dei metadati, mentre per quanto riguarda l'accesso esso era lasciato alla regolamentazione degli Stati membri che avrebbero però dovuto limitarlo a finalità di repressione di crimini gravi, era ben presto emerso come i legislatori nazionali avessero in realtà ampliato l'utilizzo dei dati conservati anche per scopi di prevenzione dei reati da parte di autorità di intelligence.

[86] Ciò è peraltro sottolineato anche da J. VERMEULEN, *Big brother may continue watching you*, in *Strasbourg Observers*, 12 ottobre 2018.

[87] Tra gli altri, P. VOGIATZOGLOU, *Centrum For Rattvisa v. Sweden: bulk interception of communications by Intelligence Services does not violate the right to privacy*, op. cit., p. 566.

che vede contrapposte le comunicazioni meramente interne a quelle esterne. Una tale differenziazione, infatti, è posta alla base di quell'approccio, in parte seguito anche dalla Corte, che individua nelle operazioni di *Foreign Intelligence*, proprio in quanto aventi ad oggetto comunicazioni esterne e quindi più generalmente dirette a colpire soggetti stranieri, una minore intrusività nella sfera privata dei cittadini svedesi o inglesi[88]. La criticità di questa affermazione tuttavia risiede nel fatto che l'esclusione dall'ambito di applicazione della normativa svedese o inglese in materia di *Foreign* o *Signals Intelligence* delle comunicazioni meramente interne non è in realtà in grado di evitare del tutto il coinvolgimento dei cittadini svedesi o inglesi nelle operazioni di sorveglianza[89]: la definizione di 'external communication' è infatti "a communication sent or received outside the British Islands. This does not, therefore, exclude the interception of communications where one of the parties is in the British Islands" (par. 516, *Big Brother Watch*); sulla base di questa definizione, sono però poi i giudici stessi ad ammettere come spesso anche comunicazioni esclusivamente interne siano state oggetto, pur 'incidentalmente', di intercettazioni nell'ambito di operazioni di *Foreign Intelligence*[90], mettendo peraltro in luce la sempre maggiore difficoltà di delineare chiari confini tra natura interna ed esterna delle comunicazioni, dinnanzi al progresso tecnologico, alla globalizzazione e 'a-territorialità' dei sistemi di comunicazione[91]. Certamente, in linea generale, forme di sorveglianza che colpiscono principalmente comunicazioni che travalicano i confini nazionali, risultano più accettabili per l'opinione

[88] Di questo parere è certamente il governo inglese nel caso *Big Brother Watch*: "Although the Government denied that the section 8(4) regime permitted mass surveillance or generalised access to communications, it accepted that it permitted, pursuant to the lawful authority of warrants, the bulk interception of bearers for wanted external communications. In the Government's opinion, *the distinction between "internal" and "external" communications was sufficiently clear, and in any event it operated primarily as a safeguard at the macro level*; that is, in determining which bearers should be targeted for interception" (par. 284, enfasi aggiunta).

[89] Per meglio comprendere i criteri che determinano la natura interna o esterna di una comunicazione, pare utile richiamare il par. 70 della *Big Brother Watch*: "In the course of the *Liberty* proceedings, Charles Farr, the Director General of the OSCT, indicated that two people in the United Kingdom who email each other are engaging in "internal communication" even if the email service was housed on a server in the United States of America; however, that communication may be intercepted as a "by-catch" of a warrant targeting external communications. On the other hand, a person in the United Kingdom who communicates with a search engine overseas is engaging in an external communication, as is a person in the United Kingdom who posts a public message (such as a tweet or Facebook status update), unless all the recipients of that message are in the British Islands". Come ben emerge da questa spiegazione, anche le comunicazioni che rientrano nella definizione di 'external', in realtà, sono suscettibili di colpire numerose attività di comunicazione svolte da cittadini inglesi.

[90] "Section 5(6)(a) of RIPA makes clear that the conduct authorised by a section 8(4) warrant may, in principle, include the interception of communications which are not external communications to the extent this is necessary in order to intercept the external communications to which the warrant relates", par. 6.6 dell' Interception of Communication Code of Practice ("the IC Code").

[91] Questa difficoltà di delineare una netta distinzione è peraltro non solo sottolineata dai ricorrenti bensì riconosciuta anche dal *Investigatory Powers Tribunal*: "the applicants had contended that following the 'sea-change in technology since 2000' substantially more communications were now external, and as a result the internal/external distinction in section 8(4) was no longer 'fit for purpose'. While the IPT accepted that the changes in technology had been substantial, and that it was impossible to differentiate at interception stage between external and internal communications, it found that the differences in view as to the precise definition of external communications did not *per se* render the section 8(4) regime incompatible with Article 8 § 2. In this regard, it considered that the difficulty in distinguishing between 'internal' and 'external' communications had existed since the enactment of RIPA and the changes in technology had not materially added to the quantity or proportion of communications which could or could not be differentiated as being external or internal at the time of interception. At worst, they had 'accelerated the process of more things in the world on a true analysis being external than internal'. In any case the distinction was only relevant at interception stage" (par. 42, *Big Brother Watch*). Anche l'*Intelligence and Security Committee of Parliament* ("the ISC") nel proprio Report del luglio 2013, richiamato dai giudici nella pronuncia *Big Brother Watch*, ha evidenziato come: "In respect of Internet communications, the ISC considered that the current system of 'internal' and 'external' communications was confusing and lacked transparency and it therefore suggested that the Government publish an explanation of which Internet communications fall under which category, including a clear and comprehensive list of communications" (par. 154).

pubblica e sono considerate meno lesive dei diritti della riservatezza e della protezione dei dati; se questo ragionamento però fosse diffuso e considerando che ogni Stato dispone ormai di misure di *Foreign Intelligence* e dunque di sorveglianza di comunicazioni caratterizzate da un qualche elemento di 'estraneità', si arriverebbe ad affermare correttamente che '*we are all foreigners*', che siamo cioè tutti stranieri rispetto ad uno Stato terzo e, in quanto tali, assoggettabili a forme di *Foreign Inteeligence* da parte di altre nazioni. Con questa consapevolezza e allontanandosi da un'interpretazione che vede nell'esclusione delle comunicazioni interne una sufficiente forma di protezione e tutela, si dovrebbe riconoscere un interesse reciproco e diffuso ad individuare e condividere principi comuni in materia di *data protection* e privacy, come possibile soluzione alla presenza di differenti livelli di tutela garantiti nei diversi ordinamenti, capaci di incidere sui diritti di tutti i cittadini che, inevitabilmente, possono divenire 'stranieri' per uno Stato terzo[92]. Questa esigenza risulta del resto ancor più sentita anche alla luce delle recenti posizioni della Corte EDU in materia di *Intelligence Sharing*, sulla base delle quali il controllo – e la responsabilità e giurisdizione dello Stato – circa il rispetto di idonee garanzie e salvaguardie da parte di sistemi di sorveglianza operanti in altri Stati deve essere limitato alla sola fase di selezione e trattamento (*processing*) dei dati richiesti e ricevuti da autorità di Intelligence straniere, mentre rimane esclusa da qualsiasi valutazione la fase di raccolta, che può anche non prevedere alcuna garanzia per i soggetti sottoposti a sorveglianza. Il ricorso sempre più diffuso ad operazioni di richiesta e scambio di dati e informazioni tra Stati può tradursi quindi in uno strumento impiegato dalle autorità nazionali per aggirare i limiti posti dal diritto interno: questa continua commistione tra dimensione interna ed esterna porta a comprendere, in maniera chiara ed evidente, come stia divenendo sempre più difficile stabilire distinzioni basate sui confini nazionali nell'ambito delle sofisticate e articolate moderne operazioni di intelligence.

Tutti i profili problematici sino ad ora evidenziati, unitamente alle rilevate discrepanze tra le salvaguardie affermate nelle ultime pronunce della Corte EDU e quelle precedenti, assumono un rilievo centrale anche in considerazione dei numerosi casi al momento ancora sul tavolo dei giudici di Strasburgo. Si pensi innanzitutto ai già richiamati e ad oggi pendenti rinvii alla Grande Camera dei casi *Centrum for Rattvisa* e *Big Brother Watch*, rinvii auspicati peraltro dai giudici Turkovic e Koskelo nella loro *Partly Dissenting and Partly Concurring Opinion*: "I'm not convinced that reliance on the Court's existing case law provides an adequate approach to the kind of surveillance regimes like the one we are dealing with here. A more thorough reconsideration [con riferimento alla richiesta dei ricorrenti di aggiornare i criteri della sentenza *Weber*] would be called for. I acknowledge that this would be a task for the Court's Grand Chamber" (par. 3, *Big Brother Watch*).

Quello che risulta però in questa sede interessante è evidenziare il differente approccio tenuto dai ricorrenti Centrum for Rattvisa e Big Brother Watch (e altre ONG) nelle rispettive *Request for referral* alla Grande Camera, entrambe accolte, come si è detto, a seguito del vaglio di un apposito *Panel* a tale valutazione preposto. Nel primo caso, infatti, la ONG svedese non ha posto in discussione la decisione della Corte nella parte in cui afferma, *de facto*, la legittimità e proporzionalità di sistemi di *bulk interception* per finalità esclusive di sicurezza nazionale; gli aspetti sui quali invece viene richiesto l'intervento chiarificatore della Grande Camera attengono alla corretta individuazione delle salvaguardie minime, all'esclusione del requisito di 'reasonable suspicion', al ruolo di controllo da parte di un organo giudiziario indipendente nonché alla mancata determinazione di salvaguardie minime nell'ambito delle operazioni di *Intelligence Sharing*. Ciò che, in altre parole, viene criticato dalla ricorrente è la restrizione del livello di tutele e garanzie stabilito dalla Corte[93]: in ultima analisi, "these two judgments [*Centrum for Rattvisa* e *Big Brother Watch* appunto], therefore, do not lay down a clear

[92] M. COLE, *We are all foreigners: NSA spying and the rights of others*, in *Just security blog*, 29 ottobre 2013.

[93] Particolare attenzione è stata prestata dai ricorrenti anche alla controversa posizione della Corte EDU nella parte in cui ha affermato, come si è visto, l'incompatibilità, per natura, di forme di *bulk interception* con i criteri del 'ragionevole sospetto' e dell'obbligo di successiva notifica.

and consistent interpretation of how Member States must uphold their obligations under Article 8 of the Convention when conducting bulk interception activities" (par. 21, *Request for referral to the Gran Chamber*, Centrum for Rattvisa). Nel ricorso di Big Brother Watch, la ricorrente invece contesta la posizione della Corte nella parte in cui afferma la conformità di sistemi di *bulk interception* e la loro riconducibilità al margine di apprezzamento riconosciuto in capo ai singoli Stati[94]. Nonostante questa rilevante preliminare differenza di approccio dei due ricorrenti sul tema centrale della intercettazione generalizzata e della sua legittimità e proporzionalità, entrambe le parti mostrano però poi di condividere una posizione fortemente critica avverso la decisione della Corte EDU di non aggiornare i criteri delineati nella sentenza *Weber* e di ritenere tali requisiti rispettati dalle normative esaminate, nonché avverso la scelta di non inserire nel novero delle salvaguardie minime la previa autorizzazione giudiziaria e nella posizione tenuta in materia di *Intelligence Sharing*. Sotto tutti questi profili, i ricorrenti ritengono che le sentenze impugnate possano avere il pericoloso effetto di 'diluire' i requisiti fissati nella sentenza *Zakharov* e di stabilire limiti e garanzie eccessivamente blandi ed ampi in un contesto, quale quello dei sistemi di *bulk interception*, che necessiterebbe al contrario di maggiori e più restrittive tutele.

I rinvii dinnanzi alla Grande Camera dei casi sopra richiamati tuttavia non sono gli unici procedimenti al momento pendenti in materia di sorveglianza di massa: si pensi al ricorso *Tretter et al. c. Austria* (2013), che riguarda il Police Powers Act austriaco (nella traduzione inglese dell'atto utilizzata dai giudici di Strasburgo); alla controversia *Association confraternelle del la presse judiciaire et 11 autres requetes c. France* (2017) avente ad oggetto la compatibilità della normativa francese in materia di intelligence del 2015 rispetto artt. 8, 10 e 13 CEDU e ancora a *Privacy International and Others c. Regno Unito* (2018), concernente l'*Intelligence Services Act* del Regno Unito.

Si vuole infine mettere in evidenza come di recente la Corte si sia nuovamente occupata di alcuni aspetti tangenzialmente connessi al tema della sorveglianza nel caso *Catt c. Regno Unito*, ricorso n. 43514715, deciso il 24 gennaio 2019 dalla Prima Camera. Tale pronuncia, pur non avendo ad oggetto la compatibilità alla CEDU di un regime normativo considerato *in abstracto* bensì vertendo sulla specifica situazione del ricorrente, presenta interessanti spunti di riflessione circa la legittimità delle operazioni poste in essere da forze dell'ordine e relative alla raccolta e conservazione di informazioni riguardanti singoli cittadini. La Corte, infatti, ha in questo caso riscontrato una violazione dell'8 CEDU a scapito del ricorrente, il Signor Catt, i cui dati relativi alla partecipazione a manifestazioni pacifiche e di carattere sindacale erano stati conservati dalla polizia in un apposito database, senza che il ricorrente fosse mai stato sospettato, indagato o condannato per aver commesso o partecipato ad attività criminose. Il ricorrente aveva sostenuto che sia la *data retention* che la previa sistematica raccolta di informazioni riguardanti la sua persona costituissero, unitamente, una violazione dell'art. 8 della Convenzione e una ingerenza sproporzionata nella propria sfera privata; la Corte non ha però totalmente accolto tale posizione, ritenendo non rispondente al requisito di 'necessità in una società democratica' la sola disciplina della conservazione, che prevedeva una *data retention* illimitata nel tempo e che non consentiva di addivenire alla cancellazione dei dati qualora fosse trascorso un ragionevole termine di tempo, non meglio delimitato e definibile[95]. Pur ribadendo che il mero 'immagazzinamento' (*storage*)

[94] Si richiama sul punto quanto già evidenziato nei previ paragrafi, nei quali è stata descritta la posizione dei ricorrenti e le argomentazioni con le quali è stata contestata la decisione della Corte su un aspetto così fondamentale quale la legittimità *per se* del sistema di intercettazione generalizzata.

[95] Tali regole risultano da specifiche disposizioni del *Data Protection Act* nonché dal *Code of Practice on the Management of Police Information* (MOPI) del 2005, che consentono di conservare i dati raccolti dalle forze di polizia qualora essi non siano eccessivi, siano necessari per *policing-purposes* e limitatamente ad un periodo di 6 anni, oltre il quale i dati devono essere controllati (vagliandone l'utilità della conservazione) e quindi eventualmente cancellati, pur non stabilendo un momento preciso entro cui tale controllo e revisione dei dati conservati debba avvenire. Interessante è anche notare come questa peculiare fonte del MOPI sia stata ritenuta dalla Corte conforme al requisito 'in accordance with the law': la Corte infatti inizialmente ha espresso riserve

di informazioni personali rappresenta, prima ancora dell'accesso ed utilizzo dei dati stessi, una intrusione nella sfera privata[96], i giudici hanno optato per una netta distinzione tra, da un lato, legittimità e proporzionalità della raccolta indiscriminata di informazioni per scopi securitari (in questo caso di prevenzione e repressione di crimini) e dall'altro della conservazione in database. Quanto al primo profilo i giudici, concordando con i rilievi della Corte Suprema inglese, hanno considerato "in the nature of intelligence gathering that the police will first need to collect the data, before evaluating its value" (par. 114), con una affermazione di grande rilevanza anche per il tema sino ad ora affrontato della proporzionalità e necessità di misure di sorveglianza. Pare così essere stabilita la legittimità di sistemi di raccolta di informazioni mossi dalla logica del "collect-it-all" o del 'nice-to-have': tali operazioni divengono il prerequisito necessario per poter poi provvedere ad una successiva 'scrematura' e analisi dei soli dati considerati potenzialmente utili, imponendo pertanto unicamente nel secondo momento della conservazione e utilizzo delle informazioni la predisposizione di salvaguardie e criteri più restrittivi. Sebbene con riferimento ad un caso molto differente da quelli sino ad ora oggetto di analisi, la Corte sembra seguire il ragionamento espresso in *Centrum for Rattvisa* e in *Big Brother Watch*, secondo cui la raccolta – in quel caso intercettazione – generalizzata di dati è da considerarsi necessaria e proporzionata per la natura stessa dei sistemi di sorveglianza, mentre la carenza di limitazioni in tale fase viene sopperita dalla imposizione di specifiche salvaguardie e controlli nella fase successiva di selezione e 'filtraggio' dei dati raccolti nonché di loro conservazione, utilizzo e trattamento. Proseguendo su questa linea, dunque, i giudici hanno vagliato le operazioni di conservazione delle informazioni: ebbene, esse non sono state ritenute rispondenti ad un 'pressing need'; anche in questo caso però merita precisare come oggetto della critica non fosse la conservazione stessa, cioè il fatto che la polizia possa avere necessità, nel caso di un eventuale futuro ma non certo processo, di immagazzinare il dato successivamente al momento di raccolta, bensì quello che viene ritenuto in violazione dell'art. 8 CEDU è il fatto che "in the absence of any rules setting a definitive maximum time limit on the retention of such data, the applicant was entirely reliant on the diligent application of the highly flexible safeguards in the MOPI to ensure the proportionate retention of his data. Where the state chooses to put in place such a system, the necessity of the effective procedural safeguards becomes decisive. Those safeguards must enable the deletion of any such data, once its continued retention becomes disproportionate" (par. 119). La problematicità della disciplina quindi viene ravvisata nella mancanza di limiti nella fase di *data retention*, che risulta sproporzionata nel caso in esame, anche alla luce del fatto che il ricorrente non era mai stato considerato in alcun momento pericoloso (par. 122) e che i dati trattenuti erano di natura 'sensibile' in quanto idonei a rivelare le convinzioni politiche del ricorrente[97]. Sotto il solo profilo dunque della carenza di uno specifico limite temporale certo di conservazione (che apre potenzialmente ad una conservazione eterna) nonché della assenza di un obbligo di cancellazione delle informazioni raccolte una volta che esse non siano più di alcuna utilità, viene dunque dichiarata la violazione dell'art. 8 CEDU. Insomma si nota anche in questo caso, che pure ha ad oggetto una disciplina normativa ed operazioni maggiormente circoscritte, una presa di posizione della Corte nella direzione,

circa l'ambiguità della base giuridica e della normativa su cui si fonda la raccolta dei dati personali connessi e finalizzati a limitare fenomeni di c.d. *domestic extremism*, termine quest'ultimo non meglio definito dalla normativa e dunque esso stesso particolarmente critico; nonostante tali rilievi, la Corte ha considerato comunque di dover leggere il requisito di 'conformità ad una legge' non isolatamente ma in relazione a quello di 'necessità in una società democratica', sul quale i giudici hanno concentrato maggiormente il proprio vaglio. Merita sottolineare come proprio su questa presa di posizione della Corte si fondi la critica maggiore mossa dai giudici Koskelo e Felici nella loro *Concurring Opinion*.

[96] Oltre al noto caso *S. e Marper c. Regno Unito* in materia di dati genetici, la Corte richiama anche le salvaguardie e i principi stabiliti in *Zakharov* e *Szabo*: pur rimarcando la differenza della situazione fattuale di base, che in quei casi riguardava misure di sorveglianza segreta, viene comunque rilevata una comunanza dei pericoli che, in entrambi i sistemi, derivano da una certa ambiguità e rischio di arbitrarietà dei poteri pubblici.

[97] Per una lettura più approfondita di tale pronuncia si rimanda a: J. VERMEULEN, *Another case of violating privacy and personal data protection: Catt v. the United Kingdom*, in *Strasbourg Observers*, 22 febbraio 2019.

già intrapresa nelle due pronunce del 2018, dell'ammissibilità di pratiche generalizzate di raccolta e 'storaggio' di informazioni: esse non debbono prevedere la sussistenza di criteri oggettivi, quali il 'ragionevole sospetto', a giustificazione della misura di controllo e sorveglianza attuata che, per sua natura, richiede di essere ampia e generalizzata per risultare strumento utile ed efficace in un possibile momento futuro. Anche sotto il profilo della *data retention* è però riscontrabile un certo allontanamento dalla giurisprudenza più risalente della stessa Corte: mentre in *Zakharov* infatti veniva affermato con chiarezza che "[the Court] deplores the lack of a requirement to destroy immediately any data that are not relevant to the purpose for which they have been obtained (compare Klass and Others, cited above, § 52, and Kennedy, cited above, § 162). The automatic storage for six months of clearly irrelevant data cannot be considered justified under Article 8" (par. 255), ritenendo dunque contraria alla CEDU una conservazione di dati non rilevanti rispetto all'obiettivo della raccolta stessa, si può notare come nella pronuncia ora esaminata venga concessa invece una conservazione di dati che non presentano una immediata connessione o utilità con l'obiettivo perseguito, soprattutto se si pensa a informazioni, come quelle riguardanti il ricorrente Signor Catt che non era mai stato sospettato o indagato per la commissione di alcun reato. Rispetto a tali informazioni dunque non è predisposto alcun 'filtro' o vaglio che possa giustificare l'interesse legittimo ad una conservazione; ciò che viene criticato dalla Corte in quest'ultima pronuncia non è infatti la possibilità *per se* di conservare genericamente dati senza che venga richiesta la sussistenza di un nesso con una minaccia o pericolo, bensì l'assenza di limiti temporali e di chiare disposizioni circa le condizioni di cancellazione e distruzione dei dati stessi. Significativo sul punto è quanto affermato dai giudici: "It shares the domestic courts' concern that there is a need for caution before overriding the judgment of the police about what information is likely to assist them in their task. *In this respect, the Court underlines that its conclusion does not call into question the fact that there may have been a pressing need for the police to retain the applicant's personal data for a period of time after it was collected*" (par. 119, enfasi aggiunta).

3. – Da Strasburgo a Lussemburgo: punti di contatto e divergenze nelle decisioni delle due Corti europee

Le riflessioni sino ad ora svolte con riferimento alla giurisprudenza della Corte EDU e alla sua evoluzione più recente – non ancora confermata né sconfessata tuttavia dalla Grande Camera – non possono però non essere lette in rapporto allo storico filone giurisprudenziale della Corte di giustizia dell'UE in materia di *data retention* e accesso ai metadati nonché alle pronunce circa il trasferimento di dati verso Stati terzi. Sebbene alcuni cenni e primi confronti tra i due differenti approcci siano già stati svolti nel corso dei precedenti paragrafi, pare purtuttavia utile mettere a sistema e raccogliere ora i rilievi che devono necessariamente scaturire da una lettura congiunta dei casi analizzati in questo e nei precedenti capitoli. Ciò allo scopo ultimo di mettere in luce le divergenze o le convergenze riscontrabili tra le posizioni espresse dalle due Corti europee in materia di raccolta, trattamento e accesso ai dati e metadati derivanti dai moderni sistemi di telecomunicazione ma anche di sottolineare le differenze fattuali e casistiche che impediscono una piena sovrapposizione delle posizioni. Come è già stato più volte precisato, infatti, un raffronto efficace e veritiero tra le sentenze dei giudici di Strasburgo e di Lussemburgo non può non considerare il diverso contesto entro cui gli stessi operano e le difformità dei casi e delle normative che si sono trovati nel tempo ad affrontare e che non devono essere taciute, pena uno stravolgimento delle conclusioni e dei principi stessi affermati. In tal senso, i casi *Centrum for Rattvisa* e *Big Brother Watch*, diversamente dalle decisioni *DRI* o *Tele2*, hanno ad oggetto operazioni di sorveglianza segreta (*Foreign Intelligence, Signals Intelligence* e *Intelligence Sharing*) utilizzate – prevalentemente anche se non esclusivamente – da servizi di intelligence per finalità di sicurezza nazionale e aventi ad oggetto – anche in questo caso prevalentemente ma non esclusivamente – 'external

communications'; le intercettazioni poste in essere nei casi richiamati ma anche nelle previe controversie *Zakharov* e *Szabo* – il caso russo era attinente a forme di sorveglianza finalizzate anche alla tutela della sicurezza pubblica da parte di autorità di *law enforcement* –, concernono inoltre sia i contenuti delle comunicazioni che i metadati. Le pronunce invece di cui si è occupata la Corte di giustizia dell'UE hanno ad oggetto normative disciplinanti principalmente l'obbligo di conservazione dei soli metadati in capo a soggetti privati[98]: mentre la maggior parte delle operazioni e dei sistemi di sorveglianza analizzati dalla Corte EDU prevedono intercettazioni direttamente poste in essere dalle autorità nazionali – siano esse di intelligence o di *law enforcement* –, che quindi non richiedono un intervento di 'mediazione' dei soggetti privati consistente ad esempio nella conservazione da parte delle compagnie di telecomunicazione dei metadati raccolti, nei casi vagliati dalla CGUE i metadati vengono conservati dai *service providers* privati in maniera generalizzata ed indiscriminata – sulla base di una disposizione di legge, nazionale o dell'UE – mentre l'accesso successivo a tali dati avviene ad opera delle autorità di *law enforcement* per finalità di repressione e lotta di crimini gravi[99]. L'unico caso in cui, sebbene indirettamente, la Corte di giustizia si è occupata di forme di trattamento del contenuto dei dati raccolti e conservati da aziende private è da individuarsi nel caso *Schrems*: in quell'occasione, così come precedentemente in *DRI*, i giudici avevano ritenuto l'accesso generalizzato e indiscriminato al contenuto delle comunicazioni lesivo del nucleo essenziale del diritto alla riservatezza, indicando peraltro come non limitata allo stretto necessario la conservazione generalizzata di tutti i dati personali trasferiti dall'UE verso gli USA.

Pur dovendo tenere a mente queste distinzioni ed imprescindibili precisazioni, è comunque possibile confrontare i principi e parametri individuati nei due filoni giurisprudenziali analizzati. Sebbene i richiami alle decisioni dei giudici di Strasburgo da parte della CGUE, nelle sentenze analizzate nei previ Capitoli, siano piuttosto limitati, merita rilevare come nella pronuncia *Tele2* si rinvengano riferimenti sia al caso *Zakharov* che a *Szabo*[100]; nell'affermare infatti la necessaria sussistenza di un criterio oggettivo che permetta di individuare una connessione – almeno indiretta – tra la finalità perseguita e l'accesso ai dati conservati, i giudici di Lussemburgo richiamano quel requisito di *reasonable suspicion* indicato nella sentenza *Zakharov* (par. 119), mentre viene fatto riferimento la pronuncia *Szabo* nella parte in cui afferma l'ulteriore requisito del previo controllo giudiziale (o di un'autorità amministrativa indipendente) sulla base di una richiesta motivata dell'autorità pubblica (par. 120). Forse quest'ultimo

[98] Nel *Parere 1/15* il sistema di scambio di dati tuttavia risulta più circoscritto ed è più difficilmente paragonabile a sistemi, quali quelli di sorveglianza esaminati dalla Corte EDU, che riguardano invece la totalità dei contenuti e metadati delle telecomunicazioni, coinvolgendo potenzialmente – direttamente o indirettamente – tutti i cittadini di uno Stato, pur stabilendo, secondo talune normative, una fase di 'selezione' e 'scrematura' preventiva alla conservazione ed utilizzo delle informazioni.

[99] Risulta chiara la differenza tra la DRD ed un sistema di sorveglianza quale quello posto al vaglio della Corte di Strasburgo in *Big Brother Watch*, nel quale i dati relativi alle comunicazioni (contenuti e metadati) vengono raccolti in maniera generalizzata (*bulk interception*) direttamente da parte dei servizi di intelligence – e in alcuni casi anche da autorità di *law enforcement* – e sottoposti a 'filtraggio' sulla base di procedimenti automatizzati, al termine dei quali le informazioni ritenute di 'intelligence value' vengono conservate e analizzate (quindi mediante trattamento e accesso) dalle competenti autorità. O ancora rispetto al sistema delineato dalla normativa russa in materia di anti-terrorismo che concedeva intercettazioni direttamente ad opera delle autorità pubbliche e potenzialmente illimitate quanto ai soggetti ad esse sottoposte, nonché una conservazione di tutti i dati raccolti per un periodo di sei mesi, indipendentemente dalla rilevanza per l'obiettivo perseguito o dal fatto che essi appartenessero o meno a soggetti indagati, sottoposti a processo o sospettati.

[100] Merita comunque premettere come richiami alla giurisprudenza della Corte EDU siano riscontrabili anche nella sentenza *DRI* e nel *Parere 1/15*: in queste decisioni il riferimento è alle pronunce *Weber, Liberty* e *S. e Marper*, tutte richiamate per sottolineare come anche i giudici di Strasburgo abbiano riconosciuto l'importanza da parte del legislatore di fissare regole chiare e precise a disciplina di normative in materia di sorveglianza o controllo dei dati delle telecomunicazioni; viene quindi rafforzata con tale richiamo la necessità di imporre requisiti minimi e garanzie sufficienti per limitare i rischi di abusi. Né nella decisione *Schrems* e neppure nel caso *Ministerio Fiscal* sono presenti rilievi che facciano riferimento alla giurisprudenza della Corte EDU.

richiamo dei giudici di Lussemburgo risulta meno appropriato ed accurato del primo[101] ma, nonostante questo, una convergenza di massima quanto alle salvaguardie fissate da entrambe le Corti (autorizzazione *ex ante*, rimedi e controlli *ex post*, criterio oggettivo che colleghi la misura di accesso ai dati con la finalità perseguita, notifica successiva) è innegabile e permette quindi di ritenere l'approccio e la posizione dei due giudici sostanzialmente allineata rispetto all'utilizzo di sistemi di sorveglianza massiva delle telecomunicazioni, seppure con le differenze già sottolineate sia in termini di contesto e competenze sia con riferimento alle normative sottoposte al vaglio dei giudici.

Se dunque sino alla pronuncia *Szabo* può individuarsi un allineamento, le ultime due decisioni della Corte EDU, analizzate nei precedenti paragrafi, sembrano segnare un allontanamento tra le posizioni dei giudici: si fa riferimento in particolare al mancato richiamo di alcuni dei criteri che invece rientrano nel novero dei requisiti minimi imposti dai giudici di Lussemburgo (nello specifico si fa riferimento alla previa autorizzazione, quindi ad un controllo *ex ante*, alla sussistenza di criteri oggettivi e alla successiva notifica alle persone interessate). Certo è da evidenziare come, se la CGUE confermasse la tesi promossa dall'Avvocato generale Campos Sanchez-Bordona nei rinvii pregiudiziali pendenti promossi dalle Corti francese, belga e inglese, le attività di *Foreign Intelligence* nonché tutte le attività di intercettazione dei dati effettuate direttamente dalle autorità pubbliche, senza l'intervento di un soggetto privato e dunque senza l'imposizione di un obbligo di conservazione in capo ai fornitori di servizi, risulterebbero escluse dall'ambito di applicazione del diritto dell'UE e dunque non sarebbero sottoposte al controllo e ai requisiti fissati dalla CGUE stessa nella sua giurisprudenza. Per quanto tale aspetto rimanga di grande rilievo e in attesa di definizione, per comprendere i limiti di estensione e i confini dei c.d. 'requisiti *Tele2*', nondimeno possono porsi importanti considerazioni più ampie quanto all'approccio dei due giudici europei con riferimento a forme di sorveglianza generalizzate, nelle sue diverse operazioni di intercettazione, raccolta, conservazione o accesso: da un lato infatti troviamo una Corte, quella dei Diritti Umani, che afferma la conformità rispetto alla Convenzione EDU di forme di *bulk interception*, accettando quindi sistemi di raccolta generalizzata di dati che vengono solo in un secondo momento 'filtrati' e scremati e che sono inoltre passibili di conservazione direttamente da parte delle autorità pubbliche, senza che sia richiesto, quanto meno nelle ultime pronunce, la sussistenza di un criterio oggettivo che connetta il trattamento dei dati – anche riguardanti il contenuto delle comunicazioni – allo scopo perseguito e dunque ad una minaccia o pericolo per la sicurezza; dall'altro lato, l'approccio della CGUE pare invece più restrittivo e maggiormente garantista dei diritti alla riservatezza e alla protezione dei dati: se le si guardano nel loro complesso, le normative poste al vaglio della CGUE riguardano un sistema meno invasivo rispetto a quello oggetto di esame dalla Corte EDU, essendo limitato alla conservazione di soli metadati da parte di operatori privati e non all'intercettazione di entrambi 'content data' e metadati, effettuati direttamente da parte di autorità di intelligence. L'interferenza nella sfera privata sembra quindi più lieve di quella posta in essere da una intercettazione generalizzata, *in bulk*: nonostante questo, tali ingerenze sono state dichiarate dalla CGUE come incompatibili con il diritto UE e in particolare la Carta di Nizza, alla luce del vaglio di proporzionalità e stretta necessità. Per tale motivo, vista la rigidità della visione della CGUE anche con riferimento a situazioni meno invasive della sfera privata, vi è chi individua nella più recente giurisprudenza della Corte di Strasburgo un allontanamento da quel divieto di conservazione e accesso generalizzato e da quella necessità di misure targettizzate e criteri oggettivi che i giudici di Lussemburgo hanno più volte affermato[102]; il confuso

[101] In questi paragrafi infatti la Corte EDU riconosce come il requisito della previa autorizzazione possa essere superato laddove vi sia un "extensive *post factum* judicial oversight" (par. 77), ribadendo come solo in determinate circostanze, ad esempio dinnanzi a misure di sorveglianza estese anche ai *media*, tale requisito di controllo *ex ante* sia obbligatorio.

[102] "According to this vision, the nature of dangers that contemporary society faces legitimises the use of bulk interception and collection of data, as only these techniques can really help uncover otherwise hidden threats. The very issue would instead lie in setting the appropriate guarantees delimiting the power of national authorities to exploit this unprecedented amount of data. In conclusion, such a position contrasts with the outright ban on bulk

confine tra attività poste in essere da autorità di intelligence e autorità di *law enforcement* nonché tra finalità di sicurezza nazionale e sicurezza pubblica, che anche nella casistica analizzata dalla CGUE paiono avere tratti poco definiti, mette in dubbio quella lettura che porterebbe a ritenere la maggiore invasività posta in essere da forme di *bulk interception* come maggiormente accettabile dinnanzi alla necessità, ben più 'fondamentale', di tutela della sicurezza nazionale, che giustifica dunque una più significativa compressione della sfera privata.

Mentre poi la CGUE distingue tra contenuti e metadati, ritenendo la raccolta e accesso massivo ai primi come lesivi della essenza del diritto stesso alla riservatezza, i giudici di Strasburgo non propongono questa distinzione: se da un lato è vero che non esiste una disposizione simile all'art. 52 della Carta di Nizza nella Convenzione EDU e che in quest'ultima è lo stesso art. 8, co. 2, più volte richiamato, a fissare le condizioni che consentono una ingerenza nell'esercizio di tale diritto da parte delle autorità pubbliche, è altrettanto vero che, nelle sue valutazioni circa la 'necessità in una società democratica', la Corte EDU non ritiene il sistema di *bulk interception* dei 'content data' come incompatibile, per natura, con il diritto al rispetto della vita privata e non propone dunque una netta differenziazione in termini di tutele e salvaguardie a seconda delle tipologie di informazioni raccolte e sottoposte a trattamento.

Altro punto sul quale le Corti sembrano divergere è quello riguardante la maggiore o minore appropriatezza di sistemi di sorveglianza targettizzata rispetto a forme generalizzate: mentre la CGUE riscontra in quella 'mirata' l'unica – quanto meno per il momento – forma legittima e accettabile di conservazione e accesso ai metadati – che siano cioè targettizzati ad uno specifico periodo di tempo, ad una zona geografica e/o ad una cerchia di persone suscettibili di essere implicate in una violazione grave o i cui dati potrebbero contribuire alla lotta contro la criminalità (par. 106, *Tele2*)[103] –, la Corte EDU, invece, nella sentenza *Big Brother Watch*, come si è sottolineato nei precedenti paragrafi, mette in dubbio la minore lesività di sistemi di raccolta, conservazione e accesso targettizzati ai dati, non rinvenendo quindi necessariamente in tale forma più limitata di sorveglianza una soluzione sufficiente e necessaria.

In conclusione, pur tenendo a mente le rilevanti differenze di fondo sia nei casi esaminati sia nello scrutinio stesso effettuato[104] e considerando i punti di contatto che pure non mancano anche nelle più recenti pronunce[105], alcune divergenze tra i principi e il bilanciamento effettuato dalle due Corti in materia di sorveglianza generalizzata sono individuabili soprattutto nelle sentenze *Centrum for Rattvisa* e *Big Brother Watch*.

---

data retention so far maintained by the Court of Justice", E. CELESTE, *The Court of Justice and the ban on bulk Data Retention: expansive potential and future scenarios*, op. cit., p. 153.

[103] Nella sentenza *Tele2* inoltre viene specificato come l'accesso ai dati 'di altre persone' (da intendersi come accesso ai dati di soggetti individuati al di fuori dell'applicazione dei criteri di un accesso targettizzato) sia consentito solo in via eccezionale – ad esempio quando interessi vitali quali sicurezza nazionale, difesa o sicurezza pubblica siano minacciati da attività di terrorismo – e "quando sussistano elementi oggettivi che consentano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro simili attività" (par. 119): da tale posizione emerge pertanto l'orientamento maggiormente restrittivo adottato dalla Corte di giustizia, che ammette un accesso più generalizzato solo in casi di particolare eccezionalità e potenziale ingente pericolo nonché richiedendo comunque la sussistenza di prove o sospetti fondati su dati oggettivi che connettano l'accesso ai dati ad un determinato pericolo.

[104] Per una più ampia ricostruzione delle rilevanti pronunce delle due Corti in materia di tutela della riservatezza, utile a mettere in evidenza differenze e vicinanze interpretative oltre alle diversità derivanti dai testi delle due Carte dei diritti con riferimento alla tutela della vita privata e della protezione dei dati, si leggano: J. KOKOTT, C. SABOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 4, 2013; S. O'LEARY, *A tale of two Cities: fundamental rights protection in Strasbourg and Luxembourg*, in *Cambridge yearbook of European Law studies*, 20, 2018.

[105] In *Big Brother Watch*, ad esempio, la posizione dei giudici di Strasburgo in merito al regime delineato nel Capitolo II DRIPA, come si è visto, richiama pedissequamente le rilevazioni della Corte di Giustizia in materia.

Sarà quindi interessante, nel prossimo futuro, valutare gli sviluppi giurisprudenziali attesi su entrambi i fronti, che non mancheranno certamente di far riflettere sulla capacità di una Corte di influenzare l'altra; se i giudici di Lussemburgo, infatti, con riferimento ai rinvii pendenti, giungessero a ritenere non rientrante nell'ambito di applicazione del diritto dell'UE il trattamento di dati effettuati direttamente dalle autorità pubbliche, quelle specifiche attività si troverebbero così a sottostare unicamente al rispetto della CEDU e alla interpretazione fornita dalla Corte EDU stessa, lasciando un più ampio margine di discrezionalità agli Stati membri quanto alle misure da adottare nello specifico campo della *Intelligence Surveillance*, pur con tutti i dubbi e le difficoltà, già evidenziate, che una netta delimitazione dei campi e dei sistemi comporta.

In questo contesto deve far riflettere del resto il fatto che proprio nella pronuncia dalla quale è originato il rinvio pregiudiziale *Privacy International*[106] venga richiesto dai giudici inglesi un raffronto tra i criteri in materia di sorveglianza indicati dalle due Corti: viene domandato infatti in particolare se, con riferimento ai sistemi di acquisizione e conservazione di *Communications Data* (metadati) da parte di *Security* e *Intelligence Agencies*[107], debbano applicarsi, in aggiunta ai criteri delineati dalla Corte EDU, anche i requisiti e le salvaguardie stabilite dalla CGUE nella sentenza *Tele2*. Negli ulteriori rinvii pregiudiziali pendenti dinnanzi alla Corte di giustizia inoltre, come sottolineato nel precedente Capitolo, viene data ai giudici europei l'occasione di chiarire e rimodulare gli aspetti maggiormente problematici emersi nella decisione *Tele2* e nella concreta applicazione da parte degli Stati membri dei criteri in essa determinati: anche in tali casi, le attese pronunce della Corte potrebbero porsi maggiormente in linea con le più recenti decisioni della Corte EDU, ad esempio 'smussando' la rigidità dei limiti posti a tutela della fase di mera conservazione ed incrementando invece le salvaguardie nella fase di accesso, adottando quella lettura 'complessiva' e cumulativa delle disposizioni normative, nonché ammettendo che sistemi di *data retention*, per necessità, non possono che avere natura generalizzata, similmente a quanto di recente affermato dalla Corte EDU. Infine anche alcune considerazioni svolte dalla Corte di Strasburgo rispetto ai sistemi Upstream e PRISM, in occasione della pronuncia *Big Brother Watch*, ben potrebbero incidere nella risoluzione dei casi pendenti innanzi alla CGUE aventi ad oggetto l'adeguatezza del sistema di protezione dei dati statunitense, sui quali certamente influiscono i sistemi di sorveglianza massiva sopra richiamati[108].

Al di là delle differenze riscontrate e degli esiti che i futuri ed attesi sviluppi giurisprudenziali porteranno, ciò che innegabilmente emerge dalla analisi svolta della giurisprudenza delle Corte EDU è come essa, similmente a quella di Lussemburgo, sia stata e sia ancora oggi chiamata ampiamente ad interrogarsi su articolate e dettagliate normative aventi ad oggetto sistemi di sorveglianza sofisticati, basati su operazioni pervasive di raccolta, conservazione, accesso, trattamento e analisi di moli ingenti di dati o metadati relativi alle comunicazioni elettroniche. Senza dubbio la complessità tecnica di queste operazioni, la non semplice determinazione della invasività nella sfera privata che esse comportano e soprattutto la difficoltà di tracciare una linea di confine tra ciò che è necessario in una società che possa veramente dirsi democratica e ciò che invece si tramuta in un inaccettabile pericolo e compressione dei diritti e principi sanciti nelle Carte dei diritti europee, rendono il compito di entrambi i giudici di Lussemburgo e Strasburgo estremamente arduo. In questo panorama, come emerso dall'analisi svolta, la giurisprudenza della Corte EDU ha mostrato di essere sensibile e consapevole della complessità delle questioni che i sistemi di sorveglianza pongono, non solo nelle più recenti pronunce analizzate ma anzi

[106] *Privacy International c. Secretary of State and others*, Case no. IPT/15/110/CH, 8 settembre 2017.

[107] Tali sistemi di sorveglianza erano già stati oggetto di una pronuncia dell'Investigatory Powers Tribunal (*Privacy International v. Secretary of State and others*, No. IPT/15/110/CH, 17 ottobre 2016) che li aveva considerati conformi ai criteri delineati dalla giurisprudenza della Corte EDU, facendo però riferimento ai casi giurisprudenziali più risalenti e citando prevalentemente i requisiti fissati nelle pronunce *Weber* e *Liberty*. Di tale pronuncia si parlerà più ampimente nella Parte III del presente lavoro.

[108] Si fa riferimento ai casi C-311/18 *Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems* e T-738/16 *La Quadrature du Net e altri c. Commissione*, già ampiamente richiamati nel Capitolo III.

sin dal 1984, quando il giudice Pettiti, nella sua *Concurring Opinion* alla decisione *Malone c. Regno Unito*[109], affermava: "The danger threatening democratic societies in the years 1980-1990 stems from the temptation facing public authorities to "see into" the life of the citizen".

Solo con il tempo sarà possibile trarre un bilancio corretto circa l'efficacia dell'approccio seguito dalle due Corti e comprendere dunque se la linea utilizzata più recentemente dalla Corte EDU, qualora confermata dalla Grande Camera, possa risultare più 'concreta' e facilmente attuabile dagli Stati[110], senza al contempo compromettere l'elevato standard di protezione della riservatezza e protezione dei dati da sempre garantito nel Continente europeo.

[109] *Malone c. Regno Unito*, ricorso n. 8691/79, deciso il 2 agosto 1984.

[110] È da ricordarsi comunque che, con riferimento alla giurisprudenza di entrambe le Corti europee, non sempre gli Stati hanno mostrato la volontà reale di attuare i principi affermati dai giudici e di dare esecuzione alle sentenze: "For instance, a majority of the European States did not execute or did not fully execute the judgement of the ECJ on the *Digital Rights Ireland* case. The Russian Federation and Hungary still have not adopted general measures to implement the judgement on *Roman Zakharov* and *Szabo*", V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, op. cit., p. 18.

PARTE III

CAPITOLO I

IL REGNO UNITO.
LA PROVA DELLA *DATA RETENTION* TRA SPINTE CONTRAPPOSTE: IL DIFFICILE – E INCOMPIUTO – PERCORSO DEL LEGISLATORE VERSO L'INDIVIDUAZIONE DI UN CORRETTO EQUILIBRIO

1. – Dall'Unione europea agli Stati membri e ritorno: il valore aggiunto di una approfondita analisi della dimensione nazionale

L'analisi e le considerazioni svolte nell'ampia ricostruzione delle scelte normative e degli interventi giurisprudenziali che hanno caratterizzato il contesto dell'Unione europea hanno contribuito ad una chiara comprensione di quanto tutti gli avvenimenti e le decisioni riportate siano state influenzate dall'approccio degli Stati membri e abbiano a loro volta influenzato gli Stati membri nella regolamentazione della *data retention* e dell'accesso ai metadati per scopi securitari. Tale disciplina, infatti, non ha solo risentito delle scelte dei legislatori nazionali, che hanno preso posizione dinnanzi alla complessa sfida del bilanciamento tra tutela dei diritti fondamentali ed utilizzo di mezzi di indagine invasivi della sfera privata degli utenti; è stata anche condizionata dai rinvii pregiudiziali promossi dai giudici nazionali, che hanno portato a sviluppi decisivi e senza precedenti nella dimensione europea. Ne deriva, come si è visto in particolare nei Capitoli II e IV della Parte II, che la stretta interrelazione tra livello nazionale e Unione europea nonché il dialogo instauratosi, mediante l'intervento della CGUE e la partecipazione dei rappresentanti dei Governi nazionali in seno al Consiglio, non possono essere ignorati e meritano anzi di essere approfonditi in tutte le loro sfaccettature.

Partendo da tale consapevolezza, bisogna quindi affermare come nella Parte II l'attenzione alla dimensione nazionale sia stata dedicata principalmente allo studio delle reazioni di quegli Stati membri che, con le proprie decisioni giurisprudenziali, hanno rappresentato il vero motore dell'azione della CGUE e del legislatore dell'UE; l'analisi dell'approccio degli Stati membri pertanto è stata affrontata in maniera funzionale alla comprensione piena delle decisioni dei giudici di Lussemburgo e delle scelte del legislatore europeo. In questa Parte si intende invece operare un esame approfondito dal punto di vista e dalla prospettiva di taluni Stati membri, mediante la ricostruzione dell'evoluzione normativa in materia di *data retention* e accesso, unitamente all'analisi della giurisprudenza nazionale, pur ovviamente non potendo prescindere, anche in questo caso, dall'intrecciarsi degli avvenimenti a livello interno con quelli dell'UE. L'oggetto di studio di questa Parte III costituisce sicuramente un punto prospettico scarsamente esplorato, poiché genericamente si tendono ad investigare meno le ragioni che hanno portato al rinvio pregiudiziale e a prestare invece maggiore attenzione al risultato finale, identificato nella pronuncia della CGUE. Non per questo, tuttavia, una analisi specifica e puntuale del livello nazionale risulta meno interessante e rilevante: essa, al contrario, permette di focalizzarsi sulle interpretazioni, sui dibattiti e sulle posizioni espresse nella dimensione interna nonché in relazione con l'UE e con gli altri Stati. Così facendo, il motto europeo volto a sottolineare l'importanza dell'unità nella diversità, viene calato nella concreta operatività dell'interazione multilivello con riferimento alla peculiare materia della conservazione e accesso ai metadati. Volgere lo sguardo alle singole dimensioni

interne e alle scelte da esse operate sul piano legislativo così come alle pronunce giurisprudenziali vuole pertanto rappresentare un valore aggiunto alla ricerca sin qui svolta, permettendo di comprendere, in ottica comparata, quanto l'esperienza propria di un ordinamento si distingua da un'altra e quanto differenti dunque possano essere le decisioni assunte a livello interno, mettendo in luce le somiglianze che caratterizzano le reazioni dei vari Stati e che possono così evidenziare anche problematiche e criticità condivise, ad esempio, nell'applicazione della normativa europea o nell'attuazione dei principi indicati dalla CGUE.

Ebbene, proprio considerando tali obiettivi ed operando in tale contesto, si deve innanzitutto rilevare come anche dopo – e, si potrebbe dire, nonostante – la sentenza *Tele2* e in assenza di una normativa specifica dell'UE in materia di *data retention*, nel territorio europeo si sia confermato un panorama normativo e giurisprudenziale assai frammentario e variegato, nel quale il dibattito sul corretto bilanciamento tra interessi e diritti differenti è risultato tutt'altro che sopito. Similmente a quanto accaduto a seguito della decisione *DRI* e anche a seguito delle precisazioni e chiarimenti forniti dalla CGUE in merito all'art. 15 Direttiva *e-Privacy*, taluni Stati membri hanno optato per non adottare una nuova disciplina normativa *ad hoc* in materia di *data retention*[1]; altri ancora hanno assistito ad un ulteriore e nuovo intervento da parte delle proprie Corti – di diverso grado – volto a determinare la compatibilità o meno con il diritto dell'UE o con la Costituzione nazionale delle disposizioni regolanti la conservazione e accesso ai metadati: è il caso di Francia, Belgio, Regno Unito, Irlanda ma anche Italia, Portogallo e Repubblica Ceca; ciò che però consente di individuare ulteriori sottocategorie all'interno di questo folto gruppo è l'esito dell'intervento giurisprudenziale.

Per i primi quattro Stati membri citati, come si è già avuto modo di vedere, le perplessità e i dubbi interpretativi – nonché attuativi – relativi ai principi delineati dalla CGUE hanno portato i giudici nazionali a formulare ulteriori rinvii pregiudiziali: riconoscendo la sussistenza di alcune problematiche e criticità relative all'assetto normativo esistente, i giudici hanno ritenuto di non poter risolvere le questioni ad esso sottese se non ottenendo chiarimenti dai giudici di Lussemburgo. Anche tra questi Stati, senza dubbio, è da sottolineare come i rinvii siano stati posti in maniera differente – espressione della diversità di approccio verso la giurisprudenza europea stessa – ma siano comunque tutti giunti al medesimo esito, di riconoscere cioè l'esistenza di diverse interpretazioni possibili della sentenza *Tele2* e la necessità quindi che una univoca e decisa posizione dirimente venisse espressa a livello sovranazionale.

In Italia, Repubblica Ceca e Portogallo, invece, le Corti nazionali hanno ritenuto, a seguito di analisi della normativa interna e dei principi determinati dalla giurisprudenza della CGUE, che la disciplina interna fosse da ritenersi conforme al diritto dell'UE e alla Costituzione nazionale; in Italia, come si avrà modo di vedere, la Corte di Cassazione e alcune Corti di merito hanno più volte, negli ultimi anni, considerato le disposizioni in materia di *data retention* e accesso ai metadati compatibili con la Carta di Nizza e l'interpretazione di essa fornita dalla giurisprudenza europea; similmente, in Repubblica Ceca la *Ústavní soud České republiky* (la Corte costituzionale) ha respinto il ricorso promosso da una ONG (la Iuridicum Remedium) volto ad ottenere la dichiarazione di illegittimità costituzionale della disciplina nazionale in materia di *data retention*[2]: sebbene già nel 2011 la medesima Corte avesse dichiarato l'incostituzionalità della normativa all'epoca vigente e adottata quale trasposizione nell'ordinamento interno della DRD, le stesse considerazioni non sono state ripetute con riferimento alla normativa successivamente adottata nel 2012, ritenuta invece proporzionata allo scopo di indagine e prevenzione

[1] L'Austria, ad esempio, a seguito della dichiarazione di incostituzionalità della normativa di trasposizione della DRD da parte della *Verfassungsgerichtshof* (Corte costituzionale), il 27 giugno 2014 (sul punto si rimanda a M. FLORA, *The unlawfulness of data retention confirmed by the Court of Justice of the European Union and the Austrian Constitutional Court*, in *Journal of European Consumer and Market Law*, 3, 2015) non si è più dotata di alcuna legislazione specifica in materia.

[2] Si fa riferimento al caso P.US 45/17 del 14 maggio 2019.

del crimine, nonostante la natura indiscriminata e generalizzata della conservazione. Ancora, nel 2017, il *Tribunal Constitucional* portoghese ha ritenuto la normativa nazionale n. 32/2008 del 17 giugno 2008, adottata quale trasposizione della DRD, conforme ai diritti fondamentali tutelati dalla Costituzione portoghese[3].

Già da questa breve e parziale ricostruzione dello scenario apertosi a seguito della sentenza *Tele2*, risulta evidente la presenza di una grande varietà di orientamenti, esemplificativi delle difficoltà, delle problematiche e dei dubbi derivanti dalla giurisprudenza della CGUE che è stata oggetto di valutazioni ed interpretazioni differenti e dunque di reazioni, da parte di legislatori o giudici nazionali, anche molto diverse. Tale disomogeneità è inevitabile frutto di una pluralità di approcci alla materia della *data retention* e accesso ai metadati, di scelte legislative e di decisioni delle Corti statali che, anche e nonostante le sentenze dei giudici di Lussemburgo, hanno seguito talvolta orientamenti differenti.

Non potendo in questa sede svolgere una dettagliata analisi di ciascuno Stato membro, si è deciso di concentrare l'attenzione su tre di essi – Regno Unito, Belgio e Italia – ritenuti esemplificativi ciascuno di un approccio significativo e di rilievo: senza mancare di considerare debitamente le peculiarità e le differenze proprie di ciascun ordinamento, che necessariamente impattano anche sulla disciplina in esame, lo studio dell'evoluzione normativa e giurisprudenziale in materia permetterà di comprendere da un lato le riflessioni e il bilanciamento svolto dai diversi attori nazionali e dall'altro di rilevare come giudici e legislatori abbiano reagito dinnanzi alle storiche sentenze della CGUE, oltre a comprendere quale dialogo, se esistente, si è instaurato con tali giudici dell'UE. In ultimo luogo, tale esame consentirà anche di svolgere alcune considerazioni quanto alle motivazioni e alle caratteristiche che distanziano o accumunano i diversi approcci, identificando possibili convergenze, divergenze o esempi e trend virtuosi.

Nella analisi dei prossimi paragrafi e Capitoli quindi l'attenzione verrà concentrata innanzitutto sulle normative dedicate alla regolamentazione della *data retention* e accesso da parte di autorità pubbliche. Esse tuttavia devono essere necessariamente lette nel peculiare e specifico contesto ordinamentale entro cui si inseriscono: innanzitutto i tre Stati membri scelti – il primo rientrante nella famiglia di *common law* mentre gli ulteriori due notoriamente Paesi di *civil law* – non presentano il medesimo riconoscimento dei diritti alla riservatezza e alla protezione dei dati. Come si avrà modo di vedere più approfonditamente in seguito, infatti, la Carta costituzionale belga contiene un riferimento specifico al diritto alla vita privata mentre nulla esprime rispetto al diritto alla protezione dei dati che è stato tuttavia ampiamente riconosciuto quale diritto fondamentale dalla giurisprudenza nazionale, sia di merito che costituzionale. Diversa è invece la Costituzione italiana che non contiene alcuna disposizione né riferita al diritto alla riservatezza né a quello alla protezione dei dati: entrambi tuttavia sono stati affermati dalla giurisprudenza nazionale e una grande attenzione in materia di *data protection* è stata dimostrata dal legislatore italiano che ha approvato numerose normative in materia di protezione dei dati – si pensi al c.d. Codice della Privacy –. Ancora differente è la garanzia prevista nel Regno Unito, che si è dotato di una disciplina sulla protezione dei dati sin dal 1998, con il *Data Protection Act*, e ha affermato il carattere di diritti fondamentali dei diritti alla vita privata e alla protezione dei dati nella sua giurisprudenza ma anche mediante il *Human Rights Act 1998* con il quale i diritti della Convenzione EDU, tra cui dunque anche quello previsto all'art. 8, sono stati incorporati nel diritto nazionale. I tre ordinamenti, già da questa ricognizione di massima, paiono pertanto caratterizzati da una diversa seppur solida regolamentazione e tutela – giurisprudenziale o legislativa – di quei diritti fondamentali che entrano fortemente in gioco nella complessa disciplina della *data retention*. Dinnanzi ad essa,

[3] La sentenza è la n. 420/2017 del 13 luglio 2017. Merita tuttavia precisare come successivamente, nel 2019, il Tribunale portoghese sia stato investito nuovamente di questioni attinenti alla legittimità della normativa nazionale in materia di accesso ai metadati da parte di agenzie di intelligence (decisione n. 464/2019). Sul punto si rimanda a T. VIOLANTE, *Data retention in Portugal*, in M. ZUBIK, J. PODKOWIK, R. RYBSKI (a cura di), *European Constitutional Courts towards data retention laws*, Springer, 2020.

l'approccio espresso dai legislatori nazionali, l'origine di tale disciplina e il suo intrecciarsi con la regolamentazione a livello dell'UE sono stati anche molto differenti: in Belgio, ad esempio, la conservazione dei dati e metadati è stata regolamentata ben prima della Direttiva *e-Privacy* o della DRD – la prima disposizione che ha introdotto un obbligo di conservazione dei dati in Belgio risale al 2000 – mentre nell'ordinamento italiano la *data retention* ha trovato la propria base nella normativa adottata a livello dell'UE: si fa riferimento cioè alla deroga garantita dall'art. 15 Direttiva *e-Privacy*, nonché, successivamente, alla DRD stessa.

Nonostante il diverso percorso che ha portato alla introduzione di normative in materia di conservazione e accesso ai dati per scopi securitari nei tre ordinamenti oggetto di approfondimento, è senza dubbio possibile affermare come le scelte di tali legislatori abbiano fortemente subìto le significative conseguenze prodotte dalla giurisprudenza della CGUE, seppure con reazioni anche molto distanti. Come si è visto in ottica generale nei Capitoli II e IV, taluni legislatori, come quello del Regno Unito, sono intervenuti immediatamente per modificare la disciplina nazionale tenendo in considerazione – sebbene con diverse interpretazioni – le pronunce dei giudici di Lussemburgo –, mentre in altri casi, come per il Belgio e l'Italia, dirimente e fondamentale è stato l'intervento delle Corti nazionali, che pure sono giunte spesso a divergenti considerazioni.

L'analisi delle vicende giurisprudenziali sarà così un ulteriore imprescindibile aspetto di estremo rilievo per la disamina delle realtà statuali scelte: anche con riferimento a questo profilo, però, dovranno essere tenute in debita considerazione le specificità di ogni ordinamento. In via preliminare e pur rimandando a ciascun singolo Capitolo per una valutazione più completa ed approfondita, i tre Stati scelti presentano significative differenze quanto agli strumenti di accesso alla giustizia e, ancora, di attivazione dell'intervento della giustizia costituzionale. Basti notare come nel Regno Unito sia stato predisposto un apposito organo giurisdizionale, il *Investigatory Powers Tribunal*, istituito con il *Regulation of Investigatory Powers Act 2000*, deputato a decidere nei casi di intrusione illegittima nella sfera privata o di illegittimo trattamento dei dati da parte di autorità pubbliche, incluse le agenzie di intelligence (*Security and Intelligence Agancies*), la Polizia e le autorità locali. Non stupisce dunque che molte – anche se non tutte – delle importanti cause che verranno analizzate e che hanno portato a rilevanti rinvii alla CGUE o ricorsi alla Corte EDU trovino origine proprio in controversie decise da questo Tribunale. Diverso è il caso del Belgio, nel quale invece si è più volte pronunciata direttamente la Corte costituzionale: questa così rapida e frequente attivazione dell'intervento dei giudici delle leggi è spiegato dalla peculiarità della giustizia costituzionale dell'ordinamento belga, che prevede la possibilità di un controllo astratto di legittimità mediante ricorso per annullamento. Quest'ultimo può essere promosso dal Consiglio dei ministri, dagli organi esecutivi delle Regioni e delle Comunità, dal Presidente dell'Assemblea legislativa (nazionale, regionale o comunitaria) nonché, a seguito di riforma intervenuta nel 1988, anche da persone fisiche e giuridiche, con un termine temporale per la presentazione del ricorso di sei mesi dalla pubblicazione della normativa da impugnare. Strumenti quale quello previsto dall'ordinamento inglese e belga non si ravvedono infine nell'ordinamento italiano: anche – ma non unicamente – per questo motivo le pronunce rilevanti in materia di *data retention* sono da riscontrarsi unicamente nell'ambito di procedimenti giudiziari di natura penale.

Queste distinzioni di rilievo incidono, come facile comprendere, sul tipo di vaglio effettuato dai giudici e non possono pertanto essere ignorate: quello di organi deputati unicamente a controversie attinenti a strumenti di sorveglianza è un controllo necessariamente differente da quello svolto da una Corte costituzionale che effettua un esame in astratto quanto alla legittimità e conformità alla Costituzione e al diritto dell'UE di normative nazionali; diverso ancora è il vaglio svolto da giudici di merito all'interno di un procedimento penale che non può che riflettersi anche sul piano dell'approccio alla specifica materia della *data retention* e della valutazione circa il bilanciamento degli interessi e diritti in gioco.

Dalle necessarie premesse e differenziazioni sopra brevemente enucleate, utili a mettere in luce alcune differenze ordinamentali che dovranno essere debitamente considerate al fine di operare una corretta e lucida comparazione tra i sistemi e tra le soluzioni normative e gli interventi giurisprudenziali dei tre Stati scelti, si potranno quindi trarre importanti considerazioni sull'approccio di Regno Unito, Belgio e Italia rispetto alla articolata tematica della *data retention* e del regime di accesso ai dati per scopi securitari che tanto ha messo alla prova, come si è visto, il legislatore dell'UE e la CGUE nonché la Corte EDU.

2. – Il legislatore del Regno Unito e la disciplina della data retention*: dal* RIPA *al* Data retention and acquisition regulations *2018, passando per Lussemburgo*

2.1. – Le prime normative in materia di data retention*: dal regime di conservazione dei metadati volontaria alla disciplina dell'accesso contenuta nel* RIPA*, sino a giungere alla trasposizione della* DRD *nel contesto nazionale*

Il primo Stato membro – per quanto tale qualifica sia certamente ad oggi da rivedere – oggetto di approfondita analisi è il Regno Unito, il cui approccio alla materia della *data retention* e le cui vicende normative e giurisprudenziali sono senza dubbio di particolare interesse. L'attenzione che legislatori, giudici e società civile hanno mostrato a questa complessa tematica traspare infatti dai molteplici interventi normativi e dalle svariate pronunce delle Corti nazionali, dalle quali peraltro hanno trovato origine il rinvio pregiudiziale nel caso *Tele2*, nonché il caso, ad oggi pendente, *Privacy International*, aventi ad oggetto due differenti ma fondamentali normative adottate dal Regno Unito: il DRIPA (*Data Retention and Investigatory Powers Act 2014*) e il IPA (*Investigatory Powers Act 2016*).

Volendo seguire una struttura che sarà similmente adottata per l'analisi degli altri due Stati membri scelti, verranno inizialmente esaminate l'evoluzione normativa, le riflessioni e le scelte operate dal legislatore nazionale, ponendo particolare attenzione al bilanciamento effettuato tra esigenze securitarie e tutela dei diritti fondamentali e, soprattutto, dei diritti alla riservatezza e alla protezione dei dati; successivamente saranno oggetto di studio gli interventi giurisprudenziali, che prendono avvio e si connettono inscindibilmente sia con l'assetto normativo esistente e le criticità in esso riscontrate, sia con le vicende caratterizzanti il contesto dell'UE.

Procedendo in ordine cronologico, merita preliminarmente sottolineare come il Regno Unito non fosse dotato, sino al 2007, di una normativa in materia di *data retention* che prevedesse un obbligo di conservazione di metadati in capo ai fornitori di servizi di telecomunicazione. Vigeva dunque la regola generale secondo cui i metadati dovevano essere cancellati quando non più utili per finalità commerciali – ad esempio per scopi di fatturazione – da parte degli operatori economici. Era tuttavia stato introdotto nel 2001, con il *Anti-terrorism, Crime and Security Act* (ATCSA), un sistema di conservazione di tipo volontario: i fornitori potevano cioè scegliere di conservare i metadati oltre quanto loro strettamente necessario, unicamente al fine di rendere tali informazioni disponibili per scopi di "safeguard of national security; or for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security" (art.102, Part 11). Ciò poteva avvenire sulla base di uno specifico accordo da stipularsi tra operatori privati e *Secretary of State*[4], al quale veniva affidato il compito di redigere un apposito '*Code of pratice*' (CoP) cui i *service providers* interessati avrebbero

[4] Il *Secretary of State for the Home Department*, anche noto come *Home Secretary*, svolge sostanzialmente le funzioni del Ministro dell'Interno nell'ordinamento italiano: gestisce e controlla le attività svolte dalle autorità di *law enforcement* e di intelligence (in particolare il *National Security Council* e il *Military Intelligence*) e si occupa di tutte le questioni attinenti all'ordine pubblico.

dovuto attenersi[5]. A dimostrazione però della complessità della materia e di quanto lo strumento della *data retention* non rappresentasse, quantomeno nei primi anni duemila, uno strumento prioritario per il Regno Unito, il primo CoP veniva approvato dal Parlamento solo nel novembre 2003, a distanza dunque di tre anni dall'entrata in vigore della normativa richiamata. Tale documento prevedeva un periodo di conservazione dei metadati derivanti da telefonia fissa, cellulare e telematica, per una durata di dodici mesi per i dati relativi ai servizi telefonici, sei mesi per SMS e dati telematici nonché quattro giorni per le attività svolte sul web (cronologia dei siti visitati, ad esempio), predisponendo inoltre forme di rimborso da parte del Governo dei costi sostenuti da soggetti privati che si impegnavano alla conservazione.

Sotto il profilo del successivo accesso e acquisizione dei metadati, invece, la disciplina era fornita dal RIPA (*Regulation of Investigaroty Powers Act*, 2000). Tale normativa prevedeva specifiche salvaguardie volte a garantire la proporzionalità e necessità dell'ingerenza nella sfera privata costituita dalle operazioni di accesso: innanzitutto venivano espressamente elencati i soggetti ai quali l'accesso era consentito, da individuarsi in "designated persons within relevant public authorities" (tra cui, a titolo esemplificativo, la polizia, la *Serious Organised Crime Agency* e i servizi di intelligence); questi necessitavano comunque e sempre di una previa approvazione da parte di un soggetto avente la qualifica di 'senior officer'; una ulteriore tutela e limitazione era rappresentata dal fatto che le autorità locali non fossero autorizzate ad accedere ai dati di traffico o di ubicazione bensì solo ai dati volti ad individuare l'utente (nome e indirizzo relativi ad una specifica utenza) o i numeri chiamati da un determinato soggetto. Venivano inoltre stabilite le finalità e gli scopi per i quali l'accesso poteva essere consentito: qualora i dati fossero necessari "in the interests of national security; for the purpose of preventing or detecting crime or preventing disorder; in the interests of the economic well-being of the UK; in the interests of public safety; for the purpose of protecting public health; for the purpose of assessing or collecting any tax, duty or levy or other imposition, contribution or charge payable to a government department; for the purpose, in an emergency, of preventing death or injury or any damage to a persons physical or mental health", ma anche per scopi identificativi di vittime di reati o che abbiano perso la memoria o incapaci di identificarsi per malattia, anche mentale. Senza dubbio, la predisposizione di un elenco risultava finalizzata a restringere unicamente a scopi considerati rilevanti le possibilità di accesso ai metadati, limitando dunque l'ingerenza nella sfera privata; nondimeno, dalla lista riportata è possibile notare come essa risulti piuttosto ampia e vasta, nonché caratterizzata da voci e definizioni indefinite e facilmente interpretabili in maniera estensiva: basti pensare a termini quali 'sicurezza nazionale', 'pubblica sicurezza' o 'salute pubblica' che costituiscono finalità particolarmente estese. Un controllo sulle attività di accesso ai metadati e sulla loro correttezza e legittimità, veniva comunque affidato in capo sia al *Interception of Communications Commissioner*, cui veniva attribuito il ruolo di vigilare in maniera indipendente sull'attuazione dei poteri e doveri stabiliti nel RIPA, sia al *Investigatory Powers Tribunal* (IPT): "this Tribunal has full powers to investigate and decide any case within its jurisdiction, which includes the acquisition and disclosure of communications data under the Act. The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of Government"[6].

Dalla ricostruzione svolta si può subito notare come, inizialmente, nessun obbligo di conservazione fosse previsto dalla normativa del Regno Unito, neppure sulla base della facoltà concessa dall'art. 15 Direttiva *e-Privacy*, e come anche la disciplina introdotta e avente carattere unicamente volontario avesse incontrato significative difficoltà ad affermarsi e a divenire applicativa; tale approccio pare

[5] Viene tuttavia specificato come "A failure by any person to comply with a code of practice or agreement under this section which is for the time being in force shall not of itself render him liable to any criminal or civil proceedings", art. 102, par. 4.

[6] È ciò che si legge nel documento redatto dal *Secretary of State for the Home Department* nell'aprile 2009 e titolato *Protecting the Public in a changing communications environment*, p. 16.

sorprendente e singolare, sia se lo si raffronta all'evoluzione normativa e giurisprudenziale, unitamente alle politiche e strategie securitarie del Governo del Regno Unito che hanno invece posto nei decenni successivi una forte attenzione e centralità allo strumento della *data retention* e dell'accesso ai metadati; sia se lo si paragona all'orientamento seguito invece in quei medesimi anni da altri Stati membri, quali il Belgio e l'Italia che, contrariamente a quanto avvenuto Oltremanica, avevano sin dai primi anni duemila adottato ed attuato un regime obbligatorio di conservazione dei metadati.

L'approccio seguito dal Regno Unito avverso lo strumento della *data retention* è mutato in maniera sostanziale a seguito di taluni avvenimenti drammatici quali gli attentati terroristici di Londra del 2005, che avevano dato ulteriore e forte impulso al dibattito europeo e alla necessità di addivenire ad una disciplina quanto più possibile armonizzata, che consentisse da un lato la corretta operatività del mercato interno e dall'altro l'efficacia dello strumento della conservazione dei metadati per finalità di repressione dei reati gravi. A seguito della DRD – la cui adozione è stata peraltro fortemente sostenuta dal Regno Unito, come ricordato nel Capitolo I, Parte II – è divenuto dunque obbligatorio per gli Stati membri predisporre una normativa interna che rispondesse agli obblighi e alle condizioni specificate nella Direttiva europea: Oltremanica quindi è stato così inizialmente approvato, il 1 ottobre 2007, il *Data Retention (EC Directive) Regulations* che disponeva tuttavia la disciplina riguardante unicamente i metadati derivanti da telecomunicazioni telefoniche. Bisogna ricordare infatti che la DRD attribuiva agli Stati membri un termine più lungo, sino al 15 marzo 2009, per trasporre gli obblighi della Direttiva con riferimento ai metadati attinenti alle comunicazioni telematiche: tale normativa è stata adottata dal legislatore inglese nel 2009, con la *Data Retention (EC Directive) Regulations* del 6 aprile 2009, che ha sostituito sia la previa disciplina del 2007, sia il più risalente regime di carattere volontario previsto dal ATCSA del 2001. Come sottolineato da Walker, dunque, "between October 2007 and March 2009 the UK thus had a two-tier regime, with fixed and mobile data governed by the mandatory regime and Internet and email data by the voluntary code under ATCSA"[7].

Solo nel 2009 dunque è stato inserito per la prima volta nell'ordinamento del Regno Unito un obbligo di conservazione riguardante tutte le tipologie di metadati: con grande decisione l'allora *Home Secretary*, Jacqui Smith, aveva riconosciuto come "governed by a strict regulatory framework, communications data is routinely used to investigate terrorist plots, to bring to justice those guilty of serious crimes, to seize illegal drugs and to protect the vulnerable in our society. It is no exaggeration to say that information gathered in this way can mean the difference between life and death"[8]. Tale posizione permette di comprendere quanto, a seguito dell'intervento della DRD e dell'affermarsi di un più marcato contesto emergenziale, anche nel Regno Unito fosse stata posta grande attenzione allo strumento della conservazione generalizzata dei dati[9] e alle sue significative potenzialità, identificato come un mezzo di fondamentale importanza nella lotta al crimine e al terrorismo internazionale. La normativa del 2009 dunque stabiliva l'obbligo in capo a tutti i "public communications providers" di conservare tutti i "communications data" – intesi come tutti i metadati prodotti dalle comunicazioni, ivi compresi i "traffic data", i "location data" e le chiamate senza risposta – per un periodo di dodici mesi, senza alcuna differenziazione quanto alla tipologia di metadati interessati. Stabilendo anche disposizioni in materia di sicurezza da garantire ai metadati, veniva riconfermato il compito di effettuare un controllo indipendente in capo sia al *Interception of Communications Commissioner* con riferimento alle attività

[7] C. WALKER, *Data retention in the UK: pragmatic and proportionate or a step too far?*, in *Computer Law and Security Review*, 25, 2009, p. 326.

[8] SECRETARY OF STATE FOR THE HOME DEPARTMENT, *Protecting the Public in a changing communications environment*, 2009, p. 2.

[9] È significativo il fatto che, nel documento *Access to communications data – respecting privacy and protecting the public from harm*, redatto dal *Home Office*, nel marzo 2008, sia stato riconosciuto come una forma sistematica di conservazione dei dati consenta di "identify suspects, examine their contacts, establish relationships between consirators and place them in a specific location at a certain time. (…) Draw up a detailed profile of the suspects either to inform prevention/disruption operations or for use as corroborative evidence in a prosecution".

poste in essere dalle autorità pubbliche, sia al IPT riguardo invece alle doglianze avanzate dai singoli utenti in caso di ritenuta violazione delle disposizioni contenute nel RIPA. A tale più risalente legislazione, le cui caratteristiche fondamentali sono state sopra analizzate, veniva infatti effettuato rinvio per quanto concerne la regolamentazione della fase di accesso e quindi anche delle finalità espressamente elencate per le quali l'accesso ai metadati era consentito e che rimanevano dunque immutate rispetto al passato.

Le misure adottate con la normativa del 2009, maggiormente organica e riguardante tutte le tipologie di metadati, rappresentavano dunque il risultato della prima vera e propria operazione di bilanciamento tra esigenze investigative e diritto alla riservatezza e alla protezione dei dati effettuata dal legislatore inglese in materia di conservazione obbligatoria: come emerge dai documenti frutto della consultazione pubblica, tenutasi nel 2008 e che aveva visto anche la partecipazione di ONG attive nel campo della difesa dei diritti alla privacy e alla *data protection*, il Governo aveva presentato studi, ricerche e analisi volte a dimostrare da un lato l'utilità e, anzi, la vitale importanza della *data retention*[10] e dall'altro il corretto punto di equilibrio tra sicurezza e diritti fondamentali identificato nella durata della conservazione fissata ad un massimo di un anno. Fondando i propri studi sulle esperienze ed informazioni raccolte nella concreta pratica operativa delle autorità pubbliche, il Governo mirava così a suffragare le proprie scelte e la proporzionalità delle disposizioni normative adottate: sulla base di tali analisi, "communications data is used as important evidence in 95% of serious crime cases and in almost all Security Service operations since 2004"[11] e, sulla base del Report elaborato dal *Interception of Communications Commissioner*, "it is evident that the acquisition of the data was justified and that it is being used as a powerful investigative tool, primarily to prevent crime and disorder; communications data plays a crucial role in the successful outcome of prosecutions and often it is the primary reason why offenders plead guilty"[12].

Accanto a tali considerazioni, ben più delicate e problematiche paiono le motivazioni a sostegno di una conservazione obbligatoria e generalizzata per una durata fissa di dodici mesi: mentre il Governo riteneva che la maggior parte dei casi per i quali i metadati si erano rivelati decisivi fossero "predominantly for long-running serious crime investigations, which without mandatory retention [of more than six months] is more at risk of deletion"[13], erano state presentate, in occasione della consultazione pubblica, anche opinioni e studi di segno avverso, secondo cui "practical experience indicates that most requests are for data of relatively recent origin, typically one to two months old"[14]. Le posizioni emerse dal dibattito nazionale circa l'utilità, proporzionalità e necessità della disciplina della conservazione dei metadati non erano quindi pacificamente concordi e condivise: così, sin da questo momento, la discussione apertasi su tale complessa disciplina e sulle conseguenze rispetto ai diritti fondamentali ha iniziato ad attirare l'attenzione di ONG, società civile e studiosi, avviando una seria riflessione che vedrà, di lì a pochi anni, alcuni primi evidenti risultati concreti nei ricorsi promossi dinnanzi alle Corti nazionali e alla CGUE.

[10] Per una ampia analisi di tale documentazione, tra cui lo studio *Home Office consultation paper: 'Regulation of Investigatory Powers Act 2000: consolidating orders and codes of practice*, del 17 aprile 2009, si rimanda a: C. WALKER, *Data retention in the UK: pragmatic and proportionate or a step too far?*, op. cit.

[11] Secondo i dati riportati dall'allora *Home Secretary* Jacqui Smith, nel discorso tenuto presso l'*Institute for Public Policy Research Commission on National Security*, del 15 ottobre 2008, disponibile al sito http://press.homeoffice.gov.uk/Speeches/speech-to-ippr

[12] *Report of the Interception of Communications Commissioner for 2007*, 22 luglio 2008, p. 15.

[13] Home Office, *Consultation Paper – Transposition of Directive 2006/24/EC*, Agosto 2008, p. 10.

[14] È quanto riportato dall'esperto Peter Milford, nello studio *The retention of communications data: a view from industry*, in *Practical Law IP & IT*, 19 novembre 2008.

2.2. – La rapida reazione del legislatore inglese alla sentenza DRI*: l'adozione del* DRIPA

La delicatezza della materia si è infatti nuovamente posta al centro dell'agenda politica e legislativa del Regno Unito nelle more e a seguito della sentenza *DRI*: i principi e criteri delineati dalla CGUE nella sua storica pronuncia sulla DRD avevano finito col confermare la fondatezza di quelle preoccupazioni e quei dubbi relativi alla proporzionalità dello strumento della *data retention* che già erano stati espressi, come si è visto, sin dal 2009, con l'introduzione del primo obbligo di conservazione generalizzata. In questo contesto si inseriva quindi la scelta del Governo del Regno Unito di non ignorare quanto affermato a livello sovranazionale e di modificare ed adeguare l'assetto normativo esistente, partendo dunque dalla *Data Retention (EC Directive) Regulations*. Pare significativo notare come tale intervento sia stato a dir poco tempestivo, tanto che il Regno Unito è risultato il primo Stato membro a dotarsi di una nuova normativa in materia di *data retention* a seguito dell'intervento della CGUE[15]. Se l'invalidazione della DRD è avvenuta infatti nell'aprile 2014, la nuova normativa in materia di conservazione dei metadati è stata adottata a soli pochi mesi di distanza, il 17 luglio 2014, con una procedura peraltro estremamente rapida, che ha portato all'approvazione del nuovo *Data Retention and Investigatory Powers Act* (DRIPA), a soli tre giorni dalla prima lettura in Parlamento, sotto forma di 'emergency legislation'; tale scelta era stata motivata dal Governo sulla base dell'esigenza di "ensure that the UK law enforcement and intelligence agencies can maintain their ability to access the telecommunications data they need to investigate criminal activity and protect the public. The Government considered it important to pass the legislation quickly to make it unequivocal that the UK will continue to have a data retention regime"[16]. Una decisione, dunque, quella di affrettare i tempi e velocizzare l'iter approvativo di tale normativa, che trovava la propria ragione nella esigenza di colmare con rapidità il vuoto lasciato dalla DRD e contenere le sue potenziali conseguenze, sebbene indirette, sulla disciplina nazionale di trasposizione, evitando dunque eventuali e problematiche controversie legate alla legittimità delle prove derivanti dai metadati conservati sulla base della previa normativa. L'*Home Office*, riconoscendo la necessità di un intervento a modifica della legislazione del 2009[17], nonché prendendo atto delle richieste pervenute dai fornitori di servizi di telecomunicazione, che chiedevano chiarezza quanto ai propri obblighi di conservazione dinnanzi alla invalidazione della normativa europea, aveva infatti affermato come "without this legislation, we face the very prospect of losing access to this data overnight, with the consequence that police investigations would suddenly go dark and criminals would escape justice. (..) We need to act immediately. If we do not, criminals and terrorists will go about their work unimpeded and innocent lives will be lost"[18]. Una scelta, quella del Governo, che ha tuttavia destato critiche e perplessità: "the Law Society argued that the passage of DRIPA as emergency legislation was an affront to parliamentary sovereignty and the rule of law on the grounds that there was insufficient time for parliamentary scrutiny and debate and insufficient consideration of a relevant judgement of the CJEU"[19]. Tali dubbi erano inoltre motivati dal contenuto

[15] Il Belgio, ad esempio, aveva adottato il 29 maggio 2016 una nuova normativa in materia, finalizzata a 'correggere' ed adeguare il regime precedente alla giurisprudenza della CGUE. La Germania invece era intervenuta il 1 luglio 2017.

[16] A. MUNIR, S. YASIN, S. BAKAR, *Data retention rules: a dead end*, in *European Data Protection Law Review*, 3, 2017, p. 76.

[17] "The judgment of the ECJ raised a number of issues concerning the Data Retention Directive. Many of these were already met by the safeguards within the United Kingdom's comprehensive data retention and access regime. Nevertheless, where appropriate, the Act adds safeguards while providing for the replacement regulations to add further safeguards in line with the judgment", par. 12, DRIPA Explanatory Notes.

[18] Queste le dichiarazioni contenute nel UK Parliament, *House of Commons Briefing Papers*, SN06934, 2014.

[19] Come riportato da A. MUNIR, S. YASIN, S. BAKAR, *Data retention rules: a dead end*, op. cit., p. 76, facendo riferimento al documento redatto da *Law Society* dal titolo *Regulation of Investigatory Powers Act consultation: acquisition and disclosure of communications data and retention of communications data codes of practice: Law Society response*, 2015. Come ben riassunto da Zedner, "introduced as emergency legislation with cross-party

del DRIPA che riprendeva sostanzialmente, nelle sue caratteristiche fondamentali, la disciplina inserita nella previgente normativa del 2009[20], riproponendo l'obbligo di conservazione[21], sebbene con una sostanziale differenza rispetto al passato: anziché disporre un obbligo generale, veniva attribuito al *Secretary of State* il potere di imporre ai fornitori di servizi di telecomunicazione, mediante '*retention notice*', la conservazione di determinate tipologie di metadati (anche la totalità dei metadati), qualora tale richiesta fosse ritenuta necessaria e proporzionata al raggiungimento di uno degli scopi, sopra elencati, specificati nel RIPA del 2000, che rimaneva la normativa di riferimento quanto alla disciplina sull'accesso ai metadati. Rispetto alla precedente legislazione del 2009, inoltre, il periodo di *data retention* non era fissato a dodici mesi bensì poteva durare 'al massimo' dodici mesi, prevedendo quindi la possibilità di stabilire un obbligo di conservazione di durata inferiore laddove appropriato all'ottenimento dello scopo. Nelle disposizioni finali era stata inserita anche una c.d. *sunset clause*, una clausola di 'scadenza'[22], nella quale si stabiliva che la validità della normativa dovesse venire meno il 31 dicembre 2016.

Le caratteristiche fondamentali del relativamente breve testo del DRIPA permettono di svolgere alcune considerazioni sulla iniziale reazione del Regno Unito al primo decisivo intervento della CGUE in materia di conservazione dei metadati: non veniva infatti messa in discussione la legittimità della *data retention* di tipo generalizzato ed indiscriminato, bensì, accanto a tale obbligo, venivano inserite talune nuove limitazioni e restrizioni, quali l'intervento del *Secretary of State* o la possibilità di modulare la durata della conservazione, accompagnate da ulteriori e più specifiche salvaguardie attinenti alla

---

support on July 10, 2014, the DRIPA was enacted just three days later. This exceptionally short timetable did not allow for the public consultation and debate that ordinarily precedes the legislative process. The usual rounds of prelegislative scrutiny were ruled out and the time available for parliamentary debate was so severely curtailed as to make review, amendment or opposition impossible. The government claimed that resort to emergency powers was necessary to clarify the legislative framework, to replace the 2009 Regulations and to provide additional safeguards stipulated in the April judgement. (..) Certainly no sufficiently grave emergency had arisen in July 2014 to justify overriding the ordinary legislative process. The claim made was that communications companies had declared themselves unwilling to share data for security and investigatory purposes unless UK law is clarified immediately. The threat that companies would otherwise start deleting data, concern about the emergence of the so called 'dark net' and fear of 'safe spaces' in which terrorists communicate unmonitored, served to silence opposition and garner unusual all-party support", L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the United Kingdom after the European Data Retention Directive*, in R. A. MILLER (a cura di), *Privacy and Power. A transatlantic dialogue in the shadow of the NSA-Affair*, Cambridge University Press, 2017, p. 565. Rispetto alla scelta di introdurre modifiche così significative mediante una normativa di emergenza, sottratta ad un più ampio ed appropriato dibattito parlamentare, si sono espressi in maniera fortemente critica anche Boehm e Cole: "Although the three main parties support the emergency legislation, there is criticism with regard to the timing of the action. The bill was introduced just shortly before the summer recess and Members of Parliament did not have time to scrutinise the law in detail and propose possible changes. Due to the untypical emergency procedure, there was not much time for other critical voices to be heard", F. BOEHM, M. COLE, *Data retention after the judgement of the CJEU*, 2014.

[20] 18 Professori appartenenti a diverse Università del Regno Unito, con una 'Open Letter' datata 14 luglio 2014, avevano messo in guardia il Parlamento quanto ai rischi derivanti dalla disciplina prevista nel DRIPA e all'impatto di essa rispetto alla tutela dei diritti fondamentali: "DRIP is far more than an administrative necessity; it is a serious expansion of the British surveillance state. We urge the British Government not to fast track this legislation and instead apply full and proper parliamentary scrutiny to ensure Parliamentarians are not mislead as to what powers this Bill truly contains", sottolineando peraltro come, nonostante le affermazioni del Governo, tale normativa non potesse essere ritenuta conforme ai criteri indicati dalla CGUE nella sentenza *DRI*. La lettera è reperibile all'indirizzo: https://paulbernal.wordpress.com/2014/07/15/open-letter-from-uk-legal-academic-experts-re-drip/

[21] È il DRIPA stesso a contenere la spiegazione di tale scelta: "Mandated data retention is crucial for law enforcement to investigate, detect and prevent crimes. Ensuring certain types of communications data are retained provides the confidence that the data required will be available when needed by public bodies that have been approved by Parliament to acquire it", par. 10, DRIPA Explanatory Notes.

[22] Per una ampia analisi dello strumento delle '*sunset clauses*' e delle '*temporary legislation*', si rimanda al lavoro monografico dedicato a tale tematica, scritto da S. RANCHORDAS, *Constitutional sunsets and experimental legislation*, Elgar, 2014.

sicurezza dei dati conservati e alle misure e garanzie che i fornitori stessi erano chiamati ad adottare (previste in maniera più completa all'interno del *Data Retention Regulations 2014*, adottato sulla base del DRIPA). Certamente, come ritenuto da alcuni studiosi, "the concept of "retention notices" constitutes an approach worth considering", poiché può rappresentare una alternativa interessante ad un obbligo generalizzato di conservazione; nonostante questo, tuttavia, l'ampiezza delle finalità per le quali l'ordine del *Secretary of State* poteva essere emanato e dunque la grande discrezionalità lasciata a tale soggetto quanto ai dati e ai servizi cui imporre la *data retention*, rendevano il risultato finale non molto dissimile a quello della previa normativa del 2009: "To date, the UK legislature has not gone far enough in limiting the retention of data to very specific objects of public safety and security, as required by the more convincing narrow understanding of the ECJ decision"[23]. Con riferimento alla disciplina dell'accesso, poi, non erano stati introdotti mutamenti sostanziali al RIPA, che non veniva dunque adeguato ai criteri indicati dai giudici di Lussemburgo, quali il controllo da parte di un giudice o di una autorità amministrativa indipendente o ancora la determinazione di specifici reati gravi limitatamente ai quali era concesso l'accesso ai metadati.

Tali lacune e il mancato corretto inserimento di questi importanti requisiti nella nuova disciplina normativa non erano sfuggiti a critiche e preoccupazioni da parte della società civile e di ONG operanti nell'ambito della tutela dei diritti fondamentali: secondo Tony Bunyan, all'epoca direttore della ONG Statewatch, "the UK is consciously acting in defiance of the CJEU ruling on mandatory data retention by requiring all CSPs/ISPs inside and outside the UK to permanently store information on all communications they handle – mass surveillance. Under DRIPA 2014, the UK is clearly ignoring the Court's ruling by maintaining the mass surveillance of communications and extending its reach, though permanent warrants, to service providers based in the EU, USA and elsewhere"[24].

Sono queste considerazioni e simili dubbi ad aver spinto Watson, Brice e Lewis a presentare nel 2015 ricorso dinnanzi alla High Court of Justice, Divisional Court, al fine di accertare la legittimità del regime di conservazione dei metadati disciplinato dal DRIPA ed in particolare la sua compatibilità con gli artt. 7 e 8 della Carta di Nizza e con l'art. 8 della CEDU: sebbene una approfondita analisi di tali decisioni e della più rilevante giurisprudenza in materia occuperà più ampiamente il prossimo paragrafo, è importante sin da ora ricordare come sia proprio da tale prima rilevante azione e a seguito del relativo appello dinnanzi alla Court of Appeal, che ha avuto avvio il noto e fondamentale rinvio pregiudiziale alla CGUE, fonte della sentenza *Tele2*. Ed è proprio alla luce del fitto intreccio che da quel momento si viene ad instaurare tra vicende giurisprudenziali, a livello nazionale ed europeo, e scelte del legislatore, che devono essere analizzati gli sviluppi normativi successivi: mentre era ancora attesa la sentenza dei giudici di Lussemburgo nel richiamato caso *Tele2*, che avrebbe chiarito l'impatto e l'estensione della decisione *DRI* rispetto alle normative nazionali in materia di conservazione e accesso ai metadati,

---

[23] S. HEITZER, J. KULHING, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in *European Law Review*, 2, 2015, p. 269.

[24] T. BUNYAN, *Analysis mass surveillance of communications in the EU: CJEU Judgement and DRIPA 2014/RIPA 2000 in the UK*, Statewatch, 2014, disponibile all'indirizzo: https://www.statewatch.org/media/documents/analyses/no-252-mand-ret-dripa-ripa.pdf . Come sottolineato da Vainio, "The new law was basically an attempt to maintain data retention, just under a different name. The system enacted by the new law is similar to the one that was implemented under the Directive, except that it does not use the same language as in the Directive. (..) According to critics, DRIPA actually went further than merely maintaining the data retention regime and fails to meet the requirements of the CJEU judgment. The civil rights organisation Liberty used strong language in its critique of the bill—according to Liberty, the bill "doesn't even pretend to comply with the CJEU judgment." Instead, it sought to re-enact a mandatory communications data retention regime for the entire population for up to 12 months, without even limiting collection to cases involving the prevention or detection of serious crime. The Act allows access to the data for a broad group of public authorities and many can do so without the need to obtain prior judicial authorization", N. VAINIO, *Fundamental rights compliance and the politics of interpretation: explaining Member State and Court reactions to Digital Rights Ireland*, in T. BRAUTIGAM, S. MIETTINEN (a cura di), *Data protection, privacy and European regulation in the digital age*, Unigrafia, 2016, p. 238.

nonché l'incidenza rispetto alla facoltà prevista dall'art. 15 Direttiva *e-Privacy*, il legislatore inglese si trovava dinnanzi all'imminente scadenza della validità del DRIPA, la cui vigenza era per legge stata limitata, come si è detto, sino al 31 dicembre 2016. Anche per tale motivo e senza potersi dunque basare sulle considerazioni finali della CGUE, bensì solo su quelle espresse dall'Avvocato generale nelle sue Conclusioni, il legislatore decideva di approvare non una proroga della validità del DRIPA, in attesa di poter meglio adattare una nuova normativa alla giurisprudenza europea, bensì un nuova legge deputata a regolare tale delicata materia: l'*Investigatory Powers Act* (c.d. IPA), che riceveva il *Royal Assent* il 29 novembre 2016, entrando in vigore il 30 dicembre 2016.

2.3. – La discussa scelta di approvare il IPA *nelle more del giudizio* Tele2

Ebbene, in tale normativa erano stati sostanzialmente mantenuti i tratti fondamentali che già caratterizzavano il DRIPA e la previa normativa del 2009, pur predisponendo un testo maggiormente comprensivo, completo e dettagliato, composto da 272 articoli. La Section 87, riguardante la *data retention*, attribuiva in capo al *Secretary of State* il potere di richiedere ai fornitori di servizi di telecomunicazione la conservazione di metadati per un periodo massimo individuato nella durata di dodici mesi, mentre la Section 136 assegnava al medesimo *Secretary* la facoltà di emanare "bulk acquisition warrants" che consentissero un accesso alla generalità dei metadati conservati dagli operatori a favore delle agenzie di intelligence. Entrambe le decisioni emanate dal *Secretary of State* dovevano tuttavia essere approvate da un *Judicial Commissioner*[25], cui era assegnato il compito di effettuare un controllo sulla proporzionalità e necessità delle misure richieste, nonché sul rispetto dei diritti fondamentali alla riservatezza e alla protezione dei dati. Ne emerge, dunque, come, accanto ad alcune rilevanti novità e maggiori salvaguardie, quali il "double lock system" rappresentato dal controllo effettuato dal *Judicial Commissioner* sui '*retention notice*' del *Secretary of State*[26], fosse riconfermato il regime di conservazione generalizzata e nessuna forma di targettizzazione, dunque di conservazione di tipo mirato sulla base di criteri geografici o soggettivi, come suggerita dalla giurisprudenza europea, fosse stata, neppure con questo intervento normativo, introdotta.

Similmente, sul fronte dell'accesso ai metadati, non si registra l'approvazione di disposizioni pienamente conformi ai criteri indicati dalla giurisprudenza europea. La Section 61, infatti, consentiva ad un elenco predefinito ma ampio di autorità pubbliche di accedere ai metadati, senza prevedere un previo controllo da parte di un giudice o di una autorità indipendente. Era però introdotta, alla Section 67, la possibilità, per i *senior officers*, di stabilire dei c.d. *filtering arrangements* relativi all'accesso ai metadati: "such arrangements could be seen as forms of internal authorisation, but they aim to establish safeguards against abuse and minimise the volume of metadata accessed. Such arrangements are, in effect, parameters for search engines or decision by certain authorized officials to access and examine

[25] Agli artt. 227 e 228 vengono indicate le modalità di nomina e le caratteristiche che tale soggetto deve possedere. In termini generali, i *Judicial Commissioners*, nominati dal Primo Ministro, possono essere definiti come "a serving or retired member of the senior judiciary in the UK. JCs provide independent authorisation of applications for the use of certain investigatory powers. The Investigatory Powers Act sets out that a JC must hold or have held a high judicial office", secondo la definizione fornita nel sito dell'*Investigatory Powers Commissioner's Office*, all'indirizzo https://www.ipco.org.uk/default.aspx?mid=21.19

[26] Questo sistema è stato definito da Theresa May – *Home Secretary* al momento della presentazione del *Draft Investigatory Powers Bill* e Primo Ministro all'epoca della entrata in vigore di tale normativa – come "one of the strongest authorisation regimes anywhere in the world" (Discorso di Theresa May del 4 novembre 2015, reperibile sul sito www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill). Senza dubbio il secondo controllo operato già nella fase della conservazione risulta una garanzia aggiuntiva; dubbi però persistono quanto alla indipendenza e alla efficacia dell'intervento del *Judicial Commissioner*, unitamente al fatto che anche tale tutela non sopperisce al carattere generalizzato che la conservazione può assumere.

generalized metadata obtained from communication operators"[27]. Questi *arrangements* potevano specificare i soggetti autorizzati a svolgere l'accesso e il trattamento dei metadati, nonché disciplinare le condizioni di conservazione o cancellazione dei risultati delle operazioni di accesso e filtraggio dei metadati quando non più necessari per finalità di indagine. Prima dell'accesso, inoltre, generalmente i *senior officers* erano chiamati a confrontarsi con i c.d. *Single Points of Contacts*, cioè funzionari formati al fine di controllare la legittimità, necessità e proporzionalità delle operazioni di accesso. Sebbene tale ulteriore vaglio caratterizzante la delicata ed invasiva fase dell'accesso abbia rappresentato certamente un intervento positivo nella direzione di un maggiore controllo, è da sottolineare nondimeno come i soggetti deputati a tale compito non potessero essere considerati autorità indipendenti, secondo quanto stabilito dalla CGUE, in quanto funzionari appartenenti ad autorità pubbliche e sottoposti gerarchicamente ai *senior officers* con cui collaboravano. Nessuna restrizione era stata inserita poi quanto alle finalità dell'accesso e, in particolare, alla gravità dei reati da perseguire e per i quali l'accesso era richiesto: le finalità restavano infatti ampie, andando da "purpose of preventing or detecting crime or of preventing disorder", "purposes of protecting public health" ad "assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a Government Department" (art. 61). Sebbene, come noto, la CGUE non abbia fornito un elenco e una lista di reati considerati gravi, nondimeno essa ha sempre fatto riferimento a crimini quali il terrorismo e forme di criminalità organizzata, così che pare potersi affermare che le finalità per le quali l'accesso era consentito, individuate in maniera così ampia e generica all'interno del IPA che parla peraltro solo di 'prevenzione e lotta alla criminalità', non riflettessero pienamente e totalmente quel carattere di 'gravità' cui la giurisprudenza europea faceva e tutt'ora fa riferimento.

Infine, sotto il profilo delle salvaguardie previste quanto alla sicurezza dei metadati conservati o alla possibilità di ottenere rimedi in caso di violazione dei diritti fondamentali avvenuti proprio mediante operazioni di conservazione e accesso, il IPA, oltre a ribadire il ruolo e il compito attribuito all'apposito *Tribunal*, già istituito nel RIPA del 2000[28], aveva anche assegnato al *Investigatory Powers Commissioner* il potere di informare gli utenti non ogniqualvolta i metadati fossero oggetto di accesso ma unicamente qualora fosse intercorso un "serious error" nelle operazioni di conservazione, accesso e trattamento dei dati e solo nel caso in cui "it is in the public interest for the person to be informed of the error" (art. 231). Sul fronte poi della sicurezza dei metadati conservati, nulla veniva specificato quanto all'obbligo di *data retention* limitatamente al territorio dell'UE.

Il quadro che risulta da questa analisi delle principali caratteristiche del IPA aiuta a comprendere come molte perplessità e dubbi fossero sorti, sin dalla sua adozione, quanto alla reale conformità di tale nuova normativa rispetto ai criteri individuati dalla giurisprudenza della CGUE: con riferimento, ad esempio, al ruolo del *Judicial Commissioner* si nota come l'indipendenza e il rigore dei controlli da esso effettuati dipendessero in gran parte "on the personality of the Commissioner, as well as on the information to which they have access. Furthermore, while a Judicial Commissioner should have regard to privacy rights, they must not act in a way 'contrary to the public interest or prejudicial to national

[27] W. R. MBIOH, *Post-Och Telestyrelsen and Watson and the Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017, p. 279.

[28] Sul punto, l'IPA introduce comunque una rilevante novità, prevedendo per la prima volta la possibilità di promuovere appello alla Court of Appeal o alla Court of Session avverso le decisioni dell'IPT, che non risultavano invece precedentemente impugnabili dinnanzi a nessun giudice. Tale importante possibilità, tuttavia, è stata sottoposta a restrittive condizioni: "An appeal under this section— (a) is to be heard by the relevant appellate court, but (b) may not be made without the leave of the Tribunal or, if that is refused, of the relevant appellate court. (7) The Tribunal or relevant appellate court must not grant leave to appeal unless it considers that— (a) the appeal would raise an important point of principle or practice, or (b) there is another compelling reason for granting leave", art. 242. Tali requisiti sono stati oggetto di critiche, anche in fase di consultazione, in quanto ritenuti eccessivamente restrittivi e passibili di divenire un vero e proprio ostacolo alla efficacia di tale rimedio.

security, the prevention or detection of serious crime or the economic well-being of the UK'. These limitations (..) may limit the Judicial Commissioners' effectiveness"[29].

Anche il meccanismo di controllo del corretto esercizio dei poteri di accesso da parte delle pubbliche autorità aveva posto del resto serie perplessità sotto il profilo della sua reale efficacia: alcuni autori avevano sul punto evidenziato come nel ruolo assegnato ai *Single Point of Contact* non potesse individuarsi un vero e proprio "external check"[30], come richiesto dai giudici di Lussemburgo.

Una ulteriore critica veniva poi mossa con riferimento alla importante facoltà assegnata al *Investigatory Powers Commissioner* di informare gli utenti in caso di errori nel trattamento dei metadati prodotti dalle proprie utenze: "this obligation is very limited, applying only where there is a serious error which has caused significant prejudice or harm to the person concerned and it is in the public interest for the person to be informed"[31]; in questo senso, il solo fatto che fosse possibile adire l'*Investigatory Powers Tribunal* senza che venisse richiesta la prova da parte del ricorrente di essere stato assoggettato a forme di sorveglianza non sembrava sufficiente per sopperire alla assenza di informazioni dirette ai singoli utenti, che sarebbero maggiormente spronati a rivolgersi ai giudici qualora venissero a conoscenza e fossero dunque consapevoli che i propri dati sono stati oggetto di accesso e trattamento. Pur non costituendo quindi un ostacolo in termini assoluti all'accesso a rimedi giurisdizionali, la mancata notifica – o per lo meno le restrittive condizioni di attuazione della stessa – rappresentavano una forte limitazione all'utilità del potere assegnato al *Investigatory Powers Commissioner*.

La riproposizione poi di un sistema di *bulk data retention*, secondo il quale cioè le richieste di conservazione espresse dal *Secretary of State* potevano avere carattere generalizzato, resta senza dubbio uno dei punti maggiormente problematici: "to make the IPA acceptable, the retention notices would need to relate to specific investigations, rather than be general in scope"[32]: una forma di targettizzazione che non era tuttavia prevista come necessaria dalla normativa e che non rappresentava una limitazione ai poteri e alle scelte del *Secretary of State*. Nonostante quindi da un lato si siano registrati dei miglioramenti, "sicuro portato delle maggiori garanzie richieste in questi processi di sorveglianza massiva, dall'altro [tale normativa] presenta alcune disposizioni che non soddisfano i criteri posti dalla Corte di giustizia"[33].

2.4. – Le ulteriori necessarie modifiche alla luce della sentenza Tele2*: il* Data Retention and acquisition regulations 2018 *e uno sguardo più attento del legislatore inglese alla tutela dei diritti fondamentali*

Alla luce delle riflessioni e delle criticità rilevate, diviene più semplice comprendere come, anche a seguito dell'adozione del IPA, il dibattito circa la disciplina della *data retention* non abbia trovato una conclusione definitiva. Le problematiche che, come si è visto, hanno caratterizzato tale normativa sin

[29] L. WOODS, *The Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017, p. 104. Viene inoltre rilevato come il vaglio effettuato dal *Judicial Commissioner* fosse fondato solo sulle considerazioni conclusive presentate dal *Secretary of State*, così che la limitata documentazione e dati messi a disposizione nella fase di controllo finivano con l'incidere sulla profondità delle valutazioni effettuate dal *Judicial Commissioner* stesso e dunque sul suo concreto potere.

[30] L. WOODS, *The Investigatory Powers Act 2016*, op. cit., p. 104.

[31] L. WOODS, *The Investigatory Powers Act 2016*, op. cit., p. 104.

[32] L. WOODS, *The Investigatory Powers Act 2016*, op. cit., p. 105. Similmente White ha affermato come l'unico modo per rendere legittimo il sistema di conservazione previsto dal IPA sia quello di far sì che "retention notices or obligations must be used for a specific purpose, not as a general fishing exercise to bring in information, based on verifiable reasonable suspicion that is necessary and proportionate", M. WHITE, *Protection by judicial oversight or an oversight in protection?*, op. cit., in *Journal of Information Rights, Policy and Practice*, 2, 2017.

[33] L. SCAFFARDI, *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016: una legge per il futuro troppo legata al passato***,** in *Quaderni Costituzionali*, 2, 2017, p. 414.

dalla sua origine, sono state inoltre successivamente accentuate dagli importanti ed ineludibili sviluppi giurisprudenziali in materia, registratisi a livello tanto europeo quanto nazionale: il 21 dicembre 2016 la CGUE ha pubblicato la nota sentenza *Tele2*, che ha inevitabilmente avuto un forte impatto sulla discussione interna relativa alla legittimità e compatibilità del regime nazionale con il diritto dell'UE e l'interpretazione di esso fornita dai giudici di Lussemburgo. In tale contesto, si sono così registrati, da un lato, numerosi i ricorsi dinnanzi alle autorità giudiziarie del Regno Unito, aventi proprio ad oggetto le disposizioni del IPA, uno dei quali è peraltro sfociato in un ulteriore rinvio pregiudiziale che ha aperto nuovamente il dialogo con la Corte di Giustizia dell'UE, e dall'altro lato una forte attenzione da parte del legislatore, che ha avviato un percorso di riforma dell'assetto normativo esistente. Ne è riprova la consultazione pubblica avviata dal Governo il 30 novembre 2017, a meno di un anno dall'entrata in vigore del IPA e dalla sentenza *Tele2*: in tale consultazione emerge con chiarezza come "the Government considers that some aspects of our current regime for the retention of and access to communications data do not satisfy the requirements of the CJEU's judgement"[34], cogliendo quindi la necessità di svolgere una dettagliata analisi dell'impatto della decisione *Tele2* rispetto alla disciplina all'epoca vigente, aprendo ad una valutazione approfondita della concreta fattibilità e applicabilità dei criteri indicati dai giudici di Lussemburgo.

Il processo di modifica e di riflessione promosso dal Governo ha subìto poi una significativa accelerazione mediante l'intervento della High Court: quest'ultima, come si avrà modo di vedere, era stata infatti chiamata a pronunciarsi con riferimento alla legittimità del IPA, anche e soprattutto alla luce della giurisprudenza europea, concludendo con una decisione – datata 27 aprile 2018 – di grande rilievo con la quale era stata dichiarata l'incompatibilità di alcune sezioni del IPA (Part 3, 4) nonché di alcune disposizioni del RIPA (che regola l'accesso ai metadati al Chapter 2 della Part 1), considerate non conformi ai diritti fondamentali riconosciuti e tutelati dal diritto dell'UE. Unitamente a ciò, veniva quindi richiesto al legislatore di emendare entro il 1 novembre 2018 la disciplina vigente.

L'ultima modifica apportata al IPA, promossa, come si è detto, in primis dal Governo, che aveva riconosciuto alcune delle criticità della normativa adottata alla fine del 2016, e poi accelerata a seguito dell'intervento della High Court, è stata così approvata il 31 ottobre 2018, mediante il *Data Retention and acquisition regulations 2018*, che ha apportato notevoli modifiche al testo normativo originario.

Innanzitutto merita rilevare come le disposizioni sull'accesso e acquisizione dei dati contenute nel RIPA del 2000, cui il IPA faceva riferimento, siano state interamente sostituite. Sotto tale profilo, i principali aspetti sui quali il legislatore è intervenuto sono da individuarsi nella predisposizione di una soglia di gravità dei reati per i quali l'accesso è previsto, nonché nella determinazione di una previa autorizzazione all'accesso ai metadati, predisposta da una autorità che possa realmente dirsi indipendente. È evidente notare come tali aree di modifica siano riconducibili a quanto enunciato dalla High Court nella sua pronuncia avente ad oggetto il IPA, nonché nei requisiti già ampiamente ribaditi dai giudici di Lussemburgo ma che il legislatore inglese aveva mancato di considerare nei suoi più recenti interventi normativi. Quanto al profilo dell'autorizzazione e dunque di un controllo preventivo sulla necessità e proporzionalità dell'accesso, tale potere viene attribuito in capo al *Investigatory Powers Commissioner*, che può delegare la funzione ad un apposito ufficio, denominato *Office for Communications Data Authorisations* (OCDA): come si legge nell'*Explanatory Memorandum*, il "OCDA will report directly to the IPC, and will be responsible for considering the vast majority of requests to access communications data made by public authorities"[35]. Viene inoltre prevista, in casi di particolare urgenza, una procedura più snella e rapida, che prevede un sistema di "internal authorisation

[34] Così si legge nel documento redatto dal Home Office nel novembre 2017, titolato *Consultation on the Government's proposed response to the ruling of the Court of Justice of the EU on 21 December 2016 regarding the retention of communications data*.

[35] Documento redatto dal Home Office nel 2018, titolato *Explanatory memorandum to "The data retention and acquisition Regulations 2018"*, p. 4.

by designated senior officer in a public authority", ad esclusione delle *local authorities*, alle quali tale prerogativa non viene concessa. Viene inoltre effettuata una significativa modifica attinente alle finalità per le quali l'accesso viene autorizzato: mentre prima era effettuato un generico riferimento al "purpose of preventing or detecting crime or of preventing disorder", ora viene invece specificato che l'analisi di metadati può avvenire per scopi di lotta alla criminalità di carattere grave ("the purpose of preventing or detecting serious crime", art. 60A, subsection 8), che si identifica laddove "the threshold will be met for investigations into all offences for which an adult is capable of being sentenced to twelve months or more in prison, any offence involving violence, any offence which involves a large number of people acting in pursuit of a common purpose, any offence committed by a body corporate, any offence which involves the sending of a communication or a breach of privacy, or any offence involving a significant financial gain"[36]. Sempre allo scopo di limitare e rendere sempre più proporzionata l'ingerenza nella sfera privata, vengono eliminate alcune delle generiche e vaste finalità autorizzative dell'accesso, che erano precedentemente previste nel RIPA e che erano state oggetto di critica proprio per la loro ampiezza ed indeterminatezza: "public health; collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; exercising functions relating to the regulation of financial services and markets, or financial stability"; tale scelta è stata motivata dalla considerazione secondo cui questi scopi "allow for communications data to be retained or acquired in relation to criminal activity that would not meet the serious crime threshold required by the CJEU"[37].

Una rilevante modifica poi ha interessato anche la disciplina della conservazione dei dati: sono stati infatti meglio specificati e precisati i criteri che il *Secretary of State* è chiamato a valutare nel momento in cui deve considerare l'opportunità e il contenuto di una '*retention notice*', cioè un ordine di conservazione. Vengono così inseriti ulteriori fattori, quali una maggiore specificazione dei servizi e degli operatori cui la conservazione deve riferirsi, la valutazione circa la possibilità di restringere l'ordine di conservazione a determinate aree geografiche o di escludere gruppi di utenti. Viene infine attribuito al *Secretary of State* l'onere di considerare e soppesare i benefici che una conservazione generalizzata può concretamente comportare rispetto alla finalità di lotta alla criminalità grave, valutando la possibilità di adottare misure meno onerose ma egualmente efficaci.

Sulla base delle specificazioni e condizioni introdotte dalla nuova normativa, il Governo ha affermato con decisione che "considering the necessity and proportionality considerations that must be taken into account, and the resulting practical effect of the regime to limit data retention by telecommunications operators or postal operators, services and data types, we do not consider that the existing data retention regime is general and indiscriminate"[38]. Sebbene tale posizione sia da considerarsi fortemente discutibile ed eccessivamente 'ottimistica', è comunque da rilevare lo sforzo del legislatore di proporre innovazioni in senso restrittivo quanto alla disciplina della *data retention*, capaci di delimitare con maggior chiarezza e trasparenza la discrezionalità che pur viene mantenuta in capo al *Secretary of State*, prendendo in considerazione, pur senza attuarli *in toto*, i criteri che la CGUE aveva individuato per definire la legittima forma di conservazione di tipo targettizzato.

Al momento non sono presenti studi che consentano di valutare efficacemente se e come queste novità abbiamo realmente portato all'esito prefissato, cioè di restringere i casi di '*retention notice*' generalizzata ed ampia, riguardanti cioè la totalità degli operatori di servizi di telecomunicazione, la totalità degli utenti e la totalità dei metadati prodotti. Certamente, quello che in questo ultimo intervento normativo si registra, diversamente da quanto avvenuto in passato, è il tentativo e la volontà del legislatore di muoversi con maggior consapevolezza e convinzione nella direzione di colmare le lacune che rendevano la disciplina vigente non conforme al diritto dell'UE, ponendo particolare attenzione a

[36] *Explanatory memorandum*, cit., p. 4.
[37] *Explanatory memorandum*, cit., p. 5.
[38] Home Office, *Consultation on the Government's proposed response to the ruling of the Court of Justice of the EU on 21 December 2016 regarding the retention of communications data*, p. 14.

quelle salvaguardie relative all'accesso ai metadati che, pur essendo state ribadite con decisione tanto dai giudici di Lussemburgo quanto da quelli nazionali, non erano state integrate, inizialmente, neppure nel IPA.

3. – Le Corti inglesi e i principi delineati dalla giurisprudenza europea: tra divergenze ed avvicinamenti

3.1. – La sentenza della **High Court** *nel caso 'Watson' e una interpretazione 'restrittiva' della sentenza* **DRI**

La giurisprudenza delle Corti inglesi in materia di *data retention* e accesso ai metadati è vasta ed articolata, resa complessa del continuo intreccio con il livello sovranazionale e, dunque, con le decisioni della CGUE. Il dialogo con quest'ultima, del resto, è continuo ed è anzi stato promosso anche a seguito della decisione espressa dal popolo inglese di uscire dall'Unione europea. Questo avvenimento, così come l'approccio, quantomeno iniziale, del legislatore nazionale che aveva adottato normative rapidamente messe in discussione proprio alla luce dei principi affermati dai giudici di Lussemburgo, hanno inciso fortemente sull'orientamento seguito dalle Corti inglesi, che pure hanno conosciuto una certa evoluzione nel corso del tempo: se da un lato si è assistito ad una sempre maggiore attuazione dei c.d. criteri *Tele2*, dall'altro i giudici non hanno mancato di mettere in discussione alcuni dei rilievi svolti dalla CGUE o di darne una interpretazione quantomeno 'elastica' o, ancora, di chiedere l'intervento chiarificatore dei giudici europei anche e soprattutto volti a determinare i confini e l'ambito di applicazione del diritto dell'UE.

Procedendo cronologicamente, prima rilevante tappa della giurisprudenza inglese in materia e 'motore' di quello che sarà il primo momento di dialogo con i giudici di Lussemburgo è da individuarsi nel ricorso promosso da alcuni cittadini, Brice, Lewis, Davis e Watson (questi ultimi due membri della House of Commons) dinnanzi alla High Court: i ricorrenti – poi sostenuti dalle ONG Open Rights Group, Privacy International e The Law Society –, fondando le proprie posizioni sui principi delineati dalla giurisprudenza della CGUE nella sentenza *DRI* e opponendosi a quanto sostenuto dal Governo e dal legislatore nel processo di approvazione del DRIPA, avevano richiesto ai giudici di dichiarare il regime nazionale di *data retention* e accesso ai metadati non conforme al diritto dell'UE[39]. La High

[39] Come noto e come specificato anche dalla High Court, "at common law, Acts of the UK Parliament are not open to challenge in the Courts. But the position under EU law is different. Decisions of the CJEU as to what EU law is, are binding on the legislatures and Court of all Member States" (par. 4). In tal senso, dunque, la controversia era attinente alla compatibilità della normativa interna rispetto ai diritti tutelati agli art. 7 e 8 della Carta di Nizza, come interpretati dalla CGUE ("the test of validity of the Act [DRIPA] and the 2014 Regulations is whether they are compliant with Articles 7 and 8 of the EU Charter and/or Article 8 ECHR", par. 7). Considerando che "the Charter [Carta di Nizza] has direct effect in national law, it only binds Member States when they are implementing EU law (art. 51)", il giudice inglese aveva sin da subito chiarito come la normativa nazionale, essendo attinente alla protezione dei dati, dovesse essere ritenuta rientrante nell'ambito di applicazione del diritto dell'UE ("data protection law has been within the scope of EU law for 20 years", par. 7). È interessante sul punto anche la successiva considerazione svolta dalla High Court: "The extent of the State's powers to require the retention of communications data and to gain access to such retained data are matters of legitimate political controversy both in the UK and elsewhere. The Queen's Speech opening the new Parliament on 27 May 2015 indicated that 'new legislation will modernize the law on communications data'. To take one example from abroad, on 2 June 2015 the US Congress passed one statute (the USA Freedom Act) restricting the data retention powers previously conferred by another statute passed in 2001 (the USA Patriot Act). It is not our function to take sides in this continuing debate, not to say whether in our opinion the powers conferred by DRIPA are excessive or not. We have to decide the comparatively dry question of whether or not they are compatible with EU law as expounded by the CJEU in *DRI*", par. 11.

Court (Divisional Court), con sentenza del 17 luglio 2015[40], aveva concluso a favore dei ricorrenti, ritenendo la Section 1 del DRIPA incompatibile con i requisiti fissati all'art. 15 della Direttiva *e-Privacy* e con l'interpretazione fornita nella sentenza *DRI*, nella misura in cui non venivano previste regole chiare e precise a disciplina dell'accesso ai metadati, non veniva limitato lo scopo dell'accesso e dell'ordine di conservazione al solo perseguimento di reati gravi e non veniva stabilito un controllo preventivo da parte di una Corte o di una autorità amministrativa indipendente[41]. Sebbene queste considerazioni avessero portato a ritenere tale pronuncia una vittoria significativa, segno della grande sensibilità che i giudici inglesi iniziavano a mostrare rispetto alla tutela dei diritti alla riservatezza e protezione dei dati, uno sguardo più attento ed una analisi maggiormente dettagliata induce a ridimensionare tale ottimistica visione. La Divisional Court infatti non era giunta – come invece ad esempio aveva fatto la Corte costituzionale belga e come si vedrà nel successivo Capitolo – ad affermare l'incompatibilità col diritto dell'UE e la Carta di Nizza di una forma di conservazione generalizzata ed indiscriminata quale quella prevista dal DRIPA. È utile ricordare preventivamente come tale normativa, diversamente dalle discipline adottate da altri Stati membri, non prevedesse direttamente un obbligo di conservazione in capo a tutti i fornitori di servizi di telecomunicazione bensì stabilisse tale imposizione solo a seguito di un '*retention notice*', da parte del *Secretary of State* che poteva quindi anche disporre una *data retention* limitata solo ad alcuni fornitori, tipologie di metadati o utenti; nonostante queste considerazioni, tuttavia, la stessa High Court aveva riconosciuto come l'ordine di conservazione ben potesse assumere carattere di generalità ed indeterminatezza e coinvolgere dunque tutti gli utenti, tutti i metadati e tutti i fornitori: "we should test the validity of DRIPA on the assumption that the retention notices issued under it may be as broad in scope as the statute permits, namely a direction to each CSP to retain all communications data for a period of 12 months. The case was argued on both sides on that basis. We shall refer in this judgment to a system under which the State may require CSPs [Comunications Service Providers] to retain all communications data for a period as a general retention regime" (par. 65). Partendo da tali premesse, i giudici avevano stabilito, sulla linea di quanto affermato dalla CGUE, che la *data retention* rappresentava *per se* una ingerenza nei diritti fondamentali tutelati dagli artt. 7 e 8 della Carta di Nizza, anche a prescindere dal successivo accesso[42]. Giunta a queste considerazioni, però, la High Court proseguiva fornendo una interpretazione ed una lettura della sentenza *DRI* piuttosto restrittiva, che ne circoscriveva significativamente la portata con riferimento alla disciplina della conservazione dei metadati: nella storica pronuncia, infatti, secondo i giudici inglesi "the Court [ECJ] was not indicating that communications data can only be retaind if they relate to particular geographical areas, or to a particular individuals likely to be involved in serious crime. It was identifying the width of the Directive [DRD], which imposed no limits on the power to retain. But the Court was not, as we read the judgement, purporting to lay down any particular limitations on that power, as opposed to conditions of access. To have done so would, apart from being to some extent impracticable, have been inconsistent with the Court's clear conclusion in par. 44 of the Judgement, that retention of data for the purpose of allowing the competent national authorities to have possible access to those data genuinely satisfies an objective

[40] [2015] EWHC 2092, Case No. CO/3665/2014; CO/3667/2014; CO/3794/2014.

[41] Veniva infatti dichiarato che il DRIPA "does not lay down clear and precise rules providing for access to and use of communications data retained pursuant to a retention notice to be strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating to such offences and access to the data is not made dependent on a prior review by a court or an independent administrative body whose decision limits access to and use of the data to what is strictly necessary for the purpose of attaining the objective pursued", par. 114. Con riferimento al requisito del previo controllo, veniva poi affermato come "The need for approval to be by a judge or official wholly independent of the force or body making the application should not, provided the person responsible is properly trained or experienced, be particularly cumbersome", par. 114.

[42] Per una ricostruzione dei punti fondamentali di tale pronuncia, nella quale la High Court ha richiamato la giurisprudenza delle due Corti europee, CGUE e Corte EDU (nello specifico la sentenza *DRI* e la decisione *Liberty v. UK*), si rimanda a M. SENOR, *Un altro 'tango down' in tema di data retention*, in *MediaLaws*, 22 luglio 2015.

of general interest" (par. 85). Da tale premessa, quindi, la High Court giungeva alla conclusione secondo cui "the solution to the conundrum, in our view, is that the legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter *unless* it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights" (par. 89). Ne risulta dunque una posizione di estremo rilievo, che sarà determinante per comprendere l'approccio dei giudici inglesi alla giurisprudenza della CGUE: non veniva riconosciuta nella sentenza *DRI* una dichiarazione di incompatibilità assoluta di forme di conservazione generalizzata rispetto al diritto dell'UE e la soluzione di una conservazione targettizzata era considerata essere solo una delle possibili soluzioni alla ingerenza nei diritti fondamentali, che non risultava tuttavia obbligatoria e non doveva pertanto essere letta quale unico strumento per garantire la proporzionalità del regime di conservazione: quest'ultimo risultava legittimo anche qualora generalizzato purché la normativa in materia fosse in grado di stabilire adeguate salvaguardie nella fase di accesso. Ed è proprio unicamente sotto tale ultimo profilo che il DRIPA veniva considerato incompatibile con il diritto dell'UE[43]. Tale visione, se da un lato "shows the difficulties national courts may have in applying the rulings of the ECJ in their respective domestic arenas", dall'altro "seems to downplay the extent of the concerns the ECJ expressed about data retention as well as the concerns of the Advocate General as to the complete and accurate picture of users being created"[44]. Agli occhi dei giudici inglesi, tuttavia, la lettura fornita della sentenza *DRI* e della legittimità del regime di conservazione dei dati risultava assolutamente coerente e chiara, tanto da giustificare il respingimento della richiesta delle parti di provvedere ad un rinvio pregiudiziale alla CGUE volto a chiarire taluni aspetti della pronuncia che risultavano invece per i ricorrenti dibattuti ed oggetto di differenti e opposte interpretazioni. Pur prendendo atto del rinvio pregiudiziale nel frattempo promosso dalla Corte amministrativa svedese nel caso *Tele2* (C-203/2015), nonché riconoscendo che le Corti costituzionali di tre Stati membri (Slovenia, Romania e Belgio) avevano dichiarato l'invalidità della normativa nazionale a seguito della sentenza *DRI* basandosi anche sulla valutazione delle criticità che il carattere generalizzato della conservazione comportava, la High Court aveva comunque ritenuto inopportuno richiedere l'intervento della CGUE: ciò sia perché i criteri delineati nella pronuncia *DRI* risultavano totalmente chiari, sia perché le conclusioni cui i giudici di Lussemburgo erano giunti non dovevano essere necessariamente le stesse cui i giudici nazionali dovevano pervenire, essendo questi ultimi chiamati a valutare normative nazionali ciascuna differente e con le loro peculiarità rispetto alla DRD, ed infine perché il DRIPA prevedeva una *sunset clause* tale da rendere concretamente inutile una pronuncia della CGUE; tale decisione infatti sarebbe certamente intervenuta troppo tardi, ovvero in un momento in cui la normativa nazionale in esame sarebbe stata già sostituita: "the CJEU typically takes two years or more to answer to a question referred to it for a preliminary ruling. It is most unlikely that an answer to a reference made now would be received before DRIPA has expired, or has been repealed and replaced by a new statute. Either way, the answer would have become academic" (par. 113).

Sulla base delle valutazioni richiamate, dunque, la High Court giungeva a dichiarare un ordine di disapplicazione della Section 1 del DRIPA poiché incompatibile con il diritto dell'UE; tale ordine tuttavia risultava sospeso sino al 31 marzo 2016, allo scopo di fornire un adeguato intervallo di tempo al legislatore per poter intervenire sulla legge e correggerne gli aspetti problematici, senza creare

[43] Veniva inoltre specificato, con riferimento al requisito della finalità dell'accesso limitato al solo perseguimento di reati gravi, che: "the requirement that access to and use of the data must be strictly restricted to the purpose of preventing and detecting precisely defined serious offences (..) does not mean that access must be limited to the data of people suspected to have committed serious crime" (par. 94).

[44] L. WOODS, *High Court strikes down data retention laws in ruling on DRIPA*, in *European Data Protection Law Review*, 3, 2015, p. 239.

pericolosi 'vuoti' normativi in un settore estremamente delicato e dagli impatti determinanti per la garanzia della sicurezza[45].

3.2. – I rinvii pregiudiziali della Court of Appeal *e del* Investigatory Powers Tribunal*: dalla sentenza* Tele2 *al caso* Privacy International

La complessità della materia in esame e le diverse interpretazioni della sentenza *DRI* che venivano promosse e sostenute, emergono però con forza nella reazione del Governo dinnanzi alla decisione della High Court: il *Secretary of State*[46], infatti, decideva di proporre appello dinnanzi alla Court of Appeal, ritenendo erronea la lettura della giurisprudenza della CGUE fornita dai giudici di primo grado. Secondo gli appellanti, infatti, i requisiti fissati dai giudici di Lussemburgo erano da ritenersi meramente "descriptive and not prescriptive"[47] e non automaticamente applicabili nella valutazione della conformità al diritto dell'UE di una normativa nazionale. Ebbene, con una fondamentale sentenza del 20 novembre 2015[48], la Court of Appeal ribaltava la posizione espressa dalla Corte di primo grado, accogliendo gran parte delle osservazioni mosse dal Governo. Secondo i giudici di seconda istanza, infatti, la sentenza *DRI* non escludeva totalmente la possibilità di ricorrere a regimi di conservazione generalizzata né obbligava gli Stati membri ad adottare discipline che limitassero l'accesso alla sola finalità di lotta alla criminalità grave; una diversa e più restrittiva interpretazione avrebbe contrastato con la più ampia discrezionalità garantita ai legislatori nazionali dall'art. 15 della Direttiva *e-Privacy*[49]. Per questo motivo, la Court of Appeal affermava che nella sentenza *DRI* "the ECJ was not laying down specific mandatory requirements of EU law but was simply identifying and describing protections that were entirely absent from the harmonised EU regime. The Court's conclusion that the DRD was unlawful was compelled by the cumulative effect of what was not in the DRD" (par. 73)[50].

---

[45] È interessante il ragionamento espresso dalla High Court a giustificazione del prolungato lasso di tempo concesso al Parlamento per addivenire ad una modifica della normativa esistente, che dimostra una certa consapevolezza dei giudici inglesi circa la complessità della materia e la volontà di mettere in guardia il legislatore quanto ai pericoli di una normativa adottata in maniera troppo affrettata – come accaduto per il DRIPA –: "The Court do not presume to tell Parliament for how long and in what detail Bills should be scrutinised, but it is right to say (to put it no higher) that legislation enacted in haste is more prone to error, and it would be highly desirable to allow the opportunity of thorough scrutiny in both Houses", par. 121.

[46] Sul punto, "although the decision was widely welcomed, police and security officials again warned that lives would be at risk if data were not retained. Under pressure from the security services, the government appealed to the UK Court of Appeal", L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the United Kingdom after the European Data Retention Directive*, op. cit., p. 568.

[47] Secondo il *Secretary of State*, infatti, "The CJEU in *DRI* did not impose mandatory requirements which must to be applied to national legislation. it simply held that the harmonized EU scheme for data retention failed to incorporate any safeguards and therefore was not compliant with EU fundamental rights", par. 54; inoltre "the EU Charter does not apply to national rules concerning access by law enforcement bodies to communications data. The judgement cannot, therefore, be read as imposing substantive requirements on national law based on the EU Charter in areas where the Charter does not apply", par. 54.

[48] [2015]EWCA Civ 1185, Case n. C1/2015/2612.

[49] "Limiting the power of Member States to legislate for access to retained data only where it is necessary and proportionate for purposes relating to serious crime, would conflict with the more extensive powers of derogation enjoyed by Member States in EU law, for example in art. 15 of the *e-Privacy Directive*" (par. 84).

[50] È importante precisare come, non accogliendo la visione del Governo secondo cui "when adopting domestic legislation relating to access and use of communications data by police or other law enforcement bodies, Member States are not implementing EU law" (par. 98), la Court of Appeal aveva riconosciuto come rientrante nell'ambito di applicazione del diritto dell'UE sia la disciplina della conservazione quanto quella dell'accesso ai metadata: "we consider that DRI establishes that when evaluating the lawfulness of a retention regime of communications data it is necessary to evaluate the safeguards in respect of access to the retained data. To this extent, provisions in relation to access fall within the scope of EU law and require to be evaluated by general principles of EU law

La posizione della Court of Appeal dunque divergeva nettamente da quanto sostenuto dai giudici di primo grado, che avevano constatato l'incompatibilità del DRIPA alla luce di quei requisiti, ritenuti obbligatori, che la CGUE aveva fissato con riferimento alla disciplina dell'accesso. Proprio sulla base di questa riconosciuta divergenza interpretativa, i giudici dell'appello decidevano di discostarsi, ancora una volta, dalle valutazioni della High Court e di promuovere, come noto, un rinvio pregiudiziale ai giudici di Lussemburgo: rispetto alla sentenza *DRI* erano, infatti, emersi "considerable doubts as to the effect of its decision. On this, we have the misfortune to have come to a provisional view which differs from that of the Divisional Court. (..) This is an issue of general and wide-reaching importance. Notwithstanding the expiry of DRIPA on 31 December 2016 it will not become academic. On the contrary, the true effect of the judgement in DRI will remain central to the validity of all future legislation enacted by the Member States in this field", par. 117. Ribaltando dunque le considerazioni svolte dalla High Court, i giudici d'appello avevano riconosciuto di fondamentale importanza – anche per la successiva normativa che il legislatore era chiamato ad adottare in materia – l'ottenimento di un chiarimento da parte della CGUE circa la posizione espressa nella sentenza *DRI*, cui viene attribuito centrale rilievo. Considerando anche la giurisprudenza di altri Stati membri, che avevano invalidato le normative nazionali in materia (nel frattempo erano divenute sei le Corti nazionali che si erano in tal senso pronunciate, ovvero Austria, Slovenia, Romania, Belgio, Olanda e Slovacchia), la Court of Appeal proponeva così il già esaminato rinvio pregiudiziale volto a stabilire, proprio sulla base della divergente posizione espressa dagli stessi giudici inglesi, se i requisiti posti dalla sentenza *DRI* avessero o meno carattere obbligatorio, soprattutto con riferimento alla disciplina dell'accesso, la cui determinazione, nella DRD, era però lasciata ai legislatori nazionali.

Sin da tali prime sentenze risalenti al periodo immediatamente successivo alla sentenza *DRI*, emerge un quadro piuttosto complesso della giurisprudenza inglese in materia di *data retention* e accesso ai metadati: i giudici nazionali non hanno mostrato un orientamento condiviso ed uniforme in materia; se da un lato, infatti, con riferimento alla disciplina della conservazione, entrambe le Corti di primo e secondo grado hanno letto la decisione dei giudici di Lussemburgo come non determinante l'incompatibilità di un regime di *bulk data retention* rispetto al diritto dell'UE, dall'altro lato, sotto il profilo dell'accesso si è verificata una netta divergenza di vedute nella interpretazione dei requisiti fissati dalla giurisprudenza della CGUE.

Da questa prima difficoltà riscontrata dai giudici inglesi, sfociata nel rinvio pregiudiziale poi risolto dalla Corte di giustizia congiuntamente a quello promosso dai giudici svedesi, ha avuto dunque origine la nota sentenza *Tele2*: come già ampiamente analizzato nel Capitolo II, Parte II, tale pronuncia era stata accolta con grande favore dalle ONG attive nell'ambito della difesa dei diritti fondamentali alla riservatezza e alla protezione dei dati e da parte della società civile; il Governo del Regno Unito e i massimi esponenti delle autorità di *law enforcement* nazionali invece avevano sin da subito espresso preoccupazioni quanto ai possibili dannosi risvolti causati dalla posizione della CGUE, che avrebbe potuto incidere sulla capacità delle autorità pubbliche di proteggere efficacemente la sicurezza pubblica e nazionale[51]. Tali valutazioni si ritrovano con chiarezza in due pronunce del *Investigatory Powers Tribunal*, intervenute proprio poco prima e poco dopo la sentenza *Tele2* e che si collocano, seguendo uno sviluppo cronologico, in un momento successivo rispetto alla sentenza della Court of Appeal appena analizzata. Queste due pronunce risultano di fondamentale rilievo per poter comprendere non solo gli sviluppi successivi della giurisprudenza inglese, bensì anche il dialogo nuovamente instaurato con la CGUE nel caso *Privacy International*. Mentre nella previa analisi di quest'ultimo rinvio (svolta nel

including EU Charter", par. 102. Nonostante questa importante affermazione, tuttavia, quanto statuito dalla CGUE in materia di accesso non poteva essere considerato obbligatorio per il legislatore nazionale.

[51] Per una ampia ricostruzione delle reazioni e delle dichiarazioni dei principali esponenti di numerose ONG così come del Governo, si rimanda a A. MUNIR, S. YASIN, S. BAKAR, *Data retention rules: a dead end*, op. cit., p. 80 ss.

Capitolo IV, Parte II) l'attenzione si era concentrata sui quesiti rivolti ai giudici europei nonché sulle successive considerazioni dell'Avvocato generale, in questa sede si ritiene essenziale ricostruire invece le doglianze della ricorrente Privacy International, la posizione espressa dai giudici inglesi e i motivi del rinvio.

La controversia dinnanzi al IPT[52] risale al ricorso promosso dalla ONG Privacy International, avente ad oggetto una disciplina in parte differente rispetto a quella che aveva interessato la High Court e la Court of Appeal in precedenza. La ricorrente infatti riteneva il *Telecommunications Act 1998* – che regolava l'acquisizione, utilizzo, conservazione, memorizzazione e cancellazione di metadati in forma generalizzata e aggregata da parte delle agenzie di intelligence (c.d. SIAs, *Security and Intelligence Agencies*, che ricomprendevano i *Government Communications Headquarters* GCHQ e il *Security Service*, noto come MI5) – incompatibile con la Convenzione EDU e con il diritto dell'UE, sulla base dei principi determinati dalla CGUE nella sua giurisprudenza in materia di conservazione e accesso ai metadati.

In una prima parziale pronuncia del 17 ottobre 2016, il IPT si era concentrato sul primo quesito posto dalla ricorrente, valutando cioè la legittimità e compatibilità della disciplina sopra indicata unicamente alla luce dell'art. 8 della Convenzione EDU; nella seconda decisione del 8 settembre 2017 il Tribunale, a seguito di ulteriori e più approfondite udienze, si era invece occupato di vagliare la compatibilità dei poteri di raccolta, conservazione e accesso di metadati attribuiti alla agenzie di intelligence con riferimento al diritto dell'UE. Sebbene tale ultima pronuncia risulti certamente di maggiore interesse ai fini della presente disamina, pare comunque di rilievo premettere come il IPT abbia considerato, nella prima sentenza del 2016[53], il potere attribuito ai *Home and Foreign Secretaries* di imporre ai fornitori di servizi di comunicazione il trasferimento generalizzato di metadati (c.d. *Bulk Communications Data*, BCD[54]) alle agenzie di intelligence compatibile con l'art. 8 della Convenzione EDU: i giudici avevano infatti ritenuto proporzionate ed adeguate le salvaguardie predisposte dalla normativa nazionale, volte a scongiurare il rischio di abusi nella fase di trattamento – anche automatizzato – dei metadati, così come la supervisione garantita dal *Independent Intelligence Service Commissioner*[55].

Nella successiva pronuncia del 2017, avente più specificamente ad oggetto la compatibilità rispetto al diritto dell'UE del sistema di raccolta e analisi dei metadati utilizzato dalle SIAs, il IPT svolgeva una premessa di rilievo: "the context of the issues before us has been as to the balance between the steps taken by the State, through the SIAs, to protect its population against terror and threat to life against the protection of privacy of the individual" (par. 6). Questa affermazione quindi mirava a chiarire come il bilanciamento che il legislatore era stato chiamato a svolgere e che i giudici dovevano vagliare vedesse da un lato un interesse collettivo e dall'altro un diritto di dimensione meramente individuale: una lettura

[52] *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, case n. IPT/15/110/CH.

[53] Come ben spiegato da Woods, "this judgement [del 2016] then effectively dealt with questions of lawfulness, as understood in the light of art. 8 ECHR. (..) The difficult topics regarding proportionality and the impact of *Tele2* remain to be dealt with", L. WOODS, *Investigatory Powers Tribunal (IPT): Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, in *European Data Protection Law Review*, 3, 2017, p. 248.

[54] Questo termine viene impiegato per distinguere tale tipologia di trasferimento da quella che aveva invece ad oggetto i c.d. *Bulk Personal Datasets* (BPDs): in sintesi questi ultimi "Are databases in which personal data relating to a large number of individuals are of no interests to the SIA. Such datasets can include what would be viewed in data protection terms as sensitive personal data. The datasets covered a potentially limitless range of topics, for example financial matters and travel. Further the datasets can be combined or analysed together", L. WOODS, *Investigatory Powers Tribunal (IPT)*, op. cit., p. 247.

[55] Merita precisare come la compatibilità con l'art. 8 della Convenzione EDU fosse stata dichiarata con riferimento alla disciplina nazionale e alle salvaguardie predisposte a seguito del 2015. Questa distinzione nasce dal fatto che dopo tale data erano stati resi noti i metodi e i poteri attribuiti alla SIAs, mediante un Report fornito al *Intelligence Security Committee of Parliament*. La pubblicizzazione del regime aveva infatti portato ad una modifica del regime previgente e all'inserimento di maggiore tutele e salvaguardie che, anche mediante la conoscenza dell'esistenza di tali sistemi di controllo dei metadati, risultavano solo da quel momento realmente efficaci.

che pareva voler mettere, sin dall'inizio, in evidenza la maggior rilevanza della tutela della sicurezza rispetto ad una prerogativa riconosciuta al singolo e che, proprio per questo, ha attirato – come si vedrà – non poche critiche, soprattutto se rapportata alla giurisprudenza di entrambe le Corti europee. A conferma e rafforzamento di quella premessa, poi, i giudici del IPT sottolineavano l'importanza da attribuire ai sistemi di *bulk acquisition* di metadati, cioè di trasferimento massivo di informazioni alle agenzie di intelligence: "the use of bulk data capabilities is critical to the ability of the SIAs to secure national security; a fundamental feature of many of the SIAs' techniques of interrogating Bulk Data is that they are non-targeted, not directed at specific targets" (par. 10). Riconoscendo il fondamentale ruolo svolto da tali regimi, i giudici giungevano alla conclusione secondo cui imporre anche a tali attività, volte alla tutela della sicurezza nazionale, il rispetto dei requisiti stabiliti nelle sentenze *DRI* e *Tele2* (quest'ultima pubblicata nelle more del giudizio in esame) avrebbe comportato una forte diminuzione in termini di efficacia dell'azione delle SIAs. Secondo il Report presentato da Anderson, *Independent Reviewer of Terrorism Legislation*, veniva stabilito come "bulk acquisition has been demonstrated to be crucial, in a variety of fields (..). The SIAs' ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means" (par. 14), così che una forma targetizzata di raccolta, conservazione e accesso ai metadati non sarebbe stata in grado di garantire il medesimo livello di efficacia e di garanzia della sicurezza. I giudici inglesi avevano poi messo in evidenza come le SIAs non esaminassero tutti i dati loro trasferiti 'in bulk' dai fornitori privati: "by process of elimination, and with minimal intrusion, [the SIAs] obtain access only to the data of persons whose activities may constitute a threat to national security" (par. 16), in modo tale che solo una ristretta porzione dei dati raccolti veniva effettivamente vagliata. Insieme a tutte queste considerazioni, che miravano a confermare la necessità di sistemi di *bulk transfer* e la loro limitata invasività nella sfera privata, il Governo, parte resistente nel procedimento, aveva sostenuto che i requisiti enunciati nella pronuncia *Tele2* non dovessero essere applicati e applicabili alla disciplina in esame: innanzitutto la finalità perseguita dal regime regolato dalla normativa del 1998 era quella di tutela della sicurezza nazionale, una materia che, ai sensi dell'art. 4 TUE, non rientrava nell'ambito di applicazione del diritto dell'UE; inoltre i principi stabiliti dalla giurisprudenza europea prendevano avvio da un caso avente ad oggetto la disciplina del DRIPA, che riguardava però non il trasferimento di metadati alle agenzie di intelligence e la diretta conservazione da parte di esse dei metadati, bensì la conservazione da parte di fornitori privati di metadati riguardanti i propri utenti al fine di rendere disponibili tali informazioni alle autorità di *law enforcement*. Per queste ragioni, il Governo aveva ritenuto, peraltro richiamando ampiamente la sentenza *Parlamento c. Consiglio*, che la disciplina posta all'attenzione del IPT non dovesse essere vagliata alla luce del diritto dell'UE ma unicamente sulla base della Convenzione EDU, rispetto alla quale il Tribunale aveva già pronunciato la compatibilità della disciplina in esame nella previa sentenza del 2016. Ne derivava che "the BCD regime is not within the scope of the Treaty and the Directive [Direttiva *e-Privacy*] and is only subject to the ECHR. In any event the Watson requirements cannot and should not apply, because there is no analogy between the activities and the legal basis for such activities under consideration in Watson and the BCD regime" (par. 49). Per Privacy International, al contrario, la posizione espressa dal Governo si fondava su erronee considerazioni, quali la convinzione secondo cui una acquisizione generalizzata e un trattamento automatizzato dei metadati rappresentassero una invasione più limitata della sfera privata rispetto ad una forma di conservazione e accesso targettizzati; o ancora la prevalenza dell'interesse alla tutela della collettività rispetto al diritto del singolo o l'incompatibilità di forme di salvaguardia più stringenti con una efficace ed efficiente attività di protezione della sicurezza nazionale.

I giudici del IPT non potevano quindi che prendere atto della divergenza di posizioni espresse dalle parti del processo: sebbene fosse pacifico che "the supply of BCD by telecoms providers to the SIAs would fall under the definition of data processing, the question was whether such supply for purposes of national security would fall outside the scope of EU law". Sul punto, il Tribunale riteneva

imprescindibile un intervento della CGUE, volto a chiarire i confini del diritto dell'UE e dunque l'ambito di applicazione dei c.d. requisiti *Tele2*. Avendo già svolto considerazioni approfondite quanto alle questioni sollevate in tale rinvio, esaminato nel dettaglio nel Capitolo IV, Parte II, ciò che merita di essere in questa sede sottolineato sono le considerazioni comunque svolte dal IPT, che aiutano a comprendere appieno l'approccio del giudice inglese in materia. Pur promuovendo il rinvio pregiudiziale, al momento ancora pendente, il Tribunale non ha mancato di concordare con la posizione espressa dal Governo, secondo cui cioè le salvaguardie indicate dalla CGUE risultano incompatibili con strumenti di garanzia della sicurezza nazionale che richiedono necessariamente forme di "bulk and unspecific processing of data" (par. 55): requisiti quali il previo controllo indipendente o la notifica ai soggetti i cui dati vengono vagliati da autorità pubbliche possono minare seriamente l'efficacia e l'utilità delle attività poste in essere dalle SIAs. Per questo il IPT concludeva sostenendo che "we are persuaded that if the Watson requirements do apply to measures taken to safeguard national security, in particular the BCD regime, they would frustrate them and put the national security of the UK, and, it may be, other Member States, at risk" (par. 69). Una considerazione forte, che risulta coerente del resto con la premessa sopra richiamata nella quale veniva evidenziato come ad essere bilanciati fosse un interesse collettivo – la sicurezza – ed un diritto unicamente dell'individuo – la privacy e la protezione dei dati – . In questo i giudici hanno dimostrato di non riconoscere nella tutela della privacy e nella necessaria proporzionalità di sistemi di sorveglianza e controllo dei metadati una rilevanza che va in realtà ben oltre l'interesse del singolo: come riconosciuto anche dalla giurisprudenza della Corte EDU, sistemi di *bulk trasfer, collection* e *retention*, privi di limiti e salvaguardie, rischiano di compromettere i valori fondamentali sui quale la stessa società democratica poggia, con un impatto che è in grado di andare oltre la mancata protezione dei dati personali per giungere a creare quella sensazione di diffusa sorveglianza che incide sul godimento di altri diritti fondamentali quali la libertà di espressione e di associazione o il principio di presunzione di innocenza. La posizione che sembra essere accolta dai rilievi svolti dal giudice inglese è quella di un bilanciamento che appare già sbilanciato in partenza laddove viene affermato che la sicurezza rappresenta comunque un interesse superiore e la privacy viene considerata un mero diritto del singolo il cui mancato rispetto su null'altro incide[56]. Oltre a questa valutazione di carattere generale che vuole porre in discussione le posizioni espresse dai giudici inglese e mostrarne i limiti, è stato rilevato anche come "some of CJEU cases relied on by the IPT and Respondents predate the entry into force of the Lisbon Treaty and thus, data from a time when the Charter was not yet applicable as a primary EU law instrument. While the IPT relies on Parliament v. Council and Ireland v. Parliament to support the assumption that the transfer of PNR data was an activity falling outside the scope of the EU law, the CJEU, in Opinion 1/15 stated that such transfers are subject to Article 8 of the EU Charter"[57]: ciò aiuta a comprendere come talune considerazioni svolte dal IPT – spesso mutuate dalla posizione espressa dal Governo – non tenessero debitamente in considerazione gli sviluppi successivi della giurisprudenza europea, riportando sentenze che trovavano la loro ragion d'essere anche e soprattutto se lette nel contesto pre-Trattato di Lisbona. Nel porre quesiti molto specifici quanto all'ambito di applicazione del diritto dell'UE e alla sua espansione anche ad attività proprie delle agenzie finalizzate a tutelare la sicurezza nazionale, il IPT ammonisce quasi la CGUE, ribadendo il peso e le conseguenze potenzialmente devastanti di un necessario adeguamento delle attività delle SIAs ai requisiti *Tele2*. Questa pronuncia, dunque, non fa che confermare quell'approccio pragmatico già evidenziato nelle previe pronunce di High Court e Court of Appeal, che avevano sottolineato l'infattibilità pratica delle soluzioni promosse dalla CGUE e l'impatto rilevante delle salvaguardie da

[56] M. WHITE, *The Privacy International case in the IPT: respecting the right to privacy?*, in *EU Law Analysis*, 14 settembre 2017, http://eulawanalysis.blogspot.com/2017/09/the-privacy-international-case-in-ipt.html.
[57] T. QUINTEL, *Investigatory Powers Tribunal: Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Ors Part II*, in *European Data Protection Law Review*, 3, 2017, p. 393.

essa imposte rispetto alla efficacia degli strumenti impiegati da autorità di *law enforcement* e di intelligence allo scopo di garantire la fondamentale esigenza della sicurezza.

3.3. – La Court of Appeal *nel caso* 'Watson II' *a seguito della sentenza* Tele2*: un complesso ed articolato contesto tra evoluzioni normative in corso e importanti casi giurisprudenziali pendenti*

Mentre il procedimento promosso innanzi al IPT risultava sospeso in attesa della pronuncia dei giudici di Lussemburgo sotto il delicato profilo dell'ambito di applicazione del diritto dell'UE, un altro caso veniva invece riesaminato dalla Court of Appeal: nel caso C1/2015/2612 & 2613, vertente tra *Secretary of State* da un lato e Watson, Brice e Lewis, dall'altro, i giudici d'appello avevano ripreso le "redini" del c.d. "caso Watson" da cui era originato il rinvio pregiudiziale alla CGUE sfociato nella richiamata sentenza *Tele2*. La decisione cui era infine giunta la Court of Appeal, in data 30 gennaio 2018[58], mostra tutta la persistente complessità della disciplina della *data retention* nel contesto inglese, anche e nonostante l'ulteriore pronuncia dei giudici europei: calare nel caso concreto della disciplina del DRIPA i requisiti e i principi fissati a livello sovranazionale si era rivelata una operazione tutt'altro che semplice, considerato tanto l'avvicendamento normativo intercorso nelle more del giudizio dinnanzi ai giudici di Lussemburgo, che aveva portato al superamento del DRIPA e all'adozione dell'IPA alla fine del 2016, quanto i numerosi "fronti giudiziari" ancora aperti e pendenti innanzi ad altre Corti nazionali all'epoca del giudizio dinnanzi alla Court of Appeal. Uno di questi "fronti" caldi era da individuarsi nella causa promossa da Privacy International davanti al IPT, appena esaminata; l'altro invece era rappresentato da un importante ricorso promosso dalla ONG Liberty dinnanzi ai giudici della High Court e avente ad oggetto la conformità della Part 4 dell'IPA ai requisiti indicati dalla giurisprudenza della CGUE (*Liberty c. Secretary of State*), che verrà più ampiamente analizzata in seguito. A ciò era da aggiungersi anche il procedimento di modifica dell'IPA avviato, nel novembre 2017, dal *Secretary of State*, mediante la pubblicazione di un documento di consultazione e di proposta di emendamenti finalizzati a recepire ed adeguare la normativa interna al diritto dell'UE, come interpretato dalla giurisprudenza della CGUE[59]: come si è già messo in evidenza, il Governo e il legislatore nazionale avevano infatti riconosciuto, a seguito della sentenza *Tele2*, la presenza nella normativa all'epoca vigente di alcune lacune rispetto ai requisiti ribaditi dai giudici di Lussemburgo in tale ultima pronuncia.

Ecco quindi come proprio alla luce di tale contesto, caratterizzato da forti cambiamenti in corso sul fronte normativo e da rilevanti aspetti ancora in attesa di chiara definizione da parte della giurisprudenza nazionale o sovranazionale, è possibile comprendere la scelta della Court of Appeal di non pronunciarsi su taluni punti delicati sui quali la sentenza *Tele2* verteva e di rimetterne la soluzione ai giudici europei nel rinvio *Privacy International* da un lato e alla High Court nel caso *Liberty* dall'altro, decidendo quindi di occuparsi solo della valutazione degli aspetti legati alla normativa previgente e rispetto alla quale il rinvio pregiudiziale *Watson* era stato promosso.

Premettendo come "the fact that DRIPA has now been repealed does not make this a pointless exercise" (par. 7), i giudici aprivano tuttavia la pronuncia con una iniziale affermazione di grande rilievo: "I regret to say that the task now facing this Court is far from easy in view of the fact that the preliminary ruling from the CJEU is lacking in clarity. This is apparent from the disputes between the parties before us as to its effect and from the fact that it has already given rise to a further reference by

[58] [2018]EWCA Civ 70.

[59] Anche nella sentenza "Watson II", i giudici avevano preso atto della consultazione avviata: "The consultation and proposed amendments deal, inter alia, with the restriction, in the context of fighting crime, to 'serious crime', the need for prior review by a court or an independent administrative authority for access to retained data, ex-post facto notification and the issue of retention of retained communications data within the EU" (par. 7).

the IPT" (par. 8). Riconoscendo dunque come anche a seguito della pronuncia *Tele2* persistessero ancora 'zone grigie' e diverse possibili interpretazioni della medesima giurisprudenza europea, l'unico punto rispetto al quale era riscontrata chiarezza era quello attinente ai requisiti in materia di accesso ai metadati: non vi erano dubbi, infatti, quanto alle salvaguardie individuate dai giudici di Lussemburgo nella restrizione dell'accesso alle sole finalità di lotta a crimini gravi nonché nella predisposizione di un necessario previo controllo da parte di una Corte o di una autorità amministrativa indipendente. Escludendo la questione, sottoposta a rinvio nel caso *Privacy International*, circa l'estensione di tali requisiti anche alle attività poste in essere dalle agenzie di intelligence per finalità di sicurezza nazionale, la Court of Appeal giungeva piuttosto rapidamente alla conclusione secondo cui, limitatamente allo scopo di lotta alla criminalità, il DRIPA fosse da considerarsi in contrasto con il diritto dell'UE nella parte in cui consentiva l'accesso ai metadati conservati per obiettivi non circoscritti ai "serious crimes" e nella parte in cui l'accesso non veniva sottoposto ad una "prior review by a Court or an independent administrative authority" (par. 13). Se dunque i criteri riferiti alla fase dell'accesso non ponevano forti dilemmi interpretativi, più problematica appariva invece la disciplina della conservazione. Una prima questione riguardava infatti il requisito stabilito dalla CGUE secondo cui i metadati raccolti dai servizi di telecomunicazione dovevano essere conservati nel solo territorio dell'UE: i giudici inglesi in particolare ritenevano non chiaro se tale requisito fosse da intendersi come assoluto, imponendo dunque l'obbligo di memorizzare dati unicamente entro i confini europei, o se invece fosse da considerarsi come riferibile solo ai metadati ma non alle informazioni prodotte ed elaborate partendo da essi, le quali ben potevano essere conservate in Stati terzi. La prima lettura, secondo l'interpretazione della Court of Appeal, pareva essere in contrasto non solo con la giurisprudenza della CGUE avente ad oggetto la validità delle decisioni di adeguatezza sul trasferimento di dati verso Stati terzi, ma anche con lo stesso art. 25 della Dir. 95/46 che disciplinava proprio la materia del *data trasnfer*. La Court of Appeal, sul punto, concludeva affermando significativamente come "in these circumstances remains considerable uncertainty in relation to this further requirement for which the Respondents and the Interveners contend. It is to be hoped that these uncertainties, which inevitably affect the vital interests of MSs, will be clarified by the CJEU when it considers the reference made by the IPT. However, as matters stand, I do not consider that this Court should make a definitive statement on this issue in the form of a declaration" (par. 19). In presenza di diverse possibili vedute, dunque, i giudici inglesi optavano per una 'non presa di posizione' su tale requisito, limitandosi a rilevare la mancata chiarezza sul punto da parte della giurisprudenza europea; ad una simile conclusione erano giunti inoltre con riferimento all'ulteriore requisito della notifica agli utenti i cui metadati erano stati oggetto di accesso da parte delle autorità di *law enforcement*: innanzitutto tale motivo di invalidità del DRIPA non era stato avanzato nel 2015 da parte dei ricorrenti dinnanzi alla High Court; tale criterio poi non compariva neppure tra i c.d. *Tele2 requirements* inseriti nel dispositivo della sentenza *Tele2*: non risultando pertanto chiara la portata di tale salvaguardia, i giudici inglesi ritenevano appropriato non pronunciarsi su di essa. Sino a questo punto e rispetto ai profili qui indicati, dunque, i giudici nazionali avevano mostrato talvolta di condividere ed applicare i criteri indicati dalla giurisprudenza della CGUE alla disciplina interna (quelli attinenti all'accesso), talaltra di ritenere i requisiti incerti, dubbi o dai contorni ancora troppo indefiniti per poter essere vagliati e attuati nel contesto nazionale (la notifica e la limitazione della conservazione al solo territorio dell'UE).

Quest'ultimo approccio ha inoltre – e ben più problematicamente – caratterizzato anche la delicata materia della conservazione dei metadati. Sul punto il Governo aveva affermato come i par. 111 e 112 della sentenza *Tele2* – che dichiaravano cioè la necessaria sussistenza di un criterio oggettivo capace di istituire un collegamento, anche indiretto, tra i dati da conservare e l'obiettivo perseguito – fossero da riferirsi unicamente alle questioni rinviate dai giudici svedesi e applicabili quindi solo ad una disciplina in materia di conservazione simile a quella disposta dalla normativa svedese. Il *Secretary of State*, sul punto, aveva infatti sostenuto come "This passage of the judgement is based on the Swedish legislation

and that it is not appropriate for this Court to move from the general principle stated by the CJEU to the conclusion that DRIPA suffers from the same vice" (par. 23); secondo il Governo, comunque, la posizione espressa dalla CGUE doveva essere interpretata nel senso che il diritto dell'UE consente a che gli Stati membri adottino regimi di *data retention* generalizzata purché accompagnati da appropriate salvaguardie nella fase dell'accesso, statuendo inoltre con decisione come una forma di conservazione targettizzata fosse da ritenersi del tutto impraticabile[60]. Ebbene sulla correttezza di tale lettura, rispetto alla quale, come noto, i giudici belgi e francesi hanno provveduto ad indirizzare rinvii pregiudiziali alla CGUE, la Court of Appeal decideva, ancora una volta, di non prendere una netta posizione: pur ritenendo condivisibile quanto sostenuto dal Governo, ovvero che le affermazioni dei giudici di Lussemburgo in materia fossero strettamente legate al linguaggio e alle caratteristiche della normativa svedese e delle questioni poste dai relativi giudici, così che tali requisiti non potevano essere suscettibili di una applicazione automatica alla diversa disciplina prevista nel DRIPA, la Court of Appeal riteneva infine che tale questione fosse pendente dinnanzi alla High Court nel caso *Liberty c. Secretary of State*, attinente al vigente IPA[61].

Dalla analisi svolta quindi si può concludere come l'unica conseguenza della trasposizione dei requisiti stabiliti nella sentenza *Tele2* al contesto nazionale sia da rilevarsi nella dichiarazione di incompatibilità della disciplina del DRIPA relativamente alla materia dell'accesso. Per questo "careful analysis of the judgement of the Court of Appeal illustrated that it was actually a pyrrhic victory, as the Court avoided a conclusive answer on crucial issues discussed above, not establishing requirements according to which retained data should remain in the EU or that such data should be destroyed at the end of the retention period, nor a requirement for ex post facto notification, and refused to declare inconsistency of DRIPA with fundamental rights"[62].

Ciò basta tuttavia per comprendere come, diversamente dalla reazione provocata in altri Stati membri, quali il Belgio e la Francia che avevano promosso un ulteriore rinvio alla CGUE vertente proprio sulla disciplina della conservazione, la giurisprudenza europea non avesse portato nel Regno Unito ad una dichiarazione di illegittimità e incompatibilità del regime generalizzato della *data retention* e neppure alla apertura di un nuovo e ulteriore dialogo con i giudici di Lussemburgo: nonostante la Court of Appeal avesse riscontrato l'incertezza della posizione espressa nella sentenza *Tele2* con riferimento tanto alla *data retention* quanto ad altri requisiti come la notifica o la conservazione nel territorio dell'UE, evidenziando peraltro come diverse interpretazioni e letture fossero possibili sul punto – riguardo alla conservazione, la posizione di numerose ONG puntava a ritenere i requisiti stabiliti dalla CGUE come tutti vincolanti, anche quelli sulla targettizzazione della conservazione, indipendentemente dalla successiva disciplina dell'accesso, mentre il Governo puntava a ritenere non illegittimo *per se* il regime di *bulk data retention* – nondimeno i giudici inglesi non erano giunti a promuovere un ulteriore rinvio pregiudiziale. Se certamente i quesiti avanzati dal IPT nel caso *Privacy International* assumevano grande importanza, riguardando l'ambito di applicazione dei *Tele2 requirements*, essi non avrebbero comunque risolto i dubbi e le perplessità interpretative sorte in materia di conservazione generalizzata. I giudici dell'appello avevano tuttavia preferito lasciare che fosse il giudice nazionale, impegnato nel caso *Liberty*, a risolvere la questione.

---

[60] Secondo la parte resistente (i *Respondents*) quindi "the solution to the conundrum is that a general retention regime for communications data infringes the EU Charter unless it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights", par. 26.

[61] "The Court was asked to rule upon the legality of data retention in general – a request that it effectively side stepped. The Court of Appeal took a similar approach, declining to issue a declaration on this point, largely because, as discussed below, the topic was the subject of ongoing debate before the Courts", I. LLOYD, *Data retention*, in *Computer Law & Security Review*, 34, 2018, p. 407.

[62] E. KOSTA, *SSHD v. Watson and Others: a thin nail on the coffin of UK data retention legislation*, in *European Data Protection Law Review*, 4, 2018, p. 524.

3.4. – La **High Court** *nei casi* **Liberty** *del 2018 e 2019: tra convergenze e difformità rispetto alla giurisprudenza della CGUE*

Quest'ultima causa[63] è stata decisa dalla High Court il 27 aprile 2018: la ONG Liberty, come si è anticipato, aveva presentato dinnanzi ai giudici un ricorso volto a determinare la compatibilità della Part 4 dell'IPA con il diritto dell'UE e la Convenzione EDU. Molto similmente a quanto era stato affermato dalla Court of Appeal nel 2018, i giudici della High Court avevano riconosciuto nel IPA e, nello specifico, nella disciplina attinente all'accesso, delle criticità e lacune tali da renderlo incompatibile con quanto stabilito a livello dell'UE nella giurisprudenza della CGUE: in questo caso, il compito della Corte era stato facilitato però dal Governo stesso che, come si è visto, con una comunicazione del 7 luglio 2017, aveva riconosciuto come la Part 4 del IPA fosse "inconsistent with the requirements of EU law in two respects and commenced a process of consultation with a view to making amendments". Così, sulla base di tali condivise e pacifiche considerazioni, la High Court aveva dichiarato l'incompatibilità del IPA nelle parti in cui "(1) access to retained data is not limited to the purpose of combating "serious crime"; and (2) access to retained data is not subject to prior review by a court or an independent administrative body"[64].

Diversamente però da quanto era stato deciso dalla stessa High Court nel 2015 con riferimento al DRIPA, questa volta i giudici non hanno ritenuto opportuno imporre una disapplicazione della normativa: riconoscendo che il caso in esame rappresentava un "very important constitutional case", nel quale "vital public interests are at stake on each side of the argument", una mera disapplicazione avrebbe potuto tradursi in una situazione di caos, a danno del pubblico interesse alla sicurezza (par. 46). Sulla base di tali considerazioni, quindi, la High Court ha concluso che "the legislation must be amended within a reasonable time and that a reasonable time would be 1 November 2018, which is just over 6 months from the date of this judgment. We have also concluded that the appropriate remedy is a declaration to reflect our judgment" (par. 100)[65]. Così facendo, questa decisione ha rappresentato un motore propulsivo per velocizzare quel processo di modifica del IPA che era già stato in precedenza promosso dal Governo e che ha portato alla adozione del *Data Retention and acquisition regulations 2018*.

Tuttavia, sebbene le posizioni e le considerazioni sino ad ora esaminate paiano in linea con la giurisprudenza della CGUE, ciò che, ancora una volta, rappresenta il punto maggiormente delicato e problematico rispetto al quale l'approccio dei giudici inglesi è di maggiore resistenza rispetto a quanto affermato dai giudici di Lussemburgo, è la disciplina della conservazione dei metadati. In maniera del tutto simile a quanto già espresso dalle previe pronunce esaminate della High Court e della Court of Appeal, infatti, anche in questo caso è stato ribadito come i principi e requisiti stabiliti nelle sentenze *DRI* e *Tele2* fossero da considerarsi riferiti principalmente alla normativa svedese. Quest'ultima, diversamente da quella inglese, prevedeva un obbligo generalizzato di conservazione dei metadati, secondo quanto già disposto dalla DRD. Il IPA quindi, a parere dei giudici, si differenziava

[63] [2018]EWHC 975 (Admin).

[64] Innanzitutto quindi la Corte ha riconosciuto come le finalità che consentono l'accesso, previste alla Section 61, co. 7 (public health, tax matters, regulation of financial services/markets and financial stability), non siano compatibili con il diritto dell'UE poiché eccedono la finalità individuata a livello sovranazionale nella lotta alla criminalità grave. Merita precisare come, già all'epoca del processo, il Governo avesse affermato che la proposta già avviata di modifica del IPA prevedesse di rimuovere i problematici ulteriori scopi dalla normativa (par. 103).

[65] I numerosi rimandi alla sentenza della Court of Appeal relativa al DRIPA, del 30 gennaio 2018, sono indicativi di come le considerazioni svolte relativamente alla previa normativa potessero essere validamente applicate anche con riferimento al IPA: "the judgement of the Court of Appeal is still a significant one declaring DRIPA incompatible with EU law, especially as Part 4 of IPA in essence contains relevant and similar provisions on data retention and the Court's findings will be crucial in the assessment of these provisions", E. KOSTA, *SSHD v. Watson and Others*, op. cit., p. 407.

significativamente dalla disciplina svedese considerata incompatibile con il diritto dell'UE: "the IPA does not contain a blanket requirement requiring the general retention of communications data. The Act does not itself impose any requirement on telecommunications operators to retain data. Instead, the Secretary of State is given a power to require retention of data by serving a notice to an operator" (par. 127), potere che può essere esercitato solo laddove considerato proporzionato e necessario al raggiungimento di uno degli scopi espressamente previsti dalla legge. La determinazione di precisi elementi che il *Secretary of State* era chiamato a considerare e valutare prima di emanare il 'retention notice' (Section 88), unitamente alla previsione di un controllo preventivo operato dal *Judicial Commissioner*, sono state considerate tutele idonee e sufficienti a far ritenere il regime di conservazione disposto dal IPA compatibile con il diritto dell'UE e con i criteri delineati dalla CGUE e a scongiurare i rischi di una conservazione generalizzata. Infatti, secondo i giudici inglesi, "In the light of this analysis of the structure and content of Part 4 of the IPA we do not think it could possibly be said that the legislation requires, or even permits, a general and indiscriminate retention of communications data. The legislation requires a range of factors to be taken into account and imposes controls to ensure that a decision to serve a retention notice satisfies the tests of necessity in relation to one of the statutory purposes, proportionality and public law principles" (par. 135). A nulla è valsa la posizione espressa dai ricorrenti, che hanno chiarito come il 'retention notice' del *Secretary of State*, benché condizionato a specifiche valutazioni e controlli, possa comunque assumere un carattere generalizzato e riguardare cioè tutti i metadati, tutti gli utenti e tutti i fornitori di servizi di telecomunicazione: le garanzie predisposte dal IPA, infatti, non permettono di eliminare ed escludere qualsiasi possibilità di adozione di una forma di *bulk data retention*.

Quanto poi ai requisiti della notifica e della conservazione dei dati nel territorio dell'UE, similmente alla sentenza della Court of Appeal, i giudici hanno deciso di non prendere su di essi posizione, ritenendo che simili questioni siano state già poste mediante rinvio pregiudiziale alla CGUE da parte del IPT nel caso *Privacy International* e che sia necessario dunque attendere tale pronuncia per veder chiariti questi controversi aspetti.

In conclusione, è possibile rilevare come, sebbene vengano riconosciute alcune criticità nella normativa IPA rispetto alle quali il legislatore avrebbe dovuto dunque intervenire, di fatto la sentenza analizzata si pone in linea di continuità e in coerenza rispetto alla precedente decisione della Court of Appeal relativa al DRIPA: le lacune e le incompatibilità individuate nelle due normative infatti sono identiche ed attinenti alla disciplina dell'accesso, mentre nessuna dichiarazione o presa di posizione viene svolta con riferimento agli ulteriori e diversi requisiti emersi dalla giurisprudenza della CGUE relativamente a notifica e limitazione territoriale della conservazione. Aspetto di grande rilievo che emerge da questa sentenza è senza dubbio quello riguardante la disciplina della conservazione dei metadati, rispetto alla quale i giudici affermano con decisione la compatibilità del regime disposto nel IPA con i requisiti indicati nelle sentenze *DRI* e *Tele2*. Nonostante il regime di *data retention* dei metadati del Regno Unito abbia caratteristiche differenti rispetto a quelle proprie della normativa svedese, belga e italiana, che prevedono un obbligo diretto ed automatico in capo ai fornitori di servizi di telecomunicazione, merita di essere rilevato come anche nella disciplina inglese non sia possibile riscontrare la presenza di quei criteri oggettivi che permettono di creare una connessione, anche indiretta, tra conservazione e atti di criminalità grave, né quelle restrizioni sulla base di criteri geografici o soggettivi indicati dai giudici di Lussemburgo[66]. Se la portata e l'ampiezza della posizione espressa su

[66] Altro punto dibattuto e che potrebbe conoscere, in futuro, ulteriori interventi da parte dei giudici o del legislatore nazionale, attiene alla determinazione della natura dei c.d. *entity data*, definiti come "data about a person or thing or about associations between such entities" (par. 145): secondo Liberty, infatti, rispetto a tali dati identificativi dell'utente non risultava chiaro, né dalla normativa interna né dalla giurisprudenza inglese ed europea, se essi dovessero essere considerati rientranti nella definizione di *communications data* e dunque sottoposti anch'essi ai requisiti indicati dalla giurisprudenza della CGUE; vista la rilevanza della questione, la ricorrente riteneva opportuno un rinvio pregiudiziale ai giudici di Lussemburgo, volto all'ottenimento di un chiarimento in materia.

tale delicato punto dalla CGUE in *Tele2* è ancora oggi oggetto di discussione, come emerso dai rinvii pregiudiziali pendenti promossi da Belgio e Francia, volti proprio ad ottenere chiarimenti rispetto alla disciplina della *data retention* e al carattere cumulativo dei requisiti indicati nelle pronunce europee, è da sottolineare come i giudici inglesi non si siano posti le medesime questioni ed interrogativi che hanno spinto invece gli omologhi di altri Stati membri a richiedere un ulteriore intervento della CGUE. Così si può condividere la posizione secondo cui "The first phase of Liberty's challenge to the IPA may have been successful – however, the real practical impact of this case remains to be seen"[67]: le modifiche apportate alla normative IPA nel 2018, come si è visto, sono state positivamente indirizzate nella direzione di rafforzare le tutele secondo le indicazioni fornite sia dalla High Court che dalla CGUE. Le possibilità di provvedere ad una conservazione generalizzata, però, sebbene limitata da vari criteri che il *Secretary of State* e il *Judicial Commissioner* sono chiamati a considerare, pare destinata a permanere e non è neppure stata smentita in una più recente decisione della High Court che si è occupata, sempre su ricorso della ONG Liberty, di valutare la compatibilità del IPA rispetto, non al diritto dell'UE, bensì al *Human Rights Act* (HRA) del 1998 – atto con cui il Regno Unito ha recepito e riconosciuto come fonte del proprio ordinamento la Convenzione EDU[68]. Il 29 luglio 2019[69] i giudici hanno rilevato, svolgendo considerazioni del tutto simili a quelle già evidenziate nelle sentenze sin ad ora analizzate, la compatibilità del IPA agli artt. 8 e 10 della Convenzione EDU, ritenendo che la disciplina predisposta dal legislatore inglese comporti una ingerenza nei diritti alla vita privata e alla libertà di espressione proporzionata e necessaria in una società democratica, predisponendo salvaguardie sufficienti a prevenire il rischio di abusi e interferenze arbitrarie da parte dei pubblici poteri. Le innovazioni introdotte dal IPA e dalle modifiche del 2018 (il sistema di 'double-lock' ad esempio) hanno portato la High Court a ritenere peraltro non applicabili a tale disamina le considerazioni critiche svolte dalla Corte

---

La High Court, invece, aveva considerato chiaro ed indiscusso come tale tipologia di dati non potesse essere ricondotta né alla normativa interna né alla Direttiva *e-Privacy*, nelle quali si faceva riferimento unicamente ai *traffic* e *location data*. Ne derivava che "The definition of event data under the 2016 Act embraces both location data and traffic data in the *e-Privacy Directive* and so entity data under 2016 Act does not fall within the scope of Par. 2 of the dispositive in Tele2", par. 154. La posizione espressa dai giudici nazionali, tuttavia, potrebbe ora essere messa in discussione alla luce di quanto affermato dalla CGUE nella sentenza *Ministerio Fiscal* – e già richiamato anche nel Capitolo IV, Parte II – che aveva ad oggetto proprio dati riguardanti l'identità di titolari di una utenza telefonica: i giudici di Lussemburgo hanno stabilito in proposito come "dal considerando 15 della Direttiva 2002/58 risulta che i dati relativi al traffico possono comprendere, in particolare, il nome e l'indirizzo della persona che emette una comunicazione o che utilizza un collegamento al fine di effettuare una comunicazione. I dati relativi all'identità civile dei titolari delle carte SIM possono, inoltre, rivelarsi necessari per la fatturazione dei servizi di comunicazione elettronica forniti e fanno pertanto parte dei dati relativi al traffico, come definiti nell'articolo 2, secondo comma, lettera b), di tale Direttiva. Questi dati rientrano quindi nell'ambito di applicazione della Direttiva 2002/58" (par. 42). Questa posizione quindi pare in contrasto con la più restrittiva determinazione dell'ambito di applicazione della Direttiva *e-Privacy* e dunque dei dati sottoponibili ai requisiti *Tele2* svolta dalla High Court. Sul punto si legga L. WOODS, *Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers*, in *EU Law Analysis*, 4 ottobre 2018, http://eulawanalysis.blogspot.com/2018/10/mobile-phone-theft-and-eu-eprivacy-law.html.

[67] C. GILMARTIN, *Privacy Rights: how should a Court remedy legislative incompatibility with EU law?*, in *UK Human Rights Blog*, 8 maggio 2018.

[68] La Section 6 del HRA stabilisce come sia da considerarsi "unlawful for a public authority to act in a way which is incompatible with a Convention right". Merita ricordare come "when primary legislation cannot be read and given effect in a way which is compatible with the Convention rights, section 4 of the HRA becomes relevant. Section 4 provides that if a relevant court determines that the legislation is incompatible with a Convention right, then it may make a declaration that it is incompatible. This determination doesn't affect the validity or continuing operation of the legislation not is it binding on the parties to the case in which the determination is made, but rather, it enables the Minister of the Crown to make a remedial order, which enables the government to amend the legislation as required", I. TRUMMER, *Liberty v. SSHD & SSFCA: you have the right to remain silent; anything you say will be gathered and retained by the* Government, in *Tulane Journal of International and Comparative Law*, 28, 2020, p. 388.

[69] *Liberty v. Secretary of State for Home Department and Secretary of State for Foreign and Commonwealth Affairs* [2019] EWHC 2057.

EDU nella controversia *Big Brother Watch* – per la cui analisi dettagliata si rimanda al Capitolo V, Parte II – che erano riferite invece alla previa normativa RIPA. Come si ricorderà, anche nella sentenza dei giudici di Strasburgo, che avevano condannato per violazione dell'art. 8 della Convenzione EDU il Regno Unito con riferimento alla normativa adottata in materia di *data retention*, accesso e *data sharing* per finalità di sicurezza nazionale, era emerso come, a seguito di un esame più approfondito, la decisione finale dei giudici europei fosse caratterizzata non solo da luci – a favore della tutela dei diritti fondamentali – ma anche da ombre. Ad una simile considerazione si può giungere rispetto alla posizione espressa dai giudici inglesi a seguito dell'adozione del IPA. Da un lato, infatti, sono state riconosciute lacune e carenze significative, meritevoli di modifica normativa, dall'altro però è stata accettata la legittimità e conformità al diritto dell'UE e alla Convenzione EDU di un regime di conservazione potenzialmente generalizzato, anche mediante una lettura piuttosto limitativa della portata della giurisprudenza dell'UE. Senza dubbio la posizione che entrambi i giudici europei esprimeranno nei rinvii pendenti – *Privacy International* dinnanzi alla CGUE e *Big Brother Watch* dinnanzi alla Grande Camera della Corte EDU – sarà determinante per comprendere se e in quale misura i requisiti più rigidi fissati dalla giurisprudenza della CGUE verranno confermati, anche con riferimento agli strumenti volti alla tutela della sicurezza nazionale, e se il più recente orientamento della Corte EDU verrà ribaltato dalla Grande Camera, ristabilendo quei requisiti e criteri in grado di limitare fortemente la legittimità di misure di sorveglianza – conservazione e accesso – generalizzata.

4. – Un percorso di luci e ombre: l'approccio del Regno Unito tra spinte contrastanti

L'analisi della evoluzione normativa e giurisprudenziale, sopra svolta, porta a muovere alcune considerazioni sull'approccio del Regno Unito in materia di *data retention* e accesso ai metadati: non si può infatti non porre in evidenza come il percorso seguito, costellato da molteplici interventi legislativi e sentenze delle Corti nazionali, unitamente agli sviluppi della giurisprudenza europea, abbia condotto ad una maggiore consapevolezza dei rischi legati all'impiego di tali strumenti di indagine e, dunque, della necessità di stabilire idonee salvaguardie e tutele, tanto nella fase di conservazione quanto in quella di accesso. Sebbene il legislatore inglese non sia giunto alla rinuncia di una forma di *retention* generalizzata, ha cercato nondimeno nel corso del tempo di far proprie ed inserire nell'ordinamento nazionale talune di quelle restrizioni e limitazioni che sono state con forza affermate dai giudici di Lussemburgo.

Quantomeno inizialmente, la tendenza ad interventi normativi di 'adeguamento' e modifica della disciplina interna, peraltro rapidi e poco coordinati – nella sostanza e nella scelta temporale – con la giurisprudenza nazionale e soprattutto sovranazionale, pareva motivata più dal timore di perdere la possibilità di utilizzare i metadati conservati come strumenti importanti per la garanzia della sicurezza e come prove fondamentali all'interno dei procedimenti penali, piuttosto che da una reale e sentita volontà di innalzare il livello di tutela dei diritti fondamentali e addivenire ad un più corretto bilanciamento con le esigenze securitarie. Una volontà, quest'ultima, che sembra invece essere maggiormente sottesa alle più recenti modifiche legislative, in particolare quella del 2018, frutto di una più seria riflessione del legislatore, spinto anche dalle critiche e dalle analisi mosse dalla dottrina nonché dall'attenzione manifestata dalla società civile, oltre che da una posizione espressa dalle Corti nazionali in taluni punti maggiormente convergente a quella della CGUE.

La giurisprudenza nazionale è stata essa stessa, infatti, testimone di un percorso evolutivo di lento, seppur non totale, avvicinamento alla giurisprudenza sovranazionale: da un lato, anche a seguito della sentenza *Tele2*, i giudici inglesi hanno mostrato una certa distanza rispetto alle considerazioni svolte dalla CGUE, soprattutto con riferimento alla disciplina della conservazione, proponendo un rinvio pregiudiziale finalizzato a chiarire i confini di applicazione dei c.d. *Tele2 requirements* e ad escludere

dalle salvaguardie da essi delineate l'area delicata e fondamentale della sicurezza nazionale e delle attività poste in essere dalle agenzie di intelligence. Nonostante questo approccio, tuttavia, i giudici inglesi hanno, in particolar modo negli ultimi anni, dimostrato di saper prendere anche decisioni significative e dagli effetti considerevoli: dichiarando l'incompatibilità della disciplina nazionale rispetto al diritto dell'UE, pur con riferimento solamente a taluni aspetti attinenti alla fase dell'accesso, le Corti hanno seguito ed applicato al regime interno il ragionamento sviluppato dai giudici di Lussemburgo, imponendo così anche al legislatore di ripensare alla normativa adottata.

Tutte le tappe che, da una iniziale difficoltà o ritrosia – che pure permane sotto taluni profili –, hanno portato ad una maggiore sensibilità ed adeguamento, sia della normativa che della giurisprudenza nazionale, ai principi fissati a livello europeo, ricostruiscono un quadro articolato e complesso, nel quale non sempre il legislatore ha saputo cogliere al momento giusto la portata delle decisioni tanto delle Corti europee quanto di quelle interne. I più recenti sviluppi – per quanto ancora lontani da una forma di conservazione targettizzata promossa dalla CGUE come strumento compatibile al diritto dell'UE e alla Carta di Nizza nonché ancora privi di alcune di quelle salvaguardie attinenti alla fase dell'accesso[70] e della sicurezza dei metadati indicate dai giudici di Lussemburgo – hanno registrato una più decisa svolta verso l'attuazione dei principi di proporzionalità e necessità, pur assegnati ancora alla discrezionalità di membri del potere esecutivo e del Governo – quali il *Secretary of State* –. Un percorso quindi che, sotto tale profilo, deve essere letto positivamente, soprattutto se paragonato a Stati membri, quali l'Italia, nei quali – come si vedrà – non si è ancora registrata una riflessione profonda sull'esigenza di adeguare la normativa nazionale a quanto emerso dalla giurisprudenza della CGUE.

Certo, nonostante questi positivi sviluppi e queste luci, non possono però essere ignorate le numerose ombre che ad oggi ancora permangono: altri Stati membri sono stati in grado di dimostrare, ben prima del Regno Unito, una maggiore attenzione e volontà di incorporare nel proprio ordinamento i principi dettati, in particolare, dalle sentenze *DRI* e *Tele2*, giungendo ad un assetto normativo, soprattutto in materia di accesso ai metadati, più garantista rispetto a quello inglese.

Il profilo dell'approccio delle Corti nazionali al tema della conservazione dei metadati resta comunque l'aspetto maggiormente problematico ancora aperto: mentre la Court of Appeal nel 2018, anche a seguito della pronuncia *Tele2*, aveva deciso di non prendere posizione quanto alla legittimità di una forma di conservazione generalizzata, ritenendo comunque come quanto in merito affermato dai giudici di Lussemburgo fosse riferibile essenzialmente alla disciplina svedese, nelle più recenti sentenze della High Court è stata affermata la compatibilità della disciplina in materia di *data retention* disposta dal IPA con il diritto dell'UE e con la Convenzione EDU, seguendo un approccio discutibile e in parte viziato: accanto alle innegabili maggiori tutele previste dalla normativa in vigore, i giudici inglesi hanno mancato di notare la lontananza che continua a persistere rispetto a quei criteri oggettivi e di targettizzazione promossi dalla giurisprudenza della CGUE. Il ragionamento seguito dalla High Court, fondato essenzialmente sulla considerazione della distanza e della differenziazione tra la disciplina inglese e quella svedese valutata dai giudici di Lussemburgo nella pronuncia *Tele2*, ha attirato forti critiche e ha portato a ridimensionare fortemente quella che poteva, a primo impatto, sembrare invece

[70] È da rilevarsi, inoltre, un ulteriore profilo problematico e di complessità: nonostante, infatti, talune delle salvaguardie e garanzie indicate dalla giurisprudenza della CGUE o della Corte EDU siano state inserite nella normativa inglese, non tutte riescono poi a risultare efficaci nella pratica applicativa concreta. Basti pensare al rimedio giurisdizionale rappresentato dalla possibilità di ricorso avverso l'IPT: "this extensive jurisdiction has received 2140 complaints from its inception (since 2000) to 2015 and it was only in February 2015 that the IPT found its first finding against the Government. From 2000 to 2015 there has been total of 16 successful complaints out of 2140, making a success rate of around 0.9%" (M. WHITE, *Protection by judicial oversight or an oversight in protection?*, op. cit.). Questi interessanti dati aiutano a comprendere come una analisi completa della disciplina della *data retention*, dell'accesso e dei rimedi previsti debba spingersi a considerarne non solo la previsione normativa ma anche l'efficacia e l'applicazione concreta.

una vittoria per i sostenitori dei diritti fondamentali[71]. Un approccio giurisprudenziale poi che ha voluto ottenere una delimitazione e specificazione dell'ambito di applicazione di quanto affermato a livello sovranazionale, come emerge dal rinvio pregiudiziale *Privacy International* e dalla richiesta, in esso contenuta, di chiarire se i *Tele2 requirements* siano applicabili anche alle agenzie di intelligence: così facendo i giudici hanno mostrato di voler "opporre una sorta di resistenza statuale che mira ad ampliare i margini di discrezionalità possibili nelle operazioni di raccolta, conservazione ed analisi dei dati relativi alle comunicazioni elettroniche"[72] in materie così fondamentali e delicate quali la sicurezza nazionale e rispetto alla quale il Regno Unito vuole mantenere un saldo ed esclusivo controllo. Da ciò affiora, forse con maggiore evidenza, quella esigenza di definire chiari confini tra competenze e 'aree di azione' dell'UE e degli Stati membri così fortemente sentita Oltremanica, che vede nella scelta di uscire dall'Unione europea e nel percorso di c.d. Brexit la sua più evidente concretizzazione.

5. – Una sfida sullo sfondo: la Brexit e le conseguenze in materia di protezione e trasferimento dei dati

5.1. – La necessità di mantenere un costante flusso di dati tra UE e Regno Unito: timori, dubbi e perplessità quanto alla adeguatezza e sostanziale equivalenza del livello di protezione dei dati garantito Oltremanica

Un ulteriore aspetto e conclusivo che merita di essere debitamente considerato per la sua rilevanza, la sua particolarità ed unicità, così come per il suo impatto anche sullo sviluppo della disciplina della *data retention* nell'ordinamento inglese, è il processo di c.d. Brexit. Come noto, infatti, a seguito di referendum del 23 giugno 2016, il Regno Unito ha notificato in data 29 marzo 2017 la propria decisione di recedere dall'Unione europea e dalla Comunità europea dell'energia atomica, sulla base della facoltà garantita dall'articolo 50 TUE. A seguito di intenso dibattito, sia in seno all'UE che Oltremanica, che ha portato a complesse negoziazioni, continui rinvii e battute d'arresto in un percorso senza precedenti nella storia dell'UE, le modalità di recesso sono state definite all'interno dell'"Accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica", del 31 gennaio 2020 (L 29/7, conosciuto anche come "Withdrawal Agreement" o "Accordo di recesso").

Pur non essendo ovviamente questa la sede per studiare approfonditamente l'evoluzione delle trattative[73] e il contenuto del conclusivo Accordo di recesso, risulta imprescindibile comprendere le disposizioni previste in tale documento finale in materia di protezione dei dati, per poter così riflettere su quali saranno le conseguenze, gli scenari futuri e le successive misure che dovranno essere adottate nell'ambito della tutela della riservatezza. Ciò permetterà inoltre di capire come – e se – gli interventi legislativi e giurisprudenziali sino ad ora analizzati in materia di *data retention*, succedutisi negli ultimi

[71] Molti commenti alle più recenti pronunce della High Court hanno segnalato proprio la mancata considerazione, da parte dei giudici e, ancor prima, del legislatore, di molti degli requisiti delineati dalla giurisprudenza europea in materia di conservazione dei metadati: "Part 4 of the IPA 2016 is neither consistent with the ECHR or EU law. The High Court have fallen into the same trap as the Court of Appeal did earlier this year when distinguishing a catch all power, and a power that can catch all", M. WHITE, *Data Retention incompatible with EU law: Victory? Victory you say?*, in *EU Law Analysis*, 24 maggio 2018; similmente Trummer ha sottolineato come "the Court followed precedent, but throughout its analysis, it erred on the side of caution and decided the case with the threat of terrorist attack, hostile actors and national security weighing heavily on its mind. The lack of focus on the fundamental rights at risk of being encroached upon resulted in a balancing test that simply lacked balance", I. TRUMMER, *Liberty v. SSHD & SSFCA*, op. cit., p. 396.

[72] L. SCAFFARDI, *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016*, op. cit., p. 415.

[73] Sul punto si rimanda, *ex multis*, a F. SAVASTANO, *Uscire dall'UE. Brexit e il diritto di recedere dai Trattati*, Giappichelli, 2019.

decenni anche e soprattutto come reazione alle decisioni della CGUE e alla disciplina normativa europea, potranno subire mutamenti a seguito della Brexit.

Innanzitutto merita specificare come all'art. 127 dell'Accordo di recesso venga indicato un periodo di transizione che terminerà il 31 dicembre 2020, durante il quale il diritto dell'Unione verrà applicato al e nel Regno Unito. Tale precisazione risulta di fondamentale importanza per l'analisi dell'art. 71, dedicato specificamente alla disciplina della protezione dei dati personali, secondo il quale viene stabilito che "1. Il diritto dell'Unione in materia di protezione dei dati personali si applica nel Regno Unito al trattamento dei dati personali degli interessati al di fuori del Regno Unito, purché tali dati personali: a) siano stati trattati nel Regno Unito ai sensi del diritto dell'Unione prima della fine del periodo di transizione; o b) siano trattati nel Regno Unito dopo la fine del periodo di transizione in virtù del presente accordo. Il paragrafo 1 non si applica al trattamento dei dati personali di cui al medesimo paragrafo, che sia oggetto di un livello di protezione adeguato quale stabilito con decisioni applicabili ai sensi dell'articolo 45, paragrafo 3, del regolamento (UE) 2016/679 o dell'articolo 36, paragrafo 3, della Direttiva (UE) 2016/680. Qualora una decisione di cui al paragrafo 2 abbia cessato di essere applicabile, il Regno Unito garantisce un livello di protezione dei dati personali sostanzialmente equivalente a quello previsto dal diritto dell'Unione in materia di protezione dei dati personali per quanto riguarda il trattamento dei dati personali degli interessati di cui al paragrafo 1".

Ne deriva, quindi, una distinzione a seconda che il trattamento avvenga durante o successivamente al periodo di transizione, così che mentre sino al 31 dicembre 2020 verrà applicato il diritto dell'UE, a partire dal 1 gennaio 2021 troverà attuazione il diritto interno inglese, determinando peraltro un rilevante passaggio: il Regno Unito verrà in quella data ad assumere, sotto il profilo della disciplina della protezione dei dati, la qualifica di "Stato terzo", comportando un cambiamento dalle enormi conseguenze. Secondo quanto ampiamente esaminato nel Capitolo III, Parte II, infatti, il GDPR regola dettagliatamente al Capo V e, in particolare, all'art. 45, la materia del trasferimento dati verso Stati terzi, incorporando peraltro i principi e l'interpretazione forniti mediante l'intervento deciso e decisivo della CGUE a partire dalla c.d. saga *Schrems*. Viene in particolare richiesto, al fine di derogare alla regola generale di divieto di trasferimento dati oltre i confini dell'UE, che lo Stato extra-UE ricevente – dunque destinatario di dati provenienti dell'UE – sia in grado di garantire un livello di protezione adeguato, intendendo per adeguatezza una 'sostanziale equivalenza' rispetto allo *standard* assicurato nel territorio dell'UE. Tale livello di protezione dovrà essere valutato dalla Commissione europea, mediante lo strumento della decisione di adeguatezza, che ha una valenza generale – riguardando tutte le operazioni di trasferimento – ed agevola dunque le operazioni di *data transfer*, pur essendo previsti, in assenza di tale decisione, strumenti alternativi che i singoli operatori possono adottare allo scopo di essere autorizzati al trasferimento (si pensi alle clausole contrattuali tipo o *Standard Contractual Clauses*). Le decisioni di adeguatezza inoltre, lo si vuole ricordare, possono assumere carattere parziale cioè vertere su di uno specifico settore o su determinate categorie di dati (come nel caso dei PNR) oppure valere per una categoria particolare di soggetti (imprese, ad esempio): in questo caso la valutazione circa l'adeguatezza può essere fondata sulle condizioni ed i requisiti fissati da specifici accordi internazionali bilaterali, riguardanti appunto la precisa tipologia di dati da trasmettere o i soggetti coinvolti, come avvenuto nel caso degli USA, rispetto ai quali sono stati adottati i noti accordi *Safe Harbour* e *Privacy Shield*, sulla base dei quali la decisione della Commissione si è fondata.

Se il Regno Unito e l'UE vorranno continuare a mantenere un flusso costante di dati, l'unica strada che possa garantire tale risultato in maniera generalizzata e al di là delle iniziative dei singoli, è rappresentata pertanto dall'ottenimento di una decisione di adeguatezza. Ne risulta che, preferibilmente entro la fine del periodo di transizione, la Commissione sarà chiamata a svolgere una analisi della disciplina vigente nel Regno Unito in materia di protezione dei dati e tutela della privacy, allo scopo di stabilire il livello di protezione garantito e determinare la possibilità di addivenire ad una decisione di adeguatezza o ad un accordo, similmente a quanto avvenuto già con gli Stati Uniti, volto a fissare le

condizioni e le tutele che dovranno essere assicurate ai dati provenienti dall'UE per garantire la sostanziale equivalenza della disciplina interna a quella propria del territorio europeo.

Come le complesse e travagliate vicende caratterizzanti il trasferimento dei dati Oltreoceano hanno insegnato, tale procedimento di negoziazione e valutazione dell'adeguatezza risulta tutt'altro che semplice e rapido, anche considerando l'estrema delicatezza della materia dovuta sia all'impatto sui diritti fondamentali sia all'ingente rilevanza economica delle operazioni di *data transfer*. Sotto quest'ultimo profilo, un blocco del trasferimento di dati comporterebbe gravi problematiche[74] alle aziende che operano nel Regno Unito e le complicazioni derivanti dall'assenza di una decisione di adeguatezza generalizzata imporrebbero ai singoli operatori di attrezzarsi con i più complessi ed onerosi – anche in termini di tempo e di procedura – strumenti alternativi previsti nel GDPR. Alla luce di queste considerazioni, unitamente alla negativa esperienza delle lunghe trattative con gli USA, la dottrina[75] nonché i fornitori di servizi di telecomunicazione o aziende con diverse sedi in UE e nel Regno Unito – per le quali dunque le operazioni di *data transfer* sono quotidiane e fondamentali – hanno espresso, sin dall'inizio del percorso di Brexit, grande preoccupazione per l'impatto del recesso dall'UE sul flusso di dati, sottolineando con forza gli effetti disastrosi che l'assenza di accordo e di decisione di adeguatezza potrebbero comportare. La situazione di incertezza che ha caratterizzato il percorso di recesso dall'UE nel suo complesso e le complicazioni che hanno accompagnato le negoziazioni hanno acuito il timore che la tematica del trasferimento dei dati potesse passare in secondo piano nel dibattito politico-istituzionale o procedere ad un passo troppo lento. Da ciò sono derivati svariati appelli a che la disciplina della protezione dei dati e del loro flusso rimanesse centrale nel dialogo tra Regno Unito e UE, in modo da poter addivenire ad una soluzione capace di bilanciare l'esigenza di una garanzia elevata dei diritti

[74] "The United Kingdom is home to a vibrant technology sector, the innovations of which underpin many of the industries, products, and services that drive the European economy. Other industries in the UK, from the banking and financial sector to headquarters of global multinational companies, also depend on flows of data across national borders. The implications of the UK's withdrawal from the European Union are profoundly uncertain, and this uncertainty is particularly pronounced in the technology sector because of European regulation of data privacy and the flow of personal information", K. WIMMER, J. JONES, *Brexit and implications for privacy*, in *Fordham International Law Journal*, 5, 2017. Anche AFME (*Association for Financial Markets in Europe*), si era interrogata, sin dal 2018, sui possibili effetti della Brexit e sulle sue implicazioni rispetto al trasferimento di dati personali come parte della attività ed operazioni necessarie al funzionamento del mercato finanziario. Nel suo studio "Effective flow of personal data post-Brexit. Implications for capital markets", AFME ha sottolineato come "the departure of the UK from the EU creates significant uncertainty as to the ability of businesses, including banks and investment firms, to continue to transfer personal data between EU and the UK post-Brexit". Anche Vanberg e Maunick hanno riportato dati interessanti, che aiutano a comprendere le proporzioni del danno economico che l'assenza di accordi in materia di protezione dei dati e dunque la mancata continuità nel flusso di dati potrebbero comportare per il Regno Unito: "The digital sector contributed 118£ billion to the UK economy and employed over 1.4 million people across the UK in 2015. This demonstrates that without an effective data protection network which allows data exchages with the EU, the UK is likely to suffer significant financial losses. As held by the Parliamentary Under-Secretary of State Lord Ashton of Hyde 'some 43% of EU tech companies are based in the UK and 75% of the UK's data transfers are with EU member states'. This shows the importance of having a smooth data transfer between the EU and the UK", A. D. VANBERG, M. MAUNICK, *Data protection in the UK post-Brexit: the only certainty is uncertainty*, in *International Review of Law, Computers and Technology*, 1, 2018, p. 192. Sul punto si legga anche K. MACASKILL, *Brexit: potential trade and data implications for digital and fintech industries*, in *International Data Privacy Law*, 1, 2017.

[75] Si pensi a P. DE HERT, V. PAPAKONSTANTINOU, *The UK contribution to the field of EU data protection: let's not go for 'third country' status after Brexit*, in *Computer Law and Security Review*, 33, 2017. Gli autori, sin dal 2017, avevano ribadito come "data protection, although one out of the myriad legal aspects pertaining to Brexit that urgently await consideration, may prove to be a crucial issue in this process. (..) Whichever the outcome of a possible Brexit in the data protection field, it is expected to affect in many ways not only formal EU and UK data protection but also business practices as well as the everyday lives of individuals. A number of important internet companies, that offer both B2B and B2C services throughout Europe, reside in the UK. The same is true for the financial sector as well.", p. 354. Esprimendo tali preoccupazioni, gli autori auspicavano che il tema della protezione dei dati assumesse un rilievo centrale nel dibattito e nelle negoziazioni tra UE e Regno Unito.

fondamentali con il bisogno di un quadro regolatorio chiaro, capace di favorire l'attività di molti operatori privati nonché di autorità pubbliche per le quali il flusso di dati è essenziale.

In questo contesto, in cui si è cercato di tenere alta l'attenzione su questo delicato fronte, non stupisce quindi che una effettiva rilevanza sia stata riconosciuta alla disciplina del trasferimento di dati sia dall'UE che dal Regno Unito, pur nella complessità e difficoltà di trovare una soluzione percorribile in tempi ristretti. Così nella Decisione del Consiglio, del 25 febbraio 2020, "authorising the opening of negotiations with the UK for a new partnership agreement", viene dato risalto alla tematica: "In view of the importance of data flows, the envisaged partnership should affirm the Parties' commitment to ensuring a high level of personal data protection, and fully respect the Union's personal data protection rules, including the Union's decision-making process as regards adequacy decisions. The adoption by the Union of adequacy decisions, if the applicable conditions are met, should be a factor for fostering cooperation and exchange of information. It is also a condition, where necessary, to achieve the high level of ambition on law enforcement and judicial cooperation in criminal matters"[76]. Stessa attenzione emerge anche, più recentemente, dalle parole della Commissione: nella comunicazione del 6 luglio 2020 – a integrazione della previa comunicazione del 9 gennaio 2018 –, titolata "Withdrawal of the UK and EU rules in the field of data protection" e indirizzata a tutti gli *stakeholders* e i soggetti interessati, viene ribadito come "during the transition period, the EU and the UK will negotiate an agreement on a new partnership, providing notably for a free trade area"; l'intenzione dunque di addivenire ad un accordo è forte e l'importanza di raggiungere una decisione di adeguatezza è ampiamente riconosciuta. La Commissione però, significativamente, procede affermando: "However, it is not certain whether such an agreement will be concluded and will enter into force at the end of the transition period. (..) It is also clear that after the end of the transition period, any transfer of personal data to the UK other than that governed by Art. 71 (1) of the Withdrawal Agreement will not be treated as sharing of data within the Union"[77]. Viene quindi parimenti preso atto della difficoltà e della molteplicità di elementi da considerare al fine di raggiungere un accordo in materia: vengono così avvisati tutti coloro che si troveranno a dover affrontare operazioni di trasferimento dati Oltremanica circa l'esistenza degli strumenti alternativi previsti nel GDPR ed elencati nelle loro caratteristiche principali; quasi a 'mettere in guardia' quanto alle misure che dovranno essere adottate a partire dal 2021 in caso non si riesca a concludere entro la fine del periodo di transizione il percorso di negoziazione di un accordo ed ottenere una decisione di adeguatezza.

Del resto, anche il GEPD ha più volte avvertito circa questa eventualità, raccomandando alle Istituzioni europee di "take steps to prepare for all eventualities"[78], non mancando di evidenziare come le valutazioni che la Commissione è chiamata ad effettuare siano complesse e tutt'altro che scontate. Proprio su questo punto le riflessioni del Garante europeo risultano di grande interesse: da un lato infatti viene riconosciuto come, differentemente dagli Stati Uniti o da altri Stati, come il Giappone, per i quali la determinazione delle condizioni di accordo sono state – e sono tuttora, soprattutto per quanto riguarda gli USA – lente e difficoltose, il Regno Unito beneficia certamente di una situazione molto particolare ed unica. Essendo stato membro dell'UE, esso ha recepito nel proprio ordinamento le Direttive in materia di protezione dei dati e, sino alla conclusione del periodo di transizione, il GDPR sarà direttamente applicabile in quel territorio; il legislatore inglese inoltre ha adottato una normativa interna, il *Data Protection Act 2018*[79], che 'trasferisce' la disciplina del Regolamento europeo in una fonte

[76] *Council Decision authorising the opening of negotiations with the UK for a new partnership agreement*, 25 febbraio 2020, doc. N. 5870/20, p. 6.

[77] COMMISSIONE EUROPEA, *Notice to stakeholders. Withdrawal of the UK and EU rules in the field of data protection*, 6 luglio 2020.

[78] GEPD, *Opinion 2/2020 on the opening of negotiations for a new partnership with the UK*, 24 febbraio 2020, p. 10.

[79] Il *Data Protection Act* ha ottenuto il *Royal Assent* il 23 maggio 2018. Come si legge nelle *Explanatory Notes* di questa normativa, "The Data Protection Act 2018 ("the Act") implements a commitment in the 2017 Conservative

primaria dell'ordinamento nazionale stesso, che sopperirà quindi, a partire dal 2021, alla perdita di vincolatività del diritto dell'UE e del GDPR stesso. Se queste caratteristiche peculiari del Regno Unito – che lo differenziano sensibilmente rispetto ad uno Stato terzo quale gli USA, che non dispone neppure di una normativa unitaria e federale in materia di protezione dei dati – fanno ottimisticamente pensare alla possibilità che la Commissione addivenga in tempi più celeri e con meno difficoltà alla adozione di una decisione di adeguatezza[80], dall'altro lato il GEPD evidenzia come "any substantial deviation that would result in lowering the level of protection would constitute an important obstacle to a finding of adequacy"[81], imponendo quindi una profonda e seria riflessione sul livello di protezione offerto dal Regno Unito e su tutti i molteplici aspetti che è necessario valutare, oltre alla disciplina della protezione dei dati fornita dal GDPR e dallo 'speculare' *Data Protection Act 2018*.

5.2. – La disciplina della data retention *come elemento di rilievo nella valutazione di adeguatezza*

Bisogna infatti ricordare come l'adeguatezza del livello di protezione garantito da uno Stato extra-UE debba essere valutata sotto svariati profili. Uno di questi, che si è rivelato peraltro determinante nella decisiva sentenza *Schrems*, è da individuarsi nella disciplina che regola la possibilità di accesso da parte della autorità pubbliche ai dati o metadati derivanti da servizi di telecomunicazioni, ottenuti direttamente mediante sistemi di sorveglianza da parte di agenzie di intelligence oppure conservati da soggetti privati. Ecco quindi che la disciplina in materia di *data retention* e accesso ai metadati per scopi securitari, che si è più sopra esaminata, diviene di fondamentale importanza anche per determinare il futuro del *data transfer* tra UE e Regno Unito. Proprio su tale aspetto, l'esito dei rinvii pregiudiziali dinnanzi alla CGUE in materia di conservazione dei dati, tra cui anche quello promosso dal IPT nel caso *Privacy International*[82], assumerà grande rilievo per le valutazioni della Commissione e le eventuali

---

Party manifesto to repeal and replace the UK's existing data protection laws to keep them up to date for the digital age in which ever increasing amounts of personal data are being processed. It sets new standards for protecting personal data, in accordance with recent EU data protection laws, giving people more control over use of their data. The Act also helps prepare the UK for a future outside the EU. The new Act replaces the 1998 Act to provide a comprehensive legal framework for data protection in the UK, in accordance with the General Data Protection Regulation (EU) 2016/679) ("GDPR"). It updates the rights provided for in the 1998 Act to make them easier to exercise and to ensure they continue to be relevant with the advent of more advanced data processing methods". Per una analisi di tale normativa, anche alla luce della Brexit, si legga L. WOODS, *UK: heading towards Brexit but with Data Protection Bill implementing GDPR*, in *European Data Protection Law Review*, 3, 2017.

[80] Lo stesso Primo Ministero Boris Johnson, il 3 febbraio 2020, ha sottolineato le peculiari caratteristiche del regime di protezione dei dati vigente nel Regno Unito, dovute proprio alla appartenenza all'UE e all'aver 'incorporato' le tutele definite a livello europeo nell'ordinamento interno; da ciò l'auspicio di una procedura rapida e semplice di riconoscimento dell'adeguatezza del livello di protezione garantito Oltremanica: "Similarly, the UK would see the EU's assessment processes on financial services equivalence and data adequacy as technical and confirmatory of the reality that the UK will be operating exactly the same regulatory frameworks as the EU at the point of exit. The UK intends to approach its own technical assessment processes in this spirit", Statement n. UIN HCWS86 del 3 febbraio 2020. Questo approccio e auspicio è stato del resto ribadito anche nel documento redatto dal Governo inglese e presentato al Parlamento nel febbraio 2020, titolato "The future relationship with the EU. The UK's approach to negotiations", nel quale si legge: "The UK will have an independent policy on data protection at the end of the transition period and will remain committed to high data protection standards. To maintain the continued free flow of personal data from the EU to the UK, the UK will seek 'adequacy decisions' from the EU under both the General Data Protection Regulation and the Law Enforcement Directive before the end of the transition period. These are separate from the wider future relationship and do not form part of trade agreements. This will allow the continued free flow of personal data from the EEA States to the UK, including for law enforcement purposes. The European Commission has recognised a number of third countries globally as providing adequate levels of data protection", p. 29.

[81] GEPD, *Opinion 2/2020*, op. cit., p. 10.

[82] Sul punto, sebbene non si voglia entrare troppo nei dettagli, si vuole precisare che l'art. 86 dell'Accordo di Recesso stabilisce che la CGUE resta competente per tutti i ricorsi proposti dal Regno Unito o contro il Regno

negoziazioni di accordi, costituendo certamente un elemento importante per comprendere se, anche sotto tale profilo, la tutela dei dati fornita dal Regno Unito sia sostanzialmente equivalente ai principi e alla normativa europea. L'interpretazione che verrà fornita dai giudici di Lussemburgo, anche e soprattutto quanto al delicatissimo nodo della compatibilità, *per se*, della conservazione generalizzata rispetto al diritto dell'UE, sarà centrale per stabilire se ulteriori interventi e modifiche alla vigente disciplina del IPA si renderanno necessarie, anche dopo la Brexit, al fine di ottenere una decisione di adeguatezza. Determinante sarà anche la lettura che la CGUE darà ancora una volta in merito alla conformità e compatibilità rispetto alla Carta di Nizza dell'Accordo *Privacy Shield* e della relativa Decisione di adeguatezza, nel rinvio pregiudiziale C-311/18. In tale pronuncia, infatti, così come nelle considerazioni già svolte dall'Avvocato generale e analizzate nel Capitolo III, Parte II, i giudici di Lussemburgo forniranno senza dubbio indicazioni preziose per comprendere quali caratteristiche debbano essere considerate nella valutazione circa l'adeguatezza e quali elementi risultino determinanti al fine di stabilire una sostanziale equivalenza tra le tutele dello Stato terzo e quelle stabilite dall'UE.

Sul punto specifico della *data retention* e della sua importanza nella valutazione della adeguatezza, non sono mancate già alcune perplessità e timori quanto alla sostanziale equivalenza rinvenibile nella disciplina inglese; tali dubbi sono stati acuiti anche dalla conclusione di un Accordo in materia di trasferimento dati, siglato tra Regno Unito e USA, in data 3 ottobre 2019 (*Agreement on access to electronic data for the purpose of countering serious crime*), che regola il trasferimento di dati e la possibilità di accesso ad essi da parte di autorità di *law enforcement* inglesi e statunitensi, per scopi securitari. Il GEPD, a ribadire la posizione già espressa nell'*Opinion 2/2020* sopra richiamata, ha provveduto ad indirizzare anche una lettera al Parlamento Europeo (15 giugno 2020, OUT 2020-0054) ed ha sottolineato come "when it comes to a possible adequacy decision for the UK, the EDPB considers that the agreement concluded between the UK and the US will have to be taken into account by the European Commission in its overall assessment of the level of protection of personal data in the UK, in particular as regards the requirement to ensure continuity of protection in case of 'onward transfers' from the UK to another third country"[83]. Quest'ultimo Accordo, infatti, è in grado di incidere sulla protezione garantita dal Regno Unito ai dati provenienti dal territorio dell'UE, sotto il profilo importante dell'ulteriore trasferimento di dati o accesso garantito ad autorità pubbliche di Paesi terzi, operazioni che qualora non debitamente regolamentate e tutelate, potrebbero avere un impatto negativo sul giudizio che la Commissione è chiamata a fornire.

Anche il Parlamento europeo, con risoluzione del 12 febbraio 2020 "on the proposed mandate for negotiations for a new partnership with the United Kingdom of Great Britain and Northern Ireland" (2020/2557(RSP)) ha messo in evidenza la delicatezza delle negoziazioni sotto il profilo della protezione

---

Unito prima della fine del periodo di transizione (co. 1), rimanendo peraltro competente a pronunciarsi in via pregiudiziale sulle domande presentate dai giudici del Regno Unito prima della fine del periodo di transizione (co. 2). L'art. 89 poi precisa come le sentenze ed ordinanze della CGUE pronunciate prima della fine del periodo di transizione o dopo la fine dello stesso nei procedimenti cui si riferisce l'art. 86, siano vincolanti nella loro totalità per e nel Regno Unito.

[83] È inoltre da evidenziare come il Regno Unito dovrà negoziare nuovi accordi con tutti quegli Stati terzi rispetto ai quali la Commissione ha sino ad ora accertato il livello di adeguatezza della protezione dei dati fornita e ha quindi accordato la possibilità di trasferimento di dati in via generale. Tali Stati, infatti, per poter garantire il livello di adeguatezza richiesto dall'UE, devono assicurare determinate garanzie anche, a loro volta, nella disciplina sul trasferimento di dati verso altri Stati extra-UE, tra cui rientrerà anche il Regno Unito, al termine del periodo di transizione. Come chiarito dal *Information Commissioner's Office* (al sito https://ico.org.uk/for-organisations/data-protection-at-the-end-of-the-transition-period/data-protection-at-the-end-of-the-transition-period/the-gdpr/international-data-transfers/), con riferimento a tali Stati extra-UE (quali Andorra, Argentina, Canada, Isole Faroe, Guernsey, Isola di Man, Israele, Giappone, Nuova Zelanda, Svizzera, Uruguay), "to have received and to maintain an adequacy decision, the country or territory is likely to have its own legal restrictions on making transfers of personal data to countries outside the EEA. This will include the UK at the end of the transition period. UK officials are working with these countries and territories to make specific arrangements for transfers to the UK where possible".

dei dati, in particolare con riferimento all'importanza di considerare con attenzione la disciplina della conservazione e accesso ai metadati per scopi di lotta alla criminalità: "Considers necessary to pay particular attention to the legal framework in the UK in the fields of national security or processing of personal data by law enforcement authorities; recalls that mass surveillance programmes might not be adequate under EU law and strongly encourages taking into consideration CJEU case-law in this field such as the Schrems case as well as European Court of Human Rights case-law" (par. 33), sottolineando in particolare come "furthermore, is of the view that the UK legal framework on retention of electronic telecommunications data does not fulfil the conditions of the relevant EU acquis as interpreted by the CJEU, and hence does not currently meet the conditions for adequacy". Un grande rilievo viene quindi attribuito alla disciplina in materia di *data retention*, riconosciuta come uno degli aspetti maggiormente problematici e sui quali permane il dubbio di una reale compatibilità al diritto dell'UE, soprattutto rispetto a quanto indicato dalla CGUE nella sua ampia giurisprudenza.

Perplessità e timori che proprio l'*Investigatory Powers Act* possa rappresentare un ostacolo all'ottenimento di una decisione di adeguatezza sono del resto stati espressi, sin dall'inizio del percorso Brexit, anche dallo stesso Parlamento del Regno Unito: nel Report, risalente al 2017, preparato dal *European Committee della House of Lords* e dedicato alle sfide del recesso ("Brexit: trade in non-financial services. 18th Report of Session 2016/2017, 22 marzo 2017, HL Paper 35), si legge l'ampia discussione sorta in seno al Parlamento anche grazie alla partecipazione di esperti. Tra questi, Antony Walker – CEO dell'azienda *techUK* e rappresentante di un significativo numero di imprese operanti nell'ambito del digitale e aventi sede nel Regno Unito – aveva significativamente messo in rilievo "the legal challenge to the 'Safe Harbour' agreement to illustrate the difficulties of securing an adequacy decision. This legal challenge followed revelations about how US security agencies processed the data of EU citizens. (..) Mr Walker raised particular concern about the Investigatory Powers Act 2016, noting that the UK could be open to challenge by European privacy campaigners and a case brought to the European Court of Justice could have real implications" (par. 140); nelle conclusioni tratte dal *Committee*, si nota come i rilievi mossi dagli esperti ed operatori nell'ambito delle comunicazioni digitali fossero stati accolti dai Parlamentari stessi, che avevano affermato come "Preserving the free flow of data across borders is seen by industry as critical to the future of UK digital services. An 'adequacy decision' by the European Commission, recognising that the UK had adequate data protection standards (as well as reciprocal arrangements), would be needed to preserve this flow of data. We note concerns that certain provisions of the Investigatory Powers Act 2016, relating to the collection and storage of personal data by security services, could stand in the way of the Commission granting such a decision" (par. 159)[84]. Sebbene questi interventi siano risalenti ad un periodo antecedente alle modifiche apportate più recentemente al testo legislativo dell'IPA, i dubbi che nei precedenti paragrafi sono stati sottolineati e le critiche che permangono rispetto ad un regime di conservazione dei metadati che resta potenzialmente generalizzato, inducono ancora a riflettere sull'impatto che la disciplina inglese in materia di *data retention* potrebbe comportare nella valutazione dell'adeguatezza del livello di protezione garantito Oltremanica.

Come si può comprendere, dunque, il percorso della Brexit, al termine soprattutto del periodo di transizione, porterà a significativi cambiamenti nei rapporti con l'UE anche sotto il profilo del trasferimento dei dati: se la garanzia di una certa continuità nel *data flow* è riconosciuta come un obiettivo importante, sia sotto il profilo economico che a fini securitari, è legittimo pensare che il Regno

[84] Della stessa opinione, in quel periodo, era anche gran parte della dottrina: "even if the UK Government adopts standards similar or equivalent to the GDPR, there is still no clarity as to the future of the relationship between UK and the EU. Securing and adequacy decision from the EC could be difficult for the UK in the light of the current case law coupled with the extensive surveillance law in the UK such as the recently introduced IPA", così A. VANBERG, M. MAUNICK, *Data protection in the UK post-Brexit: the only certainty is uncertainty*, in *International Review of Law, Computers and Technology*, 1, 2018, p. 202.

Unito cercherà di addivenire ad accordi, similmente a quanto avvenuto con gli USA, per stabilire regole in grado di garantire uno standard adeguato di protezione dei dati. La sostanziale equivalenza dovrà però essere valutata, come si è detto, sotto svariati profili attinenti al trattamento dei dati, anche di quello effettuato da autorità pubbliche per finalità di lotta alla criminalità: in tale contesto, la disciplina del IPA sarà determinante per addivenire ad una decisione di adeguatezza stabile e che non rischi, come già accaduto, di essere travolta dalle decisioni della CGUE. In questo senso, il processo di Brexit e gli sforzi che saranno profusi per cercare di ottenere un vaglio positivo da parte della Commissione, potrebbero rappresentare una ulteriore occasione per il Regno Unito di riflettere sulle tutele offerte dal proprio ordinamento e sulla loro compatibilità e sostanziale equivalenza rispetto a quelle garantite dal diritto dell'UE, in particolare in materia di *data retention* e accesso ai metadati; così sarà possibile valutare l'opportunità di introdurre eventuali modifiche necessarie, anche sulla base dell'interpretazione fornita dalla CGUE, ad un completo adeguamento ai criteri indicati dal diritto dell'UE.

Gli sviluppi futuri, così come già era stato per il percorso che ha portato all'Accordo di recesso, risultano estremamente imprevedibili: la storia e le vicende che hanno caratterizzato il trasferimento dati verso gli USA – in particolare con riferimento al *Safe Harbor* prima e al *Privacy Shield* successivamente – mettono in luce la complessità della questione dell'adeguatezza, così come la giurisprudenza in materia di conservazione dei metadati insegna quanto sia arduo adottare normative nazionali compatibili e conformi ai criteri delineati dal diritto dell'UE e, soprattutto, dalla CGUE. Per questo le insidie dettate dalle negoziazioni che si svilupperanno sino al raggiungimento – eventuale ma atteso – di una decisione di adeguatezza sono difficilmente prevedibili e rappresentano un ulteriore elemento di grande rilievo, i cui sviluppi meritano certamente di essere seguiti e valutati con attenzione. In conclusione, poi, si vuole sottolineare come proprio l'importanza di garantire continuità al trasferimento dati e l'imposizione di stringenti condizioni stabilite dal GDPR, indurranno e, in certo qual modo, imporranno certamente al Regno Unito di considerare con attenzione il diritto dell'UE. Legislatori e giudici inglesi, dunque, anche in futuro, non potranno prescindere dall'osservare gli sviluppi della giurisprudenza della CGUE in materia di protezione dei dati e *data retention* per poter garantire un livello di tutela sostanzialmente equivalente. Sotto questo profilo, quindi, la necessità di raggiungere un riconoscimento di adeguatezza, come si è già detto più in generale nel Capitolo III, Parte II, può ingenerare un virtuoso processo di innalzamento degli standard di protezione della riservatezza anche oltre i confini dell'UE e potrà continuare ad influenzare il diritto interno inglese anche a seguito della Brexit. Non è infine da dimenticarsi come il Regno Unito, pur non essendo più vincolato al rispetto della Carta di Nizza al termine del periodo di transizione[85], dovrà comunque garantire la tutela dei diritti riconosciuti nella Convenzione EDU e protetti anche sulla base delle decisioni della Corte EDU: sotto questo profilo, dunque, la convergenza dell'orientamento espresso dalle due Corti europee in materia di protezione dei dati e, in particolare, di conservazione e accesso ai dati per scopi securitari, assumerà in futuro ancor più rilievo poiché potrà determinare un maggiore allineamento o, al contrario, una divergenza tra il bilanciamento sicurezza-diritti fondamentali effettuato dai giudici di Lussemburgo nel contesto dell'UE

[85] La Carta dei diritti fondamentali dell'UE infatti rientra nella definizione di 'diritto dell'UE' di cui parla l'Accordo di recesso; anche il *European Union Withdrawal Act 2018* (come modificato dal successivo *European Union Withdrawal Act 2020*) adottato dal Parlamento del Regno Unito specifica alla Section 5, par. 4 come "The Charter of Fundamental Rights is not part of domestic law on or after exit day".

e quello svolto invece dal legislatore e dai giudici inglese anche sulla base dell'interpretazione fornita dai giudici di Strasburgo nella propria giurisprudenza[86].

[86] Come è stato evidenziato nel Capitolo V, Parte II, negli ultimi anni la Corte EDU ha mostrato un orientamento in tema di sistemi di sorveglianza che prevede criteri e requisiti di legittimità e necessità in una società democratica che paiono divergere, seppur con i dovuti distinguo, rispetto alla giurisprudenza della CGUE. Per questo, se tale approccio dovesse essere mantenuto anche nelle successive pronunce, in particolare quelle della Grande Camera nei casi *Big Brother Watch* e *Centrum for Rattvisa*, ciò potrebbe portare il Regno Unito ad adottare un livello di tutela, rispondente ai requisiti di proporzionalità e conformità al diritto fondamentale di cui all'art. 8 Convenzione EDU, inferiore rispetto a quello garantito dal diritto dell'UE, come interpretato dalla giurisprudenza della CGUE. Anche sotto questo complesso profilo, quindi, bisognerà attendere i futuri sviluppi giurisprudenziali di entrambe le Corti europee per comprendere come e se le pronunce in materia di sorveglianza e *data retention* potranno avere un impatto sulle garanzie offerte dall'ordinamento inglese.

CAPITOLO II

IL BELGIO.
DALLA CGUE ALLA COUR CONSTITUTIONNELLE *E RITORNO*

1. – Dalle prime disposizioni normative in materia di conservazione dei metadati alla trasposizione della DRD: l'approccio iniziale alla **data retention** *del legislatore belga*

1.1. – Le criticate disposizioni in materia di **data retention** *frutto di un orientamento 'pro-securitario'*

Il legislatore e i giudici costituzionali belgi si sono trovati ad affrontare, in diverse occasioni e momenti, la complessa sfida della adozione di una adeguata disciplina in materia di *data retention*: come si avrà modo di vedere approfonditamente, sia la normativa attuativa della DRD che la successiva e ancora vigente legge sulla conservazione dei metadati – entrambe approvate con grandi difficoltà – sono state sottoposte al vaglio di legittimità della Corte costituzionale, a dimostrazione del significativo dibattito che si è aperto, a livello nazionale, su tale delicata regolamentazione. Similmente a quanto già emerso dalle vicende che hanno caratterizzato la *data retention* nel Regno Unito, i continui interventi normativi e giurisprudenziali avvicendatisi in Belgio non possono essere però letti disgiuntamente dalla fondamentale giurisprudenza della CGUE nei casi ampiamente esaminati nella Parte II di questo lavoro. L'impatto e l'influenza dei giudici di Lussemburgo, infatti, risuonano chiaramente nelle scelte e nelle parole tanto del legislatore quanto della Corte costituzionale belga, che pur non hanno mancato di riconoscere criticità e zone grigie nei principi e requisiti fissati a livello dell'UE. Proprio in questo contesto si inseriscono i due rinvii pregiudiziali, al momento pendenti, promossi dai giudici belgi sia in materia di *data retention* per scopi securitari, sia con riferimento alla disciplina relativa al trasferimento e trattamento di PNR. Se dunque la grande attenzione e l'attivismo mostrato dalla società civile e dalle autorità belghe in tale ambito hanno condotto, come già accaduto per il Regno Unito, all'instaurazione di un dialogo costante con la CGUE, in un continuo rimando frutto della percepita necessità di ulteriori interventi interpretativi e chiarificatori dei giudici di Lussemburgo, è da sottolinearsi come il Belgio risulti però portatore di un approccio particolare e differente rispetto a quello mostrato Oltremanica e che, proprio per questo, diviene interessante e meritevole di debita analisi.

Svolgendo una ricostruzione cronologica delle normative che si sono susseguite nel tempo, è necessario innanzitutto notare come il primo obbligo di conservazione dei metadati imposto dallo Stato belga in capo agli operatori di servizi di telecomunicazione fosse da individuarsi già nel 2000, in particolare con la legge 28 novembre 2000[1] che modificava la previa normativa del 21 marzo 1991[2]: dinnanzi all'aumentare di reati legati al mondo digitale e delle telecomunicazioni, perpetrati mediante l'impiego di Internet o di servizi di telefonia, la normativa richiamata era intervenuta in materia penale e di procedura penale allo scopo di adattare le disposizioni esistenti e di inserirne di nuove, cogliendo così quella specificità di strumenti e istituti che la lotta a nuove forme di criminalità informatica – quali frode informatica, *hacking* o infrazioni contro l'integrità dei sistemi informatici – richiedeva[3]. Veniva

[1] *Loi du 28 novembre 2000 relative à la criminalité informatique*, M.B., 3 février 2001, p. 02909.
[2] *Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques*, M.B., 27 mars 1991, p. 6155.
[3] Per una analisi dettagliata dei nuovi reati introdotti da tale normativa, tutti legati al progresso tecnologico e all'affermarsi dell'utilizzo massiccio di sistemi di telecomunicazione, si rimanda a: F. DE VILLENFAGNE, S.

pertanto in quell'ambito introdotta l'imposizione ai fornitori di mezzi di comunicazione elettronica di conservare i dati relativi alle chiamate nonché i dati identificativi degli utenti per un periodo minimo di dodici mesi. Questa disposizione prevedeva tuttavia che la determinazione esatta dei dati da sottoporre a *retention* nonché delle diverse tempistiche di conservazione fosse predisposta da un *arret royal* (regio decreto, elaborato dal Governo a livello federale, poi formalmente emanato dal Re). La scelta di lasciare esclusivamente nelle mani del potere esecutivo la definizione di aspetti così rilevanti – quali durata e dati interessati –, in grado di determinare in maniera significativa la portata dell'ingerenza nella sfera privata, era stata oggetto di forti critiche e preoccupazioni, espresse dalla *Commission de la protection de la vie privée* nazionale[4], come emerge nel Doc. parl. Chambre, 0213/004[5]. Tele autorità aveva infatti evidenziato l'assenza, all'interno del dettato normativo, di specifiche disposizioni circa le condizioni e la procedura di accesso ai metadati, che risultavano invece necessarie e fondamentali per scongiurare possibili abusi e per limitare quella eccessiva discrezionalità e arbitrarietà che avrebbe potuto essere attribuita, mediante decreto, alle autorità giudiziarie e di *law enforcement*.

Le prime disposizioni in materia di conservazione dei dati per scopi securitari dunque regolavano in maniera piuttosto vaga e poco specifica una disciplina di estrema delicatezza, mostrando una scarsa attenzione – e forse una scarsa consapevolezza – all'impatto che si sarebbe venuto a determinare su taluni diritti fondamentali, tra cui ovviamente in primis il diritto alla riservatezza[6]: basti pensare alla

---

DUSSOLIER, *La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique*, in *A&M*, 1, 2001, p. 71.

[4] La *Commission de la protection de la vie privée* era stata istituita con legge del 8 dicembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (M.B. 18 mars 1993). A tale autorità pubblica indipendente era stato attribuito il compito di vigilanza quanto al rispetto dei diritti alla vita privata e alla protezione dei dati e gli era stata inoltre attribuita la funzione di controllo, nel territorio nazionale, circa la corretta applicazione delle disposizioni di attuazione della Direttiva 95/46/CE – questa normativa europea infatti imponeva all'art. 28 la creazione presso ciascuno Stato membro di una apposita autorità statale indipendente di controllo –. La *Commission* è rimasta operativa sino al 2017, quando la legge del 3 dicembre 2017 *portant création de l'Autorité de protection des données* ha provveduto alla istituzione presso la *Chambre des Représentants* della *Autorité de protection des données*: quest'ultima ha sostituito la *Commission* quale organo di controllo indipendente (per approfondimenti si legga N. RAGHENO, *Data protection: la future nouvelle Autorité dee protection des données*, in *Cahier du Juriste*, 2, 2017, p. 29). Con riferimento alla funzione e composizione della *Commission de la protection de la vie privée*, la cui opinione sulle normative in materia di *data retention* verrà più volte richiamata nel corso di questa analisi, si rimanda, ex multis, a E. DEGRAVE, *La Commission de la protection de la vie privée: l'Autorité de régulation du secteur des traitements de données à caractère personnel*, in *Revue du Centre d'étude et de recherches en administration publique*, 26, 2016, pp. 37-70. Per completezza e per fornire un quadro quanto più completo possibile delle autorità che vigilano sulla tutela del diritto alla vita privata, merita sottolineare come la legge del 30 luglio 2018 *relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*, abbia attribuito al *Comité permanent de controle des services des reinsegnement* il compito specifico di vigilare sul rispetto delle norme – nazionali ed europee – in materia di privacy e protezione dei dati da parte dei servizi di intelligence (*Service général du renseignement*), laddove questi pongano in essere trattamenti dei dati nell'ambito di attività di garanzia della sicurezza nazionale (art. 95). Il *Comité* (c.d. *Comité R*) è un organo pubblico permanente ed indipendente, istituito con legge del 18 luglio 1991 e il cui ruolo e composizione è stato poi inserito nella legge organica del 30 novembre 1998 *des services de renseignement et de sécurité*.

[5] Doc. Parl. Chambre, 1999-2000, 0213/011. In tale documento si legge come: "Le projet de loi belge ne contient aucune indication relative aux personnes susceptibles de faire l'objet de cette mesure de surveillance, aux circonstances dans lesquelles elle peut être ordonnée, aux moyens à employer ou aux procédures à observer (voir arrêt Amann précité, § 58). Il semble donc que l'article 14 du projet de loi belge relatif à la criminalité informatique ne pourrait pas être considéré comme suffisamment clair et détaillé pour assurer une protection appropriée contre les ingérences des autorités dans le droit des citoyens au respect de leur vie privée et à la confidentialité de leurs communications. La Commission est en outre préoccupée par le fait que le projet de loi puisse être disproportionné et onéreux de façon non nécessaire à charge des opérateurs", p. 18.

[6] Merita sin da ora fornire alcune coordinate importanti sulla tutela della riservatezza e protezione dei dati in Belgio, che pure erano state già anticipate nel Capitolo I, Parte III. L'art. 22 della Costituzione belga del 1994 afferma che: "Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit". Viene dunque tutelato il

definizione degli operatori soggetti all'obbligo di *data retention*, indicati genericamente come "opérateurs de réseaux de télécommunications et fournisseurs de services de télécommunications"[7], o ancora al fatto che la *Commission de Protection de la Vie Privée* non fosse stata consultata e coinvolta nella fase di predisposizione del progetto di legge, bensì solamente nella fase di dibattito parlamentare. Anche la durata massima di dodici mesi – da determinare poi nel dettaglio mediante intervento con regio decreto e dunque con decisione sottratta al normale procedimento legislativo – poneva alcune perplessità quanto alla proporzionalità e necessità della individuazione di un periodo temporale così esteso. Ne derivava come il più grande timore, espresso anche dalla dottrina, fosse l'affermarsi di un sistema di sorveglianza 'esplorativa' posto in essere da autorità pubbliche, favorito da una normativa ampia nel proprio dettato e carente di precisi limiti e salvaguardie[8].

A distanza di pochi anni comunque, a seguito del forte clima di paura che aveva caratterizzato il primo decennio del XXI secolo, scandito dagli attentati terroristici che avevano colpito non solo gli Stati Uniti d'America nel 2001 bensì l'Unione europea stessa nel 2004, a Madrid, il legislatore belga aveva deciso di intervenire nuovamente sulla regolamentazione delle comunicazioni elettroniche, risentendo anche della spinta proveniente dal rinnovato dibattito a livello europeo[9]. Così la legge del 13 giugno

---

diritto alla vita privata nella sua accezione più classica, inteso come "protéger l'individu contre les excès de pouvoir de l'autorité publique, mais également de lui permettre de développer librement et pleinement sa personnalité, ses relations avec ses semblables, le tout dans une perspective d'autonomie individuelle" (B. DOCQUIR, *Droit du nemérique*, Larcier, 2018, p. 347). Pur non prevedendo una specifica ed autonoma disposizione in materia di protezione dei dati, similmente a quanto stabilito ad esempio nella Carta di Nizza, la giurisprudenza belga ha avuto modo di chiarire come il diritto tutelato all'art. 22 del testo costituzionale comprenda al suo interno anche il diritto alla protezione dei dati personali. Pur non potendo in questa sede provvedere ad una puntuale ricostruzione, pare comunque utile richiamare una recente decisione della Corte costituzionale (Arret n. 29/2018) nella quale viene espresso, con grande chiarezza, come "Le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelles et conventionnelles précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée. Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles" (par. B.11). Oltre alla Costituzione, ovviamente tale diritto viene tutelato da una pluralità di normative settoriali e specifiche, tra cui, come si è visto e come si vedrà dettagliatamente, le disposizioni in materia di *data retention*. Merita comunque sottolineare la Loi 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*, più volte modificata e adeguata al progredire della tecnologia, all'evolvere delle minacce e al susseguirsi delle normative europee in materia. Per una ampia ricostruzione del tema si rimanda a C. DE TERWANGNE, E. DEGRAVE (a cura di), *La protection des données à caractère personnel en Belgique: manuel de base*, Politeia, 2019; SERVICE DE RECHERCHE DU PARLEMENT EUROPÉEN, *Le droit au respect de la vie privée: les défis digitaux, une perspective de droit comparé. Belgique*, 2018; K. LEMMENS, *Respect de la vie privée et de la personnalité*, in M. VERDUSSEN, N. BONBLED (a cura di), *Les droits constitutionnels en Belgique*, Bruylant, 2011 e nello stesso Volume, E. DEGRAVE, Y. POULLET, *Le droit au respect de la vie privée face aux nouvelles technologies*, pp. 1001-1035.

[7] Come sottolineato da alcuni autori, questa definizione apre ad una moltitudine e diversità di attori che tali vocaboli, così generici, sono in grado di ricoprendere: "Non seulement, les opérateurs de réseaux de téléphone, de téléphonie mobile ou d'Internet devront conserver les données relatives aux appels, communications et connexions, mais également tout prestataire de services délivrés par ces réseaux, ce qui englobe, nous le répétons, les fournisseurs d'accès Internet, de courriers électroniques, de forums de discussions, de chat, de services de cryptographie ou de conservation des clés, etc", così F. DE VILLENFAGNE, S. DUSSOLIER, *La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique*, op. cit., p. 31. Sul punto viene inoltre osservato come "We may observe that the greater part of these 'operators' or 'providers' have no a priori reason whatsoever to conserve this data beyond termination of the actual connection. Indeed, a good number of these services are free of charge. In other words, the only finality for the conservation of such data is in the context of a need to bring evidence in the event of an infraction being pursued. Such a conclusion has a bearing, both on the foundation for the legitimacy of such processes, as well as on the statute of those persons expected to carry out such conservation", Y. POULLET, *The fight against crime and/or the protection of privacy: a thorny debate!*, in *International Review of Law, Computers and Technology*, 2, 2004, pp. 253.

[8] Y. POULLET, *The fight against crime and/or the protection of privacy: a thorny debate!*, op. cit., che sottolinea come "there is no worse danger than this cyber-surveillance, which hunts a man down in his most intimate space and raises within him a perpetual and haunting fear of exposure", p. 264.

[9] Si rimanda sul punto all'analisi svolta nel Capitolo 1, Parte II, nel quale vengono esaminate le diverse iniziative e proposte che, a partire dal 2005, si erano susseguite in seno all'UE e che erano volte proprio alla approvazione

2005 relativa alle comunicazioni elettroniche[10], dando attuazione alla facoltà derogatoria concessa dall'art. 15 Direttiva *e-Privacy*, stabiliva all'art. 126, par. 3, l'obbligo di conservazione dei metadati nonché dei dati identificativi di tutti gli utenti di servizi di telecomunicazione, per un periodo compreso tra i dodici e i trentasei mesi e per scopi estremamente ampi, individuati nella: "investigation and prosecution of criminal acts, for the tracking of malicious calls to emergency services and to enable the research of the Ombudsman for Telecommunications in revealing the identity of people making improper use of electronic communications services or networks"[11]. Similmente alle disposizioni del 2000, anche questa disciplina, dai contorni estremamente vaghi e che demandava ad un regio decreto la determinazione di alcuni specifici aspetti, era stata accolta con numerose critiche da parte della *Commission de la protection de la vie privée*; quest'ultima aveva in particolare mostrato per la prima volta dubbi quanto alla compatibilità con i diritti fondamentali dello strumento della *data retention*, considerato *per se* e dunque nella sua natura di misura preventiva, slegata cioè dalla presenza di una indagine penale in corso tale da giustificare l'ingerenza nella sfera privata (Avis n. 08/2004 del 14 giugno 2004, *sur l'avant-projet de loi relatif aux communiations èlectroniques*).

È importante evidenziare, tuttavia, come le discusse disposizioni introdotte nel 2000 e nel 2005, non divennero comunque mai operative: non vennero mai approvati, infatti, i relativi regi decreti che, essendo chiamati a determinare le categorie di dati da sottoporre a conservazione, la durata della conservazione stessa e le condizioni circa la sicurezza da garantire nel periodo di *data retention*, risultavano imprescindibili strumenti per la concreta attuazione della disciplina, senza i quali l'obbligo imposto non poteva trovare esecuzione[12].

1.2. – Il travagliato percorso di approvazione della legge di trasposizione della DRD e il complesso intreccio con la giurisprudenza della CGUE

La *de facto* mancata attuazione della disposizione nazionale in materia di conservazione dei metadati per scopi securitari divenne poi fortemente problematica a seguito della adozione, a livello dell'UE, della Direttiva 2006/24: questa, come noto e secondo quanto ampiamente analizzato nella Parte II del presente lavoro, aveva introdotto l'onere in capo agli Stati membri di adottare normative nazionali che stabilissero l'obbligo di *data retention* per scopi di repressione e lotta alla criminalità grave, lasciando peraltro ai legislatori nazionali il compito di stabilire apposite regole attinenti alla fase di accesso da parte delle autorità di *law enforcement*. Ebbene proprio sotto il profilo della trasposizione di tale normativa europea nell'ordinamento nazionale belga, emerge tutta la complessità della disciplina della *data retention*: bisognerà attendere, infatti, sino al 30 luglio 2013 per vedere l'approvazione di una apposita legge di attuazione della DRD, frutto di un lungo e difficile procedimento legislativo, che aveva visto proprio nel 2013 una velocizzazione e un rapido sviluppo dovuto alle pressioni esercitate dalla Commissione europea. Quest'ultima, infatti, nel maggio 2013 aveva intimato il Belgio a predisporre una normativa di trasposizione della DRD e ad adeguare la propria disciplina interna all'obbligo di *data retention* stabilito a livello europeo[13].

---

di strumenti normativi in grado di stabilire una disciplina comune e condivisa in materia di conservazione dei metadati.

[10] *Loi du 13 juin 2005 relatives aux communications électroniques*, M.B., 20 juin 2005.

[11] E. KOSTA, P. VALCKE, *Retaining the data retention directive*, in *Computer law and Security Report*, 22, 2006, p. 377.

[12] A. CASSART, J-F. HENROTTE, *L'invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée*, in *Jurisprudence de Liege*, 20, 2014, p. 954.

[13] "The European Commission has asked Belgium to bring its laws into line with EU legislation on data retention, after the country failed to inform the Commission of adequate measures to transpose the rules in national law. The Commission's request takes the form of a reasoned opinion (the second step in the three-step EU infringement

In realtà, il dibattito circa la normativa nazionale da adottare era stato già da tempo avviato in Belgio ma aveva incontrato diversi ostacoli e battute d'arresto: il primo tentativo in materia era naufragato definitivamente nel 2008, dinnanzi al parere negativo espresso dalla *Commission de la protection de la vie privée* (Avis n. 24/2008 du 2 juillet 2008, p. 7). Il progetto di legge proposto era stato ritenuto, come già in passato, eccessivamente vago, col rischio dunque di attribuire prerogative e discrezionalità troppo ampi al potere esecutivo, soprattutto con riferimento alle condizioni di accesso ai dati conservati: questi ultimi, nella prima versione proposta, dovevano essere memorizzati da parte dei fornitori di servizi di telecomunicazione per ben due anni – ovvero il termine massimo di durata concesso dalla DRD stessa –; tale scelta non risultava fondata ed ancorata su nessun appropriato vaglio di necessità né tantomeno su alcuna valutazione concreta quanto alla reale utilità di una durata così estesa, mentre risultavano mancanti anche appropriate disposizioni sulla sicurezza dei dati conservati. Il secondo progetto di legge del 2009 aveva mostrato di tenere in debita considerazione le osservazioni che avevano portato al respingimento della previa proposta, limitando la durata di conservazione ad un massimo di dodici mesi e stabilendo la necessità che le condizioni e la durata stessa, variabile a seconda delle categorie di dati interessati, fossero contenute nella legge e non, come proposto in passato, in un regio decreto, assicurando così la determinazione di tali importanti dettagli al dibattito parlamentare. Pur avendo ottenuto parere positivo da parte della *Commission de la protection de la vie privée* (Avis n. 20/2009 del 1 luglio 2009), anche questo progetto di legge aveva però seguito il medesimo destino del suo predecessore, questa volta per ragioni di instabilità politica, a causa della caduta del Governo in carica, il 26 aprile 2010, con il successivo scioglimento del Parlamento e indizione di nuove elezioni[14].

Solo dunque con la legge del 30 luglio 2013[15], che modificava gli articoli 2, 126 e 145 della richiamata normativa del 13 giugno 2005 nonché l'articolo 90decies del *Code d'instruction criminelle* (M.B. 23 agosto 2013), la DRD veniva finalmente stata trasposta nell'ordinamento nazionale. Con la medesima legge inoltre era data attuazione anche alla facoltà derogatoria concessa dall'art. 15 della Direttiva *e-Privacy*. Le disposizioni della legge del 2013 venivano poi integrate dall'*Arreté royal* del 19 settembre 2013 che dava esecuzione all'art. 126 della legge 13 giugno 2005 (M.B. 8 ottobre 2013, n. 70828)[16] e che conteneva indicazioni di grande rilievo per l'attuazione della normativa stessa, determinando ad esempio con precisione la tipologia e la definizione stessa dei dati da conservare, le categorie di servizi di telecomunicazione interessati nonché le misure tecniche e amministrative che i fornitori di servizi dovevano adottare per garantire un adeguato livello di protezione dei dati conservati.

process). (..) Belgium has failed so far to transpose fully. In particular, the Belgian authorities still need to bring national legislation in line with the EU rules on requiring companies to retain data for between 6 months and 2 years with appropriate data security and data protection safeguards. Belgium now has two months to comply with European Union rules. If Belgium does not comply, the Commission may decide to refer the case to the EU's Court of Justice", Commissione europea, MEMO/13/470 del 30 maggio 2013. Nel Doc. Parl. Chambre, 2012-2013, DOC 53-2921/001, pp. 3-4, sulla legge 30 giugno 2013, viene riconosciuto come: "Fin septembre 2012, la Commission européenne a mis la Belgique en demeure de transposer la directive et a attiré l'attention de la Belgique sur les sanctions pécuniaires que la Cour de justice pourrait lui infliger pour transposition incomplète de la directive. Il est donc exclu d'attendre encore plus longtemps et, à plus forte raison, d'attendre un amendement éventuel de la directive".

[14] Come sottolineato da C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, in *Journal des tribunaux*, 13, 2017, p. 237.

[15] *Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle*, M.B., 23 aout 2013, p. 56109.

[16] Per una sintetica analisi si rimanda a: M. VAN BELLINGHEN, T. ZGAJEWSKI, *Les enjeux de la transposition en Belgique des nouvelles directives européennes sur les communications électroniques*, Academia Press, 2012, p. 39.

La normativa del 2013 stabiliva, in sintesi, un obbligo di conservazione di dati di localizzazione, comunicazione e identificazione[17], per una durata di dodici mesi. Erano tuttavia previste alcune possibili eccezioni, in grado di prolungare sensibilmente il periodo di conservazione: mediante decreto, infatti, poteva essere stabilita una diversa durata, non superiore comunque a diciotto mesi, per talune tipologie di dati, nel caso in cui se ne ravvisasse la necessità – senza ulteriori precisazioni o specificazioni –, mentre nel caso in cui fosse considerato essenziale provvedere ad una conservazione superiore ai ventiquattro mesi, comunque concessa, veniva imposta, quale unica condizione, la notifica immediata da parte del Governo alla Commissione europea e agli altri Stati membri, accompagnata da una specifica motivazione volta a giustificare l'adozione di tale misura. Le finalità perseguite dalla conservazione dei dati e per le quali dunque tali informazioni potevano essere messe a disposizione delle autorità di *law enforcement* erano quelle descritte al comma 2 dell'art. 126 della legge del 2005, così come modificato dalla legge del 2013: in sostanza si trattava della ricerca, indagine e repressione di reati indicati agli artt. 46bis e 88bis del *Code d'instruction criminelle*, della repressione di chiamate malevole o moleste ai servizi di emergenza; della ricerca dal parte del *Service de médiation pour les télécommunications*[18] dei dati identificativi di coloro che avevano utilizzato in maniera illegale un servizio di telecomunicazione o ancora per scopi di tutela della sicurezza nazionale con riferimento alle attività svolte dalle autorità di intelligence e disciplinate dalla legge organica del 30 novembre 1988.

Sin da questa schematica ricostruzione della disciplina adottata nel 2013, si può ben comprendere come, sotto un profilo prettamente formale, in Belgio non fosse stato adottato un testo unitario, completo ed esaustivo in materia di *data retention* e in trasposizione della DRD, ma anzi si fosse verificata la contemporanea presenza di diversi testi di riferimento – la normativa e il regio decreto – che peraltro contenevano modifiche alle leggi esistenti, con un continuo rimando ad ulteriori fonti e acuendo così una certa frammentarietà della disciplina, che ha finito certamente col complicare il quadro di riferimento di una materia già di per sé difficile[19]. Sotto il profilo sostanziale poi la normativa individuava una grande varietà di autorità legittimate all'accesso, anche diverse da quelle strettamente definibili come di *law enforcement* (ad esempio si pensi al *Service de médiation pour les télécommunications*, cui era attribuita tale delicata facoltà di accesso), andando così al di là di quanto era invece previsto dalla DRD, che stabiliva quale finalità giustificante la conservazione e il successivo accesso solo l'indagine, l'accertamento e il perseguimento di reati gravi[20]. Molto similmente a quanto si è detto già con riferimento alle previe discipline normative, anche la legge del 2013 aveva quindi

[17] Per dati di localizzazione si intendevano le informazioni relative al luogo da cui era partita o si era svolta la comunicazione e la durata della stessa; i dati di comunicazione si riferivano invece a quelle informazioni che permettono di individuare i destinatari di una comunicazione mentre con dati identificativi si faceva riferimento a quelli che consentivano di identificare appunto i titolari di un numero o di un indirizzo IP, nonché tutte le utenze attivate da quel soggetto e la tipologia di dispositivo sul quale l'utenza era stata attivata.

[18] Riprendendo la definizione che il *Service de médiation* fornisce nel suo sito istituzionale: "Le service de médiation, institué par la loi du 21 mars 1991 auprès de l'IBPT (l'Institut Belge des Services Postaux et des Télécommunications), fonctionne de manière totalement indépendante des opérateurs de télécoms et, dans les limites de ses attributions, ne reçoit d'instruction d'aucune autorité. Tout client mécontent de son opérateur télécoms peut demander l'intervention gratuite du service de médiation. Le médiateur est compétent pour l'ensemble du secteur des télécoms. Le service de médiation est une instance de recours : n'ayant pas pour but de se substituer au service à la clientèle des opérateurs télécoms, il peut agir lorsqu'un client n'a obtenu aucune solution satisfaisante lors de ses contacts avec son fournisseur de télécoms", http://www.ombudsmantelecom.be/fr/nos-missions.html?IDC=19.

[19] Così E. PEERAER, *Data retention: the Belgian approach*, in *Masaryk University Journal of Law and Technology*, 1, 2012, p. 125.

[20] Una spiegazione che possa giustificare l'ampiezza degli scopi indicati da tale normativa può essere ravvisata nel fatto che la medesima legge rappresentava anche la trasposizione della Direttiva 2002/58 ed in particolare della facoltà concessa dall'art. 15, che permetteva, come si ricorderà, di derogare all'obbligo generale di cancellazione dei metadati al fine di raggiungere scopi estremamente ampi quali "sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica".

attirato numerose critiche, da ravvisarsi sia nella scelta, ribadita anche in questa disposizione, di lasciare ad un decreto la determinazione di aspetti importanti della disciplina, sia nella carenza di regole procedurali precise e puntuali quanto alla delicata fase dell'accesso.

Ancora una volta, però, la disciplina nazionale è stata obbligata a confrontarsi con gli avvenimenti caratterizzanti il livello dell'Unione europea: la normativa belga era stata adottata, infatti, con grande ritardo, in un periodo in cui la legittimità della DRD risultava fortemente contestata in numerosi Stati membri[21], tanto che era stato promosso il noto rinvio alla CGUE che avrebbe poi portato, non molto tempo dopo l'entrata in vigore della legge belga del 2013, alla storica sentenza *DRI* e dunque alla invalidazione della DRD. In questo intricato contesto, proprio sulla base dei motivi che avevano spinto le Corti austriaca e irlandese a promuovere l'intervento della CGUE, nonché considerando quanto affermato nelle Conclusioni dell'Avvocato generale Cruz Villalon del 12 dicembre 2013, le ONG Liga voor Mensenrechten e Ligue des Droits de l'Homme, nonché l'Ordre des barreaux francophones et germanophone, avevano presentato dinnanzi alla Corte costituzionale belga, nel febbraio 2014, ricorso per annullamento dell'art. 5 della legge belga in materia di *data retention*. Ad un primo sguardo, potrebbe certamente sembrare curiosa la scelta dei ricorrenti di non attendere la valutazione ultima della CGUE prima di adire la Corte costituzionale: tale decisione in realtà trova una logica spiegazione nell'istituto del ricorso previsto dal sistema di giustizia costituzionale belga, il quale può essere presentato solo entro sei mesi dalla pubblicazione della normativa che si vuole impugnare[22]. Per questo motivo, vista la scadenza di tale termine nel febbraio 2014, non era stato possibile aspettare di conoscere le sorti della DRD: nondimeno, già in quel periodo, oltre alla ritenuta violazione dei diritti fondamentali tutelati dalla stessa Costituzione belga, i ricorrenti avevano potuto far affidamento sulle Conclusioni dell'Avvocato generale, che erano state considerate sufficienti e convincenti basi in grado di rafforzare le posizioni sostenute nel ricorso, in attesa della decisione della CGUE, che sarebbe comunque utilmente giunta nelle more del giudizio dinnanzi ai giudici nazionali; con il risultato che, qualora i giudici di Lussemburgo avessero confermato le considerazioni di Cruz Villalon, invalidando la DRD, la Corte costituzionale non avrebbe potuto ignorare le considerazioni e l'impatto di tale dirompente decisione, dai riflessi inevitabili – per quanto indiretti – anche nel contesto nazionale[23].

---

[21] Per un'ampia ricostruzione di tale punto, si rimanda al Capitolo II, Parte II.

[22] La Corte costituzionale belga effettua, oltre ad un controllo di costituzionalità di tipo concreto mediante rinvio di una questione pregiudiziale, anche un controllo astratto mediante ricorso per annullamento. Quest'ultimo può essere promosso dal Consiglio dei ministri, dagli organi esecutivi delle Regioni e delle Comunità, dal Presidente dell'Assemblea legislativa (nazionale, regionale o comunitaria) nonché, a seguito di riforma intervenuta nel 1988, da persone fisiche e giuridiche. Il termine temporale per la presentazione del ricorso è di sei mesi dalla pubblicazione della normativa da impugnare. Merita solo marginalmente ricordare come la *Cour d'Arbitrage*, istituita con legge del 28 giugno 1983, con la funzione di dirimere controversie essenzialmente attinenti il riparto di competenze tra Stato ed entità federate, sia stata protagonista, a partire dal 2003, di un percorso graduale di riforme che hanno portato inizialmente ad un ampiamento delle competenze sino a toccare anche la garanzia dei diritti costituzionali previsti nel Titolo II (artt. 8-32) e negli artt. 170, 172 e 191, fino a giungere, mediante *Loi de revision constitutionnelle* del 7 maggio 2007, al passaggio da *Cour d'Arbitrage* a *Cour constitutionnelle*. Per maggiori approfondimenti sull'evoluzione di tale organo nonché sulla giustizia costituzionale belga si rimanda, *ex multis*, a: N. VIZIOLI, *La giustizia costituzionale in Belgio*, in J. LUTHER, R. ROMBOLI, R. TARCHI (a cura di), *Esperienze di giustizia costituzionale*, Vol. II, Giappichelli, 2002; P. CARROZZA, *La Cour d'Arbitrage belga*, in G. F. FERRARI, A GAMBARO (a cura di), *Corti nazionali e comparazione giuridica*, ESI, 2006; E.A. FERIOLI, *Il Belgio*, in P. CARROZZA, A. DI GIOVINE, G.F. FERRARI (a cura di), *Diritto costituzionale comparato*, Tomo I, Laterza, 2019, p. 319 ss.

[23] Pur lasciando – quanto meno direttamente – intoccate le normative interne di trasposizione della Direttiva europea, è noto infatti come importanti e differenti reazioni e riflessioni siano scaturite negli Stati membri nelle more e a seguito della sentenza *DRI*: da chi non aveva predisposto alcun intervento, lasciando inalterata la normativa interna di riferimento, a chi invece aveva optato per un nuovo intervento legislativo a modifica della disciplina previgente, a quegli Stati membri in cui era stato invece promosso un intervento giudiziario volto a verificare la legittimità della normativa in materia di *data retention*. Il Belgio, per quanto il ricorso fosse stato presentato poco prima della sentenza *DRI*, può essere fatto rientrare in quest'ultimo gruppo.

2. – Dalla Cour constitutionnelle *al legislatore nazionale: le prime reazioni alla giurisprudenza della CGUE*

2.1. – Il ricorso per annullamento promosso da alcune ONG e la strenua difesa del Governo circa la legittimità della disciplina normativa del 2013: la particolarità ed unicità della decisione della Cour constitutionnelle

Mentre le ONG sopra richiamate avevano promosso ricorso ritenendo la normativa nazionale in materia di *data retention* incompatibile principalmente[24] con i diritti alla vita privata e alla protezione dei dati, tutelati sia a livello nazionale dall'art. 22 della Costituzione che dalla Carta di Nizza e dalla Convenzione EDU, l'Ordre des barreaux francophones et germanophone, ovvero l'associazione rappresentativa degli interessi degli avvocati, aveva invece considerato la legge del 2013 illegittima nella parte in cui non era prevista alcuna eccezione riguardante le conversazioni di avvocati e medici, che ne tutelasse il segreto professionale[25]. Tutte le ricorrenti, comunque, avevano provveduto a richiamare le Conclusioni dell'Avvocato generale Cruz Villalon relative al rinvio pregiudiziale *Digital Rights Ireland*: le considerazioni svolte con riferimento alla DRD erano state ritenute del tutto applicabili anche alla normativa nazionale belga che trasponeva nell'ordinamento interno la disciplina europea e che adottava, similmente a quanto disposto a livello dell'UE, una forma di conservazione generalizzata ed indiscriminata[26].

Ebbene, affrontando tali delicate questioni, con Arret n. 84/2015, del 11 giugno 2015, la legge del 30 luglio 2013, così faticosamente e lentamente adottata dal legislatore belga, era stata dichiarata incostituzionale e dunque annullata con effetto retroattivo. Con una sentenza da alcuni[27] definita una pedissequa riproposizione della pronuncia *DRI*, nel frattempo adottata dalla CGUE, la Corte costituzionale stabiliva chiaramente che, sulla base di una "identité des motifs avec ceux qui ont amené la Cour de Justice de l'Union européenne à juger la directive conservation des données invalide, il y a lieu de constater que par l'adoption de l'article 5 de la loi attaquée, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52.1 de la Charte des droits fondamentaux de l'Union européenne" (par. B.10.3). La posizione della Corte, espressa nella

[24] Le ONG in realtà hanno ritenuto la normativa capace di compromettere anche – e conseguentemente alla ingerenza nei diritti alla vita privata e alla protezione dei dati – i diritti alla confidenzialità delle comunicazioni, il diritto alla libertà personale e alla libertà d'espressione, di riunione e di associazione, alla libertà di stampa, fino anche al diritto al giusto processo e ad un ricorso effettivo, nonché i principi di proporzionalità e di presunzione di innocenza.

[25] La normativa sulla conservazione infatti permetteva di memorizzare ed eventualmente poi accedere ai metadati relativi alle comunicazioni svolte dagli avvocati e medici, permettendo così di conoscere se e quando un avvocato è stato consultat e da chi – dunque risalire ai clienti –. In questo modo, pur non avendo accesso ai contenuti delle comunicazioni, risulterebbe nondimeno possibile trarre conclusioni sul rapporto sussistente tra avvocato e cliente. Ciò finirebbe pertanto col compromettere il segreto professionale, che rappresenta un principio generale prodromico al rispetto e alla garanzia dei diritti fondamentali; vengono così in particolar modo richiamati i diritti alla eguaglianza e alla non discriminazione tutelati dagli artt. 10 e 11 della Costituzione belga: la legge del 2013 infatti porterebbe al risultato di trattare in maniera identica situazioni differenti, che necessiterebbero di appropriate e specifiche misure. Gli artt. 10 e 11 inoltre risulterebbero lesi, più genericamente, dalla assenza di distinzione tra individui che sono legalmente indagati per la commissione di un crimine e coloro invece che non lo sono: i metadati di entrambi tali soggetti infatti risulterebbero sottoposti egualmente al medesimo obbligo di conservazione.

[26] Interessante è anche il richiamo alle sentenze, esaminate nel Capitolo II, Parte II, di varie Corti costituzionali quali quella cipriota, romena, bulgara e ceca, nonché in particolare del Tribunale costituzionale federale tedesco del 2 marzo 2010, avente ad oggetto la legge tedesca di trasposizione della DRD, a conferma di come "la conservation des données créait un sentiment diffus et continu de surveillance qui peut entraver le libre exercice des droits fondamentaux", par. A.2.9.

[27] F. VERBRUGGEN, S. ROYER, H. SEVERIJNS, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, in *European Law Blog*, 1 ottobre 2018, http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/.

sintetica affermazione riportata, si rivelava già sotto tale profilo opposta rispetto a quanto sostenuto dal Governo belga, intervenuto nel procedimento, che considerava la legge nazionale nettamente più limitata in termini di ingerenza nella sfera privata e maggiormente garantista rispetto a quanto disposto dalla Direttiva europea. La legge del 2013 infatti riconosceva espressi diritti agli utenti, quali quello ad essere informati della conservazione, ad accedere ai dati, ad ottenere rettifica e a proporre azione dinnanzi alla *Commission de la protection de la vie privée* o al tribunale di prima istanza; il periodo di conservazione risultava inoltre limitato a dodici mesi, mentre l'accesso era concesso solo a determinate categorie di soggetti[28]. Secondo il Governo la disciplina inserita nella legge non doveva pertanto essere ritenuta sproporzionata rispetto allo scopo perseguito, diversamente dalla posizione espressa dalle ricorrenti, le quali invece avevano lamentato la mancanza di una modulazione della durata della conservazione a seconda della tipologia di dati interessati, nonché l'assenza di qualsiasi riferimento e limitazione delle finalità di conservazione e accesso al solo perseguimento dei reati 'gravi'; ciò che le ONG avevano poi sottolineato quale aspetto fortemente problematico era l'impatto sui diritti fondamentali derivante dal regime di *bulk data retention* scelto, capace anche di modificare significativamente il rapporto tra autorità pubblica e cittadini e di creare una sensazione diffusa di controllo costante, "contraire à la conception générale partagée dans les démocraties occidentales selon laquelle la vie privée est considérée comme un droit de défense du citoyen à l'encontre de l'intrusion injustifiée dans sa vie privée par l'autorité" (par. A.9.2.1.1.).

Proprio su questo specifico punto la Corte costituzionale aveva mostrato di essere in accordo con la ricostruzione svolta dai ricorrenti, con una decisione che costituisce pressoché un unicum nel panorama europeo: "alors que les Cours constitutionnelles qui ont eu à connaitre de la validité des lois nationales transposant la Directive 2006/24 ont principalement annulé ces lois pour insuffisance de garantie procédurales, la Cour constitutionnelle belge énonce clairement qu'une obligation de conservation généralisée et indifférenciée des données de communication est contraire au principe de proportionnalité"[29]. I giudici belgi erano giunti quindi alla medesima conclusione espressa dalla CGUE nella sentenza *DRI*, affermando come sul fronte della disciplina della *data retention* "la loi attaquée ne se distingue nullement de la directive sur ce point" (B.10.1); le categorie di dati conservati erano identiche a quelle stabilite dalla DRD, così come, "tout comme la Cour de justice l'a constaté à propos de la directive, la loi s'applique également à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, aves les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel" (B.10.1)[30]. Non sussisteva quindi alcuna disposizione volta a promuovere una conservazione di tipo mirato e targettizzato sulla base dei soggetti coinvolti, della zona geografica interessata o del periodo di tempo, secondo i criteri stabiliti dalla CGUE, e non veniva neppure richiesta la sussistenza di alcuna correlazione tra la conservazione e accesso ai metadati e una minaccia alla sicurezza pubblica. Per tutte queste ragioni dunque la Corte aveva ritenuto che, con riferimento all'art. 5 della legge del 2013 – ovvero la disposizione che specificamente prevedeva la modifica dell'art. 126 della legge del 2005 –, il legislatore avesse ecceduto i limiti imposti dal rispetto del principio di proporzionalità e avesse violato anche gli artt. 10 e 11 della Costituzione belga, volti a riconoscere i diritti alla eguaglianza e alla non discriminazione, letti in combinazione con gli artt. 7, 8 e 52 della Carta di Nizza. Considerato poi che tutte le disposizioni della legge impugnata risultavano correlate e strettamente dipendenti all'art. 5,

[28] Par. A.5.5.

[29] F. COUDERT, F. VERBRUGGEN, *Conservation des données de communications électronique en Belgique: un juste équilibre?*, in V. FRANSSEN, D. FLORE (a cura di), *Societé numerique et droit penal*, Bruylant, 2019, p. 248.

[30] Viene inoltre evidenziato come "Il ressort des travaux préparatoires de la loi attaquée que le législateur a entendu adapter la terminologie employée afin de la rendre compatible avec la directive 2006/24/CE, les catégories de fournisseurs visées par la loi correspondant à celles énumérées par ladite directive (Doc. parl., Chambre, 2012-2013, DOC 53-2921/001, p. 12)", par. B.8.

l'intera legge era stata infine dichiarata incostituzionale e annullata, senza che vi fosse bisogno di esaminare peraltro le ulteriori doglianze presentate dai ricorrenti.

Questa decisione, accolta con entusiasmo da numerose ONG, era stata in realtà per certi aspetti criticata dalla dottrina, che aveva ritenuto il vaglio della Corte costituzionale troppo 'ossequioso' verso la posizione espressa dalla CGUE, avendo invece tenuto troppo poco in considerazione le peculiarità da un lato della disciplina belga e dall'altro delle doglianze mosse dalle parti ricorrenti. Ritenendo che gli aspetti di similarità con l'invalidata DRD fossero sufficienti a determinare l'incostituzionalità stessa della normativa di trasposizione, i giudici nazionali avevano mancato oltretutto di considerare i criteri stabiliti dall'art. 15 della Direttiva *e-Privacy*, ovvero l'unica normativa europea di riferimento in assenza dell'ormai invalidata DRD, e che sarebbe divenuta pertanto la base e il fondamento di qualsiasi nuova normativa nazionale in materia di conservazione dei dati. Affrontare tali aspetti specifici, anziché effettuare una sorta di "copia-incolla" della sentenza *DRI*, avrebbe permesso ai giudici di fornire indicazioni che avrebbero potuto rivelarsi preziose ed utili per il legislatore nazionale nella difficile predisposizione della disciplina della *data retention* per scopi securitari[31]. I giudici belgi insomma, pur arrivando al medesimo esito già raggiunto da altre Corti nazionali, si erano, diversamente da queste, fermati alle considerazioni relative alla conservazione generalizzata ed indiscriminata, senza addentrarsi in una ulteriore e precisa analisi circa l'eventuale carenza di altri requisiti nella successiva fase di accesso, sulla quale poco o nulla viene detto.

Quali che siano le considerazioni e valutazioni ultime quanto alla pronuncia della Corte costituzionale[32], essa aveva comunque certamente determinato la necessità di un ulteriore intervento normativo a livello nazionale, che andasse nuovamente a disciplinare la delicata materia della conservazione dei metadati, vista dal Governo come imprescindibile ed insostituibile strumento di lotta alla criminalità ma che doveva ora confrontarsi con i principi stabiliti dalla giurisprudenza europea e nazionale. Ecco quindi che il legislatore belga, anche sulla base delle richieste e necessità espresse dalle autorità di *law enforcement*, si era mosso con grande rapidità già all'indomani della sentenza del 2015: a seguito della dichiarazione di incostituzionalità infatti tornava in vigore, quale unica disposizione applicabile, la previa versione dell'art. 126 della legge del 13 giugno 2005 – ovvero nel suo dettato precedente alle modifiche apportate dalla legge del 2013 – nonché l'*Arret royal* del 19 settembre 2013. Con riferimento a quest'ultimo infatti è bene precisare come "Aprés l'annulation d'une loi par la Cour

[31] Come ben sottolineato da Naudts, "the GwH [Corte costituzionale belga] could have taken this opportunity to expand upon the CJEU's reasoning. (..) The GwH saw no further need to examine or clarify the law's impact on the other fundamental rights that had been invoked by the applicants, such as the rights to freedom of expression and fair trial. When a future law is drafted, it is highly likely that the potential infringement of these rights will nonetheless remain a point of contention", L. NAUDTS, *Belgian Constitutional Court nullifies Belgian Data Retention Law*, in *European Data Protection Law Review*, 3, 2015, p. 210. Lo stesso autore sottolinea come anche la dichiarata violazione dei diritti all'eguaglianza e alla non discriminazione non siano stati in realtà accompagnati da una chiara argomentazione.

[32] Come riportato da Naudts, non tutti hanno accolto con favore la decisione della Corte costituzionale: "on the side of the judiciary, Investigative Judge Philippe Van Linthout referred to the judgement as 'a black day for justice'. His concern that judicial authorities had lost an important weapon in the battle against crime was shared by Belgium's Attorney Generals and Federal Prosecutor. Indeed, in Belgium, 90% of all judicial investigations rely upon data retained by telecom operators", L. NAUDTS, *Belgian Constitutional Court nullifies Belgian Data Retention Law*, op. cit., p. 211. Oltretutto si poneva il problema di determinare le sorti delle prove raccolte sulla base della legge dichiarata incostituzionale e utilizzate in procedimenti già avviati. Alcune Corti infatti avevano risolto tale criticità ritenendo illegale la conservazione dei metadati ma non la richiesta di accesso ad essi, che quindi risultava legittima, mentre altre avevano ritenuto valide le prove ottenute mediante conservazione dei metadati e accesso agli stessi qualora ottenute sulla base dell'art. 126 nella sua versione antecedente alla modifica apportata dalla legge del 2013. Per una analisi più completa delle decisioni assunte dai giudici nazionali con riferimento alle prove ottenute sulla base della normativa nazionale in materia di *data retention* poi dichiarata incostituzionale, si rimanda a: C. FIEVET et al., *Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information*, in *Revue du droit des technologies de l'information*, 68-69/2017, p. 125.

constitutionnelle, les actes réglementaires pris sur la base de la norme annulée demeurent dans l'ordre juridique, mais ils sont en sursis. En clair, l'annulation n'affecte pas comme telle l'existence de ces actes et décisions, leur validité pouvant toutefois être remise en cause par l'autorité administrative ou juridictionnelle qui les a adoptés"[33]. Si componeva così un quadro piuttosto confuso e frammentato in diverse normative, che necessitavano quindi di maggiore chiarezza e di una sistemazione coerente.

2.2. – Un nuovo difficile compito per il legislatore belga: l'adozione della legge del 2016 come soluzione di compromesso tra efficienza ed elevati standard di tutela dei diritti fondamentali

La delicatezza della disciplina, che già era emersa dalle criticità riscontrate nel lungo percorso che aveva portato alla approvazione della legge del 2013, unitamente alle posizioni complesse espresse dai giudici europei nonché nazionali, avevano reso estremamente articolato e vivo il dibattito relativo alla nuova normativa da adottare. Gli studi e le analisi svolte in sede di elaborazione del testo normativo, come emerge con chiarezza dai *Travaux préparatoires*, avevano messo chiaramente in luce la difficoltà di coniugare efficienza ed utilità dello strumento della *data retention* con i criteri indicati in primis dalla CGUE. Come già evidenziato con riferimento ad altri Stati membri e come sollevato nell'ampia discussione sviluppatasi a livello dell'UE, anche il legislatore belga aveva espresso la consapevolezza che la normativa nazionale non poteva soddisfare esattamente e congiuntamente tutti i requisiti imposti dalla giurisprudenza europea che, se intesi come necessari nella loro totalità, avrebbero finito col vanificare la stessa misura della conservazione dei metadati. Nel Doc. par. Chambre, 2015-2016, DOC 54-1567/001, nel quale sono riportate le considerazioni svolte dal Governo e il dibattito in sede parlamentare, si leggeva come, con riferimento alla conservazione targettizzata "après analyse approfondie, (..) il n'est pas possible d'opérer une différenciation a priori de cet élément. (..) Limiter la conservation des données à celles concernant des personnes qui font déjà l'objet d'une enquête pénale ou de renseignement n'a pas de sens car cette possibilité existe déjà par ailleurs" (par. 7). Vagliando poi i singoli elementi indicati dalla CGUE come fondamentali e determinanti una conservazione mirata – quali appunto limitazione temporale, dei soggetti e della area geografica – emergeva con chiarezza come essi risultassero inefficaci e concretamente irrealizzabili: ad esempio la determinazione di un periodo di tempo specifico poteva essere adottata in caso di situazioni particolari e minacce temporanee all'ordine pubblico ma difficilmente si poteva applicare alla grande maggioranza di situazioni per le quali non era invece possibile stabilire anticipatamente un lasso temporale specifico di riferimento (si pensi alla minaccia di un attentato terroristico, per il quale è pressoché impossibile indicare un periodo di tempo durante il quale la conservazione si possa rivelare utile); la individuazione poi di soggetti e di aree territoriali delimitate rispetto alle quali effettuare una conservazione mirata comportava il rischio concreto e grave di giungere a pericolose discriminazioni.

Punto centrale sul quale il legislatore belga concentrava la propria attenzione era poi il fatto che né i giudici di Lussemburgo né tantomeno i giudici nazionali avevano chiarito se i criteri e requisiti fissati relativamente alle due fasi di conservazione e accesso ai metadati dovessero essere intesi cumulativamente: proprio su questo specifico aspetto – che, come si vedrà, sarà ribadito con forza dallo stesso Governo belga nelle successive vicende giurisprudenziali che coinvolgeranno la normativa stessa – si fondava l'intero approccio normativo in materia di *data retention*. Anziché individuare nella giurisprudenza europea – e, di riflesso, in quella nazionale – la dichiarazione di una incompatibilità con i diritti fondamentali e, dunque, un divieto assoluto di adozione di forme di conservazione generalizzata ed indiscriminata, il legislatore aveva piuttosto ritenuto che tale disciplina fosse illegittima solo laddove

[33] C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, op. cit., p. 234.

non accompagnata da una regolamentazione dell'accesso rispettosa dei requisiti indicati nella sentenza *DRI*, cioè quando tutti i criteri indicati – attinenti tanto alla conservazione quanto all'accesso – fossero contemporaneamente assenti. Una disciplina più restrittiva e rigida della fase di accesso sarebbe stata in grado di compensare[34] dunque un regime più ampio e permissivo quanto alla conservazione[35].

Perplessità e critiche ad una simile lettura erano però state avanzate da alcune ONG, tra cui Datapanik, Liga voor Mensenrechten e Ligue des droits de l'Homme[36], che avevano invece rinvenuto nella nuova normativa la pericolosa riproposizione di una *bulk data retention*, considerata *per se* illegittima e sproporzionata, indipendentemente dalla disciplina dell'accesso. Sotto un profilo più generale poi veniva sottolineato come la stessa utilità ed efficacia del regime di conservazione dei dati, affermata dal Governo, non fosse in realtà fondata e supportata da studi e statistiche; le ONG, invece citavano alcune analisi e ricerche dalle quali emergeva non solo la forte invasività di strumenti di conservazione generalizzata, anche laddove limitata ai soli metadati e dunque ad esclusione del contenuto, ma anche la mancanza di prove concrete che tali sistemi avessero realmente avuto un significativo effetto positivo nella lotta alla criminalità[37]. Per questi motivi le ONG chiedevano una rinuncia definitiva a tali strumenti di sorveglianza massiva.

Nonostante le serie critiche rilevate e le difficoltà riscontrate nel predisporre un testo normativo che fosse compatibile con la giurisprudenza europea, il legislatore belga, sulla base delle riflessioni emerse dai lavori preparatori, riteneva infine di aver trovato un corretto equilibrio tra efficienza e rispetto dei diritti fondamentali[38], giungendo alla approvazione della legge del 29 maggio 2016[39] in materia di raccolta e conservazione dei metadati, recante disposizioni a modifica della legge del 13 giugno 2005.

Un esame attento di questa disciplina risulta di fondamentale importanza almeno per tre ordini di motivi: innanzitutto al fine di comprendere l'impatto che la giurisprudenza della CGUE e, successivamente, della Corte costituzionale, avevano prodotto e per rilevare dunque le modifiche e le scelte operate dal legislatore in questo delicato campo, alla luce di tali importanti interventi giurisprudenziali; ciò consentirà di mettere a fuoco l'approccio belga alla disciplina della *data retention* ovvero la soluzione normativa individuata dal legislatore come compatibile ai numerosi criteri affermati

---

[34] Questo termine viene oltretutto impiegato anche dalla *Commission pour la protection de la vie privée*, che afferma come "aucun des deux arrets ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrets ne peut pas etre retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects", *Doc. parl.*, Chambre, 2015-2016, doc. 54, 1567/001, p. 13.

[35] Di estremo rilievo è la considerazione svolta proprio su questo delicato punto relativo all'interpretazione della giurisprudenza europea e nazionale in materia di *data retention*: "Ni l'arret de la Cour constitutionnelle ni celui de la Cour de justice de l'Union européenne ne concluent toutefois qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si tel était le cas, et l'absence de différenciation entre les personnes constituant l'élément essentiel de la législation nationale et européenne annulée, on peut penser que la Cour de justice et la Cour constitutionnelle auraient uniquement examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments", par. 7, lett. c).

[36] Nel documento *Avis de Datapanik, la Liga voor Mensenrechten, la Ligue des droits de l'Homme et la NURPA concernant le projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques*, del 2 febbraio 2016.

[37] Vengono ad esempio citati gli studi elaborati dal Massachusetts Institute of Technology, *Reality mining: sensing complex social systems*, 2005; lo studio del 2011 svolto dal Centro Studi del Bundestag (*Die praktischen auswirkungen der vorratsdatenspeichrung auf die entwicklung der aufklarungsquoten in den EU-mitgliedsstaaten*), nonché uno studio del Dipartimento di criminologia del Max Planck Institute del 2012 (*Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*).

[38] "Le législateur indiqua intégrer, *dans la mesure du possible*, les critiques adressées par la CJUE et par la Cour constitutionnelle" (enfasi aggiunta), C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, op. cit., p. 237. È ciò che peraltro si legge anche nei *Doc. parl.*, Chambre, 2015-2016, doc. 54, 1567/001, p. 76.

[39] *Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques*, M.B. 18 juillet 2016.

dai giudici di Lussemburgo con riferimento alla DRD e riaffermati – e trasposti – poi dai giudici nazionali nella disciplina interna. Le valutazioni e le nuove indicazioni presenti nella legge del 2016 debbono essere lette come frutto della riflessione innescata dall'intervento giurisprudenziale europeo e delle sue ricadute sul piano interno e rappresentano dunque il primo sforzo di applicare nell'ambito della conservazione dei metadati i requisiti di proporzionalità e necessità che, letti alla luce della sentenza *DRI*, imponevano di restringere e meglio delimitare l'ingerenza nella sfera privata rappresentata sia dalle operazioni di conservazione che di accesso. L'esame della normativa belga poi risulta fondamentale per poter comprendere appieno il successivo intervento della Corte costituzionale e dunque i motivi del rinvio pregiudiziale di cui già si è accennato nel Capitolo IV, Parte II e rispetto al quale sono state analizzate le posizioni dell'Avvocato generale Campos Sanchez-Bordona.

2.3. – Le caratteristiche della disciplina normativa del 2016 tra conferma di una conservazione generalizzata e maggiori salvaguardie e restrizioni nella fase di accesso

Ecco quindi che analizzando la legge del 2016, si nota innanzitutto come il legislatore sia principalmente intervenuto l'art. 126 della legge del 13 giugno 2005, modificandolo totalmente, nonché intervenendo su alcune disposizioni del *Code d'instruction criminelle* e sulle normative che regolano le attività delle autorità di intelligence e di *law enforcement*. Partendo dunque dall'art. 126 che, come si ricorda, era già stato toccato dalla legge del 2013 poi dichiarata incostituzionale, viene ribadito come i fornitori di servizi di telecomunicazioni pubbliche ("operateur") debbano conservare i dati generati o trattati nell'ambito di fornitura dei propri servizi, ad esclusione dei contenuti delle comunicazioni. Il comma 2 poi elenca specificamente le autorità che, sulla base di una semplice richiesta ai fornitori, possono ottenere l'accesso ai dati conservati, limitatamente ed unicamente però agli scopi indicati: le autorità giudiziarie per finalità di ricerca, accertamento e perseguimento di reati; i servizi di intelligence e sicurezza per la raccolta di informazioni sulla base della legge del 30 novembre 1988 che ne regola appunto le attività; gli ufficiali di polizia giudiziaria dell'*Institut belge des services postaux et des télécommunications* (IBPT)[40] per la ricerca, accertamento e perseguimento di reati che costituiscono violazione delle norme di sicurezza delle reti di telecomunicazione; i servizi di emergenza nel caso in cui venga richiesto il loro intervento per una situazione di pericolo e questi non riescano ad ottenere dati completi o esatti circa il soggetto che ha effettuato la chiamata o l'ubicazione dello stesso; e ancora l'Ufficiale di polizia giudiziaria appartenente alla *Cellule des personnes disparues de la Police Fédérale* per operazioni di soccorso o ricerca di persone scomparse ed infine il *Service de médiation pour les télécommunications* che può però accedere solo ai dati identificativi e unicamente con l'obiettivo di identificare persone che abbiano fatto uso illecito di reti Internet o servizi di telecomunicazione. Sotto questo profilo e diversamente dalla disciplina del 2013, il legislatore ha mostrato una particolare attenzione nella determinazione, con un alto livello di precisione, dei soggetti autorizzati all'accesso e delle finalità per le quali tale ingerenza è consentita, nonché, come si vedrà, della procedura da seguire; sebbene quindi siano state colmata alcune delle lacune della previa normativa, che peraltro proprio sotto tali profili era stata reputata particolarmente insidiosa ed oggetto di critiche da parte della dottrina e della *Commission de la protection de la vie privée*, nonché dalla stessa Corte costituzione nella sua sentenza, deve comunque essere sottolineato come gli scopi e le autorità autorizzate, per quanto precisi, risultino

[40] "L'IBPT est le régulateur fédéral compétent pour le marché des communications électroniques, le marché postal, le spectre électromagnétique des radiofréquences et la radiodiffusion sonore et télévisuelle dans la Région de Bruxelles-Capitale" (https://www.ibpt.be/consommateurs/l-ibpt); tale Istituto può imporre sanzioni amministrative laddove constati, nello svolgimento e nei limiti dei propri compiti di vigilanza e controllo, il verificarsi di condotte contrarie alla legge. I suoi poteri e prerogative sono inseriti nel Capitolo II della legge 13 giugno 2005 e successive modifiche.

piuttosto numerosi così che i rischi di abusi si ampliano insieme ai dubbi quanto alla rispondenza della disciplina al principio di stretta necessità.

La durata della conservazione viene identificata in dodici mesi per tutte le tipologie di dati (dati d'identificazione, dati relativi all'accesso, alla connessione alla rete, all'ubicazione e i dati di comunicazione). Viene anche in questo caso però lasciato al Re, sulla base di una delibera del Consiglio dei Ministri[41], il compito di determinare con precisione la tipologia di dati da sottoporre a conservazione a seconda delle singole categorie di dati.

Il comma 4 dell'art. 126 poi prevede alcuni importanti obblighi in capo agli operatori di servizi di telecomunicazione, i quali sono tenuti a garantire ai dati conservati standard di sicurezza e tutela parificabili a quelli garantiti dai dati in rete, a predisporre misure tecniche ed organizzative volte a proteggere i dati conservati da qualsiasi rischio di accesso illecito o di abuso nonché a conservare i dati entro i confini dell'Unione europea. Su quest'ultimo punto, diversamente da quanto si è visto con riferimento alla normativa tedesca analizzata nella Parte II, Capitolo II[42], il legislatore belga ha valutato sufficientemente tutelante prevedere una *data retention* nei limiti del territorio dell'UE e non necessariamente e più restrittivamente nel solo territorio nazionale. Viene comunque imposto l'obbligo di distruzione dei dati conservati una volta scaduto il termine stabilito di dodici mesi, unitamente alla garanzia di tracciabilità dell'utilizzo dei dati, che trova realizzazione in un apposito registro nel quale debbono essere indicate tutte le richieste di accesso ai dati avanzate dalla autorità pubbliche sopra elencate. Questo consentirà, oltre ad un controllo preciso, anche di predisporre studi statistici relativi alla *data retention*, che dovranno essere presentati dal Ministro della Giustizia alla Camera dei rappresentanti e che permetteranno di ricostruire un quadro puntuale circa i casi in cui sono state effettuate le richieste di accesso nonché, elemento molto importante, il tempo trascorso tra la data di inizio della conservazione del metadato e il momento in cui la domanda di accesso è stata avanzata. Questo al fine evidente di poter valutare, ed eventualmente agire di conseguenza, se il termine di conservazione di dodici mesi sia da considerarsi appropriato e proporzionato o se invece esso risulti troppo esteso rispetto alla reale necessità delle autorità di intelligence e *law enforcement*.

La disciplina della conservazione ed accesso ai metadati sopra descritta viene poi coordinata con ulteriori e necessarie modifiche al *Code d'instruction criminelle* (Codice di Procedura Penale): la legge del 2016 infatti prevede un intervento rispetto agli artt. 46bis e 88bis del *Code*, inserendo alcune importanti indicazioni relative alle condizioni di accesso ai metadati. L'elemento fondamentale da rilevare ed evidenziare in queste previsioni è da individuarsi nell'esistenza di una modulazione della possibilità di accesso a seconda della gravità dei reati perseguiti e della tipologia di dati interessati. L'art. 46bis infatti stabilisce che per scopi di indagine relative a delitti – genericamente intesi, dunque senza che abbiano necessariamente carattere di gravità – il Procuratore del Re può avanzare richiesta ai fornitori di servizi di telecomunicazione al fine di ottenere l'accesso ai dati d'identificazione relativi ad un abbonato o di identificazione dei servizi di comunicazione elettronica di cui un determinato soggetto sia utente. Tale accesso tuttavia deve essere accompagnato da una decisione del Procuratore stesso che sia scritta, motivata e proporzionata, cioè rispettosa quanto più possibile del diritto alla vita privata e avente carattere di sussidiarietà nello specifico contesto dell'indagine svolta. La richiesta di accesso da parte degli ufficiali di polizia giudiziaria può invece essere effettuata solo in casi di estrema urgenza e comunque sempre sulla base di un previo accordo verbale con il Procuratore e di una decisione motivata e scritta. Con riferimento alla sopra richiamata tipologia di dati, che potremmo genericamente definire

[41] Viene anche disposto il previo parere da parte della *Commission de la protection de la vie privée* e dell'*Institut belge des services postaux et des télécommunications* (art. 126, co. 3).

[42] Come si è visto nel Capitolo II, Parte II, la Germania ha adottato nel 2015 una specifica normativa in materia di conservazione dei dati, la *Gesetz zur Einfuhrung einer Speicherflicht und einer Hochstspeicherfrist fur Verkehsdaten*, del 26 ottobre 2015, nella quale è stato imposto l'obbligo in capo ai fornitori di servizi di telecomunicazione di conservare i metadati esclusivamente entro i confini nazionali.

come dati di identificazione, viene specificato come per i reati per i quali è prevista una detenzione correttiva di un anno o una pena superiore, possano essere richiesti dal Procuratore (o in casi di urgenza, come si è detto, dalla polizia giudiziaria) solo i dati risalenti ad un massimo di sei mesi precedenti alla richiesta.

All'art. 88 bis poi è stabilito che, qualora sussistano indizi gravi di reati per i quali è stabilita una detenzione di un anno o pena superiore e laddove tali informazioni siano necessarie per stabilire la verità dei fatti, l'autorità giudiziaria ovvero, nello specifico, il giudice istruttore, potrà richiedere l'accesso ai dati relativi al traffico e i dati sulla localizzazione. Per queste informazioni, considerate maggiormente intrusive nella sfera privata, quindi la domanda deve essere effettuata solamente dal giudice e deve comunque essere correlata da una ordinanza motivata che determini le ragioni per le quali la richiesta è stata avanzata, la proporzionalità della richiesta stessa e l'efficacia temporale della domanda, che non potrà comunque essere superiore a due mesi dalla data dell'ordinanza medesima. Anche in questo caso però la possibilità di andare 'indietro nel tempo' viene differenziata sulla base della severità del reato al quale le indagini si riferiscono: per i reati di cui al libro II, titolo I ter del *Code pénal*[43], i dati richiesti possono riguardare un termine di tempo fino a dodici mesi prima dell'ordinanza, mentre per i reati indicati nell'art. 90 ter, par. 2 a 4 o per i reati perpetrati nel contesto di una organizzazione criminale (art. 324 bis) o ancora per quei reati per i quali è prevista una detenzione di cinque anni o pena superiore, i dati sono quelli attinenti ad un massimo di nove mesi prima dell'ordinanza; infine per tutti gli altri reati rientranti nella categoria indicata dalla disposizione in esame – ovvero quelli per i quali è comunque stabilita una detenzione superiore ad un anno – i dati possono riguardare i soli sei mesi precedenti alla richiesta. Viene precisata però anche una limitazione quanto ai mezzi di comunicazione elettronica impiegati da avvocati o medici e dunque soggetti sottoposti a segreto professionale: le norme disposte e sino ad ora analizzate riguardanti l'accesso, infatti, non valgono per queste categorie di soggetti, i cui dati possono essere richiesti solo nei casi in cui sussista il sospetto che i professionisti abbiamo compiuto reati punibili con almeno un anno di detenzione o abbiano concorso alla commissione degli stessi reati o ancora terzi sospettati della commissione di reati abbiano utilizzato i mezzi di comunicazione relativi a questi soggetti[44].

Ciò che infine si vuole sottolineare è la modifica apportata alla legge organica del 30 novembre 1998 sui servizi di intelligence, nella quale vengono inserite alcune specifiche condizioni per l'accesso ai metadati: è necessaria una previa decisione del dirigente del servizio di intelligence che stabilisca il metodo di accesso ai dati e, laddove possibile, le persone, associazioni, gruppi, luoghi o eventi interessati all'accesso, nonché la minaccia potenziale e la durata delle operazioni; anche in questo caso è riproposta una gradazione temporale che prevede la possibilità di richiesta di dati relativi sino a sei mesi prima della decisione per minacce derivanti da attività di criminalità organizzata; sino a dodici mesi per minacce derivanti da attività di terrorismo o estremismo e, in via residuale, sino a nove mesi per tutte le altre tipologie di minacce potenziali che rientrano nelle competenze dei servizi di intelligence. Si comprende dunque come anche per le autorità di intelligence sia previsto l'obbligo di fondare le proprie richieste e l'accesso stesso su di una minaccia specifica ed individuata, e comunque effettuando un vaglio basato su parametri oggettivi, così che l'ingerenza risulti quanto più possibile limitata allo stretto necessario[45].

---

[43] Tale Titolo è specificamente dedicato alle "Infractions terroristes".

[44] Anche in quei casi in cui l'accesso è consentito sono poi comunque previste apposite e specifiche tutele, quali l'informazione preventiva da parte del giudice istruttore dell'ordine degli avvocati o dell'ordine dei medici (art. 88bis, comma 3).

[45] Nei lavori preparatori sopra già citati, il legislatore aveva indicato come, con riferimento alla disciplina della conservazione e accesso ai dati da parte di autorità di intelligence, fosse necessario che: "les méthodes ordinaires s'avèrent insuffisantes pour récolter les informations nécessaires à une mission de renseignement (subsidiarité), il y a une menace potentielle, elles sont proportionnelles au degré de gravité de la menace, la décision du chef du

Dalla analisi svolta con riferimento alle principali modifiche introdotte con la legge del 2016, si nota con evidenza come accanto alla conferma di una forma di conservazione che mantiene i caratteri propri di *bulk data retention* ovvero di conservazione generalizzata ed indiscriminata, vengano tuttavia aumentate le salvaguardie quanto alla fase di accesso: sono stabiliti elenchi specifici – per quanto piuttosto ampi – di soggetti autorizzati a richiedere l'accesso e di scopi per i quali l'accesso può essere concesso; sono previste tutele preventive e salvaguardie da possibili abusi mediante l'obbligo di predisporre richieste scritte e motivate che devono contenere indicazioni precise soprattutto quanto alla proporzionalità e necessità dell'ingerenza. Vengono previste condizioni differenti di accesso, tenendo in considerazione le categorie di dati interessati e l'ampiezza del periodo di disponibilità degli stessi; non viene invece stabilita alcuna deroga alla regola generale della conservazione, che resta identificata in dodici mesi: ciò che varia è solo fino a quanto 'indietro nel tempo' possono giungere le autorità richiedenti nella successiva fase di accesso e le condizioni procedurali che debbono essere rispettate. Risulta pertanto chiara ed evidente la concretizzazione di quanto già emerso dai lavori preparatori, secondo cui le condizioni stabilite dal giudice dell'UE non devono intendersi come obbligatoriamente sussistenti cumulativamente, risultando invece sufficiente che una maggiore ingerenza nella fase di conservazione venga compensata da maggiori tutele nella fase di accesso.

Nonostante tale sforzo normativo e quasi fosse un passato destinato a ripetersi, a pochi mesi dall'approvazione della nuova legge in materia di *data retention*, la disciplina belga si è ancora una volta venuta a scontrare con gli avvenimenti caratterizzanti il livello dell'UE e, in particolare, nuovamente, con la posizione espressa dalla CGUE. Risale infatti al dicembre 2016 la pronuncia *Tele2*, nella quale, come si è ampiamente analizzato, i requisiti e principi riguardanti la conservazione e l'accesso ai metadati per scopi securitari sono stati riaffermati, confermando la posizione già espressa nella sentenza *DRI* e anzi chiarendo taluni aspetti con specifico riferimento al dibattuto art. 15 Direttiva *e-Privacy* e conseguentemente con espresso riferimento alle normative nazionali determinanti obblighi di conservazione dei metadati per scopi securitari.

Il nuovo intervento dei giudici di Lussemburgo, che è andato nella direzione di confermare l'incompatibilità con il diritto dell'UE e, in particolare, con la Carta di Nizza, di una forma di conservazione generalizzata ed indiscriminata, non è così passato inosservato neppure in Belgio ed ha anzi riconfermato e ravvivato i dubbi e le criticità che già nella fase di predisposizione della normativa del 2016 erano stati messi in evidenza e denunciati da talune ONG così come da parte della dottrina[46]. La normativa nazionale poco prima adottata è stata così messa in discussione sotto il profilo della sua

service est écrite et motivée. *Ces conditions impliquent que les services de renseignement doivent, pour chaque méthode, justifier le lien entre la cible et la menace*", par. 9, enfasi aggiunta.

[46] Forget ad esempio rileva come il periodo di conservazione imposto dalla normativa belga, della durata – salvo disposizioni particolari come si è visto – di dodici mesi, non rispetti i requisiti di proporzionalità e necessità: le statistiche elaborate da IBPT (Institut belge des services postaux et des télécommunications, *Informations statistiques: conservation des données pour 2014 et 2015*, del 27 settembre 2016) avevano infatti mostrato come la maggioranza dei metadati richiesti dalle autorità di *law enforcement* risalissero ai tre mesi precedenti. Sulla base di tali studi, pareva quindi piuttosto incongruente e sproporzionato attestare la durata della *data retention* al quadruplo di quanto generalmente necessario e quanto solitamente richiesto ed impiegato. C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, op. cit., p. 239. La stessa autrice poi sottolinea un ulteriore aspetto di interesse: ai sensi degli artt. 122 e 123 della medesima legge del 13 giugno 2015, i fornitori di servizi di telecomunicazione erano autorizzati a conservare i metadati derivanti dalle comunicazioni effettuate dai propri utenti, per mere finalità di marketing o di fatturazione. Tali dati risultavano accessibili dalle autorità giudiziarie mediante richiesta alle condizioni previste dagli artt. 46bis e 88bis del *Code d'instruction criminelle*. Tuttavia "celles-ci n'étant pas répertoirées ou listées par les operateurs, il n'est pas possible de déterminer si les données conservées en vertu des articles 122 et 123 de la loi du 13 juin 2005 diffèrent de celles traitées et conservées en vertu de son article 126. Dans l'hypothèse où ces données ne se recouperaient pas, il eut été intéressant de déterminer l'intérêt des données collectées à des fins de facturation dans le cadre d'enquêtes pénales et en conséquence, la réelle nécessité d'imposer la conservation de données supplémentaires aux opérateurs", p. 239.

compatibilità con il diritto dell'UE: agli inizi di gennaio 2017 è stato infatti promosso un ricorso per annullamento dinnanzi alla Corte costituzionale, che ha visto quali ricorrenti, ancora una volta, l'Ordre des barreaux francophones et germanophone, nonché l'associazione dei professionisti operanti nell'ambito fiscale (Academie Fiscale), insieme ad alcuni cittadini e ONG (non a caso le medesime Liga voor Mensenrechten e Ligue des Droits de l'Homme che avevano sollevato così tante obiezioni quanto al progetto di legge).

3. Il dialogo tra **Cour constitutionnelle** *e CGUE: i rinvii pregiudiziali in materia di* **data retention** *e* **PNR**

3.1. – La forza dirompente della sentenza **Tele2***: l'ulteriore intervento del giudice costituzionale belga e le diverse interpretazioni dei criteri individuati dai giudici di Lussemburgo*

A seguito della sentenza *Tele2*, la condanna a forme di conservazione dei metadati di tipo generalizzato ed indiscriminato, espressa in termini più chiari, sebbene, come si è visto, non del tutto scevri da dubbi interpretativi, ha portato a sollevare notevoli perplessità quanto alla conformità della normativa belga del 2016 al diritto dell'UE, così come interpretato dalla CGUE. La disciplina nazionale, come si è visto, pur avendo inserito migliorie e maggiori tutele rispetto alle previgenti disposizioni del 2013, non poteva infatti ritenersi conforme a quei criteri e requisiti di targettizzazione – sotto il profilo temporale, soggettivo e geografico – indicati dai giudici di Lussemburgo. Proprio sulla base di tali considerazioni ed aspetti critici della legge del 2016 si fondavano i motivi del ricorso alla Corte costituzionale belga: pur essendo intervenuto con significative modifiche sulla disciplina dell'accesso, il legislatore, sotto il profilo della conservazione dei metadati, non aveva in alcun modo modificato il proprio approccio rispetto alla legge del 2013, dichiarata incostituzionale. Entrambe le normative del 2013 e del 2016, infatti, prevedevano una conservazione di tipo generalizzato ed indiscriminato, e, mentre è stata certamente stabilita una forma di modulazione per quanto attiene all'accesso e dunque, come si è già messo in rilievo, alla capacità di andare indietro nel tempo, che risulta più o meno estesa a seconda della gravità del reato e dello scopo per il quale l'accesso viene richiesto, nessun intervento è stato svolto quanto alla previsione di una gradazione e modulazione della durata della conservazione dei metadati sulla base della categoria di tali informazioni e della loro possibile utilità per l'obiettivo perseguito (par. A.3.4).

L'estensione della *data retention* non poteva, a parere dei ricorrenti, essere giustificata neppure da quanto sostenuto dal Governo belga, ovvero che la generalizzazione della conservazione vada a tutto beneficio delle vittime del reato, che meritano di essere tutelate, anche indirettamente, mediante la predisposizione di tecniche di indagine che consentano una lotta più efficace alla criminalità[47], così come dello stesso sospettato che, proprio grazie ad una conservazione ampia e dunque ad una maggiore disponibilità di informazioni, potrebbe essere infine scagionato da ogni accusa. Sul punto i ricorrenti hanno affermato come "la justification apportée par le législateur à cet égard ne peut convaincre puisque le droit pénal repose sur le principe de présomption d'innocence avec pour corollaire que la charge de la preuve repose sur le ministère public (..). Il ne serait dès lors pas pertinent d'invoquer le fait que la mesure peut tout aussi bien bénéficier à la victime d'une infraction" (par. A.3.5)[48]. Similmente a quanto

[47] Il Governo aveva sostenuto che "la recherche de la vérité est dans l'intérêt tant de la victime et de l'accusé (qui pourra par exemple démontrer qu'il se trouvait ailleurs au moment des faits) que de toutes les autres personnes concernées", par. B.20.1., sottolineando peraltro come le altre finalità previste a motivazione della conservazione dei metadati (ad esempio nel caso di ricerca di persone scomparse o in caso di chiamate d'emergenza) imponessero un diverso ragionamento ed una differente valutazione circa la proporzionalità dell'ingerenza.

[48] Sotto il profilo degli ulteriori scopi e benefici che possono derivare, secondo l'interpretazione del Governo belga, da un regime di conservazione generalizzata, viene sottolineato come nella sentenza *Tele2* i giudici europei

già rilevato nel dibattito dottrinario apertosi a livello europeo, è stata anche fortemente criticata dai ricorrenti la mancanza di un concreto vaglio circa la reale utilità ed efficacia di forme di *bulk data retention* e dunque sulla necessità di sottoporre l'intera popolazione belga ad una forma di sorveglianza totalmente sproporzionata rispetto all'obiettivo da raggiungere (par. A.3.5)[49]. Oltre ai pericoli per i diritti alla vita privata e alla protezione dei dati, i ricorrenti hanno rilevato anche rischi per il diritto alla libertà di espressione: la combinazione della legge del 2016 e di quella del 1998 che regola le attività dei servizi di intelligence potrebbe comportare rischi di abuso di potere, a detrimento anche della categoria dei giornalisti, con il possibile risultato di "renforcer l'autocensure chez le citoyen qui a le vague sentiment d'être surveillé, ce qui peut avoir un impact sur l'exercice de sa liberté d'opinion et d'information et constituer de la sorte une ingérence par rapport à l'article 11 de Charte des droits fondamentaux de l'Union européenne" (par. A.18.4). Sotto questo profilo viene poi evidenziato come non solo non sia stato stabilito un appropriato previo controllo da parte di una autorità amministrativa indipendente ma non sia stato neppure disposto un obbligo di notifica nei confronti dei soggetti i cui dati risultino sottoposti ad accesso.

Gli Ordini professionali degli Avvocati e l'Academie Fiscale, anche con riferimento alla legge del 2016 e similmente a quanto era già stato oggetto di censura nella legge del 2013, avevano poi considerato le disposizioni sulla conservazione e accesso ai metadati come contrarie al rispetto del segreto professionale che caratterizza professioni delicate quali quella legale o contabile: l'accesso ai metadati in tale ambito permetterebbe di determinare se un professionista è stato consultato, consentendo di conseguenza l'identificazione dei clienti e i dati relativi alle comunicazioni avvenute (luogo, durata, data). Per quanto la normativa vigente avesse introdotto alcune disposizioni specifiche su questo profilo, nel complesso la mancata predisposizione di un divieto assoluto di conservazione dei metadati afferenti a mezzi di comunicazione appartenenti a tali soggetti e la previsione di alcuni casistiche che consentono, al contrario, l'accesso a tali metadati, risultava lesiva di un interesse generale, ravvisabile nella garanzia di una reale segretezza del rapporto tra professionista e cliente e capace di incidere sui diritti alla vita privata e al giusto processo. Ad aggravare tale quadro vi era inoltre l'assenza di meccanismi di controllo volti a consentire al professionista di opporsi alla raccolta, conservazione e accesso a dati coperti da segreto professionale.

Il Governo belga, intervenuto dinnanzi alla Corte costituzionale, aveva ribadito la correttezza delle proprie scelte e del proprio approccio, affermando innanzitutto come il segreto professionale non possa essere considerato una prerogativa assoluta bensì possa essere compresso proporzionalmente allo scopo e all'interesse pubblico da raggiungere, eventualmente concorrente alla segretezza stessa. Anche sotto il profilo della disciplina della conservazione, veniva ribadito come l'obbligo di conservazione preceda logicamente la fase di accesso e solo la richiesta di accesso permetta la determinazione della gravità del

---

abbiano affermato che non può considerarsi conforme al diritto UE una normativa nazionale che *allo scopo di combattere reati*, preveda una *bulk data retention*. Ne deriverebbe dunque che una normativa che predispone tale medesimo tipo di conservazione per scopi diversi dalla lotta alla criminalità, ad esempio, come previsto nel regime belga, per ricercare persone scomparse o identificare coloro che hanno effettuato chiamate d'emergenza, dovrebbe essere considerata esclusa da tale divieto. Al contrario, i ricorrenti hanno invece sostenuto come se neppure la lotta al terrorismo o alla criminalità organizzata sono risultati obiettivi tali da ritenere una ingerenza così vasta nella sfera privata come proporzionata allo scopo, tantomeno potranno esserlo altri scopi di 'minore impatto' e rilievo quali quelli previsti dalla normativa belga.

[49] L'Ordre des barreaux inoltre si spinge ad una analisi ancora più approfondita di tale aspetto, accusando il Governo di fingere di non comprendere il riferimento effettuato dai ricorrenti "à d'autres mécanismes moins attentatoires à la vie privée de l'ensemble des citoyens comme les méthodes de repérage existantes en droit belge ou de 'quick freeze' qui visent une décision obligeant les opérateurs a conserver des données à propos de personnes identifiées dans une zone géographique ou une période temporelle délimitée. *Le raisonnement de l'Etat belge reposerait en réalité sur une volonté politique de poursuivre a tout prix dans la voie de la conservation générale des données sous prétexte d'un contexte de risque terroriste et malgré l'inconstitutionnalité du système de surveillance généralisé mis en place*", par. A.3.6., enfasi aggiunta.

reato tale da consentire una modulazione appropriata della ingerenza: per questi motivi logici, prima ancora che giuridici, risultava impossibile provvedere ad una differenziazione della durata della conservazione *a priori*, poiché non potevano conoscersi in precedenza i reati per i quali tali dati avrebbero potuto essere utili e dunque la determinazione della proporzionalità dell'ingerenza concessa, mentre l'unica garanzia possibile risultava essere quella di una corretta e precisa modulazione dell'accesso. Facendo leva sulle considerazioni già chiaramente espresse nei lavori preparatori all'adozione della normativa nazionale, veniva anche confermata dal Governo la legittimità e compatibilità di un sistema di conservazione generalizzata rispetto al diritto nazionale ed europeo: la sola *data retention*, autonomamente intesa, ovvero senza e prima dell'accesso, non può consentire di stabilire chiare conclusioni sulla vita privata, che potrebbero invece essere definite solo con l'accesso successivo; per tali motivi, le salvaguardie poste in essere – dalla conservazione sul solo territorio dell'UE, al controllo affidato ad IBPT e all'Autorità nazionale per la protezione dei dati – risultavano sufficienti con riferimento alla conservazione, soprattutto alla luce delle ancor più stringenti tutele previste per la successiva fase di accesso. Del resto, ancora una volta con un ragionamento di tipo logico e fattuale più che giuridico, il Governo stabiliva come: "la loi attaquée permet précisément aux enquêteurs, dans un cadre soigneusement déterminé, d'accéder à certaines métadonnées concernant une personne faisant l'objet d'une telle enquête. Cela suppose que ces métadonnées aient été conservées en amont de l'enquête et donc à un moment où il n'était pas possible d'opérer la différenciation visée par le requérant" (par. A.5.12). Ribadendo quanto già sottolineato prima dell'adozione della normativa, il Governo ammetteva nuovamente nelle proprie memorie come "le législateur n'a pas pu répondre à l'ensemble des critiques formulées par la jurisprudence pour considérer que la directive 2006/24/CE était illégale. Il indique toutefois qu'un seul élément ne pourrait suffire à constituer une violation du principe de proportionnalité au sens de la jurisprudence de la Cour de justice et de celle de la Cour" (par. A.7.3). Ebbene queste posizioni sono state fortemente avversate dai ricorrenti che avevano al contrario sostenuto come questi presupposti enunciati dal Governo non potessero in alcun modo essere considerati conformi alla giurisprudenza della CGUE così come affermata nella sentenza *Tele2*, che aveva stabilito appunto la necessità per i legislatori nazionali di astenersi dal mettere in atto una misura generalizzata di conservazione, in grado di riguardare la totalità dei cittadini. Sul punto i ricorrenti hanno peraltro richiamato le Conclusioni dell'Avvocato generale nel caso *Tele2*, nelle quali Saugmandsgaard Øe aveva affermato come i requisiti di cui all'art. 15 Direttiva *e-Privacy* e quelli richiesti dall'art. 52 della Carta di Nizza dovessero essere intesi come cumulativi e che quindi tutto quanto indicato dai giudici nella sentenza *DRI* dovesse essere rispettato, sia con riferimento alla conservazione che all'accesso.

Al contrario invece il Governo ha proposto una lettura opposta secondo cui la decisione della CGUE che ha portato a ritenere la DRD come non limitata al principio di proporzionalità e necessità, fosse da considerarsi basata sulla combinazione di quattro elementi: il fatto che la conservazione fosse generalizzata, l'assenza di differenziazione quanto alle categorie dei dati conservati e alla loro utilità, l'assenza o l'insufficienza di regole riguardanti l'accesso ai metadati[50]. Tutti questi aspetti, letti in maniera combinata e laddove dunque tutti contemporaneamente sussistenti, avevano portato alla dichiarazione di mancata conformità al diritto dell'UE e con riferimento alla successiva sentenza *Tele2* era stato affermato con grande chiarezza come: "ni la Cour de justice ni la Cour n'ont jugé que l'un de ces quatre éléments pouvait suffire à conclure au caractère disproportionné de la mesure. *Le contrôle du principe de proportionnalité suppose en effet une approche globale. Contrairement à ce que soutiennent*

[50] "Si chaque citoyen n'est, en effet, pas potentiellement un criminel, chaque citoyen peut potentiellement être confronté à la criminalité, que ce soit en tant que victime, en tant que prévenu ou en tant que témoin et dès lors avoir un intérêt à la recherche de la vérité", par. A.10.3. Ne consegue dunque che sarebbe sbagliato individuare la carenza di un singolo elemento nella lista dei requisiti fissata dalla CGUE – per esempio la mancanza di una *targetd retention* – e valutare quell'unico criterio non rispettato come in sé idoneo a rendere la disciplina sulla conservazione e accesso ai metadati irrimediabilmente e totalmente incompatibile con la Carta Europea dei Diritti Fondamentali.

les parties requérantes, l'arrêt de la Cour de Justice de l'Union européenne du 21 décembre 2016 ne remettrait nullement en cause ce constat" (par. A.10.4, enfasi aggiunta)[51].

3.2. – L'attenta e consapevole lettura della Cour constitutionnelle *e il rinvio alla CGUE*

Proprio prendendo avvio da questi due diversi approcci e letture della medesima giurisprudenza della CGUE, promossi dal Governo belga da un lato e dai ricorrenti dall'altro, la Corte costituzionale nella sentenza del 19 luglio 2018, n. 96/2018, ha preso atto di come la decisione *DRI* così come la successiva *Tele2* fossero passibili di due diverse interpretazioni, sinteticamente ma magistralmente indicate: "dans une premiére interprétation, l'illégalité de l'obligation de conservation générale et indifférenciée des données résulterait de l'absence de garanties suffisantes relatives à l'accès aux données conservées et au délai de conservation; dans une deuxième interprétation, l'obligation de conservation serait illégal, précisément en raison de son caractère général et indifférencié" (par. A.14.1). Ne è conseguita, dunque, la necessità di predisporre un rinvio pregiudiziale alla CGUE, alla quale sola spetta il compito di sciogliere l'annoso e complesso nodo interpretativo in maniera definitiva, delineando quali dei due differenti approcci sia corretto. Svolgendo una puntuale e ampia ricostruzioni delle motivazioni e delle considerazioni che sostengono entrambi gli orientamenti, la Corte costituzionale belga ha cercato di fornire ai giudici di Lussemburgo un ampio quadro della difficile questione posta alla sua attenzione, richiamando peraltro anche la – all'epoca – più recente giurisprudenza della Corte europea dei Diritti dell'Uomo. In particolare, è stata presentata alla CGUE la sentenza *Centrum For Rattvisa*[52], nella parte in cui, in particolare, viene riconosciuto alle autorità nazionali un ampio margine di apprezzamento quanto alla scelta dei mezzi volti alla salvaguardia della sicurezza nazionale (par. 112). In tale pronuncia, lo si vuole ricordare, i giudici di Strasburgo avevano ritenuto la normativa svedese, comportante forme di intercettazione massiva delle comunicazioni elettroniche per finalità securitarie – tra cui la lotta alla minaccia terroristica –, conforme alla Convenzione EDU e al suo art. 8 sulla tutela della vita privata alla luce di una analisi globale di tutte le salvaguardie predisposte dal legislatore, lette nel loro insieme. La scelta dunque dei giudici belgi di richiamare proprio tale sentenza potrebbe essere vista come un suggerimento rivolto ai giudici di Lussemburgo ad osservare anche quanto sta accadendo nella giurisprudenza della Corte EDU, che pare diretta, quanto meno negli ultimi anni, verso una lettura meno stringente dei requisiti di legittimità di forme di sorveglianza e controllo delle telecomunicazioni. Su questa stessa linea può essere visto anche il richiamo espresso svolto dalla Corte costituzionale alle grandi difficoltà concretamente incontrate dalla maggioranza degli Stati membri nel predisporre o

[51] Il Governo aggiunge come sia da considerarsi impossibile "de lutter contre la criminalité grave telle que la cybercriminalité si l'on ne prévoit pas une obligation générale et indifférenciée de conservation des données de communication électronique. (..) Il répété une fois encore qu'à son estime, il n'existe pas d'autre moyen pour atteindre les objectifs poursuivis par le législateur qu'imposer une obligation générale de conservation" (par. A.13.3). Il Governo belga dunque è chiaro nel ribadire come qualsiasi considerazione quanto al mancato rispetto del requisito di stretta necessità della *bulk data retention* sia da respingersi. Sotto questo profilo inoltre vengono riportati alcuni dati, che il Governo presenta a supporto proprio della utilità di una conservazione generalizzata e della durata di dodici mesi indicata dalla legge del 2016: "Dans son mémoire en réplique, le Conseil des ministres note une fois encore que le fait qu'une différenciation sur le plan du délai de conservation des données était impossible n'est pas sans justification raisonnable. Aussi bien dans le cadre des enquêtes pénales que dans le cadre des services de renseignement, le délai concerné est apparu nécessaire. Il ressort des chiffres de l'IBPT que, pour l'année 2014, 15 % des demandes qui émanaient des autorités judiciaires et qui étaient fondées sur les articles 46*bis* et 88*bis* du Code d'instruction criminelle adressées à Base Company et Proximus avaient rapport à des données qui dataient de plus de neuf mois jusqu'à douze mois avant la demande. Il apparaît également des chiffres de la « Federal Computer Crime Unit » (FCCU) pour la période de 2012 à 2014 que 29 % des demandes avaient rapport aux données qui dataient de plus de neuf mois jusqu'à douze mois avant la demande. Les chiffres présentés par le Service général du renseignement et de la sécurité (SGRS) vont dans le même sens" (par. A.36).

[52] Per una ampia analisi di tale giurisprudenza si rimanda a quanto scritto nel Capitolo V, Parte II.

modificare una disciplina nazionale conforme e rispettosa dei criteri individuati in *DRI* e *Tele2*, quasi a sottolineare che le criticità incontrate dai legislatori belgi risultano in realtà avere carattere diffuso in tutta l'UE, affondando le proprie radici non nei limiti o nell'approccio di un singolo legislatore nazionale bensì in questioni ben più profonde e condivise a livello europeo.

Su tutte queste complesse considerazioni quindi poggia la decisione della Corte costituzionale di promuovere un rinvio pregiudiziale alla CGUE[53], chiedendo espressamente, come già visto nel Capitolo IV, Parte II, se una normativa come quella belga del 2016 sia da ritenersi in contrasto con quanto disposto dall'art. 15 Direttiva *e-Privacy* letto congiuntamente alla Carta di Nizza e alla Convenzione EDU. A ciò si aggiunge un ulteriore rilevante quesito, volto a comprendere le possibili conseguenze di una eventuale dichiarazione di incostituzionalità della legge nazionale sulla *data retention* qualora i giudici di Lussemburgo confermassero una interpretazione avversa alla possibilità di adottare forme di conservazione generalizzata ed indiscriminata[54].

Sebbene la causa innanzi alla Corte di giustizia sia ancora pendente, sono state pubblicate invece le Conclusioni dell'Avvocato generale Campos Sanchez-Bordona: per quanto esse siano già state oggetto di ampia analisi, meritano in questa sede di essere riportate le considerazioni svolte con specifico riferimento alla normativa belga e che assumono quindi grande rilievo ai fini delle riflessioni che qui si stanno svolgendo.

Sul fronte della disciplina della conservazione, infatti, l'Avvocato generale ha affermato come, nonostante le garanzie predisposte, la normativa belga preveda comunque un obbligo di *bulk* o *blanket data retention* che, in quanto tale e sulla base della interpretazione della previa giurisprudenza europea fornita nelle Conclusioni stesse, non può essere considerato conforme al diritto dell'UE e dunque alla Carta di Nizza. Così viene stabilito espressamente come "il legislatore belga dovrà esplorare altre vie che introducano formule di conservazione limitata" (par. 127, Conclusioni dell'Avvocato generale, C-520/18). Quanto alla disciplina attinente all'accesso, poi, sono stati sostanzialmente riaffermati i criteri già indicati sin dalla sentenza *DRI* ed è stato attribuito al giudice del rinvio il compito di provvedere ad una valutazione nel dettaglio della normativa nazionale e del suo rispetto di tali requisiti. Nonostante tale posizione, l'Avvocato si è comunque spinto ad una considerazione che lascia trasparire alcune perplessità e con la quale vengono individuate talune lacune nella disciplina belga del 2016: "rilevo, ad esempio, che nel contesto della normativa controversa non sembra che le autorità nazionali competenti siano sistematicamente tenute ad informare le persone interessate (sempre che tale informazione non comprometta le indagini in corso) che i loro dati sono stati consultati. Né sembra che siano previste, almeno in alcuni casi, come quelli relativi ai reati finanziari, regole predefinite riguardo alla gravità di questi ultimi, per giustificare l'accesso ai relativi dati" (par. 142). A ciò si aggiunge anche la complessa questione, più specificamente trattata nel rinvio pregiudiziale promosso dal giudice estone ed attualmente pendente[55], circa l'idoneità del Procuratore di adottare provvedimenti quali appunto le richieste di accesso ai metadati: laddove nel pubblico ministero infatti venga individuato il soggetto deputato a valutare la proporzionalità e necessità della domanda di accesso ai dati ma che, allo stesso tempo, dovrà svolgere anche la funzione di pubblica accusa nell'eventuale fase di giudizio successiva,

[53] Domanda di pronuncia pregiudiziale proposta dalla Cour constitutionnelle (Belgio) il 2 agosto 2018, Causa C-520/18.

[54] La Corte si è chiesta e ha chiesto alla CGUE se "possano essere mantenuti provvisoriamente gli effetti (*di una tale legge*) al fine di evitare una situazione di incertezza giuridica e di permettere che i dati raccolti e conservati in precedenza possano ancora essere utilizzati per il raggiungimento degli obiettivi previsti dalla legge". Questo rilievo ha chiaramente un forte impatto sui procedimenti penali fondati proprio sull'utilizzo di dati provenienti dalle comunicazioni elettroniche che siano stati raccolti o consultati sulla base di normative poi considerate non conformi ai diritti sanciti dalla Carta di Nizza. Un simile quesito è stato peraltro sollevato nel rinvio pregiudiziale pendente promosso dalla Supreme Court irlandese e analizzato nel Capitolo IV, Parte II, cui si rimanda.

[55] C-746/18, *H.K. c. Prokuratur*, già analizzato nel Capitolo IV, Parte II. Questo profilo è stato peraltro denunciato anche dalle parti ricorrenti al Par. A.23.1, laddove viene affermato come "le procureur du Roi ne constitue pas une instance juridictionnelle ou une autorité administrative indépendante".

viene da chiedersi se possa considerarsi rispettata la condizione di un controllo e vaglio preventivo effettuato da una autorità indipendente.

Molte dunque sono le questioni che rimangono ancora aperte sul tavolo del giudice europeo e che sono destinate a rivelarsi di importanza determinante per la sussistenza stessa della vigente normativa belga in materia di *data retention* e di accesso ai metadati per scopi securitari. Questo tuttavia non è da considerarsi l'unico fronte sul quale la Corte costituzionale belga ha posto l'attenzione e rispetto al quale ha richiesto l'intervento della CGUE.

3.3. – La normativa nazionale in materia di PNR e il lucido controllo del giudice costituzionale: un ulteriore rinvio alla CGUE

Sebbene certamente il rinvio sulla legge del 2016 rivesta grande rilievo, non si vuole infatti dimenticare come i giudici belgi siano stati chiamati nel 2017 a valutare la legittimità e conformità alla Costituzione anche di una ulteriore normativa nazionale, ancora una volta di trasposizione di una Direttiva europea, anche in questo caso relativa alla raccolta, conservazione e accesso a dati finalizzata alla lotta alla criminalità: si fa riferimento alla legge del 25 dicembre 2016 sul trattamento dei dati del codice di prenotazione dei passeggeri (PNR)[56], quale trasposizione della Direttiva dell'UE 2016/681 sull'uso dei PNR ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.

In estrema sintesi e richiamando quanto già ampiamente detto nel Capitolo III, Parte II in relazione alla Direttiva PNR, la normativa belga in questione prevedeva, in conformità a quanto disposto dalla disciplina europea[57], l'obbligo in capo agli operatori di viaggio di trasmettere i dati dei propri viaggiatori al *Service public fédéral intérieur* (c.d. SPF). È infatti all'interno di tale Servizio che è stata formata l'UIP, cioè l'Unità d'Informazione sui Passeggeri, richiesta dalla normativa europea e deputata a gestire la banca dati istituita allo scopo di garantire la conservazione e il trattamento dei codici di prenotazione stessi. L'accesso e dunque l'utilizzo di questi ultimi è vincolato a specifiche finalità espresse dalla legge: esse sono individuate nella finalità di indagine, azione penale ed esecuzione delle pene per qualsiasi reato previsto nel Codice penale nonché in quello di procedura penale e in leggi specifiche, di prevenzione di gravi turbative dell'ordine pubblico per radicalizzazione violenta, monitoraggio delle attività dei servizi segreti e sicurezza, controlli alle frontiere esterne e lotta all'immigrazione irregolare. Il termine massimo di conservazione dei PNR è stato fissato in cinque anni, stabilendo però il limite secondo cui i dati possono essere trattati per effettuare controlli preliminari, cioè in un momento precedente all'arrivo del passeggero, o per svolgere ricerche e indagini specifiche sostanzialmente identificate nelle finalità sopra richiamate e nelle attività di sicurezza nazionale poste in essere dai servizi di intelligence sulla base della legge del 1998. La valutazione preventiva automatizzata dei dati dei passeggeri, in un momento antecedente il loro arrivo, deve essere in ogni caso svolta in maniera non discriminatoria e non può mai fondarsi sull'impiego di dati in grado di rivelare l'origine etnica, razziale, le convinzioni religiose o politiche, la salute, le preferenze sessuali o ancora l'organizzazione sindacale; tali dati, capaci di svelare informazioni così sensibili, debbono essere immediatamente cancellati da parte dell'UIP. Ad esclusione dunque delle categorie particolari di dati, tutte le altre informazioni raccolte dalla UIP, invece, vengono inserite nella banca dati mentre i file provvisori inviati dai vettori e ricevuti dalle autorità preposte vengono distrutti entro ventiquattro ore dalla trasmissione, così come anche in capo ai vettori e agli operatori di viaggio vige l'obbligo, entro ventiquattro ore dal termine del trasporto, di distruzione di tutti i dati relativi ai propri passeggeri: ciò al fine di evitare qualsiasi

[56] *Loi du 25 décembre 2016 relative au traitement des données des passagers*, M.B. 25 janvier 2017.
[57] Per approfondimenti sulla disciplina prevista da tale Direttiva, si rimanda al Capitolo III, Parte II.

duplicazione di informazioni, che verranno conservate unicamente e in una sola copia nel database UIP. Viene predisposta inoltre una specifica disciplina relativa all'accesso alla banca dati, che può essere effettuato dai servizi di intelligence o dall'ufficiale di polizia giudiziaria incaricato dal Procuratore, sulla base di decisione scritta e motivata (art. 50, che inserisce nel *Code d'instruction criminelle* un nuovo articolo 46septies), mentre la possibilità di effettuare un eventuale raffronto tra i PNR contenuti nel database e i dati memorizzati in altre banche dati a disposizione delle pubbliche autorità è limitata solo a quei database il cui fine è identificato nel perseguimento dei medesimi scopi indicati dalla legge impugnata (non può ad esempio svolgersi un raffronto tra le informazioni raccolte dalle UIP e quelle conservate da una pubblica amministrazione per il solo scopo di accesso a servizi pubblici).

Ebbene proprio con riferimento a tale normativa nazionale, la ONG Ligue des droits humains, già protagonista, come si è visto, in altre cause finalizzate a garantire la tutela dei diritti fondamentali, ha promosso ricorso di annullamento dinnanzi alla Corte costituzionale belga. La ricorrente ha infatti considerato che, in generale, il grande numero di informazioni raccolte e trattenute sulla base della normativa in materia di PNR superasse quanto concesso dai principi di legalità, necessità e proporzionalità, mirando ad effettuare un *pre-screening* di tutti i passeggeri[58], la cui utilità per il raggiungimento degli obiettivi preposti è peraltro ritenuta dubbia; più nel dettaglio poi è stata ritenuta del tutto problematica l'attribuzione di una ampia discrezionalità al potere esecutivo, cui viene attribuito il compito di determinare, mediante regio decreto, alcuni elementi di fondamentale importanza per l'attuazione della normativa; criticità sono state riconosciute infine nell'ampiezza delle categorie di dati interessati, degli scopi e della durata della conservazione, che eccedono quanto strettamente necessario, oltre a costituire una forma di conservazione generalizzata ed indiscriminata[59] rispetto alla quale cioè non viene richiesta la sussistenza di un legame tra un sospetto e un pericolo per la sicurezza. Non manca oltretutto di essere evidenziato come le finalità previste dalla normativa belga e giustificanti il trattamento dei dati raccolti risultassero maggiormente ampie rispetto a quelle previste dalla Direttiva PNR, che non comprende ad esempio tra gli scopi quello alla lotta alla immigrazione irregolare.

Il Governo belga, al contrario, ha difeso la legge impugnata, ritenendola conforme al diritto dell'UE e alla Costituzione belga, confermando come il controllo automatizzato preventivo dei dati, volto ad una efficace lotta contro i crimini gravi, risulti coerente non solo alla Direttiva PNR ma anche a quanto affermato dalla CGUE nel *Parere 1/15*.

La Corte costituzionale, nel vagliare le doglianze dei ricorrenti e le considerazioni svolte dal Governo, ha ritenuto necessario, ancora una volta, rinviare alcuni quesiti alla CGUE[60], in considerazione dei rilevanti dubbi emersi quanto alla compatibilità con il diritto dell'UE della normativa nazionale in materia di PNR e – di riflesso – della stessa Direttiva PNR. Ciò che in questa sede si vuole sottolineare è come taluni dei numerosi quesiti, che sono già stati oggetto di analisi nel Capitolo III, Parte II, siano il frutto di una lettura attenta tanto delle considerazioni svolte dai giudici di Lussemburgo nel *Parere 1/15* quanto dei requisiti affermati invece nella sentenza *Tele2*[61]. I giudici belgi hanno quindi dimostrato,

[58] Come emerge dai lavori preparatori della legge stessa (Doc. Parl. Chambre 2018-2019, DOC 54-3652/001), tale pre-screening "permet par exemple d'évaluer si une personne présente un degré élevé de dangerosité, car elle est connue dans une banque de données policière dans le cadre d'un dossier terroriste et pour laquelle il appert de l'analyse de ses données passager, que cette dernière se rend régulièrement dans des pays abritant des camps d'entraînement pour terroristes ou dans des pays de transit vers de tels lieux".

[59] Sono infatti trasmessi alla UIP i dati riguardanti i passeggeri che intendono entrare in Belgio attraverso le frontiere esterne, i passeggeri che vogliono lasciare il Belgio e quelli che invece intendono attraversare il territorio nazionale (art. 29 della legge belga in materia di PNR).

[60] Arret n. 135/2019, del 17 ottobre 2019, sulla base del quale ha avuto origine il rinvio pregiudiziale dinnanzi alla CGUE, nella causa C-817/19, *Ligue des droits humains c. Conseil des Ministres*, al momento pendente.

[61] A titolo di esempio, nel *Parere* citato era stato affermato come i PNR – similmente ai metadati e anche nel caso in cui i codici di prenotazione non contengano dati 'delicati' o 'sensibili' – fossero idonei a permettere una ricostruzione delle abitudini dei passeggeri, delle relazioni esistenti tra due o più persone, della loro situazione finanziaria e persino delle abitudini alimentari, informazioni dalle quali è peraltro possibile giungere,

anche con riferimento alla normativa in materia di PNR, una profonda conoscenza della giurisprudenza europea e una grande capacità di osservare in maniera globale i principi da essa affermati in diverse sentenze, che, sebbene attinenti ad ambiti normativi distinti e riguardanti categorie di dati differenti, risultano sempre riconducibili alla disciplina di regimi di *data retention* per scopi securitari.

Al termine di questa fine analisi, i giudici nazionali hanno ravvisato una certa discordanza tra quanto affermato da un lato nella *Tele2*, con riferimento alla necessaria sussistenza di una connessione – anche solo indiretta – tra conservazione del dato e criminalità grave, e dall'altro nel *Parere 1/15*, nel quale invece sono stati ammessi e legittimati il trasferimento, la conservazione ed il filtraggio generali e non selettivi dei dati relativi a tutti i passeggeri, anche a quelli non sospettati di reati. La Corte costituzionale dunque si è chiesta in quale misura la giurisprudenza relativa alla *data retention* avente ad oggetto metadati fosse applicabile anche nell'ambito del trasferimento di PNR[62] e se quest'ultimo regime di conservazione generalizzata, seppur di ampiezza ridotta – essendo riferita ai soli codici di prenotazione e non a tutti i metadati prodotti da tutti i mezzi di comunicazione –, fosse da considerarsi limitato allo stretto necessario. Proprio sulla base di tali importanti valutazioni rimesse alla CGUE, la decisione di quest'ultima, pur vertendo sul trattamento dei PNR, risulterà, come si è già evidenziato nei previ Capitoli, di grande rilevanza al fine di chiarire le differenze – se esistenti – intercorrenti tra conservazione generalizzata di metadati e conservazione di codici di prenotazione appartenenti a tutti i passeggeri; tale intervento potrà così fornire una importante chiave di lettura, utile anche per i legislatori nazionali e sovranazionali impegnati a riflettere sulla possibilità di adottare regimi alternativi, ma comunque efficaci, di conservazione dei dati per scopi securitari.

4. – L'impatto delle attese decisioni della CGUE sulla legislazione belga in materia di data retention *e raccolta, conservazione e accesso dei* PNR: *un futuro incerto*

La Corte costituzionale belga nei due rinvii pregiudiziali sopra analizzati – entrambi in materia di *data retention* e accesso ai dati, sebbene riferiti a normative e dati differenti – ha mostrato di saper porre grande attenzione a tematiche tanto delicate quanto fortemente impattanti sulla tutela dei diritti fondamentali e caratterizzanti l'era dei Big Data e dell'emergenza securitaria. Stessa attenzione è stata peraltro posta da legislatore, Governo e società civile: il difficile e continuo intervento normativo, così come l'attivismo di ONG e cittadini, tutti scanditi dagli avvicendamenti che hanno segnato il percorso europeo, sono la dimostrazione chiara di una forte sensibilità verso le complesse sfide rappresentate dal discusso strumento della *data retention*.

L'affermarsi di nuove tipologie di reati perpetrati mediante l'impiego di mezzi di telecomunicazione, nonché di forme di criminalità sempre più sofisticate, organizzate e dalla dimensione transnazionale grazie anche all'utilizzo di dati digitali e sistemi informatici, unitamente alla minaccia terroristica sempre più incombente anche nel panorama europeo, avevano spinto il legislatore belga ad introdurre, sin dai primi anni 2000, un obbligo di conservazione dei metadati, inteso come mezzo efficiente ed

indirettamente, alla determinazione del credo religioso o di problematiche di salute (par. 128, *Parere 1/15*). Alla luce di tali valutazioni, che erano in quel caso riferite al trasferimento di PNR verso uno Stato extra-UE, la Corte costituzionale belga è giunta a chiedersi se l'elenco, estremamente ampio, dei dati oggetto di trasferimento, così come indicato nella normativa nazionale e mutuato dalla Direttiva PNR, dovesse considerarsi eccedente quanto strettamente necessario per il raggiungimento dell'obiettivo perseguito. Risolvere tale domanda avrebbe implicato però una interpretazione del diritto europeo, affinché fossero chiarite alcune perplessità derivanti dalla lettura fornita dalla giurisprudenza della CGUE in materia di PNR e di *data retention*: ecco dunque che si è reso necessario il ricorso ad un rinvio pregiudiziale.

[62] Considerando peraltro come dal pre-screening sistematico e automatizzato, derivante dal controllo incrociato dei PNR con i dati contenuti in altre banche dati dello Stato e volte al raggiungimento delle medesime finalità della legge in materia di PNR, possa addirittura derivare l'adozione di una misura quale il mandato d'arresto, su ordine di autorità giudiziarie e comunque a seguito di un controllo umano della corrispondenza positiva.

efficace per garantire la sicurezza. Da tale scelta emerge chiaramente la volontà di sfruttare le potenzialità offerte dalla *data retention* e dunque di poter disporre di dati che consentano di andare indietro nel tempo e di ottenere informazioni relative anche a soggetti precedentemente non sospettati o non noti alle autorità di *law enforcement*. Questo approccio normativo tuttavia si è scontrato sin dall'inizio con una ulteriore consapevolezza: quella degli effetti rilevanti che una conservazione generalizzata comporta per i diritti fondamentali e in particolare per il diritto alla riservatezza, garantito all'art. 22 della Costituzione belga, nonché al diritto alla protezione dei dati, riconosciuto oltre che nella Carta di Nizza anche dalla giurisprudenza belga stessa. I pericoli concreti di una ingerenza considerevole nella sfera privata e la conseguente necessità di stabilire limiti alla compressione di tali diritti sono del resto emersi con chiarezza nelle rimostranze, perplessità e contrasti evidenziati durante il difficile e lungo percorso legislativo che aveva portato a disciplinare a livello nazionale la materia della *data retention*.

Il dibattito su tale delicata disciplina è divenuto ancor più complesso a seguito degli interventi della Corte costituzionale belga: con le due pronunce sopra esaminate, in particolare, i giudici hanno imposto al legislatore una seria riflessione sulle salvaguardie e sui confini da determinare sia quanto alla conservazione dei metadati che al successivo accesso ad essi per scopi securitari, in correlazione ovviamente con i requisiti stabiliti dalla giurisprudenza della CGUE. Comprendendo quindi come una tale materia non potesse essere letta nella esclusiva ottica del *trade-off*, ovvero di una esclusione della sicurezza a favore della tutela dei diritti fondamentali e viceversa, il legislatore belga, e successivamente la Corte costituzionale, si sono interrogate sulla determinazione del corretto punto di equilibrio tra spinte differenti. Mentre il primo ha identificato tale bilanciamento in una restrizione maggiore nella fase di accesso ai metadati, l'altra ha invece ritenuto opportuno presentare le criticità emerse ai giudici di Lussemburgo e chiederne una interpretazione alla luce dei precedenti giurisprudenziali e delle loro articolate conseguenze applicative. Ecco dunque che da un punto di partenza fortemente sbilanciato a favore della garanzia della sicurezza e volto a sfruttare appieno la *data retention* e le sue potenzialità, si è dunque passati, anche mediante l'intervento delle Corti e il succedersi di diverse normative, ad un approccio problematico verso la materia, capace di coglierne appieno l'impatto, le criticità e il bisogno di stabilire limiti e salvaguardie appropriate.

In questo contesto, nel quale le decisioni e valutazioni dei diversi protagonisti (legislatore, Corti ma anche società civile) si sono così fortemente intrecciate con gli accadimenti avvenuti a livello dell'UE, la panoramica offerta dello sviluppo normativo e giurisprudenziale belga può – e anzi deve – essere letta anche come esemplificazione perfetta dell'incidenza delle disposizioni e delle sentenze adottate in ambito europeo entro i confini nazionali. Questo diviene evidente quando si osserva il percorso tortuoso seguito dalla disciplina belga in materia di conservazione dei metadati, segnato dall'impatto prima della sentenza *DRI*, che ha visto sia l'intervento della Corte costituzionale che un rapido successivo lavoro del legislatore nazionale, messo in crisi nuovamente dalla giurisprudenza della CGUE, la quale ha portato ad un ulteriore ricorso alla Corte costituzionale, promosso dai membri della società civile, che hanno mostrato – più che in altri Stati membri – di attribuire una grande rilevanza al tema.

Assistiamo così ad un dialogo costante, sebbene talvolta contrastante, tra giudici nazionali, legislatori nazionali e giudici europei, che assume però in Belgio un tono differente da quello registratosi nel Regno Unito. Se si guarda alle scelte del legislatore belga, infatti, si nota come questo abbia mostrato di aver attentamente studiato la portata delle pronunce della CGUE e di aver avviato una seria riflessione sui requisiti da esse stabiliti. Pur essendo giunto, anche nella normativa del 2016 e attualmente vigente, ad una soluzione consapevolmente di compromesso tra l'elevato standard di tutela posto dalla giurisprudenza europea e le necessità di efficacia ed efficienza dello strumento della *data retention*, il legislatore ha espressamente ammesso il limite e le difficoltà incontrate nella predisposizione del nuovo dettato normativo, allontanandosi così dall'atteggiamento di chi – anche nel contesto nazionale italiano – ha quasi del tutto ignorato le conseguenze dell'intervento deciso della CGUE. Al contrario, infatti, il

legislatore belga non ha cercato di aggirare i problemi, bensì ha tentato di fornire una interpretazione – non troppo forzata e lontana da quanto chiaramente espresso dai giudici di Lussemburgo – che potesse consentire di raggiungere il proprio obiettivo pur considerando i requisiti fissati a livello europeo: questo approccio può ben essere rinvenuto nel tentativo di passare da disposizioni generiche e vaghe, quali quelle della legge del 2013, che lasciavano ampio spazio all'intervento del Governo mediante l'adozione di decreti, a norme invece più precise e determinate nonché a salvaguardie più specifiche riguardanti l'accesso ai metadati. Sono state quindi inserite disposizioni limitative circa la possibilità di 'andare indietro nel tempo' che denotano un atteggiamento differente e più rigoroso rispetto a quello che ha caratterizzato ad esempio il legislatore inglese, anche se, in maniera del tutto identica a quest'ultimo, anche la normativa belga si fonda sulla medesima scelta di base, che è quella di non rinunciare ad una *bulk data retention*.

Osservando poi l'intervento dei giudici nazionali, essi si sono mostrati certamente attenti e rispettosi della giurisprudenza dei giudici di Lussemburgo: pur allontanandosi, negli ultimi anni, da un iniziale atteggiamento 'ossequioso' e forse poco attento e critico, la Corte costituzionale ha infatti promosso un dialogo con la CGUE volto a chiarire taluni rilevanti dubbi anziché propendere direttamente per l'una o l'altra delle posizioni proposte nel dibattito nazionale ed evitando di ricondurre unicamente al profilo interno la questione della corretta disciplina della *data retention*. La Corte costituzionale ha, anzi, studiato i rinvii pregiudiziali già decisi o pendenti dinnanzi alla CGUE, quali quello spagnolo nel caso *Ministerio Fiscal* o ancora quello inglese nel caso *Privacy International*, ed ha compreso che la complessità della materia e le incertezze interpretative ancora esistenti necessitavano di un chiarimento a livello europeo, comune a tutti gli Stati membri. Un atteggiamento questo che, sebbene condiviso da altre Corti nazionali che hanno mostrato, nei numerosi rinvii pregiudiziali in materia, di ritenere imprescindibile un intervento della CGUE, non è da considerarsi scontato, tanto che, come si vedrà nel Capitolo III, non è stato seguito dalla Corte di Cassazione italiana, la quale ha mostrato di non saper cogliere tutte le sfaccettature della giurisprudenza europea e di non comprendere neppure le rilevanti conseguenze che le zone grigie e i quesiti lasciati irrisolti dalla CGUE comportano nell'ambito nazionale.

La Corte costituzionale belga sembra poi, nella propria decisione di rinviare alla CGUE, voler suggerire ai giudici di Lussemburgo una possibile via, una strada interpretativa che riesca meglio a mediare le esigenze di efficacia dello strumento della conservazione e, al contempo, il rispetto dei diritti fondamentali. In questo senso la Corte belga evidenzia le difficoltà riscontrate dagli Stati membri, ponendo dinnanzi ai giudici dell'UE una situazione concreta e condivisa nel panorama europeo, situazione che non può essere ignorata nel ragionamento giuridico e nel bilanciamento da effettuare.

Questa consapevolezza non si è tuttavia concretizzata nella lettura che ha invece caratterizzato il rinvio promosso dal *Investigatory Power Tribunal* inglese, nel quale, insieme ai quesiti posti, viene evidenziato, quasi fosse un monito, anche il peso e l'impatto – potenzialmente devastante – delle decisioni della CGUE. I giudici belgi, diversamente, cercano di offrire l'occasione alla Corte di Giustizia di meglio chiarire i limiti e i criteri indicati nella *Tele2*, delimitandone i confini e l'estensione[63], chiarendo anche esplicitamente nel quesito del rinvio i diversi scopi per i quali la *data retention* viene posta in essere: finalità che ricoprono non solo la lotta alla criminalità ma anche attività poste in essere da autorità di intelligence, quindi per scopi di sicurezza nazionale, nonché da altre autorità che operano nell'ambito della ricerca di persone scomparse o che sono chiamate ad intervenire in situazioni di emergenza. Quasi a suggerire, anche in questo caso e ancora una volta solo tra le righe, che l'impatto di una conferma chiara e netta della incompatibilità di una conservazione generalizzata potrebbe avere conseguenze ampie e in grado di interessare diversi ambiti e profili, che la CGUE dovrebbe tenere in

[63] F. VERBRUGGEN, S. ROYER, H. SEVERIJNS, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, in *European Law Blog*, op. cit.

debita considerazione. Così come non dovrebbe essere ignorata neppure la più recente giurisprudenza della Corte EDU, che i giudici belgi espressamente richiamano, mettendone in luce i passaggi che potrebbero far propendere per una lettura meno rigida dei requisiti sanciti nella *Tele2*: un richiamo sicuramente 'utilitaristico' sotto questo profilo, considerando come l'attenzione non venga posta ad esempio su quelle pronunce, quali *Zakharov* o *Szabo*, che avevano invece portato i giudici di Strasburgo a fissare criteri – quali la notifica e la sussistenza di una connessione tra sorveglianza e minaccia per la sicurezza – certamente più in linea con la giurisprudenza della CGUE; ma altrettanto senza dubbio pare evidente come la Corte costituzionale abbia voluto, con tale richiamo, evidenziare anche le più recenti evoluzioni giurisprudenziali in materia di diritti fondamentali e sorveglianza massiva che dovrebbero comunque stimolare quantomeno una riflessione nei giudici di Lussemburgo.

4.1. – I possibili riflessi delle sentenze della CGUE e i timori sulle reazioni di un legislatore nazionale che non è disposto a rinunciare allo strumento di conservazione generalizzata

Considerati tutti questi profili e le rilevate possibili implicazioni di una pronuncia in materia, diviene chiaro come non solo la società civile ma anche il legislatore belga stia guardando con grande attenzione e attesa alla CGUE: le Conclusioni dell'Avvocato generale vanno nella direzione di una conferma della posizione espressa dai ricorrenti nel procedimento dinnanzi alla Corte costituzionale, riaffermando la incompatibilità, *per se*, di una forma di *bulk data retention* con il diritto dell'UE. Pur proponendo, come si è visto nel Capitolo IV, Parte II, una lettura più sfumata quanto alle discipline di conservazione dei metadati alternative a quella generalizzata, individuando non solo nella forma targettizzata bensì anche nella conservazione limitata una legittima e più efficace soluzione, l'Avvocato generale ha affermato con chiarezza come il legislatore belga dovrebbe trovare e percorrere una strada differente da quella tracciata nella legge del 2016. Ne consegue che, se la CGUE dovesse confermare tale visione, si verrebbe a riproporre nuovamente la situazione già verificatasi in passato a seguito della sentenza *DRI*: la legge nazionale, considerata sulla base dei parametri indicati dai giudici di Lussemburgo, dovrebbe essere giudicata incostituzionale, sancendo la necessità di un ennesimo intervento normativo in materia. Il legislatore dovrebbe quindi provvedere in quel caso ad adottare una nuova normativa, questa volta escludendo definitivamente la possibilità di una conservazione generalizzata e quindi abbandonando totalmente quell'obbligo di *data retention* valido per tutti i fornitori di servizi di telecomunicazione e riguardante tutti gli utenti e tutti i dati da essi prodotti. Ma le conseguenze potrebbero essere ulteriori e ancora più profonde: il timore, evidenziato da taluni studiosi[64], è che un tale sviluppo, dettato dalla necessità di un rinnovato intervento normativo, potrebbe portare, sul piano concreto, a privilegiare e rafforzare il ricorso allo strumento della cosiddetta *obligation de coopération*, stabilita dalla legge del 25 dicembre 2016[65], che ha modificato, tra gli altri, l'art. 46bis del *Code d'instruction criminelle*, rispetto a quanto previsto dalla legge del maggio 2016 sino ad ora esaminata: sulla base del più recente dettato normativo, tale disposizione, infatti, consente ora alle autorità giudiziarie (il Procuratore in particolare) di richiedere, in tempo reale, l'accesso ai dati identificativi degli abbonati o utenti a determinati servizi nonché la lista delle utenze aperte a nome di un determinato soggetto, per finalità di repressione di reati, senza alcuna specificazione circa la gravità degli stessi. Tale richiesta può essere estesa a tutti coloro "qui met à disposition ou offre, sur le territoire belge, un service qui consiste à transmettre des signaux

[64] F. COUDERT, F. VERBRUGGEN, *Conservation des données de communications électronique en Belgique: un juste équilibre?*, op. cit.

[65] *Loi du 25 décembre 2016 portant des modifications diverses au Code d'instruction criminelle et au Code penal, en vie d'ameliorer les methods particulières de recherché et certaines mesures d'enquete concernant internet, les communications électroniques et les télécommunications et créant une banque de données des empreintes vocales*, M.B. 17 janvier 2017, p. 2738.

via des réseaux de communications électroniques ou à autoriser des utilisateurs à obtenir, recevoir ou diffuser des informations via un réseau de communications électroniques, y compris les fournisseurs de service de communications électroniques", così comprendendo anche i servizi forniti da Yahoo, Google, Whatsapp e Skype, ovveero i cosiddetti servizi OTT (Over the Top). Per quanto l'efficacia ed utilità di un tale accesso sia da valutare ed accertare, considerando che ciò che viene consentito è solo l'ottenimento di dati identificativi a disposizione del *service provider* al momento della richiesta avanzata, questa misura può risultare comunque in una ingerenza nella sfera privata, similmente a quanto disposto dalla legge del 25 maggio 2016, che permette però, a differenza della disciplina ora riportata, di 'andare indietro nel tempo' e non di effettuare richieste di dati in tempo reale. Sul punto dunque "Il existe un risque que les autorités compétentes aient par exemple accès à plus de données sous l'obligation de coopération, qui n'est pas limitée aux infractions graves, que sous le régime actuel interprété à la lumière de l'arrêt *Tele2*"[66].

È infine utile sottolineare come l'attuale normativa belga sulla conservazione e accesso dei metadati riguardi anche le attività poste in essere dalle autorità di intelligence, avendo modificato la legge che ne regola l'operato: se la CGUE e, successivamente, la Corte costituzionale dovessero confermare l'incompatibilità di un regime di conservazione generalizzata, si potrebbe assistere ad una separazione delle due discipline sulla base dei soggetti e delle finalità che le caratterizzano, prevedendo così solo per la conservazione ed accesso da parte di autorità di *law enforcement* il rispetto dei criteri definiti dalla giurisprudenza europea; tale possibilità sarebbe ovviamente legata però all'esito dell'ulteriore rinvio pregiudiziale *Privacy International* promosso dal IPT inglese. Se infatti la CGUE dovesse far propri i rilievi dell'Avvocato generale, le uniche attività di totale competenza regolamentare degli Stati membri, e dunque poste al di fuori dell'ambito di applicazione del diritto dell'UE, sarebbero da individuarsi nelle forme di intercettazione e dunque di conservazione ed accesso diretto da parte di autorità pubbliche, che non prevedono cioè l'intervento o il trattamento dei metadati da parte di operatori privati. La preoccupazione[67] in questo caso è che, sulla base di una tale interpretazione, gli Stati membri – e dunque anche il Belgio – possano reagire implementando e rafforzando forme di sorveglianza diretta, svincolate dai criteri delineati dalla CGUE, sebbene sottoposte certamente al rispetto dei diritti tutelati dalla Convenzione EDU e dalla giurisprudenza della Corte EDU che, tuttavia in alcune delle sue ultime decisioni[68], come si è detto, pare lasciare maggior discrezionalità agli Stati ed accettare più ampiamente sistemi di sorveglianza massiva.

I due rilievi qui svolti e relativi alle reazioni che il legislatore nazionale potrebbe adottare, sono quindi finalizzati a far riflettere sui rischi che una posizione rigida della CGUE, che metta al bando la *bulk data retention*, potrebbe comportare, portando cioè i Governi nazionali alla adozione di forme alternative di conservazione e accesso ai dati dei propri cittadini, differenti da quelle oggetto delle decisioni dei giudici di Lussemburgo, pur di continuare a sfruttare le potenzialità derivanti dall'impiego di dati per scopi securitari, cui nessuno Stato membro pare intenzionato a rinunciare.

Anche sotto il profilo della legge in materia di PNR, si dovrà attendere la decisione della CGUE per valutare se la relativa normativa nazionale potrà essere considerata conforme o meno al diritto dell'UE e alla Carta di Nizza nonché alla Costituzione belga stessa, considerando poi l'impatto, prima evidenziato, che le valutazioni in tale ambito possono rappresentare per la disciplina della conservazione dei metadati.

Molti dunque sono i profili in attesa di definizione nell'ambito interno e rispetto ai quali la posizione che i giudici di Lussemburgo decideranno di adottare risulterà quanto mai determinante e dirimente.

---

[66] F. COUDERT, F. VERBRUGGEN, *Conservation des données de communications électronique en Belgique: un juste équilibre?*, op. cit., p. 266.

[67] F. VERBRUGGEN, S. ROYER, H. SEVERIJNS, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, op. cit.

[68] Si rimanda sul punto al Capitolo V, Parte II.

CAPITOLO III

L'ITALIA.
UNA ANALISI CRITICA DEI MOLTEPLICI INTERVENTI NORMATIVI E GIURISPRUDENZIALI IN MATERIA DI *DATA RETENTION*, TRA OCCASIONI PERDUTE E UN SERIO DIBATTITO CHE FATICA AD AFFERMARSI

Come si è avuto modo di vedere nei precedenti Capitoli, gli Stati membri sono stati portatori di approcci differenti rispetto al tema delicato e complesso della disciplina della *data retention*: nonostante il Regno Unito abbia mostrato una certa difficoltà – quando non una vera e propria riluttanza – ad applicare tutti i requisiti indicati dalla giurisprudenza della CGUE, sia il legislatore che i giudici nazionali sono più volte intervenuti in materia, evidenziando la necessità di modificare l'assetto normativo esistente ed adeguarlo, seppur secondo una interpretazione meno rigida, alle vicissitudini avvenute a livello dell'UE; il legislatore così come la Corte costituzionale belga hanno mostrato, invece, un atteggiamento più coerente con quanto affermato dai giudici di Lussemburgo e hanno avviato profonde riflessioni su come e in che misura un obbligo di conservazione possa ritenersi conforme e proporzionato ai diritti garantiti dalla Costituzione e dalla Carta di Nizza, sottolineandone le problematiche e le maggiori criticità attuative e richiedendo alla CGUE un intervento chiarificatore. Nei richiamati Stati membri, entrambi protagonisti di un intenso dialogo con i giudici di Lussemburgo, si è dunque assistito ad un ampio dibattito precedente o successivo alla adozione di specifiche normative sulla *data retention*; anche le Corti nazionali, spesso chiamate a pronunciarsi mediante l'intervento di ONG e cittadini, hanno dimostrato una profonda conoscenza della tematica, della complessità dei suoi risvolti e delle diverse interpretazioni di cui la giurisprudenza della CGUE è stata oggetto, dinnanzi alla sfida del bilanciamento tra diritti fondamentali e strumenti volti a garantire la sicurezza.

In questo articolato panorama, che conosce in realtà situazioni analoghe anche in altri Stati membri, nei quali similmente la *data retention* è stata al centro di importanti e dibattuti interventi normativi e giurisprudenziali[1], l'Italia presenta certamente un percorso singolare: esso può, sin da ora, essere riassunto da un lato nella quasi totale mancanza di considerazione, da parte del legislatore, dei principi affermati dai giudici di Lussemburgo e dell'ampio dibattito che è scaturito circa la loro corretta concretizzazione all'interno delle normative nazionali; dall'altro nella costante adozione, da parte dei giudici nazionali, di letture fortemente "restrittive degli standard garantistici enunciati dalla CGUE (..). L'intento è quello di salvare la disciplina interna sulla conservazione dei dati ed evitare ipotesi di inutilizzabilità probatoria"[2].

Questo approccio emerge dall'analisi della evoluzione normativa e dunque degli interventi che il legislatore italiano ha posto in essere, talvolta con scelte che paiono del tutto anacronistiche rispetto al dibattito in corso e che sono peraltro passate pressoché inosservate in sede parlamentare, nonostante il forte impatto sui diritti fondamentali e una spiccata lontananza – se non vera e propria divergenza – da quanto affermato dalla CGUE nelle sue storiche sentenze. Del tutto in linea con questo approccio si collocano anche le pronunce giurisprudenziali che si sono susseguite negli anni e che hanno non solo confermato la legittimità e la compatibilità con il diritto dell'UE delle disposizioni italiane in materia di

[1] Sul punto si rimanda specificamente ai Capitoli II e IV della Parte II di questo lavoro, nei quali vengono illustrate le più rilevanti reazioni degli Stati membri alle sentenze della CGUE.
[2] L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019, p. 757.

data retention ma anche rifiutato di cogliere quelle problematicità che hanno invece spinto molte altre Corti nazionali a promuovere rinvii pregiudiziali alla Corte di giustizia.

Ecco quindi che si rende necessario provvedere ad una ricostruzione critica dell'assetto normativo e dei più significativi interventi giurisprudenziali che consentiranno di tracciare un quadro della disciplina italiana della conservazione e accesso ai metadati per scopi securitari e che permetteranno di muovere alcune considerazioni finali.

1. – Un travagliato percorso normativo: il Codice Privacy, la discussa Legge Europea 2017 e il D. Lgs. n. 101/2018

1.1. – Un panorama normativo confuso: il susseguirsi di modifiche all'art. 132 Codice Privacy e la previsione di discipline 'derogatorie' che divengono, nei fatti, la 'regola'

Nell'ordinamento italiano, la principale disposizione di riferimento in materia di *retention* per scopi securitari dei metadati[3] derivanti da servizi di telecomunicazione è senza dubbio da individuarsi nell'art. 132 del D. Lgs. 196/2003, meglio noto come Codice Privacy. Questo, nella sua versione originale, prevedeva un generale obbligo di conservazione dei metadati (o "dati esterni") relativi al solo traffico telefonico per una durata di trenta mesi, posto in capo ai fornitori di servizi di telefonici[4] e per finalità di accertamento e repressione di reati[5]. È bene precisare sin da subito come tale misura, predisposta ben prima della adozione della DRD, risultasse attuativa di quanto stabilito dall'art. 15 della direttiva *e-Privacy* e dunque di quella facoltà, concessa agli Stati membri, di predisporre una disciplina derogatoria rispetto all'obbligo generale di cancellazione (o anonimizzazione) dei dati e metadati. Si veniva quindi a creare un regime di *bulk data retention* volto a consentire alle autorità di *law enforcement* l'accesso ai dati conservati per una generica finalità di repressione di qualsiasi reato, senza alcun riferimento al carattere di 'gravità' dello stesso: non risultava dunque in alcun modo necessario che lo scopo perseguito fosse di una severità tale da giustificare la significativa ingerenza nella vita privata degli utenti. Questa caratteristica di base dell'approccio italiano alla materia verrà mantenuta immutata: sin da ora, infatti, può essere sottolineato come, diversamente da molti altri ordinamenti europei, la disciplina italiana e il Codice Privacy in particolare non predisporranno mai una soglia – ad esempio individuata facendo riferimento alla pena o agli anni di reclusione – volta a determinare la gravità dei reati per i quali conservazione ed accesso devono essere ritenuti legittimi, così come non sarà mai predisposta alcuna targettizzazione quanto alla *data retention,* nonostante i molteplici interventi normativi succedutesi nel

[3] Con riferimento invece al diverso accesso ed acquisizione da parte delle autorità di *law enforcement* al contenuto delle comunicazioni dovrebbe essere applicata la disciplina relativa alle intercettazioni telefoniche, di flussi telematici o informatici che richiedono, lo si vuole ricordare, una autorizzazione da parte del giudice. Per maggiori approfondimenti sul punto, si rimanda, *ex multis* e sotto un profilo strettamente penalistico, a S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018 e A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, 2019.

[4] Venivano quindi all'epoca esclusi i dati telematici e i fornitori di tali servizi.

[5] Tale disciplina rappresentava una deroga alla regola generale fissata all'art. 123 del medesimo Codice, secondo cui il trattamento dei dati da parte dei fornitori di servizi di telecomunicazione doveva essere limitato a quanto strettamente necessario per finalità di fatturazione, pagamento in caso di interconnessione, documentazione in caso di contestazione della fattura o per pretesa di pagamento e per un periodo comunque non superiore a sei mesi. Con riferimento a tale norma dunque il principio guida generale "è quello della c.d. *data protection* (in contrapposizione alla *data retention*), per cui il soggetto interessato ha diritto a non vedere diffondere all'esterno aspetti della propria vita privata, nella specie i dati relativi alle proprie comunicazioni telefoniche", C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, 2008, p. 399 ss.

corso del tempo e che verranno in questo paragrafo analizzati nelle loro caratteristiche fondamentali nonché nelle loro criticità.

Procedendo in ordine temporale, la prima modifica dell'art. 132 è stata posta in essere proprio a pochi mesi dalla adozione del Cod. Privacy, con il D. l. 24 dicembre 2003, n. 354 (convertito con L. n. 45, 26 febbraio 2004). Piuttosto singolarmente, quindi, l'art. 132 veniva variato ancor prima di entrare in vigore e di divenire operativo: il testo riformato stabiliva innanzitutto una durata della conservazione, per finalità generiche di repressione e accertamento dei reati, pari a ventiquattro mesi, inserendo però poi una distinzione (c.d. doppio binario) riguardante la conservazione dei metadati con riferimento ai reati più gravi, individuati in quelli previsti dall'art. 407, co. 2, lett. a) c.p.p.[6] e i delitti a danni di sistemi informatici e telematici, per i quali veniva introdotta una durata di conservazione di ulteriori ventiquattro mesi aggiuntivi ai ventiquattro già previsti, arrivando quindi ad un massimo di quattro anni totali[7].

Quanto poi alla disciplina che regolava l'accesso e le procedure di richiesta di acquisizione dei metadati, veniva individuato come atto necessario un decreto motivato del giudice, su istanza del pubblico ministero, del difensore dell'imputato, di persona sottoposta a indagini, persona offesa e altre parti private[8]. Il comma 3 della disposizione in esame inoltre stabiliva una distinzione tra dati relativi

[6] Essi sono "i delitti appresso indicati: 1) delitti di cui agli articoli 285 (devastazione, saccheggio e strage), 286 (guerra civile), 416 bis (associazioni di tipo mafioso anche straniere) e 422 del codice penale (strage), 291-ter, limitatamente alle ipotesi aggravate previste dalle lettere a), d) ed e) del comma 2, e 291-quater, comma 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43; 2) delitti consumati o tentati di cui agli articoli 575 (omicidio), 628, terzo comma (rapina), 629, secondo comma (estorsione), e 630 dello stesso codice penale (sequestro di persona a scopo di estorsione); 3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416 bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo; 4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, terzo comma (associazione sovversiva), [270 bis 2], e 306, secondo comma, del codice penale (banda armata); 5) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2, comma terzo, della legge 18 aprile 1975, n. 110; 6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, comma 2, e 74 del Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni; 7) delitto di cui all'articolo 416 del codice penale (associazione per delinquere) nei casi in cui è obbligatorio l'arresto in flagranza; 7 bis) dei delitti previsti dagli articoli 600 (riduzione o mantenimento in schiavitù o in servitù), 600 bis, comma 1, 600 ter, primo e secondo comma, 601, (tratta di persone), 602 (acquisto e alienazione di schivi), 609 bis (violenza sessuale) nelle ipotesi aggravate previste dall'articolo 609 ter, 609 quater, 609 octies del codice penale, nonché dei delitti previsti dall'art. 12, comma 3, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni".

[7] Questa modifica, così rapidamente adottata, ha rappresentato la risposta alle forti critiche che avevano accompagnato la prima versione dell'art. 132, Codice Privacy, considerato pericoloso e potenzialmente dannoso in quanto rischiava di causare la perdita di informazioni e metadati di rilevante importanza per le indagini e i procedimenti penali: "la straordinaria necessità e urgenza del D. l. 24 dicembre 2003, n. 354 è stata motivata sulla base del danno irreparabile che l'originario articolo 132, una volta entrato in vigore, avrebbe prodotto, ossia l'eliminazione dei dati per i quali il periodo di custodia era scaduto; è lo stesso decreto legge a evidenziare la necessità di prevenirne la perdita nell'ipotesi in cui ne risulti necessaria l'acquisizione, in particolare, ai fini della repressione di reati di particolare gravità", M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Diritto Penale Contemporaneo*, 3, 2016, p. 171. Come lo stesso autore sottolinea, la legge di conversione ha introdotto rilevanti modifiche rispetto al testo originario del D. l.: nella versione finale infatti sparivano i riferimenti ai dati telematici, che invece erano stati inseriti inizialmente tra le categorie di metadati da conservare, nonché la più ampia durata di trenta mesi, aumenta a sessanta per reati gravi; veniva anche previsto, in una ottica maggiormente garantista, l'intervento autorizzatorio del giudice, mentre il Decreto attribuiva tale compito anche al pubblico ministero.

[8] Merita sottolineare come, diversamente dalla legge di conversione, il Decreto avesse impiegato un termine più ampio, parlando di "decreto motivato dell'autorità giudiziaria"; solo successivamente la legge ha inasprito la modalità di accesso, richiedendo esclusivamente il decreto motivato del giudice.

alle chiamate in arrivo e in uscita. Solo per le prime, infatti, veniva previsto, con un procedimento più rapido e snello, che l'accesso potesse avvenire ad opera del difensore dell'imputato mediante richiesta diretta al fornitore del servizio di comunicazione, con il limite però di dimostrare che l'ottenimento dei dati fosse finalizzato a prevenire un pregiudizio alle indagini difensive. L'accesso ai dati per esigenze di repressione dei reati gravi indicati dal legislatore stesso e sopra richiamati poteva invece avvenire solo con l'autorizzazione del giudice mediante decreto motivato qualora egli ritenesse sufficienti gli indizi relativi alla sussistenza dei delitti indicati.

A pochi anni di distanza, il c.d. Decreto o Pacchetto Pisanu, contenente misure urgenti per il contrasto del terrorismo internazionale (D. l. 27 luglio 2005, n. 144, convertito con L. n. 155 del 31 luglio 2005), prevedeva una ulteriore rilevante novità che andava a toccare l'efficacia applicativa dell'art. 132 Cod. Privacy: a seguito degli episodi terroristici di Madrid e Londra, che avevano riaffermato con forza l'esigenza di una ampia tutela della sicurezza all'interno del dibattito e delle decisioni politiche, veniva prevista una deroga alla regola della durata di conservazione indicata dall'art. 132; al fine di indagine e repressione dei soli reati di terrorismo, infatti, tutti i metadati avrebbero dovuto essere trattenuti dagli operatori sino al 31 dicembre 2007, con una estensione fissata cioè ad una data specifica e con una scelta che, come si vedrà, verrà impiegata dal legislatore italiano anche nei successivi interventi normativi[9]. Venivano però poi sostanzialmente modificati anche i termini di conservazione e la procedura di accesso generali: mentre restavano invariati i ventiquattro mesi previsti per i dati relativi al traffico telefonico, cui si aggiungevano anche quelli attinenti alle chiamate senza risposta, veniva poi per la prima volta imposto anche l'obbligo di conservazione dei dati telematici, per un periodo di sei mesi, escludendo sempre i contenuti delle comunicazioni stesse. Veniva inoltre mantenuta la distinzione (c.d. doppio binario) tra reati in generale e quelli di cui all'art. 407, comma 1, lett. a) c.p.p. e per i delitti a danno di sistemi informatici e telematici, per quali era nuovamente previsto un periodo di conservazione più ampio, di ulteriori ventiquattro mesi per i dati di traffico telefonico e sei mesi per i dati di traffico telematico. Per questi specifici reati maggiormente gravi, la richiesta di accesso ai dati doveva essere autorizzata dal giudice, mentre la disciplina generale dell'accesso subiva una sostanziale modifica quanto a tutti gli altri reati: diveniva infatti sufficiente il mero decreto motivato del pubblico ministero, secondo una scelta che pareva fondarsi su "esigenze di snellimento della procedura"[10].

Mentre sino a tale momento le riforme alla disciplina della *data retention*, con ravvicinate e confuse continue deroghe, risultavano comunque tutte attuative dell'art. 15 direttiva *e-Privacy*, con D. Lgs. n. 109 del 30 maggio 2008 veniva effettuato un intervento volto a dare attuazione alla direttiva 2006/24/CE e che ha provveduto a modificare, forse in maniera più significativa, l'art. 132 Cod. Privacy[11]. Risultava

[9] "A decorrere dalla data di entrata in vigore del presente decreto e fino al 31 dicembre 2007 è sospesa l'applicazione delle disposizioni di legge, di regolamento o dell'autorità amministrativa che prescrivono o consentono la cancellazione dei dati del traffico telefonico o telematico, anche se non soggetti a fatturazione, e gli stessi, esclusi comunque i contenuti delle comunicazioni, e limitatamente alle informazioni che consentono la tracciabilità degli accessi, *nonché, qualora disponibili,* dei servizi, debbono essere conservati fino a quella data dai fornitori di una rete pubblica di comunicazioni o di un servizio di comunicazione elettronica accessibile al pubblico, fatte salve le disposizioni vigenti che prevedono un periodo di conservazione ulteriore. I dati del traffico conservati oltre i limiti previsti dall'art. 132 del decreto legislativo 30 giugno 2003, n. 196, possono essere utilizzati esclusivamente per le finalità del presente decreto-legge".

[10] M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, op. cit., p. 176. Una scelta, questa, in realtà piuttosto dibattuta e contestata: "la soluzione maggiormente equilibrata, in linea con la disciplina dettata per i mezzi di ricerca della prova tradizionali (ispezioni, perquisizioni, sequestri), era la previsione del decreto motivato dell'autorità giudiziaria. Non ha senso, infatti, negare al giudice la legittimazione all'acquisizione", S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, 2019, p. 1584.

[11] Con L. n. 48, del 18 marzo 2008, si era provveduto a modificare nuovamente l'art. 132, prevedendo un obbligo di conservazione da tre a sei mesi dei dati di traffico, a fini di svolgimento di indagini preventive e per accertamento e repressione di determinati reati. In questa sede si vuole tuttavia concentrare l'attenzione sugli interventi normativi più rilevanti e di maggiore impatto, pur nella consapevolezza che, oltre a quelli elencati, anche altre normative

infatti superata la previa distinzione tra reati genericamente intesi, reati indicati dall'art. 407, co. II, lett. a), c.p.p. nonché reati di terrorismo, così che per la finalità generica di repressione di qualsiasi reato veniva imposta una durata fissa di conservazione di due anni per il traffico telefonico, un anno per il traffico telematico e trenta giorni per le chiamate senza risposta. Rimaneva immutata la disciplina di accesso, sulla base della quale i metadati potevano essere richiesti con decreto motivato del pubblico ministero, anche su istanza presentata dal difensore dell'imputato, del soggetto sottoposto ad indagini, della vittima o ancora di altre parti private[12], così come restavano invariate le disposizioni, già previste nel dettato normativo precedente, attinenti alla possibilità per il difensore dell'imputato o indagato di richiedere talune tipologie di metadati direttamente ai fornitori, alle specifiche condizioni che sono state sopra indicate.

Sulla base della evoluzione normativa sin qui tratteggiata, quindi, si nota una certa schizofrenia legislativa, per la quale le maggiori tutele precedentemente previste, identificate ad esempio nella attribuzione al giudice del compito di emanare il decreto motivato di autorizzazione dell'accesso per i dati telematici nel caso di richiesta a scopo di indagine di reati gravi, venivano progressivamente meno: "il decreto ha definitivamente escluso, ai fini dell'acquisizione, qualsiasi rilevanza della tipologia delle fattispecie criminose per cui si procede, parallelamente a una *reductio ad unum* delle modalità e degli organi legittimati a disporre dei dati"[13].

Ecco quindi che già in questi interventi le scelte di fondo e l'approccio del legislatore italiano in materia di *data retention* sono risultati in toto confermati: non viene proposto alcun riferimento alla gravità del reato bensì viene mantenuto il richiamo ampio allo scopo di repressione dei reati; il soggetto individuato per svolgere la richiesta di accesso viene identificato, nella generalità dei casi, nel pubblico ministero; non vengono imposte specifiche misure di sicurezza in capo ai fornitori di servizi, ai quali viene lasciata ampia discrezionalità anche nella determinazione delle "procedure interne" da porre in essere per rispondere alle richieste di accesso avanzate dalle autorità di *law enforcement*.

Proprio questi elementi e caratteristiche erano state oggetto di particolare attenzione da parte della dottrina che aveva iniziato, già all'indomani della sentenza *DRI*, a riflettere seriamente sulle implicazioni dell'invalidazione della DRD per la disciplina italiana e ad interrogarsi sulla conformità della normativa nazionale rispetto ai requisiti individuati dalla CGUE, sebbene con riferimento ad una fonte di diritto dell'UE. Molti autori avevano statuito, infatti, con decisione come le condizioni disposte dall'art. 132 Cod. Privacy non potessero essere considerate compatibili con gli elevati standard di tutela elaborati dai giudici di Lussemburgo: mancavano l'individuazione degli elementi determinanti le categorie di reati per le quali fosse possibile provvedere all'accesso, dei criteri oggettivi volti a fissare un nesso tra conservazione, accesso e pericolo o sospetto di un reato e dunque di una forma di

---

sono intervenute in materia nel corso del tempo. Per una più approfondita analisi della interezza degli interventi normativi intercorsi a partire dal 2003, si rimanda a C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, op. cit; P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1, 2016; mentre per una analisi riguardante la disciplina normativa e la giurisprudenza attinente al periodo precedente alla adozione dell'art. 132 Cod. Privacy, che qui non si vuole prendere in esame, si richiama: M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, op. cit.; G. M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, 2019, p. 1599 ss.

[12] Il dibattito, anche giurisprudenziale, finalizzato a definire quali fossero i soggetti abilitati a richiedere l'accesso ai metadati conservati e le procedure da seguire, è stato ampio: prima si riteneva che l'ottenimento dei tabulati telefonici dovesse ad esempio essere sottoposto alle medesime regole processuali valide per le intercettazioni; per passare poi a considerare sufficiente un decreto motivato del Pubblico ministero, successivamente proponendo una autorizzazione del giudice su richiesta avanzata da p.m., optando infine, per il mero decreto del p.m. Questi aspetti e la giurisprudenza maggiormente rilevante in materia di accesso, con parallelismi riferiti alla disciplina delle intercettazioni, sono analizzati da P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, op. cit., nonché M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, op. cit.

[13] M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, op. cit., p. 181.

targettizzazione del regime di conservazione e accesso; risultava dubbio il carattere di indipendenza del pubblico ministero e dunque della corretta attribuzione ad esso dell'unica forma di controllo preventivo svolta sulla richiesta di accesso stesso[14].

1.2. – Le 'schizofreniche' riforme alla normativa in materia di **data retention** *e accesso ai metadati: le critiche rispetto al mancato adeguamento ai criteri delineati dalla CGUE e l'assenza di un intervento coerente ed organico*

La problematicità e – per gran parte della dottrina che si è occupata del tema – l'insanabile ed evidente contrasto tra la disciplina italiana e quanto delineato dalla CGUE, avevano portato, ancor prima della sentenza *Tele2* avente ad oggetto normative nazionali attuative dell'art. 15 direttiva *e-Privacy*, ad invocare diverse possibili mutamenti ed evoluzioni nel panorama italiano: sebbene un intervento da parte del legislatore europeo fosse ritenuta la soluzione maggiormente auspicabile[15], poiché avrebbe risolto in maniera univoca per tutti gli Stati membri i complessi problemi di bilanciamento tra diverse esigenze e diritti interessati, come noto, il silenzio normativo a livello dell'UE ha continuato e continua a perdurare sino ad oggi, considerato che, successivamente alla DRD, nessuna legislazione in materia di *data retention* è stata mai approvata. Così, in quello che è stato definito il 'silenzio assordante' del normatore europeo, il compito di adeguare la disciplina nazionale al diritto dell'UE avrebbe dovuto essere posto nelle mani del legislatore italiano: seguendo le orme di quanto svolto da altri Stati membri (Regno Unito, Lussemburgo e Germania, ad esempio), il Governo e/o il Parlamento avrebbero dovuto promuovere un'azione volta a verificare innanzitutto che la normativa italiana fosse conforme a quei

[14] R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata quaestio(?)*, in *Diritto Penale Contemporaneo*, 3, 2017; similmente, anche Iovene afferma che, alla luce dei parametri fissata dalla giurisprudenza europea, l'art. 132 Cod. Privacy non rappresenta una limitazione legittima dei diritti tutelati dalla CGUE: "Tale norma non pone alcun limite, oltre a quello strettamente temporale, alla conservazione dei dati di traffico telefonico e telematico, che risulta quindi indiscriminata; non limita a particolari forme gravi di criminalità l'uso dei dati (..); non prevede specifiche modalità per l'accesso, né richiede il vaglio di un giudice o di altra autorità indipendente (..); non distingue la durata della conservazione in base all'obiettivo perseguito o alla persona interessata ma semplicemente distinguendo tra dati relativi al traffico telefonico, a quello telematico e alle chiamate senza risposta; non prevede misure per la sicurezza dei dati", giungendo quindi alla conclusione secondo cui la disciplina esaminata non può essere considerata conforme ai criteri delineati dalla CGUE (F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, in *Cassazione Penale*, 12, 2014). Anche Caputo si esprime in questi termini: "ci troviamo evidentemente di fronte ad una normativa, l'art. 132 Cod. Privacy, che non risponde a quanto richiesto dalla sentenza della CGUE almeno per ciò che concerne il rapporto fra l'obbligo di conservare i dati e una minaccia per la sicurezza pubblica e la mancata previsione che tale obbligo sia correlato alla necessità di prevenire gravi reati", P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, op. cit. Dello stesso avviso Marcolini, che afferma "pare difficilmente negabile che, se oggetto di scrutinio da parte della CGUE fosse stata non la Dir. 2006/24/CE, bensì l'art. 132 Cod. Privacy, l'esito sarebbe stato identico. A tacere di ogni altro profilo, una disciplina, quale quella nazionale, che consente la *data retention* per qualsiasi reato, anche in ipotesi di una contravvenzione di minima gravità, non supererebbe nemmeno lontanamente lo stress test comunitario", S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, op. cit., p. 1592. Basti pensare inoltre come alcune critiche alla disciplina dell'art. 132 fossero addirittura state mosse a partire dalle sue più risalenti formulazioni: G. E. VIGEVANI, *Articolo 132*, in AA.VV., *Codice della privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Giuffré, 2004, p. 1668, aveva espresso sin da subito dubbi e perplessità quanto ai pericoli che la disciplina in esame presentava per i diritti fondamentali, pur riguardando i soli metadati, non necessariamente ed automaticamente da considerarsi meno invasivi della sfera privata rispetto ai contenuti. Non si può non rilevare, tuttavia, per completezza, come alcuni autori avessero al contrario ritenuto la normativa italiana di trasposizione della DRD come eccessivamente restrittiva rispetto a quanto disciplinato dalla normativa dell'UE, vedendo nella durata più contenuta prevista dal decreto esaminato una tutela ulteriore e maggiore rispetto ai limiti più ampi stabiliti dalla Direttiva 2006/24 (M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, op. cit., p. 180).

[15] R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata quaestio(?)*, op. cit. e F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, op. cit.

criteri che potevano essere desunti dalla giurisprudenza della CGUE e, nel caso in cui la disciplina interna fosse stata trovata invece viziata dalle stesse carenze e violazioni dei diritti fondamentali che avevano caratterizzato la DRD, provvedere alla adozione di un nuovo testo normativo ed una nuova disciplina[16]. Similmente a quanto avvenuto a livello dell'UE, anche in Italia questo percorso non ha purtroppo avuto inizio.

Mentre in altri Stati membri (come il Belgio), nei quali pure il legislatore era rimasto inerme, i giudici nazionali erano stati però investiti di questioni di legittimità costituzionale della normativa attuativa della DRD, alla luce della sentenza della CGUE, fungendo così da motore propulsivo per un nuovo intervento normativo e imponendo al legislatore nazionale di avviare una più profonda riflessione sui criteri e requisiti che la nuova disciplina interna doveva possedere, in Italia le Corti nazionali non hanno svolto questo ruolo. Seppure l'analisi specifica e puntuale della giurisprudenza italiana in materia verrà elaborata nel successivo paragrafo, pare utile sin da ora sottolineare come non si sia all'epoca – e nemmeno oggi – registrata né alcuna pronuncia di incostituzionalità della disciplina di cui all'art. 132 Cod. Privacy, né una decisione di disapplicazione della normativa nazionale, sebbene auspicata da gran parte della dottrina.

Il mancato attivismo del legislatore e della giurisprudenza italiana hanno dunque contribuito, anche e nonostante i fondamentali e significativi interventi della CGUE, al mantenimento dello *status quo*. E non solo: l'art. 132 Cod. privacy infatti non è semplicemente rimasto intoccato a seguito della sentenza *DRI* ma, anziché propendere verso un percorso di maggior garanzia dei diritti fondamentali e dunque nella direzione di una disciplina più restrittiva in materia di *data retention*, l'Italia ha, anche a fronte delle ulteriori sentenze della CGUE in materia, imboccato un percorso inverso.

L'art. 132 Cod. Privacy, infatti, ha subito, dal 2015 in avanti, svariati altri interventi che ne hanno profondamente segnato la disciplina e che hanno determinato importanti cambiamenti applicativi. Il decreto legge antiterrorismo del 2015 (D. l. 18 febbraio 2015, n. 7, convertito con modificazioni dalla L. 17 aprile 2015, n. 43), adottato poco tempo dopo il terribile attentato terroristico che aveva colpito la sede del giornale satirico Charlie Hebdo a Parigi, aveva previsto, all'art. 4-bis, co.1, che "al fine di poter agevolare le indagini esclusivamente per i reati di cui agli articoli 51, comma 3-quater e 407, comma 2, lett. a) del c.p.p. (..) i dati relativi al traffico telefonico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto sono conservati dal fornitore fino al 31 dicembre 2016 per finalità di accertamento e repressione dei reati. Per le medesime finalità i dati relativi al traffico telematico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, esclusi comunque i contenuti della comunicazione, sono conservati dal fornitore fino al 31 dicembre 2016". La modifica o, ancor meglio, la deroga all'art. 132 Cod. Privacy, così introdotta[17], avrebbe cessato di decorrere a partire dal 1 gennaio 2017.

Con il D. l. 30 dicembre 2015, n. 210 (c.d. Decreto milleproroghe), convertito con modificazioni dalla L. 25 febbraio 2016, n. 21, però, il legislatore nazionale ha di nuovo operato in materia, ancora una volta senza agire direttamente sull'art. 132 Cod. Privacy bensì modificando la disposizione prevista dal

[16] Come ben precisato da Iovene, "spetta ai legislatori nazionali verificare se la normativa nazionale di attuazione della direttiva rispetti o meno le indicazioni fornite dalla CGUE. Infatti, poiché la direttiva lasciava margini di discrezionalità agli Stati membri in determinati ambiti, non è escluso che la legge nazionale rispetti i criteri guida contenuti nella sentenza", F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, op. cit., p. 4278. Del resto, come ricordato da Arena, anche secondo Cruz Villalon, Avvocato generale nel caso *DRI*, alcune discipline nazionali, laddove si fossero discostate dalla DRD, smorzandone o correggendone le criticità, avrebbero potuto risultare conformi al diritto dell'UE (par. 157, Conclusioni), A. ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014.

[17] "La modifica introdotta dall'art. 4-bis legge n. 43 del 2015 non costituisce una modifica al regime di conservazione dei dati di traffico telefonico e telematico previsto dall'art. 132 Cod. Privacy ma una previsione in deroga che riguarda unicamente i reati di cui agli artt. 51, co. 3-quater e 407, co. 2, lett. a)", P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, op. cit., p. 2.

previo decreto legge antiterrorismo: così facendo, l'art. 4-bis, co. 1 è stato riformato estendendo l'obbligo di conservazione, per i medesimi reati già da quella disposizioni indicati, sino al 30 giugno 2017. Tale decisione, che ancora una volta avveniva a poca distanza di tempo dagli attentati terroristici del novembre 2015 che avevano colpito nuovamente e con maggiore violenza la città di Parigi, rifletteva quindi la scelta effettuata dal legislatore già ad inizi 2015: quella cioè di porre in essere un intervento normativo motivato da ragioni emergenziali e dalla urgenza di rafforzare l'efficacia dello strumento della *data retention* ritenuto utile e prezioso per fronteggiare la minaccia terroristica[18]. Ancora una volta, quindi, la materia veniva modificata senza la predisposizione di una disciplina complessiva, di un intervento organico e maggiormente chiaro, anche per gli operatori dei servizi di telecomunicazione, che vedevano di volta in volta allungarsi i termini di conservazione mediante legislazioni che operavano continui rimandi incrociati alle fonti esistenti. L'impatto per i *service providers* inoltre era di non poco rilievo se si considera il risultato pratico provocato dal duplice intervento normativo esaminato: come già era avvenuto in passato quando ancora vigeva il c.d. doppio binario, il fornitore di servizi di telecomunicazione non poteva anticipatamente sapere se i metadati prodotti dai propri utenti sarebbero stati utilizzati nell'ambito di indagini riguardanti i reati previsti dai D. l. citati o per tutti gli altri reati per i quali i termini di conservazione restavano invece quelli fissati dall'art. 132 Cod. Privacy. L'effetto concreto era che il *service provider* si trovava costretto a conservare tutti i metadati prodotti dai propri utenti sino alla data da ultimo individuata nel 30 giugno 2017, al fine di poter essere nelle condizioni di assolvere, qualora fosse richiesto l'accesso ai dati, all'obbligo imposto dalla legge antiterrorismo e dal decreto milleproroghe. Sotto il profilo della conservazione, dunque, l'art. 4-bis, co. 1 dei D. L. del 2015 finiva, nei fatti, col soppiantare l'applicabilità della durata di *data retention* fissata all'art. 132 Cod. Privacy. Quest'ultima disposizione restava certamente operativa quanto alla disciplina dell'accesso laddove esso venisse richiesto per scopi di repressione e indagine di reati diversi da quelli indicati dall'art. 4-bis, co. 1: in tal caso, infatti, sebbene il fornitore avesse provveduto a conservare i dati per un periodo più prolungato, l'accesso sarebbe stato legittimo e valido solo nei termini temporali indicati dal Codice Privacy, e non oltre. In altre parole, nella pratica concreta, la conservazione veniva generalmente estesa, per esigenze pratiche, alla durata massima indicata dai D. l. susseguitisi nel 2015, mentre per quanto attiene all'accesso per scopi diversi da quelli in tali normative previsti, la possibilità di "andare indietro nel tempo" fornita alle autorità di *law enforcement* restava limitata a quanto stabilito dall'art. 132 Cod. Privacy. Diventa chiaro quindi come quella che avrebbe dovuto essere una eccezione, volta a fronteggiare una situazione emergenziale, è nei fatti divenuta una regola generale sotto il profilo della conservazione dei metadati.

1.2.1. – Il primato italiano di una conservazione dei metadati della durata di 72 mesi, introdotta 'furtivamente' con la Legge Europea 2017

Questa situazione particolarmente complessa per la peculiarità dell'intersecarsi di diverse normative e per la pratica conseguenza prodotta che ha finito per invertire regola straordinaria e disciplina 'ordinaria', è stata poi ancor più problematicamente riconfermata nel 2017: allo scadere della proroga definita con il secondo Decreto del 2015, l'art. 132 Cod. Privacy avrebbe dovuto tornare ad operare a pieno regime e la durata della conservazione e del relativo accesso ai metadati sarebbe quindi tornata ad essere la medesima per qualsiasi tipo di reato, senza alcuna distinzione. Il 20 novembre 2017, tuttavia,

[18] Come riportato da Scaffardi, "la ratio dell'estensione temporale rispetto alla normativa previgente si può desumere dalle schede di lettura che accompagnavano l'atto, vale a dire 'mettere a disposizione dell'autorità investigativa strumenti efficaci contro una minaccia, quella del terrorismo, sempre più grave ed estesa, che i mezzi informatici rendono pervasiva annullando i confini temporali e territoriali'", L. SCAFFARDI, *La data retention va in ascensore*, in *Forum di Quaderni Costituzionali*, 28 luglio 2017, p. 2.

con la c.d. Legge Europea 2017 (n. 167/2017), ovvero la Legge che reca le 'Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea', è stata introdotta, per mezzo di un emendamento al Disegno di Legge, una disposizione riguardante la conservazione dei metadati: l'art. 24, infatti, ha previsto che "in attuazione dell'art. 20 della Direttiva (UE) 2017/541 del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto al terrorismo, anche internazionale, per le finalità dell'accertamento e della repressione dei reati di cui agli artt. 51, co. 3-quater e 407, co. 2, lett. a) del c.p.p., il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'art. 4-bis del D. L. 18 febbraio 2015, n. 7 (..) è stabilito in settantadue mesi, in deroga a quanto previsto dall'art. 132 del Codice in materia di protezione dei dati personali". Ne emerge dunque come, per finalità di lotta al terrorismo o reati di simile gravità (i reati cui viene fatto rimando sono infatti essenzialmente delitti consumati o tentati con finalità di terrorismo e delitti di devastazione, saccheggio, strage, guerra civile, associazione di tipo mafioso) il periodo di conservazione dei metadati sia stato dilatato in maniera significativa ad una durata di ben sei anni. Sebbene ad una prima lettura tale misura possa sembrare di ristretto impatto, riguardando solo la conservazione e l'accesso per finalità limitate e particolarmente gravi, anche in questo caso – come già si è detto con riferimento ai previ interventi normativi – diviene di fondamentale importanza considerare il risultato pratico: il fornitore di servizi di telecomunicazione non può conosce in anticipo se i metadati relativi alle comunicazioni intrattenute dai propri utenti verranno utilizzati nell'ambito di indagini riguardanti i reati previsti dall'art. 24 della Legge Europea 2017 – e debbano dunque essere conservati per settantadue mesi – o per tutti gli altri reati, per i quali i termini di conservazione sono invece quelli fissati dall'art. 132 Cod. Privacy. Ancora una volta, pertanto, l'operatore sarà chiamato a conservare tutti i metadati raccolti per un periodo di settantadue mesi, in modo da poter fornire alle autorità di *law enforcement* i dati risalenti sino a sei anni prima laddove richiesti per reati di terrorismo o altri indicati dall'art. 407 c.p.p[19].

Si è venuta così a creare di nuovo la situazione complessa secondo cui l'art. 132 Cod. Privacy resta pienamente operativo sotto il profilo dell'accesso ai metadati per reati differenti da quelli disciplinati dall'art. 24 richiamato: "nel momento della trasmissione dei dati all'autorità giudiziaria il fornitore è obbligato a verificare che gli stessi siano riconducibili al periodo di conservazione che, a seconda del tipo di reato perseguito, risulta fissato dall'art. 132 Cod. Privacy o della legge europea 2017. Se ad esempio un dato da conservarsi per ventiquattro mesi (ma di fatto conservato per settantadue mesi per la ricordata ragione che è impossibile conoscere a priori per quale tipo di reato quel dato verrà richiesto), fosse richiesto dopo ventiquattro mesi ed un giorno sarebbero illegittime tanto la sua trasmissione quanto la sua acquisizione da parte dell'autorità giudiziaria"[20]. L'intervento normativo predisposto dall'art. 24 Legge Europea 2017 presenta pertanto due problematiche fondamentali: da un lato, ampliando così significativamente la durata della conservazione, sebbene per reati quali terrorismo e criminalità organizzata, si pone in una posizione divergente rispetto alla giurisprudenza della CGUE che neppure per finalità di lotta al terrorismo aveva ritenuto proporzionata una *data retention* di gran lunga inferiore.

[19] Sul punto, per una analisi dei pratici effetti per gli operatori economici del settore, si rimanda a G. NAZZARO, *Tabulati di traffico storico per finalità di accertamento e repressione dei reati: caratteristiche e tempi di conservazione*, in *Sicurezza e Giustizia*, 3, 2018, p. 58.

[20] S. SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 12 Codice Privacy da parte del D. Lgs. 10 agosto 2018, n. 101*, in *Diritto penale contemporaneo*, 11, 2018, p. 157. Sul punto, si evidenzia come la Corte di Cassazione avesse già più volte affermato l'inutilizzabilità di metadati risalenti ad un periodo superiore al termine massimo di conservazione stabilito dalla legge, come ad esempio stabilito nelle pronunce Corte di Cassazione, Sez. V Penale, 25 gennaio 2016, n. 7265: "Sono patologicamente inutilizzabili i dati relativi al traffico telefonico contenuti nei tabulati acquisiti dall'Autorità giudiziaria dopo i termini previsti dall'art. 132 D. Lgs. 30 giugno 2003, n. 196, atteso il divieto di conservazione degli stessi da parte del gestore al fine di consentire l'accertamento dei reati oltre il periodo normativamente predeterminato"; ma anche Corte di Cassazione, Sez. V Penale, sentenza n. 15613 del 5 dicembre 2014.

La motivazione di tale posizione, espressa dai giudici di Lussemburgo sin dalla sentenza *DRI*, era indicata nel fatto che non fosse "precisato che la determinazione della durata della conservazione dovesse basarsi su criteri obiettivi al fine di garantire che sia limitata allo stretto necessario" (sentenza *DRI*, par. 64): ebbene, tale specificazione, volta a comprovare la necessità di una conservazione tanto ampia, non pare essere stata presa in considerazione neppure dal legislatore italiano, che non ha fatto riferimento a studi o analisi finalizzate a determinare l'utilità e l'efficacia di una *data retention* tanto prolungata. Dall'altro lato, poi, l'estensione *de facto* della durata di *data retention* a settantadue mesi ha prodotto l'effetto di rendere la disciplina emergenziale, prevista per la straordinaria lotta al fenomeno terroristico, una disciplina ordinaria, quanto meno sotto il profilo della conservazione dei metadati[21].

Oltre a questi aspetti critici e per fugare qualsiasi dubbio o errore valutativo, è necessario precisare come la misura analizzata non abbia finito con l'introdurre alcuna qualificazione circa la gravità del reato, sulla base di quanto invece richiesto dalla giurisprudenza della CGUE: l'art. 24 Legge Europea 2017, come si è visto, interviene sulla durata della conservazione e dunque sulla possibilità di accesso ai metadati per specifiche categorie di reati, ritenuti sicuramente di una pericolosità e rilevanza tale da giustificare una *data retention* di gran lunga sopra il limite massimo di due anni previsto nel 2006 dalla DRD. Per tutti gli altri reati però la conservazione resta regolata, in maniera del tutto indistinta sotto il profilo del carattere di gravità, dall'art. 132 Cod. Privacy, che prevede sì una distinzione sulla base della tipologia di metadati e mezzi di comunicazioni interessati, ma nulla dice quanto alla finalità della conservazione e dell'accesso, che rimane quella generica di repressione dei reati, senza qualificazione o limitazione alcuna.

In conclusione, dunque, anche questo intervento normativo ha contribuito a creare un panorama confuso e ampiamente e da più parti criticato, sia per la scelta della fonte normativa impiegata, sia sotto il profilo della conformità al diritto dell'UE e alla giurisprudenza della CGUE. Con riferimento al primo aspetto, infatti, la modalità con la quale un inasprimento così significativo della disciplina della conservazione è stato adottato è sembrata quanto meno "furtiva"[22] e singolare: non bisogna ignorare che questa disposizione è stata inserita in una legge sugli adempimenti comunitari, preceduta da una disposizione di attuazione della Direttiva 2014/33 in materia di ascensori (!), anziché essere prevista in una normativa *ad hoc* e completa della materia. Ciò ha fatto sorgere il sospetto che il legislatore abbia voluto, "di soppiatto"[23] e senza attirare troppo l'attenzione, inserire nell'ordinamento una disposizione che avrebbe meritato invece, come è avvenuto in molti altri Stati membri, un ampio dibattito parlamentare, fondato su studi, analisi e dati oggettivi quanto più capaci di comprendere le reali esigenze investigative e di individuare la soluzione in grado di garantire al meglio un equilibrio tra diritti fondamentali e necessità securitarie. Sul punto, Walter Verini, uno degli allora Deputati che avevano presentato nell'estate 2017 l'emendamento integrante la modifica della disciplina della *data retention*, aveva motivato la decisione di tale proposta facendo riferimento alle affermazioni fornite dalla Procura nazionale antiterrorismo in occasione di alcune audizioni parlamentari, dalle quali era emersa l'esigenza di adottare nuovi strumenti di prevenzione e lotta al terrorismo, tra cui appunto, una conservazione dei metadati di più lunga durata. Se il bisogno di far fronte ad una situazione di emergenza cronicizzata può essere condiviso e potrebbe legittimamente giustificare un intervento normativo volto a differenziare la disciplina della conservazione dei dati a seconda della gravità del reato perseguito, pare evidente dalla

[21] S. SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 12 Codice Privacy da parte del D. Lgs. 10 agosto 2018, n. 101*, op. cit., p. 157.

[22] L. SCAFFARDI, *La data retention va in ascensore*, op. cit., p. 1.

[23] L. SCUDIERO, *La Camera porta di soppiatto la data retention a sei anni*, in *Lex Digital*, 21 luglio 2016, che afferma: "se possibile, più che il merito questa volta inquieta il metodo, secondo cui un emendamento di grandissimo impatto sulle libertà civili dei cittadini italiani viene occultato in un provvedimento di altro tenore (e criticità giuridico-politica), per sottrarlo ad una degna e trasparente discussione parlamentare sul suo contenuto". Dello stesso autore, si legga anche L. SCUDIERO, *Data retention a sei anni. La Corte di Giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR*, in *MediaLaws*, 1, 2017.

giurisprudenza europea come i principi di proporzionalità e necessità non possano però mai essere ignorati nella determinazione di misure che comprimono i diritti fondamentali: mancano quindi, da parte del legislatore italiano, considerazioni che dimostrino la proporzionalità delle misure introdotte con la Legge Europea rispetto agli scopi preposti. Proprio basandosi su tali considerazioni, anche il Presidente del Garante per la protezione dei dati italiano, all'epoca Antonello Soro, aveva espresso le proprie perplessità e contrarietà alla scelta operata dal legislatore: "la Corte di giustizia ha costruito l'architrave del rapporto tra prevenzione, tecnologia e dignità proprio sul principio di proporzionalità tra esigenze investigative e protezione dei dati"[24]. Così, aumentando significativamente la conservazione dei metadati, non solo vengono ignorate le sentenze della CGUE in materia ma si sottopongono a rischi ancora maggiori gli utenti dei servizi di telecomunicazione, i cui dati sono per un periodo ancor più lungo esposti a possibili – e invero frequenti – *data breach* e attacchi informatici, oltre che al pericolo di abusi da parte di soggetti pubblici e privati, aumentando peraltro irragionevolmente anche i costi e le responsabilità in capo agli operatori economici in tale campo, che dovranno porre in essere misure molto forti e onerose per garantire la sicurezza dei metadati conservati per una durata così estesa. Lo stesso Giovanni Buttarelli, in quegli anni Garante Europeo della Protezione dei Dati, al termine della presentazione dell'Annual Report alla Commissione per le libertà civili, giustizia e affari interni del Parlamento europeo, aveva redarguito il legislatore italiano, considerando la modifica normativa promossa con la Legge Europea un grave errore, anche alla luce della sua incompatibilità con i principi espressi a livello dell'UE[25].

1.2.2. – Il D. Lgs. 101 del 2018: una mancata occasione di riforma dell'art. 132 Codice Privacy

Nonostante le decise reazioni scatenate, le critiche e l'acceso dibattito apertosi in ambito per lo più accademico[26], la disposizione prevista dalla Legge Europea 2017 non ha conosciuto modifiche o ripensamenti, neppure quando una perfetta occasione per una più seria ristrutturazione della materia è stata offerta dalla operatività del GDPR e dunque dalla necessità di adeguare l'ordinamento interno, e

[24] È quanto affermato da Soro il 24 ottobre 2016, in occasione del Convegno svoltosi a Firenze dal titolo "Privacy digitale e protezione dei dati personali tra persona e mercato". E ancora, *"L'emendamento Verini segue la stessa impostazione di precedenti interventi che negli anni scorsi hanno modificato la disciplina della data retention. E, come già accaduto nel 2015, la norma introduce modalità di trattamento dei dati di traffico telefonico e telematico in palese contrasto con l'ordinamento e con la giurisprudenza dell'Unione europea. Pur essendo consapevole dell'esigenza di non ritardare l'approvazione della legge europea con una terza lettura* - ha concluso Soro - *penso che sia comunque indispensabile che il legislatore riconduca questa disciplina al criterio della proporzionalità. In futuro si dovrà meglio definire, con una disciplina organica e meno estemporanea, una materia così ricca di implicazioni sui diritti dei cittadini e sulle esigenze di giustizia", si legge nell'articolo reperibile sul sito web del Garante (al link:* https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6651715), *Terrorismo: Soro, troppi 6 anni di conservazione dei dati*. La posizione del Garante della Privacy è stata poi espressa anche in un apposito Parere (n. 8005333 sullo schema di decreto legislativo recante attuazione della Dir. 2016/680 del PE e del Consiglio, del 22 febbraio 2018) nel quale era stato ribadito l'invito al legislatore nazionale a rivedere e modificare la normativa in materia di *data retention*, sproporzionata rispetto ai criteri indicati dalla giurisprudenza della CGUE nonché alle reali esigenze investigative.

[25] "Da magistrato capisco che la giustizia abbia molte difficoltà e ostacoli oggi, e che organi investigativi debbano essere equipaggiati per fare indagini. (..) La scelta dell'Italia ha molto sorpreso Bruxelles, c'è molta attenzione da parte del Parlamento UE. Teniamo presente che un Paese come la Germania ha previsto un tempo di *data retention* che al massimo arriva a 10 settimane. Oltre al fatto che la Corte europea aveva annullato una Direttiva che prevedeva un massimo di due anni", intervista a Giovanni Buttarelli, pubblicata da Carola Frediani per *La Stampa*, il 13 novembre 2017.

[26] Anche la stampa nazionale si è occupata del tema, dandone risalto in diversi momenti, dalla proposta dell'emendamento alla approvazione finale della Legge Europea 2017. Tra tutti si legga R. BARBERIO, *Parliamo di Russia ma la vera anomalia sul 'data retention' è l'Italia*, in *HuffingtonPost*, 5 luglio 2018.

in particolare il Codice Privacy, alle modifiche significative apportate dal Regolamento europeo[27]. Pur essendo direttamente applicabile, infatti, il GDPR lascia su alcune materie – ad esempio sulla disciplina del trattamento di categorie particolari di dati – un certo margine di intervento e discrezionalità ai legislatori nazionali. Per rispondere a questa esigenza di riforma, che ha interessato il legislatore ma che ha richiesto anche l'intervento attivo e l'adozione di specifici atti da parte dell'Autorità Garante, è stato approvato il D. Lgs. 101 del 10 agosto 2018, nel quale si inseriscono anche talune modifiche apportate all'art. 132 in materia di *data retention*, in particolare con riferimento ai commi 3 e 5 e alla previsione di un nuovo comma 5-bis. Come si vedrà, tuttavia, tale intervento normativo non ha sostanzialmente cambiato la disciplina vigente, mettendo in luce la mancata volontà del legislatore nazionale di cogliere tale opportunità per adeguare l'assetto interno a quanto indicato dalla giurisprudenza della CGUE, nell'incapacità di dare quindi ascolto a tutte le critiche e perplessità energicamente manifestate nel corso degli anni da parte della dottrina, nonché evidenziando una certa indifferenza o quantomeno disattenzione rispetto al dibattito che, su tale complessa materia, si era invece aperto in molti altri Stati membri.

Ecco che, analizzando le modifiche apportate dal D. Lgs. 101/2018, si nota come il cambiamento operato sul comma 3, art. 132 risulti essenzialmente finalizzato a chiarire il dettato della disposizione, senza stravolgerne o cambiarne il significato: viene semplicemente sostituito il riferimento precedentemente espresso all'art. 8, co. II, lett. f) per il traffico entrante, con la più immediata previsione: "la richiesta di accesso diretto alle comunicazioni telefoniche in entrata può essere effettuata solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397". Similmente, anche il comma 5 si limita a sostituire il previo riferimento all'art. 17 sul "Trattamento che presenta rischi specifici" Codice Privacy, abrogato dal D. Lgs. 101 del 2018, con il rimando al nuovo art. 2-quinquiesdecies, che stabilisce come, con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati per i diritti e le libertà delle persone fisiche, il Garante possa prescrivere misure e accorgimenti a garanzia dell'interessato. I due indicati sono dunque interventi che mirano ad armonizzare la disciplina esistente con il GDPR e con le conseguenti modifiche apportate al Codice Privacy. Ancora più sorprendentemente e problematicamente poi il nuovo comma 5-bis ha riconfermato la – discussa, quantomeno in dottrina – modifica apportata dalla Legge Europea del 2017, prevedendo che viene "fatta salva la disciplina di cui all'art. 24 della legge 20 novembre 2017, n.167", riproponendo quindi tutte le criticità già in precedenza sottolineate.

Pur rimandando all'ultimo paragrafo di questo Capitolo per conclusioni più approfondite, sin da questa ricostruzione dell'evoluzione normativa che ha caratterizzato la disciplina italiana risulta come il legislatore non abbia mostrato un approccio attento all'evolversi della materia a livello dell'UE e alle azioni intraprese da altri Stati membri che si sono invece rivelati maggiormente sensibili alla giurisprudenza della CGUE, seppur con notevoli differenze.

Ciò che traspare è una normativa che si è evoluta in maniera disordinata, non organica ed unitaria e che ha seguito un percorso discutibile e dubbio, in una direzione per certi versi opposta rispetto all'andamento registratosi nella maggioranza degli Stati membri: mentre a seguito degli interventi decisi e decisivi dei giudici di Lussemburgo, i legislatori nazionali – spontaneamente o mediante l'intervento delle Corti – hanno cercato, pur con estrema difficoltà e dubbi, di adeguare e modificare la disciplina interna alle garanzie stabilite a livello europeo, generalmente diminuendo la durata di conservazione dei

[27] Merita ricordare come il Decreto PDR n. 15 del 15 gennaio 2018 che attua la direttiva 2016/680 non rilevi ai fini dell'esame della disciplina della *data retention*: se è vero che l'art. 10 fissa le condizioni per la conservazione dei dati, ciò non deve fuorviare il lettore poiché in quel caso il riferimento è alla conservazione di dati trattati nel corso di un procedimento penale o delle previe indagini, non avendo quindi nulla a che vedere con la più generale disciplina attinente all'obbligo di conservazione dei metadati da parte di servizi di telecomunicazione, oggetto di questo lavoro. Quest'ultima materia, infatti, risultava non solo estranea all'ambito di applicazione del Decreto stesso, ma anche già disciplinata dalla richiamata Legge Europea 2017.

dati e aumentando le salvaguardie, meglio specificando le categorie di reati per i quali l'accesso viene garantito e introducendo ulteriori controlli e tutele, l'Italia ha non solo aumentato il periodo di *data retention* con una estensione notevole e difficilmente motivabile da esigenze investigative, ma non ha neppure modificato la disciplina esistente corredandola di tutele maggiori o più definite. La parabola normativa è stata mossa essenzialmente da emergenziali necessità di innalzare il livello di tutela della sicurezza e di aumentare l'efficienza dell'intervento delle autorità pubbliche, mettendo loro a disposizione la possibilità di un accesso ampio e ad un numero elevato di metadati. Quel che sembra mancare però nelle considerazioni del legislatore è l'attenzione al bilanciamento da operare con i diritti alla riservatezza e alla protezione dei dati, nonché una riflessione approfondita sui limiti e sulla proporzionalità e legittimità di tali delicate scelte. Un approccio, come si vedrà, che, pur criticato da gran parte della dottrina, ha tuttavia ottenuto l'avvallo completo delle Corti nazionali.

2. – La giurisprudenza italiana in materia di conservazione e accesso ai metadati: un discutibile approccio 'rassicurante' e una lettura troppo rapida delle sentenze della CGUE

2.1. – Il primo – ed unico – intervento della Corte costituzionale e la conferma della legittimità e proporzionalità dell'art. 132 Codice Privacy

La giurisprudenza italiana in materia di *data retention* non è certamente ampia e neppure particolarmente innovativa sotto il profilo della tutela dei diritti fondamentali e del bilanciamento con le esigenze securitarie. Questo approccio – che, come si vedrà, si è protratto nel corso del tempo, poco curante dei rilevanti interventi dei giudici di Lussemburgo in materia – risulta evidente sin da una delle prime pronunce aventi ad oggetto l'art. 132 Cod. Privacy: nella sentenza n. 372 della Corte costituzionale, datata 14 novembre 2006, i giudici hanno addirittura valutato la normativa richiamata sotto un profilo opposto rispetto a quanto ha caratterizzato invece la giurisprudenza della CGUE. Non è stata infatti messa in dubbio la proporzionalità dell'invasione nella sfera privata causata dalla disciplina della conservazione generalizzata dei metadati, bensì da un lato la legittimità dell'imposizione di un vaglio giudiziale preventivo all'accesso alle informazioni, ritenuto un intervento eccessivo, inutile e sproporzionato, e dall'altro la legittimità del c.d. doppio binario cioè della conservazione – e dunque della possibilità di accesso ai dati – limitata ad un periodo di massimo ventiquattro mesi per finalità di repressione di reati 'comuni' non rientranti in quei reati gravi indicati nell'art. 407, co. 1, lett. a) c.p.p. per i quali veniva stabilito un termine di *data retention* più ampio. I limiti temporali e le garanzie procedurali previste all'art. 132 Cod. Privacy nella versione esistente all'epoca dei rinvii promossi dai Giudice per le indagini preliminari dei Tribunali di Pavia, di Roma e di Palmi, erano state ritenute da questi ultimi irragionevoli, in quanto pregiudicavano il buon andamento dell'amministrazione della giustizia (art. 97 Cost.) e rappresentavano dunque una ingiustificata complicazione della procedura, contrastante con il principio di obbligatorietà dell'esercizio dell'azione penale (art. 112 Cost.) nonché con la più generale aspettativa della garanzia, da parte dello Stato, delle condizioni essenziali della convivenza civile, mediante il perseguimento di comportamenti criminosi (artt. 101, 104 e 112 Cost.). "Secondo il rimettente, quale che sia la tutela costituzionalmente imposta per la riservatezza dei dati personali, il sacrificio determinatosi per i diritti appena elencati sarebbe irrazionale ed eccessivo. (..) Nel periodo compreso tra i ventiquattro ed i quarantotto mesi, in particolare, il potenziale pregiudizio per la riservatezza resterebbe inalterato, ed anzi si aggraverebbe progressivamente, senza che ciò sia compensato dalla disponibilità di eventuali prove della commissione di delitti anche molto gravi, per quanto non compresi nell'elenco fissato alla lett. a) del co. 1, dell'art. 407 c.p.p." (par. 4, sent. n. 372/2006). Ciò che viene criticato dunque è la proporzionalità e ragionevolezza del c.d. doppio binario nella parte in cui prevede una più lunga disponibilità dei metadati per i reati ricompresi nella

disposizione richiamata, mentre per quelli 'comuni' un termine più ristretto, pur imponendo, *de facto*, un obbligo di conservazione più lungo in capo agli operatori di servizi di telecomunicazione che non possono anticipatamente conoscere, come si è detto, la finalità per la quale l'accesso ai metadati potrebbe essere richiesto. Ne emerge dunque come la questione posta dai giudici di merito non fosse basata sulla considerazione della durata di conservazione eccessivamente ampia o della possibilità di accesso ai metadati estesa a qualsiasi reato, anche privo del carattere di gravità ma, al contrario, ciò che veniva ritenuto irragionevole era la mancata disponibilità dei metadati anche per i reati comuni per l'intero periodo in cui i fornitori di servizi di telecomunicazione erano comunque tenuti a conservazione. Un'analisi attenta delle posizioni dei giudici *a quo* evidenzia come il principale rilievo critico mosso all'art. 132 Cod. Privacy non fosse quello di aver introdotto tutele eccessive quanto più quello di aver previsto "garanzie sostanzialmente vuote: utili forse a massimizzare sulla carta gli standards di protezione della segretezza delle comunicazioni ma in realtà concretamente inidonee a tale scopo e quindi irragionevoli"[28]; ciò alla luce del fatto che, nonostante il 'doppio binario', i metadati venivano conservati, nella prassi concreta e per esigenze fattuali ineludibili, per la massima durata dei quarantotto mesi[29].

La posizione della Consulta è stata quella di far salva la normativa esistente, ritenendo infondate le questioni poste alla sua attenzione. Quanto al profilo dell'autorizzazione da parte del giudice, stabilita dall'art. 132 vigente all'epoca dei rinvii, la Corte costituzionale ha sottolineato come la materia, nelle more del giudizio, fosse stata profondamente innovata con il Decreto Pisanu e la legge di conversione. Questi, come si è visto, avevano eliminato l'intervento del giudice, ritenendo sufficiente il mero decreto motivato da parte del pubblico ministero, con una scelta che ha fatto e continua a far discutere tuttora la dottrina, che si interroga sulla reale capacità del p.m. di svolgere un vaglio preventivo oggettivo e terzo circa la necessità dell'accesso ed offrire così un controllo indipendente quanto alla legittimità dell'ingerenza nella sfera privata. La scelta operata dal legislatore nell'ultima modifica apportata alla normativa in esame quindi aveva eliminato tutti i rilievi di illegittimità indicati dai Giudici rimettenti: la Consulta pertanto non si è pronunciata – purtroppo, perché le valutazioni espresse sarebbero certamente state utili punti di riferimento per le successive modifiche normative – sulle delicate questioni della proporzionalità ed imparzialità del previo controllo giudiziario.

Rispetto invece all'illegittimità della disciplina della *data retention* così come concepita nell'art. 132 Cod. Privacy, i giudici costituzionali hanno affermato come: "il legislatore ha operato un bilanciamento tra il principio costituzionale della tutela della riservatezza dei dati relativi alle comunicazioni telefoniche, riconducibile all'art. 15 Cost., e l'interesse della collettività, anch'esso costituzionalmente protetto, alla repressione degli illeciti penali" (par. 5.1.)[30]. Tale bilanciamento è stato ritenuto ragionevole in quanto "affinché la norma sfugga alla censura di illegittimità costituzionale non è

[28] M. PINNA, *Doppio binario di accesso ai dati sul traffico telefonico: una scelta legislativa ragionevole ratificata (con argomenti non irresistibili) dalla Corte costituzionale*, in *Giurisprudenza Costituzionale*, 2006, p. 3929.

[29] "Secondo il giudice rimettente, l'esistenza fisica dei dati, non ancora distrutti, comporterebbe un tasso di pericolosità, derivante dalla possibile illecita diffusione degli stessi, destinato a rimanere costante per tutto il tempo anteriore la loro distruzione, senza subire variazioni in rapporto alla gravità dei reati. Da ciò discenderebbe l'irragionevolezza della bipartizione – contenuta nella norma censurata – dei termini di accessibilità dei dati da parte dell'autorità giudiziaria", par. 5.2.

[30] Merita sottolineare, per completezza, come nella Costituzione italiana non esista un espresso riferimento e riconoscimento del diritto alla riservatezza e protezione dei dati. Nondimeno questi diritti risultano protetti nell'ordinamento nazionale, da un lato mediante le fonti di livello internazionale e sovranazionale (Convenzione EDU e Carta di Nizza ad esempio) al cui rispetto l'Italia si è vincolata, e dall'altro mediante la giurisprudenza della Corte costituzionale, che ha individuato negli artt. 14 e 15 le basi costituzionali del diritto alla privacy, unitamente ai riferimenti più generici ai diritti alla libertà personale e alla dignità. Come affermato da Resta, il riconoscimento di tali diritti quindi avviene non grazie ad esplicite garanzie costituzionali bensì principalmente (soprattutto negli ultimi decenni) mediante l'interazione tra livello interno ed europeo sul piano dei diritti fondamentali (G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il Codice dei dati personali. Temi e problemi*, Giuffré, 2004).

necessario, come ritiene il giudice *a quo*, che dalla differente disciplina del tempo di accessibilità dei dati, a seconda della gravità dei reati da perseguire, derivi una maggiore o minore tutela del diritto alla riservatezza; è sufficiente che la maggiore o minore limitazione sia posta in rapporto con la maggiore o minore gravità attribuita dal legislatore a reati diversi, individuati secondo scelte di politica criminale non censurabili in questa sede" (par. 5.3).

Anche alla luce di tali considerazioni, ciò che appare di notevole interesse in questa pronuncia sono innanzitutto i dubbi espressi dai giudici *a quo*: pur andando in un senso, per certi versi, contrapposto alle pretese e censure mosse dalla dottrina e che saranno poi alla base delle sentenze di molte Corti nazionali in altri Stati membri nonché della CGUE, alcune premesse sono comunque meritevoli di attenzione. Sebbene infatti non sia stato contestato lo strumento della *data retention* generalizzata, è stata purtuttavia riconosciuta l'esistenza di una lesione dei diritti fondamentali derivante dalla sola conservazione dei metadati, indipendentemente e prima cioè dell'accesso. Nonostante i giudici giungano poi alla conclusione secondo cui la perdurante lesione protratta per quarantotto mesi rende ragionevole la differenziazione in termini di accesso e disponibilità dei metadati a seconda della gravità del reato[31], senza dubbio il riconoscimento di una ingerenza nella sfera privata ad opera della *data retention* e dunque di un conseguente necessario corretto bilanciamento degli interessi e diritti in gioco, è un aspetto di grande rilievo. Inoltre, anche nella decisione espressa dalla Corte costituzionale vi è una presa di posizione rilevante per comprendere l'approccio della giurisprudenza italiana al tema della conservazione dei metadati e del bilanciamento tra esigenze securitarie e diritti fondamentali: si tratta dell'affermazione secondo cui trascorso un periodo di tempo durante il quale i dati sono accessibili anche per reati non gravi sia ragionevole poi prevedere una ulteriore e più ampia durata di conservazione e di accesso, che dovrà però essere giustificata e proporzionale al maggior livello e gravità dell'offesa che la disponibilità dei metadati è volta a reprimere. Un ragionamento, questo, che sembra in contrasto sia con quanto poi affermerà la CGUE, sia con quello che la DRD stessa statuiva, disponendo l'obbligo di conservazione dei metadati solo per finalità di repressione di reati gravi. Nonostante tali rilievi, la posizione espressa dalla Corte costituzionale è stata ampiamente confermata e seguita dal legislatore italiano che non ha mai inserito nella normativa nazionale il requisito della gravità del reato, consentendo dunque l'accesso ai metadati per finalità generale di lotta a qualsiasi tipo di reato e prevedendo solo disposizioni eccezionali che hanno inserito deroghe alla regola generale per tipologie particolari di reati quali quelli di terrorismo.

2.2. – L'Ordinanza del Tribunale di Padova: una significativa esemplificazione dell'approccio dei giudici italiani dinnanzi alla rilevante giurisprudenza della CGUE in materia di data retention

A distanza di anni, nei quali i Giudici italiani sono sostanzialmente rimasti silenti in materia, anche dinnanzi agli accadimenti rilevanti che hanno caratterizzato la giurisprudenza dell'UE, si sono registrati in tempi recenti alcuni interventi meritevoli di nota: l'Ordinanza, che si analizzerà per prima, del Tribunale di Padova (Ord. 15 marzo 2017, Pres. Marassi) e principalmente quattro sentenze della Corte di Cassazione: Sez. V penale, 24 aprile 2018, n. 33851; Sez. III penale, 23 agosto 2019, n. 36380; Sez. III penale, 25 settembre 2019 e n. 48737 e Sez. II penale, 10 dicembre 2019, n. 5741.

Procedendo con ordine, l'Ordinanza del Tribunale di Padova viene segnalata come "uno dei rari casi, ad oggi noti, in cui l'avvocato della difesa ha chiesto al giudice di dichiarare l'inutilizzabilità nel

[31] Sul punto: "Lo stesso legislatore ha ritenuto che, per mantenere l'equilibrio, all'aumento del peso di una delle due entità debba corrispondere un proporzionale aumento dell'altra, con la conseguenza che, in corrispondenza di reati di particolare gravità, la limitazione, in termini relativi, della tutela della riservatezza è stata aumentata in ragione del maggior disvalore sociale sotteso ai reati di cui all'art. 407, comma 2, lettera *a*), cod. proc. pen.", par. 5.2.

processo di tutti i dati esterni del traffico telefonico, a chiunque intestati, acquisiti in fase di indagini dalla pubblica accusa ex art. 132 Cod. Privacy, a seguito della nota sentenza della CGUE sulla *data retention*"[32]. Tale richiesta è stata peraltro correlata, in subordine, dalla domanda di sospendere il procedimento e provvedere ad un rinvio pregiudiziale alla CGUE, sottoponendo il delicato quesito volto a determinare "se gli artt. 7, 8 e 52, par. 1 della CDFUE ostino ad una normativa nazionale, quale l'art. 132 Cod. Privacy, che consente l'acquisizione e la conservazione dei dati esterni del traffico telefonico e telematico per qualsiasi tipo di reato". Tre sono essenzialmente le motivazioni che hanno spinto i giudici a rigettare l'eccezione di inutilizzabilità dei tabulati promossa dalla difesa: innanzitutto che l'art. 132 Cod. Privacy non è norma attuativa della DRD, in quanto entrato in vigore nel 2003; ciò basta per ritenere la sentenza *DRI* come non comportante alcun effetto nei confronti della disciplina italiana richiamata[33]. La seconda considerazione svolta dal Tribunale è quella secondo cui l'accesso ai metadati nel caso in esame è avvenuto per accertare un reato di tentato incendio doloso, che risulta possedere quel carattere di gravità – richiesto dalla giurisprudenza della CGUE, ma assente nella normativa italiana – idoneo a giustificare l'invasione nella sfera privata. Infine, il terzo argomento proposto, che assume grande rilievo, è quello secondo cui l'ammissibilità delle intercettazioni telefoniche, che attengono quindi al contenuto delle conversazioni, non può che far ritenere giustificata e proporzionata la lesione del diritto alla riservatezza ben più limitata derivante dal mero accesso ai metadati. Come si vedrà, e questo spiega l'importanza della Ordinanza in esame, molte di queste posizioni verranno successivamente riprese anche dai giudici della Corte di Cassazione.

Ciò che si può innanzitutto osservare con evidenza – e la dottrina non ha mancato di rimarcarlo – è la rapidità e superficialità con la quale il Tribunale di Padova ha affrontato una questione estremamente delicata e complessa e che, già nel 2017, aveva sollevato ampia analisi e dibattito in molti Stati europei oltre che in seno all'UE e alla CGUE. Alcune delle posizioni espresse risultano sotto certi profili addirittura erronee: certo l'art. 132 Cod. Privacy nella sua versione originaria non costituiva attuazione della DRD ma lo è divenuto nel 2008, quando il legislatore è intervenuto, con il già analizzato D. Lgs. n. 109/2008, proprio sull'art. 132 per dare attuazione alla Direttiva europea 2006/24. È inoltre da rilevare come la sentenza *Tele2* della CGUE, che pure non è stata presa in considerazione dai giudici del Tribunale, abbia ribadito i criteri delineati dalla *DRI* anche con riferimento alle discipline nazionali attuative del noto art. 15 Direttiva *e-Privacy*, tra cui appunto l'art. 132 Cod. Privacy nella sua versione originaria. Sebbene poi, come ampiamente esaminato, la sentenza *DRI* non abbia avuto efficacia diretta avverso le normative nazionali di attuazione, è altrettanto vero che, qualora i vizi che avevano comportato l'invalidità della DRD fossero stati rinvenuti anche nella disciplina interna attuativa, quest'ultima sarebbe risultata non compatibile con il diritto dell'UE e in violazione dei diritti fondamentali tutelati agli artt. 7 e 8 della Carta di Nizza, per le stesse ragioni e vizi individuati nella Direttiva europea medesima[34]. Il Tribunale quindi ha dimostrato di ignorare – o di non voler prendere in considerazione – tutte quelle critiche e valutazioni che la dottrina, già a seguito della *DRI*, aveva messo in rilievo con riferimento alla normativa italiana e che sono state evidenziate nel previo paragrafo.

Quanto poi al richiamo operato nell'ordinanza al requisito di gravità del reato, deve essere obiettato come la definizione del concetto e delle caratteristiche che determinano la gravità non possano essere lasciate alla discrezionalità e libera valutazione del giudice, caso per caso, bensì debbano essere determinate dalla legge stessa, come del resto richiesto dalla giurisprudenza della CGUE e come specificato persino nella DRD, secondo cui la conservazione e l'accesso ai metadati dovevano essere

[32] R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata quaestio(?)*, op. cit., p. 356.
[33] "Il dictum della menzionata sentenza [*DRI*] non ha alcuna rilevanza nell'odierno processo. Infatti l'art. 132 Cod. Privacy non è norma di attuazione della DRD, essendo questo entrato in vigore in tempo antecedente: dunque l'invalidità della direttiva non si trasmette ad esso".
[34] Così F. RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cassazione penale*, 6. 2017.

motivati esclusivamente dalla finalità di repressione della criminalità grave, aspetto che il legislatore italiano ha mancato di considerare[35].

Infine, la motivazione secondo cui le intercettazioni, in questo caso concesse, sarebbero state maggiormente invasive della sfera privata, ritenendo quindi a maggior ragione e logicamente ancor più accettabile l'accesso ai soli metadati, pare del tutto fuorviante perché fondata sull'erroneo assunto secondo cui la lesione dei diritti alla riservatezza e protezione dei dati risulterebbe maggiore in presenza di intercettazioni riguardanti il contento delle comunicazioni rispetto alla mera conservazione ed accesso ai dati esterni. Ciò risulta smentito in primis dalla posizione espressa dalla CGUE che, a partire dalla sentenza *DRI*, ha invece riscontrato finanche nella sola conservazione dei metadati una grave ingerenza nella vita privata degli utenti, dovuta alla possibilità, mediante lettura aggregata di tali informazioni, di ricostruire abitudini, preferenze e stili di vita, a prescindere dall'esame del contenuto delle conversazioni stesse. Sebbene la CGUE non si sia spinta ad equiparare l'impatto provocato da un accesso al contenuto delle comunicazioni con quello ai metadati, ritenendo il primo come lesivo del nucleo essenziale del diritto alla riservatezza, essa è comunque giunta a richiedere un livello elevato di protezione e di salvaguardie anche con riferimento ai metadati. Oltretutto, non va dimenticato come il dibattito dottrinario, evidenziato nella Parte II di questo lavoro, abbia fortemente criticato la distinzione operata dalla CGUE, che pare ormai superata alla luce delle moderne tecnologie e delle possibilità e potenzialità estremamente invasive che la lettura aggregata dei metadati può comportare.

In conclusione, dunque, questa Ordinanza pare una significativa esemplificazione e riassunto di tutte le problematiche già evidenziate con riferimento all'evoluzione della normativa italiana in materia di *data retention* ed è strettamente correlata alle scelte del legislatore stesso ed in particolare al mancato – o, quando presente, maldestro – intervento di adeguamento ai requisiti e criteri delineati dalla giurisprudenza della CGUE: è proprio nell'atteggiamento del legislatore italiano che vanno infatti riscontrate le ragioni di "impropri fenomeni di supplenza giudiziaria, di cui il provvedimento in commento appare emblematica espressione: comprensibile nei fini (perseguire la giustizia del caso concreto) ma censurabile nell'ordito, in spregio ai principi della separazione fra poteri e della certezza del diritto"[36]. Queste criticità, unitamente alla 'leggerezza' nella lettura delle complesse e rilevanti sentenze dei giudici di Lussemburgo, saranno purtroppo riproposte anche nelle decisioni della Corte di Cassazione.

2.3. – Le pronunce della Corte di Cassazione tra una dubbia interpretazione delle pronunce dei giudici di Lussemburgo e il mancato rinvio alla CGUE: l'assenza di una considerazione approfondita e d'insieme della disciplina della conservazione e accesso ai metadati

Nelle pronunce emesse dalla Sez. V, n. 33851 del 24 aprile 2018 e Sezione III penale del 23 agosto 2019, n. 36380 – che verranno analizzate unitamente, stante le simili doglianze affrontate e le analoghe

[35] "Evidente allora l'errore commesso dal Tribunale di Padova che, decidendo quale fattispecie integri l'ipotesi del reato grave, tale da prevalere in un giudizio di proporzionalità rispetto alla riservatezza del cittadino sottoposto a processo, ha esercitato (ed usurpato) funzioni legislative. Solo il legislatore, in un paese di *civil law* come l'Italia, può predeterminare in via generale ed astratta i modi dell'intrusione nella riservatezza dei propri cittadini ai sensi degli artt. 8 CDFUE e 8 CEDU. Se il giudice di ciascun caso singolo fosse autorizzato a svolgere un proprio bilanciamento in tema di *data retention*, da un lato si produrrebbero oscillazioni interpretative difficilmente giustificabili nella demarcazione del confine tra reato grave e reato non grave. Dall'altro si correrebbe il rischio che la giurisprudenza, legittimamente, si appiattisca nel ritenere tutto 'grave', anche al fine di non disperdere attività di accertamento spesso preziosa, complessa e necessaria, sino ad arrivare ad un totale annacquamento del requisito di gravità: risultato che si collocherebbe agli antipodi rispetto agli auspici della sentenza CGUE sulla *data retention*", F. RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, op. cit., p. 2478.

[36] F. RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, op. cit., p. 2488.

considerazioni effettuate dai giudici – anche la Suprema Corte italiana ha ribadito la compatibilità dell'art. 132 Cod. Privacy al diritto dell'UE, come interpretato dalla CGUE. Entrambi i casi originavano dall'impugnazione promossa dai difensori di soggetti condannati (nel primo caso per sequestro di persona e lesioni personali gravi in danno a minore e nel secondo invece per cessione di cocaina) sulla base – non solo ma anche – di un indizio ottenuto mediante l'analisi di metadati conservati da compagnie telefoniche. Tali informazioni avevano consentito, ad esempio, nel secondo caso affrontato dalla Corte, di determinare la cellula telefonica agganciata dall'imputato – e dunque la sua ubicazione – nell'ora precisa in cui il reato era stato commesso. Al di là delle doglianze più specificamente attinenti alla natura delle prove e al rispetto del principio del ragionevole dubbio, si vuole circoscrivere la presente analisi ai profili problematici rilevati relativamente alla disciplina nazionale in materia di *data retention*: il richiamato art. 132 Codice Privacy è stato considerato dal ricorrente in contrasto con gli artt. 7, 8 e 52 della Carta di Nizza, così come letti dai giudici di Lussemburgo, poiché, rispetto ai criteri delineati da questi ultimi, in particolare nella sentenza *DRI*, "l'art. 132 conterrebbe tutti i vizi già individuati dalla Corte di giustizia, con conseguente necessità di disapplicare la norma interna e di ritenere la prova acquisita vietata dalla legge e quindi non utilizzabile" (par. 3.2, sentenza n. 36380/2019)[37]. In subordine poi il difensore dell'imputato ha richiesto alla Corte di Cassazione di provvedere al rinvio pregiudiziale alla CGUE "affinché accerti se gli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'UE ostino ad una normativa nazionale, quale quella D. Lgs. n. 196/2003, art. 132 che consente l'acquisizione e la conservazione del traffico telematico per qualsiasi tipo di reato e senza un previo controllo della richiesta da parte di un'autorità indipendente" (par. 3.2, sentenza n. 36380/2019).

La Corte di Cassazione è giunta, in entrambi i casi piuttosto rapidamente, a respingere le richieste formulate nell'impugnazione sotto il profilo della disciplina della *data retention*, ritenendo infondate le motivazioni addotte sul punto. I giudici hanno iniziato con il ricostruire la giurisprudenza della CGUE ed il bilanciamento da essa effettuato tra diritti fondamentali ed esigenza di accertamento e repressione dei reati mediante acquisizione di metadati presso *service providers*. Ebbene dalle pronunce esaminate la Corte ha concluso che esse fossero da riferirsi agli "Stati privi di una regolamentazione dell'accesso e della conservazione dei dati, mentre lo Stato italiano si è dotato di una specifica disciplina. (..) Nella disciplina italiana peraltro si rinvengono l'enunciazione della finalità di repressione dei reati; la delimitazione temporale dell'attività di memorizzazione; l'intervento preventivo dell'autorità giudiziaria, funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati" (par. 3.5, sentenza n. 36380/2019). Sulla base dell'analisi svolta dai giudici italiani, sono risultati quindi del tutto rispettati i requisiti indicati dalla CGUE, compreso quello del previo controllo di un organo indipendente: questo punto risulta invero piuttosto interessante anche alla luce di quanto affermato nelle sue Conclusioni dall'Avvocato generale nel rinvio pregiudiziale promosso dalla Corte estone[38], che si riprenderà a breve. La Corte di Cassazione, infatti, già nella sentenza del 2018, aveva sostenuto come la traduzione del testo della sentenza *DRI* della CGUE, nella parte in cui veniva utilizzato il termine *giudice* come soggetto preposto al controllo preventivo all'accesso ai metadati, fosse da considerarsi erronea e fuorviante. Se si addivenisse infatti ad una sua valutazione letterale, tale traduzione porterebbe quale esito quello di considerare i pubblici ministeri, che non possono definirsi 'giudici', come soggetti non

[37] In particolare, l'Avvocato generale evidenzia la mancanza di qualsiasi indicazione dei reati al cui accertamento è finalizzato l'accesso ai metadati, nonché il fatto che non sia previsto un controllo circa la necessità dell'accesso svolto da un giudice o un'autorità amministrativa indipendente, bensì tale delicata decisione di acquisire i metadati conservati dai fornitori di servizi di telecomunicazione venga affidato ad una parte del procedimento penale, ovvero il pubblico ministero. Viene inoltre rilevato, con riferimento alla durata della conservazione stessa, come non siano previste differenziazioni sulla base delle categorie di dati interessati e neppure garanzie sufficienti nella fase di accesso contro il rischio di abusi.

[38] Si fa riferimento al rinvio C-746/18, *H. K. c. Prokuratuur*, depositato il 29 novembre 2018 e alle Conclusioni dell'Avvocato generale Giovanni Pitruzzella depositate il 21 gennaio 2020. Per una ampia analisi delle stesse, si rimanda al Capitolo IV, Parte II.

adatti a svolgere il controllo preliminare, con la conseguenza che la normativa italiana dovrebbe considerarsi sotto tale profilo come non rispondente al requisito indicato dalla CGUE. Dal raffronto con la versione francese della pronuncia emerge però, a parere dei giudici italiani, come il termine impiegato fosse quello di "jurisdiction", da intendersi quindi come 'magistratura', considerata nella sua totalità e dunque comprensiva sia dei giudici che dei pubblici ministeri (rispettivamente *magistrats du siege* e *magistrats du parquet*). L'impiego di un termine più ampio e comprensivo viene riscontrato anche nella traduzione inglese, nella quale si utilizza la parola generica "Court", che potrebbe ricomprendere sia i "judges" che i "prosecutors". Da tale analisi, la Corte italiana fa derivare come "più che al termine giudice, riportato nella traduzione in maniera non fedele, deve farsi riferimento a quello di autorità giudiziaria, che pacificamente ricomprende anche la figura del pubblico ministero" (par. 3.6, sentenza n. 36380/2019)[39]. Vengono quindi respinte le doglianze espresse con specifico riferimento a tale criterio del controllo da parte di un organo indipendente.

Da quanto ricostruito, mentre la dottrina ha più volte e in più occasioni, come si è avuto modo di vedere, sottolineato le forti problematiche che la normativa italiana ha posto sul piano della compatibilità con la Carta di Nizza ed il diritto dell'UE, risulta evidente come la Corte di Cassazione si sia invece mostrata in entrambe le pronunce coerente – nella seconda la Corte fa ampio rinvio del resto alla sentenza precedente – nel voler mantenere quello che è stato definito un "atteggiamento 'rassicurante'", espressione di un "approccio semplicistico ad un tema complesso e colmo di nodi irrisolti"[40]. La posizione espressa dalla Suprema Corte italiana si è rivelata così per certi versi avventata e superficiale, mancando oltretutto di considerare i numerosi rinvii pregiudiziali che già erano stati promossi dai giudici di altri Stati membri nei confronti della CGUE, a dimostrazione della complessità che caratterizza numerosi aspetti della disciplina della *data retention* e dell'accesso ai metadati, che non a caso sono stati oggetto di richieste di chiarimento ai giudici europei stessi. I giudici italiani, diversamente dai colleghi inglesi, belgi, estoni, francesi, irlandesi e tedeschi, hanno invece ritenuto la giurisprudenza europea chiara, non meritevole di ulteriori interventi – anche correttivi, come si è visto, proposti più o meno tra le righe dai giudici del rinvio –, risolvendo anzi con grande agilità e semplicità molti dei quesiti che sono invece oggi sottoposti al vaglio della CGUE. Che ciò derivi da una certa ritrosia al dialogo con il giudice europeo o da una scarsa conoscenza della materia in esame e dunque dalla mancata comprensione della sua complessità e dei suoi molteplici aspetti ancora aperti e in attesa di definizione, il risultato è certamente quello di una posizione discutibile, se non addirittura erronea. Ne è esemplificazione evidente l'affermazione, peraltro ripresa dalla Ordinanza del Tribunale di Padova, secondo cui la giurisprudenza europea avrebbe riguardato Stati sprovvisti di una regolamentazione sulla conservazione ed accesso ai metadati: nulla di più sbagliato se si considera che sentenze come *Tele2* e *Ministerio Fiscal* hanno al contrario avuto ad oggetto proprio e unicamente discipline nazionali, determinando criteri e requisiti che devono quindi ispirare tutti i legislatori degli Stati membri così come quello europeo. Lo stesso può dirsi rispetto alla affermazione secondo cui "l'acquisizione del dato genera una compromissione decisamente inferiore rispetto a quella relativa alla captazione delle

[39] A ciò si aggiunge come "la soluzione italiana [di affidare il controllo preventivo al pubblico ministero] è coerente con il sistema di tipo accusatorio, nel quale, nel corso delle indagini preliminari, è il pubblico ministero l'autorità giudiziaria che procede, e con il sistema processuale che prevede, mediante le indagini difensive ed i poteri riconosciuti ai difensori anche in tema di acquisizione del dato, l'estensione, anche se parziale, del potere investigativo alla difesa. E ciò in una situazione in cui l'acquisizione del dato genera una compromissione decisamente inferiore rispetto a quella relativa alla captazione delle conversazioni, sia telefoniche che ambientali, la cui tutela è affidata invece al controllo del giudice per le indagini preliminari. Per altro, la questione, per come proposta nel caso de quo, è irrilevante, sia per l'assenza di elementi di prova nei confronti dell'imputato, anche utilizzando il dato emergente dai tabulati, sia perché il reato per cui si procede è punito con la pena da 6 a 20 anni di reclusione ed il contrasto alla criminalità collegata al mercato degli stupefacenti rientra tra le finalità indicate dalla giurisprudenza europea" (par. 3.7 e 3.8).

[40] L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, op. cit., p. 761.

conversazioni" (par. 3.7, sentenza n. 36380/2019): come si è già detto con riferimento alla simile considerazione mossa nell'Ordinanza del Tribunale di Padova, anche in questo caso emerge chiaramente la lontananza con quanto – rivoluzionariamente e chiaramente – sostenuto dalla CGUE, posizione peraltro recentemente e con più decisione accolta dalla Corte EDU nella sua giurisprudenza in materia di sorveglianza massiva[41]: i giudici nazionali dovrebbero ben conoscere e considerare nelle proprie valutazioni sulla normativa nazionale tali problematiche e complessità, anziché risolvere, forse troppo semplicisticamente, una distinzione contenuto/metadati ormai ampiamente discussa e da taluni ritenuta addirittura superata e fuorviante.

La Corte di Cassazione nella sua analisi, inoltre, mostra di concentrarsi sul requisito del controllo effettuato da un giudice o da un organo indipendente, mentre tralascia di considerare gli altri e altrettanto importanti criteri indicati dalla giurisprudenza europea: nulla viene detto circa la natura indiscriminata e generalizzata della conservazione[42], la proporzionalità della durata della *data retention* stessa[43] oppure la sussistenza di elementi che, seppur indirettamente, colleghino la conservazione alla esigenza di garanzia della sicurezza; non viene neppure preso in considerazione il requisito della gravità del reato e dunque della necessaria presenza di un elenco di reati o di una soglia specifica sulla base della quale l'accesso ai metadati risulti proporzionato alla gravità dell'ingerenza nei diritti fondamentali: non bisogna infatti dimenticare come, sebbene ai sensi della Legge Europea 2017 sia fissato un termine temporale di conservazione – e dunque di possibilità di accesso – più elevato per talune tipologie di reato, sotto il profilo della disciplina dell'accesso ai metadati, esso è garantito per la repressione e

[41] Si fa riferimento ad esempio a quanto affermato dai giudici di Strasburgo in *Big Brother Watch*, oggetto di esame nel Capitolo V, Parte II, cui si rinvia.

[42] Come affermato dalla giurisprudenza della CGUE, l'ingerenza nella vita privata rappresentata dalla conservazione dei metadati è indipendentemente dal successivo ed eventuale accesso, e deve quindi, come tale, sottostare ai principi di proporzionalità e necessità (si richiama sul punto la sentenza *DRI* nella parte in cui afferma chiaramente come "l'obbligo imposto ai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione elettronica, di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni (..) costituisce di per sé un'ingerenza nei diritti garantiti dall'art. 7 della Carta. Inoltre l'accesso della autorità nazionali competenti ai dati costituisce un'ingerenza supplementare in tale diritto fondamentale. Parimenti la direttiva 2006/24 è costitutiva di un'ingerenza nel diritto fondamentale alla protezione dei dati personali garantito all'art. 8 della Carta, perché prevede un trattamento dei dati personali", par. 34-36). Sulla base di tali considerazioni, pare evidente come una *data retention* generalizzata e decisamente prolungata quale quella italiana muova significativi dubbi di compatibilità con il diritto dell'UE. Sul piano della durata, le peculiarità dei singoli ordinamenti nazionali e delle concrete modalità di indagine penale, nonché della tipologia di criminalità che caratterizza un certo Stato – si pensi alla criminalità organizzata di stampo mafioso che rappresenta una realtà forte nel contesto italiano –, potrebbero certamente giustificare una differenziazione nella disciplina della durata della conservazione, ma ciò che dovrebbe ancor prima essere considerato in sede di scelta legislativa sono le concrete e reali esigenze investigative, i dati e le analisi oggettive che possono motivare cioè le decisioni dei legislatori nazionali e risultare in elementi importanti per una fondamentale ed ineludibile valutazione della proporzionalità della durata della *data retention* stessa. Senza dubbio comunque la determinazione di una corretta, legittima e proporzionata durata di conservazione dei dati è del resto tema fortemente dibattuto: Signorato ad esempio ritiene che un congruo arco temporale sia da individuarsi in un periodo dai trentasei ai settantadue mesi. "Si è consapevoli che una simile impostazione si scontra con quella prevalente, anche sul piano europeo, volta ad affermare la necessità di tempi di conservazione assai più brevi. Non di rado si tratta però di approcci sbilanciati nella direzione di una aprioristica tutela della privacy", S. SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 12 Codice Privacy da parte del D. Lgs. 10 agosto 2018, n. 101*, op. cit., p. 160. Una riflessione che non sia sbilanciata né dall'uno né dall'altro lato (pro securitario o garantista dei diritti fondamentali), è quindi necessaria quanto complessa da sviluppare.

[43] Le peculiarità dei singoli ordinamenti nazionali e delle concrete modalità di indagine penale, nonché della tipologia di criminalità che caratterizza un certo Stato – si pensi alla criminalità organizzata di stampo mafioso che rappresenta una realtà forte nel contesto italiano –, potrebbero certamente giustificare una differenziazione nella disciplina della durata della conservazione, ma ciò che dovrebbe ancor prima essere considerato in sede di scelta legislativa sono le concrete e reali esigenze investigative, i dati e le analisi oggettive che possono motivare cioè le decisioni dei legislatori nazionali e risultare elementi importanti per una fondamentale ed ineludibile valutazione della proporzionalità della durata della *data retention* stessa.

indagine di qualsiasi reato, senza alcuna specificazione e differenziazione sulla base della gravità del reato da perseguire[44]. Al di là della questione, ancora aperta e sottoposta al vaglio della CGUE, circa la necessità della contemporanea presenza e rispetto dei requisiti sulla conservazione e di quelli attinenti invece alla fase di accesso al fine di considerare una normativa in materia conforme al diritto dell'UE, la Corte di Cassazione non si è assolutamente posta, alla radice, la problematica e non ha ritenuto fondamentale aprire un dibattito su tale tema che ha assunto invece, come si è visto, in altri Stati membri un grande rilievo e che ha attirato l'attenzione tanto dei legislatori quanto delle Corti.

Nell'esaminare, infine, la figura del pubblico ministero e la possibilità che il controllo ad esso assegnato assolva al criterio delineato dai giudici di Lussemburgo, i giudici italiani hanno fondato la loro posizione essenzialmente sull'analisi della terminologia impiegata dalla CGUE nelle sue diverse traduzioni. Ebbene, sul punto, come chiaramente rilevato da Lupária, emerge una certa disattenzione da parte della Corte di Cassazione nel considerare l'impiego di termini simili in altre normative del diritto dell'UE: nella decisione quadro 2002/584/GAI, ad esempio, il legislatore europeo ha usato i termini di "autorité judiciare" e di "judicial authority" per riferirsi all'autorità giudiziaria ampiamente intesa e dunque comprensiva anche della pubblica accusa e non solo dei giudici intesi in senso stretto. Questa lettura più ampia ed approfondita quindi denota come la scelta di impiegare proprio le parole "juridiction" e "Court" non possa essere intesa quale generico rinvio alle autorità giudiziarie, bensì faccia emergere l'intenzione dei giudici di Lussemburgo di riferirsi più specificamente e restrittivamente ad organi precisi, quali appunto i giudici, confermando così la correttezza della traduzione italiana. Certamente l'obiettivo del requisito è da individuarsi nella indipendenza rispetto al potere esecutivo del soggetto preposto al controllo, ma è altrettanto vero che l'indipendenza deve essere intesa anche nel senso di terzietà ed imparzialità, come peraltro specificato dalla ben più risalente giurisprudenza della CGUE[45]: se il pubblico ministero italiano, diversamente da quello di altri Stati membri, risulta senza

[44] "Come affermato dalla stessa Suprema Corte, la disciplina nazionale sull'acquisizione dei dati esterni alle comunicazioni non è in alcun modo circoscritta in ordine alle tipologie di reato oggetto di indagine o accertamento. Ciononostante, nell'ottica della Corte, il mero riferimento alle 'finalità di repressione dei reati' sembra di per sé essere sufficiente a negare ogni ipotesi di contrasto della normativa nazionale con quella eurounitaria, tralasciando di considerare anche la fondamentale applicazione del principio di proporzionalità, così rilevante nella giurisprudenza della CGUE", I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *Sistema Penale*, 5, 2020, p. 186. L'autrice prosegue affermando: "Posto che il legislatore nazionale si astiene dal circoscrivere le fattispecie di reato che possono costituire il presupposto dell'operazione di accesso ai dati, i provvedimenti disposti dall'art. 132 cod. privacy non possono considerarsi conformi al principio di proporzionalità ogniqualvolta essi riguardino l'integralità – o perlomeno una parte consistente – delle informazioni presenti sul tabulato". Nella prassi concreta dell'art. 132 Cod. Privacy, infatti, l'autrice rileva come alle richieste di accesso presentate dalle autorità di *law enforcement*, i fornitori di servizi di telecomunicazione siano autorizzati a rispondere "secondo le proprie esigenze organizzative, fornendo tabulati in un formato da loro confezionato, il quale può variare sensibilmente anche in relazione al dettaglio delle informazioni ivi riportate. Il ventaglio dei dati contenuti nel tabulato sembra nella pratica esser dettato dall'organizzazione interna dei gestori, piuttosto che dalle effettive esigenze conoscitive degli organi inquirenti". Da ciò emerge come, neppure nella concreta applicazione della normativa italiana, il livello di intrusione nella sfera privata e dunque di compressione dei diritti fondamentali, risulti rispondente alla gravità del reato per il quale l'accesso è richiesto, in contrasto quindi con quanto chiaramente statuito dalla giurisprudenza della CGUE.

[45] Si legga, in particolare, la sentenza 19 settembre 2006, causa C-506/04, *Graham J. Wilson v. Ordre des avocats du barreau du Luxembourg*, nella quale viene specificato che la nozione di 'indipendenza' deve essere intesa come comprensiva di due differenti aspetti: "Il primo aspetto, avente carattere esterno, presuppone che l'organo sia tutelato da pressioni o da interventi dall'esterno idonei a mettere a repentaglio l'indipendenza di giudizio dei suoi membri per quanto riguarda le controversie loro sottoposte (v., in questo senso, sentenze 4 febbraio 1999, causa C-103/97, Köllensperger e Atzwanger, Racc. pag. I-551, punto 21, e 6 luglio 2000, causa C-407/98, Abrahamsson e Anderson, Racc. pag. I-5539, punto 36; v. anche, nello stesso senso, Corte eur. D.U., sentenza Campbell e Fell c. Regno Unito del 28 giugno 1984, serie A n. 80, § 78). Tale indispensabile libertà da siffatti elementi esterni richiede talune garanzie idonee a tutelare la persona che svolge la funzione giurisdizionale, come, ad esempio, l'inamovibilità (v., in questo senso, sentenza 22 ottobre 1998, cause riunite C-9/97 e C-118/97, Jokela e Pitkäranta, Racc. pag. I-6267, punto 20). Il secondo aspetto, avente carattere interno, si ricollega alla nozione di imparzialità e riguarda l'equidistanza dalle parti della controversia e dai loro rispettivi interessi concernenti l'oggetto di

dubbio indipendente dal Governo e dal Ministero della Giustizia, esso tuttavia assume il ruolo di vera e propria parte nel processo penale eventualmente avviato, così che verrebbe meno il carattere di imparzialità[46]. Questa considerazione, opposta rispetto alla posizione espressa dalla Corte di Cassazione, risulta in linea con quanto rilevato dall'Avvocato generale Pitruzzella nelle Conclusioni al rinvio promosso dalla Corte Suprema estone: questi infatti ha affermato come, per potersi dire 'indipendente', un'autorità debba non solo poter svolgere le proprie funzioni senza subire influenze esterne, né dirette né indirette, ma anche essere al di sopra di qualsiasi sospetto di parzialità (par. 103). Sulla base di tale assunto e pur riconoscendo l'esistenza di talune garanzie di indipendenza nella normativa estone – similmente a quelle previste nell'ordinamento italiano – l'Avvocato generale ha ritenuto infine che proprio la particolare duplicità della natura e delle funzioni esercitate dal pubblico ministero siano tali da far sorgere un legittimo dubbio sulla indipendenza di tale autorità e sulla sua capacità di esercitare un controllo preventivo neutro ed obiettivo sul carattere proporzionato dell'accesso ai dati (par. 118).

Questo richiamo alle Conclusioni dell'Avvocato generale, pur essendo successive alla sentenza della Corte di Cassazione esaminata, mette in luce come il giudice italiano non si sia posto il quesito sul quale invece la Corte Suprema estone si era interrogata, chiedendo, con rinvio risalente al 2018, l'intervento della CGUE al fine di chiarire il significato di 'indipendenza' dell'autorità cui il controllo preventivo deve essere affidato. Nelle decisioni dei giudici italiani sino ad ora esaminate nessun riferimento viene svolto a tale rinvio pendente e dunque ad una possibile interpretazione chiarificatrice sul punto da parte dei giudici europei: in questo senso, "In un quadro caratterizzato più da dubbi che certezze, la strada maestra che si sarebbe dovuta seguire (..) era quella, sollecitata, del rinvio pregiudiziale. (..) Gli ermellini avrebbero dovuto effettivamente domandare se anche un organo formalmente indipendente quale il pubblico ministero italiano, ma non terzo ed imparziale, possa soddisfare lo standard di garanzie richiesto dalla Carta di Nizza"[47]. I giudici italiani però non hanno ritenuto di dover provvedere ad un rinvio ed hanno risolto anzi la questione autonomamente. Ciò in maniera del tutto simile a quanto affermato nella sentenza del 2018, nella quale era stato ritenuto che le prove raccolte mediante l'analisi dei metadati conservati sulla base di una normativa non conforme al diritto dell'UE non dovessero essere considerate automaticamente inutilizzabili[48]: a ben vedere, infatti, anche questo punto è da considerarsi tutt'altro che pacifico e chiaro, tanto che sia la Corte costituzionale belga che la Corte Suprema irlandese[49] hanno promosso rinvii pregiudiziali alla CGUE, chiedendo proprio un chiarimento interpretativo quanto alle possibili conseguenze della dichiarazione di invalidità e incostituzionalità

---

quest'ultima. Questo aspetto impone il rispetto dell'obiettività (v., in questo senso, sentenza Abrahamsson e Anderson, cit., punto 32) e l'assenza di qualsivoglia interesse nella soluzione da dare alla controversia all'infuori della stretta applicazione della norma giuridica" (par. 51-52).

[46] "Certamente, le garanzie di indipendenza del magistrato inquirente nei riguardi del potere esecutivo possono dirsi particolarmente forti nel nostro ordinamento – a differenza di quanto accade in numerosi altri Stati membri. D'altro canto, tuttavia, risulta difficile sostenere che la posizione dell'organo di pubblica accusa all'interno del procedimento penale sia una di assoluta indifferenza quanto al risultato finale dell'accertamento di responsabilità", I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, op. cit., p. 190.

[47] L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, op. cit., p. 763.

[48] "È noto che la inutilizzabilità cosiddetta 'patologica', rilevabile, a differenza di quelle 'fisiologica' e 'relativa' anche nell'ambito del giudizio abbreviato, costituisce un'ipotesi estrema e residuale, ravvisabile solo con riguardo a quegli atti probatori assunti *contra legem*, la cui utilizzazione è vietata in modo assoluto. Nella fattispecie in rassegna, anche a voler disapplicare il D. Lgs. 196 del 2003, art. 132, ci si troverebbe in presenza di un atto compiuto in assenza di legge ordinaria, conforme, però, ai principi fondamentali dell'ordinamento e in particolare al disposto dell'art. 15 Cost. che prevede limitazioni alla libertà e segretezza di ogni forma di comunicazione mediante atto motivato della autorità giudiziaria. Pertanto l'atto sarebbe utilizzabile, qualunque fosse la conclusione sul tema dei rapporti tra normativa interna e principi sovranazionali", sentenza n. 33851 del 2018, par. 1.3.2.

[49] Si rimanda per una ampia analisi del punto, al Capitolo IV, Parte II.

della normativa nazionale in materia di *data retention* e accesso ai metadati per scopi securitari. Anche su questo punto, quindi, la Corte di Cassazione ha ritenuto non necessario l'intervento dei giudici europei, diversamente dai colleghi di altri Stati membri.

Per tutte le ragioni sopra indicate e per le incongruenze e le 'superficialità' nell'analisi di una disciplina che meriterebbe ben altro peso ed attenzione, la giurisprudenza italiana in materia di *data retention* ha attirato notevoli critiche da parte della dottrina: con riferimento alla pronuncia del 2019, ad esempio, e nello specifico alla assenza di valutazioni complete quanto alla compatibilità della normativa italiana rispetto ai numerosi requisiti fissati dalla giurisprudenza europea, si è statuito come "il vuoto motivazionale che affligge in proposito la decisione de qua non può che essere apertamente stigmatizzato: pare, invero, inaccettabile che i supremi giudici nomofilattici, vista la sostanziale impossibilità di salvare da siffatto punto di vista la legittimità delle previsioni interne, abbiano del tutto omesso di argomentare questo profilo"[50]. Una posizione, quindi, quella dei giudici italiani, che viene vista come motivata – ma non per questo giustificabile – dalla volontà di preservare l'efficacia – pur non comprovata – dello strumento della *data retention*, senza addivenire a modifiche o interventi normativi, a scapito però dell'elevato livello di tutela della riservatezza e della protezione dei dati individuato dalla giurisprudenza della CGUE.

Del tutto coerenti alle due pronunce esaminate, sono, infine, le successive sentenze Sez. III 25 settembre 2019, n. 48737 e Sez II, 10 dicembre 2019, n. 5741: in esse la Corte ha avuto modo di ribadire la compatibilità dell'art. 132 Cod. Privacy al diritto dell'UE, nonostante non siano predisposte restrizioni alla conservazione e non siano previsti limiti all'accesso ai metadati ai soli scopi di repressione di reati gravi, predeterminati per legge. Con riferimento a tale profilo, infatti, secondo i giudici italiani la determinazione del carattere di gravità rappresenta una valutazione che non può sottoporsi ad una rigida codificazione da parte del legislatore e che deve pertanto essere correttamente rimessa al vaglio, caso per caso, del giudice. Ciò non si tradurrebbe in un contrasto con la giurisprudenza della CGUE, che affermerebbe anzi solo la sussistenza di un rapporto di proporzionalità tra accesso – e dunque ingerenza – e reato sul quale investigare "in base ad una verifica che il giudice di merito deve compiere in concreto"[51]. I giudici di Cassazione citano peraltro anche la sentenza *Ministerio Fiscal* nella quale si ribadisce l'attenzione al rapporto di proporzionalità che deve intercorrere tra gravità della lesione e gravità del reato perseguito. Sebbene questa analisi, maggiormente articolata ed attenta nonché estesa anche alla recente giurisprudenza della CGUE, sia un segnale positivo che va nella direzione di attribuire una più ampia rilevanza e profondità allo studio e alle motivazioni da addurre per risolvere le questioni complesse attinenti alla materia della *data retention*, tali considerazioni risultano piuttosto discutibili: certo la CGUE non parla mai della necessità di adottare un catalogo di reati, ma altrettanto è vero che, nella sentenza *DRI*, essa afferma l'invalidità della DRD proprio nella parte in cui "non stabilisce

[50] L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, op. cit., p. 764. Dello stesso avviso anche Rezende che afferma come la Corte di Cassazione si sia "sottratta alla resa dei conti con la tormentata disciplina della *data retention* (..). Dal percorso motivazionale della Corte difficilmente emergono profili di analisi sostanziale della disciplina italiana nella materia esaminata. Al contrario, essa sembra faticare nel dare il giusto peso alle questioni poste", I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, op. cit., p. 185.

[51] "Alla luce di tali principi, deve dunque affermarsi il principio secondo cui l'articolo 132 c.pr., nella parte in cui non limita l'accesso ai dati di traffico telefonico, a fini di giustizia penale, a categorie di reati ritenuti particolarmente gravi, non si pone in contrasto con la disciplina sovranazionale di matrice Eurounitaria, il cui rispetto impone invece una valutazione in concreto della proporzione tra gravità dell'ingerenza nel diritto fondamentale alla vita privata che l'accesso ai dati comporta e gravità del reato oggetto d'indagine. Questa valutazione – che, ovviamente, dipende da una serie di variabili connesse alla particolarità dei casi concreti – mal si presta ad una preventiva, rigida, codificazione e non puo' che essere rimessa alla prudente valutazione dell'autorità giudiziaria, o comunque indipendente, che, per la normativa Eurounitaria così come interpretata dalla giurisprudenza della Corte di Lussemburgo, costituisce indefettibile garanzia rispetto alla tutela dei diritti fondamentali", par. 3.6, sentenza n. 48737/2019.

espressamente che tale accesso e l'uso ulteriore dei dati di cui trattasi debbano essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative" (par. 61), senza dimenticare che la DRD stessa imponeva che la conservazione fosse effettuata al fine di "garantire la disponibilità dei suddetti dati a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale" (art. 4). Da tale lettura della normativa e giurisprudenza della CGUE, e diversamente da quanto sostenuto dai giudici italiani, deriva come un elemento fondamentale per determinare in maniera preventiva la natura grave del reato, al di là della singola valutazione dei giudici, sia da individuarsi nell'indicazione, all'interno della disciplina normativa che regola conservazione ed accesso, o di un elenco di reati gravi o quantomeno nella fissazione dei criteri volti a determinarne la gravità (ad esempio considerando gli anni di reclusione). Tale considerazione è peraltro confermata anche dalle scelte normative effettuate nella maggioranza degli ordinamenti di altri Stati membri (Belgio, Spagna e Svezia ad esempio). Ciò peraltro va a tutto favore del rispetto del principio di certezza del diritto e di una applicazione dell'art. 132 Cod. Privacy che non sia lasciata alla discrezionalità del potere giudiziario e dunque passibile di diverse interpretazioni, dalle potenziali conseguenze significative nei confronti degli imputati o indagati e dei loro diritti.

3. – Un legislatore poco attento e un giudice 'conservatore': l'esempio italiano di un dialogo negato con la Corte di giustizia dell'UE e le prospettive future

L'analisi del percorso normativo e giurisprudenziale seguito da legislatore e giudici italiani ha messo in luce quella che può essere definita una disciplina "disarmonica"[52] rispetto ai principi delineati dalla giurisprudenza della CGUE: è innegabile, infatti, che la disciplina della *data retention*, le sue complessità e le rilevanti pronunce adottate a livello europeo, unitamente al serio dibattito apertosi in ambito accademico e politico all'interno delle diverse istituzioni dell'UE e di numerosi Stati membri, non abbiano suscitato in Italia "l'interesse che meritavano, né in dottrina né in giurisprudenza e soprattutto non hanno turbato il sonno del legislatore nazionale"[53].

Sotto il profilo normativo, gli interventi di modifica e riforma che si sono succeduti nel tempo sono andati nella direzione di ampliare, anziché restringere, la portata della conservazione e dell'accesso: non solo, come si è visto, non sono mai state inserite limitazioni e restrizioni quanto ad esempio ai reati per i quali l'accesso ai metadati deve essere concesso, ma anzi è stata aumentata la durata – quanto meno *de facto* – della conservazione[54]. L'avvicendarsi di continue riforme legislative, spesso non anticipate da un appropriato dibattito parlamentare capace di cogliere la reale portata e la delicatezza della materia in esame e il suo impatto sui diritti fondamentali, hanno finito col creare quello che è stato condivisibilmente ritenuto un "pasticcio normativo"[55]. Agire con un susseguirsi di deroghe, proroghe e

[52] F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE Online*, 2, 2017, p. 356.
[53] S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, op. cit., p. 1591.
[54] "Insomma nel sistema plasmato dal legislatore nazionale vi è un circuito di criminalità grave per il quale l'obbligo di conservazione è di sei anni, termine certamente contrario al principio di proporzionalità; ed un circuito di criminalità comune per il quale l'obbligo di conservazione riguarda tutti i reati, del pari contrario a detto principio. Con l'aggravante che, nella prassi, il gestore, non potendo ovviamente distinguere ex ante chi, fra i propri clienti, sarà autore di reati gravi, anche terroristici, e chi di 'semplici' reati comuni, dovrà conservare in modo generalizzato i dati di tutti, tenendoli a disposizione delle agenzie di *law enforcement* per sei anni", S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, op. cit., p. 1593.
[55] P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1, 2016, p. 36. Andolina parla di "tormentata stratificazione della normativa" (E. ANDOLINA,

discipline eccezionali, che finiscono nella realtà applicativa col divenire la regola, non ha che acuito la confusione di una regolamentazione frammentaria e in continuo cambiamento, che deve oltretutto fare i conti con l'evolversi della normativa europea di riferimento. Così facendo, il legislatore nazionale ha evitato quanto invece sarebbe stato di fondamentale importanza, ovvero addivenire ad una seria riflessione sulla materia, promuovendo un intervento normativo ordinato, capace di coprire la disciplina della *data retention* in modo complessivo, anziché inserirla in maniera sparsa in diverse fonti, oltretutto non sempre appropriate per regolare una materia che presenta un impatto così rilevante sui diritti fondamentali e, come si è detto più volte, sullo stesso rapporto tra Stato e cittadino dinnanzi all'esigenza di garanzia della sicurezza. La scelta di inserire singole disposizioni sulla conservazione e accesso ai metadati all'interno di strumenti quali il Decreto milleproroghe o ancora la Legge Europea, dimostra ancora più l'incapacità del legislatore nazionale di discutere e valutare i confini della regolamentazione della *data retention* andando oltre la singola e temporanea urgenza o esigenza emergenziale. Senza dubbio gli attacchi terroristici che hanno scosso il Continente europeo sono stati determinanti per spingere il legislatore italiano ad adottare con velocità e 'a caldo' eccezioni alla disciplina generale in materia di riservatezza e protezione dei dati, ma è altrettanto vero che una situazione di 'normalizzazione' dell'emergenza – seppur discussa e discutibile anche sul piano costituzionale – non può giungere a giustificare la mancanza di una successiva riflessione, 'a mente fredda', su una materia tanto delicata e articolata che dovrebbe essere oggetto di considerazioni di ben più ampio respiro. La "vicenda dell'art. 24, L. n. 167/2017 dimostra ancora una volta che interventi 'tampone' od eccezionali non possono che complicare il quadro, quando a mancare o comunque a non raggiungere gli standard richiesti è la stessa normativa base. Ed appare davvero grave che il legislatore nazionale si sottragga alla responsabilità di dettare una disciplina organica della questione"[56].

Nonostante le critiche e le riflessioni promosse da parte della dottrina, che hanno talvolta ottenuto risonanza anche in quotidiani nazionali, neppure la giurisprudenza, similmente al legislatore e diversamente da molti omologhi di altri Stati membri, ha mostrato di saper cogliere la complessità della disciplina e la problematicità di addivenire ad un corretto bilanciamento tra interessi e diritti differenti, sulla scorta anche di quanto stabilito dalla fondamentale e imprescindibile giurisprudenza della CGUE. Proprio sulla base dei criteri fissati da quest'ultima, come si è ampiamente visto, risulta difficile ritenere che la disciplina italiana abbia svolto una adeguata ponderazione tra interesse generale alla sicurezza e lotta alla criminalità da un lato e tutela della privacy e della protezione dei dati dall'altra. Sotto il profilo del diritto penale ma anche costituzionale, il binomio sicurezza-diritti fondamentali, che ha assunto con l'affermarsi del progresso tecnologico nuovi profili problematici, impone una profonda riflessione da parte di legislatori e giudici: il tema non deve essere letto nell'ottica di un trade-off e dunque del sacrificio di taluni diritti – in questo caso alla riservatezza e protezione dei dati – a favore di ampi poteri e mezzi nelle mani delle autorità pubbliche finalizzati alla garanzia della sicurezza. Deve essere, al contrario, affrontato nella prospettiva di un bilanciamento necessario e possibile: è proprio rispetto a tale prospettiva che la legislazione italiana si è mostrata carente, avendo prediletto soluzioni estemporanee, emergenziali e urgenti che hanno provocato una propensione alla tutela della sicurezza priva di quelle garanzie e salvaguardie che dovrebbero invece accompagnare scelte normative di così rilevante impatto per i diritti fondamentali. Così le critiche mosse al regime normativo italiano, fondate proprio su tali valutazioni, peraltro ampiamente argomentate anche dalla dottrina, non sono state accolte dai giudici italiani che non hanno mai valutato l'esistenza di profili di incompatibilità della normativa interna rispetto alla Costituzione italiana o al diritto dell'UE tali da portare nel primo caso ad una dichiarazione di illegittimità o, nel secondo, alla disapplicazione della legislazione nazionale. Non è possibile infatti tacere come, oltre al raffronto con i principi delineati a livello dell'UE, sia venuta a

L'acquisizione nel processo penale dei dati 'esteriori' delle comunicazioni telefoniche e telematiche, Cedam, 2018).

[56] S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, op. cit., p. 1593.

mancare nella giurisprudenza italiana una valutazione dell'impatto della disciplina sulla conservazione generalizzata ed accesso ai metadati rispetto alle tutele previste e riconosciute dalla Costituzione stessa; così come non è mai stato neppure ritenuto opportuno provvedere ad un rinvio alla CGUE, finalizzato a chiarire punti quantomeno dubbi o di difficile applicazione attinenti a tale materia.

E così, nel silenzio del legislatore – o meglio nel rumore scomposto e confuso provocato dai vari interventi e discipline eccezionali succedutesi negli ultimi anni – e nella mancata presa di posizione da parte delle Corti nazionali, la normativa sulla *data retention* in Italia continua ad essere attuata come se sul piano dell'UE nulla di determinante fosse accaduto o comunque nulla che possa avere un serio impatto per la disciplina vigente.

Certo la mera disapplicazione[57] da parte dei giudici dello strumento della conservazione e accesso ai metadati, pur da taluni auspicata, non risulta essere, a parere di chi scrive, una possibilità che possa dirsi soddisfacente[58] – rappresentando una mera soluzione ai singoli casi concreti sottoposti ai giudici – e che lascia sicuramente perplessi e preoccupati per gli effetti che potrebbe provocare sulle indagini in corso e sui procedimenti penali in atto fondati sulla raccolta e analisi dei dati di traffico e telematici. Questa preoccupazione del resto è già stata espressa anche dai giudici di altri Stati membri, che pure non hanno mancato di prendere una più energica posizione in materia, anche allo scopo di provocare una reazione e riflessione da parte del legislatore nazionale.

---

[57] Come si è visto nei casi sopra analizzati, infatti, i difensori degli imputati o indagati avevano richiesto ai giudici la disapplicazione della normativa in materia di *data retention* in quanto contrastante con il diritto dell'UE. Anche la dottrina aveva del resto ritenuto percorribile tale via: "Se l'art. 132 Cod. Privacy è contrario agli artt. 7, 8 e 52 CDFUE, esso deve essere disapplicato, come ogni norma che contrasti con il diritto comunitario, secondo gli elementari insegnamenti che governano da decenni i rapporti tra diritto dell'Unione e diritto interno. (..) L'unica risposta possibile, pertanto, è che, finché il legislatore nazionale non interviene ad emendare i profili di contrasto dell'art. 132 Cod. Privacy con il diritto dell'UE, l'attività di *data retention* non dovrebbe essere possibile: altrimenti il vuoto di disciplina – addebitabile allo Stato – gioverebbe allo Stato stesso nelle sue indagini e, viceversa, un diritto fondamentale come quello alla riservatezza dei dati risulterebbe nei fatti tutt'altro che inviolabile", S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, op. cit., p. 1592. Per Flor "se le norme interne dei singoli Stati, come nel caso italiano, non rispettano gli standard ricavabili dalla sentenza della Corte, esse dovrebbero essere disapplicate dal giudice interno per contrasto con il diritto europeo", R. FLOR, *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, in *Diritto dell'Informazione e dell'Informatica*, 2014, p. 793 e dello stesso avviso anche S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di diritto pubblico comunitario*, 3-4, 2015. In questo contesto, alcuni autori si sono anche interrogati su una ulteriore possibile soluzione, sebbene anch'essa non soddisfacente e non totalmente risolutiva delle problematiche evidenziate: potrebbe cioè il singolo operatore delle telecomunicazioni, nell'inerzia del legislatore, non ritenersi vincolato all'obbligo di conservazione dei metadati? "Da un lato la questione è quella del se il privato fornitore del servizio, destinatario di un diritto nazionale vigente che ancora obbliga a conservare i dati esterni del traffico telefonico e internet, sia tenuto a disapplicare tale imposizione, incorrendo in caso contrario in una responsabilità per violazione della privacy dei propri utenti. D'altra parte, posto che il perdurante onere di conservazione dei dati affligge non solo il diritto alla riservatezza, ma ostacola anche la libera circolazione dei servizi (ponendo costi di servizio aggiuntivi agli operatori, gravati della conservazione e delle relative spese) ci si può chiedere se anche il gestore stesso – non remunerato dall'ordinamento per un onere gestionale illegittimo – possa essere interessato a dismettere la conservazione o proseguirla con richiesta di un risarcimento per il danno economico patito", F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa*, op. cit., p. 356.

[58] "La soluzione della disapplicazione presenta evidentemente i limiti dell'essere un rimedio legato al caso concreto, destinato ad operare ex post, quando ormai la violazione dei diritti fondamentali si è verificata. E infatti, da un lato non consente di rimediare all'ingerenza, illegittima, che si è verificata a monte per effetto della conservazione dei dati; dall'altro non risolve il problema della conservazione e acquisizione per finalità di intelligence, rispetto alla quale non si pone un problema di disapplicazione, non potendo tali dati essere utilizzati all'interno di un processo penale", F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, op. cit., p. 4282.

Per questo la soluzione alla complessa situazione italiana è certamente da individuarsi in un intervento normativo, che sino ad oggi neppure l'occasione offerta dall'aggiornamento del Codice Privacy sulla base del GDPR ha saputo incentivare[59].

Sebbene taluni profili della disciplina – tra cui il nodo centrale circa l'incompatibilità, per sé, della conservazione generalizzata (c.d. *bulk data retention*) – siano ancora in attesa di definizione chiara, univoca e sperabilmente definitiva da parte della CGUE nei numerosi rinvii pregiudiziali già esaminati nella Parte II del presente lavoro, il legislatore italiano potrebbe già intervenire quantomeno sul fronte della disciplina dell'accesso ai metadati conservati, seguendo i requisiti dettati dalla giurisprudenza dell'UE: restringere l'accesso ai reati gravi, determinando tale soglia, nonché definire i soggetti indipendenti cui attribuire il delicato compito del controllo preventivo[60], salvo prevedere poi, in casi di particolare urgenza, una procedura più rapida di accesso ai metadati con un intervento di convalida successivo[61]. Pur non risolvendo il problema di una conservazione comunque generalizzata, una riforma in tale direzione consentirebbe comunque una maggiore garanzia di compatibilità della disciplina italiana rispetto al diritto dell'UE ed un più elevato standard di tutela dei diritti fondamentali. I numerosi rinvii pregiudiziali al momento pendenti dinnanzi ai giudici di Lussemburgo quindi impongono di non adottare scelte legislative affrettate, che potrebbero altrimenti risultare in breve tempo sconfessate – come già accaduto, ad esempio, nel Regno Unito – dalla giurisprudenza della CGUE. Nonostante queste necessarie consapevolezze, si ritiene però di dover sostenere l'importanza di una rapida quanto profonda riflessione da parte del legislatore – ma anche del giudice italiano – su tale tema, sino ad ora troppo frettolosamente studiato e le cui problematiche sono state troppo velocemente risolte.

[59] Nel 2019, Marcolini auspicava ed individuava come possibile soluzione un rinvio alla CGUE da parte della Cassazione, inteso "nella più ampia prospettiva di 'provocare' il legislatore nazionale – l'unico realmente legittimato a riordinare una disciplina dalle ormai troppe incongruenze e slabbrature – il cui intervento non pare più in alcun modo differibile: e il più generale aggiornamento della disciplina nazionale sul trattamento dei dati personali ai contenuti del Reg. 2016/679 potrebbe rappresentare il momento propizio", S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, op. cit., p. 1596. Purtroppo tale previsione, come si è visto, non si è realizzata.

[60] Rezende suggerisce anche l'adozione di un duplice sistema, "in cui l'intervento del giudice sia limitato alle richieste di acquisizione che riguardino l'integralità dei dati presenti sul tabulato [dunque comportanti una ingerenza grave]. (..) Al contempo il potere di accesso del pubblico ministero potrebbe essere mantenuto solo per le misure che determinino una lieve ingerenza nei diritti protetti", I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, op. cit., p. 193. Peraltro è da sottolineare come la giurisprudenza italiana abbia ristretto l'onere in capo al pubblico ministero, affermando come la motivazione richiesta a sostegno del decreto "possa dirsi soddisfatta anche con espressioni sintetiche e che la sua assenza non comporta alcuna inutilizzabilità, ma potrebbe generare al più una nullità non assoluta, da eccepirsi prima della pronuncia della sentenza di primo grado (Cass. Pen. Sez. IV, 24.5.2005, n. 20558)", S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, op. cit.p. 1586.

[61] Questa modulazione della procedura a seconda delle circostanze è del resto in parte suggerita anche dalla giurisprudenza della CGUE, che stabilisce la possibilità di ricorrere a misure d'urgenza rispetto alle quali il livello di tutela e salvaguardie può essere ridotto.

CONCLUSIONI

L'articolato percorso di analisi svolto nelle pagine di questo lavoro non può che concludersi con alcune riflessioni critiche che, ripercorrendo le varie tappe della presente ricerca, cercano di fornire risposte ai complessi quesiti inizialmente posti nell'Introduzione ed emersi lungo tutto l'elaborato.

Considerati i molteplici aspetti meritevoli di essere sviluppati, è parsa utile e quanto mai necessaria una sistematizzazione in quattro paragrafi. Essi sono costruiti sulla base dei profili assunti a fondamento dell'ordito della tesi stessa, mettendone in rilievo la trama complessa, in cui ogni parte non può essere scissa dall'altra e in cui ciascuna contribuisce a formare quella '*big picture*', sin dall'introduzione tratteggiata, che è punto di arrivo e, per altri versi, di possibile ri-partenza.

Ecco allora che nella prima sezione verranno tratte valutazioni quanto alla specifica disciplina della *data retention* nel contesto dell'UE: particolare attenzione verrà prestata non solo ai punti fermi che possono essere individuati sulla base della normativa e della giurisprudenza della CGUE, bensì anche alle conseguenze, alle possibili prospettive e alle problematiche ancora aperte che da tali punti fermi derivano. Il secondo paragrafo si occuperà della 'dimensione esterna' dell'azione dell'UE nell'ambito della disciplina della *data retention*: lo sguardo scorre oltre i confini europei, pur rimanendo strettamente legato alla dimensione interna e presentando determinanti connessioni con essa, così da indurre ad alcune autonome riflessioni sul tentativo dell'UE di promuovere e stabilire uno standard elevato di tutela della privacy e della protezione dei dati nel contesto globale e nel suo rapporto con gli Stati terzi. La terza sezione si concentrerà su una analisi comparata, fondata sullo studio di Regno Unito, Belgio e Italia e degli approcci e reazioni ordinamentali dei tre Stati in esame. Il quarto paragrafo, infine, porrà in luce come una analisi dettagliata della disciplina della *data retention* possa arrivare a determinare se il rapporto tra esigenze securitarie e tutela dei diritti fondamentali alla riservatezza e alla protezione dei dati nell'era dei Big Data sia correttamente letto nell'ottica del 'trade-off' di cui Daniel Solove ci ha parlato e con cui le pagine di questo elaborato si sono aperte, o se invece una tale visione di sintesi debba essere rifiutata e ritenuta incapace di cogliere la complessità di questa delicata tematica.

1. La disciplina della **data retention** *nell'Unione europea: la difficile sfida, ancora aperta, della determinazione di un punto di equilibrio tra esigenze securitarie e diritti fondamentali e il complesso rapporto tra Legislatore europeo e CGUE*

L'analisi svolta nella Parte II del presente lavoro e dedicata alla comprensione e allo studio tanto dell'approccio legislativo quanto di quello giurisprudenziale che ha nel tempo caratterizzato l'azione dell'UE in materia di *data retention*, ha messo chiaramente in evidenza la grande attenzione che alla specifica disciplina scelta quale 'caso di studio' è stata posta nonché l'ampio dibattito che ha interessato tutte le Istituzioni dell'UE. Esse hanno trattato la discussa materia in maniera anche molto diversificata, potendosi distinguere sin da subito e con chiarezza un legislatore assente ed immobile ed una Corte di giustizia che si è invece imposta come punto di riferimento, sopperendo all'inattività del legislatore europeo stesso e talvolta anche dei legislatori nazionali.

In quella che è divenuta la storica *data retention saga*, la posizione della CGUE dinnanzi alla complessa sfida della determinazione del rapporto tra sicurezza e tutela dei diritti fondamentali ha segnato alcuni punti fissi, di enorme rilievo e dalla portata innovativa: i giudici di Lussemburgo infatti hanno dimostrato una grande consapevolezza dei rischi e delle minacce legate all'impiego di forme di sorveglianza pervasive e massive, fondate sull'utilizzo delle potenzialità derivanti dalle nuove tecnologie. Così l'architettura normativa solida che nel contesto dell'UE tutela il diritto alla privacy così

come quello alla protezione dei dati, mediante il riconoscimento lungimirante contenuto nella Carta di Nizza, nonché nei Trattati e nel vasto numero di Regolamenti e Direttive specifiche, si arricchisce anche della garanzia fornita dalla giurisprudenza della CGUE. Questa, merita precisarlo, non si è limitata solo ad interventi determinanti in materia di *data retention* bensì ha mostrato un forte attivismo e sensibilità rispetto all'impatto delle nuove tecnologie sui diritti fondamentali anche in altri ambiti: si pensi alle sentenze *Google Spain*[1] e alla più recente *Google LLC v. -CNIL*[2], nelle quali sono stati definiti contorni e confini del c.d. diritto all'oblio, di matrice appunto giurisprudenziale.

In questo articolato panorama, dunque, le decisioni dei giudici di Lussemburgo, a partire dalla sentenza *DRI* hanno certamente il pregio e il merito di aver stabilito principi di vasto impatto, che denotano una conoscenza della tematica profonda: l'affermazione della invasività dei metadati e della loro capacità di incidere in maniera significativa sulla sfera privata, come si è già ampiamente sottolineato, non è affatto di poco conto ed appare anzi come constatazione rivoluzionaria, che si fonda sulla comprensione del funzionamento dei sistemi di *data analytics* e sulle potenzialità sconfinate che la disponibilità e lettura aggregata dei metadati comportano. Ciò si somma all'altrettanto importante dichiarazione secondo cui anche la sola conservazione, indipendentemente dal successivo e meramente eventuale accesso, comporta una invasione nella sfera privata e una compressione del diritto alla protezione dei dati. Ciò pare aspetto tutt'altro che scontato, soprattutto dinnanzi alle considerazioni, pur da taluni sostenute, secondo cui la conservazione in sé e per sé considerata non potesse ritenersi lesiva di alcun diritto: la CGUE ribadisce invece con chiarezza sia nella sentenza *DRI* che nella *Tele2* che l'obbligo di conservazione dei metadati costituisce "per sé un'ingerenza nei diritti garantiti dall'art. 7 della Carta. L'accesso delle autorità nazionali competenti ai dati costituisce un'ingerenza supplementare in tale diritto fondamentale" (par. 34-35, *DRI*) e parimenti viene sostenuto con riferimento al diritto di cui all'art. 8 Carta di Nizza. Tenendo poi conto del contesto storico e dunque anche delle rivelazioni di Snowden, che avevano determinato una più chiara consapevolezza dei rischi e dei pericoli per la riservatezza e la protezione dei dati, minacciati da sistemi di sorveglianza generalizzata, la CGUE non ha mostrato tentennamenti né nel dichiarare l'invalidità immediata della DRD – senza cioè quella dilazione dell'efficacia temporale della sentenza che invece era stata proposta dall'Avvocato generale nelle sue Conclusioni – e la non conformità alla Carta di Nizza dell'Accordo *Safe Harbour* e della relativa Decisione di adeguatezza né nel dichiarare l'incompatibilità al diritto dell'UE della bozza di Accordo negoziato con il Canada in materia di trasferimento di PNR. I giudici di Lussemburgo quindi hanno applicato un vaglio di proporzionalità e stretta necessità che, tenendo conto della delicatezza delle questioni sottoposte al loro controllo e degli effetti che esse potevano comportare per la tutela effettiva dei diritti fondamentali in una società realmente democratica e nello Stato di diritto, ha condotto ad una decisa garanzia dei diritti alla privacy e alla protezione dei dati anche di fronte alle esigenze securitarie e alle forti posizioni espresse dagli Stati membri che spingevano nella opposta direzione di lasciare un margine di apprezzamento più ampio in capo ai legislatori nazionali quanto alla adozione di misure così rilevanti in materia di sicurezza.

Non si può pertanto non rilevare come l'approccio "dato-centrico" della CGUE abbia portato ad una forte espansione della tutela del diritto alla riservatezza nell'era digitale[3], come tutto il filone giurisprudenziale inaugurato dalla pronuncia *DRI* testimonia. Ciò ha portato alla trasformazione

[1] 13 maggio 2014, C-131/12, *Google Spain SL e Google Inc. v. Agencia Espanola de Proteccion de Dator (AEPD) e al*.

[2] 24 settembre 2019, C-507/17, *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*.

[3] O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain,* in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* Roma TrE-Press, 2015, p. 7. Ma anche H. HIJMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 16 TFEU*, Springer, 2016; F. FABBRINI, *Human rights in the digital age: the European Court of Justice ruling in the Data Retention Case and its lessons for privacy and surveillance in the United States*, in *Harvard Human Rights Journal*, 28, 2015.

dell'Unione europea in quella che è stata definita una "fortress of digital privacy"[4], con conseguenze che, come si è visto e come si dirà anche in seguito, si riverberano anche nei rapporti tra UE e Stati terzi. I giudici di Lussemburgo, insomma, sembrano volersi porre come "ultimate protector of constitutional rights in Europe"[5], realizzando la propria vocazione di farsi giudici costituzionali ma anche di imporre la leadership dell'UE a livello globale in materia di privacy e *data protection*.

Certamente, la tendenza ad una lettura ampia e garantista delle tutele sancite dalla Carta di Nizza così come dalla normativa europea stessa in materia di protezione dei dati, in un momento di emergenza normalizzata e di sempre maggiore diffusione di reati transfrontalieri gravi o perpetrati online (c.d. *cybercrimes*), dimostra come "i giudici comunitari [abbiano] sperimentato la loro capacità di essere rigorosi nella tutela dei diritti su uno dei terreni più spinosi, dato che la gravità della situazione internazionale tende ad attutire la sensibilità verso i diritti dei sospetti terroristi e genera una maggiore propensione verso le esigenze della sicurezza piuttosto che verso quelle della giustizia e della libertà"[6].

Se tutte le considerazioni sino a qui svolte risultano innegabili ed imprescindibili punti fermi, tali da ispirare anche le riflessioni riguardanti l'azione dell'UE nella sua dimensione esterna così come l'impatto sugli Stati membri, nei quali anche – e soprattutto – grazie alle pronunce della CGUE si è aperto un serio e approfondito dibattito in materia di *data retention*, è tuttavia necessario mettere in rilievo anche gli elementi problematici che da tale giurisprudenza sono parimenti scaturiti. I dubbi, le difficoltà interpretative, le zone grigie ed alcuni punti deboli nel ragionamento dei giudici di Lussemburgo non possono del resto essere ignorati e sono anzi resi evidenti dai numerosi rinvii pregiudiziali ancora pendenti in tale ambito, che denotano la complessità di una materia ancora in cerca di un chiaro punto di definizione ma anche, in parte, l'eccessiva rigidità della giurisprudenza della CGUE che, a parere di molti Governi degli Stati membri e autorità di *law enforcement* nazionali, risulta poco pragmatica, con il rischio di incidere in maniera significativa sulla tutela della sicurezza.

Una delle questioni più delicate e poste in discussione è sicuramente da rinvenirsi nella determinazione dell'ambito di applicazione del diritto dell'UE: tutti i rinvii pregiudiziali promossi a seguito della sentenza *Tele2* hanno evidenziato tale problematica e tutti gli Stati membri intervenuti nei procedimenti dinnanzi alla CGUE hanno cercato, taluni con più forza e decisione di altri, di indurre i giudici di Lussemburgo a determinare in maniera più chiara il confine tra le competenze dell'UE e quelle degli Stati membri. Del resto i dubbi su tale punto presentano radici lontane nel tempo e sono stati alimentati dall'iniziale distinzione tra disciplina della conservazione e dell'accesso promossa dagli stessi giudici della CGUE nella sentenza *Irlanda v. Parlamento europeo e Consiglio*. Proprio questa decisione infatti è stata più volte richiamata a sostegno proprio di quella posizione che voleva delimitare l'ambito di applicazione del diritto dell'UE alla sola materia della *data retention*, per lasciarne invece quella relativa all'accesso interamente al di fuori e dunque 'scoperta' dai criteri rigidi individuati dalla CGUE. Quest'ultima, al contrario, a partire dalla sentenza *DRI* si è occupata di fissare condizioni e requisiti anche relativamente all'accesso: considerando che tali attività, pur poste in essere da autorità pubbliche, prevedono comunque una attività di trattamento di dati personali da parte dei fornitori privati, esse rientrano nella disciplina prevista dalla Direttiva *e-Privacy* e, dunque, dal diritto dell'UE. Su di un ragionamento simile si fonda poi, come si è visto nelle Conclusioni dell'Avvocato generale nel caso *Ministerio Fiscal*, il principio secondo cui ogniqualvolta una disciplina in materia di *data retention* e accesso per scopi securitari implichi l'obbligo di qualche tipo di trattamento del dato in capo a soggetti

[4] L. P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of the EU and US constitutional systems*¸ in L. VIOLINI, A. BARAGGIA (a cura di), *The fragmented landscape of fundamental rights protection in Europe: the role of judicial and non-judicial actors*, Elgar Publish, 2018.
[5] D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* in *ERA Paper*, 2018.
[6] M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione Europea*, in M. CARTABIA (a cura di), *I diritti in azione*, Il Mulino, 2007, p. 13.

privati, essa debba essere considerata rientrante nell'ambito di applicazione del diritto dell'UE[7]. Questo orientamento, ripreso peraltro dall'Avvocato generale Campos Sanchez-Bordona nelle Conclusioni riferite ai rinvii pregiudiziali in parte pendenti e solo ultimamente risolti dalla CGUE, ovvero quelli promossi dall'IPT inglese, dalla Corte costituzionale belga e dal Consiglio di Stato francese[8], comporta il fatto che la determinazione dell'applicabilità dei c.d. *criteri Tele2* e dunque degli stringenti requisiti fissati dalla *data retention saga* prescinda dallo scopo ultimo cui le misure di conservazione e accesso sono preposte, ben potendo essere adottate anche per finalità di tutela della sicurezza nazionale e coinvolgere agenzie di intelligence. Ne consegue che, qualora tale posizione venisse approvata e seguita dalla CGUE, ciò determinerebbe un modo di delineare il riparto di competenze tra UE e Stati membri più flessibile e a tutto favore di un ampliamento delle competenze dell'UE stessa. Solo le operazioni svolte direttamente da autorità di *law enforcement* o agenzie di intelligence, che non prevedono pertanto un intervento di soggetti privati (i *service providers*), rimarrebbero unicamente di competenza degli Stati membri e rispetto ad esse quindi non sarebbe applicabile quella lettura della Carta di Nizza e della proporzionalità delle misure di *data retention* promossa dalla CGUE. Un tale orientamento ha visto la netta opposizione degli Stati membri che hanno più volte richiamato l'art. 4 TFUE che rimette nelle loro esclusive mani la garanzia della sicurezza nazionale.

La posizione espressa sul punto dalla Corte di giustizia e dall'Avvocato generale Campos Sanchez-Bordona, che resta quindi in attesa di conferma anche con riferimento alle questioni promosse nei più recenti rinvii pregiudiziali, presenta senza dubbio numerosi risvolti positivi e meritevoli di attenzione: innanzitutto l'orientamento espresso dalla CGUE ha il vantaggio di superare la fragilità insita nella distinzione tra operazioni poste in essere da autorità di *law enforcement* e autorità di intelligence, così come tra finalità di sicurezza nazionale e sicurezza pubblica. Come si è avuto modo in più punti di sottolineare nel corso di questo lavoro, il progresso della tecnica ed i mezzi sempre più sofisticati posti a disposizioni di entrambi i soggetti sopra indicati, hanno reso sempre più sfumato e labile il confine tra attività poste in essere da autorità di *law enforcement* e autorità di intelligence[9], così da rendere complessa la distinzione sulla mera base degli scopi: la sicurezza e la sua categorizzazione in nazionale e pubblica è del resto concetto estremamente ampio e vago, che non trova ad oggi una chiara definizione e linea di demarcazione, con tutte le conseguenze che ne derivano in termini di difficoltà nella determinazione dell'ambito di applicazione del diritto dell'UE. Inoltre, se si valuta quanto affermato

[7] L'Avvocato generale Saugmandsgaard Øe nelle Conclusioni al caso *Ministerio Fiscal* infatti afferma la necessità di distinguere i dati personali trattati "*direttamente* nell'ambito delle attività – di natura sovrana – dello Stato in un settore rientrante nel diritto penale e, dall'altra, quelli trattati nell'ambito delle attività – di natura commerciale – di un fornitore di servizi di comunicazione elettronica che sono *successivamente* utilizzati dalle autorità statali competenti" (par. 47). Riferendosi dunque ad attività "sovrane" dello Stato come a quelle che si "riferiscono alle funzioni riservate allo Stato o ai suoi apparati, che esso non può delegare ad enti privati, in particolare, quelle relative alla giustizia, alla polizia o alle forze armate" (nota 43), l'Avvocato generale ritiene tra di esse rientranti il trattamento dei dati da parte di "autorità di polizia o giudiziarie al fine di ricercare gli autori di reati, ad esempio i dati raccolti e analizzati durante un'intercettazione di conversazioni telefoniche effettuata da agenti di polizia su richiesta di un giudice istruttore" (nota 44).

[8] Si fa riferimento ai rinvii, ampiamente analizzati nel Capitolo IV, Parte II, C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs* e al.; cause riunione C-511/18 e C-512/18, *French Data Network, La Quadrature du Net e al. c. Premier ministre, Garde des Sceaux, Ministre de la Justice* e C-520/18, *Ordre des barreaux francophones et germanophone e al. c. Conseil des ministres*.

[9] Sul punto si rimanda a: P. VOGIATZOGLOU, S. FANTIN, *National and public security within and beyond the Police Directive*, in A. VEDDER, J. SCHROERS, C. DUCUING, P. VALCKE (a cura di), *Security and Law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Intersentia, 2019, pp. 27-62. Ma anche Crespi, sottolinea con chiarezza come "the heightened capacity for wide-scale data harvesting by the intelligence services of the Member States, including by gaining access to data initially collected by private operators for commercial reasons, has blurred the dividing line and increased the potential for interference between activities seeking to guarantee national security and contiguous areas governed by EU law, such as for instance the protection of privacy", S. CRESPI, *The applicability of Schrems principles to the Member States: national security and data protection within the EU context*, in *European Law Review*, 5, 2018, p. 678.

dalla CGUE nella pronuncia *Promusicae v. Telefonica*[10], secondo cui "la sicurezza nazionale, la difesa e la sicurezza pubblica, costituiscono attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei singoli" (par. 51), si dovrebbe ritenere l'ambito della sicurezza nazionale di sola competenza degli Stati membri come ormai residuale e piuttosto ristretto, considerato che la maggior parte delle operazioni poste in essere dalle autorità pubbliche nella lotta alla criminalità coinvolgono sempre più spesso, come nel caso della *data retention,* soggetti privati[11].

A questo primo vantaggio è da aggiungersi sicuramente anche un pregio conseguente e forse di maggior rilievo: limitare le aree di disciplina escluse dal diritto dell'UE e dunque ricondurre le attività delle autorità di *law enforcement* o intelligence, anche qualora svolte per scopi di sicurezza nazionale, entro l'ambito di applicazione del diritto europeo significa estendere contestualmente la tutela della Carta di Nizza e la possibilità dei giudici di Lussemburgo di effettuare il proprio vaglio. Diversamente dalla Corte EDU che non ha limitazioni in tali termini e che quindi ha ben potuto esaminare anche normative riguardanti forme di sorveglianza diretta poste in essere dalle autorità pubbliche[12], ponendo requisiti e criteri di proporzionalità anche in aree nelle quali non era previsto l'intervento o la mediazione di soggetti privati, la Corte di giustizia dell'UE si trova invece ad operare in un contesto differente, che prevede limitazioni sulla base del principio di attribuzione e quindi aree specifiche lasciate al di fuori dell'ombrello del diritto dell'UE e delle garanzie offerte dalla Carta di Nizza stessa. Promuovere quindi una linea interpretativa che riconduca all'ambito di applicazione del diritto europeo attività capaci di incidere così fortemente sui diritti fondamentali, indipendentemente dallo scopo perseguito bensì sulla base dei soggetti e della natura delle operazioni svolte, consente di scongiurare il rischio che il semplice richiamo alla finalità di sicurezza nazionale diventi un ariete impiegato per sfondare le porte di quella 'fortezza della privacy' così faticosamente e meticolosamente innalzata dal legislatore ma soprattutto dalla giurisprudenza della CGUE.

---

[10] 28 gennaio 2008, C-275/06, *Productores de Musica de Espana (Promusicae) c. Telefonica de Espana SAU*.

[11] Così A. DIMOTROVA, M. BRKAN, *Balancing national security and data protection: the role of EU and US policy-makers and Courts before and after the NSA affair*, in *Journal of Common Market Studies*, 4, 2018, p. 751. A ciò si deve sommare anche quanto disposto nell'art. 83 TFUE, nei quali vengano affermate le competenze dell'UE nell'ambito della determinazione di "norme minime relative alla definizione dei reati e delle sanzioni in sfere di criminalità particolarmente grave che presentano una dimensione transnazionale derivante dal carattere o dalle implicazioni di tali reati o da una particolare necessità di combatterli su basi comuni", tra cui anche la lotta al terrorismo, più volte considerato quale uno degli obiettivi della *data retention* così come regolata nella DRD e nelle successive sentenze della CGUE.

[12] La giurisprudenza di tale Corte risulta di grande rilievo soprattutto con riferimento alle discipline escluse dall'ambito di applicazione del diritto dell'UE e rispetto alle quali potranno valere le salvaguardie e requisiti stabiliti appunto dalla Corte EDU. Come si è detto nel Capitolo V, Parte II, i giudici di Strasburgo vantano certamente una lunga storia giurisprudenziale con riferimento a tematiche e normative attinenti a forme di sorveglianza massiva. Sebbene nelle ultime pronunce, ancora sottoposte a rinvio alla Grande Camera, sia riscontrabile un certo scostamento dai requisiti indicati nei precedenti della medesima Corte, quanto nella giurisprudenza delle CGUE, è innegabile come anche i giudici di Strasburgo abbiano contributo ad affermare una solida tutela della riservatezza nel contesto di pratiche di controllo operate da autorità pubbliche: nel riconoscimento della possibilità eccezionale di ricorso e vaglio in astratto, considerato come legittimo in deroga all'art. 34 CEDU, la Corte ha dimostrato una forte sensibilità al tema, fissando importanti salvaguardie e riconoscendo i pericoli e le minacce che da pratiche di sorveglianza possono derivare. In tal senso è interessante richiamare le parole dei Giudici Koskelo e Turkovic nella loro *Joined Partly Dissenting and Partly Concurring Opinion* al caso *Big Brother Watch*, al par. 15: "There is yet another "sea change" calling for heightened attention in the assessment of the necessary standards in the context of secret surveillance of communications. It is the degradation of respect for democratic standards and the rule of law of which there is increasing evidence in a number of States. While I am not suggesting that the present respondent State is a case in point in this regard, the Convention standards must nevertheless be considered in the light of the fact that such developments testify to the actual or potential fragility of safeguards, institutional arrangements and the underlying assumptions that in ideal circumstances might appear adequate in order to minimise the risks of abuse. In fact, the same threats that are invoked to justify secret surveillance may also serve to reinforce tendencies toward a weakening of the checks and balances which underpin adherence to the rule of law and democratic governance".

Nonostante i profili positivi sin qui rilevati, che consentono anche di comprendere il pregio delle scelte e delle letture fornite dai giudici di Lussemburgo nella vasta giurisprudenza in materia di *data retention*, permangono proprio su tali aspetti dubbi e criticità che ne rivelano anche i limiti: l'interpretazione 'espansiva' dell'art. 15 Direttiva *e-Privacy* e dell'ambito di applicazione dello stesso – e dunque del diritto dell'UE – mette infatti in luce le debolezze del principio di attribuzione in materie, come quella della conservazione e accesso ai metadati, così complesse ed articolate, dalle molteplici sfaccettature. Non è un caso che molti Governi degli Stati membri, intervenuti nelle controversie dinnanzi alla CGUE, abbiano più volte ribadito la fragilità e, a tratti, la contraddittorietà della posizione espressa dai giudici europei: questi ultimi hanno talvolta ritenuto determinante l'intervento di soggetti privati, incaricati della raccolta e conservazione dei dati in primis per finalità commerciali, mettendo in luce così sia la distinzione tra le fasi di conservazione ed accesso, considerate come distinte e soggette a discipline differenti, sia lo scopo primario della normativa in materia di *data retention*, individuato nella armonizzazione delle normative nazionali adottate in tale ambito, la cui marcata disomogeneità avrebbe potuto ed invero ha prodotto un impatto sul mercato interno e sull'operato dei fornitori di servizi di telecomunicazione, col rischio ultimo di incidere negativamente in materia di concorrenza e libera circolazione dei servizi (in tal senso si legga la sentenza *Irlanda c. Parlamento e Consiglio*). Diversamente da tale lettura, però, la CGUE ha nelle più recenti pronunce messo in rilievo lo scopo principale della *data retention*, identificato nella garanzia della sicurezza e nella finalità di consentire alle autorità di *law enforcement* l'accesso ai dati[13], tanto che nella sentenza *DRI* i giudici si sono spinti a trattare criteri e condizioni relativi non solo alla conservazione, bensì anche all'accesso. Se certamente alcuni dei profili critici derivanti da queste distinzioni problematiche e forzate siano state risolti con il superamento della struttura a Pilastri e dunque mediante il Trattato di Lisbona, altri aspetti parimenti problematici permangono ancora oggi, legati come sono alla interpretazione ampia dell'ambito di applicazione della Direttiva *e-Privacy*, per mezzo del dettato dell'art. 15, a scapito di altre disposizioni della medesima Direttiva, come l'art. 1, co. 3, che mira invece a definirne i confini e i limiti. Il ragionamento dei giudici di Lussemburgo, fondato ad esempio sulla distinzione tra 'obiettivo' – riconosciuto nella armonizzazione delle disposizioni degli Stati membri relative agli obblighi dei fornitori – ed 'obiettivo sostanziale' – individuato nella lotta alla criminalità grave (par. 41, *DRI*) – o ancora su valutazioni 'alla luce dell'economia generale' della Direttiva *e-Privacy* (par. 73, *Tele2*), pare ancora piuttosto fragile, non solo da un profilo prettamente formale.

La determinazione di tali questioni rivela un forte rilievo sostanziale se si pensa agli enormi impatti 'concreti' che il ricondurre la disciplina della *data retention* e dell'accesso, anche per finalità di sicurezza nazionale, all'alveo del diritto dell'UE comporta. Ciò impone, come si è detto, il rispetto dei criteri fissati dalla giurisprudenza della CGUE e, soprattutto, il divieto di forme di *bulk data retention*. Come il IPT nel suo rinvio pregiudiziale *Privacy International* ha messo in rilievo, il rischio di tale forza 'espansiva' dell'ambito di applicazione della Direttiva *e-Privacy* e dei requisiti determinati dai giudici di Lussemburgo potrebbe essere quello di inficiare in maniera significativa l'efficacia delle misure e degli strumenti volti alla tutela della sicurezza dello Stato e, così facendo, di restringere e comprimere

[13] "Una normativa nazionale che preveda la conservazione di dati implica, necessariamente, in linea di principio, l'esistenza di disposizioni in materia di accesso" (par. 78-81, *Tele2*). Del resto l'ammissione dell'obiettivo ultimo della repressione dei reati diventava fondamentale al fine di comporre le problematiche emerse tra determinazione della corretta base giuridica e valutazione della proporzionalità: in questo senso si sottolineano, nelle Conclusioni relative alla sentenza *DRI*, le considerazioni dell'Avvocato generale nelle quali veniva messa in luce la fragilità del ragionamento della Corte: "la Direttiva 2006/24 non riuscirebbe a superare l'esame di proporzionalità per le stesse ragioni che ne giustificavano il fondamento normativo. I motivi che determinano la sua legittimità dal punto di vista del fondamento normativo sarebbero, paradossalmente, i motivi della sua carenza sotto il profilo della proporzionalità" (par. 102), il che conduceva necessariamente alla valutazione non solo dell'obiettivo preponderante e formale ma anche dell'ulteriore scopo "ultimo" della DRD, individuato appunto nella repressione dei reati gravi.

la possibilità degli Stati membri di garantire interessi, di estrema importanza, quali la sicurezza nazionale e la lotta a grandi minacce tra cui il terrorismo internazionale: in senso opposto rispetto a quanto prima evidenziato, non manca chi ammonisce rispetto al pericolo che i diritti fondamentali vengano impiegati, soprattutto dalla CGUE, quali strumento – se non pretesto – per superare i limiti ed i principi che regolano il rapporto tra Stati membri e Unione europea e il funzionamento di quest'ultima[14].

Emerge quindi dalle serie conseguenze evidenziate, dal significativo impatto che tutte le questioni e approcci rilevati producono, un secondo profilo problematico ed ancora estremamente dibattuto, di natura sostanziale, da individuarsi nella determinazione di un corretto punto di equilibrio, per quanto complesso, tra esigenze securitarie e diritti fondamentali: esso dovrebbe tener conto sia del bisogno degli Stati membri e delle loro autorità di disporre di strumenti utili ed efficienti a garantire la lotta alla criminalità e la sicurezza dello Stato, sia dell'esigenza che, pure in tale contesto, venga rispettato lo Stato di diritto e la tutela effettiva dei diritti riconosciuti nella Carta di Nizza. Ed è proprio con riferimento al dibattito che deriva dalla individuazione di questo complesso punto di equilibrio, che è possibile riscontrare la posizione sicuramente più determinante e rivoluzionaria della CGUE: la dichiarazione di incompatibilità con la Carta di Nizza di una conservazione generalizzata ed indiscriminata. Sebbene la CGUE non giunga a negare la legittimità dello strumento dell'obbligo di conservazione in capo a fornitori di servizi di telecomunicazione, in sé e per sé considerato, essa nondimeno ne limita fortemente la portata e le caratteristiche: affermando con chiarezza, quanto meno nella sentenza *Tele2*, l'incompatibilità con il diritto dell'UE di una forma di *bulk data retention* e della logica sottesa del *'collect-it-all'*, i giudici di Lussemburgo hanno poi trovato nella forma targettizzata, i cui criteri e requisiti sono stati specificati dal giudice stesso, una tipologia di conservazione proporzionata. Come si è visto, la soluzione prospettata, peraltro unicamente dalla CGUE, senza cioè che sia possibile ravvisare nelle posizioni espresse dalle parti intervenute alla controversia *DRI* alcun riferimento a tale opzione, resta oggetto di profonde critiche: non è un caso che EUROPOL abbia presentato la forma alternativa e meno rigida della *restricted data retention*, facendo leva su una lettura più flessibile delle pronunce *DRI* e *Tele2*, con una soluzione che pare peraltro trovare qualche spazio di affermazione anche nelle Conclusioni dell'Avvocato generale Campos Sanchez-Bordona ai rinvii promossi dai giudici francesi, belgi e inglesi; tale tipologia di conservazione mira proprio ad inserire tutele specifiche – quali restrizioni volte ad escludere soggetti coperti da segreto professionale o a limitare le tipologie di dati interessate da conservazione – meno circoscritte rispetto a quelle previste nella *targeted data retention*, forma quest'ultima peraltro ritenuta, oltre che irrealizzabile ed incompatibile con la stessa finalità ed utilità della *data retention*, anche discriminatoria. Nell'ammettere tuttavia che la conservazione targettizzata non deve essere considerata l'unica possibile tipologia ammessa e conforme al diritto dell'UE, resta di determinante importanza rilevare come anche l'Avvocato generale Campos Sanchez-Bordona non si discosti e non proponga alcun temperamento al divieto di *bulk data retention* espresso nella previa giurisprudenza della CGUE: questo, nonostante alcuni Stati membri, come il Belgio, ad esempio, avessero proposto una interpretazione della *data retention saga* e dei principi in essa sanciti basata sulla necessità di non considerare come globalmente obbligatori e da rispettare contemporaneamente tutti i requisiti fissati dalla Corte, così che anche una conservazione generalizzata avrebbe potuto risultare proporzionata laddove mitigata dalla presenza di idonee tutele nella fase dell'accesso o qualora ristretta – non targettizzata – così da non riguardare tutti gli utenti e tutti i mezzi di comunicazione. Nel ritenere una forma di *bulk data retention* per sé, e dunque

[14] "If balancing of competing fundamental rights leads to the result that data protection very often or even mostly prevails, this might seriously impede the efforts of the EU to guarantee security on its territory. (..) It cannot be stressed enough that the EU needs to develop a balanced approach that carefully integrates data protection within the overall system of fundamental rights protection within the EU", M. BRKAN, *The unstoppable expansion of the EU fundamental right to data protection. Little shop of horrors?*, in *Maastricht Journal of European and Comparative Law*, 5, 2016.

per sua stessa natura, incompatibile con la Carta di Nizza, in quanto rappresentativa di una invasione nella sfera privata eccessiva e sproporzionata rispetto a quanto necessario, l'Avvocato generale ha motivato tale conclusione e restrizione intendendola quale "tributo che i poteri pubblici devono pagare quando si impongono l'obbligo di salvaguardare i diritti fondamentali" (par. 102). E a nulla sono valse le rimostranze invocate a gran voce dagli Stati membri, che vedono in tale limitazione una inaccettabile perdita di efficacia dello strumento della *data retention* stessa che, per esprimere tutto il suo potenziale, deve essere generalizzata. A parere dell'Avvocato generale, infatti, "la lotta contro il terrorismo non deve essere impostata solo pensando alla sua efficacia. Da ciò deriva la sua difficoltà, ma anche la sua grandezza quando i suoi mezzi e metodi rispettano i requisiti dello Stato di diritto, che significa anzitutto assoggettamento del potere e della forza ai limiti del diritto e, in particolare, a un ordinamento giuridico che trova nella difesa dei diritti fondamentali la ragione e il fine della sua esistenza" (par. 130)[15]. Queste parole paiono dunque perfettamente riassuntive della posizione e dell'approccio fino ad ora adottato dalla CGUE nelle sue storiche pronunce: nonostante venga riconosciuta la difficoltà di trovare un corretto punto di equilibrio e soluzioni che tutelino i diritti fondamentali senza rinunciare totalmente alle potenzialità positive offerte dalle nuove tecnologie nell'ambito della lotta alla criminalità grave e al terrorismo, la *bulk data retention* viene identificata come esemplificazione evidente dei pericoli gravi che potrebbero derivare dal fornire un potere di sorveglianza troppo ampio ed incontrollato nella mani delle autorità pubbliche, pur impiegando, come tramite, l'operato di soggetti privati[16]. Un controllo sulle comunicazioni dei cittadini, in maniera massiva e generalizzata, per quanto strumento potenzialmente efficace, inciderebbe sul rapporto stesso tra Stato e consociato, sullo Stato di diritto e sulla garanzia dei diritti fondamentali che caratterizzano e qualificano le società democratiche. Da questo orientamento diviene chiaro come neppure la tutela della sicurezza nazionale e la garanzia dell'efficacia degli strumenti volti ad assicurarla, sebbene ritenuti interessi di estremo rilievo[17], possano giustificare, salvo occasioni estremamente eccezionali e circoscritte, una invasione significativa nella sfera privata e, più in generale, nei diritti fondamentali riconosciuti quale quella determinata da una conservazione generalizzata.

In conclusione, se si vuole trarre un primo benché provvisorio bilancio dell'approccio della CGUE e riflettere sui possibili sviluppi futuri, bisogna certamente partire con l'affermare che le pronunce dei giudici di Lussemburgo hanno il merito di aver innalzato il livello di tutela imposto all'interno dell'UE – e anche nella dimensione esterna – e di aver incentivato un serio dibattito e riflessione negli Stati membri: sebbene ciò non valga per tutti – e l'Italia purtroppo è di ciò testimone – e benché, va subito sottolineato, la maggioranza degli Stati membri abbiano rinunciato alla conservazione generalizzata,

[15] Così l'Avvocato generale Campos Sanchez-Bordona: "L'efficacia del potere pubblico, ripeto, trova una barriera insuperabile nei diritti fondamentali dei cittadini" (par. 131-132); "Seppur difficile, non è impossibile determinare con precisione e sulla base di criteri oggettivi sia le categorie di dati la cui conservazione è considerata imprescindibile, sia la cerchia degli interessati. Certamente la soluzione più pratica ed efficace sarebbe la conservazione generale e indifferenziata di tutti i dati che possono essere raccolti dai fornitori di servizi di comunicazione elettronica, ma ho già rilevato che la questione non può essere risolta in termini di efficacia pratica, bensì di efficacia giuridica e nel contesto di uno Stato di diritto", par. 135, Conclusioni al rinvio cause riunite C-511/18 e C-512/18, *French Data Network, La Quadrature du Net e al. c. Premier ministre, Garde des Sceaux, Ministre de la Justice*.

[16] Del resto, come ritenuto da Fabbrini, "if direct government control over the personal metadata of every citizen may be reminiscent of George Orwell's 1984, the retention of data by private companies is also liable of interfere with the private life of citizens", F. FABBRINI, *Human rights in the digital age: the European Court of Justice ruling in the Data Retention Case and its lessons for privacy and surveillance in the United States*, in *Harvard Human Rights Journal*, 28, 2015.

[17] Basti pensare alle parole dell'Avvocato generale Campos Sanchez-Bordona che nelle Conclusioni al rinvio promosso dal Consiglio di Stato francese ha affermato come la lotta al terrorismo sia "letteralmente vitale per lo Stato e il suo successo costituisce un obiettivo di interesse generale irrinunciabile per uno Stato di diritto", par. 128, ritenendo la sicurezza come "consustanziale alla stessa esistenza e sopravvivenza di una democrazia, il che giustifica il fatto che se ne tenga pienamente conto nell'ambito della valutazione della proporzionalità", par. 102.

mantenendo ferme quelle critiche e promuovendo quelle diverse e più flessibili interpretazioni che sono state sopra evidenziate, si è sicuramente registrata nelle normative nazionali adottate sulla base dell'art. 15 Direttiva *e-Privacy* una maggiore attenzione alle salvaguardie, tutele e limiti predisposti dalla giurisprudenza della CGUE, soprattutto nella fase di accesso (sul punto si vedrà poi più ampiamente il Par. 3). Questo effetto e *trend* positivo potrebbe trovare conferma qualora la CGUE riaffermasse i medesimi criteri e requisiti fissati nelle previe sentenze anche nelle decisioni che ha di recente pronunciato nell'ottobre 2020, relative ai rinvii pregiudiziali già ampiamente esaminati, ma che non sono state in questa sede oggetto di studio, nonché nei rinvii ancora pendenti, quali quelli promossi dalla Suprema Corte estone e da quella irlandese o ancora i rinvii aventi ad oggetto la Direttiva PNR. Queste attese sentenze dunque risulteranno di grande importanza per determinare il futuro della *data retention* nell'UE.

Sebbene non si voglia porre in discussione l'impatto positivo sopra riscontrato, non possono essere dimenticati o ignorati gli aspetti problematici e critici che ancora caratterizzano la posizione della CGUE e che già sono stati messi in rilievo: sotto questo profilo e con riferimento alle future prospettive, a parere di chi scrive risulta piuttosto improbabile che nella risoluzione dei rinvii pendenti i giudici di Lussemburgo possano chiarire i rilevati punti problematici e di fragilità e che possa così essere fissato un punto finale, definitivo e facilmente perseguibile ed attuabile alla complessa e profonda sfida cui UE e Stati membri sono chiamati da tempo ormai a fornire risposta.

Qualora la CGUE confermasse l'orientamento sino ad ora seguito e basato sulla incompatibilità di forme di *bulk data retention* e sulla legittimità della sola conservazione targettizzata, la situazione che si verrebbe a creare potrebbe, sotto tale profilo, continuare ad essere problematica e di non facile immediato superamento: la forte divergenza tra tale posizione della CGUE e quella degli Stati, che non paiono disposti a rinunciare allo strumento, considerato essenziale, della *bulk data retention*, potrebbe portare ad alcune resistenze e al procrastinarsi di una frammentarietà di soluzioni – evidenziate soprattutto nell'analisi comparata –, insieme al rinnovato tentativo da parte degli Stati membri stessi di promuovere interpretazioni che permettano loro un maggior margine di azione e dunque, almeno sulla base della posizione espressa da questi ultimi, anche una accresciuta efficacia dello strumento della conservazione. Inoltre, proprio alla luce di una ribadita incompatibilità della *bulk data retention*, potrebbe farsi più reale e concreta la rischiosa tendenza degli Stati di puntare maggiormente la propria attenzione su forme di sorveglianza diretta poste in essere da parte delle autorità di intelligence o di *law enforcement*, senza cioè l'intermediazione di soggetti privati – che riporterebbero altrimenti le operazioni all'ambito di applicazione del diritto dell'UE –, in questo modo aggirando gli ostacoli e gli stringenti requisiti imposti dalla CGUE[18].

Ne consegue che, con riferimento ai dubbi sopra rilevati e divenuti piuttosto problematici, divenga quanto mai necessario e di cruciale importanza la capacità dei giudici di Lussemburgo di adottare nelle future sentenze decisioni chiare e puntuali, capaci di rispondere e risolvere quelle criticità, quelle zone grigie e quelle perplessità che i tanti giudici del rinvio a seguito della *Tele2* hanno ben evidenziato: nei rinvii aventi ad oggetto la Direttiva PNR, ad esempio, sembra necessario che la CGUE chiarisca con puntualità la portata delle sue affermazioni circa i sistemi di trasferimento di dati da soggetti privati ad autorità pubbliche che prevedano un vaglio automatizzato e preventivo delle informazioni ottenute, sulla

[18] Un ulteriore pericolo, rilevato da Verbruggen, Royer e Severijns, è individuato nel rischio che "an EU-law taboo on a general data retention will also increase the dependence of intelligence agencies, especially those of small countries like Belgium, on information of foreign services that might not (or no longer) be bound by EU law or choose not to abide by it, for instance US, post-Brexit-UK or Israeli services which are important partners in the fight against terrorism and the so-called foreign fighters. Again, even if the human rights and accountability concerns behind the outright banning of blanket data retention are sincere, the remedy might be worse than the illness", F. VERBRUGGEN, S. ROYER, H. SEVERIJNS, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, in *European Law Blog*, 1 ottobre 2018, http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/.

base di criteri predeterminati e l'impiego di tecniche di lettura aggregata e confronto con quanto rilevato in altre banche dati, quali quelli appunto in materia di codici di prenotazione dei passeggeri (PNR), mettendo in luce anche il rapporto tra tale posizione e quanto invece determinato in materia di *data retention* attinente ai metadati, rispetto ai quali criteri ben più stringenti e limitativi sono stati stabiliti, seppur in parte motivati dalle diverse caratteristiche dei due sistemi di conservazione dei dati. Particolare attenzione dovrebbe essere prestata a questioni rimaste ad oggi ancora troppo poco affrontate, come la determinazione dei criteri che determinano la gravità del reato, che non aveva trovato risposta nella sentenza *Ministerio Fiscal*, o una più chiara determinazione di cosa debba intendersi lesivo del nucleo essenziale dei diritti fondamentali alla privacy e alla protezione dei dati, punto anch'esso piuttosto dibattuto in quanto basato sulla distinzione, ormai ritenuta superata, tra metadati e contenuto delle comunicazioni. Infine la Corte dovrebbe meglio considerare quelle criticità e rilievi pratici, evidenziati invero da tanti Stati membri, che derivano proprio dalla fissazione di criteri e limiti alla *data retention*: ad esempio, sulla base di quel binomio gravità dell'ingerenza-gravità del reato, risulta poco chiaro come sia possibile conciliare la legittimità e proporzionalità di un accesso, anche per finalità di lotta a reati non gravi, a talune tipologie di metadati o in modalità tali che l'ingerenza nella sfera privata non possa da considerarsi grave, con il fatto che tale accesso, sulla base di quanto affermato nella *Tele2*, deve comunque fondarsi sui dati conservati mediante una *data retention* targettizzata e in grado di stabilire una connessione anche indiretta con atti di criminalità grave (par. 111, *Tele2*). Questi profili ancora poco chiari e precisi, insieme alla tensione, ormai assodata, degli Stati membri di fornire interpretazioni più flessibili volte a far salva una forma di *bulk data retention*, potrebbero portare, anche dinnanzi al riaffermarsi netto della incompatibilità di una conservazione generalizzata, al persistere di incertezze e problematiche applicative che renderanno ancora non definita la questione, così da risultare nella probabile riproposizione di rinvii pregiudiziali sui punti rispetto ai quali permarranno dubbi interpretativi.

Una possibile soluzione, che potrebbe rendere meno necessario e gravoso l'intervento della CGUE, può certamente essere identificata nella adozione di una normativa a livello europeo che fissi criteri, limiti e requisiti quanto all'impiego dello strumento della conservazione dei dati. É infatti condivisibile l'affermazione secondo cui siano state proprio l'assenza e l'inerzia del legislatore, insieme alla obsolescenza e alla ampiezza della normativa in vigore, ovvero dell'art. 15 Direttiva *e-Privacy*, ad indurre "la Corte di Giustizia a compiere sforzi ulteriori, valorizzando il patrimonio della Carta"[19]. Sebbene fosse atteso e soprattutto auspicato[20] un intervento del legislatore dell'UE già a seguito del vuoto lasciato dalla invalidazione della DRD, ad oggi nulla o molto poco si è ancora registrato: sicuramente fissare mediante una precisa normativa le condizioni e i confini di una disciplina così delicata avrebbe imposto ed impone sforzi notevoli, volti a trovare un punto di incontro e condivisione tra le spinte degli Stati membri nella direzione di un più ampio uso dello strumento e la posizione della CGUE, sostenuta da Autorità garanti nazionali, ONG e talune Corti nazionali, protesa verso una più attenta tutela dei diritti alla riservatezza e protezione dei dati. La sfida notevole che il legislatore avrebbe dovuto e dovrebbe affrontare è quella di adottare una normativa che sia da un lato accettata dagli Stati, rispettosa del principio di attribuzione e capace di considerare le indubbie esigenze securitarie, e

[19] M. BASSINI, *La Corte di giustizia e la conservazione dei dati. Spunti di una rilettura 'postuma'*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, in corso di pubblicazione.

[20] All'indomani della sntenza *DRI* era stato auspicato un nuovo intervento normativo europeo che armonizzasse le misure nazionali in questo ambito, seguendo i parametri indicati dalla CGUE: "an EU instrument that harmonizes *data retention* regimes and thus indirectly ensures comparable data protection standards within the region would be the most appropriate solution to balance potentially conflicting interest: enhancing security and safeguarding data privacy rights", F. GALLI, *Digital Rights Ireland as on opportunity to foster a desirable approximation of data retention provisions,* in *Maastricht Journal of European and Comparative Law*, 3, 2016. Questo auspicio è stato sinora disatteso e pare continuerà ad esserlo.

dall'altro risulti anche conforme alla Carta di Nizza e dunque in grado di superare indenne il vaglio della CGUE. Del resto, "la giurisprudenza della CGUE e delle Corti nazionali dimostrano come la *data retention* rappresenti un istituto davvero magmatico e in perenne evoluzione, il quale abbisogna di un urgente intervento normativo da parte del legislatore UE"[21]. L'ampio numero di continui rinvii sottoposti ai giudici di Lussemburgo evidenzia certamente la difficoltà dei legislatori e giudici nazionali di trovare da soli soluzioni e risposte chiare e conformi al diritto dell'UE – salvo il caso in cui, come in Italia, non ci si pongano le domande corrette – e denota altresì, di riflesso, una certa difficoltà della CGUE stessa nel riuscire a definire e chiarire una questione che, proprio per la sua delicatezza e per la molteplicità di aspetti e di considerazioni che comporta, non dovrebbe essere lasciata – o quantomeno non unicamente – nelle mani dei giudici, cui viene *de facto* affidato, in questo caso, un compito suppletivo dell'inerzia del legislatore[22].

Ecco quindi che in questa *impasse* emerge tutta la complessità della materia analizzata in questo lavoro e la difficoltà di un dialogo proficuo, sia tra Stati membri ed UE, sia tra Istituzioni dell'UE stessa, in grado di trovare un equilibro definitivo e un punto di arrivo: se da un lato la Corte, nell'immobilismo del legislatore europeo, ha adottato un atteggiamento proattivo, contribuendo a "rafforzare la tenuta della *rule of law* lì dove la serietà della minaccia e le potenzialità dei mezzi rischierebbero di far arretrare le conquiste di civiltà che innervano la cultura giuridica europea"[23], ottenendo sicuramente effetti positivi, riscontrabili in un innalzamento del livello di tutela dei diritti fondamentali che difficilmente sarebbe stato altrimenti ottenuto, dall'altro i principi da essa affermati risultano ancora critici da applicare e dai confini talvolta incerti, scontrandosi anche con i limiti stessi dell'architettura della giurisdizione europea e del funzionamento della Corte che non può andare oltre quanto richiesto e quanto indicato dai giudici del rinvio, talvolta quindi dovendo limitare il proprio intervento e la portata chiarificatrice della propria giurisprudenza. Agendo sulle singole questioni sottoposte, i giudici di Lussemburgo a volte faticano a fornire condizioni chiare, dovendosi districare tra la garanzia dei diritti fondamentali, i limiti delle competenze dell'Unione e dell'ambito di azione degli Stati membri nonché del ruolo giurisdizionale che non può – e non dovrebbe – sostituirsi al legislatore tanto nazionale quanto europeo. Mentre quest'ultimo con la DRD si era mostrato "paladino della sicurezza", adottando una normativa più improntata alla efficienza dello strumento di lotta alla criminalità, per poi silenziarsi a seguito del primo intervento dei giudici di Lussemburgo in materia, la CGUE invece si è posta con le sue decisioni quale "guardiano delle libertà"[24] e dei diritti della Carta di Nizza, "[providing] the grounds to confirm and steadily expand the scope of application of EU fundamental rights to the Member States and thereby the jurisdiction of the CJEU itself for the interpretation of those rights"[25]. Così facendo però, sebbene abbia senza dubbio ottenuto il grande risultato di aver accresciuto e promosse un profondo dibattito sulla materia, l'approccio e le valutazioni rigorose di cui è stata espressione, tra cui quella di dichiarare l'incompatibilità alla Carta di Nizza della *bulk data retention*, hanno aperto sicuramente a

[21] L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019.

[22] Pare esemplificativo di tale atteggiamento la decisione del Parlamento europeo di rimettere nelle mani della CGUE la valutazione preventiva della conformità al diritto dell'UE della bozza di accordo in materia di trasferimento dei PNR negoziato con il Canada. Questa scelta, seppure da taluni ritenuta 'responsabile' e frutto della consapevolezza della complessità della materia, è stata da altri considerata una soluzione 'di comodo', che ha cioè permesso al Parlamento di scaricare la responsabilità di una decisione così delicata in capo alla CGUE.

[23] E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, in *IANUS*, 15, 2017.

[24] G. DE MINICO, *La risposta europea al terrorismo del tempo ordinario: il lawmaker e il giudice*, in *Osservatorio sulle fonti*, 2, 2017, p. 17. L'autrice sottolinea come, con riferimento a questa disciplina, il danno certo ed attuale determinato dall'ingerenza nella vita privata sia stato ritenuto maggiormente determinante rispetto al presunto e solo eventuale vantaggio futuro che il sistema di conservazione dei dati generalizzata può rappresentare.

[25] A. TORREZ PEREZ, *The federalizing force of the EU Charter of Fundamental Rights*, in *International journal of constitutional law*, 4, 2017.

problematiche complesse[26] che attengono, come si è visto, a svariati profili, tutti di grande rilievo ed estremamente ampi, andando dal rapporto tra le Istituzioni dell'UE, al ruolo attribuito alla CGUE, dal rapporto con gli Stati membri, alle difficoltà applicative, alle zone grigie e aperte a diverse interpretazioni, alla frammentarietà delle soluzioni legislative riscontrate a livello nazionale, allo scontro con posizioni che ritengono troppo proteso a sfavore della garanzia della sicurezza l'approccio della CGUE, alla determinazione chiara dell'ambito di applicazione del diritto dell'UE, così che un punto di equilibrio definitivo, nonostante tutte gli avanzamenti e i progressi svolti, pare ancora non poter essere affermato.

2. L'Unione europea come "fortezza della privacy" anche nella dimensione esterna: la disciplina in materia di **data retention** *e di trasferimento dati verso Stati terzi come mezzo per promuovere un più elevato standard globale di tutela della privacy e della protezione dei dati*

Il secondo ordine di considerazioni, come anticipato, vuole muovere principalmente dall'analisi svolta nel Capitolo III, Parte II, nella quale sono state messe in luce le scelte normative nonché le vicende giurisprudenziali in materia di trasferimento di dati verso Stati terzi. Ebbene dalla disamina effettuata discendono almeno due differenti riflessioni, strettamente connesse tra loro: la prima intende evidenziare l'impatto dell'approccio dell'UE nella dimensione esterna e le implicazioni rispetto al rapporto con gli Stati terzi, fino a delineare un provvisorio bilancio che da tale particolare posizione può essere dedotto circa il ruolo dell'UE nel contesto globale; la seconda riflessione invece si propone di rimarcare l'incidenza che le pronunce della CGUE e i principi da essa affermati con riferimento alla dimensione esterna dell'azione dell'UE possono comportare entro i confini europei e, in particolare, in quella determinazione del rapporto tra esigenze securitarie e diritti fondamentali esemplificata nello specifico contesto della disciplina della *data retention*.

Partendo dal primo profilo, dall'articolato e composito studio delle luci ed ombre che hanno caratterizzato l'azione esterna dell'UE in materia di tutela della riservatezza e protezione dei dati, emerge come una valutazione definitiva in termini di efficacia ed opportunità dell'approccio dell'UE nell'ambito del trasferimento dei dati assuma caratteri di grande complessità: da un lato infatti l'adozione di accordi e decisioni di adeguatezza risulta lo strumento necessario ed appropriato per una effettiva salvaguardia dei diritti fondamentali sanciti agli artt. 7 e 8 della Carta di Nizza anche nella dimensione esterna all'UE[27]. Tale visione si basa correttamente, a parere di chi scrive, sull'assunto secondo cui la cooperazione tra Stati (in questo caso tra UE e Stati terzi) risulta ormai l'unica arma per combattere le sfide di un mondo globalizzato e 'datizzato' che impone di trascendere i classici concetti di territorialità e sovranità territoriale e che determina quindi l'esigenza di una protezione dei dati che sappia andare anche oltre i confini nazionali[28]. Dall'altro lato tuttavia non può che notarsi come

[26] Non a caso, a seguito della pronuncia *DRI*, Tiberi scriveva come la sentenza potesse "essere vista come una «cartina di tornasole» delle molte questioni che si agitano nell'attuale sistema di protezione dei diritti fondamentali in Europa dopo l'avvento di quella «nuova era dei diritti» che il Trattato di Lisbona ha inaugurato", G. TIBERI, *La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel "dopo-Lisbona"*, in *Quaderni costituzionali*, 3, 2014, p. 720.

[27] D. COLE, F. FABBRINI, *Bridging the transatlantic divide? The United States, The European Union and the protection of privacy across borders*, in *International journal of constitutional law*, 1, 2016.

[28] Per Cole e Fabbrini, la sentenza *Schrems* ha avuto il merito di rendere "the case for a comprehensive transatlantic privacy compact all the more compelling", D. COLE, F. FABBRINI, *Bridging the transatlantic divide? The United States, The European Union and the protection of privacy across borders*, in *International journal of constitutional law*, op. cit. Sul punto si legga anche G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016, che evidenzia come nel caso *Schrems* ciò che esce

l'approccio adottato dall'Unione, basato su lunghe e difficili negoziazioni con Stati terzi e sul raggiungimento di accordi (o bozze di accordi) su cui poi fondare decisioni di adeguatezza, abbia rivelato tutta la sua debolezza alla prova della Corte, dimostrando di essere uno strumento facilmente sbilanciato a favore della garanzia della sicurezza ed inidoneo a tutelare, anche nella dimensione esterna dell'UE, l'elevato livello di protezione promosso entro i confini europei[29]. In altre parole, sia nella sentenza *Schrems* sia nel *Parere 1/15*, i giudici di Lussemburgo hanno evidenziato come il punto di equilibrio tra garanzia dei diritti fondamentali ed esigenze securitarie trovato a seguito di cooperazione e intenso dibattito con Stati terzi non rispecchiasse coerentemente ed in maniera sostanzialmente equivalente gli standard di protezione garantiti entro i confini europei, rivelandosi dunque frutto di un 'compromesso al ribasso' necessario per la conclusione dell'accordo ma a discapito di un più alto livello di garanzia dei diritti.

L'intervento 'destabilizzatore' della CGUE, mettendo in luce le potenziali esternalità negative delle decisioni di adeguatezza, è risultato essere anch'esso, al pari dello strumento giudicato, una pericolosa e delicata arma a doppio taglio, capace di mettere in discussione il risultato di complessi accordi nonché la stessa stabilità delle relazioni internazionali con il Paese terzo; quest'ultimo infatti ben potrebbe rifiutarsi di sedere nuovamente al tavolo delle negoziazioni o negare la propria disponibilità ad accettare un più alto standard di protezione dei dati, magari molto distante da quello garantito dal proprio ordinamento e differente rispetto a quello originariamente 'contrattato' negli accordi con l'UE propedeutici alla decisione di adeguatezza e invalidati dall'azione della CGUE. Le conseguenze potenziali, in tal caso, sarebbero estremamente rischiose, poiché metterebbero in pericolo la continuità del flusso transfrontaliero di dati, con serie ripercussioni anche sul piano economico, oltre che su quello della tutela dei diritti fondamentali. Dinnanzi a questo scenario diviene quindi lecito chiedersi se la conclusione di un accordo, anche imperfetto, ovvero con un livello di tutela non del tutto adeguato rispetto a quello dell'UE, non sia comunque da ritenersi preferibile e maggiormente accettabile rispetto alla totale assenza di qualsiasi accordo e dunque di qualunque salvaguardia: se si muove da tale premessa, si può giungere alla conclusione secondo cui un intervento eccessivamente rigido dei giudici di Lussemburgo potrebbe in realtà condurre, pur nell'obiettivo di innalzare il livello di tutela e scongiurare una negoziazione al ribasso, ad un esito inverso[30].

Nonostante tali possibili – ed invero realizzatisi – effetti negativi che impongono una seria riflessione tanto sullo strumento disposto dalla normativa europea quanto sulla posizione ed interpretazione della CGUE, risultano parimenti innegabili gli effetti positivi, prodotti e da riconoscersi in una capacità delle Istituzioni dell'UE di influenzare gli standard di tutela di Stati terzi, di stabilire condizioni che generalmente innalzano il livello di protezione riconosciuto nello Stato terzo stesso e di porre

rafforzata è l'extraterritorialità della normativa europea, come risposta ad un contesto che mette in discussione il significato di 'territorialità' stessa.

[29] "Such agreements, far from strengthening privacy protection, would almost certainly weaken it. Even among Western democracies, the search for transnational common ground and the institutional priorities of the negotiators would be inimical to a privacy-protective accord", S. J. SCHULHOFER, *An international right to privacy? Be careful what you wish for*, ICON, 1, 2016, p. 238. Ciò induce l'autore a chiedersi, in ultima analisi, se quella di una negoziazione tra Stati per il raggiungimento di accordi in materia di protezione dei dati e di tutela della privacy sia una soluzione, alla luce delle vicende giudiziarie europee, da considerarsi ancora percorribile ed idonea a raggiungere il reale obiettivo ultimo della adeguatezza della tutela offerta dallo Stato terzo.

[30] In mancanza di un punto di equilibrio tra questi due poli opposti e nella impossibilità di creare un dialogo proficuo con lo Stato terzo ricevente i dati, si andrebbe a generare un vuoto regolatorio, come accaduto nel caso del trasferimento dati PNR verso il Canada ma più ampiamente anche a seguito della decisione *Schrems* (pur essendo presenti in quel caso soluzioni alternative volte a garantire il flusso di dati). Tale situazione di 'stallo' e di indeterminatezza, anche in termini temporali – considerando la lunghezza ed imprevedibilità dei negoziati nonché l'incertezza circa il raggiungimento di un nuovo accordo – espone pertanto i dati degli utenti o dei passeggeri europei a seri rischi in termini di garanzie e tutele.

all'attenzione di questi ultimi problematiche e possibili soluzioni virtuose ai rischi e alle minacce per la privacy e *data protection*[31].

Se dunque un bilancio netto e chiaro sui pro e contro dell'approccio dell'UE in tale ambito è piuttosto difficile da stabilire, bisogna notare comunque come gli effetti sopra menzionati di promozione e spinta ad un più alto standard di garanzia dei diritti fondamentali nello Stato ricevente siano limitati nella maggior parte dei casi alla sola dimensione 'bilaterale' degli accordi: dinnanzi a questo limite vi è chi, riconoscendo che "It is challenging to address concerns about mass surveillance at a national level, and it is even more challenging to do so at the transatlantic, regional or global level. Yet it is precisely at these levels, and especially at the global level where meaningful legal response to strengthen privacy in the face of surveillance is urgently needed"[32], individua una possibile soluzione alla dimensione globale della sfida nell'adozione di un trattato internazionale multilaterale che fissi standard di protezione non solo tra due singole parti ma coinvolgenti l'intera – o quanto meno gran parte della – comunità internazionale. Certamente le difficoltà e rimostranze avverso un percorso di 'internazionalizzazione' della protezione dei dati e della riservatezza[33] sono molteplici, visti i differenti approcci che caratterizzano i vari ordinamenti, anche solo nei Paesi Occidentali, motivati dalle diverse storie e percorsi evolutivi che hanno portato, in maniera e misura differenti, all'affermazione e riconoscimento dei due diritti richiamati nonché al bilanciamento e al valore che ad essi viene attribuito. Dinnanzi a tali significativi ostacoli nella direzione di un approccio globale al problema, che rendono almeno al momento piuttosto improbabile una soluzione di questo tipo, senza dubbio altre opzioni più moderate e circoscritte possono essere individuate: nel campo dei PNR, ad esempio, come sembra suggerire l'UE stessa, "a possible and more cautious way forward could therefore be to elevate the recommended practice to align with the ICAO PNR guidelines contained in Annex 9 to the Chicago Convention to a 'standard' status and updating the latter with a view to setting clearer parameters on the issues of privacy and data protection, having regard to the most recent developments in both EU and domestic practice"[34].

---

[31] In risposta alla visione di Schulhofer, sopra richiamata nella nota 29 e critica rispetto alla opportunità ed utilità della adozione di accordi internazionali, Cole e Fabbrini rispondono: "Transatlantic negotiations are necessary to protect transatlantic rights. The concerns Schulhofer raises, while sound, are not a reason to reject such negotiations. Some of the concerns he has at the transatlantic level are equally present at the domestic level, and Schulhofer has not shown that the dynamics he predicts (a race to the bottom, or the watering down of domestic standards to meet transnational standards) are inevitable. Most importantly, because current domestic law in both the EU and the US provides no meaningful protection to foreign nationals from crossborder surveillance, and safeguards are unlikely to expand unilaterally on this front in the future, there is little or no downside, and considerable upside, to a transatlantic effort to address this concern", D. COLE, F. FABBRINI, *Transatlantic Negotiations for Transatlantic Rights: Why an EU-US Agreement is the Best Option for Protecting Privacy Against Crossborder Surveillance*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, 2017, p. 212.

[32] S. MITSILEGAS, *Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime*, in *Columbia human rights law review*, 3, 2016. Dello stesso avviso anche K. LACHMAYER, *Rethinking Privacy Across Borders: Developing Transnational Rights on Data Privacy*, in *Tilburg Law Review*, 20, 2015. Non a caso anche a livello delle Nazioni Unite è stata sentita l'esigenza di promuovere risposte di carattere internazionale, con l'adozione di una risoluzione sul "Right to privacy in a digital age" e la creazione della figura di un "UN Special Rapporteur on the right to privacy in a digital age", nella consapevolezza che soluzioni condivise sul piano globale possono rappresentare una possibile soluzione alle disparità degli standard di protezione e un antidoto ai rischi che sistemi statali di sorveglianza sempre più estesi possono porre rispetto non solo ai propri cittadini ma anche – e soprattutto – a quelli di Stati terzi.

[33] Ciò risulta chiaro se si riconoscono le criticità e gli ostacoli, già ben evidenziati, che caratterizzano il raggiungimento di accordi bilaterali: del resto, come rileva Vermeulen, "Apparently the demand for a genuine commitment to stop bulk collection of personal data was a political bridge too far", G. VERMEULEN, *The paper shield: on the degree of protection of the EU-US Privacy Shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services*, in D. SVANTESSON, D. KOLZA (a cura di) *Transatlantic data privacy relationship: as a challenge for democracy*, Cambridge University Press, 2017, p. 6.

[34] E. CARPANELLI, N. LAZZERINI, *PNR: problems not resolved? The EU PNR conundrum, after Opinion 1/15 of the CJEU*, in *Air and Space Law*, 42, 2017, p. 402. Si legga anche O. J. GSTREIN, *Mapping power and jurisdiction*

Al di là di queste riflessioni di più ampio respiro – che risultano comunque di fondamentale importanza e che assumeranno sicuramente forte rilievo in futuro, man a mano che la consapevolezza circa la necessità di fissare uno standard di tutele si farà largo nei diversi Stati maggiormente influenti nel panorama internazionale – e volendo tornare al piano europeo, risulta chiaro come l'Unione, anche e soprattutto mediante la giurisprudenza della sua Corte, si stia sempre più affermando nella dimensione esterna al proprio territorio come *supranational data protector*[35], facendo emergere la propria vocazione di attore globale. Nonostante i possibili effetti 'collaterali' derivanti da tale approccio, l'Unione europea ha cercato e sta cercando di "contributing to the process of "standards' globalization"[36], così che la disciplina dell'adeguatezza può essere identificata più come "uno strumento per rafforzare la leadership dell'Unione nell'intento di definire le future linee globali in materia di protezione dei dati, piuttosto che una reale garanzia di un più elevato ed efficace livello di protezione dei dati trasferiti verso Paesi terzi"[37].

In questo contesto è innegabile il ruolo preponderante e propulsivo – anche se talvolta destabilizzante – dei giudici di Lussemburgo che, tramite il filone giurisprudenziale inaugurato con la pronuncia *DRI*, hanno affermato con forza quel già richiamato approccio "eurocentrico" ai diritti alla riservatezza e alla protezione dei dati che si riflette anche nei rapporti internazionali, come appare chiaro dalle decisioni *Schrems* e *Parere 1/15*. Come da alcuni sostenuto, la Corte coglie l'opportunità, nel confrontarsi con il tema del trasferimento dati verso Stati terzi, soprattutto nella fase post-Snowden e in un clima recettivo e attento alle problematiche in materia di privacy, non solo di "reinvent itself as a main defender of the fundamental right to data privacy in EU and transatlantic relations"[38], ma anche di mandare un messaggio forte alle altre Istituzioni europee, rimarcando il bisogno di ancorare le decisioni in materia di *data transfer* e adeguatezza al rispetto dei diritti fondamentali dell'UE[39].

---

on the Internet through the lens of government-led surveillance, in *Internet Policy Review*, 3, 2020, che ha affermato come "the lack of common understanding of concepts makes global regulation unlikely" e forse anche indesiderata visto il rischio che il livello di tutela che potrebbe essere garantito in un ambito così vasto e che deve tenere conto di standard di protezione molto differenti, risulterebbe molto probabilmente una 'protezione al ribasso' rispetto al livello garantito nell'UE. L'autore però suggerisce, come alternativa tra un approccio globale ed uno solo locale (interno all'UE), una via intermedia individuata nei 'blocs of trust' raggiungibili mediante convenzioni internazionali.

[35] La giurisprudenza della Corte sembra dunque "redraw the Union's role as a data protector rather than a data collector", così A. VEDASCHI, G. M. NOBERASCO, *From DRD to PNR: looking for a new balance between privacy and security*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and trans-Atlantic relations*, Bloomsbury, 2015, p. 87. Non è però da ignorare, come già sottolineato, che accanto a posizioni che vedono con estremo favore lo scrutinio operato dalla Corte, non manca chi vi ravvisa invece un effetto distorsivo che porta a ritenere la privacy come un "super fundamental right that reigns supreme above all other rights", D. SARMIENTO, *What Schrems, Delvigne and Celaj tell us about the state of fundamental rights in the EU*, in *Verfassungsblog*, 16 ottobre 2015.

[36] T. KONSTADINIDES, *The rule of law in the European Union: the internal dimension*, Hart Publishing, 2017, p. 64.

[37] A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, RomaTrE-Press, 2016, p. 268.

[38] M. ZALNIERIUTE, *Developing a European standard for international data transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *The modern law review*, 6, 2018, p. 1056. Sul punto si legga anche V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di comunicazione*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016, p. 7.

[39] S. CARRERA, E. GUILD, *Safe Harbour or into the Storm? EU-US Data transfer after Schrems Judgement*, in *CEPD Liberty and Security in Europe Papers*, novembre 2015, https://www.ceps.eu/system/files/CEPS_LSE_85.pdf, p. 5. Non mancano tuttavia, come già analizzato, posizioni critiche rispetto a questo ruolo della Corte: si legga Falletta, secondo cui "la scelta della Corte di Lussemburgo di intervenire a piedi uniti sul Safe Harbour sia riconducibile a ragioni tanto di politica legislativa, quanto di politica in senso stretto"; i fattori che i giudici considerano sono volti da un lato ad anticipare la sostituzione di una Direttiva, la 95/46, ormai obsoleta, e dall'altro a rispondere all'esigenza di rafforzare il ruolo della Commissione nelle fasi di trattative e nuove negoziazioni con gli USA, cercando inoltre di porre rimedio al "basso livello di

Se dunque l'azione dell'UE nella dimensione esterna della tutela dei dati può essere, in parte, letta come un tentativo dell'Unione stessa di adempiere concretamente a quel 'principio missionario' (Art. 3, co. 5, TUE) di espansione dei propri valori e principi, promuovendo oltre i confini europei una convergenza regolatoria verso alti livelli di protezione dei dati e garanzia della riservatezza[40], non è ancora chiaro l'esito concreto di un tale approccio: molto dipenderà da un lato dalla coerenza dell'operato e delle scelte di tutte le Istituzioni europee e degli Stati membri, non solo sotto il profilo della disciplina del trasferimento dei dati bensì anche – e primariamente – sul fronte interno, fondamentale per creare una efficace e credibile azione esterna; dall'altro dalla capacità della Corte, nei casi di fronte ad essa pendenti e dai risvolti fortemente complessi e delicati, di chiarire i dubbi e le zone grigie ancora presenti nelle proprie decisioni, per permettere una interpretazione del diritto dell'UE e della Carta di Nizza che sia il più possibile univoca e definita nonché coerente e bilanciata, capace di scongiurare da un lato il rischio di risultare troppo a favore delle esigenze securitarie e, nella dimensione esterna, di scendere a compromessi al ribasso pur di raggiungere accordi e garantire il flusso di dati, e dall'altro lato evitando il pericolo di essere troppo sbilanciata nella direzione della garanzia dei diritti fondamentali, a discapito di una reale e concreta accettabilità, attuazione e fattibilità delle soluzioni proposte.

Sotto il profilo, infine, del rapporto tra principi riconosciuti ed affermati sul fronte esterno e quelli stabiliti nella analizzata giurisprudenza in materia di *data retention* entro i confini dell'UE, ciò che alcuni autori hanno rilevato è il rischio concreto di un atteggiamento 'ipocrita'[41] delle Istituzioni europee, che potrebbero finire con l'imporre e pretendere nelle relazioni con Stati terzi livelli di tutela che non sono però spesso rispettati e garantiti efficacemente e concretamente nel contesto interno all'Unione stessa[42]. Ciò potrebbe venirsi a determinare qualora la CGUE, nei rinvii pregiudiziali da poco risolti e non ancora esaminati, ritenesse misure di conservazione dei dati imposte in capo ad operatori privati per scopi di garanzia della sicurezza nazionale come non rientranti nell'ambito di applicazione dell'UE: in quel caso si verrebbe a creare la – quasi paradossale – situazione in cui gli standard elevati previsti dalla giurisprudenza della CGUE non sarebbero applicabili alle operazioni richiamate e poste in essere dagli Stati membri, mentre il rispetto di tale livello di garanzia potrebbe essere richiesto quale condizione determinante l'adeguatezza dello Stato terzo ai fini di approvare e garantire il trasferimento di dati. Sebbene questa opzione, dipendente dalla posizione che la CGUE ha recentemente espresso nel caso *Privacy International*, paia, anche alla luce delle Conclusioni dell'Avvocato generale, piuttosto improbabile, è da sottolinearsi come potrebbe comunque risultare delicato e problematico anche il caso in cui i giudici di Lussemburgo decidessero di optare per l'esclusione dall'ambito di applicazione del diritto dell'UE delle sole operazioni di raccolta e conservazione diretta, cioè poste in essere dalle autorità

coscienza dei cittadini europei rispetto alle proprie attività sulla rete, spesso sin troppo disinibite e, quindi, manipolabili. Com'è evidente, sono tutti fattori esterni a ragionamenti di stretto diritto, che sembrano chiarire le anzidette forzature nella motivazione della sentenza Schrems. L'esito, pur apprezzabile in termini di rafforzamento dei diritti dei cittadini europei al rispetto della vita privata e alla protezione dei dati, può, tuttavia, risultare preoccupante, perché sposta su un terreno improprio, ossia quello giurisdizionale, confronti e soluzioni che dovrebbero trovare spazio a livello, anzitutto, politico, considerata l'enorme rilevanza sociale ed economica degli interessi in gioco", P. FALLETTA, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c. DPC, C-362/14)*, in *Federalismi.it*, 24, 2015, p. 11.

[40] COMMISSIONE EUROPEA, *Comunicazione della Commissione al PE e al Consiglio: Scambio e protezione dei dati personali in un mondo globalizzato*, COM (2017) 7 final, 10 gennaio 2017.

[41] C. KUNER, *Reality and illusion in EU data transfer regulation post-Schrems*, in *German Law Journal*, 18, 2017, p. 898.

[42] L'ipocrisia può essere ravvisata anche sotto un altro profilo: "When a legal system strives for its standards to be accepted as universal values, it is inevitably engaged in a hegemonic struggle in which it seeks to have its own special interests identified with the general interest", C. KUNER, *The Internet and the global reach of EU law*, in M. CREMONA, J. SCOTT (a cura di), *EU law beyond EU borders. The extraterritorial reach of EU law*, Oxford University Press, 2019, p. 137.

di *law enforcement* o di intelligence senza la mediazione di un soggetto privato. Anche in tale opzione, infatti, la CGUE dovrebbe coerentemente evitare di negoziare e comunque considerare come sottoponibile a valutazione di adeguatezza qualsiasi pratica, per quanto invasiva, posta in essere da uno Stato terzo per scopi securitari che non implichi il coinvolgimento di *service providers*. Ciò, per quanto logico riflesso di quanto affermato dai giudici europei nel contesto interno e dunque corretta trasposizione nella dimensione esterna del livello di tutela garantito entro l'UE, potrebbe comunque portare ad una diminuzione del livello di tutela concretamente garantito mediante lo strumento della decisione di adeguatezza ai dati che fuoriescono dai confini europei e dunque, nei fatti, condurre ad una contrazione della efficacia del sistema di disciplina del trasferimento dei dati stesso, che risentirebbe, in un certo senso, dei limiti e del principio di attribuzione sui quali la 'struttura' dell'UE si basa.

Altro riflesso possibile e complesso della giurisprudenza della CGUE in materia di *data transfer* rispetto alla regolamentazione della *data retention* si sostanzia nelle affermazioni svolte dai giudici di Lussemburgo nel *Parere 1/15*: i profili problematici, colti peraltro dai giudici belgi e tedeschi che hanno promosso un rinvio con riferimento alla Direttiva PNR, possono essere ravvisati innanzitutto nella accettazione di una forma di controllo preventivo generalizzato da parte di autorità dello Stato terzo ricevente (ma in ottica europea da parte della UIP di ciascuno Stato membro), che emerge dal *Parere 1/15*. In questo caso infatti, sebbene certamente, come si è evidenziato nel Capitolo III Parte II, sia vero che i dati oggetto di controllo sono maggiormente ristretti ed interessano una cerchia delimitata di soggetti (i soli passeggeri), è altrettanto vero come in questo caso venga comunque a mancare quel criterio oggettivo e di connessione, anche indiretta, che lega il trattamento di un dato alla sussistenza di una minaccia per la sicurezza. La conservazione, inoltre, per quanto limitata al periodo di sola permanenza del viaggiatore e non anche successivamente alla partenza dallo Stato di arrivo, risulta avere carattere generalizzato, interessando infatti anche i dati di soggetti 'non sospetti' o non pericolosi sulla base del controllo automatizzato preventivo, effettuato prima dell'arrivo stesso. In tali due evidenziati profili sembra denotarsi una maggiore flessibilità nella posizione della CGUE rispetto a quanto espresso con riferimento alla *data retention* di metadati relativi alle telecomunicazioni. Non è forse vero che anche in quest'ultimo caso la conservazione generalizzata risulta finalizzata a rendere possibile l'accesso eventuale e successivo ai dati da parte delle autorità di *law enforcement*, come affermato nel *Parere 1/15*? E non è allora trasponibile anche ai casi di *data retention* analizzati dalla CGUE sul fronte interno la posizione secondo cui una forma targettizzata e limitata inficerebbe l'efficacia della conservazione stessa[43]? Dovrà essere la CGUE, nei rinvii pendenti, a chiarire tali dubbi e perplessità, e valutare se abbracciare o meno la tesi di chi ravvisa nella limitatezza dei soggetti i cui dati sono sottoposti a trasferimento e conservazione (solo i passeggeri) e nella maggiore limitatezza anche della tipologia di dati (solo i PNR anziché tutti i metadati derivanti da tutte le forme di telecomunicazione), ragioni sufficienti per giustificare le difformità ravvisabili nella posizione della CGUE.

3. – L'aiuto offerto dallo studio comparato: alcune riflessioni sul raffronto tra discipline normative e approcci giurisprudenziali caratterizzanti Regno Unito, Belgio e Italia

Il vuoto lasciato dalla dichiarazione di invalidità della DRD, in parte colmato dall'intervento suppletivo della CGUE, ha creato, come più volte sottolineato, una situazione di forte frammentarietà all'interno dell'UE: nonostante le pronunce dei giudici di Lussemburgo abbiano fissato criteri e principi in materia di *data retention*, volti a fornire un vero e proprio *vademecum* ai legislatori nazionali con riferimento alla corretta interpretazione dell'art. 15 Direttiva *e-Privacy*, l'analisi svolta nella Parte III,

[43] "La conservazione e l'uso a tal fine non possono, per loro stessa natura, essere limitati a una cerchia determinata di passeggeri aerei né essere oggetto di una previa autorizzazione di un giudice o di un ente amministrativo indipendente", par. 197, *Parere 1/15*.

come anche l'esame delle reazioni degli Stati membri a seguito delle diverse pronunce della CGUE studiate nei Capitoli II e IV Parte II, hanno ben evidenziato come sussistano ancora molteplici differenze nelle scelte ed approcci dei legislatori e giudici nazionali. Il sopra rilevato silenzio assordante del legislatore europeo ha acuito e permesso il protrarsi di questo panorama frammentario e frastagliato di soluzioni ed orientamenti.

Ciò è ben visibile anche negli Stati membri oggetto di approfondimento: Regno Unito, Belgio e Italia sono emblematici esempi di come legislatori e Corti abbiano diversamente interpretato la giurisprudenza della CGUE e i requisiti da essa stabiliti, individuando un differente punto di equilibrio tra esigenze securitarie e garanzia dei diritti fondamentali e creando così uno scenario disomogeneo, nel quale le salvaguardie e le tutele ai diritti alla riservatezza e alla protezione dei dati non sono eguali in tutti gli Stati membri. Senza dubbio però e nonostante le differenze, anche sostanziali, riscontrabili, sono tuttavia rinvenibili alcune convergenze, visibili in maniera estremamente più marcata tra Regno Unito e Belgio, in termini sia di percorso evolutivo della normativa e della giurisprudenza nazionali, sia di condivisi risultati (al momento) finali del dibattito apertosi in questi due Paesi.

Partendo dunque con una riflessione comparata sui profili di 'confluenza' e somiglianza che possono essere individuati a seguito della trattazione dei singoli ordinamenti, non può che evidenziarsi come tutti i tre Stati analizzati abbiano mantenuto costante nel tempo una posizione chiara e decisa quanto alla forma di conservazione generalizzata ed indiscriminata dei metadati. Rispetto a questo strumento, infatti, tutti gli ordinamenti analizzati in questo lavoro hanno mostrato una strenua volontà di difesa e di mantenimento in essere, pur sostenendo tale scelta con differenti ragionamenti: il Belgio, nei lavori preparatori predisposti dal Governo, ha sottolineato l'importanza di una *bulk data retention* al fine di una maggiore garanzia delle vittime di reati e degli stessi imputati, che potrebbero essere scagionati proprio mediante l'accesso ai metadati conservati in via preventiva e generalizzata, proponendo una lettura della posizione espressa dai giudici di Lussemburgo che faccia salva la conservazione massiva, seppure con alcune restrizioni, a fronte di una più rigida ed elevata tutela dei diritti fondamentali nella fase di accesso; i giudici del Regno Unito, pur giungendo, come i giudici belgi, a rinviare alla CGUE, si sono fatti portatori di una posizione più netta quanto alla legittimità di una conservazione che possa assumere anche i caratteri di generalizzazione: nel rinvio *Privacy International* infatti si coglie perfettamente come l'IPT ponga un serio e chiaro 'monito' alla CGUE, ribadendo, pur con riferimento alle operazioni svolte da agenzie di intelligence per scopi di sicurezza nazionale, l'importanza vitale e l'insostituibilità di una forma di *bulk data retention*. L'Italia infine, pur non essendosi molto interrogata sul tema e pur non potendosi riscontrare un ampio dibattito sulla materia in sede parlamentare, ha confermato, sia nelle scelte legislative sia nelle vicende giurisprudenziali, di voler mantenere, senza metterla in discussione, una conservazione generalizzata come strumento principe per la tutela della sicurezza e la lotta alla criminalità grave.

In tutti gli Stati membri analizzati emerge con evidenza come la possibilità di rinunciare all'impiego di una conservazione generalizzata non sia mai stata realmente presa in considerazione, mentre è risultata chiara la difficoltà, quando non la reticenza o la ritenuta vera e propria impossibilità[44], di porre

[44] Nel Doc. par. Chambre, 2015-2016, DOC 54-1567/001, nel quale sono riportate le considerazioni svolte dal Governo belga e il dibattito in sede parlamentare attinente alla predisposizione di una nuova normativa in materia di *data retention* a seguito della sentenza *DRI*, si legge una chiara posizione contraria alla adozione di una forma di conservazione targettizzata e alla opportunità ed utilità di un simile strumento: "après analyse approfondie, (..) il n'est pas possible d'opérer une différenciation a priori de cet élément. (..) Limiter la conservation des données à celles concernant des personnes qui font déjà l'objet d'une enquête pénale ou de renseignement n'a pas de sens car cette possibilité existe déjà par ailleurs" (par. 7). Come sottolineato anche nella sentenza della Corte costituzionale del 19 luglio 2018, n. 96/2018, il Governo ha ribadito successivamente alla sentenza *Tele2* la propria posizione di contrarietà rispetto alla forma di conservazione targettizzata: "Si chaque citoyen n'est, en effet, pas potentiellement un criminel, chaque citoyen peut potentiellement être confronté à la criminalité, que ce soit en tant que victime, en tant que prévenu ou en tant que témoin et dès lors avoir un intérêt à la recherche de la vérité", par. A.10.3. Ne consegue dunque che sarebbe sbagliato individuare la carenza di un singolo elemento nella lista dei

in essere forme alternative di *data retention* quale quella targettizzata promossa dalla CGUE: non è un caso che nessuno dei legislatori, né quello inglese né quello belga, che sono intervenuti a modifica della propria normativa nazionale a seguito delle decisioni della CGUE, abbia adottato una forma di *targeted data retention* o abbia considerato l'introduzione di criteri quali la limitazione della conservazione sulla base di aree geografiche o specifici gruppi di soggetti. Certo il Regno Unito, predisponendo, diversamente dal Belgio, un obbligo di conservazione legato unicamente al 'retention notice' emanato dal *Secretary of State*, ha potenzialmente previsto la possibilità di un ordine di conservazione più mirato e delimitato, cui si somma peraltro la previsione di specifiche condizioni e criteri che devono essere valutati prima della emanazione di un 'retention notice', ma non ha comunque del tutto escluso la possibilità di adottare forme di *bulk data retention*, che restano quindi possibili.

Nessuno Stato membro e neppure nessuna Corte nazionale pertanto ha *tout court* abbracciato un divieto assoluto di conservazione generalizzata: sebbene in un primo momento la Corte costituzionale belga avesse riproposto il medesimo ragionamento seguito dai giudici di Lussemburgo nella sentenza *DRI*, dichiarando la contrarietà ai principi di proporzionalità e necessità di una forma di conservazione generalizzata, essa ha poi operato una lettura meno 'netta' sul punto nella più recente pronuncia del 2018, nella quale, pur facendo questa volta riferimento all'art. 15 Direttiva *e-Privacy*, ha rinviato alla CGUE proprio per ottenere chiarimenti sull'incompatibilità al diritto dell'UE di una normativa nazionale che prevedesse una forma di *bulk data retention*. Questa posizione condivisa[45] e, sino ad ora, irremovibile, degli Stati analizzati, che mira a difendere e far salva la conservazione generalizzata, risulta essere del resto uno dei punti maggiormente problematici ancora aperti nel dialogo tra Stati membri e UE, che non solo sta rendendo difficile trovare una soluzione normativa a livello europeo che sia condivisa ed accettabile, e dunque capace di superare illesa il vaglio della CGUE, ma che rappresenta anche è il vero aspetto critico sulla base del quale quasi tutti i rinvii pregiudiziali in materia pendenti dinnanzi ai giudici di Lussemburgo hanno origine.

Insieme a questo profilo, che accumuna certamente gli Stati membri analizzati ma li distanzia dalla posizione che fino ad ora pare aver assunto la CGUE nella sua giurisprudenza, un ulteriore aspetto invece segnala una certa convergenza non solo tra Regno Unito e Belgio ma anche tra l'approccio da essi seguito e la posizione espressa dai giudici di Lussemburgo: per entrambi infatti è possibile affermare che le sentenze della CGUE, pur con i limiti e criticità già ampiamente rilevati, hanno prodotto quale esito un innalzamento del livello di tutela garantito dalla normativa nazionale in materia di *data retention*, portato anche dell'intervento delle Corti nazionali. Pur seguendo sicuramente approcci e percorsi differenti, Belgio e il Regno Unito sono quindi giunti ad un medesimo e comune risultato finale: entrambi tali Stati infatti hanno approvato, non senza difficoltà e diversità, discipline nazionali via via sempre più garantiste, così che partendo da un approccio fortemente 'pro-securitario', caratterizzato da normative che prevedevano salvaguardie limitate e una più ampia facoltà di accesso ai dati conservati, si è lentamente passati ad una disciplina più precisa, puntuale, con la previsione di una serie di salvaguardie specifiche e dell'intervento di organi *ad hoc*. Entrambi poi, pur senza rinunciare, come si

requisiti fissata dalla CGUE – per esempio la mancanza di una *targetd retention* – e valutare quell'unico criterio non rispettato come in sé idoneo a rendere la disciplina sulla conservazione e accesso ai metadati irrimediabilmente e totalmente incompatibile con la Carta Europea dei Diritti Fondamentali. Il Governo inoltre aggiungeva come sia da considerarsi impossibile "de lutter contre la criminalité grave telle que la cybercriminalité si l'on ne prévoit pas une obligation générale et indifférenciée de conservation des données de communication électronique", (par. A.13.3).

[45] Particolare è anche la visione, sul punto, dalla *Commission pour la protection de la vie privée* belga, che ha affermato, con riferimento ai criteri stabiliti dalla CGUE nelle sentenze *DRI* e *Tele2*, come "aucun des deux arrêts ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrêts ne peut pas être retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects", *Doc. parl.*, Chambre, 2015-2016, doc. 54, 1567/001, p. 13. Anche questa lettura quindi ha messo in evidenza come l'incompatibilità di un sistema di conservazione generalizzata con il diritto dell'UE debba essere valutato anche in correlazione al rispetto degli altri criteri e requisiti fissati dalla CGUE.

è detto, allo strumento della *bulk data retention*, hanno posto questioni importanti alla CGUE, in questo modo promuovendo, seppur con approcci differenti, un dialogo con i giudici di Lussemburgo, fondato sul previo studio e conoscenza della giurisprudenza europea, sul riconoscimento dei suoi limiti e sulla conseguente necessità di ottenere chiarimenti ed interpretazioni precise che possano favorire maggiore conformità ma anche stabilità alla normativa interna: se l'obiettivo di entrambi i rinvii promossi dalle Corti di Regno Unito e Belgio è senza dubbio quello di indurre la CGUE a rivedere la propria posizione o a meglio determinarne i confini e limiti, è comunque positiva la scelta di instaurare un rapporto dialettico con i giudico di Lussemburgo anziché prediligere soluzioni, adottate unicamente sul fronte interno, ai problemi connessi alla conservazione dei dati o addirittura negare la sussistenza di qualsiasi aspetto dubbio e meritevole di chiarimento nella discussa giurisprudenza della CGUE. Proprio sotto questo ultimo profilo, lo si vuole sottolineare sin da ora, può essere identificata una sostanziale differenza tra l'approccio del Regno Unito e del Belgio da un lato e quello invece dell'Italia dall'altro: quest'ultima infatti, come si è già visto nel Capitolo III, Parte III, ha conosciuto una storia giurisprudenziale che non è mai giunta né a promuovere un rinvio ai giudici di Lussemburgo in materia, né un rinvio alla Corte costituzionale nazionale, non essendosi dunque mai messa in discussione la scelta di una conservazione generalizzata, la sua disciplina nazionale e la sua compatibilità con la giurisprudenza della CGUE, ma anche – indirettamente – con quanto accaduto in altri Stati membri.

Pur rimandando oltre per una analisi critica dello specifico approccio 'inattivo' e poco sensibile che ha caratterizzato l'intervento di giudici e legislatori italiani, e tornando quindi ora a quei profili di somiglianza tra Belgio e Regno Unito che sono stati identificati nel risultato finale della promozione di una disciplina maggiormente garantista in materia di *data retention* e accesso, è bene evidenziare come entrambi abbiano mostrato una forte attenzione e consapevolezza circa il tema della conservazione dei metadati e dell'accesso per scopi securitari e del suo impatto sui diritti fondamentali: essi si sono mostrati quindi particolarmente attivi sia sul fronte legislativo sia giurisprudenziale, un attivismo che li ha portati a pensare e dibattere sul possibile equilibrio da rinvenire non solo tra sicurezza e diritti alla privacy e *data protection* ma anche tra scelte interne e principi e requisiti stabiliti a livello europeo. La reazione però a questi ultimi e all'avvicendarsi delle sentenze della CGUE è stata ed è tutt'ora differente.

Se si prende quale iniziale spunto di riflessione l'esame svolto con riferimento al Regno Unito, ad esempio, è possibile notare come questo Stato abbia presentato, sin dalla sentenza *DRI*, una storia normativa e giurisprudenziale estremamente complessa e travagliata, resa ancora più intricata dall'ombra della incombente Brexit. È del resto inevitabile che le radici di questo processo di uscita dall'UE senza precedenti, insieme ad altre peculiarità storiche ed ordinamentali che hanno caratterizzato sin dalle sue origini la presenza del Regno Unito all'interno dell'UE, emergano nel difficile rapporto con la giurisprudenza della CGUE, manifestatosi in maniera paradigmatica nello specifico ambito della disciplina della conservazione dei dati, rispetto alla quale si assiste addirittura alla approvazione di una nuova normativa proprio nelle more della decisione *Tele2*, peraltro derivante da un rinvio pregiudiziale promosso proprio dai giudici del Regno Unito. Questa scelta ampiamente criticata del legislatore nazionale, pur in parte motivata dalla imminente scadenza della *sunset clause* che regolava la vigenza della previa normativa, mostra senza dubbio, quantomeno inizialmente, un approccio caratterizzato da una sorta di autonomia e di voluta 'lontananza' o resistenza da parte del Governo e del Parlamento inglesi rispetto a quelle che sarebbero state le posizioni finali espresse dai giudici europei. Ciò diviene evidente se si osserva come, in maniera ancor più marcata rispetto ad altri Stati membri, le modifiche normative nel contesto inglese si siano susseguite ad un ritmo estremamente rapido, a tratti confuso e in maniera disordinatamente correlata alle pronunce delle Corti tanto nazionali quanto della CGUE. Mentre in Belgio, ad esempio, l'adozione di una nuova regolamentazione della *data retention* è intervenuta sempre a seguito di decisioni della Corte costituzionale, a loro volta pronunciate sulla base delle importanti sentenze della CGUE, con uno sviluppo che si potrebbe definire 'lineare' – che vede

sostanzialmente la sentenza della Corte di giustizia, poi il ricorso innanzi alla Corte costituzionale[46], seguito dalla dichiarazione di incostituzionalità della normativa nazionale e dal successivo intervento del legislatore –, nel Regno Unito il percorso è risultato senza dubbio più intricato ed articolato, caratterizzato da frequenti sovrapposizioni tra interventi legislativi e giurisprudenziali, non sempre coordinati ed allineati sulla stessa posizione: mentre venivano evidenziati i limiti della disciplina del DRIPA, sottoposta all'attenzione dei giudici nazionali ed europei, il Parlamento adottava contemporaneamente il IPA che, pur prevedendo innovative disposizioni maggiormente garantiste, non colmava le lacune già individuate nella normativa precedente e ribadite dal di poco successivo intervento dei giudici della CGUE nella sentenza *Tele2*. Questo intreccio temporale ha prodotto quale effetto la creazione di una situazione di forte confusione ed instabilità, nella quale, quasi in contemporanea o a poca distanza di tempo dalla loro approvazione, le scelte del legislatore sono state poste in discussione dinnanzi ai giudici nazionali: il IPA, unitamente ad altre normative che prevedevano forme di *data retention*, sono state portate repentinamente e contemporaneamente innanzi a diversi Tribunali, dal IPT nel caso *Privacy International*, alla High Court nel caso *Liberty*, alla ripresa delle 'redini' del caso *Watson* da parte della Court of Appeal a seguito della decisione della CGUE; unitamente il Governo stesso, prendendo atto con lucidità di talune discrepanze tra la normativa interna da poco approvata e i requisiti ribaditi dalla CGUE, aveva promosso un nuovo intervento normativo a modifica dell'assetto vigente, così che i giudici inglesi hanno finito o col pronunciarsi su normative non più vigenti o già sottoposte a revisione.

Nonostante il percorso certamente 'disordinato' e travagliato, frutto da un lato della volontà, ancor più chiara in anni recenti, di inserire alcune tutele e salvaguardie indicate dalla giurisprudenza della CGUE e lentamente accolte anche dalle Corti nazionali, e dall'altro dal rifiuto a rinunciare, *in toto*, ad una forma di conservazione generalizzata ed indiscriminata, cui si somma la necessità emersa dal rinvio pregiudiziale *Privacy International* di ottenere chiarezza quanto ai confini del diritto dell'UE e del sindacato della Corte, non può che rilevarsi comunque come nel Regno Unito, similmente a quanto accaduto in Belgio, si sia assistito ad una lenta erosione di quelle resistenze interne inizialmente affermate, portando giudici e legislatori nazionali a riflettere sul regime normativo adottato e ad intervenire per modificarlo, nella direzione di una maggiore tutela dei diritti fondamentali e di un bilanciamento sempre più effettivo tra garanzie ed efficacia degli strumenti di lotta alla criminalità. Certo, altri Stati membri sono stati in grado di dimostrare, ben prima del Regno Unito, una maggiore attenzione e volontà di incorporare nel proprio ordinamento i principi dettati, in particolare, dalle sentenze *DRI* e *Tele2*, giungendo più rapidamente ad un assetto normativo, soprattutto in materia di accesso ai metadati, per certi versi più garantista rispetto a quello inglese: ne è un esempio il Belgio, la cui normativa nazionale, pur sottoposta all'attenzione della Corte costituzionale, ha previsto sin dal 2016 una differenziazione dei tempi di conservazione, e dunque della possibilità di 'andare indietro nel tempo', a seconda della tipologia di reati, prestando attenzione a definire una chiara soglia di gravità dei reati per i quali l'accesso viene consentito ed un elenco più mirato di finalità che, per quanto ampie, motivano ed autorizzano una ingerenza nella sfera privata; seppur più lentamente e con maggiori difficoltà però anche il Regno Unito ha inserito simili salvaguardie nel *Data Retention and acquisition regulations 2018*, creando organi *ad hoc* deputati ad operare un controllo nella fase di accesso nonché

[46] Merita precisare come i ricorsi siano in realtà di poco precedenti rispetto alla pronuncia finale dei giudici di Lussemburgo. Ciò, lo si vuole ricordare, per mere ragioni di opportunità: il ricorso per annullamento previsto dall'ordinamento belga prevede infatti un termine di tempo di attivazione pari a sei mesi dalla pubblicazione della legge che si intende impugnare. Attendere l'esito della pronuncia della CGUE, che non sarebbe sicuramente giunto entro i sei mesi previsti per la promozione del ricorso per annullamento, avrebbe pertanto portato alla rinuncia di tale importante strumento per adire la Corte costituzionale.

disponendo una limitazione in termini sia di reati gravi per i quali l'accesso è consentito, sia di scopi e finalità per le quali risulta giustificabile una compressione dei diritti alla privacy e protezione dei dati[47].

Se dunque, quantomeno inizialmente, la tendenza ad interventi normativi di 'adeguamento' e modifica della disciplina interna, peraltro rapidi e poco coordinati – nella sostanza e nella scelta temporale – con la giurisprudenza nazionale e soprattutto europea, pareva motivata più dal timore di perdere la possibilità di utilizzare i metadati conservati che da una reale e sentita volontà di innalzare il livello di tutela dei diritti fondamentali e addivenire ad un più corretto bilanciamento con le esigenze securitarie[48], tale volontà pare invece essere maggiormente e con decisione sottesa alle recenti modifiche legislative, in particolare quella del 2018, frutto di una più seria elaborazione e studio da parte del legislatore, spinto anche dalle critiche e dalle analisi mosse dalla dottrina nonché dall'attenzione manifestata dalla società civile, oltre che dalla posizione espressa dalle Corti nazionali e in taluni punti maggiormente convergente con quella della CGUE. Un percorso quindi che, sotto tale profilo, deve essere letto positivamente, soprattutto se paragonato a Stati membri, quali l'Italia, nei quali non si è ancora registrata una riflessione profonda sull'esigenza di adeguare la normativa nazionale a quanto emerso dalla giurisprudenza europea.

Diverso è invece l'approccio del Belgio: l'analisi delle vicende giurisprudenziali e normative che caratterizzano tale Paese, infatti, hanno messo in luce innanzitutto un percorso giurisprudenziale maggiormente in linea con i dettami e l'interpretazione della CGUE, come manifestato nella prima sentenza della Corte costituzionale[49] in materia, successiva alla pronuncia *DRI* e avente ad oggetto la legittimità costituzionale della normativa nazionale in materia di *data retention* frutto del recepimento della DRD. La prima decisione del giudice delle leggi belga infatti ha ricalcato ampiamente la pronuncia e il ragionamento seguito dai giudici di Lussemburgo, ritenendo motivo sufficiente di illegittimità e incompatibilità con il diritto dell'UE il solo fatto che la conservazione prevista dalla normativa nazionale

[47] Si vuole sottolineare come anche sotto il profilo giurisprudenziale non possa che essere rilevata la restia e talvolta confusa posizione delle Corti nazionali dinnanzi alla giurisprudenza della CGUE: basti pensare all'iniziale approccio della High Court, che riteneva applicabili i criteri indicati nella sentenza *DRI* anche alla normativa nazionale, poi ribaltato dalla Court of Appeal nel caso *Watson*, così come alla reticenza ravvisabile da quest'ultima Corte nel dare risposte nette in materia soprattutto di conservazione dei dati nella causa ripresa a seguito della sentenza *Tele2*: in tale occasione infatti i giudici inglesi avevano escluso che i criteri delineati in tale sentenza fossero applicabili alla normativa inglese in quanto riferiti a quesiti posti dal giudice del rinvio svedese e aventi dunque quale oggetto la disciplina svedese. In decisioni quali quelle richiamate diviene evidente la mancanza di una posizione chiara relativamente alla disciplina della *data retention*, al carattere generalizzato della stessa e alla sua legittimità, nel tentativo di far comunque salva la *bulk data retention* e di leggere i requisiti espressi dalla CGUE come non necessariamente sussistenti contemporaneamente. Ciò è confermato ad esempio dalla High Court, chiamata a pronunciarsi sul DRIPA a seguito della sentenza *DRI*, "the solution to the conundrum, in our view, is that the legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter *unless* it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights", par. 89, [2015] EWHC 2092, Case No. CO/3665/2014; CO/3667/2014; CO/3794/2014, del 17 luglio 2015).

[48] Questa lettura pare ancora più corretta se si pensa alle parole usate dal *Home Secretary*, Jacqui Smith, che aveva riconosciuto come "governed by a strict regulatory framework, communications data is routinely used to investigate terrorist plots, to bring to justice those guilty of serious crimes, to seize illegal drugs and to protect the vulnerable in our society. It is no exaggeration to say that information gathered in this way can mean the difference between life and death", SECRETARY OF STATE FOR THE HOME DEPARTMENT, *Protecting the Public in a changing communications environment*, 2009, p. 2. Ciò a conferma dunque dell'elevata importanza attribuita allo strumento della *bulk data retention*, considerato insostituibile e fondamentale. Una convinzione che, seppure modulata e ridimensionata dall'intervento normativo e dalle pronunce dei giudici nazionali e della CGUE, permane ancora oggi ed emerge dalle parole del IPT nel caso *Privacy International*, che afferma come la questione sottoposta all'attenzione dei giudici riguardi "the balance between the steps taken by the State, through the SIAs, to protect its population against terror and threat to life against the protection of privacy of the individual", a mettere quindi nuovamente in evidenza quanto determinanti fossero le questioni trattate al fine della garanzia della sicurezza nonché le conseguenze dirompenti che la pronuncia della CGUE nel rinvio pregiudiziale promosso sono destinate ad avere in tale delicato ambito.

[49] Cour Constitutionnelle, Arrest nr. 84/2015, 11 giugno 2015.

fosse di natura generalizzata ed indiscriminata. Questa decisione, come si è visto, è stata molto criticata anche dalla dottrina, in quanto troppo 'ossequiosa' rispetto alla giurisprudenza della CGUE e incapace quindi di considerare, nel caso posto alla sua attenzione, le peculiarità delle richieste e della normativa belga del 2013; in tale iniziale approccio la posizione dei giudici belgi si è differenziata certamente dalle Corti inglesi, che avevano adottato invece un atteggiamento più restio all'attuazione dei criteri indicati dalla giurisprudenza europea, cercando di fornirne una interpretazione più 'favorevole' e meno rigida – ad esempio, come si è visto, ritenendo le considerazioni svolte nella sentenza *Tele2* con riferimento alla conservazione come specificamente riguardanti la disciplina normativa svedesi –.

Al di là comunque di questo iniziale orientamento, ciò che è significativo notare è come anche la Corte costituzionale belga, nelle questioni poste alla sua attenzione negli ultimi anni, abbia poi finito col riconoscere – forse grazie ad una maggiore maturità e conoscenza del tema – la rilevanza e la fondatezza dei dubbi interpretativi ed applicativi scaturiti dalla giurisprudenza europea. A tale risultato, sfociato nel rinvio pregiudiziale più volte richiamato però la Corte costituzionale giunge sempre distinguendosi dall'approccio del Regno Unito: non solo non viene formulato un rinvio pregiudiziale 'monitorio' quale quello promosso dall'IPT inglese, ma anzi viene messo già in conto un possibile esito confermativo di quella incompatibilità *per se* di forme di conservazione generalizzata già emersa dalla sentenza *Tele2*, tanto da portare la Corte a promuovere appositamente un quesito relativo alle conseguenze di una incompatibilità con il diritto dell'UE delle normative nazionali in materia di *data retention*, soprattutto con riferimento ai procedimenti penali fondati su prove derivanti da metadati. Nella pronuncia che ha portato al rinvio, comunque, la Corte costituzionale richiama espressamente le grandi difficoltà concretamente incontrate dalla maggioranza degli Stati membri nel predisporre una disciplina nazionale conforme e rispettosa dei criteri individuati in *DRI* e *Tele2*, quasi a sottolineare che le criticità incontrate dai legislatori belgi risultano in realtà avere carattere diffuso in tutta l'UE, affondando le proprie radici non nei limiti o nell'approccio di un singolo legislatore nazionale bensì in questioni ben più profonde e condivise a livello europeo. Questa consapevolezza non ha potuto che condurre i giudici belgi, nonostante un approccio in linea con la CGUE e una seria riflessione svolta, con grande attenzione, anche dal legislatore, a scontrarsi, successivamente alla sentenza *Tele2*, con le difficoltà e le diversità interpretative derivanti dalle zone grigie lasciate dalla giurisprudenza europea, dovendo quindi adire, in questo del tutto similmente al Regno Unito, la Corte di Giustizia stessa per ottenere indicazioni chiare e univoche, soprattutto con riferimento alla disciplina della conservazione[50].

Diametralmente differente rispetto ai due Stati sin qui analizzati, rispetto ai quali sono state individuate alcune convergenze e risultati comuni, insieme a talune divergenze nell'approccio e nel percorso che ha condotto a punti di arrivo simili, è invece l'orientamento tenuto dall'Italia, che presenta una parabola normativa e giurisprudenziale estremamente peculiare: mentre la giurisprudenza ha sempre – piuttosto rapidamente e talvolta superficialmente – concluso ritenendo la normativa nazionale conforme al diritto dell'UE, considerando peraltro inutile provvedere ad un rinvio pregiudiziale innanzi alla CGUE, il legislatore nazionale non ha dimostrato di sapersi – o volersi – interrogare quanto all'incidenza della giurisprudenza europea rispetto all'assetto normativo interno, intervenendo con singole e spesso confuse disposizioni di natura emergenziale e temporanea, con proroghe e incertezze che hanno creato peraltro non poche difficoltà operative ai fornitori di servizi di telecomunicazione, giungendo in ultimo a modificare la durata della conservazione alla attuale previsione di ben settantadue mesi, sebbene per determinate tipologie di reati. Non potendo previamente sapere però per quali reati verrà richiesto l'accesso, i *service providers* devono necessariamente memorizzare il dato per l'intera

[50] Il Belgio poi ha dimostrato una grandissima e profonda conoscenza del tema a tutto tondo, nel rinvio pregiudiziale promosso in materia di Direttiva PNR, mettendo in evidenza in tale occasione le connessioni che possono essere rilevate tra la giurisprudenza della CGUE in materia di *data retention* e quella in materia di trasferimento dati verso Stati terzi. Una conoscenza profonda che risulta chiara anche nel dibattito legislativo e nei lavori di preparazione finalizzati alla approvazione della legge del 2016.

durata massima prevista dalla legge, con l'effetto che la conservazione risulta *de facto* estremamente lunga, con una scelta peraltro che non solo non trova eguali nel panorama europeo ma non presenta neppure una giustificazione specifica o chiaramente motivata da parte del legislatore stesso. Oltre alla durata della conservazione, ciò che manca nella disciplina italiana inoltre è la previsione di una limitazione della possibilità di accesso per il solo motivo di lotta ai reati gravi: tale possibilità infatti, nel contesto italiano, è prevista per tutti i reati. È indicativo, proprio su questo ultimo aspetto, come il Belgio e – in tempi più recenti – il Regno Unito si siano invece entrambi dotati di una definizione di 'reati gravi', mostrando di voler adeguare la disciplina interna, pur con tutte le criticità ancora persistenti soprattutto sul fronte della *data retention*, a tale criterio indicato con forza dalla giurisprudenza europea.

Sin da questi rilievi, che sottolineano la forte distanza dell'Italia rispetto agli altri due Stati esaminati, si comprende come la comparazione e l'analisi delle diverse esperienze di altri Stati membri possa rappresentare in modo particolare nel panorama italiano un utile spunto di approfondimento e un prezioso punto di partenza per meglio comprendere il dibattito apertosi in altre realtà ordinamentali a seguito delle pronunce della CGUE e le conseguenti scelte legislative ma anche giurisprudenziali intercorse. Se si pensa alla legislazione vigente belga, si può notare come essa, pur presentando aspetti di somiglianza con la disciplina italiana, prevedendo anch'essa una conservazione generalizzata nonché un accesso la cui autorizzazione è generalmente assegnata al Procuratore del Re, sia il frutto di una seria riflessione del legislatore circa l'impatto delle decisioni e dei requisiti fissati dalla CGUE e la loro concreta applicazione nell'ambito interno. Così la legge belga del 2016, nonostante presenti senza dubbio anche nella sua versione attuale aspetti problematici, ha il merito comunque di prevedere una serie di più puntuali salvaguardie, quali una precisa modulazione nel tempo dell'accesso a seconda della gravità del reato, la previsione di una conservazione ben più contenuta nella sua durata rispetto a quella italiana, nonché la predisposizione di tutele da possibili accessi abusivi mediante l'obbligo di predisposizione di richieste di accesso scritte e motivate che, diversamente da quelle generiche che il p.m. è chiamato a fornire in Italia, devono contenere indicazioni precise soprattutto quanto alla proporzionalità e necessità dell'ingerenza, stabilendo inoltre che, qualora sussistano indizi gravi di reati per i quali è prevista una detenzione di un anno o pena superiore e laddove tali informazioni siano necessarie per stabilire la verità dei fatti, sia unicamente il giudice istruttore il soggetto deputato a richiedere l'accesso ai dati relativi al traffico e i dati sulla localizzazione. Per queste tipologie di informazioni, considerate maggiormente intrusive nella sfera privata, quindi, la domanda deve essere effettuata solamente dal giudice; senza considerare che l'accesso può essere effettuato non per scopi di indagine e repressione di qualsiasi tipologia di reato bensì solo di quelli *gravi*, individuati in quelli tali da comportare una detenzione principale di un anno o pena superiore; è stata prestata inoltre una maggiore attenzione ai metadati riguardanti soggetti sottoposti a segreto professionale, rispetto ai quali è stata prevista una apposita disciplina. Sebbene quindi anche nella legislazione belga sia ancora possibile individuare – similmente alla disciplina italiana – una conservazione generalizzata, in tale contesto si è nondimeno registrato un serio dibattito e valutazione, anche da parte del Governo e del Parlamento, nonché delle autorità nazionali di garanzia della privacy e protezione dei dati, basato in particolare sullo studio delle conseguenze delle sentenze della CGUE e sulle loro ripercussioni nel panorama normativo interno. A seguito di tali discussioni e con riferimento alle scelte effettuate, non sono stati negati, ed anzi si è preso consapevolezza dei limiti e delle possibili incompatibilità rispetto ai criteri fissati dai giudici di Lussemburgo, alle quali però il legislatore ha tentato di sopperire mediante l'introduzione di salvaguardie, soprattutto nella fase dell'accesso e sotto il profilo della sicurezza dei dati stessi, nonché attraverso una regolamentazione unitaria. Lo stesso può certamente dirsi per il Regno Unito, nel quale, pur con maggiore lentezza e resistenza, sono stati introdotti dei cambiamenti significativi nella direzione di una maggiore garanzia dei diritti fondamentali e di un più significativo adeguamento della disciplina nazionale ai principi definiti a livello europeo: basti pensare a come sia stata introdotta, a differenza dell'Italia, una definizione di 'serious crime' e l'accesso sia stato limitato

strettamente alla lotta a tale elenco di reati, e ancora a come sia stato effettuato il tentativo di introdurre un controllo indipendente che preceda l'accesso ai metadati nonché la previsione del c.d. *retention notice* del *Secretary of State*. Questo risultato è stato raggiunto anche grazie alla posizione espressa, quantomeno negli ultimi anni, dai giudici nazionali: nel Regno Unito, infatti, similmente a quanto accaduto in Belgio, le Corti interne, pur senza mai giungere ad una dichiarazione di illegittimità di forme di conservazione generalizzata, si sono dimostrate fortemente attive e sono intervenute in materia tenendo in considerazione la giurisprudenza della CGUE, cogliendone le criticità o le zone grigie e i principi passibili di diverse interpretazioni, promuovendo così un dialogo – dai toni più o meno accesi – con i giudici di Lussemburgo.

Tutti aspetti, quelli rilevati, che non sono invece riscontrabili nel panorama italiano, né sotto il profilo dell'intervento normativo né di quello giurisprudenziale: sebbene nel nostro ordinamento non esista un ricorso diretto alla Corte costituzionale, come in Belgio, o una specifica Corte *ad hoc* deputata a dirimere controversie attinenti alla disciplina della conservazione e accesso ai metadati, come nel Regno Unito e che certamente rappresentano istituti e istituzioni che hanno facilitato le ONG e i cittadini a richiedere l'intervento dei giudici –, nondimeno anche nel contesto italiano si sono presentate molteplici occasioni nelle quali i giudici avrebbero avuto modo di pronunciarsi sulla conformità della disciplina in materia di *data retention* rispetto al diritto dell'UE e ai diritti riconosciuti peraltro non solo nell'ambito europeo bensì anche nella Costituzione italiana. La Corte di Cassazione, nei casi, in materia penale, sottoposti alla sua attenzione e analizzati nel Capitolo III, Parte III, pur avendo avuto l'occasione di rinviare alla CGUE o di promuovere l'intervento della Corte costituzionale, come richiesto dalle parti, si è sottratta ad una analisi più approfondita e problematizzata della disciplina della *data retention*, "fatica[ndo] nel dare il giusto peso alle questioni poste"[51]. Ciò appare del tutto singolare se si pensa non solo ai molteplici rinvii pregiudiziali promossi da colleghi di molti altri Stati europei, che hanno dimostrato di cogliere la complessità della disciplina, le criticità derivanti dalla giurisprudenza della CGUE e l'esigenza di dialogare con questa per addivenire a soluzioni interpretative chiare, ma anche alla profondità e acuta analisi che altre Corti hanno svolto in materia: il riferimento è alla Corte costituzionale belga, ad esempio, che nel rinvio pregiudiziale relativo alla Direttiva PNR ha mostrato una profonda conoscenza della tematica, della giurisprudenza dei giudici di Lussemburgo nonché delle interrelazioni tra sentenze in materia di trasferimento di dati e quelle in ambito di *data retention* di metadati.

Ciò che sembra mancare in Italia è dunque uno sguardo più ampio sul tema, che sappia andare oltre le singole esigenze del momento e che sappia controllare la tensione a reagire alle minacce alla sicurezza rafforzando strumenti di sorveglianza senza considerare come essi possano portare a serie conseguenze sui diritti fondamentali, da identificarsi primariamente nei diritti alla riservatezza e alla protezione dei dati ma non solo, ben potendo impattare anche sul diritto alla libertà di espressione e di associazione e, in ultima istanza, sulle fondamenta democratiche della società. Evitare di interrogarsi su questi aspetti e di valutarne la reale portata significa non rispondere ad una delle più significative sfide che il progresso tecnologico ha posto dinnanzi al mondo del diritto.

Se sotto il profilo normativo così come giurisprudenziale il caso italiano pare quindi una 'anomalia', che potrebbe peraltro esporre l'Italia stessa a procedure di infrazione laddove la Commissione decidesse di attivarsi per valutare il corretto adempimento del diritto dell'UE come interpretato dalla CGUE, la comparazione e lo studio delle vicende e degli approcci che hanno caratterizzato le scelte legislative così come gli interventi giurisprudenziali caratterizzanti altri Stati membri possono fornire un supporto particolarmente utile e significativo sia per i legislatori nazionali, nella direzione di attivare un processo di riforma che dia maggior rilievo e consideri le complessità della materia, quanto per i giudici, nel senso di spronarli a valutare con maggior profondità e precisione la giurisprudenza dell'UE e i suoi rilievi per

[51] I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *Sistema Penale*, 5, 2020, p. 185.

la disciplina italiana, anche alla luce dei rinvii pregiudiziali pendenti, il cui esito non potrà e non dovrà essere nuovamente ignorato o scarsamente considerato dalle Corti interne.

In conclusione, l'analisi comparata ha messo in luce molti aspetti di rilievo: essi si rivelano essere di grande utilità non solo per gli Stati membri stessi, che possono studiare proficuamente le soluzioni maggiormente virtuose promosse da altri ordinamenti e valutare la possibilità di inserirle nel proprio, così da modificare la propria disciplina nazionale in una maniera più conforme e vicina ai criteri indicati dalla CGUE, ma anche per le stesse Istituzioni dell'UE. Queste ultime infatti potrebbero imparare molto dallo sguardo comparato, prendendo atto delle concrete difficoltà di attuazione dei requisiti giurisprudenziali sanciti a livello europeo, difficoltà che Stati membri differenti, pur con approcci e caratteristiche ordinamentali diverse, sembrano condividere.

Tale analisi comparata inoltre permettere di muovere un'ulteriore e conclusiva considerazione circa le possibili prospettive future: confermando quanto già sottolineato al termine del Par. 1 delle presenti Conclusioni e alla luce, questa volta, di uno studio delle reazioni e posizioni degli Stati membri anziché delle Istituzioni dell'UE, pare potersi affermare che, qualora i giudici di Lussemburgo dovessero confermare l'incompatibilità di una *bulk data retention* con la Carta di Nizza anche rispetto a discipline fortemente tutelanti nella fase di accesso e anche rispetto a quelle per finalità di sicurezza nazionale, i legislatori nazionali e – almeno nel Regno Unito – anche i giudici potrebbero mostrare profonde resistenze e difficoltà nel rinunciare definitivamente a tale strumento. Si potrebbe creare così una nuova ed ulteriore situazione di frammentarietà nel panorama europeo, nel quale taluni Stati membri potrebbero tentare, ancora una volta, di riformare le proprie normative interne, cercando di introdurre forme di targettizzazione – o restrizione, se l'idea di una tale forma di conservazione dovesse essere accolta dalla CGUE –; mentre altri potrebbero decidere di non intervenire in alcun modo o di rafforzare unicamente le salvaguardie relative all'accesso, senza però intervenire più restrittivamente in materia di conservazione. Dinnanzi a tale scenario, diventerebbe determinante l'intervento di altre due Istituzioni dell'UE, diverse questa volta dalla CGUE: da un lato la Commissione che, mediante lo strumento della procedura di infrazione, potrebbe indurre gli Stati membri ad adeguare la disciplina nazionale ai criteri definiti dalla CGUE e dunque all'interpretazione da essa fornita dell'art. 15 Direttiva *e-Privacy*; dall'altro lato il legislatore dell'UE che, come ampiamente richiamato nel Par. 1, dovrebbe promuovere un nuovo intervento normativo in grado di stabilire quantomeno principi di riferimento condivisi per la creazione di un panorama legislativo armonizzato. Anche in quest'ultimo caso, che come si è visto pare piuttosto problematico e lontano dal realizzarsi, sembra che l'approccio e lo studio comparato possa garantire un fondamentale supporto al legislatore dell'UE, che potrebbe far tesoro delle esperienze virtuose e delle salvaguardie già riconosciute in taluni ordinamenti, quali il Belgio e (seppur in un contesto più complesso post-Brexit) il Regno Unito. Un intervento normativo a livello europeo potrebbe così risolvere anche le serie problematiche che derivano dalle forti disparità di tutele e garanzie offerte in taluni ordinamenti, come quello italiano, nei quali la riflessione in materia di bilanciamento tra esigenze securitarie e diritti fondamentali pare, sul fronte almeno della *data retention,* più proteso nella direzione di garantire l'efficienza dello strumento della conservazione.

4. Rileggere il rapporto sicurezza-riservatezza/protezione dei dati in un mondo digitalizzato attraverso la disciplina della **data retention***: perché escludere una lettura nell'ottica del* **trade-off** *è una delle più grandi sfide della modernità*

L'analisi della disciplina della *data retention* nelle sue molteplici sfaccettature, ha permesso di illuminare e mettere a fuoco numerosi aspetti di quel difficile trinomio 'Big Data-sicurezza-riservatezza/protezione dei dati', inizialmente individuato e che ha rappresentato il *fil rouge* di tutto l'elaborato. Così il percorso evolutivo esaminato sul piano normativo e giurisprudenziale tanto a livello

europeo quanto a livello nazionale negli Stati membri oggetto di approfondimento, spinge ora a riflettere, con più ampio respiro ed astraendo dallo specifico ambito della *data retention*, sulla possibilità di leggere il suddetto trinomio in una logica di *trade-off* o se, al contrario, l'Unione europea e gli Stati membri abbiano mostrato un approccio volto a scongiurare tale visione e a promuovere piuttosto un bilanciamento e una attenzione alla proporzionalità delle misure adottate.

Anche alla luce delle considerazioni conclusive svolte nei paragrafi precedenti, la lezione della *data retention* emerge con chiarezza: inizialmente il legislatore dell'UE, così come molti legislatori nazionali, avevano mostrato una forte tendenza 'pro-securitaria', motivata anche dalla sempre più preoccupante emergenza terroristica, proponendo una lettura del rapporto sicurezza-diritti fondamentali' molto più vicina alla logica del *trade-off*[52]. Le tutele e le salvaguardie rispetto ai diritti alla riservatezza e alla protezione dei dati previste in questa prima fase erano limitate, sia sul fronte interno, nel quale la DRD rifletteva la posizione di preminenza della 'data-collection' anziché della 'data-protection', sia nella dimensione esterna all'UE, come dimostrato dall'accordo *Safe Harbour* che poco o per nulla considerava l'incidenza e le rilevanti conseguenze per la tutela dei diritti derivanti dal possibile accesso e trattamento dei dati trasferiti negli USA da parte delle autorità pubbliche statunitensi.

Da questa prima fase, durante la quale si erano comunque registrate alcuni voci dissonanti – il Gruppo di lavoro art. 29 o il GEPD, ed alcune ONG –, l'intervento di Corti nazionali – si pensi al Tribunale costituzionale federale tedesco – e, conseguentemente, della CGUE hanno tuttavia determinato una significativa inversione di rotta nella direzione di una più attenta valutazione della proporzionalità e necessità delle ingerenze nella sfera privata, con una più limpida consapevolezza dei rischi che la logica di *trade-off* e la deriva 'pro-securitaria' possono comportare per lo Stato di diritto e la tutela dei diritti, grazie anche alle rivelazioni di Snodwen che hanno stimolato un più accesso e profondo dibattito in materia[53]. Tale fondamentale evoluzione, sebbene abbia condotto alla negazione di una visione di esclusione reciproca delle componenti del trinomio 'Big Data-sicurezza-riservatezza/protezione dei dati', non è ancora tuttavia giunta ad un punto conclusivo e al traguardo finale: nelle articolate vicende giurisprudenziali, nei rinvii ancora pendenti e nelle difficoltà e disomogeneità delle soluzioni adottate a livello nazionale ed europeo non è infatti ancora possibile individuare una determinazione chiara e definitiva del rapporto e del punto di equilibrio tra i diversi elementi del trinomio. Tale sfida, anzi, da quanto emerso, pare ancora aperta e, nonostante i molteplici interventi della CGUE, lontana dall'essere vinta. Le perplessità, i dubbi e le critiche che ancora caratterizzano la discussione dottrinaria, politica e giurisprudenziale in materia di *data retention* sono esemplificative della complessità delle questioni da risolvere[54], sotto le spinte forti di chi pone maggior attenzione alla efficacia delle soluzioni e degli strumenti impiegati nella lotta alla criminalità e al terrorismo, e chi invece sottolinea la irrinunciabile importanza di una solida garanzia dei diritti fondamentali.

---

[52] Per usare le parole di Posner e Vermeulen, la logica del *trade-off* risulta fondata sulla concezione secondo cui "respecting civil liberties has often real costs in the form of reduced security", in E. POSNER, A. VERMEULEN, *Terror in balance: security, liberty and the Courts*, Oxford University Press, 2007, p. 32. La concezione dunque che, soprattutto dopo gli attentati alle Torri Gemelle, si era affermata con decisione era quella di intendere una erosione della privacy e della protezione dei dati come necessario sacrificio per ottenere un più elevato livello di sicurezza.

[53] Sul punto è stato infatti affermato come "The classical 'national security v. civil liberties' debate was brought back to life by Snowden's disclosures and the resulting broader awareness of the global mass surveillance measures", A. DIMOTROVA, M. BRKAN, *Balancing national security and data protection: the role of EU and US policy-makers and Courts before and after the NSA affair*, in *Journal of Common Market Studies*, 4, 2018.

[54] Si pensi ad esempio alla visione fortemente critica di Epstein, che ha ritenuto erronea e del tutto sbilanciata a favore della tutela dei diritti fondamentali la posizione espressa dalla giurisprudenza della CGUE. Sul punto si rimanda al già richiamato scritto R. A. EPSTEIN, *The ECJ's fatal imbalance: its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European constitutional law review*, 12, 2016.

Quel che rileva però, al di là delle soluzioni e punti di equilibrio ancora precari ed instabili individuati ad oggi e in continuo assestamento, è che la logica del *trade-off* pare essere, nel contesto dell'UE, superata: è esemplificativo notare come EUROPOL abbia titolato il Report del suo Convegno, realizzatosi il 23 novembre 2018, "*Freedom AND security. Killing the zero sum process*", a sottolineare come, usando le parole dell'allora Executive Director Catherine DeBolle "we do not have to choose either freedom or security. There is no need to compromise on individual privacy for the sake of public security". Similmente anche il GEPD, rappresentativo di un approccio e di finalità ben differenti da quelle di EUROPOL, ha evidenziato una forte consapevolezza quanto alle difficoltà operative ed applicative di criteri e limiti individuati dalla CGUE, quali la *targeted data retention*, mostrando così una attenzione concreta alle esigenze securitarie e alla realizzabilità operativa di soluzioni che non debbono sacrificare totalmente l'efficacia degli strumenti di garanzia della sicurezza[55].

Questo rilevato superamento di un approccio 'oppositivo' si manifesta quale frutto del difficile e travagliato percorso intrapreso dalla Corte di giustizia dell'UE così come delle Corti nazionali, anche mediante un dialogo multilivello, che procedono nella direzione – e nella vocazione – di garantire strumenti utili alla lotta alla criminalità, salvaguardando al contempo i diritti fondamentali e i valori e principi democratici delle nostre società, senza addivenire alla rinuncia unidirezionale della sicurezza a favore dei diritti fondamentali o viceversa: è questo dunque il punto di partenza dal quale ragionare nella determinazione di quei criteri e requisiti di proporzionalità che sono ancora in cerca chiara definizione.

Addivenire a tale risultato di esclusione della logica di *trade-off*, che, come si è visto, è ancora tutt'altro che scontato e fissato una volta per tutte, risultando al contrario continuamente messo alla prova dinnanzi alle spinte contrapposte che pur persistono, ha implicato ed implica innanzitutto un non semplice esercizio di valutazione degli elementi che costituiscono il trinomio. Se si compone infatti il rapporto tra sicurezza e riservatezza/protezione dei dati nei termini di un interesse collettivo – la sicurezza appunto – avverso un diritto meramente individuale, tale visione non potrà che comportare una lenta erosione delle libertà personali e dei diritti alla riservatezza e protezione dei dati in particolare, intesi nella loro dimensione meramente individuale e pertanto 'barattabili' e rinunciabili in cambio di una maggiore – e presunta – sicurezza collettiva. Abbandonare quindi una tale visione, che conduce ad abbracciare la logica del *trade-off*, significa riconoscere in primis ai diritti alla riservatezza e alla protezione dei dati un valore ulteriore e più profondo, emancipandoli da quella concezione unicamente soggettiva, relegata alla sola tutela della sfera privata, e intendendoli quali precondizione per il godimento di libertà e diritti fondamentali o, se non si vuole arrivare a tale posizione, cogliendone quantomeno l'intrinseca connessione e legame con altri diritti fondamentali quali la libertà di espressione, di associazione, di libera formazione e manifestazione del pensiero e dei propri convincimenti, che sono 'liberi' quando non condizionati dal timore di un controllo del potere pubblico sulle proprie comunicazioni, sui propri legami con altri soggetti, sulle proprie abitudini o sui luoghi frequentati. In questo senso vanno lette le parole di Rodotà che ha affermato, già nel 2004, con lucidità ed incisività come "La privacy si presenta come un elemento fondamentale della società dell'eguaglianza. Senza una forte tutela dei dati riguardanti le convinzioni politiche o l'appartenenza a partiti, sindacati, associazioni, i cittadini rischiano di essere esclusi dai processi democratici: così la privacy diventa una condizione essenziale per essere inclusi nella società della partecipazione. Senza

[55] Nelle *Pleading notes* presentate dal GEPD in occasione dell'udienza relativa ai rinvii pregiudiziali promossi dai giudici inglesi, belgi e francesi, si legge infatti come "in the specific context of retention of electronic communications data, it might not be possible to identify in advance those data subjects (or categories of data subjects) whose information may at some point in the future become part of a criminal investigation, for example victims of serious crime" (p. 11). Anche il GEPD dunque riconosce il problematico aspetto legato alla *data retention* che mal si presta, per sua natura e salvo una rinuncia sostanziale delle proprie potenzialità, ad una preventiva limitazione: così, se una forma generalizzata di conservazione dei dati non può essere considerata conforme al diritto dell'UE, una tipologia legittima di *data retention* può ravvisarsi in un forma di conservazione "limited yet effective".

una forte tutela del 'corpo elettronico', dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo. Diventa così evidente che la privacy è uno strumento necessario per difendere la società della libertà e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale"[56]. Se si parte dunque da questa concezione, che Solove denomina, non a caso, "pluralistic conception of privacy", e se si arriva a ritenere la privacy e la protezione dei dati come portatori non solo di una dimensione individuale ma anche di una collettiva[57] (un "social value", per richiamare Solove[58]), ne consegue allora che non può più funzionare ed essere accolta quella logica che vede comunque remissivi tali diritti fondamentali dinnanzi alla esigenza di garantire la sicurezza dei consociati e che conduce pertanto ad una visione di *trade-off*, in cui la tutela della sicurezza equivale necessariamente ad un abbassamento delle salvaguardie garantite in materia di riservatezza e *data protection*.

Da questo primo riconoscimento, che passa appunto per l'affermazione e attribuzione di un significato più ampio e 'collettivo' ai due diritti di riferimento, diviene così necessario prendere le distanze anche da una lettura inversa della medesima equazione: quella cioè che porta a rinvenire in una rinuncia dei propri diritti e delle salvaguardie ad essi preposte una conseguente maggiore garanzia della sicurezza. Il superamento di tale visione, che risulta forse operazione ancor più delicata, passa necessariamente per uno studio ed una riflessione che imparino a ragionare sul concetto di efficacia e necessità degli strumenti a garanzia della sicurezza utilizzati, così da verificare che realmente ad una compressione e sacrificio dei diritti discenda la possibilità di adottare sistemi più efficaci e che il medesimo risultato in termini di garanzia della sicurezza e lotta alla criminalità non possa essere ottenuto diversamente e ricorrendo a strumenti meno invasivi. Questo per scongiurare così il rischio di cedere

---

[56] S. RODOTÀ, *Privacy, libertà, dignità*, 2004, in www.garanteprivacy.it. Merita anche ricordare come Rodotà abbia riconosciuto e sottolineato l'importanza della tutela del corpo elettronico: "pezzi di ciascuno di noi sono conservati nelle numerosissime banche dati dove la nostra identità è sezionata e scomposta, dove compariamo come consumatori, ora come elettori, debitori, lavoratori e così via (..). Siamo distribuiti nel tempo e nello spazio. Ma questa, che per il corpo fisico rimane una soluzione eccezionale, è ormai la condizione essenziale di ogni persona", S. RODOTÀ, *La vita e le regole*, Feltrinelli, 2006, p. 81.

[57] Anche de Vergottini sottolinea, su questo punto, come: "non è possibile tenere separati i due profili in quanto la protezione dei dati comporta ad un tempo la tutela di profili individuali e collettivi", G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della 'emergenza normalizzata'*, in *Rivista AIC*, 4, 2019, p. 66. Similmente, molti autori hanno sottolineato il legame tra diritti alla privacy e alla protezione dei dati ed altri diritti e libertà fondamentali: Zedner ha affermato come "protection of privacy lies at the heart of a free and democratic society and, as the NSA-affair made all too clear, mass surveillance has the potential for abuse of the information gathered against political adversaries and damaging effects on press freedom, freedom of speech and open political debate", L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the UK after the European Data Retention*, in R. A. MILLER, *Privacy and power. A transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, 2017, p. 584. Anche Richards ha evidenziato l'impatto determinante che un sistema di sorveglianza massiva e dunque forme di ingerenza nella sfera privata provocano rispetto al carattere democratico della società: "Free minds are the foundation of a free society and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse", N. RICHARDS, *The dangers of surveillance*, in *Harvard Law Review*, 126, 2013. Similmente, "the practice of law enforcement agencies of mining raw data, until some criminal pattern emerges to their mind, brings back the shadows of inquisitorial justice systems more typical of totalitarian countries than healthy democracies", A. SERENA, *The Leviathan, the chains, the lock: dynamics of power in the digital surveillance state*, in *MediaLaws*, Working Paper Series, 8, 2017. Anche Rouvroy e Poullet hanno posto in evidenza come "privacy and data protection regimes are not there merely to protect the best rights holders' interests, but are necessary in a democratic society to sustain a vivid democracy", A. ROUVROY, Y. POULLET, *The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy*, in S. GURTWIRTH et al. (eds.), *Reinventing data protection?*, Springer, 2009, p. 57. Nel contesto italiano, come già richiamato nel Capitolo I, Parte I, Flick giunge a sostenere che "la privacy e l'identità del singolo sono fattori coessenziale alla sua dignità", G. M. FLICK, *Elogio della dignità (se non ora, quando?)*, in *Rivista AIC*, 4, 2014.

[58] Ma anche K. HUGHES, *The social value of privacy, the value of privacy to society and human right discourse*, in B. ROESSLER, D. MOKROSINKA (a cura di), *Social dimensions of privacy. Interdisciplinary perspectives*, Cambridge University Press, 2015.

alla "illusory conviction that global surveillance is the deus ex machine capable of combating the scourge of global terrorism"[59] e che quindi forme più pervasive di controllo delle comunicazioni e dei dati e metadati prodotti comportino necessariamente ed automaticamente un più elevato grado di efficacia delle misure poste in essere nella lotta alla criminalità e alle minacce allo Stato.

Questo è in realtà un punto ancora molto dibattuto, sotto certi aspetti ostico e rispetto al quale giudici e legislatori riscontrano difficoltà a giungere a visioni condivise e chiare: con riferimento allo strumento della *data retention*, che può costituire anche sotto tale profilo un osservatorio privilegiato, si scontrano le opinioni di chi ritiene la conservazione di tipo generalizzato uno strumento assolutamente vincente, che consente, diversamente dalle possibili alternative, quali la *data preservation*, di tornare indietro nel tempo, in un'epoca in cui ormai il passato è rinvenibile principalmente nei dati digitali[60]; e chi invece, come Scheinin, rinviene proprio nell'eccesso di informazioni e dati uno strumento che rallenta e pregiudica l'efficacia delle attività svolte da autorità di *law enforcement* e intelligence[61]. Questo dibattito, che dovrebbe fondarsi ed alimentarsi di dati e studi, rimane ancora aperto: nonostante con riferimento alla *data retention* questo profilo sia stato poco toccato dalle valutazioni di legislatori e Corti, che molto spesso hanno fatto riferimento a documenti di parte anziché promuovere un approfondimento quanto più possibile oggettivo, a parere di chi scrive proprio tali riflessioni rappresentano un punto di grande valore e rilevanza al fine non solo di confutare o confermare più correttamente l'equivalenza che vede nella maggiore ingerenza nella sfera privata una conseguente maggiore sicurezza ed efficienza degli strumenti di lotta alla criminalità e al terrorismo, ma anche al fine di valutare in maniera adeguata la proporzionalità delle misure adottate o da adottare; la comprensione infatti degli obiettivi che uno strumento è in grado di ottenere e dunque la determinazione della capacità e idoneità a perseguire un interesse legittimo, divengono elementi importanti nel corretto svolgimento di quel già complesso esercizio di bilanciamento e determinazione della proporzionalità dell'ingerenza nella sfera privata e nei diritti fondamentali[62].

Senza dubbio valutazioni di questo tipo scontano, nell'attuale contesto, ulteriori elementi di complessità: il progresso tecnologico e lo sviluppo di sistemi automatizzati e fondati su strumenti di Intelligenza Artificiale, incrementano quella visione e tentazione che rinviene in tali automatismi sofisticati dei mezzi infallibili ed oggettivi, che consentono, spesso senza che ciò sia posto in discussione, un miglior funzionamento e una maggiore efficienza. In realtà, come si è messo ampiamente in evidenza nel Capitolo I, Parte I, anche tali nuove ed avanzate tecnologie, per quanto

[59] Concurring Opinion del giudice della Corte EDU Pinto de Albuquerque nella pronuncia *Szabo*, par. 20.

[60] Drewery riporta uno studio della Commissione del 24 luglio 2013, n. 6 evidence for necessity of data retention in the EU, dove la "German federal police and state police reported in 2011: for 44,5% of the cases involving requests for historical data traffic, there was no other means of conducting investigations", L. DREWRY, *Crimes without culprits: why the EU needs data retention and how it can be balanced with the right to privacy*, in *Wisconsin international law journal*, 33, 2015.

[61] Con riferimento agli attentati terroristici che hanno colpito Parigi nel 2015, "The fact that the attack came as a surprise demonstrates a failure of intelligence coordination internally in France and in Belgium, and between those two neighbouring EU countries. More broadly, it demonstrates a failure of the collect-it-all mentality, whereby any unmonitored modalities of communication are seen as an unknown security threat worth any investment of money, personnel and political influence – often to the detriment of taking action in respect of known security threats, such as individuals already suspected of preparing acts of terrorism", M. SCHEININ, *Towards evidence-based discussion on surveillance: a rejoinder to Richard A. Epstein*, in *European Constitutional Law Review*, 12, 2016, p. 347.

[62] Sul punto si vogliono richiamare le considerazioni dell'Avvocato generale Saugmandsgaard Øe nel caso *Tele2*: "il requisito di proporzionalità stricto sensu consiste nel bilanciare i vantaggi risultanti da tale misura alla luce dell'obiettivo legittimo perseguito con gli inconvenienti che ne derivano alla luce dei diritti fondamentali garantiti in una società democratica. Tale requisito dà luogo, pertanto, a un dibattito sui valori che devono prevalere in una società democratica e, in definitiva, sul tipo di società in cui vogliamo vivere", par. 248. In questo senso una riflessione sui vantaggi e dunque anche sulla capacità della misura di raggiungere l'obiettivo, diviene parte importante del vaglio di proporzionalità che legislatori e Corti sono chiamati ad effettuare.

ricche di indubbie potenzialità positive, sono suscettibili di errori e pregiudizi, come le riflessioni sul *bias* che colpisce gli algoritmi hanno dimostrato. Del resto anche la CGUE stessa ha confermato questo profilo nel *Parere 1/15* quando ha richiesto interventi normativi decisi e volti a stabilire criteri in grado di determinare correttamente il funzionamento degli algoritmi posti alla base dei controlli preventivi automatizzati sui PNR di passeggeri in arrivo e che garantiscano il funzionamento non discriminatorio di tali sistemi, indirettamente riconoscendo l'esistenza concreta di tale pericolo. E proprio per questo che, in un contesto di pervasivo e rapido progresso tecnico-scientifico, diviene ancora più importante ragionare con profondità sul concetto di efficacia e di idoneità degli strumenti disposti, tenendo bene e chiaramente in considerazione l'impatto dirompente che il terzo elemento del trinomio, ovvero i Big Data e dunque, in generale, la tentazione che deriva dalle nuove tecnologie e da un loro utilizzo ampio, determina rispetto alla individuazione di un punto di equilibrio tra sicurezza e diritti fondamentali: come ben riassunto da Broeders, "Technological progress and the political prioritisation of security however do not develop in a vacuum. There is a context of laws and regulations and public scrutiny and debate. In constitutional states the watchers are being watched. However, the combination of new technology and securitisation also leads to various degrees of complexity and institutional secrecy that hampers the ability of lawmakers, oversight authorities and the general public to form informed views on what is going on"[63].

In conclusione, le riflessioni sopra svolte e il percorso delineato, inducono ad affrancarsi da una lettura della combinazione dei tre elementi che compongono il complesso trinomio 'Big Data-sicurezza-riservatezza/protezione dei dati' in termini di *trade-off*, imponendo una seria riflessione sull'impatto e sulla rilevanza di ciascuna singola voce del trinomio, in modo da comprenderne il valore e da evitare che nessuna di esse venga sacrificata innanzi alle altre. Se da un lato sarebbe del tutto utopistico credere di poter contrastare forme di criminalità grave senza ricorrere all'impiego delle nuove tecnologie e dei Big Data, nondimeno risulta irrealistico e non corretto, alla luce delle considerazioni svolte, leggere sicurezza e riservatezza/protezione dei dati in termini assoluti e come elementi in irriducibile contrasto[64]. In questo senso dunque "The relation between privacy and security is not a trade-off between two incompatible values. Strong privacy and data protection – which implies, for instance, data security and data minimisation – can benefit law enforcement. The challenge is to include synergies in the decision-making"[65].

---

[63] D. BROEDERS, *Quis Custodiet Ipsos Custodes: Security, Big Data and Secrecy*, in *European data protection law review*, 3, 2017.

[64] Come richiamato da Crespi (S. CRESPI, *The applicability of Schrems principles to the Member States: national security and data protection within the EU context*, in *European Law Review*, 5, 2018), l'art. 6 della Carta di Nizza, sulla base del quale ognuno ha diritto alla libertà e alla sicurezza, suggerisce una complementarietà di tali diritti, così che la garanzia della sicurezza deve rispettare i diritti e le libertà fondamentali e viceversa le libertà e i diritti non debbono essere intesi come inderogabili ed assoluti dinnanzi alle esigenze securitarie.

[65] H. HIJMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 16 TFEU*, Springer, 2016. Dello stesso avviso anche Ojanen: "one of the major lessons from *DRI* and *Schrems* is that the trade-off between privacy and security *in abstracto* should be rejected. Instead, there should be a systematic and rigorous case-by-case assessment of surveillance in accordance with the permissible limitations test in which the system for the protection of fundamental rights provides the framework for balancing, by way of applying the test of permissible limitations and the requirement of proportionality in that process *in concreto*, save occasions on which the essence of a fundamental right is triggered by surveillance", T. OJANEN, *Rights-based review of electronic surveillance after Digital Rights Ireland and Schrems in the European Union*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, 2017, p. 18. Anche Orofino, con riferimento al rapporto tra sicurezza e riservatezza afferma come esso non possa essere letto nel senso di "comportare l'integrale sacrificio dell'uno o dell'altra posizione giuridica tutelata", M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws*, 2, 2018.

Partendo da questa premessa, la vera grande sfida quindi è quella di determinare con chiarezza e in maniera univoca i confini e le tutele necessarie per far concretamente sì che sicurezza, riservatezza e protezione dei dati coesistano nel mondo dei Big Data[66].

L'analisi della disciplina della *data retention* nell'Unione europea e negli Stati membri ha permesso di comprendere come una tale coesistenza sia possibile, sebbene difficile da ottenere e come siano necessari enormi sforzi per determinare spesso provvisori punti di equilibrio, dimostrando come la sfida accettata e colta nel contesto europeo, volta a scongiurare il rischio di cedere sia alla tentazione di una garanzia della sicurezza a tutti i costi, sia ad una anacronistica ed irrealizzabile tutela dei diritti fondamentali incapace di fare i conti con le ineludibili esigenze securitarie, sia destinata ad occupare ancora per molto tempo Corti e legislatori, nazionali ed europei[67]. Se è vero che "there are few words more dangerously confusing in their meaning than 'liberty' and 'security'"[68] e che le insidie derivanti da un ulteriore termine, quello dei Big Data e delle nuove tecnologie hanno ulteriormente complicato il panorama entro cui l'Unione europea e gli Stati membri si sono trovati ad operare, è altrettanto vero che nelle vicende che hanno caratterizzato la regolamentazione della *data retention* è possibile rinvenire un momento importantissimo e forse ineguagliato in cui l'UE, le sue Istituzioni e gli Stati membri nel dialogo multilivello hanno riflettuto profondamente, non senza difficoltà, sul trinomio di cui si è così ampiamente parlato e sul come integrare la protezione dei dati e della privacy nell'epoca dei Big Data e di fronte alla necessità della garanzia della sicurezza resa sempre più presente e pressante. La determinazione di criteri e requisiti volti a garantire forme di utilizzo dello strumento della conservazione dei metadati che siano efficaci ma anche rispettose dei diritti fondamentali indica che è possibile, per quanto complesso, trovare punti di equilibrio e far coesistere esigenze differenti anche in un ambito, come quello della *data retention*, tanto delicato ed in continuo divenire[69]. Evitare di cadere in una logica del *trade-off*, più semplicistica ma molto pericolosa, e alimentare quel dibattito multilivello tra UE e Stati membri, tra legislatori e Governi, tra Parlamenti e Corti, tra Autorità garanti e autorità di *law enforcement*, tra sviluppatori di nuove tecnologie e giuristi, tra Corti nazionali e CGUE, necessario per individuare un punto di equilibrio e una coesistenza tra differenti tensioni, diviene senza dubbio uno degli sforzi di maggior rilievo che il mondo del diritto deve e dovrà sostenere in futuro.

---

[66] "Security, privacy and fundamental rights must be realized together and not at the cost of one another", S. GUTWIRTH, K. DE VRIES, R. SAELENS, *Veiligheid legitimeert niet alle middelen*, in *Juristenkrant*, 24 marzo 2010, 12, tradotto da F. Peeraer.

[67] "The correct balance to be struck between the interests protected by the right to data protection and whether the curtailment of some aspects of that right constitutes a necessary and proportionate measure to protect security will continue to be subject of debate for many years to come" Y. MCDERMOTT, *Conceptualising the right to data protection in an era of Big Data*, in *Big Data & Society*, 1, 2017, p. 4.

[68] C. GEARTY, *Escaping Hobbes: liberty and security for our democratic (not anti-terrorist) age*, in *LSE Working Papers*, 3, 2010.

[69] Intessante è la provocazione pronunciata da Vermeulen in occasione della Conferenza di EUROPOL sopra richiamata e riportata nel relativo Report: "With a bit of creativity, it is possible to come to a good set of selectors which make your life easy for the future. Not as easy as receiving everything without having to do anything, but my invitation is: why don't you give it a try?".

BIBLIOGRAFIA

- G. AGAMBEN, *Stato di eccezione,* Bollato-Boringhieri, 2003.

- AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, *Twelve Operational Fundamental Rights Considerations for Law Enforcement When Processing Passenger Name Record (PNR) Data*, gennaio 2015.

- AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume I: Member States' legal framework*, 2017.

- AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, *Big Data: discrimination in data-supported decision making*, 2018.

- AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019.

- AGENZIA DELL'UNIONE EUROPEA PER I DIRITTI FONDAMENTALI, *Coronavirus pandemy in the EU. Fundamental rights implications*, 2020.

- G. ALPA, B. MARKESINIS, *Il diritto alla privacy nell'esperienza di common law e nell'esperienza italiana,* in *Rivista trimestrale di diritto civile e procedura civile*, 1974.

- P. ALSTON, UN Special Rapporteur on extreme poverty and human rights, *Report A/74/493*, 11 ottobre 2019.

- C. ALVISI, *I trattamenti nel settore bancario, finanziario e assicurativo,* in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, Editoriale Scientifica, 2017.

- C. ALVISI, *Dati personali e diritti dei consumatori*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, Giappichelli, 2019.

- A.C. AMATO MANGIAMELI, *Algoritmi e big data. Dalla carta sulla robotica,* in *Rivista di filosofia del diritto*, 1, 2019.

- E. ANCONA, *Soggettività, responsabilità, normatività 4.0. Profili filosofico-giuridici dell'intelligenza artificiale*, in *Rivista di Filosofia del Diritto*, 1, 2019.

- D. ANDERSON, *A Question of* Trust, 2015, https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

- E. ANDOLINA, *L'acquisizione nel processo penale dei dati 'esteriori' delle comunicazioni telefoniche e telematiche*, Cedam, 2018.

- M. ANDREJEVIC, *Infoglut: how too much information is changing the way we think and know*, Routledge, 2013.

- M. ANDREJEVIC, *Surveillance in the Big Data era*, in K. PIMPLE (a cura di), *Emerging pervasive information and communication technologies*, Springer, 2014.

- M. ANDREJEVIC, *Surveillance in the big data era. Emerging pervasive information and communications technologies*, in *Law, Governance and Technology Series*, 11, 2014.

- A. ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014.

- E. ARTEMIOU, *The way out of Digital Rights Ireland*, in *CiTiP Blog*, University of Leuven, 19 giugno 2018.

- E. ASSANTE, *Cosa ci può insegnare il caso Cambridge Analytica*, in *federalismi.it*, 9, 2018.

- M. AZARMI, *European Court of Human Rights to reexamine bulk collection*, in *European Union Security & Surveillance*, 4 marzo 2019.

- G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, 2019.
- A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, 1974.

- F. BALDUCCI ROMANO, *La protezione dei dati personali nell'UE tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario*, 6, 2015.

- R. BARBERIO, *Parliamo di Russia ma la vera anomalia sul 'data retention' è l'Italia*, in *HuffingtonPost*, 5 luglio 2018.

- M. BARBERIS, *Liberté, égalité, sécurité. Gli equivoci della guerra al terrore*, in *Il Mulino*, 4, 2016.

- E. BARONCINI, *L'Unione europea e la procedura di conclusione degli accordi internazionali dopo il Trattato di Lisbona*, in *Cuadernos de Derocho Transnacional*, 1, 2013.

- M. BASSINI, L. LIGUORI, O. POLLICINO, *Sistemi di Intelligenza Artificiale, responsabilità e accountability. Verso nuovi paradigmi?*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018.

- M. BASSINI, *La Corte di giustizia e la conservazione dei dati. Spunti di una rilettura 'postuma'*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, in corso di pubblicazione.

- Z. BAUMAN, D. LYON, *Liquid surveillance. A conversation*, Polity Press, 2013.

- J.P. BELAND e al., *Big Data for agri-food 4.0: application to sustainability management for by-products supply chain*, in *Computers in Industry*, 1, 2019.

- D. BENDER, *What you need to know about NSA mass acquisition of telephony metadata*, in *Computer and Internet Lawyer*, 9, 2013.

- D. BENDER, *The Judicial Redress Act: A Path to Nowhere*, in *Privacy Advisor*, Issue 17, 2015.

- L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, in *German Law Journal*, 6, 2015.

- C. BENNETT, R. BAYLEY, *Privacy protection in the era of 'big data': regulatory challenges and social assessments*, in B. VAN DER SLOOT, D. BROEDERS, E. SCHRIJVERS (a cura di), *Exploring the boundaries of Big Data*, Amsterdam University Press, 2016.

- J. BENTHAM, *Panopticon or the inspection-house*, Payne, 1791.

- E. BERTOLINI, *Is technology really inclusive? Some suggestions from States run algorithmic programmes*, in *Global Jurist*, 1, 2020.

- E. BIANDA, *Riconoscimento facciale e capitalismo della sorveglianza*, in *Problemi dell'informazione*, 2, 2019.

- F. BIGNAMI, *Protecting privacy against the Police in the European Union: the Data Retention Directive*, in AA VV., *Melanges en l'honneur de Philippe Leger*, Editions Pedone, 2006.

- F. BIGNAMI, *Privacy and law enforcement in the European Union: the Data Retention Directive*, in *Chicago Journal of International Law*, 1, 2007.

- F. BIGNAMI, G. RESTA, *Transatlantic privacy regulation: conflict and cooperation*, in *Law and contemporary problems*, 4, 2015.

- F. BIGNAMI, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Study for the LIBE Committee, 2015.

- G. BISCONTINI et al., *Le tecnologie al servizio della tutela della vita e della salute e della democrazia. Una sfida possibile*, in *federalismi.it – Osservatorio emergenza Covid-19*, 23 marzo 2020.

- E. BLOUNSTEIN, *Privacy as an aspect of human dignity*, in *New York University Law Review*, 39, 1964.

- F. BOEHM, M. COLE, *Data Retention after the judgement of the Court of Justice of the European Union*, The Greens in the EP Working Paper, 2014.

- P. BONETTI, *Terrorismo, emergenza e costituzioni democratiche*, Il Mulino, 2006.

- A. BONFANTI, *Big data e polizia predittiva: riflessioni in tema di protezione del diritto alla privacy e dei dati personali*, in *MediaLaws*, 3, 2018.

- S. BONFIGLIO, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Diritto e Sicurezza*, 3, 2014.

- M. BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti 'violabili' in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 3, 2016.

- F. BORGIA, *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in *Il mercato unico digitale*, Numero Speciale 2017 della rivista *Diritto Mercato e Tecnologia*, 2017.

- M. BOTTA, M. VIOLA DE AZEVEDO CUNHA, *La protezione dei dati personali nelle relazioni tra UE e USA, le negoziazioni sul trasferimento dei PNR*, in *Il Diritto dell'Informazione e dell'Informatica*, 2, 2010.

- C. BOWDEN, *The US Surveillance programmes and their impact on EU citizens' fundamental rights*. *Note to the European Parliament*, 2013.

- A. BRADFORD, *The Brussels effect*, in *Northwestern University Law Review*, 1, 2012.

- F. BRAVO, *Il consenso e le altre condizioni di liceità del trattamento dei dati personali*, in G. FINOCCHIARO (a cura di), *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali*, Zanichelli Editore, 2017.

- P. BREYER, *Telecommunications data retention and human rights: the compatibility of blanket traffic data retention with the ECHR*, in *European Law Journal*, 3, 2005.

- D. BRIN, *The transparent society. Will technology force us to choose between privacy and freedom?*, Perseus Books, 1998.

- M. BRKAN, *The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning,* in *German Law Journal*, 20, 2019.

- M. BRKAN, *The unstoppable expansion of the EU fundamental right to data protection. Little shop of horrors?*, in *Maastricht Journal of European and Comparative Law*, 5, 2016.

- D. BROEDERS, *Quis Custodiet Ipsos Custodes: Security, Big Data and Secrecy*, in *European data protection law review*, 3, 2017.

- K. BRONSON, I. KNEZEVIC, *Big Data in food and agriculture*, in *Big Data and Society*, 1, 2016.

- E. BROUWER, *Ignoring Dissent and Legality. The EU's Proposal to Share the Personal Information of All Passengers*, in *CEPS Paper in Liberty and Security in Europe*, 2011.

- E. BRUGIOTTI, *La privacy attraverso le 'generazioni dei diritti'. Dalla tutela della riservatezza alla protezione dei dati personali fino alla tutela del corpo elettronico*, in *Dirittifondamentali.it*, 2, 2013

- B. BUCKLEY, M. HUNTER, *Say cheese! Privacy and facial recognition*, in *Computer Law and Security Review*, 6, 2011.

- T. BUNYAN, *Analysis mass surveillance of communications in the EU: CJEU Judgement and DRIPA 2014/RIPA 2000 in the UK*, Statewatch, 2014, https://www.statewatch.org/media/documents/analyses/no-252-mand-ret-dripa-ripa.pdf.

- G. BUQUICCHIO, *Aspetti internazionali della protezione dei dati: il ruolo svolto dal Consiglio d'Europa*, in A. MATTEUCCI, *Privacy e banche dati*, Il Mulino, 1981.

- A. BUTLER, F. HIDVEGI, *From Snowden to Schrems: how the surveillance debate has impacted US-EU relations and the future of international data protection*, in *Seton Hall Journal of Diplomacy and International Relations*, Special Issue 2015/2016.

- G. BUTTARELLI, *The Commission proposal for a Regulation on e-Privacy: why do we need a Regulation dedicated to e-Privacy in the European Union*, in *European Data Protection Law Review*, 3, 2017.

- R. CABAZZI, *Irish High Court e Corte di giustizia europea: un nuovo dialogo sul trasferimento di dati da Facebook Ireland a Facebook Inc.*, in *MediaLaws*, 1, 2018.

- A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, 2019.

- F. CAGGIA, *Libertà ed espressione del consenso*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, Giappichelli, 2019.

- G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Medialaws*, 2, 2018.

- L. CALIFANO, *Privacy e sicurezza*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli, 2013.

- L. CALIFANO, *Privacy e sicurezza*, in *Democrazia e Sicurezza*, 3, 2013.

- L. CALIFANO, *Introduzione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, Editoriale Scientifica, 2017.

- L. CALIFANO, *Il Reg. UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Editoriale Scientifica, 2017.
- L. CALIFANO, in *Brevi riflessioni su privacy e costituzionalismo al tempo dei big data*, in *federalismi.it*, 9, 2017.

- L. CALIFANO, *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, 2018.

- I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 54, 2017.

- J. CANNATACI, V. FALCE, O. POLLICINO, *Legal challenges of Big Data*, Elgar, 2020.

- G.A. CANNETTI, *Passenger Name Records tra istanze di sicurezza globale e tutela dei dati personali*, in *I quaderni europei. Il diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, 63, 2014.

- P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1, 2016.

- A. CARDONE, *La "normalizzazione" dell'emergenza*, Giappichelli, 2011.

- T. CARNEY, *The new digital future for welfare: debts without legal proofs or moral authority?*, in *UNSW Law Journal Forum*, 1, 2018.

- M. CAROLAN, *Publicising food: Big Data, precision agriculture and co-experimental techniques of addition*, in *Sociologia Ruralis*, 2, 2017.

- E. CARPANELLI, N. LAZZERINI, *PNR: problems not resolved? The EU PNR conundrum, after Opinion 1/15 of the CJEU*, in *Air and Space Law*, 42, 2017.

- S. CARRERA, E. GUILD, *The end of Safe Harbor: what future for EU-US data transfers?*, in *Maastricht Journal of European and Comparative law*, 3, 2015.

- S. CARRERA, E. GUILD, *Safe Harbour or into the Storm? EU-US Data transfer after Schrems Judgement*, in *CEPD Liberty and Security in Europe Papers*, novembre 2015, https://www.ceps.eu/system/files/CEPS_LSE_85.pdf.

- P. CARROZZA, *La Cour d'Arbitrage belga*, in G. F. FERRARI, A GAMBARO (a cura di), *Corti nazionali e comparazione giuridica*, ESI, 2006.

- M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione Europea*, in M. CARTABIA (a cura di), *I diritti in azione*, Il Mulino, 2007.

- J. CAS, R. BELLANOVA, J. P. BURGESS, M. FRIEDWALD, W. PEISSL, *Introduction: Surveillance, privacy and security*, in J. CAS, R. BELLANOVA, J. P. BURGESS, M. FRIEDWALD, W. PEISSL (a cura di), *Surveillance, privacy and security: Citizens' perspectives*, Routledge, 2017.

- C. CASONATO, *Potenzialità e sfide dell'intelligenza artificiale*, in *BioLaw Journal*, 1, 2019.

- G. CASSANO (a cura di), *Nuovi diritti della persona e risarcimento del danno*, Tomo I, Giappichelli, 2003.

- A. CASSART, J-F. HENROTTE, *L'invalidation de la directive 2006/24 sur la conservation des donnèes de communication èlectronique oy la chronique d'une mort annoncée*, in *Jurisprudence de Liege, Mons et Bruxelles*, 20, 2014.

- E. CELESTE, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019.

- M.J. CEPEDA ESPINOSA, *Privacy*, in M. ROSENFELD, A. SAJO, *The Oxford handbook of comparative constitutional law*, Oxford University Press, 2013.

- A. CHANDER, *The racist algorithm?*, in *Michigan Law Review*, 115, 2017.

- H. CHO, D. IPPOLITO, Y. YU, *Contact tracing mobile apps for Covid-19: privacy considerations and related trade-offs*, in *arXiv*, 2020.

- T. CHRISTAKIS, *A fragmentation of EU/ECHR law on mass surveillance: initial thoughts on the Big Brother Watch Judgement*, in *European Law blog*, 20 settembre 2018.

- F. CLEMENTI, G. TIBERI, *Sicurezza interna, diritti e cooperazioni internazionale nella lotta al terrorismo*, in *Astrid-online.it*, 1, 2013.

- C. COCQ, F. GALLI, *Comparative law paper on data retention regulation in a sample of EU Member States* (Deliverable 4.3 of the EU Project Surveille), 2013.

- D. COLE, F. FABBRINI, *Bridging the transatlantic divide? The United States, The European Union and the protection of privacy across borders*, in *International journal of constitutional law*, 1, 2016.

- D. COLE, F. FABBRINI, *Transatlantic Negotiations for Transatlantic Rights: Why an EU-US Agreement is the Best Option for Protecting Privacy Against Crossborder Surveillance*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, 2017.

- M. COLE, *We are all foreigners: NSA spying and the rights of others*, in *Just security blog*, 29 ottobre 2013.

- M. COLE, F. BOEHM, *EU Data Retention – Finally abolished? Eight years in light of Article 8*, in *Critical Quarterly for Legislation and Law*, 1, 2014, pp. 58-78.

- M. COLE, A. VANDENDRIESSCHE, *From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabo/Vissy in Strasbourg: what the ECtHR made of the deep pass by the CJEU in the recent cases on mass surveillance*, in *European Data Protection Law Review*, 1, 2016.

- M. COLE, T. QUINTEL, *Legal opinion (commissioned by The Greens in the EU Parliament): Data Retention under the Proposal for an EU Entry/Exit System (EES) Analysis of the impact on and limitations for the EES by Opinion 1/15 on the EU/Canada PNR Agreement of the Court of Justice of the European Union*, ottobre 2017, http://orbilu.uni.lu/bitstream/10993/35446/1/Legal%20Opinion.PDF

- C. COMELLA, *Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa. A margine della sentenza "Safe Harbor" della Corte di Giustizia dell'Unione Europea*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016.

- COMMISSIONE DI VENEZIA (CONSIGLIO D'EUROPA), *Report of the European Commission for Democracy through Law ("the Venice Commission") on the Democratic Oversight of Signals Intelligence Agencies*, 2015.

- COMMISSIONE EUROPEA, *Extended Impact Assessment. Annex to the Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC*, SEC(2005)1131, 21 settembre 2005.

- COMMISSIONE EUROPEA, *Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE)*, COM (2011) 225 def, 2011.

- COMMISSIONE EUROPEA, *Communication on smart cities and communities*, COM(2012)4701), 2012.

- COMMISSIONE EUROPEA, *Comunicazione sul funzionamento del regime 'Approdo sicuro' dal punto di vista dei cittadini dell'UE e delle società ivi stabilite*, COM(2013) 847 final, 27 novembre 2013.

- COMMISSIONE EUROPEA, *Verso una florida economia basata sui dati*, COM(2014) 442 Final, 2014.

- COMMISSIONE EUROPEA, *Agenda europea sulla sicurezza*, COM(2015) 185, final, del 28 aprile 2015.

- COMMISSIONE EUROPEA, *Comunicazione della Commissione al PE e al Consiglio, al Comitato Economico e Sociale europeo e al Comitato delle Regioni: Commercio per tutti. Verso una politica commerciale e di investimento più responsabile*, COM (2015) 497 final, 14 ottobre 2015.

- COMMISSIONE EUROPEA, *Advancing the IoT in Europe*, SWD(2016)110final, 2016.

- COMMISSIONE EUROPEA, *Comunicazione della Commissione al PE e al Consiglio: Scambio e protezione dei dati personali in un mondo globalizzato*, COM(2017) 7 final, 10 gennaio 2017.

- COMMISSIONE EUROPEA, *Industry 4.0 in agriculture: focus on IoT aspects*, 2017.

- COMMISSIONE EUROPEA, *Relazione della Commissione sul primo riesame annuale del funzionamento dello scudo UE-USA per la privacy*, COM(2017)611 final, 18 ottobre 2017.

- COMMISSIONE EUROPEA, *Communication on enabling the digital transformation of health and care in the Digital Single Market: empowering citizens and building a healthier society*, SWD(2018)126, 2018.

- COMMISSIONE EUROPEA, *Relazione della Commissione sul secondo riesame annuale del funzionamento dello Scudo UE-USA per la privacy*, COM(2018)860 final, 19 dicembre 2018.

- COMMISSIONE EUROPEA, *Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020.

- COMMISSIONE EUROPEA, *Relazione sul riesame della direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*, COM(2020)305 final, luglio 2020.

- COMMISSIONE EUROPEA, *Notice to stakeholders. Withdrawal of the UK and EU rules in the field of data protection*, 6 luglio 2020.

- CONSIGLIO D'EUROPA, *Facial recognition: situation and issues*, 2019.

- COMMISSIONE PER LE LIBERTÀ PUBBLICHE, GIUSTIZIA E AFFARI INTERNI DEL PARLAMENTO EUROPEO, *Documento di lavoro sulla proposta di una decisione quadro relativa alla conservazione preventiva di dati che sono elaborati e conservati per fornire servizi elettronici pubblici, ovvero di dati presenti nelle reti di comunicazione pubbliche, a fini di prevenzione, indagini, accertamento e perseguimento di reati, compresi atti di natura terroristica*, DT/553885IT.doc, 31 maggio 2005.

- F. COUDERT, *Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for Data Protection Authorities*, in *European Law Blog*, ottobre 2015, https://europeanlawblog.eu/2015/10/15/schrems-vs-data-protection-commissioner-a-slap-on-the-wrist-for-the-commission-and-new-powers-for-data-protection-authorities/

- F. COUDERT, *Precrime police is not for 2054, it's for now: how to regulate data intensive policing?*, Submission to the Amsterdam Privacy Conference, 2015.

- F. COUDERT, *The legitimacy of bulk transfers of PNR data to law enforcement authorities under the strict scrutiny of AG Mengozzi*, in *European Data Protection Law Review*, 4, 2016.

- F. COUDERT, *In the aftermath of Tele2 and Opinion 1/15: when are data retention measures legitimate?*, in *CiTiP Blog*, University of Leuven, 21 novembre 2017, https://www.law.kuleuven.be/citip/blog/in-the-aftermath-of-tele2-and-opinion-115-when-are-data-retention-measures-legitimate/.

- F. COUDERT, F. VERBRUGGEN, *Conservation des données de communications électronique en Belgique: un juste équilibre?*, in V. FRANSSEN, D. FLORE (a cura di), *Societé numerique et droit penal*, Bruylant, 2019.

- S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di diritto pubblico comunitario*, 3-4, 2015.

- S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, 3, 2016.

- S. CRESPI, *The applicability of Schrems principles to the Member States: national security and data protection within the EU context*, in *European Law Review*, 5, 2018.

- S. CRESPI, *Applicazione di tracciamento Immuni tra normative nazionale e diritto UE in materia di protezione dei dati personali*, in *Freedom, security & justice*, 3, 2020.

- L. CURICCIATI, *Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della* Data Retention Directive, in *Democrazia e Sicurezza*, 2, 2017.

- A. D'ALOIA (a cura di), *Intelligenza artificiale (Contributi del Convegno su 'Intelligenza artificiale e diritto. Come regolare un mondo nuovo', Parma, 12 ottobre 2018),* in *BioLaw Journal*, 1, 2019.

- G. D'IPPOLITO, *Processi decisionali automatizzati nel settore assicurativo. Un'indagine preliminare*, in *MediaLaws*, 2, 2019.

- R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, Giappichelli, 2019.

- J. DASKAL, *The un-territoriality of data*, in *Yale Law Journal*, 125, 2015.

- G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy digitale*, Giuffré, 2019.

- P. DE HERT, S. GUTWIRTH, *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, in S. GUTWIRTH, Y. POULLET, P. DE HERT. C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing data protection?*, Springer, 2009.

- P. DE HERT, R. LEENS (a cura di), *Computers, privacy and data protection: an element of choice*, Springer, 2011.

- P. DE HERT, F. BOEHM, *Notification, an important safeguard against the improper use of surveillance finally recognized in case law and EU law*, in *European Journal of Law and Technology*, 3, 2012.

- P. DE HERT, P. C. BOCOS, *Case of Roman Zakharov v. Russia: the Strasbourg follow up to the Luxembourg Court's Schrems judgement*, in *Strasbourg Observers*, 23 dicembre 2015.

- P. DE HERT, H. LAMMERANT, *Predictive profiling and its legal limits: effectiveness gone forever?*, in B. VAN DER SLOOT, D. BROEDERS, E. SCHRIJVERS (eds.), *Exploring the boundaries of Big Data*, Amsterdam University Press, 2016.

- P. DE HERT, V. PAPAKONSTANTINOU, *The UK contribution to the field of EU data protection: let's not go for 'third country' status after Brexit*, in *Computer Law and Security Review*, 33, 2017.

- A. DE MAURO, *Big Data Analytics. Analizzare e interpretare dati con il machine learning*, Apogeo, 2019.

- G. DE MINICO, *Costituzione. Emergenza e terrorismo*, Jovene, 2016.

- G. DE MINICO, *La risposta europea al terrorismo del tempo ordinario: il lawmaker e il giudice*, in *Osservatorio sulle fonti*, 2, 2017.

- G. DE MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e* lex mercatoria, in *Diritto Pubblico*, 1, 2019.

- G. DE MINICO, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *LaCostituzione.info*, 1 aprile 2020.

- C. DE SIMONE, *Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU Data Retention Directive*, in *German Law Journal*, 11, 2010.

- R. DE SIMONE, *Corte di giustizia dell'UE, Grande Sezione, sentenza 6 ottobre 2015, in causa C-362/14, Maximillian Schrems c. Data Protection Commissioner*, in *Rivista Italiana di diritto pubblico comunitario*, 4, 2015.

- C. DE TERWANGNE, E. DEGRAVE (a cura di), *La protection des données à caractère personnel en Belgique: manuel de base*, Politeia, 2019.

- G. DE VERGOTTINI, *La 'guerra' contro un nemico indeterminato*, in *Forum di Quaderni Costituzionali*, 5 ottobre 2001.

- G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della 'emergenza normalizzata'*, in *Rivista AIC*, 4, 2019.

- F. DE VILLENFAGNE, S. DUSSOLIER, *La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique*, in *A&M*, 1, 2001.

- K. DE VRIES, R. BELLANOVA, P. DE HERT, S. GUTWIRTH, *The German Constitutional Court judgement on data retention: proportionality overrides unlimited surveillance (doesn't it?)*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, R. LEENS (a cura di), *Computers, privacy and data protection: an element of choice*, Springer, 2011.

- E. DEGRAVE, *La Commission de la protection de la vie privée: l'Autorité de régulation du secteur des traitements de données à caractère personnel*, in *Revue du Centre d'étude et de recherches en administration publique*, 26, 2016.

- E. DEGRAVE, Y. POULLET, *Le droit au respect de la vie privée face aux nouvelles technologies*, in M. VERDUSSEN, N. BONBLED (a cura di), *Les droits constitutionnels en Belgique*, Bruylant, 2011.

- D. DEL VESCOVO, *L'accesso delle autorità pubbliche a dati personali di natura meramente identificativa non costituisce ingerenza grave nei diritti fondamentali degli interessati*, in *Amministrativamente – Rivista di diritto amministrativo*, 11-12, 2018.

- G. DELLA MORTE, *La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, in *SIDI Blog*, 30 marzo 2020.

- A. DI MARTINO, *La protezione dei dati personali*, in S. PANUNZIO (a cura di), *I diritti fondamentali e le Corti in Europa*, Jovene, 2005.

- A. DI MARTINO, *Bundesverfassungsgericht dichiara l'incostituzionalità della* data retention *e torna sul rapporto tra libertà e sicurezza*, in *Giurisprudenza costituzionale*, 5, 2010.

- A. DI MARTINO, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, 2017.

- A. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR?*, in *Diritti Umani e Diritto Internazionale*, 1, 2017.

- A. DI ROSA, *Hate speech e discriminazione. Un'analisi performativa tra diritti umani e teorie della libertà*, Mucchi, 2020.

- M. DICOSOLA, *La data retention directive e il dialogo tra Corti costituzionali e Corte di giustizia nel sistema multilivello europeo*, in *Diritti Comparati*, 20 febbraio 2014.

- F.X. DIEBOLD, *On the origin(s) and development of 'Big Data': the phenomenon, the term and the discipline*, PIER Working Paper, 13, 2012.

- A. DIMITROVA, M. BRKAN, *Balancing national security and data protection: the role of EU and US Policy-Makers and Courts before and after the NSA affair*, in *Journal of Common Market Studies*, 4, 2018.

- D. DOBREV, *A definition of Artificial Intelligence*, in *arXiv*, 2004.

- C. DOCKSEY, *Opinion 1/15: privacy and security, finding the balance*, in *Maastricht Journal of European and Comparative Law*, 6, 2017.

- C. DOCKSEY, *Ministerio Fiscal: holding the line on ePrivacy*, in *Maastricht Journal of European and Comparative Law*, 4, 2019.

- B. DOCQUIR, *Droit du nemérique*, Larcier, 2018.

- L. DREWRY, *Crimes without culprits: why the EU needs data retention and how it can be balanced with the right to privacy*, in *Wisconsin International Law Journal*, 4, 2015.

- A. DUBOV et al., *The value and ethics of using technology to contain the Covid-19 epidemic*, in *The American Journal of Bioethics*, 7, 2020.

- F. DUBUISSON, *La Cour européenne des droits de l'homme et la surveillance de masse*, in *Revue Trimestrelle des droits de l'homme*, 108, 2016.

- R. DUCATO, *I dati biometrici*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, 2019.

- R. DUCATO, *Il riconoscimento facciale tra rischi di 'mitridatizzazione sociale' e prospettive di regolamentazione*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, in corso di pubblicazione.

- J. DURICA, *Directive on the retention of data on electronic communication in the rulings of the Constitutional Courts of EU Member States and efforts for its renewed implementation*, in *The Lawyer Quarterly*, 2, 2013, p. 143-158.

- EDRI, *EU Member States plan to ignore EU Court data retention rulings*, 2017, https://edri.org/eu-member-states-plan-to-ignore-eu-court-data-retention-rulings/

- EDRI, *EU Member States willing to retain illegal data retention*, 2019, https://edri.org/eu-member-states-willing-to-retain-illegal-data-retention/

- P. EECKHOUT, *EU external relations law*, Oxford University Press, 2011.

- R.A. EPSTEIN, *The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European Constitutional Law Review*, 12, 2016.

- R.A. EPSTEIN, *The deepening EU blindness on privacy: a pointed response to Professor Martin Scheinin*, in *European Constitutional Law Review*, 12, 2016.

- S. EREVELLES, N. FUKAWA, L. SWAYNE, *Big Data consumer analytics and the transformation of marketing*, in *Journal of Business Research*, 2, 2016.

- V. EUBANKS, *Automating inequality: how high-tech tools profile, police and punish the poor*, St. Martin's Press, 2018.

- EUROJUST, *Consultative forum of Prosecutors General and Directors of Public Prosecutors of the MSs of the EU* e del *Workshop on data retention in the fight against serious crime: the way forward*, 2015.

- EUROJUST, *Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15*, 2017.

- EUROPOL, *Conference report: freedom AND security. Killing the zero sum process*, 23 novembre 2018.

- F. FABBRINI, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quaderni Costituzionali*, 2, 2009.

- F. FABBRINI, *Human rights in the digital age: the European Court of Justice ruling in the Data Retention Case and its lessons for privacy and surveillance in the United States*, in *Harvard Human Rights Journal*, 28, 2015.

- F. FABBRINI, *The EU Charter of Fundamental Rights and the rights to data privacy: the EU Court of Justice as a Human Rights Court*, in S. DE VRIES et al. (a cura di), *The EU Charter of Fundamental Rights as a binding instrument: five years old and growing*, Bloomsbury, 2015.

- F. FAINI, *Big data, algoritmi e diritto*, in *DPCE Online*, 3, 2019.

- F. FAINI, *Data society. Governo dei dati e tutela dei diritti nell'era digitale*, Giuffré, 2019.

- P. FALLETTA, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c. DPC, C-362/14)*, in *Federalismi.it*, 24, 2015.

- G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto*, in A. D'ALOIA (a cura di), *Bio-tecnologie e valori costituzionali. Il contributo della giustizia costituzionale*, Giappichelli, 2004.

- M. FARINA, *La data protection ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, 20 marzo 2020.

- M. FASAN, *La tecnologia ci salverà? Intelligenza artificiale, salute individuale e salute collettiva ai tempi del coronavirus*, in *BioLaw Journal – Instant Forum: Diritto, diritti ed emergenza ai tempi del Coronavirus*, 20 marzo 2020.

- C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, 2008.

- L. FEILER, *The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection*, in *European journal of Law and Technology*, 3, 2010.

- D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018.

- E.A. FERIOLI, *Il Belgio*, in P. CARROZZA, A. DI GIOVINE, G.F. FERRARI (a cura di), *Diritto costituzionale comparato*, Tomo I, Laterza, 2019.

- C. FIEVET et al., *Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information*, in *Revue du droit des technologies de l'information*, 68-69, 2017.

- G. FINOCCHIARO, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quaderni costituzionali*, 4, 2018.

- G.M. FLICK, *Dei diritti e delle paure* in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, ESI, 2009.

- G.M. FLICK, *Elogio della dignità (se non ora, quando?)*, in *Rivista AIC*, 4, 2014.

- R. FLOR, *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constitutionala*, in *Cassazione Penale*, 5, 2011.

- R. FLOR, *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, in *Diritto dell'Informazione e dell'Informatica*, 2014.

- R. FLOR, *Dalla 'data retention' al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de jure condendo'*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, 2015.

- R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata quaestio(?)*, in *Diritto Penale Contemporaneo*, 3, 2017.

- M. FLORA, *The unlawfulness of data retention confirmed by the Court of Justice of the European Union and the Austrian Constitutional Court*, in *Journal of European Consumer and Market Law*, 3, 2015.

- L. FLORIDI, *Soft ethics and the governance of the digital*, in *Philosophy and Technology*, 1, 2018.

- L. FLORIDI, *What the near future of AI could be*, in *Philosophy and Technology*, 7 aprile 2020.

- F. FONTANELLI, *La Corte di Giustizia e il 'favor communitatis'. Il percorso della giurisprudenza della Corte di Giustizia delle Comunità europee sul fondamento normativo degli atti dell'Unione*, in *Rivista di diritto pubblico comunitario*, 1, 2010.

- C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, in *Journal des tribunaux*, 13, 2017.

- N. FORGO, S. HANOLD, B. SCHTZE, *The principle of purpose limitation and Big Data*, in M. CORRALES et al. (a cura di), *New technology, Big Data and the Law*, Springer, 2017.

- G. FORMICI, *Sistemi di riconoscimento e dati biometrici: una nuova sfida per i legislatori e le Corti*, in *DPCE Online*, 2, 2019.

- C. FOSSA', *Facebook nel mirino delle Corti: accanimento giurisprudenziale a cavallo del caso Schrems?*, in *Ricerche giuridiche*, 1, 2017.

- M. FOUCAULT, M. PIERROT (a cura di), *Jeremy Bentham. Panopticon ovvero la casa d'ispezione*, traduzione italiana di V. Fortunati, Marsilio, 1997.

- L. FRIEDMAN, *The Republic of choice, law, authority and culture*, Harvard University Press, 1990.

- B. FRIEDMAN, H. NISSENBAUM, *Bias in computer systems*, in *ACM transactions on information systems*, 3, 1996.

- T.E. FROSINI, *La tutela dei dati e il diritto all'oblio*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, 2018.

- V. FROSINI, *Cibernetica, diritto e società*, Edizioni di Comunità, 1968.

- V. FROSINI, *La protezione della riservatezza nella società informatica*, in N. MATTEUCCI, *Privacy e banche dei dati*, Il Mulino, 1981.

- V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in AA. VV., *Il riserbo e la notizia*, Jovene, 1983.

- V. FROSINI, *Teoria e tecnica dei diritti umani: i diritti umani nella società tecnologica*, ESI, 1993.

- V. FROSINI, *The lawyer in technological society*, in *European journal of law, philosphy and computer science*, 1-2, 1998.

- V. FROSINI, *L'orizzonte giuridico di Internet*, in *Il diritto dell'informazione e dell'informatica*, 2, 2000.

- F. GALLI, *Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions*, in *Maastricht Journal of European and Comparative Law Journal*, 3, 2016.

- D. GAMBETTA, *Datacrazia, politica, cultura algoritmica e conflitti al tempo dei Big Data*, D Editore, 2018.

- M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *EJJL*, 1, 2013.

- S. GAMBINO, A. SCERBO, *Diritti fondamentali ed emergenza nel costituzionalismo contemporaneo. Un'analisi comparata*, in *DPCE*, 4, 2009.

- V. GANTCHEV, *Data protection in the age of welfare conditionality: respect for basic rights or a race to the bottom?*, in *European Journal of Social Security*, 1, 2019.

- GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Parere del garante europeo della protezione dei dati (GEPD) sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della direttiva 2002/58/CE*, 26 settembre 2005.

- GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Opinion 7/2010 on the European Commission's Communication on the global approach to transfers of PNR data to third countries*, 12 novembre 2010.

- GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Opinion 7/2015 Meeting the challenges of Big Data*, 2015.

- GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Opinion 2/2020 on the opening of negotiations for a new partnership with the UK*, 24 febbraio 2020.

- GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, *Dichiarazione sul trattamento di dati personali nel contesto dell'epidemia da Covid-19*, 19 marzo 2020.

- R. GAVISON, *Privacy and the limits of law*, in F. D. SCHOEMAN (a cura di), *Philosofical dimensions of privacy: an anthology*, Cambridge University Press, 1984.

- C. GEARTY, *Escaping Hobbes: liberty and security for our democratic (not anti-terrorist) age*, in *LSE Working Papers*, 3, 2010.

- C. GILMARTIN, *Privacy Rights: how should a Court remedy legislative incompatibility with EU law?*, in *UK Human Rights Blog*, 8 maggio 2018.

- F. GIOVANELLA, *Le persone e le cose: la tutela dei dati personali nell'ambito dell'*Internet of Things, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, Giappichelli, 2019.

- E. GIOVANNINI, *Scegliere il futuro. Conoscenza e politica al tempo dei Big Data*, Il Mulino, 2014.

- G. GONZALES FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Spinger, 2014.

- M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review*, 6, 2014.

- C. GRAZIANI, *La creazione di database di dati biometrici: l'Unione europea tra sfide alla sicurezza e data protection*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, in corso di pubblicazione.

- C. GRAZIANI, *PNR EU-Canada, la Corte di giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali*, in *DPCE Online*, 4, 2017.

- G. GREENWALD, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*, Hamish Hamilton, 2014.

- T. GROPPI, *Democrazia e terrorismo*, ESI, 2009.

- GRUPPO DI LAVORO ART. 29, *Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism*, 11885/04, 9 novembre 2004.

- GRUPPO DI LAVORO ART. 29, *Parere 4/2005 sulla proposta di direttiva del Parlamento europeo e del Consiglio riguardante la conservazione di dati trattati nell'ambito della fornitura di servizi pubblici di comunicazione elettronica e che modifica la direttiva 2002/58/CE (COM(2005)438 definitivo del 21.9.2005)*, 1868/05, 21 ottobre 2005.

- GRUPPO DI LAVORO ART. 29, *Opinion 3/2013: Purpose Limitation*, WP 203, 2013.

- GRUPPO DI LAVORO ART. 29, *Parere 8/2014 sui recenti sviluppi nel campo dell'Internet of Things*, WP223, 2014.

- GRUPPO DI LAVORO ART. 29, *Working Document on surveillance of electronic communications for intelligence and national security purposes*, WP 228, 2014.

- GRUPPO DI LAVORO ART. 29, *Opinion 01/2016 on the draft EU-US Privacy Shield adequacy decision*, WP 238, 13 aprile 2016.

- GRUPPO DI LAVORO ART. 29, *Linee guida sul consenso ai sensi del Reg. UE 2016/679*, WP259, 2017.

- GRUPPO DI LAVORO ART. 29, *EU-US Privacy Shield – First Annual Joint Review*, 17/EN WP 255, 28 novembre 2017.

- O.J. GSTREIN, *Mapping power and jurisdiction on the Internet through the lens of government-led surveillance*, in *Internet Policy Review*, 3, 2020.

- F. GUELLA, Data retention *e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina EU al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE Online*, 2, 2017.

- E. GUILD, S. CARRERA, *The political and judicial life of metadata: Digital Rights Ireland and the trial of the Data Retention Directive*, CEPS Paper in Liberty and Security in Europe, 65, 2014.

- A. GUINCHARD, *Our digital footprint under Covid-19: should we fear the digital contact tracing app?*, in *International Review of Law, Computers & Technology*, 15 luglio 2020.

- S. GUTWIRTH, K. DE VRIES, R. SAELENS, *Veiligheid legitimeert niet alle middelen*, in *Juristenkrant*, 24 marzo 2010, 12, tradotto da F. Peeraer.

- S. HEITZER, J. KULHING, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in *European Law Review*, 2, 2015.

- E. HERLIN-KARNELL, *Annotation of Ireland v. Parliament and Council*, in *Common Market law Review*, 46, 2009.

- H. HIJIMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 16 TFEU*, Springer, 2016.

- H. HIJIMANS, *PNR Agreement EU-Canada scrutinised: CJEU gives very precise guidance to negotiators*, in *European Data Protection Law Review*, 3, 2017.

- M. HILDEBRAND, *Profiling and the rule of law*, in *Identity in the information society*, 1, 2008.

- J. HIND, E. WILLIAMS, A. JONSON, *'It wouldn't happen to me': privacy concerns and perspectives following the Cambridge Analytica scandal*, in *International Journal of Human-Computer*, 143, 2020.

- HOME OFFICE UK, *Consultation Paper – Transposition of Directive 2006/24/EC*, agosto 2008.

- P. HOWARD, *Algorithms, bots and political communication in the US 2016 Election: the challenge of automated political communication for election law and administration*, in *Journal of Information Technology and Politics*, 2, 2018.

- K. HUGHES, *The social value of privacy, the value of privacy to society and human right discourse*, in B. ROESSLER, D. MOKROSINKA (a cura di), *Social dimensions of privacy. Interdisciplinary perspectives*, Cambridge University Press, 2015.

- IBM, *What is big data? Bringing big data to the enterprise*, luglio 2013.

- F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, in *Cassazione Penale*, 12, 2014.

- G.F. ITALIANO, *Intelligenza artificiale: passato, presente, futuro*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018.

- G.F. ITALIANO, *Raccogliere, analizzare e prevedere. L'importanza dei dati al tempo del Covid-19*, in *Luiss Open – Focus Covid*, 7 aprile 2020.

- C. JONES, B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, in *Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness – Paper*, 2013.

- J. KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, 2017.

- B. KELLER, *Big Data and insurance: implications for innovation, competition and privacy*, The Geneva Association, 2018.

- G. KIM, S. TRIMI, J. CHUNG, *Big data applications in the Government sector*, in *Communications of the ACM*, 3, 2014.

- T. KIM, C. RAMOS, S. MOHAMMED, *Smart city and IoT*, Elsevier, 2017.

- R. KITCHIN, *Big data and human geography: opportunities, challenges and risks*, in *Dialogues in human geography*, 3, 2013.

- R. KITCHIN, *Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of Covid-19*, in *Space and Polity*, 3 luglio 2020.

- J. KOKOTT, C. SABOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law*, 4, 2013.

- T. KONSTADINIDES, *Wavering between Centres of Gravity: comment on Ireland v. Parliament and Council*¸ in *European Law Review*, 35, 2010.

- T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, in *European Current Law Issue*, 1, 2012.

- T. KONSTADINIDES, *The rule of law in the European Union: the internal dimension*, Hart Publishing, 2017.

- E. KOSTA, P. VALCKE, *Retaining the data retention directive*, in *Computer Law & Security Report*, 22, 2006.

- E. KOSTA, F. COUDERT, J. DUMORTIER, *Data protection in the Third pillar: in the aftermath of the ECJ decision on PNR data and the Data Retention Directive*, in *International Review of Law Computers and Technology*, 3, 2007.

- E. KOSTA, *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, in *SCRPITed*, 3, 2013.

- E. KOSTA, *SSHD v. Watson and Others: a thin nail on the coffin of UK data retention legislation*, in *European Data Protection Law Review*, 4, 2018.

- J. KUHLING, S. HEITZER, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in *European Law Review*, 2, 2015.

- C. KUNER, *Transborder data flows and data privacy law*, Oxford University Press, 2013.

- C. KUNER, *A super right to data protection? The Irish Facebok case and the future of EU data transfer regulation*, in *LSE Blog*, 24 giugno 2014.

- C. KUNER, *Reality and illusion in EU data transfer regulation post-Schrems*, in *German Law Journal*, 18, 2017.

- C. KUNER, *International agreements, data protection and EU fundamental rights on the international stage: Opinion 1/15, EU-Canada PNR*, in *Common Market Law Review*, 3, 2018.

- C. KUNER, *The Internet and the global reach of EU law*, in M. CREMONA, J. SCOTT (a cura di), *EU law beyond EU borders. The extraterritorial reach of EU law*, Oxford University Press, 2019.

- C. KUNER, *International data transfers, standard contractual clauses and the Privacy Shield: the AG Opinion in Schrems II*, in *European Law Blog*, 7 gennaio 2020.

- K. LACHMAYER, *Rethinking Privacy Across Borders: Developing Transnational Rights on Data Privacy*, in *Tilburg Law Review*, 20, 2015.

- D. LANEY, *3-D data management: controlling data volume, velocity and variety*, 2001, in https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf

- F. LE DIVELEC, *Charte des droits fondamentaux – Protection des données personnelles – Safe Harbor (Sphére sécurité)*, in *Revue du droit de l'Union européenne*, 2, 2015.

- M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, in *Rivista di Diritti Comparati*, 2, 2017.

- E. LEHNER, *Democrazia e tutela dei dati personali nell'UE: l'evoluzione nella negoziazione sul PNR dopo il Trattato di Lisbona*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli Editore, 2013.

- K. LEMMENS, *Respect de la vie privée et de la personnalité*, in M. VERDUSSEN, N. BONBLED (a cura di), *Les droits constitutionnels en Belgique*, Bruylant, 2011.

- K. LENAERTS, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, in *German Law Journal*, 20, 2019.

- J. LI, X. GUO, *Covid-19 contact-tracing apps: a survey on the global deployment and challenges*, in *ArXiv*, 2020.

- I. LLOYD, *Data retention*, in *Computer Law & Security Review*, 34, 2018.

- D. LOWE, *The European Union's Passenger Name Record Data Directive 2016/681: is it fit for purpose?*, in *International Criminal Law Review*, 16, 2016.

- A. LUBIN, *'We only spy on foreigners': the myth of a universal right to privacy and the practice of foreign mass surveillance*, in *Chicago Journal of International Law*, 2, 2018.

- A. LUBIN, *Legitimising foreign mass surveillance in the European Court of Human Rights*, in *Just Security*, 2 agosto 2018.

- L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019.

- O. LYNSKEY, *The foundations of EU data protection law*, Oxford University Press, 2015.

- O. LYNSKEY, *The DRD is incompatible with the rights to privacy*, in *Common Market Law Review*, 2014.

- K. MACASKILL, *Brexit: potential trade and data implications for digital and fintech industries*, in *International Data Privacy Law*, 1, 2017.

- A. MANTELERO, *Big Data: i rischi della concentrazione del potere informativo digitale e gli strumenti di controllo*, in *Diritto dell'Informazione e dell'Informatica*, 1, 2012.

- A. MANTELERO, *Il costo della privacy tra valore della persona e ragione dell'impresa*, Giuffré, 2007.

- A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, RomaTrE-Press, 2016.

- S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, 2019.

- F. MARIATTE, *La sécurité intérieure des États-Unis ne relève pas des compétences externes des Communautés*, in *Révue Europe*, 7, 2006, étude 8.

- C. MARKOU, *The Cyprus and other EU Courts rulings on data retention: the Directive as a privacy bomb*, in *Computer Law & Security Review*, 28, 2012.

- V.R. MASTROIANNI, *Art. 47 TUE*, in A. TIZZANO (a cura di), *Trattati dell'Unione europea*, Giuffré, 2014.

- S. MATZ, *Using Big Data as a window into consumers' psychology*, in *Current Opinion in Behavioral Sciences*, 18, 2017.

- V. MAYER-SCHONBERGER, K. CUKIER, *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, traduzione di Roberto Merlini, Garzanti, 2013.

- W.R. MBIOH, *Post-Och Telestyrelsen and Watson and the Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017.

- Y. MCDERMOTT, *Conceptualising the right to data protection in an era of Big Data*, in *Big Data & Society*, 1, 2017.

- M. MENDEZ, *Passenger Name Record Agreement*, in *European Constitutional Law Review*, 3, 2007.

- M. MENDEZ, *Opinion 1/15: the Court of Justice meets PNR data (again!)*, in *European Papers*, 3, 2017.

- D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Anlaytica"*, in *federalismi.it*, 20, 2018.

- F.P. MICOZZI, *Le tecnologie, alla protezione dei dati e l'emergenza coronavirus: rapporto tra il possibile e il legalmente consentito*, in *BioLaw Journal*, 15 marzo 2020.

- F. MIDIRI, *La giuridificazione della protezione dei dati in Italia*, in *Giustamm*, 5, 2016.

- L. MIGLIETTI, *Profilo storico-comparativi del diritto alla privacy*, in *Diritti Comparati*, 4 dicembre 2014.

- M. MILANOVIC, *ECtHR Judgement in Big Brother Watch v. UK*, in *EJIL Talk*, 17 settembre 2018.

- P. MILFORD, *The retention of communications data: a view from industry*, in *Practical Law IP & IT*, 19 novembre 2008.

- R.A. MILLER (a cura di), *Privacy and power. A transatlantic dialogue in the shadow of the NSA affair*, Cambridge University Press, 2017.

- T. MISRA, *The tenants fighting back against facial recognition technology*, in *Citylab*, 7 maggio 2019.

- S. MITSILEGAS, *Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime*, in *Columbia Human Rights Law Review*, 3, 2016.

- V. MITSILEGAS, *The value of privacy in an era of security: embedding constitutional limits on preemptive surveillance*, in *International Political Sociology*, 1, 2014.

- L. MONTUORI, M. SIANO, *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Aracne, 2017.

- A. MUNIR, S. YASIN, S. BAKAR, *Data retention rules: a dead end*, in *European Data Protection Law Review*, 3, 2017.

- M.H. MURPHY, *Algorithmic surveillance: the collection conundrum*, in *International Review of Law, Computers and technology*, 2, 2017.

- C.C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, in *Common Market Law Review*, 3, 2010.

- C.C. MURPHY, *Fundamental rights and security: the difficult position of the European judiciary*, in *European Public Law*, 16, 2010.

- D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, in *Israel Law Review*, 1, 2019.

- G.R. MURRAY, *Microtargeting and electoral segmentation: data mining the american national elections studies*, in *Journal of Political Marketing*, 3, 2018.

- B. NASCIMBENE, *European Judicial Cooperation in criminal matters: what protection for individuals under the Lisbon Treaty?*, in *ERA Forum*, 10, 2009.

- L. NAUDTS, *Belgian Constitutional Court nullifies Belgian Data Retention Law*, in *European Data Protection Law Review*, 3, 2015.

- G. NAZZARO, *Tabulati di traffico storico per finalità di accertamento e repressione dei reati: caratteristiche e tempi di conservazione*, in *Sicurezza e Giustizia*, 3, 2018.

- S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, 2006.

- M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Diritto dell'Unione europea*, 4, 2014.

- M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE*, in *Il diritto dell'informazione e dell'informatica*, 4, 2015.

- A. NOLAN, R. THOMPSON, E. LIU, *Overview of Constitutional Challenges to NSA Collection Activities and Recent Developments*, Congressional Research Service, aprile 2014.

- R. NORBERG, DAN HORNE, DAVID HORNE, *The privacy paradox: personal information disclosure intentions versus behaviors*, in *Journal of Consumer Affairs*, 1, 2007.

- E. NUNZIANTE, *Big Data. Come proteggerli e come proteggerci. Profili di tutela tra proprietà intellettuale e protezione dei dati personali*, in *MediaLaws. Law and Media working paper series*, 6, 2017.

- S. O'LEARY, *Balancing rights in a digital age*, in *Irish Jurist*, 59, 2018.

- S. O'LEARY, *A tale of two Cities: fundamental rights protection in Strasbourg and Luxembourg*, in *Cambridge yearbook of European Law studies*, 20, 2018.

- C. O'NEIL, *Armi di distruzione di matematica. Come i big data aumentano la diseguaglianza e minacciano la democrazia*, traduzione italiana di Bompiani, 2017.

- S. O'SULLIVAN, C. WALKER, *From the interpersonal to the internet: social service digitization and the implications for vulnerable individuals and communities*, in *Australian Journal of Political Sciences*, 4, 2018.

- T. OJANEN, *Making the essence of fundamental rights real: the Court of Justice of the EU clarifies the structure of fundamental rights under the Charter*, in *European Constitutional Law Review*, 12, 2016.

- T. OJANEN, *Rights-based review of electronic surveillance after Digital Rights Ireland and Schrems in the European Union*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, 2017.

- M. OREFICE, *I Big Data e gli effetti su privacy, trasparenza e iniziativa economica*, Aracne, 2018.

- ORGANIZZAZIONE PER LA COOPERAZIONE E LO SVILUPPO ECONOMICO (OECD), *Tracking and tracing COVID: protecting privacy and data while using apps and biometrics*, 2020.

- M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws*, 2, 2018.

- G. ORWELL, *1984*, Secker&Warburg, 1949.

- U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffré, 2008.

- U. PAGALLO, M. DURANTE, S. MONTELEONE, *What is new with the IoT in privacy and data protection? Four legal challenges on sharing and control in IoT*, in R. LEENES, R. VAN BRAKEL, S. GUTWIRTH, P. DE HERT (a cura di), *Data protection and privacy: (in)visibilities and infrastructures*, Springer, 2017.

- L. PALADINI, *I conflitti tra Pilastri dell'Unione europea e le prospettive del Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, 1, 2010.

- P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffré, 2002.

- M. PALMISANO, *The surveillance cold war: recent decisions of the ECtHR and their application to mass surveillance in the USA and Russia*, in *Journal of International Law*, 2, 2017.

- PARLAMENTO EUROPEO, *Big Data and Data Analytics. The potential for innovation and growth*, Briefing Paper, settembre 2016.

- PARLAMENTO EUROPEO, *Risoluzione del 14 marzo 2017 sulle implicazioni dei Big Data per i diritti fondamentali: privacy, protezione dei dati, non discriminazione, sicurezza e attività di contrasto* (2016/2225(INI), 2017.

- PARLAMENTO EUROPEO, *Public security exception in the Area of non-personal data in the EU*, PE 618.986, aprile 2018.

- PARLAMENTO EUROPEO, *Risoluzione sull'adeguatezza della protezione offerta dallo Scudo UE-USA per la privacy* (2018/2645 (RSP)), 5 luglio 2018.

- F. PASQUALE, *The black box society. The secret algorithms that control money and information*, Harvard University Press, 2015.

- E. PAVARANI, *Diritto al rispetto della vita privata e familiare*, in C. DEFILIIPPI, D. BOSI, R. HARVEY, *La Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, ESI, 2006.

- E. PEDILARCO, *Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione europea-Stati Uniti sul trasferimento dei dati dei passeggeri aerei*, in *Diritto Pubblico Comparato ed Europeo*, 2006.

- E. PEERAER, *Data retention: the Belgian approach*, in *Masaryk University Journal of Law and Technology*, 1, 2012.

- L. PEGORARO, A. RINELLA, *Sistemi costituzionali comparati*, Giappichelli, 2017.

- W.L. PERRY et al., *Predictive policing. The role of crime forecasting in law enforcement operations*, Rand Corporation, 2013.

- A. PERUZZI, F. ZOLLO, W: QUATTROCCHI, A. SCALA, *How new ways affect markets complex structure: the case of Cambridge Analytica*, in *Entropy*, 10, 2018.

- F. PETRUCCO, *The right to privacy and new technologies: between evolution and decay*, in *MediaLaws*, 1, 2019.

- S. PEYROU, *La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques*, in *Journal de droit européen*, 2, 2015.

- V. PFISTERER, *The Right to Privacy—A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, in *German Law Journal*, 20, 2019.

- A. PIN, *Non esiste la 'pallottola d'argento': l'Artificial Face Recognition al vaglio giudiziario per la prima volta*, in *DPCE Online*, 4, 2019.

- M. PINNA, *Doppio binario di accesso ai dati sul traffico telefonico: una scelta legislativa ragionevole ratificata (con argomenti non irresistibili) dalla Corte costituzionale*, in *Giurisprudenza Costituzionale*, 2006.

- P. PIRODDI, *Art. 16 TFUE*, in F. POCAR, M. C. BARUFFI, *Commentario breve ai Trattati dell'Unione europea*, Cedam, II Ed., 2014.

- P. PIRODDI, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo Regolamento generale sulla protezione dei dati*, in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015.

- A. PISAPIA, *La tutela multilivello garantita ai dati personali nell'ordinamento europeo*, in *federalismi.it*, 3, 2018.

- G. PITRUZZELLA, O POLLICINO, S. QUINTARELLI (a cura di), *Parole e potere. Libertà d'espressione, hate speech e fake news*, Egea, 2017.

- G. PITRUZZELLA, O. POLLICIINO (a cura di), *Disinformation and hate speech. A European constitutional perspective*, Bocconi University Press, 2020.

- F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA, M. D'AMICO (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, 2009.

- F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale*, in *federalismi.it*, 13, 2013.

- F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016.

- S. POLI, *The legal basis of Internal market measures with a security dimension: comment on case C-301/06, Ireland vs. Parliament/Council*, in *European Constitutional Law Review*, 6, 2010.

- O. POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in *www.forumcostituzionale.it*, 31 dicembre 2013.

- O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, 2015.

- O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'UE nel reasoning dei giudici di Lussemburgo*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "safe harbour principles" al "privacy shield",* RomaTrE-Press, 2016.

- O. POLLICINO, M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 9 gennaio 2017.

- O. POLLICINO, M. BASSINI, *Social network e tutela dei dati personali*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, 2018.

- O. POLLICINO, *Riflettere su distonie e utopie del rapporto tra tecnologia e società*, in *Giustizia Insieme*, 18 aprile 2020.

- K.R. POPPER, *Congetture e confutazioni*, traduzione italiana di G. Pancaldi, Il Mulino, 1972.

- M.G. PORCEDDA, *The recrudescence of 'Security v. Privacy' after the 2015 terrorist attacks and the value of privacy rights in the European Union*, in E. ORRÙ, M. G. PORCEDDA, S. WEYDNER-VOLKMANN (a cura di), *Rethinking surveillance and control: beyond the 'security versus privacy' debate*, Nomos, 2017.

- E. POSNER, A. VERMEULEN, *Terror in balance: security, liberty and the Courts*, Oxford University Press, 2007.

- Y. POULLET, *The fight against crime and/or the protection of privacy: a thorny debate!*, in *International Review of Law, Computers and Technology*, 2, 2004.

- PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, *Report on the telephone record program conducted under section 215 of the USA Patriot Act and on the operations of the foreign intelligence surveillance Court*, 2014.

- PRIVACY INTERNATIONAL, *National Data Retention Laws since the CJEU's Tele2/Watson judgement*, 2017.

- M.P. QUEK, *Personal data privacy protection in an age of globalization: the UE-USA Safe Harbour compromise*, in *Journal of European Public Policy*, 3, 2002.

- T. QUINTEL, *Investigatory Powers Tribunal: Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Ors Part II*, in *European Data Protection Law Review*, 3, 2017.

- N. RAGHENO, *Data protection: la future nouvelle Autorité dee protection des données*, in *Cahier du Juriste*, 2, 2017.

- S. RANCHORDAS, *Constitutional sunsets and experimental legislation*, Elgar, 2014.
- S. RANCHORDAS, *Public law and technology: automating welfare, outsourcing the State*, in *International Journal of Consistutional law Blog*, 15 gennaio 2020.
- S. RANCHORDAS, *Automation of public services and digital exclusion*, in *International Constitutional Law Blog*, 11 marzo 2020.
- M. RATH, B. PATTANAYAK, *Technological improvement in modern health care applications using IoT and proposal of novel health care approach*, in *International Journal of Human Rights in Healthcare*, 2, 2019.
- J. RAUHOFER, D. MAC SITHIGH, *The data retention directive never existed*, in *Scripted* n. 118, 2014.
- J. REIDENBERG, *The transparent citizen*, in *Loyola University Chicago Law Journal*, 47, 2015.
- G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il Codice dei dati personali. Temi e problemi*, Giuffré, 2004.
- G. RESTA, *Identità personale e identità digitale*, in *Diritto dell'informazione e dell'informatica*, 3, 2007.
- G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016.
- G. RESTA, *Governare l'innovazione tecnologica: decisioni algoritmiche, diritti digitali e principio di uguaglianza*, in *Forum disuguaglianze e diversità*, 2020.
- I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *Sistema Penale*, 5, 2020.
- M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Diritto Penale Contemporaneo*, 3, 2016.
- K. RINGROSE, *Law enforcement's pairing of facial recognition technology with body-worn cameras escalates privacy concerns*, in *Virginia law Review Online*, 105, 2019.
- S. RODA, *Shortcomings of the PNR Directive in light of Opinion 1/15 of the Court of Justice of the European Union*, in *European data protection law review*, 6, 2020.
- S. RODOTÀ, *Tecnologia e diritti*, Il Mulino, 1995.
- S. RODOTÀ, *Privacy, libertà, dignità, discorso conclusivo della Conferenza internazionale sulla protezione dei dati*, www.privacy.it/archivio/rodo20040916.html, 2004.
- S. RODOTÀ, *La vita e le regole*, Feltrinelli, 2006.
- S. RODOTÀ, *Il diritto di avere diritti*, Laterza, 2013.
- S. RODOTÀ, *Iperdemocrazia. Come cambia la sovranità democratica con il web*, Laterza, 2013.
- S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Editori Laterza, 2014.

- M. ROSENFELD, *Judicial balancing in times of stress: comparing diverse approaches to the war of terror*, Benjamin N. Cardozo School of Law Working Paper, 119, 2005.

- F. ROSSI DAL POZZO, *Servizi di trasporto aereo e diritti dei singoli nella disciplina comunitaria*, Giuffré, 2008.

- F. ROSSI DAL POZZO, *Protezione dei dati personali e diritti fondamentali della persona: le nuove norme sui "codici di prenotazione" (PNR)*, in *Rivista di diritto internazionale privato e processuale*, 4, 2016.

- A. ROUVROY, Y. POULLET, *The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy*, in S. GUTWIRTH, Y. POULLET, P. DE HERT. C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing data protection?*, Springer, 2009.

- M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it*, 23, 2016.

- A. RUGGERI, *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)*, in *Consulta Online*, III, 2016.

- F. RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cassazione penale*, 6. 2017.

- H. RUHRMANN, *Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement*, University of California Berkley, 2019.

- V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroads*, Working Papers HSE, 2019.

- C.M. RYNGAERT, N. VAN EIJK, *International cooperation by (European) security and intelligence services: reviewing the creation of a joint database in light of data protection guarantees*, in *International data privacy law*, 1, 2019.

- S. SANDRU, *About data protection and data retention in Romania*, in *Masaryk University Journal of Law and Technology*, 2, 2013.

- D. SARMIENTO, *What Schrems, Delvigne and Celaj tell us about the state of fundamental rights in the EU*, in *Verfassungsblog*, 16 ottobre 2015.

- C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web*, in *federalismi.it*, 13, 2019.

- E. SAULNIER-CASSIA, *La Directive (UE) 2016/681: miscellanies sur l'utilisation des données des données des dossier passagers dans l'Unione Européenne du PNR eurpéen*, in C. CHEVALLIER GOVERS (a cura di), *L'èchange des données dans l'Espace de liberté, de sécurité et de Justice de l'Unione Européenne*, Mare & Martin, 2017.

- F. SAVASTANO, *Uscire dall'UE. Brexit e il diritto di recedere dai Trattati*, Giappichelli, 2019.

- S. SAXBY, *European Parliament says 'No!' to Member States' data retention proposal*, in *Computer Law & Security Report*, 21, 2005.

- L. SCAFFARDI, *Nuove tecnologie, prevenzione del crimine e privacy, alla ricerca di un difficile bilanciamento*, in A. TORRE (a cura di), Costituzioni e sicurezza dello Stato, Maggioli, 2013.

- L. SCAFFARDI, *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016: una legge per il futuro troppo legata al passato***,** in *Quaderni Costituzionali*, 2, 2017.

- L. SCAFFARDI, *La data retention va in ascensore*, in *Forum di Quaderni Costituzionali*, 28 luglio 2017.

- L. SCAFFARDI, *Dati genetici e dati biometrici: nuove frontiere per le attività investigative*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto*, Giappichelli, 2018.

- M. SCHEININ, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin: Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight*, Doc. A/HRC/14/46, 17 maggio 2010.

- M. SCHEININ, *Towards evidence-based discussion on surveillance*, in *European Constitutional Law Review*, 12, 2016.

- M. SCHEININ, *Towards evidence-based discussion on surveillance: a rejoinder to Richard A. Epstein*, in *European Constitutional Law Review*, 12, 2016.

- S.J. SCHULHOFER, *An international right to privacy? Be careful what you wish for*, ICON, 1, 2016.

- P.M. SCHWARTZ, D. SOLOVE, *Reconciling personal information in the United States and European Union*, in *California Law Review*, 102, 2014.

- O. SCHWARZ-HERION, *The role of Smart Cities for the realization of the sustainable development goals*, in A. OMRAN, O. SCHWARZ-HERION, *Sustaining our environment for better future*, Springer, 2020.

- S. SCHWEDA, *Parliament adopts new data retention law*, in *European Data Protection Law Review*, 1, 2015, pp. 223-226.

- L. SCUDIERO, *La Camera porta di soppiatto la data retention a sei anni*, in *Lex Digital*, 21 luglio 2016.

- L. SCUDIERO, *Data retention a sei anni. La Corte di Giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR*, in *MediaLaws*, 1, 2017.

- V. SCUOTTO, A. FERRARIS, S. BRESCIANI, *IoT: applications and challenges in smart cities*, in *Business Process Management Journal*, 2, 2016.

- SECRETARY OF STATE FOR THE HOME DEPARTMENT, *Protecting the Public in a changing communications environment*, 2009.

- M. SENOR, *Un altro 'tango down' in tema di data retention*, in *MediaLaws*, 22 luglio 2015.

- A. SERENA, *The leviathan, the chains, the lock: dynamics of power in the digital surveillance state*, in *MediaLaws. Law and media Working Paper Series*, 8, 2017.

- SERVICE DE RECHERCHE DU PARLEMENT EUROPÉEN, *Le droit au respect de la vie privée: les défis digitaux, une perspective de droit comparé. Belgique*, 2018.

- O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, Editoriale Scientifica, 2017.

- G. SHAFFER, *Globalization and social protection: the impact of EU and International Rules in the ratcheting up of US data privacy standards*, in *Yale Journal of International Law*, 25, 2000.

- K. SHU et al., *Disinformation, misinformation and fake news in social media: emerging research challenges and opportunities*, Springer, 2020.

- S. SICA, V. D'ANTONIO, *I Safe Harbour privacy principles: genesi, contenuti, criticità,* in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015.

- S. SICA, V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016.

- E. SIEGEL, *Predictive analytics: the power to predict who will click, buy, lie or die*, Wiley, 2016.

- S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018.

- S. SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 12 Codice Privacy da parte del D. Lgs. 10 agosto 2018, n. 101*, in *Diritto penale contemporaneo*, 11, 2018.

- A. SIMONCINI, S. SUWEIS, *Il cambio di paradigma nell'intelligenza artificiale e il suo impatto sul diritto costituzionale*, in *Rivista di filosofia del diritto*, 1, 2019.

- M. SMITS, *Comparative law and its influence on national legal systems*, in M. REIMANN, M. ZIMMERMANN (a cura di), *The Oxford handbook of comparative law*, Oxford University Press, 2006.

- E. SNOWDEN, *Errore di Sistema*, Longanesi, traduzione italiana a cura di Netphilo Publishing, 2019.

- D. SOLOVE, *Conceptualizing privacy*, in *California Law Review*, 90, 2002.

- D. SOLOVE, *Nothing to hide. The false tradeoff between privacy and security*, Yale University Press, 2011.

- A. SORO, Garante per la protezione dei dati personali, *Big Data e Privacy. La nuova geografia dei poteri*, Atti del Convegno 30 gennaio 2017.

- A. SORO, Intervento del Presidente del Garante all'incontro "Verso una nuova privacy?", https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6937167, 6 ottobre 2017.

- A. SORO, *Democrazia e potere dei dati. Libertà, algoritmi e umanesimo digitale*, Baldini+Castoldi, 2019.

- M. SPATTI, *Il trasferimento dei dati relativi ai PNR: gli accordi UE con Austria e USA*, in *Diritto del commercio internazionale*, 3, 2013.

- E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, in *IANUS*, 15, 2017.

- A. SPINA, *La medicina degli algoritmi: intelligenza artificiale, medicina digitale e regolazione dei dati personali*, in F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, 2018.

- J. STANKOVIC, *Research directions for the IoT*, in *Internet of Things Journal*, 1, 2014.

- A. SUTTON, T. LANSDALL, N. CRISTIANINI, *Biased embeddedings from wild data: measuring, understanding and removing*, in *International symposium on Intelligent data analysis*, Spinger, 2018.

- M. TADDEO, L. FLORIDI, *How AI can be a force for good*, in *Science*, 24 agosto 2018.

- D. TALIA, *La società calcolabile e i Big Data. Algoritmi e persone nel mondo digitale*, Rubettino, 2019.

- M. TAYLOR, *The EU Data Retention Directive*, in *Computer Law & Security Report*, 22, 2006.

- F. TERPAN, *EU-US data transfer from Safe Harbour to Privacy Shield: back to square one?*, in *European Papers*, 3, 2018.

- G. TIBERI, *L'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura elettronica dei passeggeri aerei al vaglio della Corte di giustizia*, in *Quaderni costituzionali*, 2006.

- G. TIBERI, *Il diritto alla protezione dei dati personali nelle Carte e nelle Corti sovranazionali (in attesa del Trattato di Lisbona)*, in *Cassazione Penale*, 11, 2009.

- G. TIBERI, *La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel "dopo-Lisbona"*, in *Quaderni costituzionali*, 3, 2014.

- G. TIBERI, *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?*, in *Quaderni costituzionali*, 4, 2018.

- A. TORREZ PEREZ, *The federalizing force of the EU Charter of Fundamental Rights*, in *International journal of constitutional law*, 4, 2017.

- I. TOURKOCHORITI, *The transatlantic flow of data and the national security exception in the European data privacy regulation: in search for legal protection against surveillance*, in *University of Pennsylvania Journal of International Law*, 3, 2015.

- X. TRACOL, *Legislative genesis and judicial death of a directive: the European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it*, in *Computer Law & Security Review*, 30, 2014.

- X. TRACOL, *"Invalidator" strikes back: the harbour has never been* safe, in *Computer Law and Security Review*, 3, 2016.

- X. TRACOL, *EU–U.S. Privacy Shield: The saga continues*, in *Computer Law and Security Review*, 32, 2016.

- X. TRACOL, *The judgement of the Grand Chamber dated 21 December 2016 in the two joint Tele2Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level*, in *Computer Law & Security Review*, 33, 2017.

- X. TRACOL, *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada*, in *Computer Law and Security Review*, 4, 2018.

- X. TRACOL, *Ministerio Fiscal: access of public authorities to personal data retained by providers of electronic communications services*, in *European Data protection Law Review*, 1, 2019.

- M. TRIPOLI, J. SCHIMDHUBER, *Emerging opportunities for the application of blockchain in the Agri-food Industry*, in *FAO Issue Paper*, 2018.

- G. TROPEA, *Il contact tracing digitale e l'epidemia: sindrome cinese?*, in *LaCostituzione.info*, 9 aprile 2020.

- I. TRUMMER, *Liberty v. SSHD & SSFCA: you have the right to remain silent; anything you say will be gathered and retained by the* Government, in *Tulane Journal of International and Comparative Law*, 28, 2020.

- T. TZANOU, *Data protection as a fundamental right next to privacy*? *Reconstructing a not so new right*, in *International data privacy law*, 2, 2013.

- M. TZANOU, *European Union regulation of transatlantic data transfers and online surveillance*, in *Human Rights Law Review*, 17, 2015.

- T.M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, Cedam, 2004.

- UNCTAD, *Data protection regulations and international data flows: implications for trade and development*, 2016.

- S. VAIDHYANATHAN, *Antisocial media: how Facebook disconnects us and undermines democracy*, Oxford University Press, 2018.

- N. VAINIO, S. MIETTINEN, *Telecommunications data retention after DR: legislative and judicial reactions in the Member States*, in *International Journal of Law and Information Technology*, 23, 2015.

- N. VAINIO, *Fundamental rights compliance and the politics of interpretation: explaining Member State and Court reactions to Digital Rights Ireland*, in T. BRAUTIGAM, S. MIETTINEN (a cura di), *Data protection, privacy and European regulation in the digital age*, Unigrafia, 2016.

- M. VAN BELLINGHEN, T. ZGAJEWSKI, *Les enjeux de la transposition en Belgique des nouvelles directives européennes sur les communications électroniques*, Academia Press, 2012.

- R. VAN BRAKEL, P. DE HERT, *Policing surveillance and law in a pre-crime society: understanding the consequences of technology based strategies*, Cahiers Politiestudies Jaargag, 3, 2011.

- B. VAN DER SLOOT, *Legal fundamentalism: is data protection really a fundamental right?*, in R. LEENES et al. (a cura di), *Data protection and privacy. (In)visibilities and infrastructure*, Springer, 2017.

- B. VAN DER SLOOT, E. KOSTA, *Big Brother Watch and others v. UK: lessons from the latest Strasbourg ruling on bulk surveillance*, in *European Data Protection Law Review*, 2, 2019.

- H. VAN KOLFSCHOOTEN et al., *Covid-19 and privacy in the EU: a legal perspective on contact tracing*, in *Contemporary Security Policy*, 3, 2020.

- A.D. VANBERG, M. MAUNICK, *Data protection in the UK post-Brexit: the only certainty is uncertainty,* in *International Review of Law, Computers and Technology*, 1, 2018.

- L.P. VANONI, *Il IV emendamento della Costituzione americana tra terrorismo internazionale e datagate: security v. privacy*, in *federalismi.it*, 1, 2015.

- L.P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of the Eu and US constitutional systems*¸ in L. VIOLINI, A. BARAGGIA (a cura di), *The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and non-Judicial Actors*, Elgar Publish, 2018.

- F. VECCHIO, *L'ingloriosa fine della direttiva data retention, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy,* in *Diritti Comparati*, 12 giugno 2014.

- A. VEDASCHI, *A' la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Giappichelli, 2007.

- A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Diritto pubblico comparato ed europeo*, 3, 2014.

- A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy. A European perspective*, in *Tilburg Law Review*, 20, 2015.

- A. VEDASCHI, G. M. NOBERASCO, *From DRD to PRN: looking for a new balance between privacy and security*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and trans-Atlantic relations*, Bloomsbury, 2015.

- A. VEDASCHI, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione Europea*, in *Giurisprudenza Costituzionale*, 4, 2017.

- A. VEDASCHI, *Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement*, in *International Data Privacy Law*, 2, 2018.

- F. VERBRUGGEN, S. ROYER, H. SEVERIJNS, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, in *European Law Blog*, 1 ottobre 2018, http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/.

- P. VERHOEF, E. KOOGE, N. WALK, *Creating value with Big Data analytics*, Routledge, 2016.

- G. VERMEULEN, *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities*, in G. VERMEULEN, E. LIEVENS (a cura di), *Data protection and privacy under pressure. Transatlantic tensions, EU serveillance and Big Data*, Maklu, 2017.

- G. VERMEULEN, *The paper shield: on the degree of protection of the EU-US Privacy Shield against unnecessary or disproportionate data collection by the US intelligence and law enforcement services*, in D. SVANTESSON, D. KOLZA (a cura di) *Transatlantic data privacy relationship: as a challenge for democracy*, Cambridge University Press, 2017.

- J. VERMEULEN, *Big brother may continue watching you*, in *Strasbourg Observers*, 12 ottobre 2018.

- J. VERMEULEN, *Another case of violating privacy and personal data protection: Catt v. the United Kingdom*, in *Strasbourg Observers*, 22 febbraio 2019.

- G.E. VIGEVANI, *Articolo 132*, in AAVV, *Codice della privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Giuffré, 2004.

- T. VIOLANTE, *Data retention in Portugal*, in M. ZUBIK, J. PODKOWIK, R. RYBSKI (a cura di), *European Constitutional Courts towards data retention laws*, Springer, 2020.

- A. VIVARELLI, *The crisis of the rights to informational self-determination*, in *The Italian Law Journal*, 1, 2020.

- N. VIZIOLI, *La giustizia costituzionale in Belgio*, in J. LUTHER, R. ROMBOLI, R. TARCHI (a cura di), *Esperienze di giustizia costituzionale*, Vol. II, Giappichelli, 2002.

- P. VOGIATZOGLOU, *Centrum For Rattvisa v. Sweden: bulk interception communications by Intelligence Services in Sweden does not violate the right to privacy*, in *European Data Protection Law Review*, 4, 2018.

- P. VOGIATZOGLOU, S. FANTIN, *National and public security within and beyond the Police Directive*, in A. VEDDER, J. SCHROERS, C. DUCUING, P. VALCKE (a cura di), *Security and Law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Intersentia, 2019.

- P. VOGIATZOGLOU, *Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity*, in *European Journal of Law and Technology*, 1, 2019.

- P. VOGIATZOGLOU, *Data Retention tales: the Council of the EU strikes back*, in *CiTiP Law Blog*, luglio 2019.

- C. WALKER, *Data retention in the UK: pragmatic and proportionate or a step too far?*, in *Computer Law and Security Review*, 25, 2009.

- C. WALTER (a cura di), *Terrorism as challenge for national and international law: security versus liberty?*, Springer, 2004.

- J.S. WARD, A. BARKER, *Undefined by data: a survey of Big Data definitions*, in *arXiv Cornell University*, 2013.

- K. WARD, *Social networks, the 2016 US Presidential election and Kantian ethics: applying the categorical imperative to Cambridge Analytica's behavioral microtargeting*, in *Journal of Media Ethics*, 3, 2018.

- S.D. WARREN, L.D. BRANDEIS, *The right to privacy*, in *Harvard Law Review*, 4, 1890.

- R. WEBER, *IoT: new security and privacy challenges*, in *Computer Law and Security Report*, 26, 2010.

- A. WESTIN, *Privacy and freedom*, in *Washington and Lee Law Review*, 20, 1968.

- D. WESTPHAL, *German federal constitutional Court delivers roadmap for national data retention laws – without transferal to ECJ*, in *Vienna Journal on International Constitutional Law*, 5, 2011.

- M. WHITE, *Protection by judicial oversight or an oversight in protection?*, op. cit., in *Journal of Information Rights, Policy and Practice*, 2, 2017.

- M. WHITE, *The Privacy International case in the IPT: respecting the right to privacy?*, in *EU Law Analysis*, 14 settembre 2017, http://eulawanalysis.blogspot.com/2017/09/the-privacy-international-case-in-ipt.html.

- M. WHITE, *Data Retention incompatible with EU law: Victory? Victory you say?*, in *EU Law Analysis*, 24 maggio 2018.

- K. WIMMER, J. JONES, *Brexit and implications for privacy*, in *Fordham International Law Journal*, 5, 2017.

- J. WITHMAN, *The two Western culture of privacy: dignity versus liberty*, in *Yale Law Journal*, 113, 2004.

- L. WOODS, *High Court strikes down data retention laws in ruling on DRIPA*, in *European Data Protection Law Review*, 3, 2015.

- L. WOODS, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*, in *EU Law Analysis*, 21 dicembre 2016, http://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html.

- L. WOODS, *Trasnferring personal data outside the EU: clarification from the ECJ?*, in *EU Law Analysis*, 4 agosto 2017.

- L. WOODS, *The Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017.

- L. WOODS, *Investigatory Powers Tribunal (IPT): Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, in *European Data Protection Law Review*, 3, 2017.

- L. WOODS, *UK: heading towards Brexit but with Data Protection Bill implementing GDPR*, in *European Data Protection Law Review*, 3, 2017.

- L. WOODS, *Analysis of the ECtHR judgement in Big Brother Watch (Part 1 and 2)*, in *EU Analysis Blog*, 16 settembre 2018.

- L. WOODS, *Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers*, in *EU Law Analysis*, 4 ottobre 2018, http://eulawanalysis.blogspot.com/2018/10/mobile-phone-theft-and-eu-eprivacy-law.html.

- L. WOODS, *The AG Opinion in Schrems II: Facebook, national security and data protection law*, in *EU Law Analysis*, 21 dicembre 2019.

- W.B. WRAY, *A European approach to the United States Constitutional privacy*, in *Craighton International and Comparative Law Review*, 51, 2015.

- L. ZAGATO, *Il trasferimento di dati personali verso Stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*, in *Diritto del commercio internazionale*, 2, 2008.

- M. ZALNIERIUTE, *Developing a European standard for international data transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *The modern law review*, 6, 2018.

- M. ZALNIERIUTE, L. BENNETT MOSES, G. WILLIAMS, *The rule of law and automation of Government decision-making*, in *The modern law review*, 3, 2019.

- A. ZAVRSNIK, *Blurring the line between law enforcement and intelligence: sharpening the gaze of surveillance?*, in *Journal of contemporary european research*, 1, 2013.

- L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the UK after the European Data Retention*, in R. A. MILLER, *Privacy and power. A transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, 2017.

- V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di comunicazione*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, 2016.

- V. ZENO-ZENCOVICH, G. GIANNONE CODIGLIONE, *Ten legal perspectives on the 'big data revolution'*, in *Concorrenza e mercato*, 23, 2016.

- V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemologia del giurista*, in *MediaLaws*, 2, 2018.

- V. ZENO-ZENCOVICH, *La 'datasfera'. Regole giuridiche per il mondo digitale parallelo*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, 2018.

- G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina, 2015.

- G. ZICCARDI, *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina, 2019.

- S. ZUBOFF, *Il capitalismo della sorveglianza*, traduzione italiana di P. Bassotti, Luiss University Press, 2019.