AIC
ASSOCIAZIONE ITALIANA
DEI COSTITUZIONALISTI

OSSERVATORIO COSTITUZIONALE
Codice ISSN: 2283-7515
Fasc. 3/2018
26 novembre 2018

Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia *Ministerio Fiscal*•

di **Giulia Formici** – *Dottoranda in Diritto Pubblico, Internazionale ed Europeo, Università degli Studi di Milano*

ABSTRACT: While in its landmark judgement *Tele2 Sverige*, the CJEU set fundamental principles and criteria in the delicate field of national data retention and access measures, it also raised relevant questions. The CJEU's ruling *Ministerio Fiscal* C-207/16 could be seen as one of the results of these open issues. This paper analyses this recent decision, concerning national authorities' access, for criminal investigative purposes, to personal data retained by providers of telecommunications services. Underlining the particular post-*Tele2 Sverige* context, characterized by a fragmented legislation and a complex jurisprudence, both at the European and national level, this article aims to assess unresolved doubts, current challenges and the possible future scenario.

1. *Introduzione: la riservatezza delle comunicazioni elettroniche come quadro incompiuto*

Se trasponessimo in pittura la complessa quanto delicata tutela - nel contesto europeo - della riservatezza dei dati relativi alle comunicazioni elettroniche, ne emergerebbe un quadro dalle forme non ancora perfette: in termini tecnici, un abbozzo. Non ci troveremmo pertanto di fronte né ad un mero schizzo, una rapida improvvisazione dell'artista che traccia sulla tela la sua primigenia idea dell'opera ma neppure ad un lavoro compiuto. Osserveremmo invece un dipinto già strutturato ed

• Scritto sottoposto a referaggio secondo le Linee guida della Rivista.

elaborato nel suo insieme, con tratti decisi che permettono di suggerirne l'aspetto finale ma ancora privo di quei particolari volti a meglio definirne, con ulteriori tratti di colore, le immagini. Tali elementi sono fondamentali per la conclusione del dipinto e per attribuirgli l'aspetto definitivo e completo.

Attorno a questo quadro, che alcuni critici ritenevano ormai quasi pronto per essere esposto, ancora molti artisti si stanno invece affaccendando, aggiungendo man a mano i necessari dettagli, con tratti talvolta sovrapposti.

La pronuncia del 2 ottobre 2018, *Ministerio Fiscal* C-207/16, decisa dalla Grande Sezione della Corte di Giustizia dell'Unione Europea, rappresenta, in questa metaforica tela, proprio un nuovo e importante tratto che definisce e arricchisce l'abbozzo: a dimostrazione di quanto il bilanciamento tra tutela del diritto alla privacy e alla protezione dei dati, da un lato, e conservazione e utilizzo dei dati a garanzia della sicurezza, dall'altro, presenti ancora molti punti oscuri e interrogativi aperti.

Le storiche decisioni *Digital Rights Ireland* e *Tele2 Sverige,* che costituiscono invece l'abbozzo del nostro quadro immaginario, sono quindi imprescindibile base di partenza di quella che potremmo definire l'analisi critica di un'opera ancora incompiuta. Va dunque ricostruito il complesso intreccio di disposizioni normative e decisioni giurisprudenziali, che intersecano il livello europeo a quello nazionale, in tema di *data retention* e accesso, per finalità di sicurezza, ai dati raccolti dai fornitori di servizi di telecomunicazione nello svolgimento delle proprie attività. Questo preventivo sforzo ricostruttivo permetterà di meglio comprendere innanzitutto le motivazioni che hanno spinto il giudice spagnolo a richiedere l'intervento della Corte di Giustizia dell'Unione Europea nel caso *Ministerio Fiscal* e successivamente anche di cogliere appieno la portata di questa più recente decisione.

Di quest'ultima verranno sottolineati gli aspetti maggiormente problematici e di delicata quanto controversa soluzione; è muovendo da questa analisi che potranno essere delineate le questioni ancora irrisolte, i persistenti dubbi e le prospettive future, da leggersi anche alla luce di alcuni interessanti rinvii pregiudiziali, al momento pendenti di fronte alla Corte di Giustizia.

2. *L'abbozzo: dalla Digital Rights Ireland all'era post-Tele2 Sverige*

Il rinvio pregiudiziale promosso dall*'Audiencia Provincial de Tarragona,* che ha portato alla pronuncia *Ministerio Fiscal* del 2 ottobre 2018, verte, sull'interpretazione dell'art. 15 della Direttiva 2002/58/CE **(**cd. Direttiva e-Privacy[1]), letto alla luce degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea (cd. Carta di Nizza). La richiamata Direttiva e la specifica disposizione di cui all'art. 15, nonché le questioni attinenti la riservatezza delle comunicazioni

[1] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, 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).

elettroniche, non sono però affatto sconosciute ai giudici di Lussemburgo. Questi, infatti, hanno avuto più volte modo di pronunciarsi su tali temi con decisioni dalla storica portata.

La Direttiva e-privacy stabilendo quale regola generale la riservatezza delle comunicazioni e dei dati da esse derivanti[2], prevede una importante deroga: ben consapevole delle potenzialità che tali dati rappresentano ai fini di prevenzione e repressione dei reati, nonché per la tutela della sicurezza nazionale, l'articolo 15 della stessa Direttiva attribuisce tuttavia la possibilità ai singoli Stati Membri di obbligare i fornitori di servizi di comunicazione a conservare i dati, qualora ciò si renda necessario per determinati fini, espressamente indicati[3], riconducibili genericamente alla tutela della sicurezza pubblica. Ulteriormente, vengono poste alcune limitazioni alla discrezionalità del legislatore nazionale, stabilendo che tali misure derogatorie debbano essere necessarie, opportune e proporzionate allo scopo. La normativa statale non può quindi essere sbilanciata arbitrariamente in favore della garanzia della sicurezza, a discapito dei diritti fondamentali alla riservatezza e alla protezione dei dati, e deve pertanto stabilire un corretto bilanciamento tra i diversi interessi in gioco.

Sulla base di questa disposizione, ampiamente utilizzata dagli Stati Membri soprattutto a seguito del crescente numero di attacchi terroristici che hanno colpito l'Europa, si era venuto a creare un panorama normativo in materia di *data retention* estremamente frammentato e diversificato da Stato a Stato, capace di incidere anche sulla circolazione dei servizi[4]. Tale situazione aveva spinto il legislatore sovranazionale ad armonizzare la materia mediante l'approvazione della tristemente nota Direttiva 2006/24/CE[5], dichiarata invalida dalla storica pronuncia *Digital Rights Ireland*[6]: le

[2] La Direttiva e-privacy impone infatti ai fornitori di servizi di comunicazioni elettroniche di cancellare o rendere anonimi i dati raccolti e conservati, una volta che essi non siano più necessari per la fornitura o la fatturazione dei servizi stessi. La normativa europea fa riferimento in particolare a quelli che vengono definiti "dati relativi al traffico" (art. 2, lettera b), nonché ai "dati relativi all'ubicazione" (art. 2, lettera c): queste informazioni permettono di individuare fonte, destinatario, data, ora, durata, localizzazione e tipo di comunicazione. Pur non riguardando il contenuto delle comunicazioni, tali dati (cd. metadati) sono di estrema delicatezza e, come la costante giurisprudenza della Corte di Giustizia dell'UE ha sempre affermato, "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 permanenti 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, pronuncia *Digital Rights Ireland*).

[3] "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", art. 15, co. 1, Dir. 2002/58/CE.

[4] Si leggano più ampiamente sul punto le considerazioni espresse a livello europeo in EUROPEAN COMMISSION, *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.

[5] 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 e che modifica la Direttiva 2002/58/CE, cd. Data Retention Directive. Riconoscendo le potenzialità offerte dall'uso delle comunicazioni elettroniche, come emerge dai Considerando da 7 a 11 della Direttiva 2006/24, il legislatore europeo giunge ad affermare la necessità di "garantire a livello europeo la conservazione, per un

disposizioni contenute nella normativa europea non avevano superato il test di proporzionalità, risultando in una compressione dei diritti fondamentali non limitata allo stretto necessario. Non potendo in questa sede soffermarci sui numerosi rilievi emersi da questa decisione, ciò che qui interessa ai fini della ricostruzione del quadro attuale è il vuoto normativo che si era venuto successivamente a creare in materia di conservazione dei dati per finalità di sicurezza e che aveva portato ad una ri-espansione della disciplina dettata in materia dalla Direttiva 2002/58/CE[7]. In un simile contesto, si è dunque registrato nuovamente il formarsi di una realtà normativa estremamente complessa: se da un lato, infatti, l'invalidità della *Digital Rights Ireland* non aveva toccato direttamente le legislazioni nazionali adottate in attuazione della Direttiva 2006/24/CE, dall'altro, con riguardo a queste ultime, sono spesso sorti dubbi di legittimità costituzionale o di conformità della normativa interna rispetto ai parametri indicati dalla Corte di Giustizia, registrandosi così differenti reazioni[8]. Che fosse a seguito della dichiarazione di incostituzionalità della previa

certo periodo di tempo, alle condizioni previste dalla presente Direttiva, dei dati generati o trattati dai fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione" (considerando 11), mediante l'armonizzazione resa possibile dall'approvazione di una Direttiva in materia.

[6] Corte di Giustizia dell'Unione Europea, Grande Sezione, 8 aprile 2014, cause riunite C-293/14 e C-594/12, *Digital Rights Ireland Ltd, Seitlinger e a.* Per una completa ricostruzione e analisi critica della pronuncia *Digital Rights Ireland*, si vedano, tra la folta dottrina in merito: L. TRUCCO, *Data retention: la Corte di giustizia si appella alla Carta UE dei diritti fondamentali,* in *Giur. It.*, 2014, 8-9, 1850 ss; F. FABBRINI, *The European Court of Justice ruling in the Data retention case and its lessons for privacy and surveillance in the US*, in *Harvard Human Rights Journal*, 28/2015, 65 ss.; R. FLOR*, La Corte di Giustizia considera la direttiva europea 2006/24 sulla c.d. data retention contraria ai diritti fondamentali. Una lunga storia a lieto fine?* in *Dir. Pen. Cont.,* 2/2014, 178 ss.; O. POLLICINO, *Interpretazione o manipolazione? La Corte di giustizia definisce un nuovo diritto alla privacy digitale*, in *Federalismi.it,* 3/2014; A. VEDASCHI*, I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Dir Pubb Comp ed Eur*, 3/2014; M. P. GRANGER, K. IRON, *The Court of Justice and the Data retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching lesson in privacy and data protection*, in *European Law Review*, 39 (6), 2014, 835 ss.; A. VEDASCHI, V. LUBELLO*, Data retention and its implications for the fundamental right to privacy: a European perspective*, in *Tilburg Law Review*, 14/2015; L. MARIN, *The fate of the Data retention Directive: about mass surveillance and fundamental rights in the EU legal order*, in V. MITSILEGAS e al. (a cura di), *Research Handbook on Eu Criminal Law*, Elgar Publishing, 2016; O. LYNSKEY, *The Data retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Common Market Law Review*, 51 (6), 2016, 1789 ss.

[7] La Direttiva e-privacy dunque è rimasta, da allora, l'unica fonte legislativa europea in tema di conservazione dei dati relativi a comunicazioni elettroniche e che prevede la possibilità di deroghe per scopi securitari o investigativi, come stabilito all'art. 15. Come si avrà modo di vedere più approfonditamente in seguito, è al momento al vaglio del Consiglio europeo la proposta di modifica della Direttiva e-privacy con un Regolamento (COM (2017) 10: *Proposal for a Regulation of the European Parliament 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*), che andrebbe quindi a sostituire anche il controverso art. 15.

[8] Taluni Stati avevano modificato la normativa nazionale di recepimento della direttiva europea invalidata, direttamente mediante l'intervento del legislatore, in modo da adeguarla ai principi indicati dalla CGUE; altri non erano invece intervenuti in alcun modo, mantenendo invariata la propria disciplina in materia (Italia, Portogallo); per altri ancora invece è stato decisivo l'intervento dei giudici, chiamati spesso a valutare la legittimità delle norme interne in

normativa o di una decisione del legislatore, molti Stati membri si sono dunque dotati di nuove legislazioni in materia di conservazione e accesso ai dati relativi alle telecomunicazioni, approvate sulla base di quella deroga concessa dal redivivo art. 15, Dir. 2002/58/CE. La vaghezza e l'ampiezza di quella disposizione, i dubbi persistenti circa i limiti ad essa legati, l'attivismo di singoli cittadini, politici o organizzazioni a tutela dei diritti fondamentali davanti ai tribunali nazionali, non hanno reso necessario attendere molto tempo prima che l'intervento della Corte di Giustizia dell'Unione Europea (CGUE) fosse nuovamente invocato. Questa volta però la richiesta era quella di fornire indicazioni relative all'interpretazione, alla luce della Carta di Nizza, di quel problematico art. 15 che si inseriva ormai in un contesto di principi fissati dalla giurisprudenza sovranazionale: questa, nel corso degli anni, aveva consolidato sempre più un elevato standard di tutela dei diritti alla riservatezza e protezione dei dati, anche a fronte di esigenze securitarie[9].

Si arriva così nel 2016 alla storica pronuncia da parte dei giudici di Lussemburgo, nel già richiamato caso *Tele2 Sverige*[10]. Con un restrittivo test di proporzionalità, la decisione giunge ad affermare che una normativa nazionale che preveda una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e all'ubicazione di tutti gli abbonati e utenti iscritti a servizi di comunicazione elettronica, non rispetta le condizioni di stretta necessità e non rappresenta quindi una corretta applicazione dell'art. 15, Direttiva e-privacy[11].

---

materia di *data retention*, giungendo all'annullamento o disapplicazione delle disposizioni nazionali (Belgio). Per un maggiore approfondimento: S. CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del Sistema UE di protezione dei dati*, in *Rivista italiana di Diritto Pubblico Comparato*, 3/2015, 819 ss.; A. ARENA, *La Corte di Giustizia sulla conservazione dei dati: quali conseguenza per le misure nazionali di recepimento?*, in *Quaderni Costituzionali*, 3/2014, 722 ss.; F. BOEHM, M. D. COLE, *Data retention after the judgement of the Court of Justice of the European Union Study*, Study for the Greens/EFA Group in the European Parliament, 30 giugno 2014. Merita rilevare, per completezza, che già prima della pronuncia *Digital Rights Ireland,* alcuni Stati membri avevano sollevato, all'interno del contesto nazionale, dubbi di conformità delle norme di recepimento della Data Retention Directive rispetto alla tutela costituzionale del diritto alla riservatezza. Così la Corte costituzionale tedesca, quella bulgara, rumena e cipriota, ben prima dell'intervento della CGUE, avevano dichiarato incostituzionali le leggi di attuazione della direttiva europea in materia di conservazione dei dati. Per una ricostruzione del tema, si legga: N. VAINIO, S. MIETTENIN, *Telecommunications data retention after Digital Rights Ireland: legislative and judicial reactions in the Member States*, in *International Journal of Law, Information and Technology*, 23/2015, 290 ss.; 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 rivolta alle discipline nazionali*, in *DPCE on line*, 2/2017.

[9] Corte di Giustizia dell'Unione Europea, 13 maggio 2014, C-131/12, *Google Spain SL*, *Google Inc. v. Agencia Espanola de Proteccion de Datos e Mario Costeja Gonzalez*; Corte di Giustizia dell'Unione Europea, 6 ottobre 2015, C-362/14, *Maximillian Schrems v. Data protection commissioner*. Diventava quindi di primaria importanza, in questo contesto di sempre maggiore espansione "giurisprudenziale" della tutela del diritto alla riservatezza, comprendere quanto la pronuncia *Digital Rights Ireland* e i principi in essa sanciti incidessero sui margini di autonomia lasciati agli Stati membri dall'art. 15 della Direttiva e-privacy.

[10] Corte di Giustizia dell'Unione Europea, Grande Sezione, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e a.*

[11] "Per contro, l'art. 15, par. 1, della Direttiva 2002/58, letto alla luce degli articoli 7,8 e 11 nonché dell'articolo 52, par. 1, della Carta, non osta a che uno Stato membro adotti una normativa la quale consenta, a titolo preventivo, la

Quanto maggiormente rileva, ai fini dell'analisi della recente pronuncia *Ministerio Fiscal,* è tuttavia il *reasoning* della Corte nella seconda questione pregiudiziale, ovvero quella riguardante l'accesso delle autorità nazionali competenti ai dati conservati. Prima di stabilire le condizioni che le normative nazionali adottate ex art. 15 devono possedere per rispettare il requisito di stretta necessità[12], anche sotto il profilo dell'accesso, i giudici evidenziano un importante rapporto consequenziale: quello tra obiettivo perseguito dalla normativa che regola l'accesso ai dati e gravità dell'ingerenza nei diritti fondamentali. Ciò li porta a concludere che solo la lotta contro la criminalità grave è in grado di giustificare "un simile" accesso ai dati. Tale interpretazione, è bene rilevarlo sin da ora, aggiunge un tassello rilevante al semplice dato letterale dell'art. 15 della Direttiva e-privacy: quest'ultimo, infatti, fornendo l'elenco degli obiettivi ritenuto dalla Corte tassativo e che quindi giustificano l'adozione di norme nazionali in deroga ai principi generali della Direttiva stessa, parla genericamente di prevenzione, ricerca, accertamento e perseguimento di attività criminali, senza connotarle ulteriormente con il criterio di "gravità". I giudici di

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 comunicazioni interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario", par. 108. La Corte afferma dunque la legittimità di quella che può essere definita una *targeted data retention*, che, come vedremo, pone non poche problematiche sul fronte della sua concreta realizzabilità, utilità ma anche legittimità. Per una completa ricostruzione dei rilievi di questa complessa pronuncia, si leggano, tra i tanti: 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 *European Law Analysis Blog*, 21 dicembre 2016, http://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html; I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 5/2017, 1467 ss.; P. SCHAAR, *New ECJ ruling on data retention: preservation of civil rights even in difficult times!*, in https://www.eaid-berlin.de/?p=1545, 22 dicembre 2016; L. SCAFFARDI, *Data retention e diritti della persona*, in *Costituzionalismo.it*, 2/2017; G. TIBERI*, Il caso Tele2 Sverige/Watson: una iconica sentenza della Corte di Giustizia nella saga sulla Data retention*, in *Quaderni Costituzionali,* 2/2017, 434 ss.; O. POLLICINO, G.E. VIGEVANI, *Privacy digitale e conservazione dei dati di traffico per finalità di sicurezza: la sentenza Tele2 Sverige della Corte di giustizia UE*, in *Forum di Quaderni Costituzionali,* 1/2017; X. TRACOL, *The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level*, in *Computer Law and Science Review*, 4/2017, 541 ss.

[12] La CGUE afferma infatti che l'accesso delle autorità nazionali ai dati conservati debba avvenire solo nei limiti dello stretto necessario. Perché questo si realizzi, il legislatore deve prevedere norme che stabiliscano in maniera chiara e precisa le circostanze e le condizioni (sostanziali, procedurali e fondate su criteri oggettivi) alle quali i fornitori in possesso dei dati debbano concedere l'accesso alle autorità nazionali (par. 117-118). I giudici di Lussemburgo si spingono oltre: l'accesso può essere concesso, in linea di principio, solo relativamente ai dati di persone sospettate "di progettare, commettere o aver commesso una violazione grave, o anche di essere implicate in una maniera o in un'altra in una violazione siffatta", specificando che in casi di tutela di interessi vitali della sicurezza nazionale, l'accesso sia consentito "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). L'accesso viene quindi subordinato ad un controllo preventivo effettuato da un giudice o un'entità amministrativa indipendente, a seguito di una richiesta motivata delle autorità nazionali (par. 120), che dovrà peraltro essere seguita dalla notizia di accesso alle persone interessate (par. 121), nel momento in ciò non comporti più una compromissione delle indagini.

Lussemburgo, applicando il principio di proporzionalità e disponendo un tale legame tra grado di ingerenza e finalità dell'accesso, giungono a richiedere la "gravità" dell'obiettivo perseguito, ovvero la lotta alla criminalità grave, quale condizione necessaria e rafforzata per ammettere l'accesso stesso, che, merita ricordarlo, era caratterizzato in quel caso da confini ampi e che implicava per questo una ingerenza notevole nella riservatezza dell'utente dal quale i dati provenivano.

Dopo questa seppur breve ricostruzione della cornice attuale in materia di riservatezza delle comunicazioni elettroniche, è possibile chiedersi se, anche alla luce della pronuncia *Tele2 Sverige*, le questioni relative alla conservazione e all'accesso ai dati siano da ritenersi definitivamente chiarite. La Corte, con la sua giurisprudenza, ha fornito criteri dettagliati che arricchiscono di limiti e di condizioni specifiche il dettato piuttosto generico e riassuntivo dell'art. 15, Direttiva e-privacy: ogni dubbio quindi è risolto?

Una risposta a questa domanda, è stata fornita dalla recente decisione *Ministerio Fiscal*, che origina proprio dai dubbi degli Stati membri stessi che, non potendo da un lato ignorare la ricca giurisprudenza europea sul tema della riservatezza delle comunicazioni elettroniche, faticano dall'altro a comprenderne e applicarne tutti i principi e criteri, anche - e soprattutto - dopo la *Tele2 Sverige*[13].

3. *Un nuovo tratto: la pronuncia Ministerio Fiscal*

Ripercorrendo dunque quel tortuoso percorso fatto di intrecci tra normative nazionali e disposizioni sovranazionali, di tentativi di armonizzazione e interventi giurisprudenziali, giungiamo alla recente pronuncia *Ministerio Fiscal*. Appare quindi chiaro come, con questa decisione, sia stata ancora una volta offerta ai giudici di Lussemburgo l'occasione di svolgere quella operazione, già iniziata con la *Tele2 Sverige,* di lettura e interpretazione in chiave "costituzionale" dell'art. 15 della Direttiva 2002/58/CE[14]. Questa volta, però, i dubbi del giudice del rinvio si sono concentrati

[13] Gli Stati membri stessi si erano posti questa domanda anche a seguito della pronuncia *Tele2*, dinnanzi alla quale essi hanno reagito in maniera differente: alcuni si sono interrogati sulla necessità di modificare ancora una volta la normativa nazionale per renderla conforme ai principi delineati nella più recente decisione della CGUE. In alcuni Paesi, come vedremo, la legislazione in materia di *data retention* è stata nuovamente portata all'attenzione dei giudici nazionali (come nel caso del Belgio e del Regno Unito). Per una ricostruzione delle reazioni alla pronuncia *Tele2*, si veda PRIVACY INTERNATIONAL, *National data retention laws since the CJEU's Tele2/Watson Judgement (September 2017)*, https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf.

[14] Tale operazione interpretativa, che si estrinseca in una serie di pronunce della CGUE in materia di garanzia della *privacy digitale,* come abbiamo visto, si può inserire in quella più ampia dinamica di "ridefinizione di un perimetro costituzionalmente orientato o quanto meno *human rights oriented* di disposizioni già in vigore quando la transizione da un'Europa dei mercati a un'Europa dei diritti non si era ancora del tutto completata", 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*

principalmente sul profilo dell'accesso ai dati e, in particolare, su quel criterio, indicato dalla previa giurisprudenza europea, di gravità dei reati.

La questione pregiudiziale trae origine da un caso di rapina ai danni del 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 le tracce del telefono: al fine di attivare una SIM, infatti, è necessario fornire, oltre alle informazioni relative all'identità del richiedente, anche il codice relativo all'identificatore internazionale di apparecchiature mobili (cd. IMEI). Ingiungendo alle compagnie telefoniche di accedere e comunicare i dati in loro possesso, sarebbe stato possibile risalire all'identità del soggetto che aveva attivato una utenza telefonica utilizzando il codice IMEI del dispositivo rubato; questi poteva dunque essere, presumibilmente, l'autore stesso del furto o comunque a conoscenza di informazioni utili alle indagini.

Il giudice istruttore si era però rifiutato di emanare l'ingiunzione richiesta dalla polizia: la legge 25/2007[15] stabiliva la possibilità di accesso e comunicazione dei dati conservati dai fornitori di servizi di telefonia solo in caso di reati gravi che, ai sensi del codice penale nazionale, erano quelli puniti con detenzione superiore a cinque anni. Poiché il furto non rientrava nella definizione spagnola di reato grave, la richiesta veniva respinta.

Il pubblico ministero proponeva appello avverso tale decisione di fronte alla *Audiencia Provincial de Tarragona*. Quest'ultima rilevava l'adozione di una ulteriore fonte normativa di riferimento, approvata in un momento successivo al provvedimento impugnato: la legge organica 13/2015[16]. Tale normativa andava ad incidere sulle modalità di determinazione del concetto di "gravità" del reato, stabilendo due criteri alternativi: un criterio materiale (rilevanza criminosa della condotta e grave lesione dei beni giuridici) e uno normativo formale, meramente basato sulla durata della pena che, per determinare la gravità del reato, doveva essere non inferiore a tre anni. Ebbene, quest'ultimo criterio, che avrebbe potuto potenzialmente portare al di sopra della soglia di gravità la maggior parte dei reati, faceva sorgere in capo al giudice dell'appello un dubbio di conformità della normativa rispetto alla tutela dei diritti fondamentali sanciti dalla Carta di Nizza e dai principi enucleati della Corte di Giustizia nella pronuncia *Digital Rights Ireland*[17]. Di fronte a tali dubbi il

di sicurezza e ordine pubblico, in *Diritto Penale Contemporaneo,* 9 gennaio 2017, https://www.penalecontemporaneo.it/upload/POLLICINOBASSINI_2017a.pdf.

[15] 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 Dir. 2006/24/CE.

[16] 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.

[17] Merita tuttavia precisare che la nozione di reato grave, diversamente da quanto previsto nella Direttiva e-privacy, era espressamente inserita nella Direttiva 2006/24, oggetto della *Digital Rights Ireland* (Considerando 9, Considerando 21 e art. 1, par. 1). Nella pronuncia *Tele2 Sverige* invece, distanziandosi dal dato letterale dell'art. 15 Dir. 2002/58/CE, la Corte riprende e mutua il criterio di "gravità del reato", trasponendolo nella valutazione di conformità al diritto europeo delle norme nazionali adottate ex art. 15, e identificandolo come uno dei criteri giustificativi della conservazione dei dati e dell'accesso agli stessi a scopi investigativi, capace di legittimare l'ingerenza nei diritti fondamentali. Questo aspetto è di grande importanza per una analisi critica della pronuncia in esame.

giudice spagnolo sottoponeva dunque alla Corte di Giustizia due questioni pregiudiziali, chiedendo (i) quale dei criteri individuati dalla più recente normativa spagnola fosse corretto, se quello formale o materiale, e (ii) chiedendo in subordine che fosse specificata la compatibilità "rispetto ai principi costituzionali dell'Unione" di una soglia di tre anni di reclusione come criterio formale di gravità del crimine. Merita sottolineare come il rinvio pregiudiziale descritto, proposto nell'aprile 2016, fosse stato sospeso in attesa della pronuncia nel caso *Tele2 Sverige* che avrebbe potuto, potenzialmente, 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 Sverige*) 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"[18].

Sin da questo primo aspetto emerge con chiarezza dunque come anche a seguito della *Tele2 Sverige* permangano dubbi relativamente ai limiti e all'interpretazione dell'art. 15 della Direttiva e-privacy. Ecco allora che si può affermare come i criteri individuati fino ad allora dalla giurisprudenza europea per legittimare l'adozione di una normativa nazionale restrittiva dei diritti alla riservatezza e protezione dei dati non risultino del tutto chiari e precisamente determinati. Come vedremo, la decisione in esame non è figlia unica della situazione venutasi a creare a seguito delle vicende di *Tele2 Sverige*: altri rinvii pregiudiziali, al momento pendenti e riguardanti vari aspetti della conservazione e accesso ai dati, testimoniano come la nota pronuncia del 2016, per quanto certamente rilevante, non abbia liberato il campo dalle perplessità.

Nel caso *Ministerio Fiscal* la Corte, con una decisione relativamente breve datata 2 ottobre 2018, risponde innanzitutto alle eccezioni di incompetenza sollevate dal governo spagnolo. Quest'ultimo ritiene infatti che la richiesta di accesso promossa dalle autorità nazionali rientri nell'esercizio dello *ius puniendi*, ricompreso nel novero delle attività escluse dall'ambito di applicazione della Direttiva 2002/58/CE, ai sensi del suo art. 1, co. 3[19]. Ripercorrendo lo stesso ragionamento seguito nella pronuncia *Tele2 Sverige* (e, come vedremo, non senza problemi), la Corte afferma invece che le normative nazionali adottate sulla base della deroga sancita dall'art. 15 della Direttiva e-privacy, vengono per ciò stesso "attirate" nell'ambito di applicazione della Direttiva stessa, 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 stabilisce, infatti, le condizioni

[18] Conclusioni dell'Avvocato generale Henrik Saugmandsgaard Øe, 3 maggio 2018, par. 27.

[19] "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", art. 1, co. 3, Dir. 2002/58/CE.

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[20].

Sempre con un breve paragrafo e sempre - forse sbrigativamente - richiamando le conclusioni adottate sul tema nella pronuncia *Tele2,* i giudici di Lussemburgo risolvono un altro nodo problematico attinente la propria competenza: la Corte, infatti, afferma la riconducibilità alla Direttiva e-privacy non solo delle norme in materia di *data retention*, ma anche di quelle riguardanti l'accesso delle autorità statali ai dati conservati dai fornitori di servizi di comunicazioni elettroniche. Siccome le attività di accesso, al pari di quelle di conservazione, prevedono un trattamento dei dati[21], tali operazioni sono riconducibili a soggetti privati e non a soggetti pubblici o autorità dello Stato, considerato che il trattamento rientra nelle attività svolte da fornitori di servizi e disciplinate dalla Dir. 2002/58 (par. 37-38).

Risolta la questione preliminare della competenza della Corte e affermata la ricevibilità delle questioni poste, che presentano un rapporto diretto con l'oggetto della controversia principale (par. 46), i giudici passano dunque all'analisi del merito.

Va sottolineata a tal proposito una prima fondamentale decisione: seguendo le argomentazioni ben più elaborate dell'Avvocato generale nelle sue Conclusioni, la prima domanda pregiudiziale proposta dal giudice spagnolo viene riletta dalla Corte e fatta precedere dall'introduzione di un passaggio preliminare aggiuntivo. Per stabilire quale tipo di criterio debba essere utilizzato per determinare la gravità di un reato, è necessario prima valutare se l'ingerenza rispetto ai diritti fondamentali sia tale da richiedere, sulla base di quanto espresso nel diritto e nella giurisprudenza europea, la presenza di un reato grave per poter essere legittimata.

Questa riformulazione[22] porta la Corte a ricondurre le questioni promosse dal giudice del rinvio all'interpretazione dell'art. 15 della Direttiva 2002/58, con riferimento, in questo specifico caso, ai requisiti relativi all'accesso da parte di autorità pubbliche ad una particolare e ristretta categoria di dati, cioè, è bene tenerlo sin da ora a mente, 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). L'interpretazione dell'art. 15, dunque, è volta a determinare innanzitutto se l'accesso a quella particolare tipologia di dati comporti una ingerenza nei diritti fondamentali tale da richiedere, per essere giustificata e legittimata come finalità, la lotta contro la criminalità grave. Solo dopo aver risposto a tale quesito ci si potrà quindi chiedere quali criteri debbano essere usati

[20] Sul punto si legga anche par. 53, Conclusioni Avvocato generale, che al par. 56 richiama inoltre l'orientamento della giurisprudenza della Corte EDU in materia.

[21] Su questo punto, cioè sulla natura di trattamento del dato rappresentata dalle attività di accesso ai dati stessi, la Corte richiama peraltro il parere 1/15 (Accordo PNR EU-Canada) del 26 luglio 2017, in cui si afferma appunto che l'accesso, costituendo una forma di trattamento del dato, rappresenta una ingerenza rispetto al diritto sancito all'art. 8 della Carta di Nizza (par. 51).

[22] "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 vedi anche par. 87.

per determinare la gravità o meno del reato, rispondendo solo successivamente agli interrogativi posti dal giudice spagnolo.

Seguendo questo iter argomentativo, la Corte specifica preventivamente che non saranno oggetto di valutazione né la conformità della conservazione[23] dei dati né tanto meno ogni altro requisito di accesso individuato dalla previa giurisprudenza europea: questi aspetti restano pertanto esclusi dal vaglio della Corte in detta decisione. Pur premettendo che l'art. 15, come già sottolineato nel precedente paragrafo, si limita a parlare di lotta ai crimini, senza alcuna ulteriore accezione, i giudici risolvono la questione di merito richiamando quel rapporto consequenziale tra obiettivo perseguito e gravità dell'ingerenza già affermato nella pronuncia *Tele2 Sverige*. 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 verrà richiesta, ai fini della legittimità dell'accesso e dell'obiettivo perseguito mediante esso, la presenza di un reato grave. Ecco dunque che, per comprendere se sia richiesta la natura grave del reato, si rende necessaria una previa valutazione circa la natura grave o meno dell'ingerenza.

Nel caso *Tele2 Sverige* la Corte aveva ritenuto sussistente una ingerenza grave rispetto ai diritti fondamentali poiché l'accesso aveva ad oggetto una mole indiscriminata di dati personali 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 Sverige*). Nel caso in esame invece, come sottolineano i giudici, l'accesso ha ad oggetto non solo un ristretto numero di dati ovvero solo i numeri di telefono legati alla carta SIM attivata usando il codice IMEI del telefono rubato, ma anche una ristretta tipologia di dati ovvero solo quelli identificativi del soggetto titolare di tale carta, ristretti inoltre ad uno specifico e limitato periodo di tempo di dodici giorni (par. 59)[24].

---

[23] "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, Dir. 2002/58/CE.

[24] "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 la diversa conclusione cui i giudici giungono circa la natura dei dati, rispetto al caso *Tele2 Sverige*. 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

Ne deriva che l'accesso a questa particolare tipologia di dati, che si può quasi definire un "*accesso targetizzato"* cioè che potremmo altrimenti definire mirato*,* non rappresenta una ingerenza grave nei diritti fondamentali degli interessati. Giunti a tale conclusione e applicando quel principio di proporzionalità prima individuato, ne deriva che tale ingerenza non richieda, per essere giustificata, la lotta ad un crimine grave[25]. Per usare le parole della Corte, l'accesso a questo tipo di dati comporta un'ingerenza "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). L'Avvocato generale, nelle proprie conclusioni, si spinge ad affermare 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 "reati" è idoneo a giustificare una siffatta ingerenza" (par. 89).

4. *Un'opera in evoluzione: prospettive future e questioni aperte*

Per quanto le questioni pregiudiziali poste dal giudice spagnolo siano state risolte dalla Corte di Giustizia in poche pagine, la pronuncia non è certo da ritenersi priva di novità interessanti e di molteplici spunti di riflessione, soprattutto se si procede allo sforzo di leggerla nel più ampio contesto post-*Tele2 Sverige*. Come si avrà modo di vedere, molti sono i dubbi e le perplessità che possono essere considerate retaggio ed eredità della previa giurisprudenza europea, così come molti sono i dubbi e le perplessità che anche a seguito di questa nuova decisione permangono.

È certamente importante però sgombrare sin da subito il campo da possibili letture eccessivamente estensive e per certi versi fuorvianti della portata della pronuncia analizzata. Una prima lettura disattenta, infatti, potrebbe portare a vedere nella posizione della Corte una sorta di "revirement" rispetto allo stringente requisito di gravità del reato indicato nella giurisprudenza *Tele2 Sverige*. In altre parole, si potrebbe ritenere che non sia più reputato necessario il criterio rafforzato di gravità del crimine per giustificare l'accesso da parte delle autorità nazionali ai dati conservati. Questa erronea interpretazione viene scongiurata, con grande chiarezza, dall'Avvocato generale che nelle sue conclusioni afferma chiaramente "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).

---

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).

[25] L'Avvocato generale non nega la sussistenza di una forma di ingerenza nel diritto alla riservatezza rappresentata dall'accesso ai dati e dalla loro comunicazione ad un terzo, ritenendo comunque poco rilevante a tal fine la natura sensibile o meno del dato o che dalla rivelazione di esso siano derivati inconvenienti per l'interessato (par. 76-77). Nelle sue Conclusioni tuttavia afferma come nel caso in esame sia mancante l'elemento della gravità dell'ingerenza che, altrimenti, richiederebbe una giustificazione rafforzata della normativa "ingerente".

La natura mirata dell'accesso, limitata nella estensione e nella tipologia dei dati richiesti nonché sotto il profilo della dimensione temporale, non può che differire fortemente da quell'accesso riferito ad un ventaglio più ampio di dati, che caratterizzava invece le vicende giurisprudenziali precedenti. La portata del ragionamento della Corte, 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.

Tenendo in considerazione questa premessa, utile a circoscrive il *reasoning* dei giudici di Lussemburgo, il primo punto delicato che emerge dalla lettura della pronuncia è certamente quello relativo alla competenza della Corte.

Quest'ultima, infatti, attinge a piene mani a quanto affermato nella *Tele2 Sverige*, richiamando i nodi più rilevanti che in quella sede avevano permesso di ricondurre nell'ambito di applicazione della Dir. 2002/58 le normative nazionali adottate sulla base dell'art. 15 non solo nella parte in cui esse disciplinavano la conservazione dei dati, ma anche dove si fa riferimento all'accesso ai dati raccolti e conservati[26]. In realtà questa conclusione non è e non era affatto di semplice soluzione e l'interpretazione della Corte, già all'epoca della pronuncia *Tele2 Sverige* non aveva mancato di sollevare perplessità[27]: nella soluzione del caso *Ministerio Fiscal*, incentrato unicamente sul tema dell'accesso ai dati da parte delle pubbliche autorità, si ripropongono in maniera ancora più marcata gli stessi dubbi del passato.

Secondo la ricostruzione del governo spagnolo, così come già il Regno Unito aveva fatto nel caso *Tele2 Sverige*, le attività di accesso ai dati, essendo operazioni proprie delle autorità pubbliche nazionali, effettuate a scopi di indagine o garanzia della sicurezza, dovrebbero rientrare in quelle azioni escluse dall'ambito di applicazione della normativa e-privacy sulla base del già richiamato art. 1, co. 3. Questa lettura dunque indurrebbe ad affermare una distinzione tra attività strettamente relative alla conservazione dei dati e quelle invece relative all'accesso ad essi.

Del resto, una tale distinzione era stata proprio alla base della decisione *Ireland v. Parliament & Council* (C-301/06, 10 febbraio 2009), con cui la CGUE aveva fatto salva la Direttiva 2006/24/CE. In quel caso infatti l'Irlanda aveva richiesto l'annullamento della Direttiva sulla *data retention* in quanto considerata fondata su una base giuridica non adeguata: se infatti lo scopo fondamentale e pregnante della Direttiva era individuato dai ricorrenti nell'armonizzazione di normative nazionali che facilitassero l'accertamento e il perseguimento di reati, soprattutto a carattere terroristico, la corretta base giuridica non poteva essere individuata nell'art. 95 TCE che invece attribuiva a

[26] "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 Sverige*).

[27] D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* in *ERA Forum*, Springer, pubblicato online il 25 giugno 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),* op. cit.

Parlamento e Consiglio il potere di adottare Direttive vertenti sull'instaurazione e il funzionamento del mercato interno[28].

In questo caso, uno degli argomenti che aveva permesso alla Corte di affermare la correttezza della base giuridica e quindi di circoscrivere lo scopo della Dir. 2006/24/CE all'area del funzionamento del mercato interno e non all'allora III pilastro sulla cooperazione di polizia e giudiziaria, riguardava proprio l'affermazione della esclusione dall'ambito di applicazione della Direttiva 2006/24/CE di qualsiasi aspetto riguardante l'accesso ai dati. I giudici, infatti, avevano con chiarezza stabilito che la Direttiva in esame non si estendeva all'"attuazione di qualsiasi eventuale azione di cooperazione di polizia e giudiziaria in materia penale" (par. 83, *Ireland v. Parliament & Council*), non disciplinando né l'accesso ai dati né il loro uso da parte delle autorità di polizia o giudiziarie degli Stati membri. "Tali questioni, rientranti in linea di principio nell'ambito coperto dal titolo VI del Trattato UE, sono state escluse dalle disposizioni di detta Direttiva, com'è indicato segnatamente al venticinquesimo 'considerando' ed all'art. 4 di quest'ultima" (par. 84, *Ireland v. Parliament & Council*).

Questo *reasoning* della Corte, fondato pertanto sulla modulazione dell'ambito di applicazione della Dir. 2006/24/CE a seconda che si trattasse di accesso o di conservazione, non è stato trasposto anche con riferimento alla Direttiva e-privacy: nella pronuncia *Tele2 Sverige* ogni distinzione in merito a disciplina sulla conservazione dei dati e disciplina sull'accesso, viene meno. Anzi la Corte in questo senso opta per una "concezione unitaria che considera i due momenti della "conservazione" e dell'"accesso" come espressione di un atto invero complessivamente unitario"[29].

La Corte, con riferimento alla Dir. 2002/58/CE, fornisce una interpretazione da alcuni autori[30] ritenuta estensiva dell'art. 15, inteso dunque come comprensivo anche della disciplina sull'accesso. In quanto operazione attinente alle attività dello Stato, infatti, l'accesso richiede comunque un intervento del fornitore privato del servizio nonché un trattamento del dato stesso.

Sotto questo profilo, l'Avvocato generale nelle sue conclusioni aggiunge un ulteriore spunto di riflessione, proponendo una distinzione differente circa la natura dei dati, con il fine di ricondurre le operazioni dell'accesso nell'alveo delle attività comunque svolte dal soggetto privato fornitore del servizio e, quindi, della Dir. 2002/58/CE. In questo modo, rafforzando la posizione già tenuta dalla Corte nella pronuncia *Tele2 Sverige*, l'Avvocato generale afferma la necessità di distinguere i dati personali trattati direttamente all'interno di una attività dello Stato nel settore del diritto penale (ad esempio le intercettazioni, effettuate in maniera diretta dalle forze di polizia e quindi rientranti nel novero delle attività di natura sovrana dello Stato) e quelli invece trattati dai fornitori di servizi per

[28] Per una analisi approfondita: 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. 419; E. HERLIN-KARNELL, *Case C-301/06, Ireland v. Parliament and Council, Judgment of the Court (Grand Chamber) of 10 February 2009*, in *Common Market Law Review*, 46, 2009, 1667.

[29] 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*, op. cit., 5.

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

ragioni commerciali e solo successivamente utilizzati dalle autorità statali, come i dati in discussione. Sulla base di questa differenziazione, la prima tipologia di dati esulerebbe dall'ambito di applicazione della Direttiva e-privacy mentre la seconda, avendo alla base un trattamento che non rientra tra quelli esclusi dalla Direttiva stessa, sarebbe invece ricompresa.

Al di là del chiedersi se tale ricostruzione possa considerarsi riconciliabile con la posizione adottata dalla Corte nel precedente *Ireland v. Parlament & Council* e se la diversa normativa di riferimento (nel caso in esame la Dir. 2002/58/CE e non la Dir. 2006/24/CE come nel caso *Ireland v. Parlament & Council*) debba invece far ritenere inapplicabile lo stesso ragionamento anche alla Direttiva e-privacy, ciò che emerge con chiarezza è la complessità e delicatezza della questione.

Da un lato, ricomprendere le attività riguardanti l'accesso all'interno dell'ambito di applicazione della Direttiva permette alla Corte di pronunciarsi sul merito delle questioni e dunque di estendere il bilanciamento con i diritti fondamentali anche sul fronte di una operazione certamente invasiva nel diritto alla riservatezza, quale l'accesso. Dall'altro, pare altrettanto vero che il confine tra le attività ricomprese nella Direttiva e quelle invece escluse risulta estremamente sottile alla luce del *reasoning* della Corte. Tale percorso argomentativo, se allargato ai dati utilizzati - e quindi previamente trattati - dalle agenzie di intelligence, che possono essere trasmessi dai fornitori di comunicazioni elettroniche, potrebbe portare ad una estensione delle competenze dell'Unione Europea anche in ambiti, quali quello della sicurezza nazionale, prerogativa degli Stati membri[31].

Determinare il confine del ragionamento della Corte e della sua possibile estensione o limitazione è operazione estremamente delicata poiché non attiene solo il profilo formale della competenza, ma determina il fatto che i criteri espressi nella *Tele2 Sverige* relativamente all'accesso ai dati possano o meno estendersi anche a campi diversi da quelli della lotta alla criminalità grave, quali ad esempio le attività di intelligence.

A testimonianza di quanto questi timori e dubbi, derivanti dalla pronuncia *Tele2 Sverige,* siano ben chiari ai governi e ai giudici degli Stati membri, si può leggere il rinvio pregiudiziale, attualmente pendente dinnanzi alla CGUE[32], promosso dal Regno Unito. Esso, come si vedrà, verte proprio sulla applicabilità o meno dei criteri di accesso indicati dalla *Tele2 Sverige* anche ai casi in cui i dati siano finalizzati all'uso da parte delle agenzie di sicurezza e di intelligence nazionali e siano loro trasmessi in massa dai fornitori di servizi di comunicazione.

Si può comprendere sin da ora come le perplessità e gli interrogativi, originati dalla *Tele2 Sverige* in merito all'ambito di applicazione della Direttiva 2002/58/CE, rispetto a quanto estensivamente debbano essere applicate le prescrizioni delineate dal giudice di Lussemburgo in merito alle disposizioni nazionali adottate sulla base dell'art. 15, siano tutt'altro che risolti. La

[31] "What is perhaps of most concern – from the perspective of the principle of conferral – is that the same reasoning could justify the extension of the EU competence into the field of national security, which is placed beyond the scope of the EU law not only by Article 1 (3) of the e-privacy Directive but also by Article 4(2) TEU", D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* op. cit., 14.

[32] Domanda di pronuncia pregiudiziale proposta dall'Investigatory Powers Tribunal, Londra (Regno Unito) del 31 ottobre 2017 – *Privacy International/Secretary of State for Foreign and Commonwealth Affairs* e a., C-623/17.

pronuncia *Ministerio Fiscal* non sembra sotto questo profilo aggiungere elementi utili di soluzione: non a caso l'Avvocato generale sostiene nelle proprie Conclusioni che, per la risoluzione dei quesiti posti dal giudice spagnolo, non sia necessario occuparsi delle questioni emerse dal rinvio pregiudiziale promosso dal Regno Unito (par. 47).

Un altro nodo di rilievo che i giudici sono stati chiamati a trattare, in un certo senso preliminarmente rispetto alla soluzione del caso posto e in stretta connessione alle peculiarità dello stesso, è la questione attinente la natura dei dati oggetto di accesso.

Questi, come richiamato, sono relativi alla identificazione del nome, cognome ed eventualmente indirizzo del titolare della SIM, attivata mediante l'uso del codice IMEI del dispositivo rubato. Secondo i governi spagnolo, danese, irlandese, lettone, del Regno Unito e della Commissione, tali dati non possono essere ricondotti alla definizione di dati relativi al traffico o all'ubicazione di cui la Dir. 2002/58/CE si occupa e, per tale ragione, non sarebbero sottoposti alla disciplina di tale disposizione. Questa interpretazione, estremamente rilevante, viene rigettata dalla Corte che considera anche i dati identificativi come rientranti nella disciplina della Direttiva e-privacy, ritenendoli "necessari, da un punto di vista commerciale, alla fornitura dei servizi di comunicazione elettronica, quanto meno al fine di fatturare il servizio fornito, a prescindere dalle telefonate effettuate o meno nell'ambito della prestazione" (par. 53, Conclusioni dell'Avvocato generale)[33]. La Corte peraltro aggiunge, ancora più estensivamente, che la Direttiva 2002/58/CE 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, *Ministerio Fiscal*).

Venendo all'analisi del merito della decisione, deve essere prestata innanzitutto particolare attenzione all'effetto della riformulazione operata dalla Corte rispetto alle questioni pregiudiziali poste dal giudice spagnolo. Tale intervento di riscrittura delle questioni sottopostale, porta a ben vedere la Corte ad esimersi, secondo alcuni autori con un giudizio "tattico"[34], 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 come al termine della lettura della decisione non si riescano a trovare posizioni della Corte in merito: i giudici di Lussemburgo, infatti, hanno risolto la domanda

[33] 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 peraltro 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 secondo cui gli "entity data", ovvero quelli relativi all'identificazione dell'utente, non rientrerebbero nell'ambito di applicazione della Direttiva e-privacy e non si applicherebbero quindi ad essi i criteri individuati dalla *Tele2 Sverige*. La posizione della Corte di Giustizia dell'UE potrebbe dunque avere implicazioni anche sulla case-law inglese. 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.

[34] L. WOODS, *Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers*, in *EU Law Analysis*, op. cit.

derivante dalla riformulazione dei quesiti e alla luce di tale risposta non si sono spinti oltre. Quello che viene analizzato, in conclusione, pare essere non tanto la gravità in sé del reato o i criteri utili a definirla, bensì il suo rapporto con la gravità dell'ingerenza nei diritti fondamentali; si può quasi affermare, in ultima istanza, che i giudici si siano piuttosto pronunciati sulla determinazione della gravità dell'ingerenza e della sua relazione consequenziale con la necessaria gravità del reato. Il risultato pertanto è che l'esito del vaglio iniziale, frutto della riformulazione dei quesiti, ha portato a chiudere la decisione prima di arrivare ai punti che più interessavano ai giudici spagnoli. Ciò ha precluso alla Corte, seppur con un ragionamento logico e coerente, di occuparsi della individuazione dei criteri necessari ad affermare la gravità del reato, che non risultava, a quel punto, più necessaria nel caso caratterizzato da ingerenza non grave[35].

[35] 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 Sverige*) ha un rilievo importante; ciò non permette tuttavia di negare la mancata determinazione di una definizione di reato grave e dei criteri necessari per individuarlo. È da chiedersi dunque se la Corte potrà pronunciarsi su questo punto dinnanzi ad un nuovo rinvio pregiudiziale in un caso di ingerenza e lesione grave dei diritti fondamentali, richiedente pertanto la gravità del reato come elemento rafforzativo di legittimità. Merita comunque sottolineare come l'Avvocato generale, nelle sue Conclusioni, spinga la propria analisi a valutazioni attinenti anche ai criteri di determinazione della gravità del reato. Questo perché l'Avvocato propone 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 invece non è avvenuta. Pare utile mettere in luce, in questa sede, i punti salienti individuati dall'Avvocato: innanzitutto, alla luce della giurisprudenza *Digital Rights Ireland* e *Tele2 Sverige,* quella di reato grave non può essere considerata una nozione autonoma del diritto dell'Unione (93-101), la cui determinazione spetterebbe dunque agli Stati membri e non alla Corte. Alla luce comunque della disomogenità delle soluzioni normative e definitorie nazionali, l'Avvocato è 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 però: richiamando la necessità di una interpretazione restrittiva dell'art. 15 stesso, anche la nozione di "reato grave" deve essere restrittiva e intesa in modo non eccessivamente ampio da parte degli Stati membri. Ancora in subordine, se la Corte avesse ritenuto tale nozione come autonoma, la pronuncia dei giudici di Lussemburgo avrebbe dovuto spingersi a valutare anche i criteri che consentono di stabilire la gravità di un reato. In quel caso, l'Avvocato ha ritenuto necessario fondare la definizione di gravità su una pluralità di criteri di valutazione (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 ai requisiti del 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 europeo, viene ripreso quel principio, più volte affermato, secondo cui l'utilizzo della deroga prevista all'art. 15 deve rimanere una eccezione. Partendo da questa considerazione di base, anche in questo caso, l'Avvocato è giunto ad affermare come non sia possibile fissare una soglia, che pur rimane prerogativa degli Stati membri, talmente bassa "da far diventare principio l'eccezione" (par. 114). L'Avvocato ammonisce comunque la Corte dai rischi derivanti dalla determinazione giurisprudenziale di una soglia: "poiché una (simile) 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 determinare un quantitativo specifico, si conclude che gli Stati membri sono liberi di

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 appare al momento non poco disorientato. Questo perché i criteri, i principi e i limiti alla conservazione e all'accesso sono presenti e delineati primariamente dalla giurisprudenza europea, mentre il legislatore degli Stati membri sembra avere ancora dubbi su come applicarli, su come soddisfarli e dunque, problematicamente, su come metterli in pratica nella concretezza delle misure legislative.

Molto si è dibattuto e si dibatte tuttora sulla concreta attuabilità delle tutele indicate dalla Corte nelle sue storiche pronunce, soprattutto con riguardo alla disciplina della *data retention*: quest'ultima pare, per certi versi, mancare di un approccio pragmatico nell'effettuare il bilanciamento tra interessi in gioco, non considerando realmente la fattibilità di quanto scrive e pretende dal legislatore nazionale. Estremamente nota e delicata è, in questo contesto, la questione circa la realizzabilità di una forma di *targeted data retention*: escludendo una conservazione generalizzata, infatti, quella che i giudici indicano nella *Tele2 Sverige* pare essere una conservazione ristretta e mirata, che soddisfi e risponda a criteri oggettivi in grado di stabilire un rapporto tra i dati da conservare e l'obiettivo che si vuole raggiungere (par. 110), con la sussistenza di situazioni che forniscano una connessione, almeno indiretta, con atti di criminalità grave o con un rischio grave per la sicurezza pubblica (par. 111). Questi requisiti aprono scenari estremamente complessi e dibattuti, in particolare quando la Corte si spinge a consigliare che una delimitazione della conservazione dei dati possa essere ottenuta "mediante un criterio geografico qualora le autorità nazionali competenti considerino, 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). Una tale conservazione mirata, pur fondata su dati attendibili, può comunque ingenerare problemi di discriminazione e di possibile profilazione di soggetti solo perché appartenenti ad una area geografica considerata maggiormente a rischio, con una tutela della riservatezza quindi ristretta in maniera parimenti discriminatoria[36].

Emerge con chiarezza, in sostanza, come la Corte intenda supportare una *data retention* "successiva" e basata su sospetti giustificati (per quanto generici) piuttosto che una *data retention* "preventiva", non fondata su sospetti, ma anzi giustificativa essa stessa di sospetti che sorgono proprio a seguito della conservazione.[37] Così facendo, tuttavia, si pone in discussione l'utilità stessa della *data retention*, che fonda la propria forza proprio sul rendere possibile un "andare indietro nel tempo", che permette di esercitare un controllo su persone prima mai e in alcun modo sospettate[38].

---

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).

[36] D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* op. cit., 18.

[37] 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),* op. cit.

[38] "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. Targeted *data retention*, however this is constructed, cannot satisfactorily replace a general duty of retention.", I. CAMERON,

In questo contesto di difficile applicazione dei criteri individuati dalla giurisprudenza europea in materia, in particolar modo con riferimento alla conservazione dei dati, la pronuncia *Ministerio Fiscal* lascia da parte ogni questione relativa alla legittimità della disciplina sulla *data retention*. Se questo è certamente utile per la definizione dei quesiti posti all'attenzione dei giudici, che si concentrano sulla dimensione dell'accesso ai dati, una tale visione può 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. Una conservazione del dato è infatti prerequisito fondamentale per poter procedere successivamente ad un accesso. Pur non trattando la questione relativa alla conservazione, non di meno viene da chiedersi quali potrebbero essere le conseguenze o l'impatto del ragionamento della Corte, riferito all'accesso, rispetto alla disciplina della *data retention*. In altre parole, il quesito che emerge è se sia possibile parlare di accesso mirato o meno, se prima alla base non vi è una conservazione generalizzata o se e in quale misura, avendo come base una conservazione mirata, sia possibile parlare nella stessa misura di requisiti necessari per un legittimo accesso.

Chiarire questi punti avrebbe forse potuto aiutare ulteriormente gli Stati membri che, mediante l'opera dei propri giudici, giungono spesso a porre quesiti alla Corte di Giustizia dell'Unione Europea sulla regolamentazione di attività vitali per la garanzia della sicurezza, ma estremamente controverse da disciplinare.

Ciò è testimoniato dai rinvii pregiudiziali, al momento pendenti dinnanzi alla CGUE. Uno di questi è proprio la già richiamata domanda pregiudiziale promossa dall'*Investigatory Powers Tribunal*[39] del Regno Unito. Non è un caso che tale rinvio provenga proprio dal Regno Unito che, sotto il profilo della disciplina della *data retention* e dell'accesso ai dati, presenta una storia normativa e giurisprudenziale estremamente complessa e travagliata, resa ancora più intricata dalle ombre della incombente Brexit. Non potendoci qui soffermare su tutte le vicende che hanno caratterizzato l'esperienza britannica successivamente al caso *Tele2 Sverige*[40], si vuole qui porre

Balancing data protection and law enforcement needs: Tele2 Sverige and Watson, in *Common Market Law Review* op. cit.

[39] Questo organo giudiziario è preposto a decidere sui ricorsi aventi ad oggetto possibili violazioni dei diritti fondamentali dei cittadini ad opera di attività svolte di autorità pubbliche, agenzie di sicurezza e intelligence, con riferimento soprattutto a casi di lesione del diritto alla riservatezza perpetrati mediante l'utilizzo di mezzi di indagine occulta da parte di agenzie di sorveglianza e intelligence.

[40] Non possono non essere qui richiamati innanzitutto il caso *Secretary of State for the Home Department v. Watson & Others (2018) EWCA Civ 70* (con cui la Corte d'Appello si è pronunciata sul caso *Watson*, da cui ha avuto origine la decisione *Tele2 Sverige,* una volta tornato dinnanzi al giudice del rinvio) e il caso *Liberty v. Secretary of State for the Home Department (2018) EWHC 975,* deciso dalla *High Court* il 27 aprile 2018. Mentre il primo giudizio aveva ad oggetto la precedente normativa in materia di conservazione e accesso ai dati (*Data retention* and Investigatory Powers Act, DRIPA, 2014), il secondo riguardava invece la normativa attualmente vigente e sostitutiva del DRIPA, ovvero l'Investigatory Powers Act (IPA), adottato nel 2016 nelle more del caso *Tele2 Sverige*. Merita solo accennare all'esito di questa ultima pronuncia che ha stabilito la non conformità ai diritti fondamentali tutelati dalla Carta di Nizza della Parte 4 dell'IPA, assegnando al Governo e al Parlamento un termine di tempo per adeguarne il contenuto (adempimento che è stato in parte rispettato, mediante la adozione di emendamenti al testo originario dell'IPA, a far data dal 1

l'accento sulle questioni sollevate dal tribunale inglese. Questo si è infatti interrogato sull'applicabilità - e dunque sull'estensione - di quelle che chiama emblematicamente le "prescrizioni della pronuncia Watson" rispetto alle attività svolte da agenzie di sicurezza e di intelligence (SIA). Il giudice d'oltremanica rileva che l'utilizzo e la conservazione da parte di queste ultime dei dati di comunicazione di massa (quindi anche dei dati e metadati derivanti dalle comunicazioni elettroniche, disciplinate dalla Dir. 2002/58/CE) costituiscono elemento essenziale per la tutela della sicurezza nazionale, consentendo di rilevare minacce prima ignote, che solo una raccolta di dati non mirata permette[41]. La Corte del Regno Unito dunque si chiede se le prescrizioni indicate nella pronuncia *Tele2 Sverige* relativamente all'accesso[42] e riguardanti dati trasmessi in massa dai fornitori di servizi, debbano considerarsi applicabili anche nel caso in cui tale accesso riguardi le attività delle SIA. Viene chiesto in altre parole se e in quali limiti l'ambito di applicazione del diritto dell'Unione e della Dir. 2002/58/CE si estenda anche all'ordine (proveniente, nel caso del Regno Unito, dal *Secretary of State*) rivolto ad un gestore di servizi di comunicazione elettronica, avente ad oggetto la fornitura in massa di dati di comunicazione alle agenzie SIA.

Merita sin da ora rilevare come anche in questo caso la questione sollevata riguardi l'accesso ai dati, senza considerare dunque la conformità o meno della conservazione dei dati stessi; anche in questo caso, peraltro, come già rilevato nella *Tele2 Sverige* e ripreso nella *Ministerio Fiscal*, emerge come ancora problematica e bisognosa di chiarimento la delimitazione del campo di applicazione della Direttiva e-privacy rispetto ad attività che parrebbero esclusivo appannaggio degli Stati membri, come la sicurezza nazionale, come emerge dall'espresso richiamo sia dell'art. 1, par. 3 della Direttiva stessa che, più generalmente, dell'art. 4 TUE.

A dimostrazione della grande attualità e rilevanza delle questioni irrisolte lasciate aperte dalla pronuncia *Tele2 Sverige*, più recentemente anche la Corte costituzionale del Belgio ha promosso domanda di rinvio pregiudiziale, avente ad oggetto proprio l'interpretazione dell'art. 15 della Dir. 2002/58/CE[43]. In questa nuova richiesta di intervento della CGUE, i giudici belgi si sono chiesti se

novembre 2018). Per approfondimenti si legga: M. WHITE, *Data retention is still here to stay, for now…*, in *EU Law Analysis Blog*, 5 febbraio 2018, http://eulawanalysis.blogspot.com/2018/02/data-retention-is-still-here-to-stay.html; M. WHITE, *The Privacy International case in the IPT: respecting the right to privacy?*, in *EU Law Analysis Blog*, 14 settembre 2017, http://eulawanalysis.blogspot.com/2017/09/the-privacy-international-case-in-ipt.html.

[41] Nel rinvio pregiudiziale si legge infatti: "tenuto conto dell'esigenza fondamentale delle SIA di utilizzare tecniche di acquisizione in massa e di trattamento automatizzato per proteggere la sicurezza nazionale", in Domanda di pronuncia pregiudiziale proposta dall'*Investigatory Powers Tribunal*, Londra (Regno Unito) il 31 ottobre 2017 – *Privacy International/Secretary of State for Foreign and Commonwealth Affairs* e a., C-623/17.

[42] Richiamate in questa analisi alla nota 12.

[43] Domanda di pronuncia pregiudiziale proposta dalla Cour constitutionnelle (Belgio) il 2 agosto 2018, Causa C-520/18. Il caso trae origine da alcuni ricorsi promossi, a seguito della decisione *Tele2 Sverige*, avverso la normativa nazionale "*loi du 29 mai 2016 relative aux communications électroniques*", del 18 luglio 2016, ritenuta non conforme ai principi individuati dalla CGUE nella sua giursprudenza. È interessante sottolineare come la Corte costituzionale belga si fosse già in precedenza pronunciata, a seguito della decisione *Digital Rights Ireland*, sulla previa normativa nazionale in materia di *data retention* (*Loi du 30 juillet 2013*), annullandola con sentenza del 11 giugno 2015.

la discussa disposizione, letta alla luce non solo dei diritti al rispetto dei dati, ma anche del diritto alla sicurezza, tutelati dalla Carta di Nizza, impedisca agli Stati membri di adottare normative nazionali che prevedano un obbligo generale di conservazione dei dati in capo ai fornitori di servizi di comunicazioni elettroniche, non limitato alla lotta alla criminalità grave bensì esteso anche alla sicurezza nazionale, sicurezza pubblica, lotta a criminalità diversa da quella grave ma che sia in compenso soggetto a garanzie specifiche quanto a modalità di conservazione e accesso. La Corte costituzionale pare dunque offrire l'occasione alla Corte di Giustizia di meglio chiarire i limiti e i criteri indicati nella *Tele2 Sverige,* delimitandone i confini e l'estensione[44].

I giudici del rinvio poi rilevano, per quanto qui interessa, un ulteriore profilo problematico e di grande rilevanza pratica, non ancora affrontato dai giudici di Lussemburgo: nel caso in cui la normativa nazionale in campo di conservazione e accesso ai dati venga considerata, ad opera del giudice nazionale e sulla base dei principi fissati dalla giurisprudenza della CGUE, non conforme alle disposizioni del diritto europeo e al rispetto dei diritti fondamentali, quali sono le conseguenze e gli effetti sui dati raccolti e utilizzati sulla base di quella normativa? Ci si chiede, in altre parole, 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[45].

Il complesso panorama che si sta costruendo grazie alle pronunce della CGUE ma anche alla giurisprudenza degli organi di giustizia ordinaria e costituzionale degli Stati membri nonché ai rinvii pregiudiziali da essi promossi e di cui si è detto nelle pagine di questo lavoro, non può tuttavia dirsi completo senza un accenno anche alle attuali proposte legislative sul tavolo del legislatore europeo: in assenza di una precisa normativa sovranazionale in materia di *data retention*, che riempia il vuoto normativo lasciato dalla Dir. 2006/24/CE[46], è al momento in fase di

[44] 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/.

[45] Una simile questione è stata peraltro sollevata da un cittadino irlandese dinnanzi alla High Court nel caso *Dwyer v. Commissioner of An Garda Siochana & others,* n. 2015/351P, di cui si attende a breve la pronuncia.

[46] 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 dati 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*, 23 (3), 2016. Questo auspicio è stato sinora disatteso e pare continuerà ad esserlo.

discussione davanti al Consiglio una proposta[47] di Regolamento volto a sostituire la ormai datata Dir. 2002/58/CE. Dallo stato presente dei lavori emergerebbe la rinuncia all'adozione di una disposizione a sé stante in materia di *data retention* e accesso ai dati[48]. E' interessante però notare come anche nella proposta di Regolamento venga inserita una norma avente la stessa funzione dell'attuale art. 15 della Direttiva e-privacy, che al momento farebbe peraltro richiamo ad un elenco di eccezioni contenuto nell'art. 23 della *General Data Protection Regulation* 2016/679. Pare ancora presto per valutare l'efficacia e la portata della disposizione proposta (che è comunque stata sino ad ora soggetta a numerose modifiche nel corso del suo iter legislativo): quello che sembra evidente, tuttavia, è che l'assenza reiterata di una armonizzazione delle normative nazionali in materia di conservazione e criteri di accesso ai dati relativi alle comunicazioni elettroniche da parte delle autorità pubbliche, comporterà inevitabilmente il perdurare di un panorama frammentario all'interno dell'Unione, che continuerà a dare adito a diverse interpretazioni, anche mediante l'intervento di giudici nazionali e, come si è visto, sempre in più casi, ad un rinvio alla Corte di Giustizia dell'UE, i cui criteri e principi tuttavia 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 differenti.

Per concludere, non vi è dubbio che tutte queste valutazioni e problematiche relative alla conservazione e accesso ai dati si inseriscano in un contesto ancora più ampio, che ci impone di riflettere sul ruolo della Corte di Giustizia nella tutela dei diritti fondamentali alla riservatezza e alla protezione dei dati.

Non si può infatti non rilevare come l'approccio "dato-centrico" della CGUE abbia portato ad una forte espansione della tutela del diritto alla riservatezza nell'era digitale[49], come tutto il filone giurisprudenziale inaugurato dalla *Digital Rights Ireland* testimonia. Trasformando l'Europa in quella che è stata definita una "fortress of digital privacy"[50], con conseguenze che si riverberano anche nei rapporti tra UE e Stati terzi[51], i giudici di Lussemburgo sembrano volersi porre come

[47] Procedimento 2017/0003/COD, COM (2017) 10: Proposal for a Regulation of the European Parliament 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 (Regulation on Privacy and Electronic Communications).

[48] Per un maggiore approfondimento sul punto si rimanda a: 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.

[49] 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, 7.

[50] 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.

[51] Come ben rappresentato dai richiamati casi *Schrems* e *Opinion 1/15,* che hanno sostanzialmente ad oggetto bozze di accordi o decisioni di adeguatezza tra Unione Europea e Stati terzi (nei casi richiamati, USA e Canada) e nei quali la Corte riafferma con forza una visione "eurocentrica" dei diritti alla riservatezza e alla protezione dei dati. Per maggiori approfondimenti su questi aspetti "transfrontalieri" della tutela garantita a livello europeo agli artt. 7 e 8 della Carta di

"ultimate protector of constitutional rights in Europe"[52]. Così facendo, il rischio potrebbe essere quello di restringere e comprimere la possibilità di tutelare altri interessi, di estrema importanza, quali la sicurezza nazionale e dell'Europa intera e la prevenzione di grandi minacce quali il terrorismo internazionale[53]. Certamente, la tendenza ad una lettura espansiva delle tutele garantite dalla Carte di Nizza così come dalla normativa europea stessa in materia di protezione dei dati, dimostra come "I giudici comunitari hanno 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"[54]; ma d'altro lato tale tendenza si pone anche in rapporto problematico rispetto alla determinazione di un corretto confine delle competenze tra Stati Membri e Unione stessa, nonché del principio di attribuzione, che si dimostra essere estremamente delicato con riferimento al terreno complesso e scivoloso della tutela della sicurezza.

L'Avvocato generale Henrik Saugmandsgaard Øe, nelle sue Conclusioni per il caso *Ministerio Fiscal*, con grande realismo e concretezza afferma 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).

Viene però da chiedersi se ciò sia possibile concretamente alla luce della posizione della Corte di Giustizia nella sua lunga e costante giurisprudenza. Una lettura più "attenuata" dei criteri indicati dai giudici di Lussemburgo è forse possibile?[55] Gli interrogativi sul ruolo della CGUE, sul riparto

---

Nizza, si leggano tra gli altri: 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,* 14 (1), 2016, 220; M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, in *Rivista di Diritti Comparati*, 2/2017.

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

[53] "If balancing of competing fundamental rights leads to the result that data protection very often or even mostrly 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 ustoppable expansion of the EU fundamental right to data protection. Little shop of horrors?*, in *Maastricht Journal of European and Comparative Law,* n. 5/2016.

[54] M. CARTABIA, *L'ora dei diritti fondamentali nell'Unione Europea*, in M. CARTABIA (a cura di), *I diritti in azione*, Il Mulino, 2007, 13.

[55] Si veda sul punto una possibile diversa lettura, proposta da 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/. L'autrice infatti indica una possibile interpretazione della *Tele2 Sverige* letta alla luce della Opinion 1/15, che la porterebbe a ritenere i principi delineati nella pronuncia come un "reminder to the legislator to conduct impact assessments when introducing privacy-intrusive measures", proponendo dunque una visione meno rigida dei criteri

delle competenze, sui pericoli di una espansione incontrollata dei diritti alla riservatezza e alla protezione dei dati, restano certamente aperti e rappresentano forse una delle più grandi sfide dell'era digitale.

Come si è visto in questa analisi, con la pronuncia *Ministerio Fiscal* i giudici di Lussemburgo non hanno risolto gli interrogativi emersi nell'era post-*Tele2 Sverige* relativamente alla gravità del reato come requisito per l'accesso ai dati[56], pur chiarendo taluni aspetti di rilievo e slegando da tale criterio rafforzato alcune tipologie di indagini, limitatamente a taluni particolari dati.

I rinvii pregiudiziali al momento pendenti potrebbero essere una preziosa occasione per chiarire questi dilemmi e magari per fornire nuove indicazioni e principi nella difficile sfida rappresentata dall'esigenza di bilanciamento tra interessi securitari e tutela dei diritti fondamentali.

Individuare al momento l'aspetto finale di questa complessa opera incompiuta è operazione estremamente ardua.

delineati dalla Corte. Tale lettura permetterebbe di superare le critiche, rivolte ai giudici di Lussemburgo, di aver adottato una interpretazione del diritto alla riservatezza e del suo necessario bilanciamento con altri interessi, "of another age which was not adapted to our modern times".

[56] Un commento alle Conclusioni dell'Avvocato generale nel caso *Ministerio Fiscal* veniva emblematicamente e forse provocatoriamente titolato "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), facendo sorgere la domanda e l'auspicio che, con la successiva pronuncia, la Corte indicasse in maniera più concreta alle autorità nazionali un modo legittimo per accedere ai dati conservati dai fornitori di servizi di comunicazione: "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 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".