AIC
ASSOCIAZIONE ITALIANA
DEI COSTITUZIONALISTI

OSSERVATORIO COSTITUZIONALE
Codice ISSN: 2283-7515
Fasc. 1/2022
Data: 1° febbraio 2022

'The three Ghosts of data retention': passato, presente e futuro della disciplina italiana in materia di conservazione e acquisizione dei metadati per scopi investigativi. Commento a margine del d.l. 30 settembre 2021, n. 132 e relativa legge di conversione[*]

di **Giulia Formici** – *Assegnista di Ricerca in Diritto Pubblico Comparato nell'Università degli Studi di Parma*

ABSTRACT: The so-called *data retention saga* is still open at the European Union level, both before the Court of Justice of the EU and the EU Legislators – the proposal for a new e-Privacy Regulation, disciplining also the *data retention* regime, is now under discussion –. Together with these relevant and awaited evolutions, the principles and requirements already affirmed in the CJEU case-law have produced a serious debate also at the Member States level: national Legislators and Courts are asked to comply with the strict proportionality requirements indicated by the CJEU and to correctly balance the guarantee of fundamental rights on the one hand and national and public security needs on the other hand. In this complex and articulated context, the Italian Legislator has recently adopted a legislative reform, specifically modifying the access-to-metadata discipline. As Scrooge, in the famous novel *A Christmas Carol*, encounters the revelatory *three Ghosts*, this paper aims at providing an analysis of the past, present and future of *data retention* regime, discussing the necessary steps the Italian Legislator as well as national Courts are asked to take in order to

[*] Lavoro sottoposto a referaggio secondo le linee guida della Rivista.

promote a conscious and serious debate on the proportionality of such a delicate investigatory instrument.

SOMMARIO: 1. Alcune preliminari notazioni di contesto. – 2. *The Ghost of data retention Past*: la discussa disciplina italiana e la difficile convivenza con i principi stabiliti dalla giurisprudenza della Corte di giustizia dell'UE. – 3. *The Ghost of data retention Present*: le modifiche apportate dal recente d.l. 30 settembre 2021, n. 132 e dalla legge di conversione 23 novembre 2021, n. 178. – 4. *The Ghost of data retention Future*: l'importanza di una seria riflessione sui possibili sviluppi normativi e giurisprudenziali, nazionali e sovranazionali.

1. Alcune preliminari notazioni di contesto

La disciplina della conservazione – c.d. *data retention* – e accesso ai metadati derivanti da telecomunicazioni elettroniche[1] è ormai da alcuni decenni al centro di un vivace e complesso dibattito legislativo, giurisprudenziale nonché dottrinario. Questo strumento investigativo si sostanzia nella memorizzazione preventiva e spesso generalizzata di metadati a carico di soggetti privati – i fornitori di servizi, nello specifico – e nella successiva possibilità di accesso agli stessi da parte di autorità di *law enforcement* e di intelligence. Come emerso con chiarezza soprattutto a seguito dei drammatici attentati terroristici che hanno colpito gli USA prima e il continente europeo dopo, la disponibilità di una enorme mole di dati conservati consente alle autorità pubbliche di "andare indietro nel tempo"[2] e di reperire informazioni utili a scopi di prevenzione, indagine e repressione di minacce alla sicurezza pubblica e nazionale, riguardanti soggetti previamente

[1] I metadati, anche denominati "dati di traffico" o "dati esterni alle telecomunicazioni", rappresentano l'«involucro delle comunicazioni elettroniche» – come definiti da G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, 2, 2018, p. 65 –. Si fa riferimento cioè alle informazioni raccolte dai fornitori di servizi di telecomunicazione per finalità di erogazione, gestione e fatturazione dei servizi e che non attengono al contenuto della comunicazione bensì al luogo (cioè la cella di aggancio e la possibile – per quanto talvolta vaga e ampia – ubicazione del dispositivo telefonico –, ora, data, durata e destinatario di una comunicazione, unitamente all'identità dell'utilizzatore). L'art. 1 del d.lgs. 30 giugno 2003, n. 196, c.d. Cod. Privacy, definisce i "dati di traffico" come «qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione». Per tabulato telefonico si fa invece specifico riferimento ad un documento contenente i metadati di una telecomunicazione e che consente di ricostruire il flusso telefonico o telematico.

[2] Espressione impiegata da I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 54, 2017, p. 1428.

sconosciuti e non sospettati dalle forze dell'ordine e dunque non sottoposti a controlli mirati o intercettazioni dirette[3].

Nonostante tali rilevanti potenzialità, l'imposizione di un obbligo vasto e generalizzato di conservazione dei metadati in capo agli operatori delle telecomunicazioni ha ben presto evidenziato rischi e pericoli per il godimento dei diritti fondamentali: indipendentemente dall'eventuale successivo accesso ai dati da parte di soggetti terzi, una *bulk data retention* rappresenta una forte intrusione nella sfera privata, ingenerando negli utenti quella che è ormai stata ampiamente riconosciuta come una «sensazione di costante sorveglianza»[4]. Ciò incide indubbiamente e primariamente sui diritti alla riservatezza e alla protezione dei dati ma anche, indirettamente, sull'esercizio di quelle libertà, quali le libertà di opinione e di espressione, poste alla base di uno sviluppo incondizionato e pieno della personalità nonché, in ultima istanza, della realizzazione di una società realmente democratica, priva cioè di controlli ed interferenze pervasive, massive ed indiscriminate nella sfera più intima dei cittadini – dunque non giustificate da specifiche ragioni di indagine o dalla sussistenza di un nesso oggettivo con una minaccia alla sicurezza –[5]. Il rischio che, grazie anche alle più moderne e sofisticate tecnologie[6], possano essere massicciamente impiegati mezzi di sorveglianza in grado di determinare preferenze, abitudini, relazioni sociali e convincimenti personali di ciascun individuo diventa così uno dei più insidiosi e ormai nettamente

[3] In questo senso, «the aim of this bulk accumulation of data is to generate useful and reliable correlations and ultimately to generate suspects», M. ANDREJEVIC, *Surveillance in the big data era*, in *Law, Governance and Technology Series*, 11, 2014, p. 55. È bene sin da subito precisare come questo strumento si distingua fortemente dalle intercettazioni telefoniche che hanno ad oggetto la raccolta ed analisi dei dati relativi al contenuto delle telecomunicazioni e che sono quindi disciplinate da disposizioni differenti; si rimanda sul punto, per lo specifico contesto italiano, a S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, 2018 e ancora, S. MARCOLINI, *L'istituto della data retention dopo la sentenza della CGUE del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, 2019, p. 1580 ss.

[4] Come chiaramente affermato dalla Corte di giustizia dell'UE, 8 aprile 2014, cause riunite C-293/12, C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications e al.*, para. 37.

[5] È nota, infatti, l'importanza strumentale e finalistica dei diritti alla riservatezza e alla protezione dei dati, la cui portata e rilievo sono tali da «poter compromettere, in caso di [loro] violazione, tutta un'altra serie di principi, diritti e libertà (..). Non vi è dubbio che una compressione del diritto del singolo all'autodeterminazione informativa pone in discussione la salvaguardia della dignità stessa della persona, intesa quale valore costituzionale indisponibile», L. CALIFANO, *Principi e contenuti del Reg. UE 2016/679 in materia di protezione dei dati personali*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, 2018, p. 1. Sul punto anche, *ex multis*, S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, 2013; M.G. PORCEDDA, *The recrudescence of 'Security v. Privacy' after the 2015 terrorist attacks and the value of privacy rights in the European Union*, in E. ORRÙ, M.G. PORCEDDA, S. WEYDNER-VOLKMANN (a cura di), *Rethinking surveillance and control: beyond the 'security versus privacy' debate*, Nomos, 2017.

[6] Ad esempio mediante la c.d. lettura aggregata dei *Big Data*; per approfondimenti sulle potenzialità del mondo dei dati e della *Big Data analysis*, si legga V. MAYERSCHONBERGER, K. CUKIER, *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, 2013.

percepiti pericoli del nuovo Millennio[7], anche laddove una simile compressione dei diritti fondamentali risulti motivata dalla certamente importante finalità di garanzia della sicurezza.

La necessità di rileggere nel moderno contesto "digitalizzato" il problematico rapporto tra esigenze securitarie e diritti fondamentali[8] e di promuoverne un attento bilanciamento, rappresenta dunque una significativa sfida per le democrazie stabilizzate, capace di impegnare legislatori e Corti, nazionali e sovranazionali, nel continuo sforzo di regolare sistemi di lotta e prevenzione della criminalità efficaci e al contempo in grado di tutelare quei diritti e libertà riconosciuti quali basi fondative dello Stato di diritto.

È in questo contesto così articolato e delicato che si inseriscono, nello specifico ambito europeo, gli interventi della Corte di giustizia dell'UE (d'ora in avanti CGUE) in materia di *data retention*, seguiti – o talvolta preceduti – da numerose pronunce di giudici nazionali chiamati a valutare la legittimità delle normative in materia di conservazione e acquisizione di metadati per scopi securitari nonché la loro compatibilità con i diritti riconosciuti e protetti tanto dalle Carte costituzionali quanto dal diritto dell'UE e, in particolare, dalla Carta di Nizza[9]. Da questo intenso e a volte teso dialogo multilivello tra Corti ha avuto origine la c.d. *data retention saga*, nella quale i giudici di Lussemburgo si sono più volte pronunciati con sentenze dalla storica portata.

Sebbene alcuni rinvii pregiudiziali in materia siano ancora pendenti[10], a dimostrazione della complessità e della forte attenzione alla disciplina in discussione, la CGUE ha già avuto modo di

[7] Del resto, già nel 1984, Luis-Edmond Pettiti, all'epoca giudice della Corte europea dei diritti dell'uomo, affermava: «the danger threatening democratic societies (..) stems from the temptation facing public authorities to "see into" the life of citizens», sentenza 2 agosto 2984, *Malone v. UK*, ricorso n. 8691/79, Concurring Opinion del Giudice Pettiti, para. 5.

[8] Sullo storico rapporto sicurezza-diritti fondamentali, la dottrina si è già ampiamente interrogata. Tra i tanti, si rinvia a G. DE VERGOTTINI, *Guerra e Costituzione. Nuovi confini e sfide alla democrazia*, Il Mulino, 2004; AA.VV., *Convegno AIC, Libertà e sicurezza nelle democrazie contemporanee. Atti del Convegno annuale, Bari 17-18 ottobre 2003*, Cedam, 2008; C. BASSU, *Terrorismo e costituzionalismo. Percorsi comparati*, Giappichelli, 2010; T.E. FROSINI, *Il diritto costituzionale alla sicurezza*, in *Forum di Quaderni Costituzionali*, 2006, p. 1 ss.; G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore super primario*, in *Percorsi costituzionali*, 1, 2008, p. 31 ss.

[9] Per un'analisi delle pronunce di Corti nazionali che, già in un momento antecedente all'intervento della CGUE, erano intervenute in materia di *data retention* interrogandosi sulla legittimità costituzionale di un simile strumento investigativo, si rimanda a T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, in *European Current Law Issue*, 1, 2012, p. I ss.; E. KOSTA, *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, in *SCRIPTed*, 3, 2013, p. 339 ss.; L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, in *German Law Journal*, 6, 2015, p. 1727 ss.

[10] Si fa riferimento ai rinvii *SpaceNet AG c. Repubblica federale di Germania*, C-793/19 e *Repubblica Federale di Germania c. Telekom Deutschland GmbH*, C-794/19, entrambi promossi dal *Bundesverwaltungsgericht* tedesco il 29 ottobre 2019; nonché al rinvio *G.D. c. The Commissioner of the Garda Siochana e al.*, C-140/20, promosso invece dalla

delineare e fissare principi di grande rilievo quanto alla proporzionalità e necessità dello strumento della *data retention* e della acquisizione dei metadati da parte di autorità pubbliche, giungendo addirittura ad invalidare, con la nota decisione *Digital Rights Ireland*, la direttiva 2006/24/CE, c.d. *data retention directive*[11]. Questa normativa, pensata per armonizzare il confuso e disomogeneo panorama regolatorio venutosi a creare nei diversi Stati membri, introduceva per la prima volta a livello sovranazionale l'obbligo in capo ai legislatori nazionali di imporre ai *service providers* di servizi di telecomunicazione una conservazione generalizzata ed indiscriminata di metadati, lasciando poi alla discrezionalità dei singoli Stati la predisposizione di norme volte a regolare l'accesso a tali informazioni per scopi di repressione di reati "gravi", la cui definizione era però anch'essa rimessa alle scelte nazionali. Proprio questi profili della obbligatorietà di una *bulk data retention* e dell'assenza di regole chiare e precise quanto alla fase dell'acquisizione, erano stati però considerati dai giudici di Lussemburgo incompatibili con il diritto dell'UE e, in particolare, con i diritti di cui agli artt. 7, 8 e 52 della Carta di Nizza[12].

Nelle successive pronunce, dalla *Tele2*[13] sino alle più recenti *La Quadrature du Net*[14] e *H.K. c. Prokuratuur*[15], i giudici di Lussemburgo hanno ribadito e meglio specificato, nel dettaglio e

Supreme Court irlandese il 25 marzo 2020. Con riferimento al primo e all'ultimo rinvio qui richiamati, sono state depositate, il 18 novembre 2021, le Conclusioni dell'Avvocato generale. A questi si aggiunge anche il più recente rinvio promosso dalla *Spetsializiran nakazatelen sad* bulgara, il 4 giugno 2021, C-350/21.

[11] Direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione e che modifica la Direttiva 2002/58/CE, 15 marzo 2006.

[12] Tra i numerosi commenti, si rinvia a A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La 'data retention' al test di legittimità*, in *Diritto Pubblico Comparato ed Europeo*, 2014, p. 1224 ss; M. GRANGER, K. IRION, *The Court of Justice and the Data retention Directive in Digital Rights Ireland*, in *European Law Review*, 4, 2014, p. 835 ss; M. DICOSOLA, *La data retention directive e il dialogo tra Corti costituzionali e Corte di giustizia nel sistema multilivello europeo*, in *Diritti Comparati*, 20 febbraio 2014; S. CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista Italiana di Diritto Pubblico Comparato*, 3-4, 2015, p. 819 ss; F. FABBRINI, *Human rights in the digital age: the ECJ ruling in the data retention case and its lessons for privacy and surveillance in the US*, in *Harvard Human Rights Journal*, 28, 2015, p. 66 ss.

[13] CGUE, 21 dicembre 2016, cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB c. Post-och telestyrelsen* e *Secretary of State for the Home Department c. Tom Watson e al.* Altro rilevante caso è CGUE, 2 ottobre 2018, C-2017/16, *Ministerio Fiscal*. Per una analisi di quest'ultima sentenza, sia consentito il rinvio a G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, in questa rivista, 3, 2018,p. 453 ss.

[14] CGUE, 6 ottobre 2020, C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e al.*; CGUE, 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18 *La Quadrature du Net e a. c. Premier Ministre e a.* e *Ordre des barreaux francophones et germanophone e al. c. Conseil des Ministres*. Per una vasta disamina di queste ultime pronunce nonché della *data retention saga*, sia permesso di fare riferimento a G. FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Giappichelli, 2021, e alla bibliografia in esso riportata.

predisponendo una sorta di *vademecum* per il legislatore, i criteri e requisiti di legittimità della disciplina della conservazione e accesso; in questi casi, così come in quelli ancora pendenti, i rinvii da parte dei giudici nazionali derivavano dalla necessità di definire i limiti e confini di applicazione dell'art. 15 Direttiva *e-Privacy*[16]: questa è, ancora oggi, l'unica disposizione di livello sovranazionale che, a seguito dell'invalidazione della *data retention directive*, attribuisce agli Stati membri la *facoltà*[17] di derogare alla regola generale determinante la cancellazione dei metadati raccolti dai fornitori nello svolgimento dei propri servizi, così garantendo la possibilità di istituire discipline di conservazione dei metadati per vaghe e ampie finalità di sicurezza nazionale e repressione dei reati – senza alcuna specificazione quanto al loro carattere di gravità –. Fornendo quindi delucidazioni quanto all'interpretazione di tale incerta disposizione, la CGUE ha via via stabilito precisi paletti entro cui l'obbligo di conservazione dei metadati deve essere inserito, al fine di rendere tale disciplina proporzionata e di limitare a quanto strettamente necessario la compressione dei diritti fondamentali degli utenti dei servizi di telecomunicazione – cioè la quasi totalità della popolazione europea –.

Così, volendo fornire un'immagine estremamente riassuntiva e solo per quanto in questa sede utile e necessario, i giudici di Lussemburgo hanno stabilito, *in primis* con riferimento alla disciplina della *data retention*, che non è conforme al diritto dell'UE una forma di conservazione generalizzata ed indiscriminata quando essa sia finalizzata alla repressione della criminalità grave. A tale scopo, infatti, solo una conservazione targettizzata, cioè mirata sotto il profilo soggettivo, geografico o temporale[18], può essere ritenuta proporzionata e limitata a quanto strettamente necessario[19]. Qualora invece la conservazione sia volta a tutelare la sicurezza nazionale, la rilevanza

[15] CGUE, 2 marzo 2021, C-746/18, *H.K. c. Prokuratuur*. Questa pronuncia sarà più ampiamente richiamata nel successivo paragrafo, in considerazione del suo rilievo rispetto all'evoluzione normativa e giurisprudenziale italiana in materia.

[16] Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Direttiva relativa alla vita privata e alle comunicazioni elettroniche), 12 luglio 2002, nota anche come Direttiva *e-Privacy*.

[17] Diversamente dalla disciplina prevista nella *data retention directive*, che disponeva un obbligo in capo ai legislatori di porre in essere un regime di conservazione dei metadati, l'art. 15 della Direttiva in esame prevede invece una mera possibilità, rimessa alla discrezionale scelta dei legislatori dei singoli Stati membri.

[18] Sin dalla sentenza *Digital Rights Ireland* i giudici di Lussemburgo hanno chiarito come anche la durata della conservazione debba essere motivata dalla sussistenza di criteri obiettivi in grado di limitare l'arco temporale della *data retention* a quanto strettamente necessario, a seconda, ad esempio, della tipologia dei dati conservati e della loro eventuale utilità ai fini dello scopo perseguito o delle persone interessate.

[19] La *targeted data retention* si concretizza dunque in una forma di conservazione limitata ad uno specifico periodo di tempo e/o ad un'area geografica e/o una cerchia di soggetti che possono essere coinvolti in un reato grave o di

dell'obiettivo consente un'ingerenza maggiore dei diritti fondamentali, tale da giustificare una forma di *bulk data retention*. Pur riconoscendo dunque questa possibilità, peraltro fortemente auspicata dai Governi intervenuti dinnanzi alla CGUE, quest'ultima non ha mancato di sottolineare il carattere eccezione e residuale di tale regime, che deve pertanto anch'esso sottostare a precisi limiti e condizioni; in particolare debbono ricorrere circostanze sufficientemente concrete da consentire di ritenere sussistente una minaccia grave, reale, attuale o quantomeno prevedibile per la sicurezza nazionale; anche in tal caso, comunque, il regime generalizzato di conservazione deve essere temporalmente limitato allo stretto necessario, accompagnato da garanzie rigorose di protezione dei dati contro il rischio di abusi nonché sottoposto al controllo preventivo di un giudice o di un organo amministrativo indipendente[20]. Ne deriva, pertanto, come il ricorso a tale invasivo strumento non possa assumere carattere abituale o sistematico bensì debba sottostare a condizioni piuttosto dettagliate indicate dalla CGUE, per quanto certamente un margine di discrezionalità attuativa sia rimasta in capo ai legislatori nazionali, soprattutto con riferimento alle parti nelle quali i giudici di Lussemburgo hanno impiegato termini piuttosto ampi o vaghi e suscettibili di diverse interpretazioni.

Sul fronte dell'acquisizione dei metadati e quindi dell'accesso a questi ultimi da parte di autorità pubbliche per scopi securitari, viene stabilito innanzitutto un limite relativo allo scopo: l'acquisizione di metadati può avvenire solo per scopi di indagine e lotta a reati di carattere grave, per quanto i giudici di Lussemburgo non provvedano a fornirne una specifica definizione; devono essere inoltre stabilite regole chiare e precise relativamente alle condizioni per le quali i *service providers* sono tenuti a garantire ad autorità pubbliche l'accesso alle informazioni conservate; nello specifico, viene richiesta la sussistenza di requisiti sostanziali e processuali, stabiliti per legge, in

persone i cui metadati possono contribuire alla prevenzione o accertamento di reati gravi (para. 59, sentenza *Digital Rights Ireland*). La concreta realizzazione di una simile tipologia di *data retention* è stata ampiamente discussa e fortemente criticata da Governi nazionali, autorità di *law enforcement* e intelligence che hanno ravvisato nelle preventive restrizioni temporali, geografiche e soggettive un significativo limite all'efficacia della misura stessa, considerando la difficoltà di determinare in anticipo persone, aree o momenti all'interno dei quali la conservazione dei dati possa risultare utile per scopi investigativi.

[20] Per uno studio di tali pronunce si leggano J. SAJFERT, *Bulk data interception/retention judgements of the CJEU. A victory and a defeat for privacy*, in *European Law Blog*, 26 ottobre 2020; I. CAMERON, *EU law restraints on intelligence activities*, in *International Journal of Intelligence and Counter-Intelligence*, 3, 2020, p. 453 ss.; M. ZALNIERIUTE, *The future of data retention regimes and national security in the EU after the Quadrature du Net and Privacy Internazional judgements*, in *Insights*, 28, 2020, p. 1 ss.; sia consentito anche il rinvio a G. FORMICI, *La data retention saga al capolinea? Le ultime pronunce della CGUE in materia di conservazione dei metadati per scopi securitari, tra conferme e nuove aperture*, in *DPCE Online*, 1, 2021, p. 1361 ss.

grado di individuare una connessione, anche solo indiretta, tra accesso ai dati e finalità di lotta alla criminalità. Tali operazioni di acquisizione, infine, debbono essere sottoposte ad un controllo preventivo da parte di un giudice o di una entità amministrativa indipendente, subordinato ad una richiesta motivata delle parti interessate.

Come si vedrà anche nel caso italiano, le rigide condizioni sin qui brevemente delineate hanno sollevato profonde perplessità in capo a Governi, legislatori ma anche Corti degli Stati membri, spesso convinti che il rispetto puntuale della totalità di tali requisiti, pur fortemente tutelanti, finisca con l'inficiare la funzionalità e l'efficacia dello strumento della conservazione e accesso ai metadati e dunque l'utilità della disciplina stessa. Le reazioni e le interpretazioni nazionali della ricca giurisprudenza europea sono state dunque estremamente variegate e complesse, traducendosi in taluni casi in *defensive reactions*, quando non in una vera e propria resistenza a modificare le disposizioni interne alla luce dei principi sanciti a livello sovranazionale[21]. Una difficoltà di adeguamento, quella appena indicata, che permane tutt'ora e che emerge non solo nel difficile percorso di approvazione di una nuova normativa europea in materia di *data retention*[22] ma anche in un frammentario dibattito legislativo, giurisprudenziale e dottrinario venutosi a creare nelle diverse realtà statuali, favorendo così l'affermarsi di un panorama di soluzioni e approcci estremamente disomogeneo.

In Belgio, ad esempio, da decenni le decisioni della CGUE hanno prodotto immediati e dirompenti effetti, portando in diversi casi all'intervento della Corte costituzionale belga: quest'ultima, accogliendo i principi sanciti dai giudici di Lussemburgo, ha annullato per ben due volte la normativa nazionale in materia di conservazione e accesso ai metadati; il legislatore, grazie ad un'analisi approfondita ed estremamente attenta della giurisprudenza interna e sovranazionale,

[21] Si legga ad esempio sul punto il report elaborato da Eurojust, *Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15*, 10098/17, 2019, ma anche M. ZUBIK, J. PODKOWIK, R. RYBSKI (a cura di), *European Constitutional Courts towards data retention laws*, Springer, 2020.

[22] Nel documento *Conclusioni sulla conservazione dei dati per finalità di lotta contro la criminalità*, n. 9336/19 del 27 maggio 2019, il Consiglio dell'UE ha affidato alla Commissione il delicato compito di valutare l'opportunità e la realizzabilità di una specifica iniziativa legislativa *ad hoc* in materia di *data retention*, volta a superare la lacuna normativa lasciata a seguito dell'invalidazione della *data retention directive* e ad oggi solo parzialmente colmata dall'intervento della CGUE. Ad oggi però la possibilità di addivenire ad una nuova normativa sovranazionale pare obiettivo estremamente complesso da raggiungere. Anche nel contesto della Proposta di Regolamento relativo al rispetto della vita privata e della tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE, di cui si parlerà anche in seguito e rispetto alla quale sono state nel febbraio 2021 avviate le negoziazioni tra Parlamento europeo, Commissione e Consiglio dell'UE, la disciplina della *data retention* e dunque la riscrittura dell'art. 15 dell'attuale Direttiva *e-Privacy* rappresenta uno dei maggiori terreni di scontro.

sta ora discutendo la possibilità di attuare una *targeted data retention* e di rafforzare ed integrare le già esistenti salvaguardie e limiti all'acquisizione dei metadati conservati[23].

Mentre numerosi Stati, tra cui Francia e Regno Unito – prima della finalizzazione della procedura di Brexit –, hanno poi promosso rinvii pregiudiziali significativi nei confronti della CGUE, al fine di stimolare chiarimenti interpretativi e spronare ad una delimitazione precisa e specifica dei criteri definiti nella *data retention saga*[24], in Italia questo delicato e complesso tema non ha affatto trovato spazio dinnanzi al Parlamento, Governo e alle Corti. Al contrario, il panorama italiano è risultato caratterizzato da un lato da preoccupante immobilismo normativo, contraddistinto da interventi talora confusi e poco – o per nulla – attenti a quanto veniva invece affermato dalla CGUE o dalle scelte caratterizzanti altre realtà ordinamentali, e dall'altro lato da un approccio giurisprudenziale che ha optato per una lettura «restrittiva degli standard garantistici enunciati dalla CGUE», al fine di «salvare la disciplina interna (..) ed evitare ipotesi di inutilizzabilità probatoria»[25]. Solo in tempi recentissimi risulta possibile ravvisare un lento, parziale e timido cambiamento di rotta: accanto al primo rinvio pregiudiziale alla CGUE in materia di acquisizione dei metadati promosso dal Tribunale di Rieti, si inserisce un nuovo intervento del legislatore italiano mediante l'adozione del d.l. 30 settembre 2021, n. 132 e la successiva legge di conversione 23 novembre 2021, n. 178. Pur finalizzata a modificare la normativa previgente in senso maggiormente garantista e conforme ai principi sanciti dalla giurisprudenza europea, tale riforma, intervenendo solo in merito alla disciplina dell'accesso e lasciando intatto invece il regime di conservazione, resta ad oggi piuttosto discussa e oggetto di considerazioni critiche talvolta di segno discordante.

Questo elaborato si propone quindi di esaminare la portata delle recenti ed attese modifiche normative e di favorire una comprensione critica delle persistenti problematiche nonché dei punti di

[23] Sul punto si rimanda a C. FORGET, *L'obligation de conservation des 'métadonnes': la fin d'une longue saga juridique?*, in *Journal des Tribunaux*, 13, 2017, p. 233 ss.; F. COUDERT, F. VERBRUGGEN, *Conservation des donnees de communications electronique en Belgique: un juste equilibre?*, in V. FRASSEN, D. FLORE (a cura di), *Societe numerique et droit penal*, Bruylant, 2019, p. 248 ss.; sia consentito anche il rinvio a G. FORMICI, *La disciplina della data retention*, cit., nel capitolo specificamente dedicato allo studio della giurisprudenza e dell'evoluzione normativa in materia di *data retention* nell'ordinamento belga.

[24] Si fa riferimento ai rinvii nei casi *La Quadrature du Net* e *Privacy International*, sopra richiamati, nei quali i giudici nazionali hanno promosso un dialogo, talvolta anche dai toni aspri, con la CGUE, chiedendo in sostanza di rivedere i criteri restrittivi di proporzionalità e necessità previamente stabiliti nella giurisprudenza sovranazionale.

[25] L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019, p. 757.

forza; per fare ciò risulta tuttavia indispensabile svolgere una ricostruzione della disciplina previgente, di quella attualmente in essere nonché delle prospettive che permangono in attesa di definizione. Come il percorso di consapevolizzazione e redenzione di Ebenezer Scrooge ha avuto luogo solo grazie all'incontro con i tre Spiriti del Natale – *Ghost of Christmas Past, Present, Future* –, così questo lavoro intende proporre un fondamentale viaggio nel passato, nel presente e nel futuro della disciplina italiana della conservazione e acquisizione di metadati. Queste necessarie tappe risultano essenziali per poter proporre considerazioni critiche ed approfondite su ciò che ancora attende i legislatori e le Corti italiane: questi ultimi, similmente a quanto accaduto per il protagonista del romanzo di Dickens, abbisognano di "risvegliarsi" ed intraprendere con maggiore decisione un cammino di "ravvedimento". Un cammino, quest'ultimo, che non è affatto di poco conto: ad essere in gioco, in questo caso, è la delicata scelta, da parte delle autorità pubbliche, di rinunciare alla tentazione di una garanzia della sicurezza "a tutti i costi"[26], per inserire ed inglobare invece gli obiettivi securitari entro l'inviolabile contesto dello Stato di diritto e della tutela dei diritti fondamentali.

2. *The Ghost of data retention Past*: la discussa disciplina italiana e la difficile convivenza con i principi stabiliti dalla giurisprudenza della Corte di giustizia dell'UE

Primo rilevante momento del percorso che qui si vuole tracciare è da rinvenirsi nell'analisi della evoluzione normativa e giurisprudenziale che ha caratterizzato la disciplina italiana della conservazione e accesso ai metadati negli ultimi decenni; questo iniziale passaggio risulta propedeutico alla comprensione piena non solo delle ragioni che hanno spinto al più recente intervento legislativo, oggetto di approfondimento nella successiva tappa che qui si vuole proporre, ma anche dei limiti e delle carenze che in esso possono essere rinvenuti e che potranno quindi utilmente orientare le scelte e i passi futuri.

[26] Il rischio, da molti studiosi evidenziato, è che l'impiego di mezzi di sorveglianza potenti ed invasivi, pur per scopi securitari, finisca col favorire l'affermarsi di scenari tutt'altro che fantascientifici di un *Big Brother* orwelliano, facilitando peraltro la trasformazione verso una società *trasparente*, secondo l'interessante lettura fornita da D. Brin, nel suo celebre libro significativamente titolato *The transparent society. Will technology force us to choose between privacy and freedom?*, Perseus Books, 1998.

L'articolo di riferimento per esaminare, seppur riassuntivamente, la richiamata materia deve essere identificato nell'art. 132 del d.lgs. 30 giugno 2003, n. 196[27] che ha introdotto in capo ai fornitori di servizi di telecomunicazioni un generale obbligo di conservazione dei c.d. "dati esterni delle comunicazioni" (i c.d. metadati) per finalità di accertamento e repressione dei reati. Tale disposizione ha subìto, nel corso del tempo, diverse modifiche, intervenute a riformare le categorie di metadati da conservare – prima i soli dati derivanti da servizi telefonici, poi anche quelli derivanti dai sempre più rilevanti e diffusi servizi telematici – nonché il numero di mesi di conservazione richiesti – dai trenta iniziali agli attuali ventiquattro mesi per i metadati telefonici, dodici mesi per il traffico telematico e trenta giorni per le chiamate senza risposta –. Uno dei primi interventi riformatori dell'art. 132 è da rinvenirsi nel d.l. 24 dicembre 2003, n. 354 che, in deroga a quanto disposto dal da poco vigente Cod. Privacy, definiva un c.d. "doppio binario" di conservazione: per i soli reati previsti dall'art. 407, co. 2, lett. a) c.p.p. e per i delitti a danni di sistemi informatici e telematici il periodo di conservazione diveniva più ampio, dilatato di ulteriori ventiquattro mesi per i dati telefonici e di sei mesi per quelli di traffico telematico. Tale differenziazione tra reati "in generale" e reati di terrorismo o altri fattispecie criminose comunque considerate particolarmente serie non deve però indurre a pensare che il legislatore italiano avesse previsto una soglia di gravità, sulla scia di quanto richiesto dalla *data retention directive* e di quanto poi la CGUE avrebbe affermato; al contrario, i fornitori di servizi di telecomunicazione non potevano certo sapere anticipatamente se i metadati sarebbero stati impiegati nell'ambito di indagini riguardanti un qualsiasi reato o quelli più gravi espressamente indicati dalla normativa analizzata, così che *de facto* tali operatori si trovavano costretti a conservare tutte le informazioni per il termine massimo previsto di quattro anni; quella che veniva stabilita, in sostanza, era solo una limitazione attinente alla fase di acquisizione: ciò che cambiava a seconda della categoria di crimini interessati era semplicemente la possibilità delle autorità di *law enforcement* di "andare indietro nel tempo" e dunque di acquisire i metadati, possibilità che risultava ristretta a ventiquattro mesi per tutti i reati, mentre subiva un ampliamento con riferimento a tutti quelli identificati dal legislatore come maggiormente seri[28]. Quanto sin da qui emerge, pertanto, è come nella disciplina italiana non

[27] D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, più semplicemente Codice Privacy.

[28] Per approfondimenti, C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, 2008, p. 399 ss.; ma anche M. RICCARDI, *Data esteriori*

fossero previste, né originariamente né nelle prime modifiche, limitazioni quanto alla conservazione e alla possibilità di accesso ai metadati raccolti: pur risultando soggetta a diverse tempistiche, tali operazioni non erano mai, in alcun caso, precluse.

Similmente alla disciplina della conservazione, anche con riferimento alla procedura di acquisizione delle informazioni conservate si sono registrate diverse e profonde riforme già a poco tempo di distanza dall'entrata in vigore del Cod. Privacy: mentre la versione originaria dell'art. 132, come modificata dal d.l. 24 dicembre 2003, n. 354, di cui sopra, prevedeva che la richiesta di accesso venisse approvata con decreto motivato del giudice, ottenibile su istanza del pubblico ministero, del difensore dell'imputato, di persona sottoposta ad indagini o della persona offesa o altre parti private, con il c.d. Decreto o Pacchetto Pisanu[29] veniva stabilito come solo con riferimento ai reati considerati più gravi – quelli di cui all'art. 407, co. 1, lett. a) c.p.p., delitti a danno di sistemi informatici e telematici – l'acquisizione dovesse essere autorizzata con decreto di un giudice, mentre per tutti gli altri reati diveniva sufficiente il mero decreto motivato del pubblico ministero. Questa significativa riforma della disciplina attinente all'accesso, motivata da esigenze di «snellimento della procedura»[30], era accompagnata anche da una novità sul piano della conservazione, adottata sulla spinta di quella deriva pro-securitaria che aveva caratterizzato gli anni successivi agli attentati terroristici di Madrid e Londra: per il solo fine di repressione dei reati di terrorismo, infatti, tutti i metadati dovevano essere trattenuti dagli operatori sino al 31 dicembre 2007, estendendo dunque la *data retention* anche oltre i termini stabiliti dall'art. 132 Cod. Privacy.

Il d.lgs. 30 maggio 2008, n. 109[31], con cui si dava attuazione alla Direttiva 2006/24/CE, stabiliva nuovamente innovazioni alla disciplina descritta: innanzitutto il sistema a "doppio binario", sopra richiamato, veniva eliminato, così che la *data retention* tornava unicamente ad essere quella disposta dall'art. 132 Cod. Privacy, senza distinzioni sulla base della tipologia di reato

delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore, in *Diritto Penale Contemporaneo*, 3, 2016, p. 170 ss.

[29] D.l. 27 luglio 2005, n. 144, convertito con l. 31 luglio 2005, n. 155.

[30] Così scrive M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, cit., p. 176.

[31] Pare necessario precisare che in questa sede e ai fini della presente trattazione non verranno esaminati tutti gli interventi normativi di modifica della disciplina citata, bensì saranno richiamate solo le riforme maggiormente significative. Per una analisi più dettagliata e completa sotto questo profilo, si rinvia a C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention*, cit.; P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1, 2016; G.M. BECCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. CADOPPI, S. CANESTRATI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, cit., p. 1599 ss.

eventualmente perseguita dalle autorità pubbliche e per la quale i dati venivano richiesti. Quanto alla disciplina dell'accesso veniva poi affermato il ruolo unico ed esclusivo del p.m., quale soggetto incaricato di autorizzare le richieste di acquisizione dei metadati. Come si comprende, la minaccia terroristica, che in quegli anni si faceva concreta anche nel vecchio continente, aveva via via finito con l'assottigliare le tutele e le limitazioni inizialmente previste dal legislatore nostrano, prevendendo una conservazione generalizzata ed un accesso garantiti per la repressione di qualunque tipologia di reato e non solo per quelli "gravi", come invece richiesto, a quel tempo, dalla Direttiva 2006/24/CE.

Tale approccio non è mutato neppure dinnanzi ai chiari principi delineati nel 2014 dal primo intervento della CGUE in materia di *data retention* e alle conseguenti perplessità e preoccupazioni espresse anche dalla dottrina[32]: in Italia, infatti, non si è assistito – come invece accaduto in altri Stati membri[33] – ad un dibattito normativo o giurisprudenziale volto a verificare la conformità della disciplina nazionale ai criteri fissati dalla giurisprudenza dei giudici di Lussemburgo. A seguito della sentenza *Digital Rights Ireland* molti Parlamenti nazionali avevano adottato riforme significative delle disposizioni interne in materia di conservazione e accesso ai metadati, spesso coadiuvati e spinti dall'intervento delle Corti nazionali che iniziavano, al contempo, a promuovere numerosi rinvii pregiudiziali avverso la CGUE al fine di ottenere chiarimenti quanto all'interpretazione del *redivivo* art. 15 Direttiva *e-Privacy*. Nel nostro Paese, invece, si è proceduto lungo un percorso per certi versi molto distante da quello intrapreso da altri Stati membri: prima col c.d. decreto legge antiterrorismo[34], poi con il Decreto milleproroghe del 30 dicembre 2015[35] ed infine con la Legge Europea 2017[36], l'art. 132 Cod. Privacy, direttamente o indirettamente, è stato oggetto di numerosi interventi, spesso confusi e disordinati, tutti motivati da esigenze emergenziali e dunque privi di organicità. A seguito degli attentati di Parigi veniva infatti esteso l'obbligo

[32] Ci si riferisce alle perplessità e ai dubbi quanto alla legittimità e proporzionalità della disciplina italiana mossi, sin dalle più risalenti formulazioni dell'art. 132 Cod. Privacy, da diversi autori, tra i quali, G.E. VIGEVANI, *Articolo 132*, in AA.VV., *Codice della privacy. Commento al D.Lgs. 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Giuffré, 2004, p. 1668; A. ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014; F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, in *Cassazione Penale*, 12, 2014, p. 808 ss.; R. FLOR, *Data retention ed art. 132 Cod. Privacy: vexata quaestio(?)*, in *Diritto Penale Contemporaneo*, 3, 2017.

[33] Si pensi al già richiamato Belgio, ma anche al Regno Unito, alla Francia e alla Germania.

[34] D. l. 18 febbraio 2015, n. 7, convertito dalla l. 17 aprile 2015, n. 43.

[35] D.l. 30 dicembre 2015, n. 219, convertito con l. 25 febbraio 2016, n. 21.

[36] Legge 20 novembre 2017, n. 167, ovvero la Legge che reca le disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea.

generalizzato di conservazione sino al 31 dicembre 2016 per tutte le categorie di metadati, successivamente prorogato al 30 giugno 2017; con la Legge Europea poi è stato stabilito che, anche in considerazione di esigenze di contrasto al terrorismo, i *service provides* sono tenuti alla conservazione dei metadati per un termine di settantadue mesi, in deroga a quanto previsto dal Cod. Privacy, sebbene solo per scopi di repressione e accertamento di reati di terrorismo, saccheggio, associazione di tipo mafioso etc.[37] Certo questa dilatazione dei tempi di conservazione potrebbe apparire, ad un primo sguardo, complessivamente limitata alle specifiche finalità indicate; in realtà, ad un occhio attento, può comprendersi la vera e ampia portata di queste continue riforme: come già osservato con riferimento al "doppio binario", il fornitore non può conoscere in anticipo per quali obiettivi i metadati verranno eventualmente acquisiti, così che egli è tenuto a conservare tutti i metadati per il termine massimo di settantadue mesi, in modo da poter assicurare alle autorità pubbliche l'accesso a dati risalenti anche a sei anni prima, laddove necessari per la lotta a reati di terrorismo e gli altri indicati dalla normativa. Ancora una volta, dunque, l'effetto sostanziale delle disposizioni eccezionali introdotte è diventato quello di invertire il rapporto tra disciplina ordinaria e straordinaria, così che quest'ultima ha sostanzialmente e nella sua effettiva attuazione finito col soppiantare l'applicabilità della più contenuta durata prevista dal Cod. Privacy: l'art. 132 diviene rilevante solo per disciplinare la fase di acquisizione dei metadati, peraltro rimasta possibile per qualsiasi tipologia di reato, anche in questo caso senza alcun limite di gravità[38].

Numerose sono state le critiche mosse a seguito della Legge europea 2017, tanto sotto il profilo della tipologia di intervento scelta[39], quanto sotto quello della sostanza dello stesso, che ha portato

[37] Artt. 51, co. 3-*quater* e 407, co. 2, lett. a) c.p.p.

[38] In altre parole, «nel momento della trasmissione dei dati all'autorità giudiziaria il fornitore è obbligato a verificare che gli stessi siano riconducibili al periodo di conservazione che, a seconda del tipo di reato perseguito, risulta fissato dall'art. 132 Codice Privacy o dalla legge europea 2017. Se, ad esempio, un dato da conservarsi per 24 mesi – ma di fatto conservato per 72 mesi per la ricordata ragione che è impossibile conoscere a priori per quale tipo di reato verrà domandato l'accesso –, fosse richiesto dopo 24 mesi ed un giorno, sarebbero illegittime tanto la sua trasmissione quanto la sua acquisizione da parte dell'autorità giudiziaria», S. SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 132 Codice Privacy da parte del D.Lgs. 10 agosto 2018*, in *Diritto penale contemporaneo*, 11, 2018, p. 157. Anche il Garante per la Protezione dei Dati Personali, nella *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*, del 2 agosto 2021 – di cui si parlerà in seguito più ampiamente – ha sottolineato come, a seguito della Legge Europea 2017 e «benché l'acquisibilità dei dati raccolti oltre il termine ordinario sia limitata a reati particolarmente gravi, proprio la natura retrospettiva di questo strumento investigativo implica la conservazione generalizzata dei dati di traffico per sei anni, salvo poi limitarne l'utilizzabilità processuale ai soli casi normativamente considerati».

[39] Come evidenziato da Scaffardi, un inasprimento della disciplina della conservazione così rilevante quale quello introdotto dalla Legge Europea è stato attuato con una modalità quanto meno "furtiva" e singolare: la disposizione in esame è inserita infatti in una legge sugli adempimenti comunitari, preceduta da una disposizione in materia di

l'Italia ad imporre un periodo di conservazione dei metadati tra i più lunghi di tutta l'UE[40]; eppure nessuna modifica di rilievo è stata apportata negli anni successivi su questo profilo: volendo anticipare quanto è recentemente avvenuto, infatti, le novità introdotte dal d.l. 30 settembre 2021, n. 132 e relativa legge di conversione non hanno riguardato la disciplina della conservazione bensì unicamente quella dell'accesso.

Il percorso sin qui delineato volto a ripercorrere le scelte normative che sino ai tempi più recenti hanno caratterizzato il panorama nostrano – e che in parte ancora lo caratterizzano – permette sin da subito di porre in evidenza diverse criticità e limiti della disciplina nazionale. Nonostante i molteplici interventi giurisprudenziali della CGUE e i chiari e rigorosi principi e tutele riassunte nel primo paragrafo di questo contributo, nel nostro Paese nessun tentativo è stato promosso nella direzione di restringere la *data retention* non solo nella sua durata ma anche nella portata, essendo del tutto assenti forme di targettizzazione, soggettiva o geografica, in grado di stabilire un nesso tra l'ingerenza nella sfera privata perpetrata dalla conservazione e le finalità perseguite. Nessun ripensamento è stato mostrato, sino alla riforma del 2021, neppure rispetto alla disciplina dell'accesso: le diverse modifiche che si sono susseguite nel tempo non hanno mai né ristretto lo strumento dell'acquisizione alla sola finalità di repressione di reati *gravi*, rendendola invece possibile per qualsiasi crimine, né messo in dubbio la legittimità del controllo preventivo della richiesta di acquisizione, attribuito, come si è visto, al pubblico ministero; questo nonostante la CGUE, nella sua costante giurisprudenza, a partire dalla *Digital Rights Ireland*, abbia sempre fatto riferimento all'intervento di un "giudice" o di una "autorità amministrativa indipendente".

Insomma, mentre l'evolversi della disciplina della conservazione e accesso ai metadati, attuata sulla base prima della *data retention directive* e successivamente dell'art. 15 Direttiva *e-Privacy*, è stato spesso caratterizzato, in numerosi Stati membri, da un'attenta considerazione dell'avvicendarsi della *data retention saga* e del portato dei requisiti e dei principi di proporzionalità e stretta necessità forniti dalla CGUE, in Italia la parabola normativa registratasi

ascensori (L. SCAFFARDI, *La data retention va in ascensore*, in *Forum di Quaderni Costituzionali*, 28 luglio 2017). Scudiero non ha mancato di evidenziare come il metodo scelto per introdurre la novella indicata suggerisca che il legislatore italiano abbia voluto intenzionalmente introdurre nell'ordinamen-to, "di soppiatto" e senza attirare troppo l'attenzione, una modifica che avrebbe meritato invece un ampio dibattito parlamentare (L. SCUDIERO, *Data retention a sei anni. La Corte di Giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa-Canada sui Pnr*, in *MediaLaws*, 1, 2017.

[40] Estremamente critici Scudiero e Scaffardi (*supra*) ma anche R. BARBERIO, *Parliamo di Russia ma la vera anomalia sul data retention è l'Italia*, in *Huffington Post*, 5 luglio 2018; S. SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 132 Codice Privacy da parte del D.Lgs. 10 agosto 2018*, cit.

sino al 2021 appare disordinata, non organica, caratterizzata dal susseguirsi di continui regimi eccezionali, mossi da necessità emergenziali in risposta ad accresciute minacce alla sicurezza pubblica e nazionale[41]. In altre parole, ciò che è venuto a mancare in tali scelte legislative è una riflessione approfondita e sistematica tanto sul corretto bilanciamento tra misure pro-securitarie e adeguate garanzie dei diritti fondamentali quanto sui limiti entro cui una compressione degli stessi avrebbe potuto essere considerata proporzionata, necessaria e costituzionalmente legittima. Una carenza, questa, che ha peraltro contraddistinto non solo le scelte del legislatore nazionale bensì anche gli interventi – invero neppure numerosi – delle Corti italiane in materia.

Pur non potendo in questa sede approfondire nel dettaglio l'interessante evoluzione giurisprudenziale verificatasi nel nostro Paese[42], ciò che deve utilmente essere chiarito è come, in particolare a partire da una nota e discussa ordinanza del Tribunale di Padova del 2017[43] nonché in svariate pronunce della Corte di Cassazione[44], i giudici italiani chiamati a valutare la legittimità delle acquisizioni di tabulati telefonici in procedimenti penali abbiano adottato un approccio sbrigativo, a tratti superficiale e nel complesso certamente poco attento alle complessità e alla profondità della materia trattata. Come la dottrina non ha mancato di rimarcare, alcune affermazioni e considerazioni svolte con riferimento al portato della giurisprudenza della CGUE sono risultate erronee, a causa forse di una poco accurata analisi di tali pronunce o forse di un approccio "difensivo" delle Corti italiane, che hanno preferito promuovere un'interpretazione più ampia e meno stringente dei principi promossi dai giudici di Lussemburgo, così però allontanandosene in

[41] Andolina parla di «tormentata stratificazione della normativa» (E. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Cedam, 2018); Caputo invece ravvede anche nella vicenda dell'art. 24 della Legge Europea un intervento "tampone" ed eccezionale che non fa che complicare il quadro della disciplina, dinnanzi ad un legislatore nazionale che si sottrae alla responsabilità di dettare disposizioni organiche e chiare in materia (P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, cit., p. 36 in particolare).

[42] Si richiama *ex multis* un recente contributo di G. LEO, *Le indagini sulle comunicazioni e sugli spostamenti delle persone: prime riflessioni riguardo alla recente giurisprudenza europea su geolocalizzazione e tabulati telefonici*, in *Sistema Penale*, 2021, p. 1 ss., che propone un utile sunto della più rilevante giurisprudenza italiana in materia.

[43] Ord. 15 marzo 2017, Pres. Marassi. Si rimanda sul punto a F. RUGGERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cassazione Penale*, 6, 2017, p. 2486 ss.

[44] Ci si riferisce, ad esempio, alle sentenze Sez. V, 24 aprile 2018, n. 33851, Sez. III Pen, 23 agosto 2019, n. 36380 e ancora, Sez. III 25 settembre 2019, n. 48737, Sez. II 10 dicembre 2019, n. 5741. Per una analisi di tali sentenze, si leggano L. LUPARIA, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, cit.; I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention*, in *Sistema penale*, 5, 2020, p. 183 ss.

maniera talvolta netta e contrastante[45]. Neppure la Suprema Corte, dunque, ha mai messo in dubbio e tanto meno rilevato criticità o incompatibilità della disciplina interna rispetto a quanto definito a livello sovranazionale. In un momento in cui le Corti di numerosi Stati membri proponevano rinvii pregiudiziali circa l'interpretazione dell'art. 15 Direttiva *e-Privacy* nonché quanto all'ambito di applicazione del diritto dell'UE in materie complesse e articolate quali quelle della difesa della sicurezza nazionale – si pensi ai rinvii, già richiamati, promossi dalle Corti di Belgio, Regno Unito, Francia, Estonia, Irlanda, Germania e Bulgaria –, i giudici nostrani risolvevano in maniera rapida ed agile gran parte di tali quesiti, senza mai porre in discussione la costituzionalità o la conformità al diritto dell'UE del regime di *bulk data retention* e della vastissima durata dell'obbligo di conservazione dei metadati. Persino a seguito delle sentenze *Privacy International* e *La Quadrature du Net* dell'ottobre 2020, che hanno chiaramente ribadito l'incompatibilità di una forma di conservazione generalizzata ed indiscriminata per scopi di sicurezza pubblica, la Corte di Cassazione ha ribadito la propria già consolidata giurisprudenza "rassicurante", «espressione di un approccio semplicistico ad un tema (..) colmo di nodi irrisolti»[46]; diversamente da quanto accaduto in altri Stati membri, nei quali si sono registrate interessanti e significative reazioni[47], già nella sentenza n. 10022 del 10 novembre 2020 i giudici della Suprema Corte italiana affermavano nuovamente la legittimità della disciplina italiana e la sua compatibilità rispetto al diritto sovranazionale, così rifiutando un altamente atteso ed invocato mutamento di indirizzo[48].

[45] Nella citata Ordinanza del Tribunale di Padova, ad esempio, veniva stabilito come l'art. 132 Cod. Privacy non fosse norma attuativa della *data retention directive* in quanto entrato in vigore prima del 2003, ovvero ben prima della direttiva europea, così che la sentenza *Digital Rights Ireland* ad essa riferita non poteva comportare alcun effetto, neppure indiretto, sulla disciplina italiana. Questa considerazione non può in alcun modo essere condivisa ed è stata invero criticata quale esempio di una superficiale conoscenza da parte di taluni giudici del portato e del significato stesso della giurisprudenza europea ma anche della normativa nazionale: se è vero infatti che l'art. 132 nella sua versione originale non costituiva attuazione della Direttiva 2006/24/CE, esso lo è nondimeno divenuto quando il legislatore è intervenuto su di esso mediante il d.lgs, n. 109/2008, volto proprio a dare attuazione alla normativa europea. E ancora, la Corte di Cassazione, nella pronuncia 23 agosto 2019, n. 36380, affermava che la giurisprudenza della CGUE e i relativi requisiti erano da riferirsi unicamente agli «Stati privi di una regolamentazione dell'accesso e della conservazione dei dati», così che l'Italia, essendo dotata di una specifica disciplina in materia, non veniva considerata in alcun modo toccata da tali sentenze. Anche queste statuizioni paiono del tutto erronee: basti pensare che in pronunce quali *Tele2* o *Ministerio Fiscal* i giudici del rinvio fondavano le loro questioni pregiudiziali proprio sulla difficoltà interpretativa relativa a normative in materia di *data retention* e acquisizione dei metadati, presenti tanto nel Regno Unito e in Svezia quanto in Spagna.

[46] L. LUPARIA, *Data retention e processo penale*, cit., p. 761.

[47] Per una ricostruzione delle più significative reazioni della giurisprudenza di altri ordinamenti europei, sia consentito rinviare a G. FORMICI, *La disiplina della data retention*, cit.

[48] Sul punto L. LUPARIA, *Data retention e processo penale*, cit., p. 764; E.N. LA ROCCA, *A margine della sentenza della CGUE (C-748/18): riflessi sinistri sulla disciplina delle intercettazioni in Italia*, in *Diritti Comparati*, 8 aprile 2021.

Se fino alla metà del 2021, insomma, la disciplina della *data retention* e dell'accesso ai metadati non ha suscitato «l'interesse che meritava, né in dottrina né in giurisprudenza e soprattutto non ha turbato il sonno del legislatore nazionale»[49], solo a seguito della più recente sentenza della CGUE in materia, la *H.K. c. Prokuratuur* del 2 marzo 2021, si è registrata una prima inversione di tendenza. Questa pronuncia, che non è passata inosservata dai giudici italiani forse a causa del richiamo all'ordinamento nostrano svolto dall'Avvocato generale Pitruzzella nelle sue Conclusioni del 21 gennaio 2020, aveva ad oggetto un rinvio promosso dalla Suprema Corte estone che, per quanto qui interessa, riguardava la disciplina dell'accesso e, nello specifico, l'indipendenza delle autorità preposte al controllo preventivo all'acquisizione dei metadati; il giudice estone, infatti, chiedeva se tale requisito fosse da considerarsi assolto nel caso in cui tale funzione fosse attribuita ad un pubblico ministero che dirige la fase istruttoria ma che rappresenta anche la pubblica accusa nel corso del procedimento giudiziario eventualmente avviato. Ebbene su tale delicato punto la CGUE affermava che al fine di essere "indipendente" l'autorità incaricata di controllo preventivo deve essere in grado di «garantire un giusto equilibrio tra gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e i diritti fondamentali al rispetto delle vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso»[50]. Conseguentemente, l'autorità preposta al controllo deve necessariamente risultare *terza* rispetto a quella incaricata di formulare la richiesta di accesso ai metadati, così da garantire un vaglio preventivo realmente imparziale ed oggettivo. Pertanto è richiesto che il controllore non sia coinvolto nella conduzione dell'indagine penale e che sia in posizione di neutralità rispetto a tutte le parti del procedimento. Sulla base di tali considerazioni, la CGUE rilevava alcune criticità nella disciplina estone: i principi di terzietà ed indipendenza, così definiti, non potevano sussistere in capo al pubblico ministero estone a causa sia della natura dell'incarico assegnatogli – valutare l'opportunità e necessità di sottoporre al giudice una controversia o di archiviare il caso –, sia del cumulo di posizioni ricoperte – anche quella di parte attiva dell'eventuale processo –[51].

[49] S. MARCOLINI, *L'istituto della data retention dopo la sentenza della CGUE del 2014*, cit., p. 1591.

[50] Para. 52, *H.K. c. Prokuratuur*.

[51] Per un'analisi dettagliata di tale pronuncia, si rimanda, *ex multis*, a E. CELESTE, *Commission v. Spain and H.K. v. Prokuratuur: taking the plank out of EU's own eye*, in *Bridge Blog*, 15 marzo 2021; S. ROYER, S. CARREL, *Access denied. The CJEU raffirms la Quadrature du Net and clarifies requirements for access to retained data*, in *CiTiP Law Blog*, 23 marzo 2021; S. ROVELLI, *Case Prokuratuur: proportionality and the independence of authorities in data retention*, in *European Papers*, 6, 2021, p. 199 ss. Sia concesso anche il rimando a G. FORMICI, *L'incerto futuro della*

Le similitudini tra la figura del pubblico ministero estone e quello italiano, parimenti titolare della pubblica accusa nel procedimento eventualmente instaurato e incaricato, a seguito di indagini preliminari, di richiedere al G.i.p. tanto l'archiviazione quanto il rinvio a giudizio, hanno aperto un vivace dibattito giurisprudenziale sulla disciplina interna in materia di acquisizione dei metadati, giungendo anche a soluzioni estremamente disomogenee. A pochi giorni di distanza, il Tribunale di Milano, VII Sez. Penale[52] e il Tribunale di Roma, Sez. G.i.p.-G.u.p.[53] sono infatti addivenuti a due opposte conclusioni in merito alla medesima questione: il giudice milanese ha rigettato l'eccezione di inutilizzabilità delle acquisizioni di tabulati a carico dell'imputato, ritenendo conforme al diritto dell'UE la normativa nazionale nonché rilevando una netta distinzione tra il pubblico ministero estone e quello italiano[54]. Mentre secondo il giudice meneghino l'orientamento della giurisprudenza nostrana – e la normativa stessa – non era da ritenersi sotto nessun profilo superato dalla pronuncia della CGUE, i colleghi romani hanno invece dichiarato l'incompatibilità dell'art. 132 Cod. Privacy rispetto al diritto eurounitario nella parte in cui il controllo sull'accesso viene affidato al pubblico ministero[55]. In tale contesto così frammentario e confuso, nel quale anche la dottrina ha auspicato

data retention saga nell'Unione europea: osservazioni a partire dalla sentenza H.K. v. Prokuratuur, in *SIDI Blog*, 27 aprile 2021.

[52] Ordinanza n. 585/2021 del 22 aprile 2021; per approfondimenti, si veda: V. TORDI, *La disciplina italiana in materia di data retention a seguito della sentenza della CGUE: il Tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sistema Penale*, 7 maggio 2021; F. TORRE, *Data retention. Una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della CGUE 2 marzo 2021, C-746/18)*, in *Consulta Online*, II, 2021, p. 540 ss.

[53] Decreto del 25 aprile 2021. Si rimanda sul punto anche a J. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della CGUE: la svolta garantista in un primo provvedimento del G.i.p. di Roma*, in *Sistema Penale*, 29 aprile 2021; C. PARODI, *Tabulati telefonici e contrasti interpretativi: come sopravvivere in attesa di una nuova legge*, in *ilPenalista*, 3 maggio 2021. Con riferimento invece ad un approccio di segno opposto manifestato all'interno del medesimo Tribunale di Roma, si legga la decisione del 28 aprile 2021 del G.i.p. Dott. Fanelli, Sez. G.i.p.-G.u.p. e sul punto A. MALACARNE, *Ancora sulle ricadute interne della sentenza della CGUE in materia di acquisizione di tabulati telefonici: il Gip di Roma dichiara il 'non luogo a procedere' sulla richiesta del p.m.*, in *Sistema Penale*, 5 maggio 2021.

[54] Mentre il pubblico ministero estone è autorità «soggetta alla sfera di competenza del Ministero della Giustizia che partecipa alla pianificazione delle misure necessarie per la lotta all'accertamento dei reati», quello italiano è invece «chiamato ad esercitare sotto la vigilanza del Ministero di Grazia e Giustizia le funzioni che la legge gli attribuisce, con garanzia dell'impersonalità del suo ufficio e con la caratteristica ulteriore che esso riveste nel processo penale il ruolo di parte pubblica e non privata», Ord. N. 585/2021 del Tribunale di Milano, p. 4.

[55] Il giudice romano però, con una interpretazione discutibile e discussa, ha ritenuto di non dover disapplicare la normativa interna bensì di poter direttamente applicare il diritto dell'UE come interpretato dalla CGUE; a ciò non osta la mancata previsione normativa della categoria dei reati gravi: la determinazione della stessa, infatti, sarebbe facilmente individuabile, a parere del giudice romano, mediante il rinvio integrale ai reati previsti nel catalogo dettato dagli artt. 266 c.p.p. e 266-*bis* c.p.p., ovvero nei casi in cui sono ammesse le attività di intercettazione. Una simile soluzione, pur essendo stata in qualche misura paventata anche nel *Bollettino Protocollo Cassazione-CGUE*, 1/2021, para. 5.6.2., non ha riscosso molto seguito né in dottrina né da altre Corti. Per lo più è stato ritenuto che l'art. 15 Direttiva *e-Privacy*, non contenendo obblighi chiari, precisi ed incondizionati, non possa ritenersi *self executing* e capace di produrre effetti diretti. Per tale ragione, anche dinnanzi alla decisione della CGUE del 2 marzo 2021, non si

un intervento chiarificatore di un'alta Corte[56] o – ancor meglio – un intervento del legislatore nazionale[57], il Tribunale di Rieti, Sez. Penale, con ordinanza del 4 maggio 2021 ha promosso il primo rinvio pregiudiziale italiano alla CGUE in materia di conservazione e accesso ai metadati[58], chiedendo se l'art. 15 Direttiva *e-Privacy* osti ad «una normativa nazionale che renda il p.m., organo dotato di piene totali garanzie di indipendenza e autonomia (..) competente a disporre mediante decreto motivato l'acquisizione dei dati relativi al traffico e all'ubicazione ai fini di un'istruttoria penale»[59]. Certo non può essere taciuto il fatto che lo stesso Tribunale di Rieti abbia notificato alla CGUE, con lettera del 5 ottobre 2021, il ritiro della sua domanda di pronuncia pregiudiziale, così che la causa risulta ad oggi conclusa: l'intervenuta riforma della normativa nazionale ha fatto venir meno l'utilità, ai fini della soluzione del caso concreto, della determinazione da parte dei giudici di Lussemburgo del profilo problematico loro sottoposto, all'epoca del rinvio ancora fortemente dibattuto. Ciò che qui rileva comunque è evidenziare come la difformità di interpretazioni ed approcci delle Corti italiane dinnanzi alla sentenza *H.K. c. Prokuratuur* abbia portato ad un inedito e tanto caldeggiato dialogo con la CGUE, sintomo anche di una maggiore comprensione della complessità e delicatezza delle questioni emerse. E il richiamato rinvio assume certamente rilievo se si pensa alla diversa posizione espressa in quegli stessi mesi dalla Corte di Cassazione: quest'ultima, infatti, nella sentenza n. 28523 del 22 luglio 2021, aveva sostenuto che «la richiamata pronuncia Europea sembra incapace di produrre effetti applicativi immediati e diretti a causa dell'indeterminatezza delle espressioni ivi utilizzate al fine di legittimare l'ingerenza dell'autorità pubblica nella vita privata dei cittadini: infatti, il riferimento alle "forme gravi di criminalità" ed alla funzione di "prevenzione di gravi minacce alla sicurezza pubblica", sembra necessariamente implicare un intervento legislativo volto ad individuare, sulla base di

dovrebbe ricorrere alla disapplicazione dell'art. 132 Cod. Privacy, pur se considerato in contrasto con il diritto dell'UE. Sul punto si legga ampiamente il documento redatto dall'Ufficio del massimario e del ruolo, Servizio penale, della Corte Suprema di Cassazione, *Relazione su novità normativa. Misure urgenti in tema di acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, 13 ottobre 2021.

[56] *Ex multis*, F. TORRE, *Data retention. Una ventata di "ragionevolezza" da Lussemburgo*, cit., p. 552.

[57] F. RINALDINI, *Data retention e procedimento penale. Gli effetti della sentenza della CGUE nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore*, in *Giurisprudenza Penale Web*, 5, 2021.

[58] Domanda di pronuncia pregiudiziale C-334/21, proposta dal Tribunale di Rieti nel procedimento penale a carico di G.B. e R.H. Per approfondimenti: G. STAMPANONI BASSI, *Acquisizioni dei tabulati telefonici e telematici: il Tribunale di Rieti propone questione pregiudiziale alla CGUE*, in *Giurisprudenza Penale*, 13 maggio 2021; L. GRANOZIO, *Corte di Giustizia sui tabulati: soluzioni contrastanti*, in *Penale. Diritto e Procedura*, 18 maggio 2021.

[59] Para 4.3.1. della richiamata Ordinanza.

"criteri oggettivi", così come richiesto dalla stessa pronuncia della Corte Europea, le categorie di reati per i quali possa ritenersi legittima l'acquisizione dei dati di traffico telefonico o telematico». Escludendo dunque la diretta applicabilità della decisione della CGUE – allontanandosi così da quanto affermato dal giudice romano, come sopra evidenziato –, la Suprema Corte riconosceva, per la prima volta, l'importanza e la necessità di un intervento normativo volto quantomeno a determinare la soglia di "gravità" dei reati per i quali è possibile procedere all'accesso; ciò diversamente da quell'orientamento, ravvisabile ad esempio nell'Ordinanza del Tribunale di Padova e precedentemente sposato dalla Cassazione stessa[60], secondo cui la gravità della fattispecie criminosa può essere determinata, caso per caso, dal giudice, senza la necessità di un preciso elenco da parte del legislatore. Nella pronuncia del luglio 2021, dunque, è ravvisabile senz'altro un primo timido e solo parziale cambio di approccio nella giurisprudenza della Suprema Corte.

Ciò che la rapida carrellata delle più rilevanti e recenti decisioni in materia di acquisizione e conservazione dei metadati ha posto in evidenza è stato proprio il rilievo della pronuncia *H.K. c. Prokuratuur* che, in maniera praticamente inedita nel contesto italiano, ha risvegliato il dibattito sulla legittimità, proporzionalità nonché sui limiti e requisiti che debbono accompagnare l'impiego di tale strumento investigativo. Il primo rinvio pregiudiziale, sopra richiamato e promosso da una Corte italiana in tale materia, rappresenta, nonostante il suo rapido epilogo, un primo importante passo sia verso un più efficace e consapevole dialogo multilivello, sia nella direzione di una più seria consapevolezza del rilevante impatto che la giurisprudenza europea produce rispetto alla discussa normativa interna. Anche dinnanzi a tale maggiore sensibilità e comprensione della materia, l'approccio del giudice italiano ha mostrato però, ancora una volta, limiti e criticità. Nessun dubbio o discussione, infatti, sono sorti quanto alla pur problematica disciplina della *data retention* generalizzata ed indiscriminata, che invece tanto ha occupato l'attenzione di legislatori e Corti in altri Stati membri oltre che della CGUE stessa. Sebbene, quindi, non si possa certamente attribuire agli sviluppi giurisprudenziali del più recente passato un significato rivoluzionario o il segno di una decisa inversione del senso di marcia – molte, infatti, come si è detto, sono state le Corti che non hanno rilevato dubbi circa la conformità della disciplina nazionale rispetto al diritto dell'UE come interpretato dai giudici di Lussemburgo –, essi innegabilmente rappresentano un passo timido ma rilevante verso un dibattito più consapevole su tale delicata materia. E proprio da

[60] Si pensi alla sentenza 25 settembre 2019, n. 48737, in particolare para. 3.6.

queste ultime reazioni ed evoluzioni, registratesi tanto a livello sovranazionale quanto italiano, prende avvio quell'intervento del legislatore nazionale che caratterizza lo scenario presente.

3. *The Ghost of data retention Present*: le modifiche apportate dal recente d.l. 30 settembre 2021, n. 132 e dalla legge di conversione 23 novembre 2021, n. 178

Come anticipato, le prime e significative reazioni alla giurisprudenza della CGUE in materia di *data retention* si sono registrate, piuttosto sorprendentemente e criticamente, in Italia solo a seguito della pronuncia *H.K. c. Prokuratuur*. In tale contesto, la sopra evidenziata risposta delle Corti italiane, ancora per molti versi confusa e frammentaria, non è però l'unico e forse neppure il più evidente riscontro all'ennesimo intervento dei giudici di Lussemburgo: il 1 aprile 2021, infatti, il Governo nostrano ha accolto l'ordine del giorno 9/2670-A/10 – proposto in occasione dell'esame del disegno di Legge Europea 2019/2020 –, impegnandosi a rivedere la normativa all'epoca vigente alla luce dei principi e requisiti sempre più chiaramente affermati a livello europeo e che non parevano poter essere più ignorati[61]. Poco tempo dopo la pubblicazione della sentenza relativa al caso estone, il Governo italiano ha dunque mostrato una nuova ed auspicata attenzione alla disciplina della conservazione e accesso ai metadati, riconoscendone la distanza rispetto al portato della giurisprudenza della CGUE e ammettendo così, per la prima volta, la necessità di un intervento normativo. Insieme al vivace dibattito dottrinario[62], che non ha mancato di rilevare il significativo impatto che la decisione dei giudici di Lussemburgo del marzo 2021 poteva produrre nell'ordinamento italiano, anche il Presidente del Garante per la Protezione dei Dati Personali, Pasquale Stanzione, ha rimarcato l'importanza e l'improrogabilità di una decisa riforma legislativa

[61] Nell'OdG citato sono presenti alcune considerazioni di grande rilievo, che mettono in luce una più profonda consapevolezza dei rischi e delle serie minacce che lo strumento della *data retention* e accesso ai metadati comportano per il godimento dei diritti fondamentali. Viene dunque colta la delicatezza della materia e del bilanciamento sotteso: nel riconoscere come nel 2014 la compagnia Vodafone fosse stata destinataria di oltre 600.000 richieste di tabulati, in tale documento si legge come «esistono persino appositi programmi che, analizzando i registri delle chiamate su un determinato periodo, costruiscono un grafico delle relazioni di una persona; con l'evoluzione tecnologica e le nuove conoscenze sarà possibile progressivamente ottenere dai tabulati un controllo della persona sempre più pregnante».

[62] Anche la dottrina ha da più parti sottolineato l'importanza di un intervento normativo, come suggerito da G. BATTARINO, *CGUE e dati relativi al traffico telefonico e telematico. Uno schema di lettura*, in *Questione Giustizia*, 21 aprile 2021. L'autore evidenziava peraltro come una strada alternativa a tale intervento – o in caso di inerzia del legislatore – potesse essere ravvisata in un giudizio incidentale di legittimità costituzionale vertente sull'art. 132 Cod. Privacy.

in materia. Nella Relazione per l'anno 2020, tenutasi il 2 luglio 2021, nonché nella *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico* del 2 agosto 2021, il Garante ha sollecitato nuovamente[63] una riforma dell'art. 132 Cod. Privacy nonché dell'art. 24 della Legge Europea del 2017, richiamando Governo e Parlamento a riflettere più approfonditamente sulla compatibilità della disciplina italiana con i principi stabiliti dalla CGUE[64].

Sotto la spinta di tali puntuali e dirette indicazioni e dinnanzi all'urgenza[65] di un'azione chiarificatrice della disciplina nazionale, il Governo ha adottato il d.l. 30 settembre 2021, n. 132 recante *Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP*, pubblicato in G.U. il medesimo giorno ed avente immediata efficacia.

L'art. 1 di tale normativa che, come si comprende bene dalla titolazione, non è interamente dedicata alla disciplina della *data retention* ma contiene anzi disposizioni estremamente variegate tra loro, introduce modifiche alla disciplina sull'acquisizione dei metadati per scopi investigativi, agendo direttamente sul testo dell'art. 132 Cod. Privacy.

In particolare, le innovazioni di forte rilievo che hanno interessato tale norma hanno da un lato ripristinato[66] in capo al giudice il controllo preventivo all'acquisizione, controllo che deve sfociare in un decreto motivato e che deve essere attivato mediante richiesta del pubblico ministero, del difensore dell'imputato, di persona sottoposta ad indagini, di persona offesa e altre parti private[67];

[63] Diversi infatti sono stati, nel corso del tempo, i richiami in tal senso espressi dal Garante per la Protezione dei Dati, il quale peraltro non ha mancato di esprimere perplessità e preoccupazioni sin dalla adozione della Legge Europea. Sul punto si rimanda alle dichiarazioni rese da Antonello Soro in occasione del Convegno *Privacy digitale e protezione dei dati personali tra persona e mercato*, reperibili sul sito web del Garante, nonché al Parere n. 8005333 sullo schema di decreto legislativo recante attuazione della Dir. 2016/680, del 22 febbraio 2018. Interessanti sono anche le dichiarazioni rese dall'allora Garante europeo della protezione dei dati, Giovanni Buttarelli, che aveva redarguito il legislatore italiano quanto alla sproporzionata durata della conservazione, soprattutto dinnanzi a scelte, quali quelle del legislatore tedesco, che avevano invece previsto un periodo di *data retention* massimo di dieci settimane (si legga l'intervista a Giovanni Buttarelli, su *La Stampa*, 13 novembre 2017).

[64] Rilevando peraltro le posizioni contrastanti «registratesi in sede pretoria dopo la sentenza del 2 marzo scorso», il Garante ha affermato l'importanza di riflettere su una «riforma della disciplina della *data retention* tale da differenziare condizioni, limiti e termini di conservazione dei dati di traffico telefonico e telematico in ragione della particolare gravità del reato per cui proceda, comunque entro periodi massimi compatibili con il su richiamato principio di proporzionalità, come interpretato dalla CGUE. Occorrerebbe inoltre valutare – anche sulla scorta di alcuni OdG accolti dal Governo nell'ambito di recente procedimenti legislativi – l'opportunità di subordinare l'acquisizione dei dati all'autorizzazione del Gip, ferma restando, ovviamente, nei casi d'urgenza, la possibilità per il p.m. di provvedervi con proprio decreto, soggetto a convalida solo in fase successiva, sul modello dell'art. 267, co. 2, c.p.p.».

[65] Questo giustifica, a parere del Governo, l'urgenza dell'atto avente forza di legge adottato, come riportato nello stesso preambolo del d.l. nel quale vengono illustrati i presupposti di straordinaria necessità ed urgenza ex art. 77 Cost.

[66] Come si è visto nella ricostruzione svolta nel previo paragrafo, infatti, inizialmente questa scelta era già stata promossa dal legislatore italiano.

[67] Così si legge al co. 1, lett a), che ha così modificato l'art. 132, co. 3, Cod. Privacy.

dall'altro lato, hanno limitato l'acquisizione di metadati ai soli casi di procedimenti penali e attività di indagine finalizzati alla repressione di un catalogo preciso di reati presupposto, così fornendo per la prima volta una definizione dei reati *gravi* legittimanti le operazioni di accesso. Queste ultime, dunque, secondo quanto stabilito dal decreto-legge, potevano avvenire unicamente in caso di sussistenza di «*sufficienti indizi* di reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 del c.p.p., e di reati di minaccia e di molestia o disturbo alle persone col mezzo del telefono, quando la minaccia, la molestia e il disturbo sono gravi, *ove rilevanti ai fini della prosecuzione delle indagini*»[68].

L'atto disposto dal Governo ha poi aggiunto all'art. 132 Cod. Privacy il co. 3-bis, nel quale è stata prevista un'eccezionale procedura d'urgenza che consente, similmente a quanto disposto dall'art. 267, co. 2 c.p.p., direttamente al pubblico ministero di provvedere all'acquisizione dei metadati laddove vi sia un fondato motivo di ritenere che dal ritardo possa derivare un pregiudizio grave alle indagini; tale disciplina eccezionale e residuale consente sì una maggiore rapidità nell'accesso ma impone comunque una successiva convalida da parte del giudice entro le quarantotto ore successive alla comunicazione fornita dal pubblico ministero, che deve a sua volta essere fatta pervenire entro quarantotto ore dall'accesso stesso, pena l'inutilizzabilità dei metadati raccolti e acquisiti[69]; la analizzata previsione, oltre ad avere una evidente utilità in termini di chiarezza, è parsa del tutto in linea con quanto affermato anche dalla CGUE, che ha espressamente

[68] Per completezza è utile indicare come sia stato eliminato ogni riferimento alla possibilità, prima attribuita dall'art. 132, co. 3 al difensore dell'imputato o dell'indagato, di un accesso diretto ai dati relativi alle comunicazioni telefoniche in entrata; non è stata confermata infatti la previa statuizione secondo la quale «Il difensore dell'imputato o della persona sottoposta alle indagini può richiedere direttamente al fornitore i dati relativi alle utenze intestate al proprio assistito con le modalità indicate dall' articolo 391-quater del codice di procedura penale. La richiesta di accesso diretto alle comunicazioni telefoniche in entrata può essere effettuata solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397; diversamente, i diritti di cui agli articoli da 12 a 22 del Regolamento possono essere esercitati con le modalità di cui all'articolo 2-undecies, comma 3, terzo, quarto e quinto periodo». Secondo la normativa vigente, quindi, anche il difensore dell'imputato o indagato è tenuto a richiedere l'acquisizione al giudice.

[69] Un ulteriore co. 3-ter è stato poi inserito, volto a riconoscere forme di tutela dei diritti dell'interessato, stabilendo che «rispetto ai dati conservati per le finalità indicate al co. 1, i diritti di cui agli artt. da 12 a 22 del Regolamento [GDPR, quali il diritto all'accesso, alla rettifica, alla cancellazione, etc.] possono essere esercitati con le modalità di cui all'art. 2-*undecies*, co. 3, terzo, quarto e quinto periodo», cioè anche per il tramite del Garante. Questo inserimento, successivo rispetto alla versione originaria del decreto, è frutto delle segnalazioni svolte dal Garante stesso nel *Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, 10 settembre 2021, doc. web 9704851, di cui si parlerà più ampiamente a breve.

stabilito la possibilità di derogare al previo controllo in «situazioni di urgenza debitamente giustificate, nel quale caso il controllo deve avvenire entro termini brevi»[70].

Tutte le modifiche richiamate, dunque, sono state motivate dall'esigenza impellente di conformare la disciplina nazionale al diritto dell'UE, così come interpretato dalla CGUE nella pronuncia del marzo 2021: l'innovativo e prima del tutto assente carattere di gravità del reato quale limitazione all'acquisizione, insieme all'approccio maggiormente garantista sotto il profilo procedurale, tramite la piena giurisdizionalizzazione dell'acquisizione stessa, sono chiari segnali di una maggiore attenzione prestata dal Governo rispetto ai principi delineati a livello europeo. Per la prima volta dall'avvio della c.d. *data retention saga*, una pronuncia dei giudici di Lussemburgo in tale delicata materia riesce a provocare un effetto dirompente nel contesto italiano, portando ad un "cambio di rotta": le modifiche normative introdotte puntano ad agire nella direzione di una più solida garanzia dei diritti fondamentali e a delimitare maggiormente e con precisione i casi in cui le esigenze securitarie e di repressione dei reati sono tali da giustificare una significativa compressione della sfera privata.

Pur avendo certamente avuto il merito di risolvere quelle incertezze e molteplicità di interpretazioni emerse nella giurisprudenza nazionale a seguito della pronuncia *H.K. c. Prokuratuur*, l'intervento del Governo non è rimasto esente da critiche e perplessità, anche di carattere e segno estremamente differente. Volendo qui riportare alcuni dei più rilevanti commenti alla normativa analizzata, punto di partenza di grande interesse è certamente rappresentato dal *Parere sullo schema di decreto-legge per la riforma della disciplina dell'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*[71] disposto dal Garante per la Protezione dei Dati Personali. In tale documento, infatti, quest'ultimo ha sottolineato come le novità da introdursi mediante decreto-legge fossero certamente conformi alle indicazioni e ai principi stabiliti dalla rilevante giurisprudenza della CGUE; anche la distinzione tra la disciplina dell'acquisizione dei metadati e quella delle intercettazioni operata attraverso l'impiego di diversi termini – "carattere sufficiente" e non "grave" degli indizi di reato, "rilevanza" investigativa di tali informazioni anziché "assoluta indispensabilità" –, è risultata del tutto ragionevole e motivata dalla maggiore intrusività nella sfera privata rappresentata dalle captazioni dirette dei contenuti delle

[70] Così si legge al para. 58 della sentenza *H.K. c. Prokuratuur*.
[71] Vedi *supra* nota 69.

comunicazioni che, proprio per tale superiore ingerenza risultano tali da giustificare regole procedurali e requisiti sostanziali più stringenti. Una simile distinzione è stata riproposta anche con riferimento alla definizione dei reati presupposto, rispetto ai quali non sono «state infatti accolte quelle proposte volte ad estende al mezzo *de quo* le ipotesi legittimanti l'intrusione nella sfera privata degli utenti previste in materia di intercettazioni telefoniche ai sensi dell'art. 266 c.p.p., nell'evidente convinzione della sussistenza di una differenza ontologica tra i due strumenti in oggetto»[72]. Insomma, al Garante – ma anche a buona parte della dottrina – è parsa assolutamente condivisibile la scelta del Governo di ravvicinare le due discipline sopra richiamate sotto lo specifico profilo della giurisdizionalizzazione del vaglio preventivo, salvo mantenere poi un margine di opportuna differenziazione per quanto concerne gli altri presupposti legittimanti l'impiego di simili strumenti, impiegando termini e condizioni più flessibili per l'acquisizione dei metadati[73].

Nonostante i profili positivi dell'intervento normativo, ben evidenziati nel Parere, all'interno di quest'ultimo è stato però individuato anche un profilo critico di estremo rilievo: «resta da adeguare alla giurisprudenza di Lussemburgo la disciplina della durata della conservazione dei tabulati (..). La legittimità dell'acquisizione dei tabulati (..) esige infatti una parimenti legittima conservazione (alla prima preordinata), che tale non potrebbe ritenersi se incompatibile con il principio di proporzionalità (..). Alla luce di tale criterio andrebbe, dunque, ripensato – se del caso anche in sede di conversione del decreto-legge – il termine di conservazione di 72 mesi previsto dalla disciplina vigente, riconducendolo entro margini maggiormente compatibili con il canone di proporzionalità», para. 2. Con questa osservazione puntuale e precisa il Garante ha quindi suggerito – al Governo ma anche, eventualmente, al Parlamento in occasione della necessaria approvazione della legge di conversione – di adottare una riforma più completa e capace di interessare anche la fase di

[72] A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici: breve commento a prima lettura del d.l. 30 settembre 2021, n. 132*, in *Sistema Penale*, 8 ottobre 2021.

[73] Questo approccio pare peraltro condivisibile e compatibile con quanto affermato dalla giurisprudenza della CGUE nella richiamata *data retention saga*, nonché dalla Corte EDU, in particolare nella pronuncia Grande Sezione, 21 maggio 2021, ricorsi n. 58170/13, 62322/14 e 24960/15, *Big Brother Watch & others v. UK*, nella quale è stata riconosciuta l'invasività della mera conservazione ed acquisizione dei metadati, benché in misura differente rispetto all'accesso ai contenuti delle comunicazioni. Del resto, anche la Corte costituzionale italiana, nella sentenza n. 38/2019 ha affermato come, per quanto sia ravvisabile una distinzione tra disciplina – ed ingerenza nella sfera privata – perpetrata dalle intercettazioni, diversamente dall'acquisizione di dati esterni di una comunicazione, anche tale ultima tipologia di informazioni debba «beneficiare della garanzia che alla libertà e alla segretezza di ogni forma di comunicazione è assicurata dall'art. 15 Cost.», para. 2.3; questo perché anche ai metadati è attribuito un «indubbio significato comunicativo».

conservazione. Tracciando un legame tra quest'ultima e la successiva acquisizione, viene evidenziato ciò che già la CGUE da tempo ha affermato, ovvero che la lesività dei diritti fondamentali non avviene, come invece sostenuto da taluni Governi nazionali, solo nel momento dell'accesso, bensì si realizza già con la conservazione, che deve pertanto anch'essa sottostare ai principi di proporzionalità e stretta necessità[74]. La durata straordinariamente lunga della *data retention* italiana, statuita dalla Legge Europea 2017, viene così ritenuta un elemento potenzialmente critico, da "riportare" entro i confini di quelle condizioni e limiti sanciti dalla giurisprudenza dei giudici di Lussemburgo.

Accanto a tali attenti moniti del Garante, che pure non negano la correttezza e la compatibilità al diritto dell'UE delle modiche proposte in materia di acquisizione, anche la dottrina – in gran parte studiosi del diritto processuale penale – si è interrogata sulla portata del decreto-legge, rilevandone taluni profili critici e lacune di non marginale rilievo.

Un primo aspetto di interesse è da individuarsi senza dubbio nella mancata predisposizione di un limite soggettivo all'acquisizione dei metadati, ovvero di soggetti ben individuati e specificati rispetto ai quali l'accesso ai dati è legittimo. Sul punto, la sentenza *H.K. c. Prokuratuur* infatti specificava la necessità di stabilire criteri volti a «definire le circostanze e le condizioni in presenza delle quali deve essere concesso alle autorità nazionali competenti l'accesso ai dati in questione. A questo proposito, un accesso siffatto può, in linea di principio, essere consentito, in relazione con l'obiettivo della lotta contro la criminalità, soltanto per i dati di persone sospettate di progettare, di commettere o di aver commesso un illecito grave, o anche di essere implicate in una maniera o in un'altra in un illecito del genere», para. 50. Una simile restrizione e determinazione preventiva dei soggetti destinatari delle operazioni di accesso, però, è parsa a taluni eccessiva e potenzialmente critica: «un'eventuale operazione di tipizzazione (*numerus clausus*) dei soggetti passivi [delle operazioni di acquisizione dei metadati] risulterebbe alquanto impervia e destinata, quasi certamente, a prestare il fianco a censure dirette ad evidenziarne l'inadeguatezza rispetto alle

[74] Nei rinvii pregiudiziali *La Quadrature du Net* e *Privacy International*, ad esempio, come evidenziato dall'Avvocato generale Campos Sanchez-Bordona, nelle sue Conclusioni del 15 gennaio 2021, la maggioranza degli Stati membri che hanno presentato osservazioni hanno sostenuto che «sarebbero sufficienti norme rigorose sull'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica, che possano compensare, in qualche modo, la gravità dell'ingerenza che la conservazione generalizzata e indifferenziata di tali dati comporta», para. 71. Tale approccio è stato completamente smentito dalle già richiamate decisioni della CGUE, nelle quali è stato ribadita l'incompatibilità, salvo per esigenza di sicurezza nazionale, della *bulk data retention* con il diritto dell'UE, indipendentemente cioè dalla disciplina dell'accesso: i requisiti e criteri indicati dai giudici di Lussemburgo nella consolidata giurisprudenza in materia debbono dunque essere tutti cumulativamente e complessivamente sussistenti.

molteplici situazioni che si potrebbero concretamente manifestare nella prassi»[75]. La scelta di non riproporre una elencazione definita sulla scia della richiamata statuizione dei giudici di Lussemburgo non è sembrata quindi, a parere di taluni studiosi, del tutto irragionevole, soprattutto in termini di concreta efficacia dello strumento dell'acquisizione stessa[76]. Ma con riferimento a tale profilo, invero estremamente delicato perché in grado di circoscrivere significativamente la concreta attuazione dello strumento investigativo in analisi, le considerazioni sopra proposte sono tutt'altro che pacifiche: secondo Filippi, ad esempio, «si sarebbe dovuti legislativamente individuare anche i "soggetti" perché, di regola, l'accesso è ammesso soltanto ai dati di chi è sospettato di reato e solo eccezionalmente, in "situazioni particolari" (come quelle in cui gli interessi vitali della sicurezza nazionale, delle difesa o della sicurezza pubblica siano minacciati da attività di terrorismo), si può ammettere l'accesso ai dati di persone non sospettate, ma a condizione che esistano "elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo". Invece nulla al riguardo è stato precisato nel decreto-legge»[77]. Secondo l'autore – che, come si è visto, ha ampiamente richiamato principi e considerazioni emerse dalla giurisprudenza della CGUE – risulterebbe pertanto inevitabile sollevare su tale punto e con riferimento a tale lacuna normativa una questione di legittimità costituzionale «in rapporto all'art. 117 Cost., che vincola la potestà legislativa dello Stato al rispetto, tra l'altro, dei vincoli derivanti dall'ordinamento comunitario e dagli obblighi internazionali»[78].

Anche il rilevante profilo della determinazione dei reati presupposto non ha mancato di destare commenti spesso divergenti: mentre per taluni la scelta compiuta dal Governo ha comportato, *de facto*, un'apertura molto ampia e in realtà assai poco selettiva delle fattispecie di reato legittimanti l'acquisizione, considerando che i criteri stabiliti finiscono di fatto col comprendere fattispecie che

[75] A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici,* cit. L'autore sottolinea come l'assenza di una limitazione sotto questo profilo e il mancato richiamo da parte del Governo dell'espressione promossa dei giudici di Lussemburgo consenta ad esempio di non limitare solo agli indagati o imputati l'acquisizione dei metadati, bensì di renderla possibile anche nel caso di procedimenti contro ignoti o «di garantire al p.m. di poter accedere alle informazioni di tutti i soggetti che, seppur indirettamente, abbiano facilitato l'*iter criminis* (ad esempio prestando inconsapevolmente il proprio smartphone allo stesso indagato) ovvero siano coinvolti, anche in veste di persona offesa o possibile testimone, nei fatti oggetto di accadimento».

[76] In questi termini, come si è visto, si è espresso A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici,* cit.

[77] L. FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, in *Penale. Diritto e procedura*, 1 ottobre 2021, p. 11.

[78] *Ibidem*, p. 12.

paiono carenti di una reale gravità[79], per altri invece l'indicazione prevista ha finito con l'escludere una serie di reati per i quali sarebbe stato invece corretto e proporzionato poter disporre dello strumento di acquisizione dei metadati[80].

Come si nota, quindi, le scelte sostanziali del Governo hanno aperto un significativo dibattito, espressione della delicatezza della materia e del diverso punto di equilibrio che può essere individuato tra esigenze securitarie e tutela dei diritti fondamentali. Di ciò è estremamente indicativa la diversità di vedute espresse con riferimento alla giurisdizionalizzazione della procedura di acquisizione, anch'essa oggetto di opposti pareri e valutazioni. Vi è infatti chi ha ravvisato nella "svolta garantista" operata dal d.l. un'insidia reale e profonda all'efficacia ed efficienza dello strumento dell'accesso ai metadati: per Pestelli la riforma esaminata, «oltre a riportare indietro le lancette dell'orologio della nostra legislazione di quasi vent'anni (quando invero i tabulati potevano essere acquisiti solo con decreto del giudice su richiesta delle parti), nel dare seguito – del tutto acriticamente – a tale giurisprudenza [della CGUE], da un lato ha (re)introdotto disposizioni farraginose per lo sviluppo delle indagini e pesanti limiti all'attività di ricerca della prova penale, dall'altro non ha tenuto conto delle difformità tra il caso che aveva determinato suddetta pronuncia e la figura del nostro p.m., così come emergente dall'ordinamento costituzionale»[81]. In senso contrario, invece, si è espresso chi ha ritenuto che il ruolo attribuito al giudice, «se pure aggrava la concreta operatività degli uffici inquirenti anche nei loro sinora più agili rapporti in materia con la polizia giudiziaria, pone al riparo da contestazioni l'uso di una così importante fonte di conoscenza investigativa»[82]. Una maggiore salvaguardia dei diritti fondamentali, insomma, che giustifica un irrigidimento, pur ragionevole e proporzionato, della disciplina normativa[83].

[79] In questi termini G. AMATO, *Nella 'costruzione' normativa si è sminuito il ruolo del Pm*, in *Guida al diritto*, 39, 2021, p. 22, come richiamato anche da F. RINALDINI, *La nuova disciplina del regime di acquisizione dei tabulati telefonici e telematici: scenari e prospettive*, in *Giurisprudenza Penale*, 10, 2021.

[80] In questo senso G. PESTELLI, *D.l. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonico e telematici*, in *Quotidiano giudirico*, 4 ottobre 2021, che svolge un dettagliato elenco di importanti e gravi reati esclusi dalla definizione fornita dalla normativa in esame.

[81] G. PESTELLI, *D.l. 132/2021: un discutibile e inutile aggravio di procedura per tabulati telefonico e telematici*, cit.

[82] G. BATTARINO, *Acquisizione di dati di traffico telefonico e telematico per fini di indagine penale: il decreto-legge 30 settembre 2021, n. 132*, cit.

[83] Tale questione si era peraltro presentata nel passato, quando, come anticipato, l'art. 132 Cod. Privacy modificato dal d.l. 24 dicembre 2003, n. 354 aveva previsto l'intervento autorizzatorio del giudice ai fini dell'acquisizione di metadati. Ebbene già sulla legittimità di tale scelta normativa era stata chiamata a pronunciarsi la Corte costituzionale, che aveva però sbrigativamente rilevato come la questione fosse del tutto superata dalla sopravvenienza del d.l. 27

Le divergenze di vedute, anche sostanziali, tra chi identifica nella riforma un inutile e sproporzionato appesantimento procedurale, in grado di minarne l'efficacia, e chi invece ne elogia la portata garantista – sottolineando anzi la carenza di talune restrizioni più rigide –, sono infine riscontrabili in un'ulteriore scelta del Governo: quella di non inserire nel testo finale del decreto-legge alcuna disciplina transitoria, invero originariamente proposta all'art. 2, così lasciando aperta all'interpretazione del giudice la questione relativa alla retroattività delle nuove disposizioni rispetto alle acquisizioni svolte nei procedimenti in corso. La disposizione inizialmente prevista dal Governo sanciva l'utilizzabilità dei metadati acquisiti mediante autorizzazione del pubblico ministero nei procedimenti pendenti al momento dell'entrata in vigore del decreto-legge, imponendo però una forte limitazione atta a restringerne l'impiego solo nei casi di ricorrenza dei presupposti sanciti dal decreto-legge e sulla base di una valutazione a posteriori, rimessa al Giudice – in sede di successiva convalida da svolgersi alla prima udienza successiva all'entrata in vigore della normativa esaminata – o al G.i.p. nei procedimenti ancora in fase di indagine. Secondo taluni, tuttavia, questa disciplina avrebbe comportato «notevoli problemi in sede applicativa»[84], così che «forse non è infondato ritenere che la mancata riproposizione, che avrebbe consentito di porre la questione in tutti i procedimenti in qualsiasi grado si fossero trovati, sia stata determinata dalla diseconomia della procedura legata al ritardo che la richiesta di trasmissione di atti – per la decisione – avrebbe determinato»[85].

Mentre alcuni primi commentatori hanno quindi condiviso la scelta di eliminare la disposizione transitoria[86], vi è invece chi ha ritenuto precipuo compito del legislatore sciogliere tale delicato nodo, anziché attribuirne la definizione in capo ai singoli giudici: «spetterebbe al legislatore stabilire, senza rimetterne la soluzione ad oscillanti scelte pretorie, tenuto conto dei riflessi della nuova disciplina sul momento valutativo della prova già acquisita dal p.m. secondo la previgente normativa, viziata da una sostanziale incompatibilità, pur sopravvenuta, con la giurisprudenza

luglio 2005, n. 144 che aveva modificato la disposizione oggetto di vaglio di legittimità, assegnando al pubblico ministero il compito di provvedere al previo controllo in merito all'acquisizione di metadati. Per approfondimenti sui rilievi svolti nella pronuncia 14 novembre 2006, n. 372, si rinvia a M. PINNA, *Doppio binario di accesso ai dati sul traffico telefonico: una scelta legislativa ragionevole ratificata (con argomenti non irresistibili) dalla Corte costituzionale*, in *Giurisprudenza costituzionale*, 2006, p. 3929; E. BASSOLI, *Acquisizione dei tabulati vs. privacy: la data retention al vaglio della Consulta*, in *Diritto in Internet*, 3, 2007, p. 14 ss.

[84] C. GITTARDI, *Sull'utilizzabilità dei dati del traffico telefonico e telematico acquisiti nell'ambito dei procedimenti pendenti alla data del 30 settembre 2021*, in *Giustizia Insieme*, 7 ottobre 2021.

[85] G. SPANGHER, *Data retention: le questioni aperte*, in *Giustizia Insieme*, 9 ottobre 2021.

[86] Di questa opinione Gittadi e Pestelli, già citati *supra*.

europea»[87]. In altre parole, sebbene molti studiosi abbiano concordato che, in assenza di una espressa previsione e considerato il principio *tempus regit actum*, le acquisizioni operate sulla base della previa normativa avrebbero dovuto essere considerate utilizzabili e legittime[88], escludendo dunque la retroattività della nuova disciplina, la mancanza di una disciplina transitoria è stata comunque ritenuta tale da aprire potenzialmente la strada a differenti interpretazioni giurisprudenziali, creando una possibile situazione confusa e disomogenea, a detrimento della certezza del diritto, specialmente in una materia tanto delicata quanto quella penale; in assenza di specifica disposizione, pertanto, il decreto-legge, ha lasciato all'«interprete di ogni livello [il compito di] risolvere il problema della sorte dei dati di traffico telefonico e telematico già acquisiti nei procedimenti (e nei processi) pendenti, se non tutti, quanto meno dal 2 marzo 2021 (data di pubblicazione della sentenza [*H.K. c. Prokuratuur*] (..) al 29 settembre 2021 (vigilia dell'entrata in vigore del d.l. n. 132 del 2021»[89].

Ebbene sotto questo profilo, così dibattuto e complesso, è specificamente intervenuto il Parlamento in sede di approvazione della legge di conversione del d.l. sin qui esaminato: la l. 23 novembre 2021, n. 178 ha infatti reinserito la disposizione transitoria inizialmente prevista nel decreto-legge e successivamente espunta nel testo finale, modificandone però il contenuto. La versione attuale così dispone che i metadati «acquisiti nei procedimenti penali in data precedente all'entrata in vigore del decreto, possono essere utilizzati a carico dell'imputato solo unitamente ad altri elementi di prova ed esclusivamente per l'accertamento dei reati per i quali la legge stabilisce la pena dell'ergastolo o della reclusione non inferiore nel massimo a tre anni, determinata a norma dell'art. 4 c.p.p., e dei reati di minaccia e di molestia o disturbo alle persone con il mezzo telefonico, quando la minaccia, la molestia o il disturbo sono gravi». Questa disposizione ha, sin dai primi commenti "a caldo" della legge di conversione, sollevato notevoli perplessità. Scardinando l'interpretazione che aveva ritenuto applicabile il principio *tempus regis actum* con riferimento alla disciplina prevista nel decreto-legge, la misura transitoria riportata, considerata da taluni «improvvida», è apparsa censurabile innanzitutto sotto il profilo della tecnica legislativa: essa è

[87] F. RESTA, *La nuova disciplina dell'acquisizione dei tabulati*, in *Giustizia Insieme*, 2 ottobre 2021.

[88] In questo senso Battarino, Pestelli, Gittardi e Spangher, mentre ha sostenuto la sopravvenuta inutilizzabilità dei metadati acquisiti sulla base della previgente disciplina S. MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: una proposta*, in *Cassazione Penale*, 2, 2015, p. 760 ss. Sul punto si rimanda alla ampia e dettagliata analisi presentata nel documento Ufficio del Massimario della Corte Suprema di Cassazione, *Relazione su novità normativa*, cit.

[89] Ufficio del Massimario della Corte Suprema di Cassazione, *Relazione su novità normativa*, cit., p. 31.

stata infatti inserita non nell'art. 132 Cod. Privacy, come tutte le altre modifiche apportate dal decreto-legge, bensì nel decreto-legge stesso, all'art. 1, co. 1-bis, così rendendo «più difficoltosa la conoscenza e la lettura dei precetti normativi»[90]; oltre a tale profilo, certamente discutibile, ciò che è apparso ancor più problematico è stata la retroattività del requisito della gravità del reato introdotto con decreto, nonché l'espressa previsione secondo cui i metadati acquisiti su autorizzazione del pubblico ministero possono essere impiegati solo a carico dell'imputato – e non dell'indagato ad esempio – e solo unitamente ad altri elementi di prova. Il rischio è quello, serio, di veder travolgere «interi atti di indagine ritualmente e legittimamente compiuti secondo disposizioni *ratione temporis* vigenti all'epoca in cui sono stati compiuti, sulla base di una norma successiva che ne sancisce l'inutilizzabilità retroattiva (..). Verranno così definitivamente travolte, per legge, tutte le attività acquisitive di dati telefonici o telematici svolte in relazione a fatti particolarmente odiosi, che non rientrano tra i limiti edittali della nuova disciplina»[91]. Uno scenario così tratteggiato potrebbe richiedere un ulteriore provvedimento normativo ma anche rendere necessario un intervento della Corte costituzionale al fine di chiarire la legittimità di una simile disposizione transitoria dalle potenziali dirompenti conseguenze.

Certamente è ancora troppo presto per valutare la portata dell'introduzione, in sede di conversione, di una disposizione capace di agire nel passato, provocando cioè effetti rispetto ad acquisizioni già legittimamente svoltesi sulla base della previa normativa; se si comprende come la *ratio* di una simile misura sia quella di tutelare la necessaria terzietà ed indipendenza del controllo preventivo richiesto dalla giurisprudenza della CGUE – tanto è vero che con riferimento ai dati che possono essere usati a vantaggio dell'imputato la norma transitoria non dispone nulla, così che in tal caso dovrebbe essere applicata la disciplina vigente al momento dell'acquisizione, sulla base del principio *tempus regit actum*[92] –, desta comunque perplessità una rigida estensione al passato dei requisiti ad oggi previsti, che rischiano di incidere – in che misura non è ancora possibile dirlo – sull'effettivo svolgimento della fondamentale attività repressiva e di indagine e produrre dunque un

[90] G. PESTELLI, *Convertito in legge il D.l. 132/2021: le modifiche apportate (e quelle mancate) in materia di tabulati*, in *Il Quotidiano Giuridico*, 18 novembre 2021; l'autore sottolinea, in una dettagliata analisi della legge di conversione, alcuni profili positivi e utili innovazioni, non mancando tuttavia di mettere in luce gli aspetti ancora problematici e i nodi irrisolti nonché le modifiche che hanno destato maggiori perplessità.

[91] G. PESTELLI, *Convertito in legge il D.l. 132/2021*, cit.

[92] In questi termini si legga il Dossier *Misure urgenti in materia di giustizia e di difesa, nonché proroghe in tema di referendum, assegno temporaneo e IRAP Elementi per l'esame in Assemblea D.L. 132/2021 – A.C. 3298-A*, 5 novembre 2021, elaborato dal Servizio Studi del Senato.

danno all'interesse pubblico e alla legittima aspettativa della collettività di ottenere una repressione dei reati. Senza dubbio questa modifica disposta dalla legge di conversione darà luogo nei prossimi mesi ad un più profondo dibattito che, del resto, va inserito in un quadro ben più ampio e complesso: già nei rinvii pregiudiziali promossi dalle Corti di Belgio e Irlanda[93] era stato infatti richiesto alla CGUE di pronunciarsi quanto alla possibilità da parte dei giudici nazionali di limitare nel tempo gli effetti di una dichiarazione di incompatibilità della normativa nazionale in materia di conservazione e accesso ai metadati con il diritto dell'UE[94]. Su tale punto la CGUE ha, ad oggi, già avuto modo di pronunciarsi in senso negativo – benché in maniera piuttosto rapida – nel caso *La Quadrature du Net*[95], mentre l'occasione di meglio specificare tale profilo di evidente grande interesse per i Governi nazionali è offerta dal pendente rinvio elaborato dalla *Supreme Court* irlandese. Anche gli attenti e rilevanti quesiti posti da giudici di altri Stati membri contribuiscono quindi a comprendere come l'utilizzabilità dei metadati acquisiti sulla base di una normativa dichiarata non conforme al diritto dell'UE rappresenti una questione di estrema delicatezza ed importanza che potrebbe inficiare, in misura estremamente profonda, la possibilità di ricorrere allo strumento investigativo dell'accesso ai metadati, talvolta assolutamente essenziale per la lotta e il perseguimento di reati.

Insieme a questo primo e fortemente discusso profilo, la legge di conversione ha inoltre inserito altre rilevanti innovazioni rispetto al testo del decreto-legge, pur confermandone nella sostanza la portata generale e lasciando intoccato l'elenco dei reati presupposto e la disciplina d'urgenza. Innanzitutto il Parlamento è intervenuto quanto al criterio della *rilevanza* dell'accesso ai metadati: essa non deve essere più valutata rispetto al fine della prosecuzione delle indagini, come

[93] Si far riferimento ai rinvii *supra* richiamati, *La Quadrature du Net* e *Ordre des Barreaux Francophone et Germanophones*, già decisi dalla CGUE con sentenza del 6 ottobre 2020, nonché al rinvio ancora pendente promosso dalla Supreme Court irlandese *G.D. c. The Commissioner of the Garda Siochana e al.*, C-140/20.

[94] Anche il rinvio pregiudiziale promosso dal Tribunale di Rieti presentava tale quesito, chiedendo alla CGUE di fornire ulteriori chiarimenti interpretativi quanto ad una eventuale applicazione irretroattiva dei principi stabiliti nella pronuncia *H.K. c. Prokuratuur*, «tenuto conto delle preminenti esigenze di certezza del diritti nell'ambito della prevenzione, accertamento e contrasto di gravi forme di criminalità o minacce alla sicurezza» (così si legge nella domanda di pronuncia pregiudiziale).

[95] In tale pronuncia la CGUE ha stabilito come «il mantenimento degli effetti di una normativa nazionale, come quella di cui trattasi nei procedimenti principali [incompatibile cioè con il diritto dell'UE], implicherebbe che detta normativa continui ad imporre ai fornitori di servizi di comunicazione elettronica obblighi che risultano contrari al diritto dell'Unione e comportano ingerenze gravi nei diritti fondamentali delle persone i cui dati sono stati conservati. (..) Il giudice del rinvio non può applicare una disposizione del suo diritto nazionale che lo autorizza a limitare nel tempo gli effetti di una dichiarazione di illegittimità ad esso incombente, in forza di tale diritto, della legislazione nazionale di cui trattasi nei procedimenti principali», para. 42 ss.

previamente disposto, bensì più genericamente «per l'accertamento dei fatti». In tal modo vengono fugati i dubbi che la previa dicitura aveva sollevato quanto alla possibilità da parte del difensore dell'indagato o imputato di richiedere l'accesso ai metadati, accesso che in quel caso sarebbe servito per lo svolgimento delle indagini difensive e dunque per l'"accertamento dei fatti" e non, propriamente, per la prosecuzione delle indagini[96]. Similmente, intervenendo su di un ulteriore profilo dubbio ed eccessivamente vago del decreto-legge, la legge di conversione ha meglio precisato le modalità di acquisizione: mentre sulla base del decreto-legge i dati dovevano essere «acquisiti presso il fornitore con decreto motivato del giudice», facendo sorgere perplessità con riferimento al soggetto che concretamente avrebbe dovuto provvedere alla acquisizione – il giudice direttamente, il pubblico ministero o la parte richiedente l'autorizzazione? –, ora tale dubbio interpretativo è superato dall'impiego dell'espressione «i dati sono acquisiti previa autorizzazione rilasciata dal giudice con decreto motivato», facendo dunque comprendere come sia in capo al soggetto istante il compito di attivarsi presso il fornitore per ottenere l'accesso ai metadati, una volta autorizzato. Sempre nella direzione di meglio precisare la disciplina in oggetto, la legge di conversione ha introdotto al co. 3-*quater* anche un espresso riferimento – che prima era formulato in maniera poco chiara e solo rispetto alla disciplina urgente ed eccezionale di cui al co. 3 bis – alla inutilizzabilità dei dati acquisiti nel caso di violazione delle norme di cui agli art. 3 e 3 bis del d.l., prima analizzati.

In conclusione, dunque, anche la legge di conversione, così come il decreto-legge, presenta tanto aspetti positivi quanto criticità persistenti: nonostante alcune migliorie nella direzione di una più marcata precisione del dettato normativo siano indubbiamente state introdotte, l'incertezza relativamente alla disciplina transitoria e a taluni punti ancora potenzialmente problematici getta alcune ombre sull'intervento del Parlamento. Accanto a queste considerazioni, che solo l'evoluzione giurisprudenziale e l'applicazione concreta contribuiranno a chiarire, profilo certamente critico è da rilevarsi nella perdurante assenza, anche nella legge di conversione, di modifiche relative alla disciplina della conservazione dei metadati. Allontanandosi dai suggerimenti

[96] Questo specifico profilo del d.l. era già stato, invero, oggetto di critiche: l'impiego della disposizione "ai fini della prosecuzione delle indagini", infatti, era sin dall'inizio parsa una formula infelice, in quanto «sembrerebbe peccare di eccessiva specificità (..). È già stato sottolineato il rischio di un'interpretazione – invero priva di ogni ragionevole fondamento – volta a delimitare la facoltà di acquisizione dei metadati di traffico solo con riguardo alle attività svolte nel corso delle indagini preliminari e finalizzate all'apprensione di informazioni dirette a sostenere esclusivamente l'ipotesi accusatoria», A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici,* cit.

forniti dal Garante nel Parere sopra analizzato, nel quale veniva messa in evidenza l'importanza di provvedere ad una riforma della *data retention* in un senso maggiormente conforme al principio di proporzionalità promosso dalla giurisprudenza della CGUE, il Parlamento ha deciso di porre la propria attenzione unicamente sulla disciplina dell'acquisizione e dunque sull'impatto della sentenza *H.K. c. Prokuratuur* nel contesto nazionale. Ma le ancor più dirompenti pronunce dell'ottobre 2020, che hanno peraltro in maniera innovativa promosso una distinzione tra limiti della *data retention* a seconda che essa si proponga di perseguire scopi di sicurezza nazionale e pubblica, non avrebbero forse anch'esse dovuto stimolare un approfondito e serio dibattito sulla compatibilità della normativa italiana vigente rispetto al diritto dell'UE?

4. *The Ghost of data retention Future*: l'importanza di una seria riflessione sui possibili sviluppi normativi e giurisprudenziali, nazionali e sovranazionali

Il viaggio nel "passato" e nel "presente" della disciplina in materia di conservazione e acquisizione di metadati ha evidenziato molteplici spunti di riflessione che non possono che confluire in alcune considerazioni sulle possibili tappe future; anche questo sguardo alle ripercussioni che, tanto nel panorama interno quanto in quello sovranazionale, potranno caratterizzare la legislazione italiana risulta fondamentale per completare quel percorso di "consapevolizzazione" su di un tema così rilevante e che forse per troppo tempo è passato inosservato dai giudici e dal legislatore nostrani.

Il travagliato percorso evolutivo della normativa sopra analizzata fa certamente emergere la complessità delle questioni trattate e la difficoltà di individuare un chiaro punto di equilibrio tra esigenze securitarie e garanzia dei diritti fondamentali. Sotto tale profilo, si sono registrate oscillazioni in diverse direzioni, talvolta sospinte dalla volontà di fornire risposte decise e rapide dinnanzi a fenomeni emergenziali quali gli attentati terroristici, talaltra invece – ma più raramente – mosse da tensioni più spiccatamente garantiste derivanti dalla giurisprudenza sovranazionale. Dinnanzi a quella che da più parti è stata definita una disciplina «disarmonica»[97] rispetto ai principi

[97] F. GUELLA, *Data retentione circolazione dei livelli di tutela dei diritti in Europa: dai giudici di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE Online*, 2, 2017, p. 356.

sanciti nella lunga e articolata *data retention saga*, i disordinati e spesso confusi interventi normativi promossi sino al 2021 si erano rivelati infatti per la maggior parte derogatori di una disciplina ordinaria della *data retention* che è ormai divenuta recessiva di fronte a disposizioni eccezionali, producendo l'effetto di ribaltare il rapporto "regola generale-regola straordinaria", quantomeno sotto il profilo del regime della conservazione. Ciò che è andato a definirsi, insomma, è un «moto pendolare che, nell'era dei *big data* e della telefonia digitale, con le sempre più pervasive metodologie di investigazioni offerte dal progressivo sviluppo tecnologico-scientifico, è indicativo delle mutevoli sensibilità del decisore politico (nazionale) in punto di garanzie rispetto ai diritti inviolabili della persona incisi dai *data retention*»[98].

Con riferimento a tale "moto pendolare", una spinta decisa – anche se non sarà certamente l'ultima – in una direzione più marcatamente garantista è stata impressa dal più recente intervento riformatore: il Governo prima e il Parlamento poi hanno sicuramente mostrato, per la prima volta, la volontà di modificare l'assetto esistente al fine – peraltro espressamente dichiarato – di conformarsi alla giurisprudenza della CGUE e a quel più rigido principio di proporzionalità da essa stabilito.

Nonostante l'impegno in tal senso, come in parte già illustrato nel previo paragrafo, il risultato raggiunto ha lasciato forti perplessità e insoddisfazioni. Innanzitutto, il monito del Garante così come di gran parte della dottrina[99], avente ad oggetto la necessità di un serio e coerente intervento specificamente sulla materia della *data retention*, è rimasto inascoltato. Le ripercussioni, sotto questo specifico e rilevante profilo, potrebbero essere molteplici e ancora difficili da determinare: la giurisprudenza della CGUE vede ancora pendenti numerose pronunce nelle quali i giudici di Lussemburgo certamente avranno modo di ribadire il proprio approccio quanto alla incompatibilità di una forma di *bulk data retention* per scopi di sicurezza pubblica e repressione dei reati gravi, quale quella presente nel nostro Paese, riproponendo quel *vademecum* di limiti e requisiti specifici che debbono accompagnare l'eccezionale possibilità di impiegare tale strumento solo per esigenze di sicurezza nazionale. Bisognerà dunque osservare se, anche dinnanzi a tali ulteriori pronunce, le Corti italiane e il legislatore nostrano rimarranno nuovamente inerti e "sordi" – come dinnanzi alle pronunce *Privacy International* e *La Quadrature du Net* – o se invece le nuove decisioni adottate a

[98] Ufficio del Massimario della Suprema Corte di Cassazione, *Relazione su novità normativa*, cit., p. 3.

[99] Filippi su questo profilo ha espresso un giudizio estremamente chiaro, descrivendo come "biasimevole" la scelta – o l'imperizia – del Governo di lasciare la discussa durata della *data retention* intoccata (L. FILIPPI, *La nuova disciplina dei tabulati: il commento "a caldo" del Prof. Filippi*, cit.).

livello sovranazionale, in particolare nei rinvii tedesco, irlandese e bulgaro – tutti specificamente incentrati sulla fase della conservazione – offriranno l'occasione per un nuovo intervento riformatore.

Il dibattito legislativo che sta oggi ancora interessando le Istituzioni europee e gli Stati membri e che è volto a sostituire l'ormai risalente Direttiva *e-Privacy* con un nuovo Regolamento, potrebbe inoltre incidere sulle scelte normative e giurisprudenziali nazionali. Anche in tale sede, del resto, la discussione è estremamente vivace, caratterizzata dall'azione di taluni Governi finalizzata a limitare l'impatto dei requisiti stringenti e rigidi stabiliti dalla CGUE, proponendo l'inserimento di una più chiara determinazione dell'ambito di applicazione del diritto dell'UE in questo delicato ambito, che tocca anche materie quali appunto la garanzia della sicurezza nazionale, strettamente di pertinenza degli Stati membri[100]. Accanto alle scelte che Parlamento, Consiglio e Commissione europee adotteranno in sede legislativa, un ulteriore profilo che potrebbe, anche significativamente, influenzare la disciplina italiana attiene alle azioni future della Commissione: quest'ultima, infatti, come auspicato da numerosi attivisti per i diritti fondamentali e ONG, potrebbe attivare procedure di infrazione avverso quegli Stati che non hanno correttamente trasposto nell'ordinamento interno la facoltà sancita dall'art. 15 Direttiva *e-Privacy*, così come interpretato dalla costante giurisprudenza dei giudici di Lussemburgo. La previsione di una conservazione generalizzata ed indiscriminata, unitamente alla durata estremamente ampia della *data retention* disposta dal legislatore nostrano fanno certamente pensare che l'Italia potrebbe essere esposta ad una tale azione da parte della Commissione[101], nonostante i recenti interventi "correttivi" adottati dal normatore sul fronte della disciplina dell'acquisizione dei metadati.

[100] Con riferimento alla proposta di Regolamento *e-Privacy*, già richiamato *supra* e volta a sostituire l'ormai vetusta Direttiva *e-Privacy*, la versione approvata dal COREPER il 10 febbraio 2021 (doc. 6078/21) ha in ultimo stabilito, dopo una seria e complessa negoziazione e compromessi raggiunti dai rappresentanti degli Stati membri, che «the Regulation does not apply to activities which fall outside the scopo of Union law, and in any event measures, processing activities and operations concerning national security and defence, regardless who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority», art. 2, co. 2, lett. a); questa disposizione risulta in aperto contrasto con la lettura promossa dalla CGUE, la quale ha ampiamente chiarito come, indipendentemente dalla finalità di garanzia della sicurezza pubblica o nazionale perseguita, la disciplina della *data retention* e acquisizione di metadati rientri nell'ambito di applicazione del diritto dell'UE ogni volta che viene previsto un intervento – un trattamento – da parte di soggetti privati. La disposizione inserita è l'evidente frutto di quelle resistenze, di cui si è già parlato, manifestate dagli Stati membri avverso l'attuazione all'interno delle discipline nazionale dei criteri restrittivi e stringenti disposti dalla CGUE.

[101] L'appello di 40 ONG alla Commissione è volto proprio a spingere quest'ultima da un lato ad evitare qualsiasi futuro tentativo di reintrodurre a livello europeo un obbligo di conservazione dei metadati per scopi securitari, e dall'altro ad avviare «infringement procedures to ensure that national data retentionlaws are repealed in all member

Insomma, dinnanzi a queste possibili e molteplici spinte "garantiste" che potrebbero in futuro provenire dall'Unione europea, nella direzione di una più solida ed attenta tutela dei diritti fondamentali compressi dallo strumento della *data retention*, l'approccio legislativo e giurisprudenziale nel contesto nostrano è ancora difficile da prevedere. Senza dubbio si può però ipotizzare un duplice scenario: le innovative decisioni che le Istituzioni sovranazionali potrebbero adottare, sui diversi fronti ancora aperti e sopra delineati, potrebbero essere fonte di una rinnovata attenzione e di un più acceso dibattito sulla disciplina interna, così da promuovere, similmente a quanto accaduto a seguito della sola sentenza *H.K. c. Prokuratuur*, una più consapevole riforma della disciplina della conservazione, agendo dunque in maniera complessiva e omnicomprensiva sull'art. 132 Cod. Privacy nonché sul richiamo, da esso operato, alla disciplina straordinaria di cui all'art. 24 della L. 20 novembre 2017, n. 167. In questo ambito, anche le Corti nazionali potrebbero contribuire, abbandonando quell'approccio definito "rassicurante" manifestato – in parte – persino a seguito della sentenza della CGUE del marzo 2021, per promuovere invece decisioni che siano in grado di tenere maggiormente in considerazione la portata e le conseguenze anche dirompenti della giurisprudenza europea, spronando così il legislatore nazionale ad un intervento deciso. Ciò, del resto, è quanto si è registrato già in passato in altri ordinamenti, nei quali le pronunce dei giudici o l'attivismo del normatore hanno portato ad affrontare con maggiore attenzione la complessa questione della *data retention*, giungendo a riforme, tutele e garanzie che in Italia invece hanno faticato e tuttora faticano ad arrivare. Il secondo e diverso scenario che potrebbe venire a determinarsi dinnanzi ai progressi da registrarsi a livello sovranazionale potrebbe invece essere quello di un confermato immobilismo da parte di Governo e Parlamento nonché del riproporsi di decisioni delle Corti italiane caratterizzate, come accaduto in passato, dalla promozione di una lettura restrittiva – e talvolta poco puntuale – dei requisiti stabiliti dalla CGUE, tali da far salva la disciplina interna, non rilevando alcuna incompatibilità con il diritto dell'UE. Tale scenario, ovviamente, risulterebbe più difficile da realizzarsi laddove la Commissione promuovesse una procedura di infrazione o nel caso in cui il legislatore europeo giungesse ad una significativa modifica della normativa attuale, incorporando in essa l'interpretazione e il vaglio di proporzionalità promosso dai giudici di Lussemburgo.

states concerned»; la lettera è reperibile all'indirizzo https://www.statewatch.org/news/2020/october/joint-ngo-letter-no-data-retention-in-the-eu/.

Al momento pare arduo azzardare pronostici, visti tanto l'articolato contesto sovranazionale in continua evoluzione, quanto l'imprevedibilità delle reazioni di Parlamento, Governo e Corti italiane in materia, come già il più recente intervento normativo ha dimostrato nella scelta di non provvedere ad una riforma completa e sistematica dello strumento della *data retention*. Dinnanzi a tale approccio, lo studio attento e approfondito della giurisprudenza europea aiuta certamente a comprendere come non basti una più restrittiva e rigida disciplina relativa alla fase dell'acquisizione dei metadati per giustificare una conservazione ampia e generalizzata[102]: su questo profilo tanto le Corti quanto il legislatore italiano dovranno seriamente riflettere e anche da simili valutazioni dipenderà il futuro della disciplina nazionale.

Del tutto similmente, pare ancora presto per trarre un chiaro e netto bilancio della riforma recentemente introdotta quanto alla disciplina dell'acquisizione: se è innegabile che in questo ambito il Governo prima e il Parlamento poi[103] hanno «scelto la linea garantista»[104], pare altrettanto innegabile come la determinazione dei profili ancora dubbi e in parte oscuri assuma un rilievo determinante per stabilire la reale portata del decreto-legge e della relativa legge di conversione. Si pensi alle rilevate problematiche attinenti alla disciplina transitoria, il cui impatto sui procedimenti pendenti e la cui precisa interpretazione è ancora tutta da determinarsi nella concreta pratica attuativa; si considerino, ancora, le caratteristiche che l'autorizzazione richiesta al giudice dovrà possedere: quanto approfondite dovranno risultare le motivazioni del decreto emesso? E quanto il pubblico ministero o le parti richiedenti dovranno, a loro volta e anticipatamente, motivare la loro richiesta al giudice? Tale questione è tutt'altro che meramente tecnica o di secondaria importanza: dal livello di specificazione delle motivazioni, e dunque anche dalla solidità del nesso che si riuscirà a determinare tra necessità dell'acquisizione ed efficace svolgimento dell'attività investigativa, dipenderà la possibilità stessa di ricorrere in misura maggiore o minore allo strumento dell'accesso ai metadati. In altre parole, anche da questi profili attuativi di grande rilievo si determinerà la portata della "svolta garantista" promossa con la recente riforma: meno stringente e motivato sarà il vaglio operato dal giudice e meno effettive risulteranno le tutele predisposte dalla riforma

[102] Su tale profilo, del resto, le sentenze *La Quadrature du Net* e *Privacy International* non lasciano più alcuna ombra di dubbio.

[103] Sul punto merita però sottolineare come rispetto alla legge di conversione sia stata posta questione di fiducia, che ha dunque in certa misura limitato il dibattito parlamentare.

[104] L. FILIPPI, *La nuova disciplina dei tabulati*, cit.

normativa[105]. Vi sono inoltre profili riguardanti l'accesso ai metadati che non sono stati espressamente trattati dal legislatore: con riferimento ad esempio agli indirizzi IP e ai dati identificativi degli utenti non è prevista alcuna specificazione; sul punto invece la giurisprudenza della CGUE ha, in particolare in alcune sue ultime pronunce[106], proposto una lettura differenziata del principio di proporzionalità, vista la minore invasività rappresentata da tali peculiari dati e la loro limitata capacità di consentire la determinazione di abitudini, preferenze, relazioni sociali etc. degli utenti.

Insomma, carenze, critiche ed incertezze ancora caratterizzano la disciplina italiana, tanto sotto il profilo della conservazione quanto dell'acquisizione di metadati per scopi securitari. Trarre dunque conclusioni certe e nette quanto alla portata della recente riforma diviene un esercizio alquanto complesso: con riferimento al decreto-legge, vi è chi ha ritenuto che «un giudizio complessivamente negativo sarebbe davvero ingeneroso per un legislatore che, perlomeno stavolta, sembra aver preso davvero sul serio gli insegnamenti della Corte di giustizia in una tematica particolarmente delicata come quella in oggetto»[107]. Se per certi profili si concorda con tale lettura, considerando senz'altro positiva l'introduzione di disposizioni consigliate dal Garante per la Protezione dei Dati Personali[108], pare doversi però sottolineare come la scelta di "prendere sul serio" la giurisprudenza della CGUE si sia rivelata per certi versi "selettiva" – riguardando solo la disciplina della acquisizione dei metadati – e dunque non del tutto puntuale e debitamente

[105] Come ben rilevato da Battarino, la Corte di Cassazione nella sentenza 28 aprile 2014, n. 37212 ha stabilito come, ai fini dell'acquisizione di metadati, «l'obbligo di motivazione del provvedimento acquisitivo, stante il modesto livello di intrusione nella sfera di riservatezza delle persone, è soddisfatto anche con espressioni sintetiche, nelle quali si sottolinei la necessità dell'investigazione, in ragione al proseguimento delle indagini ovvero all'individuazione dei soggetti coinvolti nel reato», G. BATTARINO, *CGUE e dati relativi al traffico telefonico e telematico. Uno schema di lettura*, cit. Sulla base dei rilievi sopra esposti, bisognerà osservare l'approccio del giudice nella concreta attuazione della nuova normativa: se il mero richiamo ad espressioni sintetiche, come statuito in passato dalla Suprema Corte, sembra confliggere con i requisiti e il previo controllo indicato dalla giurisprudenza della CGUE, sarà necessario valutare in futuro come i giudici decideranno di muoversi dinnanzi alle richieste di accesso ai metadati e quanto attento e motivato sarà il vaglio da essi disposto.

[106] I giudici di Lussemburgo hanno affermato, nella più recente giurisprudenza, come una normativa nazionale che prevede la conservazione generalizzata di indirizzi IP non possa considerarsi, in linea di principio, contraria all'art. 15 Direttiva *e-Privacy* purché questa possibilità sia limitata alla sola lotta verso forme gravi di criminalità, abbia una durata limitata e sia oggetto di rigorose garanzie. Quanto ai dati identificativi, essi risultano in una ingerenza solo lieve nella sfera privata tale da non richiedere che normative nazionali disciplinanti la loro conservazione siano limitate al rispetto dei criteri stabiliti nella pronuncia *Tele2*.

[107] Così A. MALACARNE, *La decretazione d'urgenza del Governo in materia di tabulati telefonici*, cit.

[108] Le garanzie disposte al comma 3-ter erano infatti assenti nella primissima versione del decreto e sono state introdotte sulla base dei rilievi mossi dal Garante nel Parere sullo schema di decreto-legge, già sopra ampiamente richiamato.

approfondita. Un primo segnale verso una maggiore attenzione al bilanciamento tra esigenze securitarie e diritti fondamentali è indubbiamente ravvisabile nell'intervento del Governo prima e del Parlamento poi; un più vasto e completo dibattito su tale materia e sul puntuale contenuto ed effetto della *data retention saga* è però rimasto, sino ad ora, altrettanto indubbiamente assente.

Gli insegnamenti e i moniti che sono emersi durante le tappe qui percorse, nella disciplina del passato, nelle evoluzioni del presente e negli scorci di un possibile futuro, non possono lasciare indifferenti: come il vecchio Scrooge, a seguito degli incontri rivelatori con i tre Spiriti del Natale, si fa protagonista di un "risveglio" morale, così il legislatore e le Corti nostrane non possono guardare alle vicende che hanno contraddistinto e che tuttora contraddistinguono la disciplina della *data retention* e dell'acquisizione dei metadati, tanto dentro quanto fuori dai confini nazionali, senza operare un qualche ravvedimento. Quest'ultimo dovrebbe essere al più presto promosso affinché le riforme normative promosse si rivelino capaci di assumere un carattere realmente sistematico e completo, così da evitare il rischio di incorrere nuovamente negli errori di un passato segnato da interventi emergenziali urgenti e incapaci di cogliere la complessità e delicatezza della disciplina nel suo insieme.

Uno sguardo ampio e consapevole degli effetti prodotti da sistemi investigativi altamente invasivi rispetto alla garanzia di diritti fondamentali diviene, nel delineato contesto, questione di fondamentale rilievo al fine di scongiurare gli insidiosi pericoli di una società della sorveglianza[109], nella quale cioè la pur centrale esigenza di garantire la sicurezza finisce col comprimere, financo a disconoscere, la salvaguardia dei diritti fondamentali. In questo senso sono utili e potenti le parole dell'Avvocato generale Campos-Sanchez Bordona nelle Conclusioni alla Causa *La Quadrature du Net*: la tutela della sicurezza «non deve essere impostata solo pensando alla sua efficacia. Da ciò deriva la sua difficolta, ma anche la sua grandezza quando i suoi mezzi e metodi rispettano i requisiti dello Stato di diritto, che significa anzitutto assoggettamento del potere e della forza ai limiti del diritto e, in particolare, a un ordinamento giuridico che trova nella difesa dei diritti

[109] Del resto Rodotà, già nel 2004, affermava con lucida incisività come la privacy – e dunque la tutela della sfera privata da ingerenze esterne illegittime e sproporzionate – rappresenti «uno strumento necessario per difendere la società della libertà e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale», S. RODOTÀ, *Privacy, libertà, dignità*, 2004, disponibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293. E l'insidia di una tale società deve essere riconosciuta come sempre più preponderante e minacciosa: non a caso Bauman utilizza l'immagine della liquidità per trasmettere l'idea di una società pervasa ormai da forme di sorveglianza dilaganti, mutevoli e dall'architettura flessibile (Z. BAUMAN, D. LYON, *Liquid surveillance. A conversation*, Polity Press, 2013).

fondamentali la ragione e il fine della sua esistenza. (..) Se si abbandonasse semplicemente alla mera efficacia, lo Stato di diritto perderebbe la qualità che lo contraddistingue e potrebbe diventare esso stesso, in casi estremi, una minaccia per il cittadino. Nulla potrebbe assicurare che, dotando il potere pubblico di strumenti esorbitanti per il perseguimento dei reati, mediante i quali esso potesse ignorare o svuotare di contenuto i diritti fondamentali, la sua azione incontrollata e totalmente libera non si risolverebbe in definitiva in un pregiudizio alla libertà di tutti»[110]. La disciplina della *data retention* e dell'acquisizione di metadati risulta essere, alla luce di tali parole, una chiara esemplificazione di tali insidie, rivelando l'importanza di stabilire tutele e limiti che, allontanandosi da un semplicistico e più comodo approccio di *trade-off*, sappiano individuare un punto di equilibrio tra spinte differenti.

Leggendo dunque la questione della *data retention* entro questo più ampio e delicato contesto, il legislatore e le Corti italiane debbono ora imboccare una strada differente rispetto a quella sin qui percorsa; una strada certamente ardua ma quantomai necessaria che, evitando le derive pro-securitarie, forti delle potenzialità che l'innovazione tecnologica presenta, sia in grado di dirigersi verso una rinnovata, approfondita ed attenta riflessione sulla proporzionalità dell'invasione e compressione dei diritti fondamentali e sui nuovi, più chiari, precisi e stringenti requisiti e salvaguardie che debbono essere a tali pericoli opposti. Perché, per usare, le parole di Dickens, che ci ha accompagnato in questo percorso, «Il cammino degli uomini preannuncia determinate conclusioni alle quali esso, se vi si persevera, conduce. Ma se da quel cammino ci si allontana, la meta finale muterà»[111].

[110] Para. 129-135. Per usare le parole di un altro Avvocato generale, Saugmandsgaard Oe, nelle Conclusioni al caso *Tele2*, se i sistemi di conservazione dei metadati consentono al governo di controllare i governati, risulta tuttavia di fondamentale rilievo obbligare il governo a controllare sé stesso. Nel richiamare la nota citazione di James Madison «if angels were to govern men, neither external nor internal controls on government would be necessary», nella quale peraltro riecheggia il quesito di Giovenale *"Quis custodiet ipsos custodes?"*, l'Avvocato generale riconosce che spetta a Corti e legislatori definire un «punto di equilibrio tra l'obbligo incombente agli Stati membri di garantire la sicurezza delle persone che si trovano sul loro territorio e il rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati di carattere personali sanciti dagli artt. 7 e 8 della CDFUE», para. 5.

[111] C. DICKENS, *Il Canto di Natale*, Feltrinelli, traduzione di B. Amato, IV Ed., 2019, p. 107.