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

di Giulia Formici

Title: The end of the data retention saga? The last ECJ decisions on the data retention regime for security purposes, between confirmations and innovations

Keywords: Data Retention; Fundamental Rights; Security.

1. – Le attese e complesse pronunce della Corte di giustizia dell'UE del 6 ottobre 2020 – la *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e a.*, C-623/17 e la *La Quadrature du Net e a. c. Premier Ministre e a.* e *Ordre des barreaux francophones et germanophone e a. c. Conseil des Ministres*, cause riunite C-511/18, C-512/18 e C-520/18 –, aventi entrambe ad oggetto questioni riguardanti la disciplina della conservazione (c.d. *data retention*) ed accesso ai metadati per finalità di prevenzione e repressione di minacce alla sicurezza, rappresentano una significativa tappa di quella articolata *data retention saga* che ancora oggi fatica a trovare un epilogo. Se da un lato, infatti, le più recenti decisioni dei giudici di Lussemburgo hanno certamente il merito di aver chiarito taluni interrogativi e dubbi emersi dalla previa giurisprudenza, dall'altro il destino della conservazione dei metadati nell'UE continua a risultare ancora incerto, essendo legato agli esiti di ulteriori rinvii pregiudiziali in materia, al momento pendenti, e alle reazioni delle Istituzioni europee, nonché dei legislatori e delle Corti nazionali.

Al fine di giungere ad una analisi delle riconferme e degli aspetti innovativi affermati dai giudici di Lussemburgo e ad una riflessione sui possibili scenari futuri, si vuole innanzitutto tratteggiare sinteticamente il contesto nel quale le pronunce oggetto della presente disamina si inseriscono: esse infatti vertono tutte sull'interpretazione del discusso art. 15 Direttiva 2002/58 (c.d. Direttiva *e-Privacy*) che, merita ricordarlo, risulta essere ad oggi l'unica disposizione normativa stabilita a livello sovranazionale in materia di *data retention*. Prevedendo una eccezione alla regola generale della cancellazione o anonimizzazione dei metadati derivanti da servizi di telecomunicazione, l'art. 15 garantisce agli Stati membri la possibilità di adottare, per scopi di salvaguardia della sicurezza nazionale nonché di prevenzione, ricerca, accertamento e perseguimento di reati, normative nazionali volte ad obbligare i *service providers* alla conservazione, per un periodo di tempo limitato, delle informazioni raccolte nello svolgimento dei propri servizi. La vaghezza del dettato normativo e il richiamo agli ampi requisiti di 'necessità', 'opportunità' e 'proporzionalità all'interno di una società democratica', hanno determinato, sin dalle prime attuazioni di tale disposizione, significative difformità interpretative da parte degli Stati membri, venendosi così ben presto a creare nel contesto europeo un frammentario quadro di discipline in materia di *data retention*. Dalle criticità che

il disomogeneo panorama normativo aveva comportato – anche per gli operatori di telecomunicazioni, vincolati ad una moltitudine di differenti obblighi di conservazione –, nonché sulla spinta della tragica ondata di attentati che avevano scosso Londra e Madrid, è stata approvata la Direttiva 2006/24, che imponeva a ciascuno Stato membro di dotarsi di normative sulla conservazione dei metadati, fissando peraltro una forbice temporale di *retention* dai 6 mesi ai 2 anni (per una analisi della Direttiva, E. Kosta, P. Valcke, *Retaining the Data Retention Directive*, in *Comp Law & Sec Rep* 22, 2006; F. Bignami, *Privacy and law enforcement in the EU: the Data Retention Directive*, in 8 *Chicago Journal of International Law* 1, 2007, 233 ss). Come noto, il destino di questa Direttiva è stato segnato dall'intervento della CGUE, che con la storica sentenza *Digital Right Ireland Ltd c. Minister for Communications e a.* e *Kärntner Landesregierung e a.* (cause riunite C-293/12 e C-594/12, 8 aprile 2014, d'ora in avanti sentenza *DRI*), ha invalidato la disciplina europea. Consentendo una conservazione generalizzata, ovvero riguardante tutti i mezzi di comunicazione elettronica, tutti i dati da essi prodotti e tutti gli utenti (c.d. *bulk data retention*), la Direttiva comportava infatti una ingerenza nei diritti alla riservatezza e alla protezione dei dati (artt. 7 e 8 Carta di Nizza) non limitata a quanto strettamente necessario (tra i tanti commenti A. Vedaschi, *I programmi di sorveglianza di massa nello Stato di diritto. La 'data retention' al test di legittimità*, in *Dir pubbl comp eur*, 2014, 1224 ss; M. Granger, K. Irion, *The Court of Justice and the Data retention Directive in Digital Rights Ireland*, in 39 *Eu Law Rev* 4, 2014, 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; M. Cole, F. Boehm, *EU Data Retention: finally abolished? Eight years in light of Art. 8*, in 97 *Critical Quarterly for Leg and Law* 1, 2014, 58 ss; S. Crespi, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Riv It di Dir Pub Com* 3-4, 2015, 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 28 *Harvard Human Rights J*, 2015, 66 ss). Fallito tale tentativo di armonizzazione della disciplina della *data retention* per scopi securitari, gli Stati membri – restii a rinunciare alle potenzialità dello strumento della conservazione generalizzata e quindi alla possibilità di poter 'andare indietro nel tempo' (I. Cameron, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in 54 *Common Mkt L Rev* 1, 2017, 1467 ss) e disporre di informazioni utili per creare collegamenti con persone altrimenti sconosciute alle autorità di *law enforcement* – sono tornati ad adottare o hanno mantenuto, sulla base dell'art. 15 Direttiva *e-Privacy* (e nonostante i principi emersi dalla sentenza *DRI*), regimi di *bulk data retention* (sul punto A. Arena, *La Corte di Giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento*, in *Quad Cost* 3, 2014; F. Boehm, M. Cole, *Data retention after the Judgment of the Court of Justice of the EU*, The Greens in the EP Working Paper, 2014; F. Iovene, *Data retention tra passato e futuro. Ma quale presente?*, in *Cass Pen* 12, 2014; S. Heitzer, J. Kulhing, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24*, in *Eur Law Rev* 2, 2015, 263 ss). Queste normative hanno fatto emergere profondi timori nella società civile, sempre più consapevole, anche grazie alle note rivelazioni di Snowden (A. Butler, F. Hidvegi, *From Snowden to Schrems: how the surveillance debate has impacted US-EU relations and the future of international data protection*, in *Seton Hall J of Diplomacy and International Relations*, Special Issue 2015/2016; A. Dimitrova, M. Brkan, *Balancing national security and data protection: the role of EU and US policy-makers and Courts before and after the NSA affair*, in 56 *J of Comm Mkt Studies* 4, 2918, 751 ss), della pervasiva ingerenza nella sfera privata rappresentata dalla predisposizione di un obbligo diffuso di conservazione dei metadati, capace di consentire, come peraltro affermato dai giudici di Lussemburgo, una profilazione degli utenti, delle loro preferenze, frequentazioni e abitudini.

Così i dubbi quanto alla legittimità e conformità al diritto dell'UE di tali strumenti, seppur finalizzati alla garanzia della sicurezza, sono sfociati in numerosi casi giurisprudenziali, giunti dinnanzi alla CGUE, prima nel già richiamato rinvio *Tele2 Sverige AB c. Post-och telestyrelsen* e *Secretary of State for the Home Department c. Tom Watson e a.* (cause riunite C-203/15 e C-698/15, 21 dicembre 2016) e successivamente nel caso *Ministerio Fiscal* (C-207/16, 2 ottobre 2018). In entrambe queste decisioni i giudici di Lussemburgo si sono confrontati con l'interpretazione dell'art. 15, riconoscendo la mancata proporzionalità di una forma di *bulk data retention* e identificando in una conservazione targettizzata (per aree geografiche, gruppi sociali o periodi di tempo) l'unica forma legittima di *data retention*; la CGUE si è poi spinta, con un approccio che può definirsi para-legislativo, a delineare un vero e proprio *vademecum* di criteri che i legislatori nazionali sono chiamati a rispettare nella predisposizione di un obbligo di conservazione dei metadati, quali la determinazione di norme chiare e precise in grado di fissare requisiti e garanzie in grado di scongiurare rischi di abusi, la sussistenza di un criterio oggettivo capace di mettere in relazione l'ingerenza nella sfera privata e la minaccia alla sicurezza, o ancora la necessaria gravità del reato (Eurojust, *Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15*, 2017; F. Guella, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina EU al giudizio della Corte di giustizia rivolto alle discipline nazionali*, in *DPCE Online* 2, 2017, 349 ss; O. Pollicino, M. Bassini, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Dir Pen Contemp*, 9 gennaio 2017; E. Spiller, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, in *IANUS* 15, 2017; sulla sentenza *Ministerio Fiscal*, sia consentito anche il richiamo a G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia* Ministerio Fiscal, in *Osservatorio AIC* 3, 2018, 453 ss). Ebbene, è proprio nel confuso e complesso scenario apertosi a seguito di queste pronunce che si inseriscono i rinvii pregiudiziali promossi dal *Conseil d'État* francese, dalla *Cour Constitutionnelle* belga e dal *Investigatory Powers Tribunal* (IPT) del Regno Unito, dai quali le sentenze del 6 ottobre 2020 hanno origine. A seguito della sentenza *Tele2*, infatti, i legislatori e i governi nonché le stesse Corti nazionali hanno manifestato serie perplessità e difficoltà nella predisposizione di normative in materia di *data retention* in grado di essere, al contempo, conformi ai c.d. 'criteri *Tele2*' stabiliti dalla CGUE ed efficaci strumenti di garanzia della sicurezza, soprattutto in un contesto di "emergenza normalizzata" (tra i molti, G. de Vergottini, *La 'guerra' contro un nemico indeterminato*, in *Forum di Quaderni Costituzionali*, 5 ottobre 2001; M. Rosenfeld, *Judicial balancing in times of stress: comparing diverse approaches to the war of terror*, in *Benjamin N. Cardozo School of Law Working Paper*, 119, 2005; S. Gambino, A. Scerbo, *Diritti fondamentali ed emergenza nel costituzionalismo contemporaneo. Un'analisi comparata*, in *Dir Pubb Com Eur*, 4, 2009, 99 ss; T. Groppi, *Democrazia e terrorismo*, Napoli, 2009; A. Cardone, *La "normalizzazione" dell'emergenza*, Torino, 2011; L. Scaffardi, *Nuove tecnologie, prevenzione del crimine e privacy, alla ricerca di un difficile bilanciamento*, in A. Torre (a cura di), Costituzioni e sicurezza dello Stato, Rimini, 2013, 425 ss; G. De Minico, *Costituzione. Emergenza e terrorismo*, Napoli, 2016; G. de Vergottini, *Una rilettura del concetto di sicurezza nell'era digitale e della 'emergenza normalizzata'*, in *Rivista AIC*, 4, 2019). Mentre alcuni Stati membri, come l'Italia, non si sono attivati per modificare la normativa nazionale in materia di *data retention* ed integrare i principi e le limitazioni previste dalla giurisprudenza europea (R. Flor, *Data retention e art. 132 Cod. Privacy: vexata quaestio(?)*, in *Dir Pen Contemp*, 3, 2017), in altri Paesi invece il dibattito sulla legittimità della disciplina della conservazione dei metadati per scopi securitari ha assunto toni ben più accesi, portando all'intervento dei giudici nazionali e, in seguito, della CGUE, nuovamente chiamata a chiarire molti dei punti

DPCE online
ISSN: 2037-6677

rimasti irrisolti e oscuri, nel perdurante ed assordante silenzio del legislatore europeo. Quest'ultimo, non avendo avviato un dibattito sulla adozione di una nuova normativa *ad hoc* in materia di *data retention* a seguito della invalidazione della Direttiva 2006/24, ha *de facto* lasciato ai giudici il delicato compito di determinare un punto di equilibrio tra esigenze securitarie e tutela di quei diritti alla riservatezza e alla protezione dei dati sempre più riconosciuti quali fondamentali prerogative dell'Unione dei diritti (L. Curricciati, *Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della Data Retention Directive*, in *Democrazia e Sicurezza* 2, 2017; G. Caggiano, *Il bilianciamento 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, 64 ss). Così i giudici belga, francese ed inglese, nei rinvii oggetto di analisi hanno richiesto alla CGUE di chiarire, temperare o addirittura riconsiderare vari aspetti della sua giurisprudenza in materia di conservazione dei metadati, giungendo quasi ad 'ammonire' i giudici di Lussemburgo circa le conseguenze, anche drammatiche e profonde, che una rigida ed integrale attuazione dei criteri delineati nella previa giurisprudenza può comportare sulla concreta capacità degli Stati membri di garantire la sicurezza nazionale e pubblica (in questo senso si pone, con grande chiarezza ed evidenza, il IPT). Ecco allora che le risposte fornite dalla CGUE nelle sentenze che ci si appresta ad analizzare risultano di estrema delicatezza e rappresentano uno sviluppo fortemente atteso e dai dirompenti effetti nella complessa *data retention saga.*

2. – Procedendo con l'analisi delle sentenze, che devono necessariamente essere lette congiuntamente, è possibile ricondurre i molteplici profili trattati dalla CGUE a quattro argomenti principali: la determinazione dell'ambito di applicazione della Direttiva *e-Privacy*; la compatibilità con il diritto dell'UE di una conservazione generalizzata ed indiscriminata per scopi di sicurezza nazionale o di sicurezza pubblica; la determinazione sia delle categorie di dati che debbono sottostare al rispetto dei 'criteri *Tele2*' sia dei limiti all'accesso ai dati conservati; la possibilità di modulare nel tempo gli effetti di una dichiarazione di illegittimità di una normativa nazionale in materia di *data retention.*

Seguendo l'ordine logico argomentativo adottato dai giudici, la prima questione – trattata con più precisione nella pronuncia *Privacy International*, per essere poi ripresa nella sentenza complementare *La Quadrature du Net* – assume un valore tutt'altro che formale: la definizione dell'ambito di applicazione della Direttiva 2002/58 rappresenta, infatti, sin dalla decisione *Tele2*, un profilo estremamente dibattuto e oggetto di un acceso scontro tra la CGUE e gli Stati membri. Questi ultimi hanno con forza sostenuto come la Direttiva richiamata, e dunque i limiti da essa stabiliti, non possano applicarsi a normative, quali quelle oggetto dei rinvii in esame, finalizzate alla salvaguardia della sicurezza nazionale. Tale posizione trova fondamento nel richiamo all'eccezione prevista all'art. 1, co. 3 della Direttiva *e-Privacy*: tra le "attività dello Stato nei settori del diritto penale, della difesa, della sicurezza dello Stato" che tale disposizione esclude dall'ambito di applicazione della Direttiva stessa, non possono che rientrare necessariamente anche quelle che prevedono un obbligo di conservazione in capo ai *service providers* per scopi di sicurezza nazionale. È proprio questa specifica finalità a rafforzare la posizione dei governi intervenuti, che hanno peraltro ampiamente richiamato l'art. 4, co. 2 TUE che attribuisce appunto agli Stati membri competenza esclusiva in materia di sicurezza nazionale, per questo sottratta all'ambito di applicazione del diritto dell'UE e al vaglio della CGUE. Ciò, come ribadito anche dal IPT nel rinvio *Privacy International*, consente agli Stati membri l'adozione di normative disciplinanti la conservazione dei metadati non vincolate ai rigidi 'criteri *Tele2*',

laddove finalizzate alla tutela della sicurezza nazionale. Contrariamente a tali posizioni e seguendo quanto affermato dall'Avvocato generale Campos Sanchez-Bordona nelle sue Conclusioni del 15 gennaio 2020, nonché ribadendo la posizione già chiaramente espressa nella sentenza *Tele2* e nella successiva *Ministerio Fiscal*, , i giudici di Lussemburgo respingono però una lettura della Direttiva *e-Privacy* – nonché dello stesso TUE – che porti alla esclusione di una normativa nazionale dall'ambito di applicazione del diritto dell'UE per il semplice richiamo a scopi di tutela della sicurezza nazionale; in particolare, le "attività dello Stato" cui l'art. 1, co. 3 della Direttiva *e-Privacy* fa riferimento comprendono unicamente le "attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati" (par. 92, C-511/18). Per tale ragione non risultano attinenti ad "attività dello Stato" quelle normative nazionali adottate in deroga all'obbligo generale di cancellazione dei metadati che disciplinano l'attività di fornitori di servizi di telecomunicazione, imponendo loro una forma di conservazione o trasmissione dei dati. A nulla vale neppure il richiamo, operato dai Governi intervenuti, alla risalente sentenza *Parlamento c. Consiglio e Commissione* (C-317/04, 30 maggio 2006): in quel caso ad essere rilevante era la Direttiva 95/46, che escludeva dal proprio ambito di applicazione i trattamenti di dati aventi ad oggetto la pubblica sicurezza, la difesa e la sicurezza dello Stato, senza operare alcuna distinzione sulla base del soggetto chiamato a porre in essere tali azioni (art. 3, co. 2). Al contrario, l'espresso riferimento, nell'art. 1, co. 3 della Direttiva *e-Privacy*, alle "attività dello Stato" e dunque allo specifico soggetto che svolge il trattamento, rappresenta l'elemento distintivo fondamentale che consente di negare qualsiasi parallelismo con le argomentazioni svolte nella sentenza del 2006. Con questo ragionamento, quindi, la CGUE conferma come una normativa nazionale che imponga ai fornitori di servizi di telecomunicazione una forma di conservazione dei metadati, anche per finalità di sicurezza nazionale, debba considerarsi rientrante nell'ambito di applicazione del diritto dell'UE, mentre ne risultano escluse le attività svolte unicamente ed autonomamente da autorità pubbliche, senza che venga cioè richiesta alcuna collaborazione di soggetti privati.

3. – Chiarito così il primo e complesso punto, i giudici di Lussemburgo si dedicano più ampiamente all'interpretazione dell'art. 15 Direttiva *e-Privacy* e alla possibilità di imporre, sulla base di tale disposizione, forme di conservazione generalizzata ed indiscriminata di metadati. La CGUE ribadisce inizialmente sia il carattere eccezionale della *data retention*, che non può costituire la regola e che anzi deve essere limitata all'elenco tassativo di finalità indicate all'art. 15, sia l'ingerenza nella sfera privata rappresentata dalla sola conservazione, indipendentemente dall'eventuale successivo accesso. Dopo aver significativamente ripercorso quanto già affermato sin dalla sentenza *DRI*, i giudici si dedicano ad un ampio e dettagliato vaglio di proporzionalità; ed è proprio sotto questo profilo che emerge la prima e forse più rilevante novità delle pronunce in esame. Viene infatti per la prima volta stabilita una distinzione tra finalità di sicurezza nazionale e quelle di salvaguardia della sicurezza pubblica e lotta alla criminalità, accogliendo in parte le forti richieste degli Stati membri e delle autorità di *law enforcement* che avevano ribadito più volte e in maniera decisa l'importanza dello strumento della conservazione generalizzata ed indiscriminata per la garanzia della sicurezza nazionale. Così facendo i giudici di Lussemburgo prevedono una 'eccezione', pur circostanziata, alla dichiarata incompatibilità della *bulk data retention* con la Carta di Nizza e il diritto dell'UE.

Definendo la salvaguardia della sicurezza nazionale come "l'interesse primario di tutelare le funzioni essenziali dello Stato e gli interessi fondamentali della società e comprende la prevenzione e la repressione di attività tali da destabilizzare gravemente le strutture costituzionali, politiche, economiche o sociali fondamentali di un paese e in particolare da minacciare direttamente la società, la

DPCE online
ISSN: 2037-6677

popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo" (par. 135, C-511/18), la CGUE afferma, in maniera del tutto innovativa, la superiorità di tale obiettivo rispetto a quello di lotta alla criminalità grave e di tutela della sicurezza pubblica in generale. Questa attribuzione di un maggiore peso alla garanzia della sicurezza nazionale si sostanzia in un'ulteriore fondamentale considerazione: se le minacce per la sicurezza nazionale risultano essere maggiormente pericolose ed insidiose rispetto a quelle per la sicurezza pubblica, esse debbono consentire l'adozione di ingerenze ancor più profonde nella vita privata e nel diritto alla protezione dei dati. Ne deriva quindi che l'art. 15 Direttiva *e-Privacy* non osta, in linea di principio, alla adozione di normative nazionali che impongano una conservazione generalizzata ed indiscriminata dei dati relativi al traffico e all'ubicazione, purché siano rispettate specifiche condizioni, individuate dai giudici stessi sia nella sussistenza di circostanze sufficientemente concrete tali da far ritenere che lo Stato membro affronti una minaccia grave per la sicurezza nazionale che si riveli reale e attuale o prevedibile, sia in una restrizione temporale della *bulk data retention*, la cui durata deve dunque essere limitata allo stretto necessario, pur potendo essere soggetta a rinnovo in caso di persistenza della minaccia. La conservazione generalizzata, inoltre, non deve assumere carattere sistematico e deve risultare accompagnata tanto da garanzie rigorose in grado di proteggere i dati dal rischio di abusi, quanto da un controllo effettivo svolto da un giudice o da un organo amministrativo indipendente "la cui decisione sia dotata di efficacia vincolante, diretto ad accertare la sussistenza di una delle suddette situazioni nonché il rispetto delle condizioni e della garanzie che devono essere previste" (par. 139, C-511/18). Qualora tali condizioni siano rispettate, può essere superato quel restrittivo requisito, affermato sin dalla sentenza *DRI*, che richiede la sussistenza di un nesso, anche indiretto, tra la conservazione dei metadati e una minaccia per la sicurezza: l'esistenza stessa di un pericolo per la sicurezza nazionale è ritenuta di per sé idonea a stabilire tale collegamento.

Se, sulla base di queste considerazioni, la CGUE giunge ad ammettere la proporzionalità e dunque la compatibilità con la Carta di Nizza di una forma di *bulk data retention*, purché sia in gioco la tutela della sicurezza dello Stato e siano rispettati particolari limiti, il divieto di tale tipologia di conservazione 'estensiva' viene invece ribadito con riferimento all'obiettivo di prevenzione, ricerca e perseguimento di reati gravi. Sotto questo profilo i giudici di Lussemburgo ribadiscono quanto già espresso nella previa giurisprudenza: in particolare, le normative nazionali alla base dei rinvii in esame impongono una forma di *data retention* che coinvolge sistematicamente tutti gli utenti di servizi di telecomunicazione in maniera globale, senza che i soggetti i cui dati sono conservati si trovino, anche solo indirettamente, in una posizione che possa dar luogo ad indagini penali o senza che sia possibile ritenere sussistente un nesso con una minaccia alla sicurezza pubblica; poiché non risultano circoscritte ad uno specifico periodo di tempo, ad un'area geografica determinata o ad una individuata cerchia di soggetti, tali discipline nazionali non possono essere considerate limitate allo stretto necessario e giustificate in una società democratica. Ne deriva una riconferma della conservazione targettizzata (*targeted* o *ciblée*) quale unica forma di *data retention* compatibile con il diritto dell'UE laddove ad essere garantita sia la sicurezza pubblica. Non vengono pertanto accolte dalla CGUE quelle numerose critiche riguardanti i limiti e i seri rischi derivanti da una conservazione targettizzata, mosse tanto dalle autorità nazionali di *law enforcement* quanto da ONG e dal Garante europeo per la protezione dei dati (GEPD). Facendo proprie tali rimostranze, l'Avvocato generale, nelle sue Conclusioni, aveva al contrario sottolineato come una tale tipologia di *data retention* aprisse a possibili forme di discriminazione a carico di soggetti residenti in una determinata area o appartenenti a specifici gruppi sociali (ad esempio sulla base della religione o della razza), tanto

ISSN: 2037-6677

da poter risultare nell'instaurazione di un regime di sospetto generalizzato su alcuni segmenti della popolazione e in una pericolosa stigmatizzazione; allo stesso tempo una conservazione targettizzata si rivelava potenzialmente inefficace, sussistendo una forte contraddizione tra il carattere preventivo della conservazione mirata e il fatto che non sia possibile, nella gran parte dei casi, conoscere in anticipo luoghi, autori e momento di commissione di un reato (par. 88). È proprio sulla base di queste valutazioni che l'Avvocato generale aveva peraltro proposto una 'terza via' tra la forma di conservazione *mirata* e quella *generalizzata*, individuata nella c.d. conservazione *limitata* (*restricted* o *limitée*), prospettata da Europol e ribadita dal Consiglio nell'ambito del rinnovato dibattito sulla adozione di una normativa europea *ad hoc* in materia di *data retention*, di cui si dirà in seguito. Questa ulteriore tipologia intermedia si fonda su una limitazione della conservazione solo a specifiche categorie di dati, oggettivamente necessarie per la salvaguardia della sicurezza, nonché a determinati tipi di fornitori e di servizi, individuati sulla base di una connessione tra *retention* e obiettivo da raggiungere: risultando più ampia rispetto alla conservazione mirata, ma più ristretta di quella generalizzata, la *restricted data retention* consentirebbe ad esempio di escludere dall'obbligo di conservazione piccoli fornitori di servizi o ancora dati di soggetti le cui attività sono coperte da segreto professionale. Questa proposta alternativa, tuttavia, non è stata accolta, come si è detto, dalla CGUE che, riconfermando la *targeted data retention*, non ha neppure svolto alcun riferimento o considerazione in merito alla ulteriore opzione di conservazione, pur da più parti prospettata.

4. – Sebbene il profilo di maggior interesse e novità delle pronunce in esame sia certamente da ravvisarsi nella distinzione, sopra analizzata, dell'esito del vaglio di proporzionalità a seconda della finalità perseguita dalla conservazione, si vogliono sinteticamente richiamare ulteriori profili di rilievo affrontati dalla CGUE. Concentrando l'attenzione sulla disciplina dell'accesso, accanto alla riconferma dei criteri e requisiti già individuati nella previa giurisprudenza i giudici di Lussemburgo hanno svolto, in particolar modo nella sentenza *Privacy International*, una considerazione importante: la disciplina del Regno Unito – da cui il rinvio traeva origine – stabiliva l'obbligo in capo ai fornitori di servizi di telecomunicazione di trasmettere i metadati in maniera generalizzata ed indiscriminata alle agenzie di sicurezza e di *intelligence* nazionali, le quali poi raccoglievano e conservavano le informazioni in apposite banche dati finalizzate allo svolgimento di trattamenti ed analisi di massa automatizzati. In tale contesto la CGUE statuisce l'equivalenza tra accesso e trasmissione, così che "una normativa che consente una trasmissione generalizzata e indifferenziata dei dati alle autorità pubbliche implica un accesso generale" (par. 80, C-623/17): una tale forma di accesso, anche qualora si sostanzi in analisi meramente automatizzate o sia finalizzata alla salvaguardia della sicurezza nazionale, risulta svolgersi in assenza non solo di un qualsiasi nesso, indiretto o remoto, con l'obiettivo perseguito, ma anche di criteri oggettivi e condizioni sostanziali e procedurali che disciplinino l'utilizzo delle informazioni così ottenute: ne deriva che un simile accesso generalizzato non può essere considerato limitato a quanto strettamente necessario. Se questa equivalenza 'trasmissione-accesso' rappresenta una precisazione importante e dagli attesi effetti dirompenti sulle discipline nazionali, soprattutto quelle regolanti l'attività di autorità di intelligence, un ulteriore profilo di maggiore chiarezza e specificazione rispetto alla previa giurisprudenza emerge con riferimento a due particolari categorie di dati: gli indirizzi IP e i dati relativi all'identità civile degli utenti. A parere dei giudici di Lussemburgo, infatti, queste informazioni presentano un grado di sensibilità inferiore rispetto agli altri dati di traffico e di ubicazione, poiché non consentono di ricostruire, da soli, abitudini o relazioni sociali degli utenti. Sulla base di tali considerazioni dunque, una normativa

nazionale che prevede la conservazione generalizzata di indirizzi IP non risulta, in linea di principio, contraria all'art. 15 Direttiva *e-Privacy* purché questa possibilità sia limitata alla sola lotta avverso forme gravi di criminalità, abbia una durata limitata e sia oggetto di rigorose garanzie; quanto ai dati relativi all'identità, conformemente a quanto già affermato nella sentenza *Ministerio Fiscal*, essi risultano in una ingerenza nella sfera privata non grave e non richiedono pertanto che le normative nazionali disciplinanti la loro conservazione siano limitate al rispetto dei *'criteri Tele2'*, ben potendosi così prevedere per tali informazioni una *bulk data retention* anche finalizzata alla repressione di reati non gravi.

L'ultimo profilo di grande interesse che si vuole qui evidenziare è da rilevarsi nella posizione espressa dalla CGUE circa la questione posta dalla *Cour Constitutionnelle*, relativa alla possibilità di limitare nel tempo gli effetti di una dichiarazione di illegittimità di una normativa in materia di *data retention* (par. 213). Tale interrogativo è estremamente delicato: nella maggior parte dei casi, infatti, i dati conservati rappresentano informazioni o elementi di prova di grande rilievo nei processi penali, tanto che l'illegittimità della normativa sulla conservazione dei metadati potrebbe compromettere gravemente procedimenti penali di estrema importanza per la sicurezza pubblica. Divergendo, anche sotto tale profilo, da quanto affermato dall'Avvocato generale, la CGUE stabilisce che il giudice nazionale non può limitare nel tempo gli effetti di una dichiarazione di illegittimità delle normative nazionali in materia di *data retention* in contrasto con il diritto dell'UE poiché ciò implicherebbe la persistenza dell'obbligo di conservazione in capo ai fornitori di servizi e dunque il protrarsi di ingerenze gravi nei diritti fondamentali degli utenti (par. 219, C-511/18). I giudici di Lussemburgo precisano nondimeno che la determinazione dell'ammissibilità di informazioni ed elementi di prova ottenuti mediante una conservazione contraria al diritto dell'UE spetta unicamente al diritto nazionale, pur stabilendo che il giudice nazionale, dinnanzi ad un procedimento penale basato su prove ottenute in violazione della Direttiva *e-Privacy*, non potrà tenere conto di queste informazioni qualora i sospettati non siano in grado di "dedurre efficacemente in merito a un mezzo di prova che rientra in un settore che esula dalla competenza del giudice e che è fondamentale per la ricostruzione dei fatti" (par. 226, C-511/18). Su tale punto, la CGUE non considera affatto quegli elementi che invece l'Avvocato generale aveva mostrato di tenere fortemente in conto, quali le difficoltà riscontrate da tanti legislatori nazionali nell'adeguare le proprie normative ai requisiti indicati dalla giurisprudenza europea, l'impegno mostrato da taluni Stati membri di operare nella direzione di un adeguamento il più possibile completo ai *'criteri Tele2'*, nonché gli effetti estremamente pregiudizievoli che potrebbero prodursi sulla effettiva tutela della sicurezza pubblica e dello Stato in caso di annullamento o disapplicazione immediata di una normativa sulla *data retention* adottata ex art. 15 Direttiva *e-Privacy*.

5. – L'analisi svolta nei precedenti paragrafi impone un tentativo di sintesi conclusiva che tragga un bilancio finale della posizione espressa dai giudici di Lussemburgo. Effettuare una tale operazione risulta tuttavia esercizio quanto mai complesso: da un lato, infatti, attingendo ampiamente alla propria giurisprudenza, la CGUE consolida alcuni principi e criteri già propri della previa *data retention saga* e maggiormente orientati verso una ampia tutela dei diritti fondamentali alla privacy e alla protezione dei dati. D'altro lato, non possono essere ignorati i rilevanti profili di novità che aprono le porte ad alcune significative 'deroghe' al divieto generale di conservazione generalizzata ed indiscriminata per scopi securitari, con riferimento al delicato ambito della sicurezza nazionale. Identificare nell'orientamento della CGUE una prevalenza netta degli interessi alla sicurezza o

ISSN: 2037-6677

della tutela dei diritti fondamentali non pare del tutto possibile: non stupisce, quindi, che le prime reazioni, tanto delle ONG e dei promotori dai quali i rinvii hanno tratto origine, quanto degli Stati membri e delle autorità di *law enforcement*, siano state estremamente caute e timide (la ONG Statewatch ha significativamente titolato il suo commento alle sentenze in esame "*a victory and a defeat for privacy*").

Con la decisione di ribadire il divieto di *bulk data retention* per scopi di sicurezza pubblica e di riportare sotto l''ombrello' del diritto dell'UE – e dunque delle garanzie offerte dalla Carta di Nizza e dal vaglio della Corte stessa – anche i regimi di conservazione e di trasmissione dei metadati volti alla tutela della sicurezza nazionale, la CGUE fuga gli ultimi dubbi e le critiche mosse in precedenza da molti Stati membri e da talune Corti nazionali, ampliando in maniera chiara e limpida i confini di tutela dei diritti fondamentali dinnanzi alle esigenze securitarie. Anche la conferma, quale unica forma proporzionata di ingerenza nella sfera privata, dello strumento della *targeted data retention* per finalità di garanzia della sicurezza pubblica si pone nella stessa direzione di un rafforzamento di quell'orientamento 'dato-centrico' che negli ultimi decenni ha trasformato sempre più l'UE in una 'fortress of digital privacy' (L.P. Vanoni, *Balancing privacy and national security in the global digital era: a comparative perspective of the EU and US constitutional systems*, in *Forum Quad. Cost.*, 14 giugno 2017; F. Fabbrini, *The EU Charter of Fundamental Rights and the rights to data privacy: the EU Court of Justice as a Human Rights Court*, in S. de Vries e al. (a cura di), *The EU Charter of Fundamental Rights as a binding instrument: five years old and growing*, Londra, 2015, 261 ss). Non accogliendo la proposta di una forma intermedia di conservazione dei dati, maggiormente invasiva rispetto alla *targeted retention* ma al contempo più efficace nella lotta alla criminalità e maggiormente realizzabile in concreto, la CGUE sembra non considerare quelle difficoltà pratiche e quei limiti evidenziati anche da quei legislatori nazionali che più hanno cercato di adeguare le proprie normative ai principi delineati nella *data retention saga* (il Belgio, ad esempio, sulla cui legislazione in materia si legga F. Coudert, F. Verbruggen, *Conservation des données de communications électronique en Belgique: un juste équilibre?*, in V. Franssen, D. Flore (a cura di), *Societé numerique et droit penal*, Bruxelles, 2019, 245 ss; C. de Terwangne, E. Degrave (a cura di), *La protection des données à caractère personnel en Belgique: manuel de base*, Bruxelles, 2019). La posizione della Corte sin qui delineata, nel rifiutare l'approccio sotto taluni profili più 'compromissorio' promosso dall'Avvocato generale, nega così l'introduzione di quegli aggiustamenti e rimodulazioni – soprattutto sotto il profilo della conservazione targettizzata – invocate da governi nazionali, legislatori, autorità di *law enforcement* e persino, per certi versi, dal GEPD: tale orientamento non mancherà certo di destare perplessità e dibattiti vivaci dinnanzi ad una espansione dell'ambito di applicazione del diritto dell'UE che, pur avendo il pregio di ampliare le garanzie previste dalla Carta di Nizza, rischia di mettere significativamente in ombra quelle che dovrebbero essere competenze esclusive degli Stati membri (estremamente critico sul punto, sin dalla sentenza *Tele2*, D. Fennnelly, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018).

Se quanto esaminato sino ad ora potrebbe far propendere per l'affermazione di una netta vittoria della privacy e protezione dei dati, ad indirizzare invece l'ago della bilancia verso una preminenza delle esigenze securitarie sono le posizioni, più innovative, assunte dai giudici di Lussemburgo con riferimento a talune importanti questioni: innanzitutto la chiara ammissione della possibilità di utilizzare una conservazione generalizzata ed indiscriminata per scopi di sicurezza nazionale, ma anche i minori limiti previsti quanto all'impiego di indirizzi IP e di dati identificativi di un utente. In tutti questi punti la CGUE allenta le rigide maglie sopra richiamate, anche se sarebbe eccessivo e fuorviante rinvenire in tale posizione un deciso passo indietro rispetto alle tutele stabilite nelle previe pronunce: da un lato, ad esempio,

DPCE online
ISSN: 2037-6677

la bassa ingerenza nella sfera privata rappresentata dai meri dati identificativi dell'utente era già stata riconosciuta nel caso *Ministerio Fiscal* e dall'altro l''apertura' ad una forma di *bulk data retention* per scopi di sicurezza nazionale viene nondimeno accompagnata da precisazioni circa i limiti e le condizioni entro cui tale eccezione può estrinsecarsi. Questa apertura, che pure non giunge, ad avviso di chi scrive, a ribaltare totalmente l'approccio della giurisprudenza precedente (benché non siano mancate letture in senso opposto quale quella di M. ZALNIERIUTE, *The future of data retention regimes and national security in the EU after the Quadrature du Net and Privacy International judgments*, in *Insights* 28, 2020), è stata oggetto di preoccupazioni espresse dalle ONG che hanno visto in questa concessione maggiormente pro-securitaria una possibile fonte di abusi da parte delle pubbliche autorità: la terminologia impiegata riguardo alle determinazione delle condizioni che possono giustificare l'uso della *bulk data retention* si presenta infatti sotto taluni aspetti piuttosto vaga e dai contorni ampi, lasciando una certa discrezionalità agli Stati membri (P. VOGIATZOGLOU, J. BERGHOLM, *Privacy International and La Quadrature du Net: the latest on data retention in the name of national and public security*, in *CITIP Law Blog*, 27 ottobre 2020). Viene rimessa in capo ai legislatori e ai Governi nazionali l'individuazione delle circostanze "concrete" che rappresentano una "minaccia grave, reale, attuale o prevedibile" per la sicurezza nazionale, nonché delle tutele da apprestare (ad esempio i poteri e le informazioni che verranno fornite a giudici o autorità indipendenti per garantire un controllo effettivo ed efficace dell'impiego di tale strumento, o ancora la definizione dei casi in cui si renda possibile rinnovare l'obbligo di conservazione generalizzata). Sarà sulla base dell'ampiezza delle condizioni previste e dell'impiego più o meno frequente e precisamente regolamentato di tale disciplina eccezionale che si giocherà la partita fondamentale del futuro della *data retention* per scopi di sicurezza nazionale. Con riferimento a questi aspetti, comunque, la posizione dei giudici di Lussemburgo sembra orientarsi più verso una 'vittoria' per la sicurezza, peraltro avvicinandosi all'approccio maggiormente 'permissivo' e flessibile adottato della Corte EDU nei casi *Centrum for Rattvisa* e *Big Brother Watch* (*Centrum For Rattvisa c. Sweden*, n. 35252/08, 19 giugno 2018; *Big Brother Watch e a. c. UK*, n. 58170/13, 13 settembre 2018; sulla giurisprudenza della Corte EDU in materia: F. Dubuisson, *La Cour européenne des droits de l'homme et la surveillance de masse*, in *Revue Trimestrelle des droits de l'homme* 108, 2016, 887 ss; P. Vogiatzoglou, *Centrum for Rattvisa v. Sweden: bulk interception communications by Intelligence Services in Sweden does not violate the right to privacy*, in 4 *Eur Data Prot Law Rev* 4, 2018, 563 ss; G. Tiberi, *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?*, in *Quad Cost* 4, 2018, 391 ss; sia concesso anche il rinvio a G. Formici, *La* digital mass surveillance *al vaglio della Corte Europea dei Diritti dell'Uomo: da* Zakharov *a* Big Brother Watch, in *Federalismi.it – Focus Human Rights* 23, 2020, 44 ss). In queste più recenti pronunce, che pure sono ora sottoposte all'ulteriore vaglio della Grande Camera e che, piuttosto sorprendentemente, non vengono mai citate dalla CGUE, i giudici di Strasburgo hanno ammesso forme di conservazione generalizzata dei dati per scopi securitari, restringendo l'elenco delle salvaguardie necessarie ed imprescindibili che debbono essere offerte nel caso di sorveglianza massiva. In questo senso, la dichiarata conformità al diritto dell'UE della *bulk data retention* per finalità di sicurezza nazionale porta ad una convergenza verso l'orientamento della Corte EDU, mentre le due Corti sembrano ancora divergere quanto ai limiti e alla garanzie che debbono accompagnare sistemi di conservazione generalizzata: sotto questi ultimi profili, i giudici di Lussemburgo paiono porre condizioni più stringenti di proporzionalità e stretta necessità, salvo le attese decisioni della Grande Camera della Corte EDU non portino nel prossimo futuro ad una inversione di tendenza da parte dei giudici di Strasburgo su questi complessi e delicati aspetti.

6. – In conclusione, le posizioni qui ricostruite, che rendono particolarmente difficile addivenire ad un bilancio chiaro e netto della giurisprudenza della CGUE, delineano un panorama ancora incerto e che non consente di considerare la *data retention saga* definitivamente chiusa e chiarita. I tanti scenari ancora in attesa di definizione impongono di osservare con attenzione, nel prossimo futuro, le reazioni e le concrete ricadute delle esaminate pronunce, con riferimento soprattutto a tre grandi protagonisti, da individuarsi nei giudici di Lussemburgo, nel legislatore europeo e negli Stati membri.

Per quanto attiene la CGUE, bisogna ricordare che dinnanzi a quest'ultima sono ancora pendenti tre rinvii pregiudiziali in materia di della *data retention* e della sua compatibilità con il diritto dell'UE: si tratta del rinvio della Corte suprema estone *H. K. c. Prokuratuur* (C-746/18, rispetto al quale sono state depositate le Conclusioni dell'Avvocato generale Pitruzzella il 21 gennaio 2020) e dei rinvii *SpaceNet AG c. Repubblica federale di Germania* C-793/19 e *G.D. c. Commissioner of the Garda Siochana e al.* C-140/20. Sebbene l'esito finale di taluni dei quesiti posti nei rinvii risulti in parte piuttosto prevedibile alla luce delle sentenze del 6 ottobre 2020, nondimeno i giudici avranno l'opportunità di chiarire ulteriormente, confermare ed arricchire quanto già emerso sino ad ora (in questo senso, particolare attenzione merita senza dubbio il rinvio estone, incentrato sulla disciplina dell'accesso e sui criteri per la determinazione del carattere di indipendenza dell'autorità di controllo).

Passando al secondo dei soggetti le cui reazioni assumono carattere determinante per la definizione della *data retention* nell'UE, merita sottolineare come il Consiglio dell'UE, nel documento *Conclusioni sulla conservazione dei dati per finalità di lotta contro la criminalità* (n. 9336/19) del 27 maggio 2019 abbia affidato alla Commissione il compito di procedere a consultazioni e studi approfonditi sulla opportunità di avviare una iniziativa legislativa *ad hoc* in materia di conservazione dei metadati. In quella occasione, il Consiglio ha invitato la Commissione a valutare i concetti di conservazione generale, mirata e limitata nonché ad esaminare in che misura l'effetto cumulativo di forti garanzie e limitazioni all'accesso ai dati conservati possa contribuire ad attenuare l'impatto complessivo della *data retention* sulla protezione dei diritti fondamentali (par. 2). Così facendo, il Consiglio ha suggerito di tenere in considerazione sia quella nuova forma di *restricted data retention*, promossa dal dibattito sorto in seno ad Europol, sia quel possibile contemperamento tra le salvaguardie disposte all'accesso e quelle previste nel campo della mera conservazione. Entrambe tali alternative sembrano doversi ora ritenere scartate e respinte alla luce delle pronunce esaminate: i giudici di Lussemburgo hanno fortemente avversato il ragionamento che vede nella predisposizione di un accesso più limitato la precondizione di una conservazione più ampia, oltre a riconoscere quale unica forma di conservazione legittima quella di tipo targettizzato. Di conseguenza, sebbene molti autori abbiano individuato proprio in un intervento del legislatore sovranazionale l'unica soluzione definitiva alle criticità derivanti dal panorama frammentario e confuso che caratterizza le normative degli Stati membri (L. Lupária, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giur Pen*, 4, 2019, 753 ss), la predisposizione di una proposta legislativa *ad hoc* in materia di conservazione dei dati pare ora rappresentare una sfida ancora più complessa, che impone una ponderazione molto attenta da parte della Commissione tra efficacia dello strumento e tutela dei diritti fondamentali. Nel frattempo, un altro fronte sul quale le sentenze analizzate sembrano avere già sortito effetto è quello della proposta di Regolamento *e-Privacy*, volto ad abrogare e sostituire l'ormai vetusta Direttiva *e-Privacy*: tale iniziativa ha incontrato proprio nella adozione di specifiche misure in materia di *data retention* un terreno di scontro e di acceso dibattito, rispetto al quale è parso sin da subito difficile trovare una soluzione condivisa tra spinte differenti.

DPCE online
ISSN: 2037-6677

Così, l'ultima versione della proposta di Regolamento, approvata dal COREPER il 10 febbraio 2021 (n.6087/21) e frutto di sostanziali e complessi compromessi tra differenti visioni degli Stati membri in seno al Consiglio, prevede all'art. 7, co. 4 e al Considerando 26 una generica possibilità per gli Stati membri di adottare normative che, in deroga al divieto generale di memorizzazione, prevedano, per le ampie finalità securitarie indicate, una conservazione dei metadati proporzionata e limitata a quanto necessario in una società democratica, disponendo inoltre all'art. 2, co. 2, lett. a) l'esclusione dall'ambito di applicazione del Regolamento di trattamenti di dati svolti per finalità di sicurezza nazionale. Qualora il Regolamento venisse approvato nella sua versione attuale, dunque, potrebbero emergere significative problematiche quanto alla conformità di tali disposizione rispetto alla lettura offerta dalla CGUE nella *data retention saga*. Alla luce di tali considerazioni, si può ben affermare come la perdurante assenza di armonizzazione delle normative nazionali e l'inerzia del legislatore dell'UE, che preferisce attendere le pronunce della CGUE per comprendere come affrontare la sfida complessa del bilanciamento tra istanze securitarie e tutela dei diritti fondamentali, finiscano con l'acuire le incertezze sul futuro della *data retention* nell'UE, lasciando in gran parte anche alle reazioni degli Stati membri la determinazione di tale delicato e fondamentale equilibrio.

Proprio sotto quest'ultimo profilo, la giurisprudenza della CGUE avrà sicuramente una forte ricaduta, a livello nazionale, sulle scelte normative e sulle decisioni delle Corti, spingendo a reazioni che, con grande probabilità, saranno differenti a seconda dello Stato membro, riconfermando quella già critica disomogeneità che ha caratterizzato il contesto dell'UE sino ad oggi. Come a seguito della sentenza *Tele2*, tutto dipenderà dall'approccio dei singoli legislatori e delle Corti e, conseguentemente, anche dalla società civile che deve attivarsi al fine di portare all'attenzione delle istituzioni questioni legate alla disciplina della *data retention*.

Nell'inerzia di governi e Parlamenti, i giudici degli Stati membri potrebbero svolgere una funzione di estremo rilievo qualora chiamati a vagliare la legittimità del regime nazionale in essere, assumendo così un ruolo di sprone e di impulso all'instaurazione di un dibattito normativo sul tema, come avvenuto in Belgio (L. Naudts, *Belgian Constitutional Court nullifies Belgian Data Retention* Law, in *3 Eur Data Prot Law Rev* 3, 2015, 208 ss; C. Forget, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, in *Journal des Tribunaux*, 13, 2017). In altri casi, governo e legislatore potrebbero invece aprire spontaneamente o sulla spinta della società civile, un processo di riflessione e modifica della disciplina esistente, similmente a quanto verificatosi negli ultimi anni nel Regno Unito (E. Kosta, *SSHD v. Watson and Others: a thin nail on the coffin of UK data retention legislation*, in *Eur Law Rev* 2, 2015, 520 ss; P. De Hert, V. Papakonstantinou, *The rich UK contribution to the field of EU data protection*, in *33 Comp Law and Sec Rev* 3, 2017, 354 ss; W. Mbioh, *Post-Och Teledtyrelsen Watson and the IPA 2016*, in *3 Eur Data Prot Law Rev* 2, 2017, 273 ss; L. Woods, *IPT: Privacy International v. Secretary of State*, in *3 Eur Data Prot Law Rev* 2, 2017, 247 ss). Indipendentemente dalle vicende e dai soggetti che conducono ad un intervento riformatore, pare comunque chiaro come le soluzioni normative adottabili siano, a seguito delle ultime pronunce della CGUE, ben più limitate rispetto al passato, essendo ora definitivi sia il divieto di conservazione generalizzata quale mezzo di repressione e prevenzioni di crimini gravi, sia la conferma della *targeted data retention* come unico strumento compatibile con il diritto dell'UE. Nonostante, e anzi, proprio alla luce di queste posizioni, si potrebbero riproporre quelle notevoli e serie difficoltà che già in passato i legislatori nazionali avevano riscontrato nell'approvare normative in grado di soddisfare sia le esigenze di salvaguardia della sicurezza, sia la necessità di garantire una tutela dei diritti fondamentali in linea con quanto affermato dalla CGUE. Le problematiche

incontrate nel passato, quindi, potrebbero nuovamente presentarsi anche nelle scelte future, richiedendo ai legislatori nazionali uno sforzo considerevole, soprattutto nel perdurante silenzio del legislatore europeo.

Se tale interventismo e dinamismo, pur con tutte le criticità e i dubbi applicativi sopra delineati, possono senza dubbio contribuire a quel virtuoso percorso evolutivo che già ha condotto taluni Stati membri verso una più ampia tutela dei diritti fondamentali nella disciplina della *data retention* (A. Munir, S. Yasin, *Data retention rules: a dead end*, in *3 Eur Data Prot Law Rev*, 1, 71 ss; E. Celeste, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *15 Eur Const Law Rev*, 1, 2019, 134 ss), un ulteriore scenario resta comunque possibile: quello della inazione. L'esempio dell'Italia è in tal senso il più calzante: nonostante l'avvicendarsi delle pronunce della CGUE, né il legislatore né le Corti nazionali hanno negli ultimi decenni avviato una seria ed approfondita discussione in materia di *data retention*, neppure dinnanzi ad un obbligo di conservazione generalizzata di 72 mesi che rappresenta un *unicum* (tutt'altro che positivo) nel panorama europeo e che ha destato non poche e peraltro lampanti perplessità nella dottrina (P. Caputo, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale* 1, 2016; F. Ruggieri, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cass Pen* 6, 2017; L. Scaffardi, *La data retention va in ascensore*, in *Forum di Quad Cost*, 28 luglio 2017; L. Scudiero, *Data retention a sei anni. La CGUE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR*, in *MediaLaws* 1, 2017; G. M. Baccari, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. Cadoppi, S. Canestrari, A. Manna, M. Papa (a cura di), *Cybercrime*, Milano, 2019, 1599 ss; I. Rezende, *Dati esteriori alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention*, in *Sistema Penale 5*, 2020). Se neppure dinnanzi alle più recenti e maggiormente chiare decisioni della CGUE venisse promosso alcun intervento sul fronte legislativo o su quello giurisprudenziale – ad esempio mediante rinvio alla Corte costituzionale o alla CGUE –, nulla cambierebbe nel contesto nazionale. Questo rappresenterebbe un significativo problema, non solo per una efficace garanzia dei diritti fondamentali nel territorio europeo, ma anche per la disomogeneità di discipline cui i fornitori di servizi di telecomunicazione dovrebbero far fronte. Dinnanzi ad una tale situazione, la Commissione europea potrebbe giocare un ruolo di rilievo laddove decidesse di intervenire con procedure di infrazione, cui Stati membri come l'Italia risulterebbero particolarmente esposti.

Saranno quindi le reazioni di tutti gli attori nazionali ed europei indicati, con un evidente intreccio e reciproca influenza, a determinare il concreto portato della giurisprudenza della CGUE in questa sede analizzata.

7. – Da tutte le considerazioni sin qui mosse, può affermarsi come, senza dubbio, le sentenze *Privacy International* e *La Quadrature du Net* abbiano il merito di aver risposto a molti quesiti rimasti a lungo aperti a seguito della sentenza *Tele2*. La direzione largamente confermata dalla CGUE resta quella di un rafforzamento della tutela dei diritti fondamentali anche di fronte ad esigenze securitarie. Nel non vietare *tout court* qualsiasi forma di conservazione dei metadati e ammettendo la proporzionalità di una *bulk data retention* per scopi di sicurezza nazionale, i giudici di Lussemburgo dimostrano però di voler prendere le distanze da una lettura in termini di *trade-off* degli elementi del binomio 'sicurezza-diritti fondamentali', che vede cioè nella garanzia dell'uno una inevitabile rinuncia dell'altro (D. Solove, *Nothing to hide. The false trade-off between privacy and security*, New Haven, 2011; M.G. Porcedda, *The recrudescence of 'security v. privacy' after 2015 terrorist attacks and the value of privacy rights in the EU*, in E. Orrù, M.G. Porcedda, S. Weydner-Volkmann (a cura di), *Rethinking surveillance and control: beyond the 'security v. privacy'*

DPCE online
ISSN: 2037-6677

debate, Baden-Baden, 2017, 137 ss; D. Broeders, *Quis custodiet ipsos custodes: security, big data and secrecy*, in 3 *Eur Data Prot Law Review* 3, 2017, 306 ss; M. Orofino, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws* 2, 2018, 82 ss). Nonostante la direzione del cammino risulti sempre più definita, la difficile sfida della *data retention* non può al momento dirsi completamente risolta e un rapido superamento delle attuali criticità e della frammentarietà di soluzioni nazionali sembra da escludersi.

I rinvii ancora pendenti, le risposte attese dal legislatore europeo e le reazioni degli Stati membri delineeranno nei prossimi anni il futuro della *data retention* nell'UE: se le pronunce analizzate hanno stabilito e confermato alcuni capisaldi, saranno ora gli approcci tenuti dagli attori nazionali e sovranazionali a determinare una concreta assonanza con i principi delineati dalla giurisprudenza della CGUE o una rinnovata e continua distonia di scelte e di orientamenti, che potrebbe esacerbare i toni di un dibattito e di un dialogo già a tratti articolato e aspro. La sfida di proporre una soluzione univoca e realizzabile in materia di conservazione dei metadati, capace di scongiurare il rischio di cedere sia alla tentazione di una garanzia della sicurezza "oltre ogni limite", sia ad una anacronistica tutela dei diritti fondamentali incapace di fare i conti con ineludibili ed importanti esigenze di sicurezza, è quindi destinata ad impegnare ancora a lungo Corti e legislatori nazionali, nonché le Istituzioni dell'UE.

Giulia Formici
Dip.to di Giurisprudenza
Università degli Studi di Parma
giulia.formici@unipr.it