COMITATO EDITORIALE EDIZIONE 2021

GRUPPO DI COORDINAMENTO EDIZIONE 2021

QUADERNI DI SIDIBLOG

SEZIONE III
Diritto delle migrazioni

SEZIONE IV
Cooperazione giudiziaria europea in materia penale

SEZIONE V
Dati e mercato digitale dell'Unione europea

SEZIONE VI
Le sanzioni oggi. Legalità, efficacia e implicazioni sistemiche nel diritto internazionale e dell'Unione europea

SEZIONE VII
Adattamento del diritto internazionale al diritto interno

SEZIONE VIII
L'attualità del pensiero giuridico di Antonio Cassese

SEZIONE IX
Cinema e diritto internazionale

La sentenza *H.K. c. Prokuratuur* e il difficile dialogo tra CGUE e Stati membri in materia di conservazione e accesso ai metadati per finalità securitarie: spunti di riflessione su una questione vecchia ma ancora irrisolta

GIULIA FORMICI*

SOMMARIO: 1. La *data retention* nella giurisprudenza della CGUE: storia, sviluppi e persistenti criticità. – 2. I requisiti della gravità del reato e del previo controllo di un'autorità giudiziaria o amministrativa indipendente: il significativo portato della sentenza *H.K. c. Prokuratuur*. – 3. Le reazioni alla sentenza *H.K. c. Prokuratuur* tra resistenze ed evoluzioni normative e giurisprudenziali: l'incerto futuro della disciplina della *data retention* e dell'accesso ai metadati.

ABSTRACT: A partire dal 2006 la regolamentazione della conservazione dei dati di traffico e ubicazione derivanti da telecomunicazioni è stata oggetto di numerosi e complessi interventi dei giudici di Lussemburgo. Nelle sue storiche pronunce e nelle sue più recenti pronunce, la CGUE ha stabilito l'incompatibilità con il diritto dell'UE di forme di conservazione generalizzata ed indiscriminata per scopi di sicurezza pubblica, lasciando una possibilità di impiego di tale invasivo strumento solo in casi eccezionali di minacce concrete e reali alla sicurezza nazionale, prevedendo al contempo restrittive condizioni di accesso ai dati stessi. I dubbi interpretativi legati a tali posizioni, unitamente alle forti tensioni venutesi a creare negli Stati membri – restii a rinunciare o limitare la possibilità di accedere ad un'enorme mole di dati utili per prevenire e reprimere crimini gravi –, hanno dato vita ad un vivace dibattito non solo in seno a legislatori e corti nazionali bensì anche dinnanzi alle Istituzioni europee. Mediante l'analisi della sentenza *H.K. c. Prokuratuur*, il presente contributo intende riflettere sui possibili sviluppi della disciplina della *data retention* e del connesso accesso ai metadati, osservando il bilanciamento tra esigenze securitarie e tutela dei diritti fondamentali – in particolare quelli alla vita privata e alla protezione dei dati – nell'articolato intreccio tra livelli e nel dialogo tra attori nazionali e sovranazionali coinvolti.

PAROLE CHIAVE: *data retention* – protezione dei dati – sicurezza nazionale – reati gravi – accesso ai metadati – CGUE.

* Giulia Formici, Ricercatrice RTD/A in Diritto pubblico comparato, Università degli Studi di Milano, giulia.formici@unimi.it.

1. La *data retention* nella giurisprudenza della CGUE: storia, sviluppi e persistenti criticità

La sentenza della Corte di giustizia dell'Unione europea (CGUE) del 2 marzo 2021, C-746/18, *H.K. c. Prokuratuur* si inserisce in una lunga serie di rilevanti e complesse pronunce in materia di conservazione dei metadati per scopi securitari – c.d. *data retention*, per mutuare la sintetica quanto chiara terminologia inglese –. Tale pratica consiste essenzialmente nell'obbligo imposto ai fornitori di servizi di telecomunicazione di conservare – *retain*, appunto – i metadati prodotti dai propri utenti al fine di consentire un successivo ed eventuale accesso a tali informazioni da parte di autorità di *law enforcement* o di *intelligence* nell'ambito di azioni di prevenzione, indagine e lotta contro minacce alla sicurezza pubblica o nazionale. Pur non riguardando il contenuto della comunicazione, i metadati – ovvero i dati di traffico indicanti ora, durata, destinatario e frequenza delle chiamate, o di ubicazione e localizzazione dell'apparecchio utilizzato, nonché gli indirizzi IP o i dati relativi all'identità dell'utente[1] – sono in grado di svelare relazioni, abitudini e luoghi frequentati, consentendo quindi di trarre conclusioni precise sulla vita degli utenti[2]. L'enorme mole di metadati quotidianamente prodotta e conservata rappresenta, dunque, da un lato, una fonte preziosa di informazioni per creare collegamenti tra soggetti, anche ignoti alle forze dell'ordine, e delineare utili piste investigative; dall'altro lato, costituisce uno strumento capace di porre in essere una profonda invasione nella sfera privata, rischiando così di inverarsi in una forma pervasiva di sorveglianza massiva[3].

[1] Tali dati sono altrimenti denominati "dati di traffico" o "dati esterni delle telecomunicazioni" e ricomprendono anche i "dati di ubicazione". Sul punto, si legga, *ex multis*, 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*, 2018, p. 65 ss.

[2] Per usare le parole della CGUE, «Questi dati [metadati], presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati», CGUE, sentenza dell'8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications e al.*, para. 27.

[3] Più approfonditamente sulle potenzialità e i rischi di tali strumenti investigativi, I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 2017, p. 1428 ss.; M. ANDREJEVIC, *Surveillance in the big data era. Emerging pervasive information and communications technologies*, in *Law, Governance and Technology Series*, 2014, p. 55 ss.

La complessa sfida della determinazione di un corretto equilibrio tra tutela dei diritti fondamentali e garanzia della sicurezza pubblica e nazionale, in un periodo di c.d. emergenza normalizzata[4], trova così nella conservazione dei metadati derivanti da telecomunicazioni uno dei più insidiosi terreni di scontro, sul quale la CGUE risulta ormai impegnata da quasi un decennio.

A partire dalla nota e dirompente sentenza *Digital Rights Ireland c. Minister for Communications e a.*[5], con la quale è stata invalidata la Direttiva 2006/24/CE (c.d. *Data retention Directive*)[6] per violazione dei diritti di cui agli artt. 7 e 8 della Carta dei diritti fondamentali dell'Unione europea (CDFUE), i giudici di Lussemburgo si sono ulteriormente pronunciati su tale delicata materia in altre sei decisioni[7], tutte aventi ad oggetto l'interpretazione dell'art. 15 della Direttiva 2002/58/CE (c.d. Direttiva *e-Privacy*)[8], che rappresenta, ad oggi, l'unica fonte normativa sovranazionale disciplinante la conservazione di metadati relativi alle telecomunicazioni per finalità securitarie. Questa disposizione, estremamente vaga nel proprio dettato, consente agli Stati membri di derogare alla regola generale che impone la cancellazione dei metadati, stabilendo un obbligo di conservazione in capo agli operatori privati per un periodo limitato di tempo e unicamente a scopo di salvaguardia della sicurezza nazionale, difesa, sicurezza pubblica, prevenzione e perseguimento dei reati[9].

[4] G. DE VERGOTTINI, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Bologna, 2004; E. POSNER, A. VERMEULEN, *Terror in balance: security, liberty and the Courts*, Cambridge-Massachusetts, 2007.

[5] CGUE, sentenza dell'8 aprile 2014, C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications e al.*

[6] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

[7] Tale ricca giurisprudenza verrà ampiamente richiamata ed esaminata nel presente contributo.

[8] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche).

[9] L'art. 15 stabilisce che «Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli artt. 5 e 6, all'art. 8, para. Da 1 a 4, e all'art. 9 della presente direttiva [attinenti essenzialmente alla regola generale che impone la cancellazione dei metadati conservati per scopi commerciali e di erogazione della fornitura del servizio] qualora tale restrizione costituisca (..) una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo». Come si può immediatamente notare dal testo riportato, in esso non è presente alcun riferimento o limitazione alla lotta alla criminalità qualifi-

Nelle successive storiche pronunce *Tele2* e *Ministerio Fiscal*[10] la CGUE ha stabilito che forme di conservazione di tipo generalizzato ed indiscriminato, riguardanti cioè tutti gli utenti, tutti i mezzi di comunicazione e tutte le tipologie di metadati – c.d. *bulk data retention* –, qualora impiegate per finalità di garanzia della sicurezza pubblica, non superano il test di proporzionalità: una conservazione di tale estensione, che attiene alla quasi totalità della popolazione europea e che non si fonda sulla sussistenza di una connessione, anche solo indiretta, tra l'ingerenza nella sfera privata e un reato grave, non può infatti essere considerata limitata allo stretto necessario. L'unica forma di *data retention* compatibile con il diritto dell'UE è stata individuata, a partire dalla sentenza *Digital Rights Ireland*, nella conservazione di tipo *targeted* o mirata, inerente cioè a un determinato periodo di tempo, a un'area geografica specifica e/o a una precisa cerchia di persone[11]. Nonostante i dubbi circa la reale efficacia di quest'ultimo strumento, nonché i timori sulla possibile deriva discriminatoria che una ingerenza mirata di tale tipo potrebbe comportare[12], la CGUE ha riaffermato tale interpretazione anche nelle decisioni più

cata come "grave", diversamente da quanto previamente statuito dalla Direttiva 2006/24/CE. Tale requisito di gravità dei reati perseguiti è stato invece ribadito dalla costante giurisprudenza della CGUE: a partire dalla sentenza del 21 dicembre 2016, 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 a.*, nonché successivamente nella pronuncia del 2 ottobre 2018, C-207/16, *Ministerio Fiscal*, i giudici di Lussemburgo hanno infatti stabilito che solo un crimine di carattere "grave" può giustificare un'ingerenza grave nella sfera privata quale quella determinata dalla conservazione e accesso ai metadati. Pur stabilendo, dunque, questo importante e decisivo criterio, che rende sproporzionata la conservazione dei metadati e l'accesso agli stessi per finalità di repressione di reati "semplici", la CGUE non ha mai indicato cosa debba intendersi per "reato grave"; anche la Direttiva 2006/24/CE, del resto, attribuiva tale determinazione al legislatore nazionale. Il concetto di gravità, quindi, resta ancora dibattuto e la giurisprudenza europea non ha provveduto a chiarimenti sul punto, come si vedrà anche nella pronuncia oggetto del presente contributo.

[10] Vedi *supra* nota n. 9.

[11] Cioè una conservazione limitata ad un determinato periodo di tempo e/o ad un'area geografica determinata e/o ad una cerchia di persone che possano essere coinvolte in un reato grave. Sui punti rilevanti di tale pronuncia, si veda, tra la vastissima dottrina, M. GRANGER, K. IRION, *The Court of Justice and the Data retention directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson on privacy and data protection*, in *European Law Review*, 2014, p. 835 ss.; A. VEDASCHI, V. LUBELLO, *Data retention and its implications for the fundamental right to privacy*, in *Tilburg Law Review*, 2015, p. 14 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*, 2015, p. 65 ss; D. FENNELLY, *Data retention: the life, death and afterlife od a Directive*, in *ERA Papers*, 2018, p. 1 ss.

[12] Secondo Cameron, ad esempio, la conservazione mirata indicata dalla CGUE pone problemi in termini di tutela del principio di non discriminazione: «while this power [to use the geographic criterion] would enable temporary monitoring of large public gatherings (such as sporting events), it also raises the spectre of permanent monitoring of, not simply zones surrounding government offices and other obvious terrorist targets, or even targets of organized crime, such as concentrations of banks, but, more disturbingly, large urban areas with marginalized populations, such as immigrants

recenti, *Privacy International*[13], *La Quadrature du Net*[14], respingendo con forza e chiarezza la legittimità di ulteriori forme di conservazione alternative a quella *targeted* – ci si riferisce ad esempio alla conservazione *limitata*, proposta da Europol[15], e consistente in una forma di *data retention* 'intermedia', più ampia rispetto a quella mirata, ma meno invasiva di quella generalizzata.

Nelle rilevanti e, per certi versi, rivoluzionarie[16], sentenze del 6 ottobre 2020 i giudici di Lussemburgo hanno però poi per la prima volta specificamente e dettagliatamente affrontato il tema della disciplina della conservazione dei dati finalizzata alla tutela della sicurezza nazionale. Così è stato innanzitutto ribadito e meglio precisato che la regolamentazione della *data retention* rientra nell'ambito di ap-

communities», I. CAMERON, *Balancing data protection and law enforcement needs*, cit., p. 1489. Simili perplessità e preoccupazioni si leggono peraltro anche nelle *Pleading Notes* presentate dal Garante europeo della protezione dei dati (GEPD) in occasione dell'udienza pubblica tenutasi il 9 settembre 2019 con riferimento ai rinvii inglese, francese e belga (*Privacy International* e *La Quadrature du Net*).

[13] CGUE, sentenza del 6 ottobre 2020, C-623/17, *Privacy International c. Secretary of State for Foreign and Commonwealth Affairs e a.*

[14] CGUE, sentenza del 6 ottobre 2020, C-511/18, C-512/18 e C-520/18, *Ordre des barreaux francophones et germanophone e a. c. Conseil des Ministres*. Si vuole sin da ora evidenziare come l'approccio individuato in tali pronunce sia stato riconfermato anche in tempi recenti in CGUE, sentenza del 5 aprile 2022, C-140/20, *G.D. c. Commissioner of An Garda Síochána e a.*

[15] Come riportato dal Consiglio dell'UE nel documento del 23 novembre 2018, n. 14319/18, attinente allo *State of play* della disciplina europea della conservazione e accesso ai metadati alla luce della giurisprudenza della CGUE. In tale documento, il Consiglio riporta la proposta di Europol di considerare legittima e proporzionata una conservazione limitata a specifiche categorie di dati, oggettivamente necessarie per la salvaguardia della sicurezza, nonché a certi tipi di fornitori e di servizi, individuati sulla base di una rilevata connessione tra *retention* e obiettivo securitario da raggiungere. Una simile forma di conservazione, a parere di Europol, sarebbe così risultata in grado di escludere dall'obbligo di conservazione piccoli fornitori di servizi di telecomunicazione o ancora i dati di soggetti le cui attività risultavano coperte da segreto professionale. Sul contenuto di tale proposta, sia consentito rinviare a G. FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, Torino, 2021. Merita comunque ricordare che la CGUE ha invece ribadito, anche nella recente pronuncia *G.D. c. Commissioner of An Garda Síochána e a.*, la proporzionalità di una conservazione mirata basata su un criterio geografico, quale il tasso medio di criminalità in una data zona geografica: diversamente dalle preoccupazioni da più parti sottolineate, tale tipologia di conservazione «non è, in linea di principio, idonea a dar maggiormente luogo a discriminazioni, dato che il criterio relativo al tasso medio di criminalità grave non presenta, di per sé, alcun nesso con elementi potenzialmente discriminatori», CGUE, *G.D. c. Commissioner of An Garda Síochána e a.*, cit., para. 80.

[16] Per approfondimenti su tali decisioni, si leggano, I. CAMERON, *Metadata retention and national security: Privacy International and La Quadrature du Net: Case C-623/17*, in *Common Market Law Review*, 2021, p. 1433 ss.; M. NINO, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il diritto dell'Unione europea*, 2021, p. 93 ss; M. ROJSZCZAK, *National security and retention of telecommunications data in light of recent case law of the European Courts*, in *European Constitutional Law Review*, 2021, p. 607 ss.; sia concesso 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*, 2021, p. 1361 ss.

plicazione del diritto dell'UE anche laddove essa sia volta alla garanzia della sicurezza nazionale: l'obbligo di conservazione, implicando comunque un trattamento dei dati da parte di soggetti privati – gli operatori dei servizi di telecomunicazione – e non unicamente attività svolte da autorità dello Stato, deve dunque rispettare i requisiti e principi stringenti fissati dal diritto – e soprattutto dalla giurisprudenza – sovranazionale, indipendentemente dalla finalità perseguita[17]. Questa posizione è stata da più parti accolta come una netta vittoria a favore di una forte tutela dei diritti fondamentali, «poiché tend[e] ad attribuire all'Unione europea un ruolo rilevante anche nel contesto della sicurezza nazionale»[18].

La CGUE, in tale contesto, ha tuttavia individuato, in maniera innovativa rispetto al passato, anche una possibilità eccezionale ed unica di ricorso alla *bulk data retention*: la garanzia della sicurezza nazionale – ad esempio in caso di pericolo di terrorismo – costituisce un obiettivo superiore alla mera lotta alla criminalità grave[19], tale quindi da giustificare la maggiore ingerenza nei diritti fondamentali

[17] Sin dalla pronuncia *Digital Rights Ireland* gli Stati membri hanno spesso invocato, nel dibattito in materia di *data retention*, l'art. 4, co. 2, Trattato sull'Unione europea (TUE), ritenendo che le condizioni e i criteri di proporzionalità stabiliti dalla CGUE nella propria giurisprudenza non potessero applicarsi anche a normative finalizzate alla salvaguardia della sicurezza nazionale: in tal caso, infatti, la disciplina nazionale, ricadendo tra le materie assegnate esclusivamente alla competenza degli Stati membri, avrebbe dovuto sottostare unicamente ai limiti – più blandi – dettati dalla Corte europea dei diritti dell'uomo (CEDU) e dalla Convenzione europea dei diritti dell'uomo (Convenzione EDU). Sul punto si legga S. CRESPI, *The applicability of Schrems principles to the Members States: national security and data protection within the EU context*, in *European Law Review*, 2018, p. 669 ss; M. ZALNIERIUTE, *A struggle for competence: national security, surveillance and the scope of EU law at the Court of Justice of the EU*, in *Modern Law Review*, 2021, p. 1 ss.

[18] In tal senso M. NINO, *La disciplina internazionale ed europea della* data retention *dopo le sentenze* Privacy International *e* La Quadrature du Net *della Corte di giustizia UE*, cit., p. 106. Similmente anche M. ZALNIERIUTE, *A struggle for competence: national security, surveillance and the scope of EU law at the Court of Justice of the European Union*, cit.; J. SAJFERT, *Bulk data interception/retention judgements of the CJEU. A victory and a defeat for privacy*, in *European Law Blog*, 26 ottobre 2020. Sulle criticità e i dubbi concernenti il *reasoning* seguito dalla CGUE sul punto, si rimanda a I. CAMERON, *Metadata retention and national security: Privacy International and La Quadrature du Net: Case C-623/17*, cit., in particolare p. 1457 ss. ma anche a Vogiatzoglou e Bergholm che hanno espresso perplessità quanto alla definizione di "attività dello Stato" fornita dai giudici: «the way the Court defines "activities of the State" (Art. 1(3) E-Privacy Directive) as "activities unrelated to the fields in which individuals are active" further begs the question if such a field can ever exist in a state and what is left of the exception of national security, as enshrined in the TEU», 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.

[19] Per minacce alla sicurezza nazionale si intendono 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 popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo», CGUE, *La Quadrature du Net*, cit., para. 135. Non viene invece fornita una definizione di reati gravi, indicati solamente come «forme gravi di criminalità» e «minacce gravi alla sicurezza pubblica» (para. 140), senza ulteriori specificazioni.

rappresentata dalla conservazione generalizzata. Nonostante questa inedita apertura, mai specificata con tale chiarezza nelle previe sentenze e derivante dal preciso rinvio promosso dall'*Investigatory Powers Tribunal* inglese che per la prima volta ha posto quesiti riguardanti unicamente l'attività di agenzie di intelligence, l'impiego legittimo dello strumento della *bulk data retention* per finalità di sicurezza nazionale viene comunque sottoposto a stringenti condizioni, delineate dai giudici: il carattere non sistematico della conservazione generalizzata, la presenza di circostanze sufficientemente concrete che consentano di ritenere esistente una minaccia grave per la sicurezza nazionale reale e attuale o prevedibile, la previsione di un tempo di *data retention* limitato allo stretto necessario, la determinazione di garanzie rigorose contro il rischio di abusi, nonché la previsione di un effettivo controllo giurisdizionale o di un organo indipendente.

Quanto invece alla disciplina dell'accesso ai metadati conservati, nella sua giurisprudenza la CGUE ha più volte ribadito come esso possa avvenire solo per finalità di lotta contro un reato grave e debba essere accompagnato da requisiti sostanziali e procedurali chiari e precisi, nonché da criteri oggettivi tali da permettere una limitazione del numero di soggetti autorizzati ad accedere e a condizione che venga effettuato un previo controllo da parte di un giudice o di un'entità amministrativa indipendente in grado di valutare la stretta necessità dell'accesso nell'ambito di indagini penali.

Pur brevemente e per quanto rileva ai fini della presente disamina, è utile evidenziare come le richiamate sentenze dell'ottobre 2020 siano state accolte dagli Stati membri, dalle autorità di *intelligence* e *law enforcement*, ma anche da ONG, società civile e dottrina in maniera molto differente, provocando reazioni discordanti che hanno reso alquanto complesso lo sforzo di trarre un bilancio preciso delle posizioni espresse dai giudici di Lussemburgo[20]: da un lato, la riconferma della incompatibilità con il diritto dell'UE di forme di *bulk data retention* per scopi di pubblica sicurezza e repressione di reati gravi nonché la affermata applicazione del diritto dell'UE e dei suoi principi a tutte le disposizioni che impongono un trattamento di dati e metadati da parte di soggetti privati, indipendentemente dalla finalità perseguita, unitamente alle condizioni ribadite quanto alla disciplina dell'accesso ai metadati conservati, rappresentano una indubbia vittoria per la garanzia dei diritti fondamentali, in grado di comprimere significativamente la discrezionalità degli Stati membri nell'impiego di strumenti di sorveglianza massiva;

[20] Paiono significative le espressioni impiegate da talune ONG a commento delle pronunce esaminate: la ONG Statewatch ha parlato di «a victory and a defeat for privacy», mentre la ONG La Quadrature du Net di «victorious defeat».

dall'altro lato, tuttavia, l'"apertura" eccezionale verso forme di conservazione generalizzata quando minacce alla sicurezza nazionale sono in gioco[21] ha destato non poche critiche ed è stata vista quale preoccupante cambio di approccio verso una direzione maggiormente pro-securitaria; pur individuando condizioni specifiche di ammissibilità e proporzionalità della *bulk data retention*, che si conferma quale strumento eccezionale e dalla natura non sistematica, le indicazioni della Corte sono infatti apparse troppo ampie o vaghe, passibili quindi di interpretazioni estensive da parte delle autorità nazionali e in grado quindi di condurre alla adozione quasi "illimitata" di misure eccessivamente lesive della sfera privata dei cittadini europei[22]. In tale inedito approccio della Corte, che per la prima volta e in maniera espressa si è pronunciata sull'impiego della conservazione dei metadati nell'ambito della sicurezza nazionale, taluni autori hanno pertanto ravvisato una scelta di compromesso dinnanzi alle forti spinte degli Stati membri, strenui sostenitori dell'utilità e necessità dello strumento della conservazione generalizzata[23]. Tali differenti letture del resto riflettono le mai sopite diversità di vedute rispetto alla giurisprudenza della CGUE che sin dalla sentenza *Tele2* è stata dai più favorevolmente accolta come tangibile segno di una Unione europea baluardo dei diritti fondamentali – in particolare quelli alla vita privata e alla protezione dei dati personali – dinnanzi a spinte pro-securitarie, ma che è stata anche oggetto di perplessità e critiche da parte di chi ha invece riconosciuto nell'approccio garantista dei giudici e nella difficile concretizzazione di forme di *targeted data retention* uno sbilanciamento – anche dovuto al peculiare riparto delle competenze tra Stati membri e UE in materia di sicurezza – che rischia di minare l'efficacia degli strumenti

[21] Merita ricordare solo brevemente come ulteriori aperture a forme di conservazione generalizzata ed indiscriminata vengano individuate dalla Corte rispetto a specifiche tipologie di dati, quali profili IP e dati relativi all'identità civile, nonché con riferimento alla conservazione rapida dei dati di traffico e di ubicazione e a quella in tempo reale, pur con limitazioni da rinvenirsi nella necessità di disporre condizioni procedurali e sostanziali precise. Per una analisi di questi interessanti e rilevanti profili delle sentenze dell'ottobre 2020, si rinvia alla dottrina citata *supra* nota n. 16.

[22] Tzanou sostiene che «while Privacy International continues along the same lines of this expansive data protection jurisprudence and can be seen as another victory for fundamental rights, this time in the context of national security, Quadrature du Net marks an important departure form the CJEU's prohibitive approach to bulk data retention to a more nuanced one», M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net: one step forward two steps back in the data retention saga?*, in *European Public Law,* 2021, p. 124.

[23] In questo senso si esprimono, ad esempio, M. NINO, *La disciplina internazionale ed europea della* data retention *dopo le sentenze* Privacy International *e* La Quadrature du Net *della Corte di giustizia UE*, cit., e M. ZALNIERIUTE, *A struggle for competence: national security, surveillance and the scope of EU law at the Court of Justice of the European Union*, cit.; M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net: one step forward two steps back in the data retention saga?*, cit.

investigativi della conservazione e accesso e dunque gli interessi securitari[24]. In questo senso, riassuntivamente, con riferimento alla giurisprudenza esaminata, Cameron afferma come «depending on one's perspective, the Court has shown a fearless willingness to intervene to uphold fundamental rights, or a foolhardy willingness to throw spanners into the works of delicately balanced systems of national regulation and international cooperation. There is undoubtedly much room for reform in many EU Member States, both as regards law enforcement and national security use of communications metadata. (...) Whichever perspective one takes on the Court's approach, its commitment to data protection and its expansive view of its own competence mean that many more cases on these issues can be expected»[25].

E in effetti, come testimoniato dal tratteggiato vivace e continuo dibattito dottrinario, la ricca giurisprudenza della CGUE non è quindi giunta a porre un punto conclusivo alla complessa *data retention saga*: anche a seguito delle decisioni del 2020, i governi e i legislatori nazionali – e talvolta anche gli stessi giudici interni – hanno mostrato profonde difficoltà nello stabilire normative interne in materia di conservazione e accesso ai metadati in grado da un lato di rispondere alle esigenze di efficacia nella lotta alla criminalità e al terrorismo e dall'altro di adeguarsi ai rigidi limiti e alle tutele determinate dai giudici di Lussemburgo. Nel tentativo di adottare approcci più *flessibili* quanto alla regolamentazione – e dunque all'utilizzo – della *data retention*, così da non rinunciare del tutto all'impiego di

[24] Oltre alle posizioni in tale direzione espresse da Europol e dai rappresentanti delle autorità di *law enforcement* e di *intelligence* di numerosi Stati membri, si legga, in dottrina, D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, cit. Tale dibattito e diversità di considerazioni quanto alla posizione espressa dalla Corte in materia di *data retention* è peraltro particolarmente viva ed evidente anche con riguardo alle pronunce della CGUE sul trasferimento dei dati verso Stati terzi (si pensi alla c.d. *Schrems saga*): nella dichiarata invalidità delle decisioni di adeguatezza che consentivano il *data flow* tra UE e USA, taluni autori hanno ravvisato il segno di una "esaltante illusione" dell'UE e della sua Corte, in particolare, di poter proteggere i diritti dei propri cittadini anche oltre i confini e dinnanzi alle necessità securitarie e agli strumenti di tutela della sicurezza disposti da Stati terzi. Sull'approccio eccessivamente garantista o invece meritoriamente rispettoso dei diritti fondamentali e della loro salvaguardia, sia consentito rimandare all'acceso dibattito dottrinario ricostruito in G. FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali*, cit., in particolare p. 198 ss., nel quale vengono richiamati, *ex multis*, R. EPSTEIN, *The ECJ's fatal imbalance: its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European Constitutional Law Review*, 2016, p. 339, M. BRKAN, *The unstoppable expansion of the EU fundamental right to data protection. Little shop of horrors?*, in *Maastricht Journal of European and Comparative Law*, 2016, p. 812 ss.; C. KUNER, *Reality and illusion in the EU data transfer regulation post Schrems*, in *German Law Review*, 2017, p. 898 ss.; O. POLLICINO, *Diabolical persistence. Thoughts on the Schrems II decision*, in *MediaLaws*, 2020, p. 315 ss.

[25] I. CAMERON, *Metadata retention and national security: Privacy International and La Quadrature du Net: Case C-623/17*, cit., p. 1471.

tale strumento investigativo – ancora considerato essenziale[26] –, il panorama di soluzioni e discipline nazionali nell'UE è così rimasto – nonostante gli interventi della Corte sovranazionale – estremamente frastagliato e disomogeneo[27], mentre i significativi dubbi e preoccupazioni quanto alla corretta interpretazione e applicazione dei principi individuati dalla giurisprudenza europea hanno portato cittadini e ONG a richiedere sovente l'intervento delle corti nazionali; queste ultime, a loro volta, hanno promosso ulteriori rinvii pregiudiziali dinanzi alla CGUE, alcuni dei quali ancora pendenti[28], al fine di ottenere chiarezza quanto alle condizioni e alle salvaguardie che devono guidare l'attuazione della disciplina derogatoria garantita dall'art. 15 Direttiva *e-Privacy*.

In tale articolato scenario si inserisce la sentenza *H.K. c. Prokuratuur* che, di poco successiva alle discusse pronunce dell'ottobre 2020, è sin da subito apparsa innovativa e di estremo interesse quanto ai profili trattati e alle considerazioni svolte dalla CGUE.

Il presente contributo intende pertanto analizzare tale decisione per poi evidenziare le forti reazioni e i significativi dibattiti provocati nei Parlamenti e nelle Corti degli Stati membri; simili considerazioni conducono a talune riflessioni finali quanto alle prospettive future e alle criticità persistenti che impediscono di spegnere i riflettori sulla disciplina della *data retention* e impongono, anzi, di osservarne con attenzione gli sviluppi.

[26] Si consideri «the broad support expressed by Ministers at the March 2021 Justice and Home Affairs Council for a functioning data retention regime. The Portuguese Presidency stressed on that occasion: "The retention of data is a crucial tool for our law enforcement authorities when carrying out investigations, and it is clear the current situation of uncertainty increases the risks to the security of our citizens. Today we reiterated our commitment to finding a common solution; one which allows our police and judicial authorities to carry out their work while fully ensuring the rights to privacy of our citizens"», A. JUSZACZAK, E. SASON, *Recalibrating data retention in the EU. The jurisprudence of the CJEU – is this the end or the beginning?*, in *Eucrim*, 2021, p. 262.

[27] Per una ricostruzione di tale complesso panorama, si legga M. ZUBIK, J. PODKOWIK, R. RYBSKI (a cura di), *European Constitutional Courts towards data retention laws*, Cham, 2020; N. NI LOIDEAIN, *EU data privacy law and serious crime. Data retention and policymaking*, Oxford, 2022.

[28] Oltre ai rinvii pregiudiziali C-793/19, *SpaceNet AG c. Repubblica federale di Germania* e C-794/19, *Repubblica federale di Germania c. Telekom Deutschland GmbH*, entrambi promossi del *Bundesverwaltungsgericht* tedesco il 29 ottobre 2019 – dunque concomitanti ai rinvii che hanno originato le sentenze dell'ottobre 2020 – e rispetto ai quali sono state depositate le Conclusioni dell'Avvocato generale Campos Sanchez-Bordona in data 18 novembre 2021, si fa riferimento al rinvio pregiudiziale C-350/21, proposto dallo *Spetsializirian nakazatelen sad* (Bulgaria) il 4 giugno 2021 e a quello italiano, di cui si parlerà *infra*. Tutti i rinvii citati attengono, in assenza di una più specifica disciplina in materia di *data retention*, all'interpretazione dell'art. 15 della Direttiva 2002/58/CE.

2. I requisiti della 'gravità' del reato e del previo controllo di un'autorità giudiziaria o amministrativa indipendente: il significativo portato della sentenza *H.K. c. Prokuratuur*

Diversamente dalle pronunce sopra brevemente richiamate, il caso *H.K. c. Prokuratuur* attiene principalmente alle condizioni e ai requisiti riguardanti l'accesso ai metadati conservati. I quesiti posti alla CGUE, infatti, concernevano specificamente tanto i criteri da valutare per determinare la gravità dell'ingerenza nei diritti fondamentali – e dunque la conseguente necessità che l'accesso fosse finalizzato alla prevenzione e perseguimento di reati gravi – quanto il controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente e, in particolare, se tale condizione potesse essere legittimamente assolta laddove il controllo venisse effettuato da un pubblico ministero che dirige il procedimento istruttorio ma che dovrà poi anche rappresentare la pubblica accusa nel corso del procedimento giudiziario eventualmente avviato.

Ripercorrendo i principi delineati nella propria giurisprudenza in tema di *data retention* e richiamando soprattutto le rilevanti decisioni del 6 ottobre 2020, i giudici di Lussemburgo hanno chiarito preliminarmente che le operazioni di accesso possono essere consentite solo qualora la conservazione dei metadati stessi sia conforme all'art. 15 Direttiva *e-Privacy*; è stata così colta l'occasione per confermare quanto affermato nelle attese pronunce *La Quadrature du Net* e *Privacy International*, ovvero la chiara e ormai incontrovertibile incompatibilità con il diritto dell'UE di una forma di conservazione generalizzata e indiscriminata dei dati di traffico e di ubicazione e l'eccezionalità della *bulk data retention* in limitati casi di minaccia alla sicurezza nazionale. Ciò a dire, nuovamente, che è lo strumento prodromico e funzionale all'accesso, quello cioè della *retention*, a dover essere in primo luogo legittimo e proporzionato secondo le valutazioni svolte dalla CGUE.

Passando poi più specificamente all'impiego dei metadati da parte delle autorità pubbliche, i giudici hanno ribadito il necessario parallelismo tra gravità dell'ingerenza nella sfera privata e importanza dell'obiettivo di interesse generale che, tramite l'accesso ai dati, si vuole perseguire. Ne deriva pertanto che, nel caso in cui si vogliano trattare dati relativi al traffico e all'ubicazione, solo la lotta alla criminalità grave o la presenza di gravi minacce alla sicurezza pubblica possono giustificare l'accesso da parte di autorità pubbliche: questo perché, come del resto già emerso nella previa giurisprudenza in materia, tale particolare categoria di dati consente di dedurre abitudini, relazioni sociali o frequentazione di luoghi, costituendo quindi una ingerenza grave. A nulla devono rilevare, in questa analisi, la durata del periodo per il quale viene chiesto l'accesso o la quantità di dati interes-

sati, considerando che anche l'accesso a un quantitativo limitato di dati relativi al traffico o all'ubicazione, oppure l'accesso a dati per un breve periodo, risultano comunque idonei a fornire precise informazioni sulla vita privata dell'utente. L'ingerenza nei diritti fondamentali derivante dall'accesso a dati di traffico e ubicazione, in conclusione, è tale da assumere in ogni caso quel carattere di gravità che richiede necessariamente un obiettivo *rafforzato*, da indentificarsi appunto nella repressione dei soli reati gravi o gravi minacce alla sicurezza pubblica.

Alla luce dei principi espressi, la normativa estone risultava particolarmente problematica: secondo tale legislazione, infatti, l'accesso ai dati poteva essere richiesto per qualsiasi tipo di reato, senza specificazione circa la gravità dell'obiettivo perseguito. Ciò apriva inevitabilmente, nello specifico caso da cui il rinvio originava, a questioni riguardanti l'ammissibilità dei processi verbali fondati sull'utilizzo di metadati raccolti e trattati mediante l'attuazione di una disposizione nazionale in contrasto con l'art. 15 Direttiva *e-Privacy*. Su questo fronte, la CGUE ha ribadito quanto previamente emerso nella pronuncia *La Quadrature du Net*: spetta al solo diritto nazionale il compito di stabilire regole relative all'ammissibilità di informazioni ed elementi di prova ottenuti, nell'ambito di un procedimento penale, mediante forme di conservazione o accesso non conformi al diritto dell'UE. Ciò a condizione che tali regole rispettino però il principio di effettività[29], il principio del contraddittorio e il diritto all'equo processo[30].

[29] Con particolare riferimento a tale profilo, i giudici di Lussemburgo hanno affermato che «il principio di effettività impone al giudice penale nazionale di escludere informazioni ed elementi di prova che siano stati ottenuti mediante una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione incompatibile con il diritto dell'Unione, od anche mediante un accesso dell'autorità competente a tali dati in violazione del diritto dell'Unione, nell'ambito di un procedimento penale instaurato nei confronti di persone sospettate di atti di criminalità, qualora tali persone non siano in grado di svolgere efficacemente le proprie osservazioni in merito alle informazioni e agli elementi di prova suddetti, riconducibili ad una materia estranea alla conoscenza dei giudici e idonei ad influire in maniera preponderante sulla valutazione dei fatti», para. 44.

[30] La questione relativa agli effetti nel tempo di una declaratoria di incompatibilità rispetto al diritto dell'UE del diritto nazionale in materia di conservazione dei metadati è di estrema delicatezza e rilevanza, avendo impatto diretto sulla legittimità dei dati impiegati nei procedimenti penali. Non stupisce che tanto il giudice belga nel rinvio *La Quadrature du Net*, quanto quello irlandese nel rinvio recentemente deciso dalla CGUE con sentenza del 5 aprile 2022, *G.D. c. Commissioner of An Garda Síochána e a.*, cit., abbiano messo in rilievo tale profilo problematico e dai potenziali dirompenti effetti. I giudici di Lussemburgo, anche nella pronuncia del 5 aprile 2022, hanno affermato che il diritto dell'UE «osta a che un giudice nazionale limiti nel tempo gli effetti di una declaratoria di invalidità ad esso spettante, in forza del diritto nazionale, nei confronti di una normativa nazionale che impone ai fornitori di servizi di comunicazione elettronica la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione, a causa dell'incompatibilità di tale normativa con l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce della Carta. L'ammissibilità degli elementi di prova ottenuti mediante una siffatta conservazione rientra, con-

Definito questo fondamentale primo quesito, i giudici di Lussemburgo hanno esaminato l'ulteriore questione posta dal giudice estone riguardante la determinazione della natura "indipendente" dell'autorità deputata a svolgere il controllo di legittimità preventivo all'accesso. Se questo vaglio rappresenta uno dei requisiti ormai cristallizzati nella giurisprudenza della CGUE, le qualità e la definizione della "indipendenza" richiesta non erano mai state analizzate dai giudici di Lussemburgo. In questo rinvio, dunque, è stata offerta l'occasione di entrare ulteriormente nel dettaglio di tale criterio e di fornire una lettura ancor più approfondita della disciplina dell'accesso. Nello specifico, la normativa estone identificava nel pubblico ministero l'autorità preposta al controllo preventivo alla fase di accesso: tale soggetto, pur essendo sottoposto solo alla legge e avendo l'obbligo di esaminare sia gli elementi a carico sia quelli a discarico nel corso del procedimento istruttorio, assumeva su di sé anche il compito di raccogliere elementi di prova per lo svolgimento, eventuale, di un futuro processo. Date tali caratteristiche, alcuni dubbi erano sorti quanto all'indipendenza del pubblico ministero e, in particolare, se esso godesse di uno status che gli consentisse di agire, nell'assolvimento dei propri compiti, in modo obiettivo, imparziale e al riparo da qualsiasi influenza esterna.

Secondo la CGUE, il requisito dell'indipendenza richiede che l'autorità incaricata del controllo preventivo sia «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 della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso» (para. 52). Da tale ricostruzione del requisito di "indipendenza" deriva che l'autorità alla quale viene affidato il delicato compito del controllo preventivo deve necessariamente essere terza rispetto a quella che formula la richiesta di accesso ai dati, in modo che il vaglio esercitato possa essere realmente imparziale e oggettivo. La terzietà, dunque, impone che l'autorità di controllo non sia coinvolta nella conduzione dell'indagine penale e sia quindi in una posizione di neutralità rispetto a tutte le parti del procedimento. Se queste sono le condizioni, diviene evidente che un pubblico ministero quale quello estone non poteva essere in grado di soddisfarle a causa della natura stessa del proprio incarico – quello cioè di valutare, a seguito di una istruttoria penale, se sottoporre o meno al giudice una controversia – e della

formemente al principio di autonomia procedurale degli Stati membri, nell'ambito del diritto nazionale, sempreché nel rispetto, in particolare, dei principi di equivalenza e di effettività», CGUE, sentenza del 5 aprile 2022, *G.D. c. Commissioner of An Garda Síochána e a.*, cit., para. 128.

propria posizione, che non era quella di soggetto terzo bensì di vera e propria parte che esercitava l'azione penale nell'eventuale processo.

Ritenendo, quindi, che il requisito del controllo indipendente non potesse ritenersi soddisfatto in casi di cumulo di competenze nella persona del pubblico ministero, la CGUE ha precisato inoltre un aspetto di grande rilievo: all'assenza di un vaglio preventivo non può sopperire un controllo successivo da parte di un giudice. Un tale intervento postumo, infatti, non riuscirebbe a garantire il perseguimento dell'obiettivo cui il controllo preventivo è preposto, ovvero impedire che l'accesso ai dati – e dunque l'invasione nei diritti fondamentali – ecceda i limiti dello stretto necessario. Con questo i giudici di Lussemburgo hanno respinto quella posizione, espressa invece dalla Corte EDU nella sentenza *Szabo*[31] in materia di sorveglianza di comunicazioni, che ammetteva, a determinate condizioni, la legittimità di un mancato controllo preventivo laddove un controllo giurisdizionale *ex post* venisse garantito[32]. È stata respinta, in sostanza, una lettura complessiva e globale delle tutele, capace cioè di compensare talune carenze in presenza di altre e diverse garanzie; una simile visione, del resto, era già stata negata anche dall'Avvocato generale Campos Sanchez-Bordona nei casi *La Quadrature du Net* e *Privacy International*[33], nei quali era stata respinta quella interpretazione che considerava legittima la conservazione generalizzata qualora compensata da maggiori tutele nella fase di accesso. Proprio con riferimento a quest'ultima attività, la CGUE, nella sentenza in esame, non ha perso occasione per ribadire che i legislatori degli Stati membri devono comunque soddisfare il requisito di proporzionalità.

Tra le condizioni sostanziali e procedurali che debbono essere garantite, i giudici hanno infatti previsto la determinazione di criteri oggettivi in grado di stabilire la sussistenza di un collegamento, almeno indiretto, tra accesso e finalità perseguita e dunque una limitazione dell'ingerenza solo ai dati di persone sospettate di progettare, di aver commesso o di essere implicate in un reato grave; è stato così ancor meglio specificato il divieto di un accesso generalizzato ed "esplorativo", che trova l'unica eccezione possibile nel caso in cui interessi vitali della si-

[31] CEDU, sentenza del 12 gennaio 2016, ric. n. 37138/14, *Szabo e Vissy c. Ungheria*. Per un'analisi della giurisprudenza di tale Corte in materia, sia consentito 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*, 2020, p. 44 ss.

[32] Sul punto si legga anche S. ROVELLI, *Case Prokuratuur: proportionality and the independence of authorities in data retention*, in *European Papers*, 2021, p. 199 ss.

[33] Conclusioni dell'Avvocato generale Campos Sanchez-Bordona presentate il 15 gennaio 2020, C-623/17, *Privacy International*, cit.

curezza nazionale, difesa e sicurezza pubblica siano soggetti a minaccia – quale ad esempio quella terroristica –; solo in tali limitate circostanze l'accesso può essere concesso anche in assenza di un sospetto specifico, riguardando dunque anche persone diverse dai soli sospettati e solo qualora vi siano elementi oggettivi tali da consentire di ritenere l'accesso ai dati utile nel caso concreto. Veniva pertanto riconfermato quell'allentamento – pur condizionato – delle stringenti condizioni fissate dalla CGUE nel caso in cui ad entrare in gioco sia la finalità di garanzia della sicurezza nazionale, del tutto similmente a quanto le sentenze dell'ottobre 2020 avevano precisato con riferimento alla disciplina della conservazione.

In conclusione, dunque, nella pronuncia *H.K. c. Prokuratuur* sono stati da un lato sostanzialmente riproposti i requisiti e i criteri già indicati nella previa giurisprudenza, mentre dall'altro, con specifico riferimento alla fase dell'accesso, i giudici hanno fornito importanti chiarimenti quanto alla determinazione dell'indipendenza dell'autorità deputata al controllo preventivo nonché in merito alla valutazione della gravità della ingerenza.

3. Le reazioni alla sentenza *H.K. c. Prokuratuur* tra resistenze ed evoluzioni normative e giurisprudenziali: l'incerto futuro della disciplina della *data retention* e dell'accesso ai metadati

Come alcuni commenti – invero non molto numerosi – della pronuncia esaminata hanno posto in rilievo[34], la decisione della CGUE qui analizzata si inserisce in maniera coerente nel solco profondo già tracciato dalla nutrita giurisprudenza sovranazionale in materia di *data retention*. In particolare, letta unitamente alle fondamentali decisioni dell'ottobre 2020, la sentenza *H.K. c. Prokuratuur* ha contribuito a chiarire quel complesso quadro di limiti, criteri e condizioni che i giudici di Lussemburgo, ormai da oltre un decennio, stanno definendo e dal quale inizia ora ad affiorare un'immagine dai contorni sempre più precisi benché non ancora del tutto nitidi.

Sebbene le sentenze *La Quadrature du Net* e *Privacy International* siano caratterizzate, come si è detto, da alcune criticate innovazioni che hanno aperto al possibile impiego di strumenti di *bulk data retention* per scopi di sicurezza nazionale – pur sottoponendo tale eccezionale ricorso al rispetto di condizioni e salvaguar-

[34] E. CELESTE, *Commission v. Spain and H.K. v. Prokuratuur: taking the plank out of EU's own eye*, in *BridgeBlog*, 15 marzo 2021; E. ANDOLINA, *Ancora una pronuncia della Grande Camera della CGUE in tema di condizioni di accesso ai traffic data*, in *Processo Penale e Giustizia*, 2021, p. 1195 ss.

die[35] –, non può infatti essere negato come i giudici di Lussemburgo abbiano ribadito e riconfermato numerosi principi e tutele stabiliti nella giurisprudenza precedente, fornendo ulteriori e precise indicazioni – ad esempio quanto alla disciplina dell'accesso o a quella riferita a determinate tipologie di dati – che hanno contribuito a far luce su taluni profili rimasti discussi a seguito di storiche pronunce quali *Tele2* e *Ministerio Fiscal*.

Sotto tale profilo, le specificazioni fornite nelle ultime sentenze non lasciano più spazio alla adozione da parte degli Stati membri di *permissive interpretations*[36] che, fino al 2020, avevano trovato fondamento in letture meno rigide della giurisprudenza della CGUE, ad esempio ritenendo possibile una conservazione generalizzata laddove circondata da salvaguardie e limitazioni precise e stringenti quanto all'accesso – quali l'esclusione di talune categorie di dati o di utenti[37] –. Ora invece i tentativi degli Stati membri di mantenere in vita la *bulk data retention* quale strumento "ordinario" di lotta alla criminalità grave paiono ormai destinati a cedere il passo dinnanzi alla netta posizione assunta dai giudici di Lussemburgo.

Questo, pertanto, suggerisce la ancor più urgente necessità di interventi legislativi o giurisprudenziali a livello nazionale, come risposta alle sentenze della CGUE: in altre parole, gli Stati membri nei quali persistono disposizioni volte a imporre ai fornitori di servizi di telecomunicazione un obbligo di conservazione generalizzata per scopi di repressione di reati sono chiamati a modificare tale disciplina, ormai apertamente in contrasto con il diritto dell'UE, optando per una forma di conservazione mirata. Con riferimento alle attività di *intelligence* finalizzate alla garanzia della sicurezza nazionale, inoltre, l'intervento legislativo viene ri-

[35] Tale tipologia di conservazione, vale la pena ribadirlo, è considerata come proporzionata solo laddove non diventi la regola, sia limitata temporalmente a quanto strettamente necessario e qualora ricorrano circostanze sufficientemente concrete da consentire di ritenere che lo Stato membro affronti una minaccia grave per la sicurezza nazionale, reale, attuale o prevedibile.

[36] N. VAINIO, S. MIETTINEN, *Telecommunications data retention after DR: legislative and judicial reactions in the Member States*, in *International Journal of Law and Information Technology*, 2015, p. 290 ss.

[37] Questa la lettura adottata dal legislatore, dai governi e, talvolta, dalle corti di Italia e Belgio: in tali Stati membri, infatti, la conformità della disciplina nazionale rispetto al diritto dell'UE, così come interpretato dalla CGUE, è stata affermata ritenendo sufficienti e proporzionate le maggiori tutele e restrizioni poste alla fase dell'accesso, così considerando legittima una forma di conservazione generalizzata ed indiscriminata purché accompagnata da limitazioni quanto al trattamento dei dati da parte delle autorità di *law enforcement*. Mentre in Italia questo approccio non è stato abbondonato dal legislatore nazionale, neppure in occasione di alcune più recenti modifiche normativi, di cui si parlerà *infra*, trovando anche l'avvallo della Corti, in Belgio la Corte costituzionale ha dichiarato l'illegittimità della normativa nazionale nella parte in cui consentiva una forma di *bulk data retention* anche per scopi di repressione di reati gravi. Per un'analisi comparata dei due sistemi, emblematici esempi di approcci differenti dinnanzi al portato della giurisprudenza della CGUE, sia consentito di rimandare a G. FORMICI, *La disciplina della* data retention*,* cit., in particolare pp. 275 ss.

chiesto allo scopo di delineare quelle condizioni e salvaguardie che, secondo quanto individuato dalla Corte nelle sentenze del 2020, sarebbero in grado di legittimare l'eccezionalità della *bulk data retention*: pur lasciando agli Stati membri quello che da diversi autori è stato definito un ampio margine di azione e di interpretazione che potrebbe condurre ad un utilizzo estensivo dello strumento di conservazione generalizzata[38], la CGUE non ha mancato di precisare il bisogno di accompagnare l'eccezione con tutele e dunque regole precise e chiare, in tal modo imponendo un rinnovato dibattito normativo e – in caso di inerzia – financo giudiziario. Alla luce dei principi delineati in *H.K v Prokuratuur*, dovranno poi essere individuate autorità indipendenti che svolgano controlli preventivi all'accesso e che non potranno più coincidere con figure che non assumono carattere di terzietà nel procedimento penale e nella fase di indagini preliminari, come il pubblico ministero in ordinamenti quali quello estone e italiano.

Considerati tali interventi e future evoluzioni, la giurisprudenza più recente dei giudici di Lussemburgo, con le sue conferme ma anche con le sue innovazioni, non permette dunque di considerare certo e definito il futuro della *data retention* nel contesto europeo: l'articolato intreccio tra il piano nazionale – caratterizzato sovente da legislatori, governi e, in taluni casi, corti, restie a rinunciare ad uno strumento investigativo dalle grandi potenzialità – e quello europeo, segnato dalle tensioni provocate da interventi della Corte non sempre concordi con l'approccio della Commissione e del Consiglio[39], rende difficile affermare che sentenze quali quella appena esaminata possano mettere un punto definitivo e risolutivo alla lunga *data retention saga*, garantendo omogeneità e condivisione di soluzioni.

Per riflettere sui possibili sviluppi in tale ambito, dunque, è necessario osservare le reazioni – o l'inerzia – di tre attori principali: gli Stati membri (legislatori, governi e corti nazionali), la Commissione e la CGUE.

[38] Si rimanda sul punto al dibattito già rilevato *supra* nel paragrafo 1 e alla dottrina ivi richiamata.

[39] L'interpretazione garantista fornita dalla CGUE nel complesso bilanciamento tra esigenze securitarie e tutela dei diritti fondamentali non è ravvisabile solo nella c.d. *data retention saga* bensì caratterizza le pronunce in materia di trasferimento dati verso Stati terzi: questa giurisprudenza ha preso avvio con la prima sentenza c.d. *Schrems I* (CGUE, sentenza del 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*), seguita poi da CGUE, sentenza del 16 luglio 2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems*) ed ha poi interessato anche il più specifico trasferimento di PNR (CGUE, Parere n. 1/15 del 26 luglio 2017). Anche in queste pronunce, infatti, i giudici di Lussemburgo hanno ritenuto non conformi al diritto dell'UE, e al principio di proporzionalità in particolare, le decisioni di adeguatezza adottate dalla Commissione e determinanti la sostanziale equivalenza del livello di protezione dei dati e della vita privata offerti dall'ordinamento ricevente i dati. Si nota pertanto anche sotto questo profilo una divergenza di valutazioni tra Commissione, Consiglio e Parlamento, da un lato, e CGUE dall'altro.

Partendo da quest'ultima, dinnanzi a essa restano ancora pendenti taluni casi attinenti all'interpretazione dell'art. 15 Direttiva *e-Privacy*[40]; nella recentissima pronuncia del 5 aprile 2022, originata dal già richiamato rinvio promosso dalla *Supreme Court* irlandese, la CGUE ha ribadito con forza quanto già stabilito nelle pur criticate e dibattute *Privacy International* e *La Quadrature du Net*, così che pare al momento alquanto improbabile che possano verificarsi stravolgimenti nella linea interpretativa adottata in materia di *data retention* negli ultimi anni. Vista la somiglianza dei quesiti posti, tutti inerenti ai limiti dell'impiego di una forma di conservazione generalizzata ed indiscriminata o alla disciplina dell'accesso ai metadati conservati, è altamente probabile che anche nei rinvii ad oggi pendenti la CGUE riconfermi l'indirizzo sin qui stabilito. Quel che è certo, però, è che l'intenso dialogo instaurato dalle Corti nazionali con i giudici di Lussemburgo sottolinea non solo la centralità e il rilievo dello strumento della conservazione dei metadati ma anche la difficoltà dei legislatori nazionali e sovranazionali di adottare soluzioni normative in grado di conformarsi ai requisiti fissati dalla CGUE e quanto invece la società civile, grazie anche all'intervento di numerose organizzazioni non governative (ONG), abbia mostrato una forte attenzione alla delicata sfida della proporzionalità dell'intervento invasivo dello Stato nella vita privata, anche quando esso risulti finalizzato a garantire la sicurezza[41]. Un bilanciamento tra interessi e diritti differenti che dimostra, così, di non aver ancora trovato una semplice ed indiscussa determinazione, dinnanzi a persistenti derive pro-securitarie che ancora abbisognano di essere arginate e adeguatamente regolate.

[40] Si veda *supra* nota n. 27.

[41] Più ampiamente, numerosi sono stati i rinvii che hanno interessato, come anticipato, l'altrettanto complessa materia del trasferimento di dati dall'UE verso Stati terzi, nonché quelli aventi ad oggetto la conformità al diritto dell'UE delle normative nazionali adottate quale trasposizione della Direttiva (UE) 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione pensale nei confronti dei reati di terrorismo e dei reati gravi – ci si riferisce al rinvio promosso dalla *Cour constitutionnelle* belga il 31 ottobre 2019, C-817/19, *Lingue des droits humains c. Conseil des Ministres*, a quelli avviati dal *Amtsgericht* di Colonia, il 20 gennaio 2020, C-148/20, *AC c. Deutsche Lufthansa AG* e il 17 marzo 2020, C-150/20, *BD c. Deutsche Lufthansa AG*, nonché i rinvii del *Verwaltungsgericht* di Wiesbaden del 19 maggio 2020, C-215/20, *JV c. Repubblica federale di Germania* e del 27 maggio 2020, C-222/20, *OC c. Repubblica federale di Germania*. Nonostante la Direttiva in materia di PNR disciplini una tipologia di conservazione e trattamento di dati per scopi securitari differente rispetto a quella sino ad ora esaminata, avendo ad oggetto i soli codici di prenotazione aerea, risulterà comunque importante seguire gli sviluppi di questi procedimenti, che potranno fornire importanti indicazioni sui limiti e sulle salvaguardie da porre in essere in tutte quelle normative che comportano forme di *retention* e di accesso a dati raccolti da operatori privati e che hanno quale scopo quello di prevenire o perseguire minacce alla sicurezza.

Venendo poi agli Stati membri, questi, come si è detto, hanno – ora più che mai, visti i recenti sviluppi giurisprudenziali della CGUE – il difficile compito di predisporre normative nazionali che, pur utilizzando la deroga concessa dall'art. 15 Direttiva *e-Privacy*, rispettino i requisiti indicati dai giudici sovranazionali. Le prime reazioni registratesi in taluni ordinamenti nazionali non paiono tuttavia procedere – o quanto meno non del tutto – in tale direzione e la rinuncia definitiva allo strumento della *bulk data retention* nell'ambito della lotta alla criminalità grave pare ancora alquanto lontana. Ciò che emerge in maniera cristallina è senz'altro la disomogeneità ed eterogeneità delle posizioni espresse, che neppure le ultime pronunce dei giudici di Lussemburgo – quelle dell'ottobre 2020 e la sentenza in questa sede analizzata – hanno, al momento, saputo del tutto superare.

Se si prende quale primo esempio l'Italia, si può notare come il caso *H.K. c. Prokuratuur* abbia, in maniera particolare, prodotto significativi risultati; e questo rappresenta una svolta decisiva nel peculiare panorama nostrano, nel quale nessuna delle precedenti pronunce della CGUE era riuscita ad indurre né il legislatore a riformare la disciplina interna in materia di *data retention* e di accesso ai metadati[42], né le Corti a dichiarare l'incompatibilità del diritto nazionale rispetto a quello dell'UE o, quanto meno, a proporre rinvii alla Corte sovranazionale[43], con un ap-

[42] La disciplina italiana in materia di *data retention* risulta al momento ancora frammentaria ed estremamente dibattuta: pur trovando collocazione principalmente nell'art. 132 del d.lgs. 30 giugno 2003, n. 196 (c.d. Codice Privacy), tale disposizione ha subìto nel tempo numerosi interventi di modifica, per lo più dettati dall'esigenza di rafforzare lo strumento della conservazione dei metadati dinnanzi alle emergenze terroristiche. Da ultimo la Legge 20 novembre 2017, n. 167, ovvero la Legge che reca le disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'UE (c.d. Legge europea), ha previsto un obbligo di conservazione della durata di 72 mesi (!) in capo ai *service providers*. Sebbene tali dati conservati siano accessibili solo per scopi di repressione e accertamento di reati gravissimi quali terrorismo e associazione di tipo mafioso – e altri delineati all'art. 51, co. 3-*quater* e 407, co. 2, lett. a), c.p.p. –, il fornitore, non potendo conoscere in anticipo per quali obiettivi i metadati verranno eventualmente acquisiti in futuro, dovrà operare una *data retention* generalizzata per una durata estremamente lunga; sino alle recentissime modifiche, inoltre, l'accesso ai dati avveniva a seguito di controllo del pubblico ministero e senza alcuna limitazione o restrizione quanto alla gravità del reato perseguito. Per un'analisi della normativa italiana si veda, *ex multis*, L. SCAFFARDI, *La data retention va in ascensore*, in *Forum di Quaderni Costituzionali*, 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, 2017; S. SIGNORATO, *Novità in tema di data retention*, in *Diritto Penale Contemporaneo*, 2018, p. 157 ss; E. ANDOLINA, *L'acquisizione nel processo penale dei dati "esteriori" delle comunicazioni telefoniche e telematiche*, Padova, 2018; I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di data retention*, in *Sistema Penale*, 2020, p. 183 ss.

[43] Sulla discussa e articolata giurisprudenza italiana in materia di *data retention*, considerata rappresentativa di una lettura «restrittiva degli standard garantistici enunciati dalla CGUE», al fine di «salvare la disciplina interna (..) ed evitare ipotesi di inutilizzabilità probatoria», si legga L. LUPARIA, *Data retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 2019, p. 757; ma anche G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accer-*

proccio, quindi, che risultava estremamente diverso da quello adottato da molti altri giudici nazionali a seguito soprattutto della sentenza *Tele2*, in quell'intenso e talvolta acceso dialogo multilivello che nei previ paragrafi è stato sottolineato. Alla luce invece della sentenza del marzo 2021 il Tribunale di Rieti ha proposto rinvio pregiudiziale alla CGUE avente ad oggetto l'interpretazione dell'art. 15 Direttiva *e-Privacy* con specifico riferimento alla disciplina dell'accesso e alle caratteristiche del previo controllo di un organo indipendente[44]. Sebbene tale domanda di pronuncia pregiudiziale sia stata poi ritirata dal Tribunale stesso dinnanzi alla sopraggiunta riforme normativa, di cui si parlerà a breve, essa rimane nondimeno rappresentativa di un "cambio di rotta" segnata innanzitutto della proposta, per la prima volta, di un rinvio in materia di *data retention* ai giudici sovranazionali e, di conseguenza, dal riconoscimento dell'impatto della giurisprudenza europea sulla disciplina italiana, già da più parti criticata[45] e rispetto alla quale una riforma indirizzata all'introduzione di maggiori salvaguardie e garanzie era da tempo invocata[46]. Proprio nelle more del procedimento dinanzi alla CGUE e forse anche grazie all'intenso dibattito e all'attenzione che le conseguenze della sentenza *H.K. c. Prokuratuur* avevano prodotto nel contesto nostrano, il legislatore italiano ha appor-

tamento dei reati, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Milano, 2019, p. 1599 ss.

[44] Si tratta della domanda di pronuncia pregiudiziale proposta dal Tribunale di Rieti nel procedimento penale a carico di G.B. e R.H., causa C-334/21. Sul punto si veda G. STAMPANONI BASSI, *Acquisizioni dei tabulati telefonici e telematici: il Tribunale di Rieti propone questione pregiudiziale alla CGUE*, in *Giurisprudenza Penale*, 13 maggio 2021; 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*, 2021, p. 1 ss.; 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.

[45] Ciò non solo per la forte somiglianza in termini di funzioni e ruoli tra il pubblico ministero estone, oggetto di rilievi nella pronuncia *H.K. c. Prokuratuur*, e il pubblico ministero italiano, ma anche per i diversi orientamenti mostrati dalle Corti italiane all'indomani della sentenza della CGUE del marzo 2021. Su tali profili, 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; 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; F. RESTA, *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna*, in *Giustizia Insieme*, 6 marzo 2021.

[46] Fra i molti, L. LUPARIA, *Data retention e processo penale*, cit. Anche il Garante per la protezione dei dati personali aveva posto particolare attenzione alla giurisprudenza della CGUE e ai suoi riflessi sulla disciplina italiana, spronando ad un intervento deciso del legislatore nazionale in materia di *data retention* e accesso ai metadati – Garante per la protezione dei dati personali, *Tecnica, protezione dei dati e nuove vulnerabilità. Relazione del Presidente Pasquale Stanzione*, 2021, p. 16 in particolare; ma anche *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*, inviata dal Garante il 2 agosto 2021 al Ministro della Giustizia, Prof.ssa Marta Cartabia –.

tato nel settembre 2021 talune modifiche al regime vigente, prestando però attenzione unicamente alla fase di accesso ai metadati, introducendo la previsione del carattere di gravità del reato quale limitazione all'acquisizione nonché provvedendo, sotto il profilo procedurale, ad una piena giurisdizionalizzazione dell'acquisizione di tali dati[47]. Nonostante questa importante modifica lasci intoccato il preoccupante obbligo di conservazione dei metadati fissato a 72 mesi (!)[48], senza dubbio la pronuncia della CGUE analizzata nel presente contributo ha avuto l'evidente effetto di spingere il legislatore italiano ad adottare riforme volte a fornire una più solida garanzia dei diritti alla vita privata e alla protezione dei dati e a delimitare i casi nei quali le esigenze securitarie e di repressione dei reati siano tali da giustificare un'ingerenza nella sfera privata.

Mentre l'Italia, dunque, non ha abbandonato il sistema di *bulk data retention*, pur limitando l'accesso ai metadati a specifiche condizioni, in Belgio è ravvisabile un approccio sostanzialmente differente: a seguito della pronuncia della Corte costituzionale che, per la seconda volta, ha dichiarato l'illegittimità della normativa nazionale in materia di conservazione e accesso ai dati di traffico e ubicazione[49], il Governo ha avviato un serio dibattito sull'opportunità di istituire una forma di *targeted data retention*[50]*,* rinunciando e superando così il ricorso ad una conservazione generalizzata ed indiscriminata per finalità di garanzia della sicurezza pubblica.

[47] Si fa riferimento al d.l. 30 settembre 2021, n. 132 e legge di conversione 23 novembre 2021, n. 178. Per una disamina dettagliata del contenuto di tale normativa, sia consentito il rimando a G. FORMICI, *'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*, in *Osservatorio costituzionale*, 2022, p. 125 ss.

[48] Anche il Garante per la protezione dei dati personali italiano, nel suo *Parere sullo schema di decreto-legge per la riforma della disciplina sull'acquisizione dei dati relativi al traffico telefonico e telematico a fini di indagine penale*, del 10 settembre 2021, doc. web 9704851, ha rilevato i limiti della disciplina nazionale rispetto ai principi statuiti dalla CGUE, esortando il legislatore ad intervenire anche in materia di conservazione dei metadati – e non solo sotto il profilo dell'accesso –.

[49] Il rinvio è all'*Arrêt* della Corte costituzionale belga n. 57 del 22 aprile 2021. Per un'analisi di tale pronuncia, si legga M-C. DE MONTECLER, *Conservation des données: la Court constitutionnelle belge donne sa lecture*, in *Dalloz. Le quotidien du Droit*, 28 aprile 2021; M. ROJSZCZAK, *The uncertain future of data retention laws in the EU*, cit.

[50] I *vice-Premiers Ministres* Van Quickenborne e De Sutter, insieme ai Ministri Dedonder e Verlinden, hanno presentato il 7 maggio 2021 un primo *avant-project de loi* relativo alla conservazione dei metadati e un *project d'arreté royal* volto a modificare la disciplina vigente in materia di accesso ai dati conservati per scopi giudiziari e di indagine. Tale progetto, approvato nell'inverno 2021 dal Consiglio dei Ministri belga e in corso di discussione dinnanzi al Parlamento, promuove non solo una forma di conservazione targettizzata, principalmente sulla base di criteri geografici, della durata massima di 12 mesi – ben lontana dagli attuali 72 mesi della disciplina italiana –, ma anche una regolamentazione fortemente distinta a seconda che la finalità perseguita sia quella di garanzia della sicurezza pubblica e contrasto ai reati gravi o quella di tutela della sicurezza nazionale, rispetto alla quale è stabilita

Ancora differente è poi il caso della Francia. Il Governo francese, infatti, all'indomani delle sentenza dell'ottobre 2020, ha invocato dinnanzi al Consiglio di Stato – giudice che aveva formulato il rinvio *La Quadrature du Net* e dinnanzi al quale il caso è stato ripreso – la necessità di ricorrere al concetto di "*identité constitutionnelle*"[51] quale eccezione capace di consentire al legislatore nazionale di discostarsi dai principi delineati dalla giurisprudenza della CGUE e di superare dunque i limiti da essa imposti in materia di *data retention*[52]. Sebbene una simile posizione non sia stata seguita dalla corte francese nella decisione al caso richiamato[53], essa appare nondimeno paradigmatica di un approccio di "resistenza" dei governi nazionali all'elevato livello di tutela dei diritti fondamentali imposto dai giudici di Lussemburgo.

Tale approccio, del resto, si evince anche dall'atteggiamento di taluni Stati membri nell'ambito della procedura legislativa avente a oggetto l'adozione di un nuovo Regolamento volta ad abrogare la ormai vetusta Direttiva *e-Privacy*[54]. In

una durata di conservazione più prolungata sulla base di livelli di minaccia individuati dall'*Organe de coordination pour l'analyse de la menace*.

[51] Su tale concetto, si veda D. ROUSEAU, *L'identité constitutionnelle, bouclier de l'identité nationale ou branche de l'etoile europeenne?*, in L. BURGORGUE-LARSEN (a cura di), *L'identité constitutionnelle saisie par les Juge en Europe*, Parigi, 2011, p. 89 ss.

[52] Come ben riassunto da Perlo, «nella memoria difensiva depositata tra il gennaio e l'aprile 2021, il governo si è dichiarato contrario all'applicazione del diritto dell'Unione poiché "la risposta della Corte di giustizia dell'Unione europea alle questioni pregiudiziali che le erano state poste ha manifesta-mente violato il principio di attribuzione previsto dall'articolo 5 del TUE e, in tal modo, la Corte si è intromessa nelle competenze degli Stati membri, secondo quanto è previsto dall'articolo 4 par. 2 TUE". Inoltre, tale risposta "non permette di garantire l'effettività degli obiettivi di valore costituzionale che sono la salvaguardia degli interessi fondamentali della Nazione, la prevenzione dei reati e la ricerca degli autori di reati, e la lotta contro il terrorismo"», N. PERLO, *La decisione del Consiglio di Stato francese sulla data retention: come conciliare l'inconciliabile*, in *Rivista di Diritti Comparati*, 2021, p. 168.

[53] Il riferimento è all'*Arrêt* n. 393099 del 21 aprile 2021, pronunciato dal *Conseil d'Etat* a solo un giorno di distanza dalla decisione della Corte costituzionale belga, sopra richiamata. Per approfondimenti su questa pronuncia e sul richiamo alla teoria degli atti *ultra vires*, si legga L. AZOULAI, D. RITLENG, *L'État c'est moi. Le Conseil d'État, la sécurité et la conservation des données*, in *Revue trimestrelle de droit européen*, 2, 2021, p. 349 ss.; J. ZILLER, *Il Conseil d'Etat si rifiuta di seguire il pifferaio magico di Karlsruhe*, in *CERIDAP*, 2021, p. 1 ss.; V. SIZAINE, J-P. FOEGLE, *Les fausses notes du souverainisme juridique*, in *La Revue des Droits de l'Homme*, giugno 2021, p. 1 ss.; M. AUDIBERT, *Conservation des données de connexion. Comment le Conseil d'État a sauvé la majorité des enquête judiciaires*, in *Vielle Juridique*, 96, 2021, p. 16 ss. Sebbene in questa sede non si voglia entrare nel dettaglio di tale pronuncia, quanto invece pare utile rilevare in maniera funzionale alle riflessioni sugli effetti della giurisprudenza della CGUE in materia di *data retention*, è come la posizione del Governo francese rifletta la resistenza mostrata dinnanzi alle pronunce della CGUE e del tentativo, anche mediante tale discusso richiamo alla teoria degli atti *ultra vires*, di scongiurare gli effetti dirompenti di una possibile dichiarazione di incompatibilità della normativa nazionale in materia di *data retention* rispetto al diritto dell'UE.

[54] Proposta di Regolamento del Parlamento europeo e del Consiglio relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva

questo complesso percorso normativo che dura ormai da anni e che pare ancora lontano dal trovare conclusione[55], proprio la disciplina della conservazione dei metadati per scopi securitari ha rappresentato un grande ostacolo al raggiungimento di una soluzione condivisa. Nella proposta finale, approvata dal COREPER il 10 febbraio 2021[56], è stato previsto, all'art. 2, co. 2, lett. a, che «the Regulation does not apply to activities, which fall outside the scope 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». Questa disposizione risulta particolarmente problematica poiché in aperto contrasto con la lettura sino ad ora promossa dalla CGUE, che ha ampiamente chiarito come, indipendentemente dalla finalità di sicurezza nazionale o sicurezza pubblica perseguita, la disciplina della conservazione e accesso ai metadati rientri nell'ambito di applicazione del diritto dell'UE laddove implichi un intervento – un trattamento – da parte di soggetti privati – i fornitori di servizi di telecomunicazione –, lasciando escluse solo le attività proprie dello Stato, quali le intercettazioni dirette da parte di autorità pubbliche[57]. La previsione normativa richiamata, unitamente alla riproposizione della disciplina derogatoria dell'art. 15 Direttiva *e-Privacy*, senza alcuna specificazione o limitazione chiara e precisa che rimandi ai principi delineati dalla CGUE, sono evidenza lampante del tentativo di taluni Stati membri di smarcarsi dai requisiti stabiliti dai giudici di Lussemburgo e di non voler limitare il ricorso allo strumento della conservazione generalizzata, soprattutto nell'ambito delicato della garanzia della sicurezza nazionale. Non è un caso che il Comitato europeo per la protezione dei dati abbia espresso preoccupazione quanto alla disciplina inserita nella proposta, ritenendo che il Regolamento «cannot derogate from the application of the latest CJEU case law. (…) With regard to the

2002/58/CE (regolamento sulla vita privata e le comunicazioni elettroniche), COM/2017/010 final.

55 I negoziati tra Commissione, Consiglio e Parlamento dell'UE hanno preso avvio il 20 maggio 2021 e sono al momento ancora in corso.

56 Il testo può essere reperito al seguente link: www.eur-lex.europa.eu.

57 «Quando gli Stati membri adottano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di servizi di tali comunicazioni, la tutela dei dati delle persone interessate rientra non già nell'ambito di applicazione della direttiva 2002/58 ma in quello del solo diritto nazionale», CGUE, *Privacy International*, cit., para. 48. Per quanto, sulla base di tale interpretazione, le "attività proprie degli Stati" escluse dall'ambito di applicazione del diritto dell'UE divengano dunque piuttosto limitate, anche per queste non bisogna dimenticare che sulla base del principio di leale collaborazione, così come letto dai giudici di Lussemburgo nella giurisprudenza sui c.d. "retained powers" degli Stati membri, questi ultimi sono chiamati ad esercitare le proprie prerogative considerando sempre il diritto dell'UE.

exclusion from the scope of application of the Regulation of processing activities by providers, the EDPB considers that such exclusion runs against the premise for a consistent EU data protection framework»[58].

Le sorti di questa proposta, e del suo possibile impatto sulla disciplina della *data retention*, si intrecciano anche con il difficile compito di cui la Commissione è stata investita dal Consiglio nel maggio 2019[59] e consistente nell'avvio di iniziative volte a raccogliere informazioni e procedere a consultazioni al fine di vagliare possibili soluzioni circa la disciplina della conservazione dei dati, compresa l'opportunità di adottare una nuova normativa europea in materia di *data retention*[60]. L'assenza di una disciplina *ad hoc* a livello sovranazionale e il persistente silenzio del legislatore europeo in tale delicato ambito hanno certamente rappresentato i fattori scatenanti di una forte disomogeneità di soluzioni normative impiegate dai singoli Stati membri e delle così numerose richieste di un intervento chiarificatore da parte della CGUE. Quest'ultima, adottando un attento al rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati approccio – pur nelle sue più recenti "inflessioni" –, ha fissato condizioni che rendono ora la predisposizione di una disciplina armonizzata europea in materia di *data retention* estremamente ardua da approvare: da un lato, gli Stati membri opporrebbero certamente una forte resistenza a una applicazione rigida dei criteri indicati dalla CGUE, anche dinanzi alle maggiori aperture sul fronte dell'utilizzo dello strumento nell'ambito della garanzia della sicurezza nazionale; dall'altro lato, una normativa più "flessibile" – volta cioè ad assicurare più ampie possibilità di applicazione della conservazione e dell'accesso ai metadati anche nel campo della sicurezza pubblica – rischierebbe di non superare indenne il successivo ed eventuale – ma altamente probabile – vaglio dei giudici di Lussemburgo, seguendo così le drammatiche sorti della previa Direttiva 2006/24/CE[61].

[58] Si rimanda allo *Statement 3/2021 on the e-Privacy Regulation* del 9 marzo 2021.

[59] Consiglio dell'UE, *Conclusioni sulla conservazione dei dati per finalità di lotta contro la criminalità*, n. 9336/19 del 27 maggio 2019.

[60] Dinnanzi a questa prospettiva e a seguito delle pronunce *Privacy International* e *La Quadrature du Net*, 40 ONG hanno indirizzato una lettera alla Commissione chiedendo da un lato di evitare qualsiasi tentativo di introdurre obblighi di conservazione dei metadati per scopi securitari a livello dell'UE, dall'altro invocando un intervento della Commissione volto ad avviare «infringement procedures to ensure that national data retention laws are repealed in all Member States concerned. Furthmore, we appeal to you to work towards an EU-wide ban on blanket and indiscriminate data retention practices that capture people's activities», www.statewatch.org.

[61] Del resto, una situazione simile si è già verificata con riferimento alla disciplina del trasferimento di dati verso Stati terzi: nelle pronunce *Schrems I* e *II* infatti la decisione di adeguatezza adottata dalla Commissione è stata per due volte invalidata dalla CGUE. Ciò a dimostrazione di quanto sia concreto il rischio che il bilanciamento effettuato dalla Commissione tra diritti fondamentali ed esigen-

Da questa breve ricostruzione degli scenari ancora aperti si comprende come la disciplina della *data retention* e dei suoi limiti rappresenti una sfida estremamente complessa, dagli sviluppi futuri tutt'altro che facilmente prevedibili.

Nonostante le criticità riscontrate nelle pronunce dell'ottobre 2020, che aprono a inediti scenari e le cui conseguenze devono essere certamente osservate con grande attenzione, la riportata giurisprudenza della CGUE ha senza dubbio il merito di aver prodotto, nell'ultimo decennio, effetti importanti nel contesto europeo e nazionale: sebbene in misura diversa e in maniera estremamente disomogenea, in taluni Stati membri i principi sanciti nella *data retention saga* hanno impresso alle scelte normative e alle vicende giurisprudenziali una spinta maggiormente garantista, nella direzione di una promozione di misure più tutelanti e attente alla salvaguardia dei diritti fondamentali dinnanzi alla tentazione di una sorveglianza massiva[62]. Anche laddove ciò non si è verificato appieno – si pensi contesto nostrano –, le pronunce dei giudici di Lussemburgo si sono rivelate nondimeno in grado di stimolare un dibattito – dottrinario, politico e civile – significativo e profondo sui rischi e sulle necessarie salvaguardie che devono circondare l'impiego di strumenti non solo fortemente invasivi rispetto ai diritti alla *privacy* e alla protezione dei dati ma anche capaci di incidere sul rapporto tra cittadini e potere pubblico. Certamente molto resta in attesa di essere determinato: il percorso normativo ancora in essere a livello sovranazionale, le reazioni degli Stati membri e quelle delle Istituzioni europee dinnanzi al probabile immobilismo di molte realtà nazionali, intenzionate a non adottare misure normative conformi ai principi delineati dalla CGUE, nonché l'interpretazione concreta delle condizioni eccezionali individuate nelle pronunce *La Quadrature du Net* e *Privacy International* come legit-

ze securitarie non coincida con quello maggiormente "garantista" promosso dai giudici di Lussemburgo.

[62] Quanto avvenuto ad esempio in Belgio, nel Regno Unito e in Italia, pur con modalità e tempi differenti dimostra un'influenza della giurisprudenza della CGUE sulle scelte dei legislatori e sulle pronunce delle Corti nazionali, portando, pur in misura differente, alla previsione di maggiori salvaguardie e tutele quanto alla disciplina della conservazione e dell'accesso ai metadati, limitando così l'ingerenza delle autorità di *law enforcement* nella sfera privata e accompagnando l'impiego di questo strumento invasivo con specifiche garanzie e limiti. Nonostante dunque non tutti i criteri e requisiti indicati dalle sentenze della CGUE siano stati recepiti negli ordinamenti nazionali – e talvolta, anzi, questi siano ben lontani dall'essere rispettati, come nel caso della lunghissima *data retention* prevista dal legislatore italiano –, senza dubbio nella gran parte dei casi esaminati le pronunce dei giudici di Lussemburgo hanno avuto l'effetto di rafforzare le tutele previste e "smorzare" i toni marcatamente pro-securitari promossi da governi e legislatori nazionali dinnanzi alle sempre più pressanti minacce alla sicurezza.

timanti il ricorso alla *bulk data retention*, tengono necessariamente viva la necessità di studiare e osservare gli sviluppi di un dibattito ancora aperto[63].

Un dibattito, quello delineato, che non può risolversi nel mero – e semplicistico – scontro tra posizioni pro-securitarie e difensori dei diritti fondamentali[64], e che dovrà cercare di giungere a una sintesi delle disomogenee e frammentarie posizioni e soluzioni adottate, promuovendo la determinazione di un punto di equilibrio – che dovrebbe essere definito da una specifica normativa e non più solo mediante l'intervento della CGUE o dei giudici nazionali[65] –, capace di fare i conti anche con la complessità della cornice del diritto dell'UE e del riparto di competenze tra UE e Stati membri in un ambito delicato quale quello della garanzia della sicurezza.

[63] Come affermato da Tzanou e Karyda, «the future will show whether Quadrature du Net opened the gate for an electronic Big Brother in Europe or led the way towards a less-absolute, more pragmatic (and perhaps less naïve) approach to surveillance», M. TZANOU, S. KARYDA, *Privacy International and Quadrature du Net: one step forward two steps back in the data retention saga?*, cit., p. 154.

[64] Sul tema del c.d. *trade-off* tra tutela della riservatezza e protezione dei dati da un lato e garanzia della sicurezza pubblica e nazionale, si leggano D. SOLOVE, *Nothing to hide. The false trade-off between privacy and security*, New Haven, 2011; T. OJANEN, *Rights-based review of electronic surveillance after Digital Rights Ireland and Schrems in the European Union*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Londra, 2017, p. 18 ss.; 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*, Baden-Baden, 2017, p. 137 ss.

[65] Del resto, «the reception of the judgments by the referring courts demonstrates that the interpretation provided by the Court of Justice will not contribute, in the short term, to developing universally accepted standard for the assessment of national retention rules», M. ROJSZCZAK, *National security and retention of telecommunications data in light of recent case law of the European Courts*, cit., p. 633, così che pare sempre più necessario e urgente un intervento legislativo che, per quanto difficile e complesso, sembra rappresentare l'unica soluzione in grado di garantire soluzioni armonizzate e una tutela dei diritti fondamentali omogenea nella materia in esame all'interno dei confini europei. Sull'importanza di una soluzione normativa si legga anche A. JUSZACZAK, E. SASON, *Recalibrating data retention in the EU. The jurisprudence of the CJEU – is this the end or the beginning?*, cit., p. 238 ss.

Finito di stampare nel mese di dicembre 2022
presso Grafica Elettronica srl, Napoli

Amministrazione
Editoriale Scientifica srl
80138 Napoli via San Biagio dei Librai, 39 tel. 081.5800459
info@editorialescientifica.com
www.editorialescientifica.com

Direttore responsabile
Pasquale De Sena

Legale rappresentante
Pasquale De Sena

Rivista annuale gratuita pubblicata esclusivamente on-line su
www.sidiblog.org
www.editorialescientifica.com

Registrazione
Tribunale di Napoli n. 3134/15 del 29 luglio 2015