Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2022, n. 2

EDITORIALE SCIENTIFICA
ES

Rivista quadrimestrale on line "Freedom, Security & Justice: European Legal Studies"
www.fsjeurostudies.eu
Editoriale Scientifica, Via San Biagio dei Librai, 39 - Napoli
CODICE ISSN 2532-2079 - Registrazione presso il Tribunale di Nocera Inferiore n° 3 del 3 marzo 2017

Indice-Sommario
2022, n. 2

Éditorial

Saggi e Articoli

Commenti e Note

IL DIFFICILE BILANCIAMENTO TRA SICUREZZA NAZIONALE E TUTELA DEI DIRITTI FONDAMENTALI NELLA "*DATA RETENTION SAGA*" DINANZI ALLA CORTE DI GIUSTIZIA UE

Giovanna Naddeo*

SOMMARIO: 1. Note introduttive in materia di "sicurezza nazionale" nel diritto dell'Unione europea. – 2. Il trattamento dei dati personali nel settore delle comunicazioni elettroniche "*per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica*": profili normativi. – 3. Evoluzione in senso diacronico della c.d. *data retention saga* dinanzi alla Corte di giustizia dell'Unione europea. – 4. (*segue*) La legittimazione della conservazione generalizzata dei dati alla luce dell'art. 4, par. 2, TUE. – 5. Sguardo alla giurisprudenza della Corte EDU: l'atteso epilogo dell'*affaire Big Brother Watch and Others v. the United Kingdom*. – 6. La sentenza della CGUE del 5 aprile 2022, C-140/20, *Commissioner of An Garda Síochána*. – 7. Osservazioni conclusive.

1. Note introduttive in materia di "sicurezza nazionale" nel diritto dell'Unione europea

L'interesse primario degli Stati membri a fronteggiare minacce sempre più complesse alla sicurezza dei propri cittadini[1] pone il tema della disciplina della conservazione dei metadati[2] derivanti da comunicazioni elettroniche – c.d. *data retention* – al centro di un

Articolo sottoposto a doppio referaggio anonimo.

* Dottoranda di ricerca, *curriculum* internazionalistico-europeo-comparato, Dipartimento di Scienze Giuridiche, Università degli Studi di Salerno. Indirizzo e-mail: gnaddeo@unisa.it.

[1] EUROPOL, *European Union Terrorism Situation and Trend Report*, Lussemburgo, 2021, disponibile qui.

[2] La Commissione europea per la Democrazia attraverso il Diritto (c.d. Commissione di Venezia) ha definito i metadati "*all data not part of the content of the communication*" nel *Report on the Democratic Oversight of Signals Intelligence Agencies* adottato il 20-21 Marzo 2015, par. 2, disponibile *online*. Nel dettaglio, il riferimento è ai "dati esterni" delle comunicazioni (anche detti tabulati telefonici e telematici) i quali attengono alla data, all'ora, alla durata, alla localizzazione, alle apparecchiature utilizzate e ai destinatari delle comunicazioni elettroniche. Sulle peculiarità di tale tipologia di dati personali, già le Conclusioni dell'Avvocato generale P. CRUZ VILLALÓN, presentate il 12 dicembre 2013, nelle cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd*, par. 74: "*I dati di cui trattasi […] non sono dati personali nel senso classico del termine, che si riferiscono a informazioni specifiche sull'identità delle persone, ma dati personali, per così dire, qualificati, il cui impiego può permettere di creare una mappatura tanto fedele quanto esaustiva di una parte importante dei comportamenti di una persona facenti strettamente parte della sua vita privata, se non addirittura un ritratto completo e preciso della sua identità privata*".

ISSN 2532-2079
DOI:10.26321/G.NADDEO.02.2022.09

intenso dialogo pregiudiziale tra giudici nazionali e Corte di giustizia dell'Unione europea teso ad individuare un punto di equilibrio nella dicotomia *privacy vs. security*.

Com'è noto, a metà tra gli obiettivi perseguiti dall'Unione e i principi su cui essa fonda l'esercizio delle proprie competenze, il Trattato sull'Unione europea (TUE) contempla una clausola – c.d. "identitaria"[3] – di salvaguardia della sovranità degli Stati membri in materia di sicurezza nazionale: l'art. 4, par. 2, TUE non soltanto pone a carico dell'Unione l'obbligo di rispettare "*le funzioni essenziali dello Stato*" (tra le quali sono elencate, a titolo esemplificativo, il mantenimento dell'ordine pubblico e la tutela della sicurezza interna), bensì specifica che "*la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro*". Introdotta con la riforma di Lisbona[4], tale disposizione riconosce l'intangibilità, da parte dell'Unione, della materia della sicurezza nazionale, quale prerogativa degli Stati membri inerente alla soggettività internazionale degli stessi[5]. A livello di diritto primario, ulteriori riferimenti alla sicurezza nazionale figurano tra i motivi di deroga alla libera circolazione dei fattori di produzione[6] o, ancora, nell'ambito dello spazio di libertà, sicurezza e giustizia: degna di menzione, in particolare, è la previsione di cui all'art. 72 TFUE, in virtù del quale le disposizioni del Titolo V della Parte III del Trattato non ostano "*all'esercizio delle responsabilità incombenti agli Stati*

[3] Cfr. Conclusioni dell'Avvocato generale M. POIARES MADURO, presentate l'8 ottobre 2008, nella causa C-213/07, *Michaniki AE*, par. 31. In dottrina, tra gli altri, L. S. ROSSI, *2, 4, 6 (TUE)...l'interpretazione dell'"Identity clause" alla luce dei valori fondamentali dell'UE,* in A.A. V.V., *Liber Amicorum Antonio Tizzano*, Torino, 2018, pp. 858-870; G. DI FEDERICO, *Il ruolo dell'art. 4, par. 2, TUE nella soluzione dei conflitti interordinamentali*, in *Quaderni costituzionali*, 2019, n. 2, pp. 333-357; F. CASOLARI, *Leale cooperazione tra Stati membri e Unione europea*, Napoli, 2020, in particolare pp. 203-210; P. FARAGUNA, *On the Identity Clause and Its Abuses: 'Back to the Treaty',* in *European Public Law,* 2021, vol. 27, n. 3, pp. 427-446. Sull'interpretazione di tale clausola quale "controlimite", che consenta al giudice nazionale di sottrarsi all'obbligo di disapplicazione nel caso di contrasto tra norma nazionale e diritto dell'Unione, in particolare nella c.d. "saga Taricco", R. PALLADINO, *I principi della legalità e della proporzionalità dei reati e delle pene nell'art. 49 della Carta dei diritti fondamentali dell'UE*, in A. DI STASI (a cura di), *Tutela dei diritti fondamentali e spazio europeo di giustizia*, Napoli, 2019, pp. 327-330. Ancora con riferimento all'ordinamento italiano merita segnalarsi la recentissima Corte Costituzionale, sentenza dell'11 marzo 2022, n. 67, in cui la Corte ha tributato al principio del primato del diritto dell'Unione europea e all'art. 4, parr. 2 e 3, TUE il riconoscimento di "*architrave su cui poggia la comunità di corti nazionali, tenute insieme da convergenti diritti e obblighi*" sottolineando che in tale sistema il sindacato di costituzionalità di cui all'art. 134 Cost., non è alternativo a un meccanismo diffuso di attuazione del diritto europeo, ma con esso confluisce nella costruzione di tutele sempre più integrate. A riguardo, B. NASCIMBENE, I. ANRÒ, *Primato del diritto dell'Unione europea e disapplicazione. Un confronto fra Corte costituzionale, Corte di Cassazione e Corte di giustizia in materia di sicurezza sociale*, in *Giustizia insieme*, 31 marzo 2022, reperibile *online.*

[4] M. C. BARUFFI, *Art. 4 TUE*, in F. POCAR, M. C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'Unione europea*, Padova, 2014, pp. 13-24. Sulla definizione di "sicurezza nazionale" nell'ordinamento giuridico europeo, S. PEERS, *National Security and European Law*, in *Yearbook of European Law*, 1999, pp. 363-404; di recente, F. FERRARO, *Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale,* in A.V. V.V., *Annali AISDUE*, vol. I, Bari, 2020, pp. 117-132.

[5] Per una recente ricostruzione del processo d'integrazione europea come mezzo per la soluzione della crisi dello Stato nazionale, L. F. PACE, *La natura giuridica dell'Unione europea: teorie a confronto*, Bari, 2021.

[6] Il riferimento è agli artt. 36, 45, 52 e 65 TFUE contenenti deroghe alla libera circolazione delle merci, dei lavoratori, al diritto di stabilimento e alla libera prestazione dei servizi, alla libera circolazione dei capitali. V., per tutti, L. DANIELE, *Diritto del mercato unico europeo e dello spazio di libertà, sicurezza e giustizia*, IV ed., Milano, 2019.

membri per il mantenimento dell'ordine pubblico e la salvaguardia della sicurezza interna". Come noto, tale disposizione riconosce agli Stati membri uno "*spazio di apprezzamento discrezionale*"[7] in relazione all'applicazione di misure nazionali derogatorie del diritto dell'Unione per ragioni di ordine pubblico e di sicurezza interna, purché tali misure siano limitate allo stretto necessario.

A tal riguardo, nella sentenza *Commissione europea c. Repubblica di Polonia, Ungheria e Repubblica ceca*, resa all'esito di una procedura di infrazione relativa all'inadempimento di obblighi di ricollocazione di richiedenti protezione internazionale, la Corte di giustizia ha evidenziato che l'art. 72 TFUE "*non conferisce agli Stati membri il potere di derogare a disposizioni di diritto dell'Unione mediante il mero richiamo agli interessi connessi al mantenimento dell'ordine pubblico e alla salvaguardia della sicurezza interna, ma impone loro di dimostrare la necessità di avvalersi della deroga prevista da tale articolo al fine di esercitare le loro responsabilità in tali materie*" [8], fermo restando che il riconoscimento di siffatte prerogative nazionali non consente di dedurre l'esistenza di "*una riserva generale […] che escluda dall'ambito di applicazione del diritto dell'Unione qualsiasi provvedimento adottato per motivi di ordine pubblico o di pubblica sicurezza. Ammettere una riserva del genere […] rischierebbe di compromettere la forza cogente e l'applicazione uniforme del diritto dell'Unione*"[9].

Tale orientamento ha trovato conferma nella recente sentenza *Valstybės sienos apsaugos tarnyba* in cui la Corte di giustizia ha descritto la "sicurezza nazionale" in questi termini: essa "*comprende la sicurezza interna di uno Stato membro e la sua sicurezza esterna e, pertanto, il pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali nonché la sopravvivenza della popolazione, come il rischio di perturbazioni gravi dei rapporti internazionali o della coesistenza pacifica dei popoli, o ancora il pregiudizio agli interessi militari, possono ledere la pubblica sicurezza*"[10].

Ancora nell'ambito del diritto primario, esigenze di sicurezza nazionale possono essere fatte valere nel porre limitazioni alle garanzie riconosciute ai singoli dalla Carta dei diritti fondamentali dell'Unione europea, purché nel rispetto della clausola limitativa generale di cui all'art. 52, par. 1, in base alla quale eventuali restrizioni dei diritti e delle libertà garantite dalla Carta devono essere previste dalle legge, rispettare il contenuto essenziale di tali diritti nonché, in conformità al principio di proporzionalità, risultare necessarie e rispondenti effettivamente a finalità di interesse generale dell'Unione o all'esigenza di proteggere i diritti e le libertà altrui. Pertanto, la stessa Corte di giustizia,

[7] Così A. ADINOLFI, *Art. 72 TFUE*, in F. POCAR, M. C. BARUFFI (a cura di), op. cit., p. 468.
[8] Corte di giustizia, sentenza del 2 aprile 2020, *Commissione c. Polonia, Ungheria e Repubblica ceca*, cause riunite C-715/17, C-718/17, C-719/17, par. 152. Per un commento alla sentenza, si rinvia a S. PROGIN-THEUERKAUF, V. ZUFFEREY, *Aucune justification du refus de participer au mécanisme temporaire de relocalisation de demandeurs d'une protection internationale*, in *European Papers*, 2020, vol. 5, n. 1, pp. 587-595; A. LANG, *Gli obblighi si rispettano: note intorno alla sentenza della Corte di giustizia dell'Unione europea del 2 aprile 2020, cause riunite C-715/17, C-718/17 e C-719/17, Commissione c. Polonia, Ungheria e Repubblica ceca,* in *Osservatorio AIC*, 2020, n. 6, pp. 260-289.
[9] *Ibidem*, par. 143.
[10] Corte di giustizia, sentenza del 30 giugno 2022, *Valstybės sienos apsaugos tarnyba*, causa C-72/22 PPU, par. 88.

nella pronuncia *J.N. c. Staatssecretaris van Veiligheid en Justitie*, ha riconosciuto che la tutela della sicurezza nazionale risponde non soltanto a un obiettivo di interesse generale, ma contribuisce parimenti alla tutela dei diritti e delle libertà altrui[11].

In tale contesto, l'utilizzo di mezzi tecnologici sempre più innovativi nell'ambito di azioni di prevenzione, indagine e lotta contro minacce alla sicurezza nazionale solleva interrogativi di stringente attualità in ordine all'alto grado di invasività nei diritti fondamentali della persona, e dunque alla legittimità di tali ingerenze nella sfera privata.

È alla luce di tali considerazioni che il presente contributo intende guardare, senza pretese di esaustività, al rapporto tra esigenze securitarie e tutela dei diritti fondamentali alla vita privata e alla protezione dei dati personali nel contesto di quella che è stata definita *"data retention saga"*[12] dinanzi alla Corte di giustizia - senza tuttavia prescindere dalla recente giurisprudenza della Corte europea dei diritti dell'uomo -, in cui va sempre più delineandosi una nozione di "sicurezza nazionale" distinta da quella di "sicurezza pubblica" tale da legittimare, a differenza della seconda, la conservazione generalizzata, preventiva e indiscriminata dei dati di traffico e di ubicazione degli utenti al fine di fronteggiare minacce alle funzioni essenziali e agli interessi primari dello Stato ma che, al contempo, rischia di aprire "*the gates for an electronic "Big Brother" in Europe*"[13].

2. La conservazione dei dati personali da parte dei fornitori di comunicazioni elettroniche "*per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica*": profili normativi

Da oltre un decennio, la disciplina della conservazione dei dati nel settore delle telecomunicazioni (c.d. *data retention*) è al centro di un intenso dibattito legislativo e giurisprudenziale. Com'è noto, per *data retention* si fa riferimento alla conservazione dei dati relativi al traffico[14] e all'ubicazione[15] (detti anche metadati) degli utenti - e dunque alla memorizzazione preventiva degli stessi - da parte di *service providers* al fine di un

[11] Corte di giustizia, Grande Sezione, sentenza del 15 febbraio 2016, *J.N. c. Staatssecretaris van Veiligheid en Justitie*, causa C-601/15 PPU, par. 53.

[12] A riguardo, E. CELESTE, *The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future*, in *European Constitutional Law Review*, 2019, n. 15, pp. 134-157; G. FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali*, Torino, 2021; A. JUSZCZAK, E. SASON, *Recalibrating Data Retention in the EU The Jurisprudence of the Court of Justice of the EU on Data Retention – Is this the End or is this the Beginning?,* in *Eucrim-The European Criminal Law Associations' Forum*, 2021, n. 4, pp. 238-266.

[13] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 21 maggio 2021, *Big Brother Watch and Others v. the United Kingdom*, ricorsi nn. 58170/13, 62322/14 e 24960/15, in particolare *Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque*, par. 60.

[14] Art 2, lett. *b)* della direttiva 2002/58/CE in cui per "*«dati relativi al traffico»: qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione*".

[15] Art. 2, lett. *c)* della direttiva 2002/58/CE in cui per "*«dati relativi all'ubicazione»: ogni dato trattato in una rete di comunicazione elettronica che indichi la posizione geografica dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico*".

successivo ed eventuale accesso da parte delle autorità di *law enforcement* per fini di giustizia[16]. Se per un verso il progresso scientifico-tecnologico contribuisce al potenziamento delle misure di polizia mediante la configurazione di sempre più pervasive metodologie di investigazione, dall'altro risulta altrettanto evidente come tali operazioni nascondano in sé rischi e pericoli al godimento dei diritti fondamentali dei singoli[17]: se non motivate da specifiche ragioni di indagine o dalla sussistenza di un nesso oggettivo con una minaccia alla sicurezza, tali metodologie rischiano di trasformarsi in una vistosa ingerenza nei diritti alla riservatezza e alla protezione dei dati, ma anche nell'esercizio delle libertà fondamentali in una società democratica[18] (*e.g.,* libertà di espressione e d'informazione, di riunione e associazione).

In coerenza con l'obiettivo di "*rafforzare la tutela dei diritti fondamentali, alla luce […] degli sviluppi scientifici e tecnologici, rendendo tali diritti più visibili*"[19], l'art. 8 della Carta dei diritti fondamentali riconosce in capo a ogni individuo "*il diritto alla protezione dei dati di carattere personale che lo riguardano*".

L'affermazione di una fattispecie giuridica autonoma e distinta dalla tutela della vita privata e familiare di cui all'art. 7 rappresenta, come è stato osservato, "*il culmine del percorso di codificazione e di costituzionalizzazione del diritto europeo alla protezione dei dati personali*"[20], segnando il passaggio da una dimensione essenzialmente negativa (obbligo di non-ingerenza da parte dei pubblici poteri, salvo nel caso di deroghe regolamentate dalla legge e limitate a quanto strettamente necessario in una società democratica) a una dimensione di carattere positivo (obbligo di adottare misure volte a rendere effettivo l'esercizio del diritto alla protezione dei dati personali)[21].

Siffatta interpretazione trova conferma nelle "Spiegazioni"[22] alla Carta: l'elencazione delle fonti normative alla base dell'art. 8 annovera, infatti, oltre all'art. 8 CEDU[23] e alla

[16] Per un'analisi del tema della *data retention* e delle libertà fondamentali incise da tale fenomeno, S. MARCOLINI, *L'istituto della* data retention *dopo la sentenza della Corte di Giustizia del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA (a cura di), *Trattati giuridici - Cybercrime*, Milano, 2019, pp. 1579-1582.

[17] Sul bilanciamento tra esigenze di accertamento e repressione dei reati e tutela penale di "tradizionali e nuovi beni giuridici nell'era digitale", R. FLOR, S. MARCOLINI, *Dalla* data retention *alle indagini ad alto contenuto tecnologico*, Torino, 2022.

[18] Con specifico riferimento alla recente esperienza di una sorta di "sorveglianza di massa" nella società democratica europea per motivi di protezione della salute pubblica, e specificatamente di contrasto al Covid-19, S. CRESPI, *Applicazione di tracciamento* Immuni *tra normativa nazionale e diritto UE in materia di protezione dei dati personali*, in *Freedom, Security & Justice: European Legal Studies*, 2020, n. 3, pp. 49-73.

[19] Preambolo alla Carta dei diritti fondamentali dell'Unione europea, 4° cpv.

[20] Così O. POLLICINO, M. BASSINI, *Art. 8*, in S. ALLEGREZZA, R. MASTROIANNI, F. PAPPALARDO, O. POLLICINO, O. RAZZOLINI (a cura di), *Carta dei diritti fondamentali dell'Unione europea*, Milano, 2017, p. 135.

[21] *Ibidem*, p. 136. Cfr. S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma nel sistema UE di protezione dei dati,* in *Rivista Italiana di Diritti Pubblico Comunitario*, 2015, nn. 3-4, in particolare p. 822.

[22] Sul valore delle "Spiegazioni" quale strumento d'interpretazione della Carta dei diritti fondamentali, A. DI STASI (a cura di), *Tutela dei diritti fondamentali e spazio europeo di giustizia*, cit., pp. 65-69.

[23] Cfr. L. TOMASI, *Art. 8*, in S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (a cura di), *Commentario breve alla CEDU - Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali*, Padova, 2012, pp. 297-368. Sui profili distintivi del diritto alla riservatezza e del diritto alla protezione dei

Convenzione del Consiglio d'Europa *sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere* personale[24], anche l'attuale art. 16 TFUE[25], nonché due fonti di diritto dell'Unione europea di secondo livello: la direttiva 95/46/CE (oggi sostituita dal regolamento (UE) 2016/679[26]) e il regolamento (CE) 45/2001 (oggi, regolamento (UE) 2018/1725[27]).

Ordunque, filo conduttore delle pronunce della Corte di giustizia in materia di *data retention* concerne l'interpretazione dell'art. 15 della direttiva 2002/58/CE[28] (c.d. direttiva *e-Privacy*): a seguito dell'annullamento della direttiva 2006/24/CE[29] (c.d.

---

dati personali, si rinvia a J. KOKOTT, C. SOBOTTA *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR,* in *International Data Privacy Law*, 2013, vol. 3, n. 4, pp. 222-228.

[24] Convenzione del Consiglio d'Europa *sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale* del 28 gennaio 1981 (c.d. Convenzione 108). Come noto, si tratta dell'unico strumento internazionale giuridicamente vincolante in materia di protezione dei dati, di recente interessato da un intervento di "modernizzazione". In particolare, in materia di *data retention*, l'art. 11 del Protocollo n. 223 di emendamento alla Convenzione (aperto alla firma dal 2018) amplia il contenuto dell'attuale art. 9, prevedendo che restrizioni ai diritti fondamentali sono consentite purché tali misure siano previste dalla legge, rispettino l'essenza dei diritti e delle libertà fondamentali e costituiscano "*una misura necessaria e proporzionata in una società democratica per: a) la protezione della sicurezza nazionale, della difesa, della sicurezza pubblica e di importanti interessi economici e finanziari dello Stato, l'imparzialità e l'indipendenza del potere giudiziario o la prevenzione, l'investigazione e il perseguimento di reati e l'esecuzione di sanzioni penali e altri obiettivi essenziali di interesse pubblico generale*". Ad oggi il Protocollo è stato ratificato da diciassette Stati Contraenti, tra i quali figura l'Italia (Legge 22 aprile 2021, n. 60). Tra gli Stati non-membri del Consiglio d'Europa, il suddetto Protocollo è stato ratificato da Uruguay e Mauritius, quest'ultimo uno dei cinque Stati del continente africano Parti della Convenzione. Sull'influenza esercitata dalla Convenzione 108 e dal diritto dell'Unione europea negli ordinamenti giuridici africani, v. G. GREENLEAF, B. COTTIER, *International and regional commitments in African data privacy laws: A comparative analysis*, in *Computer Law & Security Review,* 2022, vol. 44, n. 105638.

[25] Cfr. F. ROSSI DAL POZZO, *La giurisprudenza della Corte di giustizia sul trattamento dei dati personali*, in A.A. V.V., *Quaderni AISDUE*, vol. I, Bari 2020, pp. 70-71, secondo il quale l'art. 16 TFUE ha prodotto "*l'effetto di introdurre una nuova autonoma competenza dell'Unione che consente di superare in modo definitivo i dubbi sull'ambito di applicazione della disciplina derivata*". Al riguardo, si veda la Dichiarazione n. 20 allegata all'atto finale della Conferenza intergovernativa che ha adottato il trattato di Lisbona firmato il 13 dicembre 2007, *Dichiarazione relativa all'articolo 16 del trattato sul funzionamento dell'Unione europea* secondo la quale *"[…] ogniqualvolta le norme in materia di protezione dei dati personali da adottare in base all'articolo 16 possano avere implicazioni dirette per la sicurezza nazionale, si dovrà tenere debito conto delle caratteristiche specifiche della questione. Rammenta che la legislazione attualmente applicabile* (*vedasi in particolare la direttiva 95/46/CE) prevede deroghe specifiche al riguardo",* in GUUE, C 115 del 9 maggio 2008, p. 345.

[26] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)*, in GUUE, L 119 del 4 maggio 2016, pp. 1-88.

[27] Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, *sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE*, in GUUE, *L 295 del 21 novembre 2018, pp. 39-98.*

[28] 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)*, in GUUE, L 201 del 31 luglio 2002, pp. 37-47.

[29] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, *riguardante la*

direttiva *data retention*) - la quale prevedeva un generale obbligo di conservazione di dati di telefonia e di accesso ad *Internet*, per un arco temporale da sei a ventiquattro mesi, per finalità di accertamento e perseguimento di reati qualificati come "gravi" da ciascuno Stato membro nella propria legislazione nazionale -, il suddetto art. 15 ha acquisito un'indubbia centralità in quanto, allo stato, costituisce l'unica disposizione in materia di *data retention* nell'ordinamento giuridico dell'Unione europea[30].

Nel dettaglio, tale disposizione accorda agli Stati membri la possibilità di adottare misure legislative che deroghino al divieto generale di memorizzazione dei dati degli utenti in assenza del loro consenso[31] qualora tali misure costituiscano "*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*".

La proposta di regolamento che intende abrogare la direttiva 2002/58[32] è attualmente in fase di negoziazione tra Consiglio e Parlamento europeo[33]. Tale proposta si inserisce nel pacchetto di riforme che nell'ultimo periodo hanno profondamente mutato il quadro normativo europeo[34] al fine di rispondere alle nuove sfide che il progresso tecnologico

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, in GUUE, L 105 del 13 aprile 2006, pp. 54-63. Tale direttiva fu adottata in seguito agli attentati consumatisi a Madrid e Londra tra il 2004 e il 2005, allo scopo di armonizzare le discipline nazionali in materia di conservazione dei dati esterni delle comunicazioni elettroniche. Per una ricostruzione, v., per tutti, M. NINO, *Terrorismo internazionale*, *privacy e protezione dei dati personali*, Napoli, 2012.

[30] Con riferimento alla *data retention* quale materia propria dell'ordinamento giuridico dell'Unione, F. TORRE, Data retention*: una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della Corte di giustizia 2 marzo 2021, C-746/18)*, in *Consulta Online*, 2021, n. 2, pp. 615-628, secondo cui "*I giudici del Kirchberg hanno dato alla conservazione e all'accesso dei dati esteriori la dignità che tale materia merita, fuggendo dallo sterile raffronto "qualitativo" con la disciplina delle intercettazioni del contenuto telefonico. La* data retention *è dotata, a livello europeo, di un'indipendenza e di un'autonomia strutturale, impensabili per la giurisprudenza interna"*.

[31] Il riferimento è all'art. 5 ("*Riservatezza delle comunicazioni*"), ma si vedano anche gli artt. 6 ("*Dati sul traffico*"), 8 ("*Presentazione e restrizione dell'identificazione della linea chiamante e collegata*") e 9 ("*Dati relativi all'ubicazione diversi dai dati relativi al traffico*") della direttiva 2002/58/CE. La Corte di giustizia ha ripetutamente affermato che con l'adozione di tale direttiva *"il legislatore dell'Unione ha concretizzato i diritti sanciti dagli articoli 7 e 8 della Carta, di modo che gli utenti dei mezzi di comunicazione elettronica hanno il diritto di attendersi, in linea di principio, che le loro comunicazioni e i dati a queste correlati, in mancanza del loro consenso, rimangano anonimi e non possano essere registrati",* in sentenza del 6 ottobre 2020, *La Quadrature du Net, Ordre des barreaux francophones et germanophone e al.,* cause riunite C-511/18, C-512/18 e C-520/18, par. 109.

[32] *Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications),* Bruxelles, 10 febbraio 2021. In dottrina, tra gli altri, M. ROJSZCZAK, *The uncertain future of data retention laws in the EU: Is a legislative reset possible?*, in *Computer Law & Security Review*, 2021, vol. 41, n. 105572.

[33] Comunicato stampa del Consiglio n. 81/21 del 10 febbraio, 2021, disponibile *online*.

[34] Cfr. COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni, *Un approccio globale alla protezione dei dati personali nell'Unione europea,* Bruxelles, 4 novembre 2010, COM(2010) 609 def.

pone rispetto al diritto alla tutela dei dati personali[35] e, in generale, di contribuire al rafforzamento del ruolo dell'Unione europea quale *global standard-setter* globale in materia di *e-Privacy*[36]. Tuttavia, tale proposta di regolamento, approdata all'esame dei co-legislatori europei dopo oltre quattro anni di negoziati, all'art. 2, par. 2, lett. *a)* ("*Material Scope*") prevede 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*". Pertanto, l'art. 11 ("*Restrictions*") della proposta licenziata non contempla, tra le ipotesi di deroghe e restrizioni ai diritti degli utenti, la finalità di sicurezza nazionale.

Come osservato dallo *European Data Protection Board*[37], tale orientamento *"runs against the premise for a consistent EU data protection framework"*, risultando in aperto contrasto con il consolidato orientamento della Corte di giustizia: nelle pronunce sulla materia, infatti, la Corte ha affermato che, nel caso di trattamenti di dati da parte di soggetti privati (quali sono, appunto, i fornitori di servizi di comunicazione elettronica) dettati da esigenze securitarie, la disciplina di tali trattamenti e della successiva acquisizione degli stessi rientra nell'ambito di applicazione del diritto dell'Unione. Tale lettura è maturata nel contesto di rinvii pregiudiziali successivi all'invalidazione della direttiva 2006/24 e in cui la Corte è stata chiamata dai giudici nazionali a pronunciarsi "*sulle condizioni alle quali è costituzionalmente possibile per l'Unione europea prevedere una limitazione all'esercizio dei diritti fondamentali nel senso particolare di cui all'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea, mediante una direttiva e i relativi provvedimenti nazionali di recepimento*"[38].

[35] La dottrina sull'argomento è ampissima. Per un primo tentativo di ricostruzione nella dottrina italiana, F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016; S. SICA, V. D'ANTONIO, G. M. RICCIO (a cura di), *La nuova disciplina europea della privacy,* Padova, 2016; G. M. RUOTOLO, *Scritti di diritto internazionale ed europeo dei dati,* Bari, 2020. Sulla progressiva costruzione di un quadro giuridico sulla *cybersecurity*, tra gli altri, D. MARRANI, *Il coordinamento delle politiche per la* cybersecurity *dell'UE nello spazio di libertà, sicurezza e giustizia*, in *Freedom, Security & Justice: European Legal Studies*, 2021, n. 1, pp. 77-98.

[36] Così A. GOLIA, *La sovranità europea alla prova del digitale. I nodi della* data retention *alla luce di una decisione del Consiglio di Stato francese*, in *Rassegna di diritto pubblico europeo*, 2021, n. 2, p. 441.

[37] *Statement* n. 3/2021 *on the ePrivacy Regulation* dello *European Data Protection Board* del 9 marzo 2021, disponibile *online*.

[38] Conclusioni dell'Avvocato generale P. CRUZ VILLALÓN, *Digital Rights Ireland Ltd*, cit., par. 1.

3. Evoluzione in senso diacronico della c.d. *data retention saga* dinanzi alla Corte di giustizia dell'Unione europea

Sotto il profilo giurisprudenziale, il primo tassello posto dalla Corte di giustizia nella c.d. *data retention saga* risale al 2014[39], nel caso *Digital Rights Ireland*[40]: in tale pronuncia, la Corte, adita in via pregiudiziale dalla Corte suprema irlandese e dalla Corte costituzionale austriaca[41], dichiarava l'invalidità della direttiva 2006/24/CE previo

[39] EUROPEAN DATA PROTECTION SUPERVISOR, *Annual Report 2014*, ove il Garante europeo descrive tale anno "*watershed, the moment the rights to privacy and to the protection of personal data as set down in the Charter of Fundamental Rights moved decisively from legal theory to reality*". Nel 2014, infatti, la Corte di Lussemburgo ha reso numerose pronunce in materia di *data protection:* sentenza del 13 maggio 2014, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, causa C-131/12; sentenza del 19 giugno 2014, *Pharmacontinente-Saúde e Higiene SA c. Autoridade Para As Condições do Trabalho,* causa C-683/13; *sentenza del* 17 luglio 2014, cause riunite C-141/12 e C-372/12, *Y.S. v. Minister voor Immigratie, Integratie en Asiel*; sentenza del 2 dicembre 2014, *Ryneš v. Úřad pro ochranu osobních údajů,* causa C-212/12. Nello stesso anno perveniva alla cancelleria della Corte una domanda di pronuncia pregiudiziale in materia di trasferimento di dati personali verso Stati terzi la cui sentenza ha sin da subito assunto il rango di *leading case* della materia*:* si tratta della sentenza del 6 ottobre 2015, *Schrems c. Data Protection Commissioner,* C-362/14, alla quale nel 2020 segue la sentenza della Grande Camera del 16 luglio 2020, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems*, causa C-311/18, ai più nota come *Schrems II.* In quanto esula dal presente contributo la questione del trasferimento di dati personali da e verso Stati terzi, si rimanda, tra gli altri, a M. NINO, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della Corte di giustizia UE,* in *Il Diritto dell'Unione europea,* 2016, n. 4, pp. 755-787; I. OLDANI, *The Impact of the Schrems II Judgment on International Data Transfers*, in *Quaderni di SIDIblog,* 2020, vol. 7, pp. 547-563.

[40] Corte di giustizia, Grande Sezione, sentenza dell'8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications e al.*, cause riunite C-293/12 e C-594/12. In dottrina, tra gli altri, S. PEERS, *The data retention judgment: The CJEU prohibits mass surveillance*, in *EU Law Analysis*, 8 aprile 2014, reperibile *online*; O. LYNSKEY, *Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly,* in *European Law Blog,* 8 aprile 2014, reperibile *online;* F. VECCHI, *L'ingloriosa fine della direttiva* Data retention*, la ritrovata vocazione costituzionale della Corte di giustizia e il destino dell'art. 132 del Codice della privacy*, in *Diritti comparati*, 10 giugno 2014; G. TIBERI, *La Corte di giustizia sulla conservazione dei dati: la protezione dei diritti fondamentali nel «dopo-Lisbona»,* in *Quaderni costituzionali,* 2014, n. 3, pp. 719-721; T. OJANEN*, Privacy Is More Than Just a Seven-Letter Word: The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance: Court of Justice of the European Union Decision of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others,* in *European Constitutional Law Review,* 2014, vol. 10, n. 3, pp. 528-541; F. FABBRINI, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, in *Harvard Human Rights Journal*, 2015, vol. 28, pp. 65-95.

[41] Il primo rinvio pregiudiziale (C-293/12) originava da un ricorso proposto da una società irlandese impegnata nella protezione dei diritti umani e relativo alla presunta illegittimità costituzionale del *Communications (Retention of Data) Act 2011*, legge nazionale di recepimento della direttiva 2006/24/CE. Nella stessa sede, la ricorrente aveva invitato il giudice *a quo* a sollevare dinanzi alla Corte di Lussemburgo questione pregiudiziale di validità della suddetta direttiva, lamentando la presunta contrarietà della stessa agli *standard* di tutela accordati dalla Carta dei diritti fondamentali e dalla CEDU. Analogamente, il secondo rinvio pregiudiziale (C-594/12) muoveva da un ricorso per l'annullamento dell'art. 102 *bis* del *Telekommunikationsgesetz*, disposizione nazionale di recepimento della medesima direttiva, nella parte in cui prevedeva un obbligo per il *service provider* di conservazione generalizzata dei dati, a detta del ricorrente, contrario all'art. 8 della Carta dei diritti fondamentali. In verità, la Corte di giustizia nella sentenza del 10 febbraio 2009, *Irlanda c. Parlamento europeo e Consiglio*, causa C-301/96, era stata già

accertamento della violazione del principio di proporzionalità di cui all'art. 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea.

Lo scrutinio della Corte muoveva dalla qualificazione dell'ingerenza - ritenuta "*di vasta portata e particolarmente grave*"[42] - perpetrata dalla cd. *bulk data retention* nella sfera di riservatezza del singolo, in ragion del fatto che le specifiche categorie dei dati di telefonia e di ubicazione consentono, nel loro complesso, 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*"[43], suscitando negli interessati "*la sensazione che la loro vita sia oggetto di costante sorveglianza*"[44]. Orbene, se per un verso tale intrusione non era ritenuta lesiva del nucleo essenziale degli artt. 7 e 8 della Carta e la *ratio* sottesa a tale intrusione era considerata di per sé legittima (in quanto strumentale al mantenimento della sicurezza nello spazio europeo, e, in definitiva, volta a garantire il diritto fondamentale di ogni persona *"alla libertà e alla sicurezza"* di cui al richiamato art. 6 della Carta[45]), tuttavia la direttiva impugnata non superava il *test* di proporzionalità applicato dalla Corte, in ragione della mancata previsione, da parte del legislatore europeo, di garanzie procedurali e sostanziali idonee a scongiurarne il rischio di usi illeciti[46]. Pertanto, la grave portata dell'ingerenza nei diritti fondamentali e la carenza di disposizioni che potessero effettivamente limitare tale ingerenza allo stretto necessario conducevano la Corte di

investita di un ricorso d'annullamento che, aveva riguardato "*unicamente sulla scelta del fondamento normativo e non già su un'eventuale violazione dei diritti fondamentali derivanti dalle ingerenze nell'esercizio del diritto al rispetto della vita privata, che la direttiva 2006/24 implica*", par. 57, richiamato nelle Conclusioni dell'Avvocato generale P. C. VILLALÓN presentate il 12 dicembre 2013, nella causa C-293/12, *Digital Rights Ireland Ltd contro Minister for Communications, Marine and Natural Resources e al*, par. 82. Inoltre, vale la pena evidenziare come già in sede di recepimento della direttiva 2006/24 erano sorti numerosi interrogativi in relazione alle gravi ingerenze perpetrate dalla cd. *bulk data retention* nel godimento dei diritti fondamentali garantiti dalla Carte costituzionali e dalla Carta dei diritti fondamentali, interrogativi poi sfociati in numerosi ricorsi promossi dinanzi alle Corti costituzionali di Bulgaria, Romania, Germania, Repubblica Ceca e Cipro. Per approfondire le pronunce richiamate, si rinvia a G. FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali,* op. cit., pp. 63-68.

[42] Corte di giustizia, *Digital Rights Ireland*, cit., par. 37.

[43] *Ibidem,* par 27.

[44] *Ibidem*, par. 37.

[45] *Ibidem*, par. 42.

[46] Tra i fattori di criticità evidenziati dalla Corte di giustizia nella disciplina della direttiva 2006/24 vi erano la previsione di un sistema di conservazione dei dati complessivamente riguardante "*qualsiasi persona e qualsiasi mezzo di comunicazione elettronica nonché l'insieme dei dati relativi al traffico, senza operare alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi*" (par. 57); la mancata previsione di criteri oggettivi tali da circoscrivere l'accesso agli stessi, da parte delle autorità nazionali competenti, soltanto per finalità di prevenzione, di accertamento o di indagini penali riguardanti reati sufficientemente gravi; la mancata previsione di criteri geografici e temporali per delimitare la platea dei soggetti interessati.

giustizia a dichiarare, per la prima volta nella sua giurisprudenza, l'invalidità *ex tunc*[47] di un atto di diritto derivato dell'Unione per contrasto con la Carta dei diritti fondamentali[48].

I profili di incertezza interpretativo-applicativi[49] lasciati aperti dalla sentenza *Digital Rights Ireland* venivano in parte colmati con la pronuncia resa nel caso *Tele2 Sverige*[50]: in tale occasione, infatti, la Corte affermava la sostanziale incompatibilità con il diritto dell'Unione dell'obbligo di conservazione universale dei metadati, seppur giustificata da esigenze di pubblica sicurezza. Viceversa, la Corte riconosceva la legittimità di una conservazione, a titolo preventivo, di tipo "mirato" (o anche detto "targettizzato") per finalità di lotta contro la criminalità grave, e in particolare contro la criminalità organizzata e il terrorismo, "*a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista, limitata allo stretto necessario*"[51]. E a tal proposito, la Corte individuava gli elementi minimi indispensabili che la normativa nazionale era tenuta a prevedere per il superamento del *test* di proporzionalità, ovverosia criteri oggettivi che consentissero di delimitare il periodo di tempo, la zona geografica e la cerchia di persone interessate. Anche in relazione al profilo dell'accesso ai dati - specificatamente consentito se motivato da finalità di lotta alla criminalità *grave*[52] -, la Corte ribadiva la necessità di disposizioni nazionali chiare e

[47] La Corte di giustizia non ha accolto il suggerimento dell'Avvocato generale VILLALÓN di "*sospendere gli effetti della constatazione dell'invalidità della direttiva 2006/24 per dar tempo al legislatore dell'Unione di adottare le misure necessarie per porre rimedio all'invalidità accertata",* par. 58, rimettendo sostanzialmente agli Stati membri la scelta se abrogare le leggi di trasposizione della direttiva invalidata oppure modificare tali leggi alla luce dell'interpretazione fornita dalla Corte di giustizia.

[48] Cfr. O. POLLICINO, *I diritti digitali: il caso dell'*enforcement *della* digital privacy, in C. AMALFITANO, M. D'AMICO, S. LEONE (a cura di), *La Carta dei diritti fondamentali dell'Unione europea nel sistema integrato di tutela. Atti del convegno svoltosi nell'Università degli Studi di Milano a venti anni dalla sua proclamazione*, Torino, 2022, p. 396.

[49] In estrema sintesi, sul piano legislativo, tali dubbi riguardavano se la conservazione massiccia di dati fosse *di per sé* una misura incompatibile con il diritto dell'Unione. Per una ricostruzione, G. FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali*, cit., pp. 76-87.

[50] Corte di giustizia, Grande Sezione, sentenza del 21 dicembre 2016, *Tele2 Sverige e al.*, cause riunite C-203/15 e C-698/15. In estrema sintesi, nel primo caso (C-203/15) la Corte di giustizia era stata adita in via pregiudiziale nell'ambito di un contezioso scaturito dal rifiuto opposto il giorno successivo alla pubblicazione della sentenza *Digital Rights Ireland* da parte di un fornitore di servizi di comunicazione elettronica alle autorità svedesi di continuare a conservare i dati di traffico e di ubicazione degli utenti, sulla base della presunta contrarietà della disciplina svedese (di recepimento della direttiva 2006/24) al diritto dell'Unione. Il secondo rinvio pregiudiziale (C-698/15) originava da un ricorso promosso nel Regno Unito da un gruppo di ricorrenti vertente sulla supposta illegittimità dell'art. 1 del *Data Retention and Investigatory Powers Act 2014*: tale norma, infatti, riconosceva in capo al Ministro dell'Interno piena discrezionalità nell'emissione di cd. "avvisi di conservazione", al fine di imporre agli operatori di telecomunicazione la conservazione, totale o parziale, dei dati degli utenti per esigenze di sicurezza nazionale, ordine pubblico, prevenzione e repressione della criminalità o di qualsiasi altra finalità, non prevedendo l'autorizzazione preventiva da parte dell'autorità giudiziaria o di un'autorità amministrativa indipendente. Sulla sentenza, F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa: dai giudizi di costituzionalità rivolti alla disciplina UE al giudizio della Corte di giustizia rivolto alle discipline nazionali,* in *DPCE online*, 2017, n. 2, pp. 349-357; E. SPILLER, *La sentenza Tele2 Sverige: verso una* digital rule of law *europea*?, in *Ianus,* 2017, nn. 15-16, pp. 279-302.

[51] Corte di giustizia, *Tele2 Sverige*, cit., par. 108.

[52] "*In materia di prevenzione, ricerca, accertamento e perseguimento di violazioni penali, soltanto la lotta*

precise relative alle circostanze e alle condizioni, sostanziali e procedurali[53], alle quali i fornitori di servizi di comunicazione elettronica fossero tenuti, all'occorrenza, a trasmettere alle autorità competenti i dati raccolti.

Merita evidenziare come tali approdi abbiano trovato ulteriore applicazione nel parere *ex* art. 218, par. 11, TFUE reso nel 2017 sull'accordo previsto tra Unione europea e Canada sul trasferimento e trattamento dei dati del codice di prenotazione (cd. *PNR, Passenger Name Records*)[54]. Chiamata a pronunciarsi per la prima volta sulla compatibilità di un progetto di accordo internazionale con la Carta dei diritti fondamentali[55], la Corte applicava il *test* di stretta necessità secondo gli *steps* già collaudati nelle pronunce fin qui esaminate: esaminata la gravità delle ingerenze nel nucleo essenziale dei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali, la Corte valutava dapprima la legittimità di tale interferenza in relazione al perseguimento di finalità di interesse generale dell'Unione - nel caso di specie, la garanzia della pubblica sicurezza e la lotta al terrorismo e ad altri gravi reati di natura transnazionale (allo scopo ultimo di tutelare il diritto di ogni persona alla sicurezza come riconosciuto dall'art. 6 della Carta[56]) - e poi la stretta necessità delle interferenze con i diritti fondamentali, indagando il grado di chiarezza e di precisione delle disposizioni relative alla conservazione e all'accesso ai dati dei passeggeri da parte delle

---

contro la criminalità grave è idonea a giustificare un simile accesso ai dati conservati" (par. 115). Merita evidenziare come tale riferimento non derivasse dal dettato normativo dell'art. 15 della direttiva 2002/58, bensì dall'interpretazione fornita dalla Corte di giustizia sulla base della richiamata sentenza *Digital Rights Ireland* che aveva invalidato, tra gli altri, l'art. 1 della direttiva 2006/24 ove il riferimento ai reati gravi era contemplato. Tuttavia, sul significato e gli elementi determinanti la "gravità" dei reati restava silente, rimettendone la disciplina ai legislatori nazionali. Cfr. X. TRACOL, *The judgment of the Grand Chamber dated 21 December 2016 in the two joint Tele2 Sverige and Watson cases,* in *Computer law & security review,* 2017, vol. 33, pp. 541-552, in cui si propone di prendere a riferimento le "*sfere di criminalità*" contemplate all'art. 83, par. 1, TFUE (terrorismo, tratta degli esseri umani e sfruttamento sessuale delle donne e dei minori, traffico illecito di stupefacenti, traffico illecito di armi, riciclaggio di denaro, corruzione, contraffazione di mezzi di pagamento, criminalità informatica e criminalità organizzata).

[53] Tra questi, la necessaria previsione di criteri oggettivi relativi all'individuazione della platea dei destinatari interessati, con riferimento non solo ai "*dati di persone sospettate di progettare, di commettere o di aver commesso una violazione grave, o anche di essere implicate in una maniera o in un'altra in una violazione siffatta*", ma anche ai dati di altre persone le quali potessero fornire "*un contributo effettivo*" alla lotta contro minacce alla sicurezza nazionale, della difesa o della sicurezza pubblica; la garanzia di un controllo preventivo effettuato da autorità, amministrative o giudiziarie, indipendenti del rispetto di siffatti criteri e, in generale, del rispetto dei livelli di protezione garantiti dall'Unione.

[54] Corte di giustizia, Grande Sezione, Parere 1/15 reso il 26 luglio 2017. Per un primo commento, tra gli altri, M. LEFFI, *L'Accordo PNR tra Canada e UE non prende il volo. Nota sul parere della Corte di giustizia europea a proposito del trasferimento dei dati del codice di prenotazione,* in *Medialaws,* 2017, n. 1, pp. 134-138; G. TIBERI, *Il parere 1/15 della Corte di Giustizia: la prima volta di uno scrutinio di compatibilità di un accordo internazionale con la Carta dei diritti fondamentali*, in *Quaderni Costituzionali*, 2017, n. 4, pp. 940-943. Sulla funzione consultiva della Corte di giustizia, P. IANNUCCELLI, *Commento al Titolo VII - Pareri*, in C. AMALFITANO, M. CONDINANZI, P. IANNUCCELLI (a cura di), *Le regole del processo dinanzi al giudice dell'Unione europea*, Napoli, 2017, , pp. 921-937; T. VON DANWITZ, *La procédure d'avis selon l'article 218, paragraphe 11, TFUE*, in *Il Diritto dell'Unione europea*, 2017, n. 2, p. 199 ss.; M. FRAGOLA, *Alcune riflessioni sulla funzione consultiva della Corte di giustizia dell'Unione europea*, in AA.VV., *Scritti in onore di Giuseppe Tesauro*, Napoli, 2014, pp. 1025-1040.

[55] Comunicato stampa n. 84/17 della Corte di giustizia del 26 luglio 2017, disponibile qui.

[56] Corte di giustizia, Parere 1/15, cit., par. 149.

autorità competenti. In linea con la propria giurisprudenza, la Corte ribadiva la necessaria circoscrizione dei dati conservati attraverso criteri oggettivi che collegassero le informazioni da conservare con l'obiettivo perseguito.

Nella successiva sentenza *Ministerio Fiscal*[57] la Corte di giustizia tornava a pronunciarsi sull'interpretazione dell'art. 15 della direttiva 2002/58, questa volta con riferimento al profilo dell'accesso ai dati e, in particolare, alla soglia di sufficiente gravità dei reati quale criterio che giustifichi l'ingerenza nei diritti fondamentali garantiti agli artt. 7 e 8 della Carta. Superate le eccezioni di incompetenza della Corte a pronunciarsi sul caso in esame[58], nel merito la pronuncia si soffermava, in realtà, sul parallelismo tra obiettivo perseguito e gravità dell'ingerenza perpetrata: rilevato primariamente come il dato testuale dell'art. 15 della direttiva 2002/58 non facesse alcun riferimento al carattere di gravità dei reati perseguiti, la Corte statuiva che "*una grave ingerenza può esser giustificata, in materia di prevenzione, ricerca, accertamento e perseguimento di un reato, solo da un obiettivo di lotta contro la criminalità che deve esser qualificata come «grave»*"[59]; viceversa, la conservazione di tipologie di dati (quali, ad esempio, i nominativi dei titolari di carte SIM di telefonia) dai quali non sono ricavabili dettagli concernenti la vita privata degli interessati - e dunque tali da determinare ingerenze "non gravi" nella sfera della riservatezza dei singoli - era ritenuta ammissibile per finalità di prevenzione e repressione di ogni ipotesi di reato, e non solo per quelli qualificati come "gravi"[60].

4. (*segue*) La legittimazione della conservazione generalizzata dei dati alla luce dell'art. 4, par. 2, TUE

Le non poche perplessità suscitate dalle sentenze fin qui esaminate circa l'adozione di misure nazionali sì rispettose dei *dicta* della Corte di giustizia ma, al contempo, ritenute, dagli stessi Stati, di scarsa efficacia sotto il profilo della salvaguardia della sicurezza nazionale non tardavano a tradursi in nuovi quesiti pregiudiziali; questa volta i

[57] Corte di giustizia, Grande Sezione, sentenza del 2 ottobre 2018, *Ministerio Fiscal*, causa C-207/16. A seguito del rigetto, da parte del giudice istruttore spagnolo, di una richiesta di autorizzazione a disporre l'acquisizione di una determinata tipologia di dati (*e.g.*, nominativi dei titolari di carte SIM) e per un arco temporale limitato (dodici giorni), il pubblico ministero proponeva appello dinanzi al *giudice a quo,* il quale decideva, altresì, di interrogare la Corte di Lussemburgo in ordine alla determinazione del concetto di "gravità" del reato. Sulla sentenza, si rinvia a L. WOOD, *Mobile phone theft and EU eprivacy law: the CJEU clarifies police powers,* in *EU Law Analysis*, 4 ottobre 2018.

[58] In risposta alla tesi del governo spagnolo secondo la quale l'accesso ai dati conservati dai *service provider* nell'ambito dell'attività istruttoria penale non rientrava nell'ambito di applicazione del diritto dell'Unione, in quanto esercizio dello *ius puniendi* dello Stato, la Corte di giustizia affermava come legislazioni nazionali volte a disciplinare un'attività di trattamento di dati quale la conservazione e il successivo (eventuale) accesso da parte delle autorità nazionali per esigenze di sicurezza rientravano nel novero delle operazioni svolte dai fornitori di servizi e, dunque, nel campo di applicazione della direttiva 2002/58/CE, in virtù del combinato disposto dei suoi artt. 3 e 15.

[59] Corte di giustizia, *Ministerio Fiscal*, cit., par. 56.

[60] *Ibidem*, parr. 59-63.

giudici nazionali sollecitavano l'esame della Corte di giustizia sulla sostanziale possibilità di prevedere sistemi di *bulk data retention* per ragioni imperative di tutela della sicurezza nazionale, in virtù del dettato dell'art. 4, par. 2, TUE. Ed è in tale scenario che si collocano le sentenze rese il 6 ottobre 2020 nei casi *La Quadrature du Net*[61] e *Privacy International*[62].

Dinanzi alle osservazioni presentate da numerosi Stati membri dirette a far valere l'inapplicabilità della direttiva 2002/58 nel caso di misure nazionali sulla *data retention* per scopi precipui di sicurezza nazionale (in quanto materia di esclusiva competenza statale), la Corte di giustizia sosteneva che "*una misura nazionale […] adottata a fini di salvaguardia della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto*"[63]. Inoltre, in coerenza con la propria giurisprudenza, la Corte ribadiva che tutti i trattamenti di dati effettuati da fornitori di servizi di comunicazione elettronica rientravano nell'ambito di applicazione della direttiva 2002/58, inclusi i trattamenti derivanti da obblighi loro

[61] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2020, La *Quadrature du Net, Ordre des barreaux francophones et germanophone e al.,* cause riunite C-511/18, C-512/18 e C-520/18. Le domande pregiudiziali originavano da diversi ricorsi promossi, in Francia e in Belgio, da organizzazioni non governative e diretti all'annullamento di alcune disposizioni nazionali in materia di *data retention* per presunta contrarietà all'ordinamento dell'Unione. Sulla sentenza si rinvia J. SAJFERT, *Bulk data interception/retention judgments of the CJEU – A victory and a defeat for privacy,* in *European Law Blog,* 26 ottobre 2020, reperibile *online*; 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, n. 1, pp. 93-124. Sulle ricadute della sentenza della Corte di giustizia nell'ordinamento francese con particolare riguardo alla richiesta avanzata dal governo al giudice *a quo* di opporre il controlimite dell'*ultra vires*, N. PERLO, *La decisione del Consiglio di Stato francese sulla* Data retention*: come conciliare l'inconciliabile*, in *Rivista di Diritti Comparati*, 2021, n. 2, pp. 163-183.

[62] Corte di giustizia, Grande Sezione, sentenza del 6 ottobre 2020, *Privacy International c. Secretary of State for Foreign and Commowealth Affairs, Security Intelligence State e al.*, causa C-623/17. La questione sottoposta alla Corte originava da un ricorso proposto da un'organizzazione non governativa britannica a seguito della pubblicazione di un rapporto del Parlamento britannico denunciante l'esistenza di pratiche di conservazione di massa e accesso da parte dei servizi di *intelligence* del Regno Unito. La domanda giudiziale promossa dinanzi all'*Investigatory Powers Tribunal* era volta all'accertamento della presunta contrarietà dell'art. 94 del *Telecommunications Act 1984* (in virtù del quale, nell'interesse della sicurezza nazionale o delle relazioni internazionali, un ministro impone ai *service provider*, mediante ordini, di trasmettere ai servizi di intelligence i dati relativi alla comunicazione di massa) al diritto dell'Unione europea. Merita evidenziare come la pubblicazione della sentenza della Corte di giustizia sia avvenuta successivamente all'entrata in vigore dell'Accordo di recesso del Regno Unito dall'Unione europea, conformemente all'art. 86, par. 2, del suddetto Accordo, in virtù del quale "*La Corte di giustizia dell'Unione europea resta competente a pronunciarsi in via pregiudiziale sulle domande presentate dai giudici del Regno Unito prima della fine del periodo di transizione*". Sul ruolo della Corte di giustizia nel sistema giurisdizionale britannico nel dopo *Brexit*, E. HANCOX, *Interpreting the Post-Brexit Legal Framework*, in *The Cambridge Law Journal*, 2021, vol. 80, n. 3, pp. 428-433; M. SIMONCINI, *Profili costituzionali della giurisprudenza europea dopo la Brexit*, in *Federalismi,* 2022, n. 10, pp. 116-131.

[63] Corte di giustizia, *La Quadrature du net*, cit., par. 99; *Privacy International*, cit., par. 44. A riguardo, M. NINO, *La disciplina internazionale ed europea…*, op. cit., in cui "*Le statuizioni della Corte vanno salutate con favore, poiché tendono ad attribuire all'Unione europea un ruolo rilevante anche nel contesto della sicurezza nazionale, rispetto alla quale gli Stati membri, anche in ragione della competenza esclusiva ad essi riconosciuta dal TUE, storicamente hanno manifestato una certa riluttanza a concedere poteri e competenze ad istituzioni sovranazionali*".

imposti da pubblici poteri per il mantenimento dell'ordine pubblico e della sicurezza interna.

A tal proposito, merita sottolineare come la Corte abbia colto, nella pronuncia *La Quadrature du Net*, l'occasione per chiarire un aspetto affrontato solo incidentalmente nella sentenza *Digital Rights Ireland* e nel Parere 1/15, concernente il riferimento all'art. 6 della Carta dei diritti fondamentali quale parametro interpretativo *in subiecta materia*: in virtù della c.d. "clausola di equivalenza" di cui all'art. 52, par. 3 della Carta, il significato e la portata dell'art. 6 è da rintracciarsi esclusivamente nel corrispondente art. 5 CEDU, disposizione finalizzata ad impedire privazioni arbitrarie ed ingiustificate della libertà dell'individuo da parte dei pubblici poteri, allo scopo di garantirne la "*sicurezza personale*"[64].

Orbene, come sottolineato dalla stessa Corte[65], elemento di novità delle pronunce in esame atteneva alla ricerca di un punto di equilibrio tra l'ingerenza nella riservatezza degli interessati e lo specifico obiettivo di salvaguardia della sicurezza nazionale.

In virtù dell'art. 4, par. 2, TUE, la Corte descriveva la competenza statale in materia di sicurezza nazionale quale "*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 popolazione o lo Stato in quanto tale, quali in particolare le attività di terrorismo*"[66]. Sulla base di questa lettura, per la prima volta nella sua giurisprudenza la Corte di giustizia individuava una sorta di ordine gerarchico tra gli obiettivi di interesse generale di cui all'art. 15 della direttiva 2002/58; in posizione preminente, vi collocava l'obiettivo della sicurezza nazionale ritenuto *"idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare altri obiettivi"*[67]. In presenza, dunque, di minacce alla sicurezza dello Stato, alle autorità nazionali non era precluso imporre ai fornitori di servizi di comunicazione elettronica di procedere alla conservazione preventiva dei dati di traffico telefonico e telematico di tutti gli utenti dei mezzi di comunicazione, a prescindere da un loro collegamento con la minaccia in questione, purché tale attività fosse limitata a una durata strettamente necessaria e, al contempo, fosse prevista una pluralità di rigorose garanzie sia procedurali che sostanziali (in particolare, la previsione di un effettivo controllo giurisdizionale o di un organo indipendente) contro il rischio di conservazioni illecite.

---

[64] Corte di giustizia, *La Quadrature du Net*, par. 125. Cfr. Conclusioni dell'Avvocato generale CAMPOS SÁNCHEZ-BORDONA, presentate il 15 gennaio 2020, nelle cause riunite C-511/18 e C-512/18, *La Quadrature du Net e al.,* parr. 98-99 in cui si distingue tra *"*sicurezza personale*, riferita alle condizioni nelle quali può essere limitata la libertà fisica delle persone" e "*sicurezza pubblica*, inerente all'esistenza dello Stato, che costituisce il presupposto imprescindibile, in una società sviluppata, per conciliare l'esercizio dei poteri pubblici con il godimento dei diritti individuali"* (enfasi non aggiunta).

[65] Corte di giustizia, *La Quadrature du net*, cit., par. 134.

[66] Corte di giustizia, *La Quadrature du net*, cit., par. 135; *Privacy international*, cit., par. 75.

[67] Corte di giustizia, *La Quadrature du net*, cit., par. 136; *Privacy International*, cit., par. 76.

Diversamente, dinanzi a minacce alla sicurezza pubblica ed esigenze di lotta a gravi forme di criminalità, metodologie di conservazione "mirata" erano ritenute legittime, a condizione che tale conservazione restasse - per quanto concerne le categorie dei dati da conservare, i mezzi di comunicazione interessati, le persone riguardate, nonché la durata di conservazione prevista - limitata allo stretto necessario alla luce dell'obiettivo perseguito e delle circostanze del caso concreto[68].

Degno di menzione anche l'esame sulla legittimità di altri due sistemi di conservazione dei metadati, cc.dd. "rapida" e "in tempo reale". La Corte riteneva legittime entrambe le ipotesi purché: nel primo caso, l'aspettativa degli utenti alla cancellazione o "anonimizzazione" dei loro dati alla scadenza dei termini previsti dalla legge fosse disattesa esclusivamente in ragione della repressione di fenomeni di grave criminalità e della salvaguardia della sicurezza nazionale[69]; nel secondo caso, la legislazione nazionale prevedesse rigorosi condizioni oggettive e non discriminatorie atte a riservare tale tipologia di sorveglianza unicamente alle persone in qualche modo collegate con una minaccia terroristica[70]. Pertanto, risultava necessario che l'adozione del provvedimento di autorizzazione alla raccolta in tempo reale fosse subordinata ad un controllo effettuato da un giudice o da un organo amministrativo indipendente.

E proprio il profilo dell'indipendenza dell'organo deputato al controllo preventivo sulla richiesta di accesso ai dati era oggetto della successiva pronuncia *H.K. c. Prokuratuur*[71]: in tale sentenza la Corte di giustizia affermava che il vaglio sulla rispondenza tra la gravità dell'ingerenza nella sfera privata dell'interessato e la gravità dell'obiettivo perseguito allo scopo di ottenere un'autorizzazione all'accesso ai dati relativi al traffico e ai dati relativi all'ubicazione in sede di attività istruttoria spettasse esclusivamente al giudice o a un organo amministrativo "*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*"[72], e dunque che

[68] Corte di giustizia, *La Quadrature du net*, cit., parr. 147-151.

[69] *Ibidem*, par. 162 in cui si evidenziava come la conservazione "rapida" dei dati, ossia la conservazione dei suddetti oltre i termini di legge, per finalità di indagine, fosse già prevista dall'art. 16 ("*Expedited preservation of stored computer data*") della Convenzione del Consiglio d'Europa *sulla criminalità informatica* del 23 novembre 2001 (c.d. Convenzione di Budapest).

[70] *Ibidem,* par. 189. La "raccolta in tempo reale di dati sul traffico" è altresì disciplinata all'art. 20 della Convenzione di Budapest.

[71] Corte di giustizia, Grande Sezione, sentenza del 2 marzo 2021, *H. K. c. Prokuratuur*, causa C-764/18. Le questioni pregiudiziali - sollevate dalla Corte suprema estone nelle more di un ricorso per cassazione - vertevano sull'ammissibilità degli elementi di prova acquisiti in base a misure nazionali di conservazione generalizzata dei dati ritenute contrarie al diritto dell'Unione perché, appunto, non circoscritte a persone sospettate di reati gravi, nonché sul requisito dell'indipendenza del pubblico ministero, il quale, come previsto dalla legislazione estone, senza alcun tipo di richiesta preventivo, ingiunge direttamente ai fornitori di servizi di comunicazione la trasmissione dei dati relativi al traffico telefonico e telematico. Per un commento alla sentenza, G. FORMICI, *L'incerto futuro della* data retention *nell'Unione europea: osservazioni a partire dalla sentenza H.K. v Prokuratuur,* in *SIDIBlog,* 27 aprile 2021, reperibile *online;* S. ROVELLI, *Case Prokuratuur: Proportionality and the Independence of Authorities in Data Retention,* in *European Papers,* 2021, vol. 6, n. 1, pp. 199-210.

[72] *Ibidem*, parr. 52-55.

fosse neutrale e imparziale, al riparo da qualsiasi influenza esterna. In una parola, indipendente[73]. Ne conseguiva l'affermazione della sostanziale incompatibilità con il diritto dell'Unione di una normativa nazionale che consentiva al pubblico ministero, in quanto parte che esercita l'azione penale, di accedere in via diretta ai dati in questione al fine di condurre un'istruttoria penale[74].

Appare, dunque, evidente come, a partire dall'annullamento della direttiva 2006/24/CE, la Corte di giustizia abbia aperto una sorta di "vaso di Pandora" della *data retention*, stimolando un intenso dibattito sulla necessità, in una società democratica, di rigorosi limiti ed adeguate garanzie nella disciplina della conservazione e dell'accesso ai dati del traffico telefonico e telematico. Appare, altresì evidente, come tale dibattito continui ad animare il dialogo tra la Corte di Lussemburgo e i giudici nazionali nella ricerca di un punto di equilibrio tra esigenze di sicurezza dello Stato e tutela dei diritti fondamentali dei singoli; equilibrio che deve tener conto anche del riparto di competenze tra Unione europea e Stati membri in un settore delicato e gelosamente custodito dagli stessi qual è quello della sicurezza nazionale.

5. Sguardo alla giurisprudenza della Corte EDU: l'atteso epilogo dell'*affaire Big Brother Watch and Others v. the United Kingdom*

Tali questioni, come noto, non sono appannaggio esclusivo della Corte di giustizia, dal momento che sin dagli anni Settanta[75] e parallelamente al crescente ricorso a nuove tecnologie di sorveglianza per finalità investigative, la Corte europea dei diritti dell'uomo ha avuto modo di pronunciarsi su pratiche di sorveglianza massiva in virtù di

[73] Cfr. Conclusioni dell'Avvocato generale G. PITRUZZELLA, presentate il 21 gennaio 2020, nella causa C-746/18, *H.K. c. Prokuratuur*, parr. 100-105, in cui, con riferimento alla giurisprudenza della Corte relativa all'indipendenza dell'autorità giudiziaria emittente un mandato di arresto europeo, si ribadisce che il carattere dell'"indipendenza" si concretizza: nell'impermeabilità del giudice verso qualsiasi pressione esterna; nell'imparzialità; nell'equidistanza dalle parti della controversia e dai loro rispettivi interessi. Sul tema, tra gli altri, G. PITRUZZELLA, O. POLLICINO, M. BASSINI (a cura di), *Corti europee e democrazia. Rule of law, indipendenza e accountability*, Milano, 2019; G. DE AMICIS, *Stato di diritto, garanzie europee di indipendenza della magistratura e cooperazione giudiziaria penale: quadri di un'esposizione* in fieri, in *Diritto Penale Contemporaneo*, 2021, n. 4, pp. 143-179.

[74] Sulle particolari ricadute della sentenza nell'ordinamento giuridico italiano si rinvia a E. ANDOLINA, *La sentenza della Corte di giustizia UE nel caso H.K. c. Prokuratuur: un punto di non ritorno nella lunga querelle in materia di 'data retention'*?, in *Processo penale e Giustizia*, 2021, fasc. 5, pp. 1204-1217; M. ARANCI, *L'acquisizione dei dati esteriori delle comunicazioni nel processo penale italiano dopo la sentenza H.K.: alcuni spunti di riflessione sulle prime applicazioni giurisprudenziali*, in *La legislazione penale*, 2021, n. 3, pp. 66-92.

[75] Corte europea dei diritti dell'uomo, Plenaria, sentenza del 6 settembre 1978, *Klass and Others v. Germany*, ricorso n. 5029/71; Grande Camera, sentenza del 4 maggio 2000, *Rotaru v. Romania*, ricorso n. 28341/95; sentenza del 12 gennaio 2016, *Szabó and Vissy v. Hungary*, ricorso n. 37138/14. Per una ricostruzione della giurisprudenza della Corte europea in materia di *data retention* si rinvia a P. BREYER, *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR,* in *European Law Journal*, 2005, vol. 11, n. 3, pp. 365-375*;* G. FORMICI, *La* digital mass surveillance *al vaglio della Corte Europea dei Diritti dell'Uomo: da Zackarov a Big Brother Watch,* in *Federalismi,* 2020, n. 23, pp. 44-71.

un'interpretazione estensiva dell'art. 8 CEDU, letto alla luce della Convenzione del Consiglio d'Europa *sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale*[76]. Pertanto, vale la pena volgere un seppur rapido sguardo a una delle ultime pronunce sull'argomento, resa il 25 maggio 2021 dalla *Grand Chambre* nel caso *Big Brother Watch and Others v. the United Kingdom*; pronuncia richiamata anche nella decisione di adeguatezza della Commissione europea[77] relativa alla circolazione dei dati personali tra Unione europea e Regno Unito a seguito dell'inedita attivazione della procedura di recesso *ex* art. 50 TUE[78].

La decisione della Corte di Strasburgo costituisce l'atteso epilogo di un articolato *iter* processuale iniziato nel 2013 nel Regno Unito, a seguito delle rivelazioni del *whistleblower* statunitense Edward Snowden relative all'impiego, da parte dei servizi di *intelligence* britannici e statunitensi, di programmi di sorveglianza di massa[79].

Le questioni sottoposte al vaglio della Corte europea dei diritti dell'uomo da parte di numerose organizzazioni non governative (ONG) attive nella protezione dei diritti umani attenevano alla presunta violazione degli artt. 8 e 10 CEDU di alcune disposizioni del *Regulation of Investigatory Powers Act 2000*[80] (all'epoca dei fatti ancora vigente nel

---

[76] L. TOMASI, *Art. 8*, in S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (a cura di), *Commentario breve alla CEDU,* op. cit., p. 315.

[77] Ai sensi degli artt. 45, par. 1, del regolamento (UE) 2016/679: "*Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche"* (v. per analogia art. 36 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016*, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati,* in GUUE *L 119 del 4 maggio 2016, pp. 89-131).*

[78] Regolamento di esecuzione (UE) 2021/1772 della Commissione del 28 giugno 2021 *a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio sull'adeguata protezione dei dati personali da parte del Regno Unito*, in GUUE *L 360 dell'11 ottobre 2021, pp. 1-68 in cui la Commissione europea, con riferimento ai mezzi di ricorso giurisdizionale, condivide la valutazione della Corte di Strasburgo sull'Investigatory Powers Tribunal britannico quale "solido ricorso giurisdizionale per chiunque sospetti che le proprie comunicazioni siano state intercettate dai servizi di intelligence*" (par. 269). *Per quanto concerne il regime di circolazione dei dati personali contemplato nell'accordo sugli scambi commerciali e la cooperazione tra Unione europea e Regno Unito si rinvia a D. ERDOS, The UK and the EU personal data framework after Brexit: a new trade and cooperation partnership grounded in Council of Europe Convention 108+?, in Computer Law & Security Review, 2022, vol. 44, n. 105639.*

[79] In seguito allo scoppio del caso *Datagate*, l'Assemblea generale delle Nazioni Unite ha adottato la risoluzione *The right to privacy in the digital age* (A/RES/68/167) con cui ha sollecitato gli Stati "*To review their procedures, practices and legislation regarding the surveillance of communications, […] with a view to upholding the right to privacy by ensuring the full and effective implementation of all their obligations under international human rights law"*. Per una ricostruzione della questione si rinvia a M. NINO, *Il caso* Datagate*: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy,* in *Diritti umani e diritto internazionale*, 2013, vol. 7, n. 3, pp. 727-746; P. MARGULIES, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, in *Fordham Law Review*, 2014, vol. 82, n. 5, pp. 2137-2167; D. JOYCE, *Privacy in the digital era: human rights online?,* in *Melbourne Journal of International Law,* 2015, vol. 16, n. 1, pp. 270-285.

[80] Il riferimento è alla Sezione 8(4) *RIPA*, il quale consentiva al *Government Communications Headquarter*

Regno Unito, poi abrogato e sostituito dall'*Investigatory Powers Act 2016*) relative, nella sostanza, a tre diversi regimi di sorveglianza: l'intercettazione massiccia delle comunicazioni (c.d. *bulk interception*) su mandato del *Government Communications Headquarter*; lo scambio di dati tra agenzie *intelligence* straniere; l'acquisizione dei dati di comunicazione da parte di *service providers.*

Nella sentenza resa il 13 settembre 2018[81], la Prima Sezione della Corte di Strasburgo riconosceva esplicitamente in capo agli Stati *"a wide margin of appreciation in deciding what type of interception regime is necessary to protect national security"*[82]; tuttavia, l'assenza di alcune condizioni procedurali ritenute necessarie, sulla base dei c.d. criteri *Weber*[83]*,* ad arginare il rischio di abusi da parte delle pubbliche autorità[84] conducevano i giudici di Strasburgo a condannare il Regno Unito per violazione degli artt. 8 e 10 della Convenzione[85].

Non soddisfatti, i ricorrenti decidevano di deferire la questione alla Grande Camera[86], lamentando che il sistema di sorveglianza di massa fosse da considerarsi di per sé *"neither*

di intercettare, previo mandato, comunicazioni trasmesse e ricevute nel Regno Unito.

[81] Corte europea dei diritti dell'uomo, Prima Sezione, sentenza del 13 settembre 2018, *Big Brother Watch and Others v. the United Kingdom*, ricorsi nn. 58170/13, 62322/14 e 24960/15.

[82] *Ibidem*, par. 315.

[83] Corte europea dei diritti dell'uomo, sentenza del 29 giugno 2006, *Weber and Saravia v Germany,* ricorso 54394/00, par. 95 in cui la Corte elenca sei condizioni minime che la legge nazionale è tenuta a rispettare nella previsione di regole sulla sorveglianza di massa. Esse concernono: 1) la definizione della natura dei reati che possono dare luogo ad intercettazione; 2) la determinazione delle persone che possono essere sottoposte ad intercettazione; 3) i limiti di durata delle operazioni di raccolta dati; 4) la disciplina della procedura di esame, trattazione e conservazione dei dati; 5) le salvaguardie che devono essere messe in campo per il trasferimento di dati ad altri soggetti; 6) le circostanze sulla base delle quali i dati possono o devono essere distrutti.

[84] In estrema sintesi, con riferimento alla Sezione 8(4) *RIPA* Corte rilevava l'assenza di un controllo indipendente sulla individuazione e determinazione dei criteri di ricerca usati per "filtrare" le comunicazioni intercettate e la mancanza di salvaguardie sufficientemente robuste da prevenire abusi in questa fase (par. 347). Nessun rilievo problematico emergeva con riguardo ai meccanismi di richiesta e utilizzo di informazioni derivanti da sistemi di intelligence straniera (parr. 446-447). Sotto il profilo della compatibilità del Capitolo II *RIPA,* la Corte rilevava, sulla scia delle sentenze *Digital Rights Ireland* e *Tele2* della Corte di giustizia, che la normativa inglese non limitava l'accesso ai *serious crime* e non prevedeva un previo controllo da parte di un'autorità indipendente, con conseguente accertamento della violazione dell'art. 8 CEDU. Sulla sentenza, si rinvia a M. MILANOVIC, *ECtHR Judgment in Big Brother Watch v. UK*, in *EJIL:Talk!*, 17 settembre 2018, reperibile *online*; G. TIBERI, *Il caso Big Brother Watch quale cambio di paradigma nel bilanciamento tra sicurezza e tutela dei diritti fondamentali?,* in *Quaderni Costituzionali,* 2018, n. 4, pp. 931-933; B. VAN DER SLOOT, E. KOSTA, *Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance,* in *European Data Protection Law Review,* 2019, vol. 5, n. 2, pp. 252-261.

[85] La Corte accertava, altresì, l'assenza di misure atte a tutelare il diritto alla confidenzialità delle fonti giornalistiche quale condizione essenziale per garantire l'esercizio della libertà di stampa e il diritto della collettività a ricevere informazioni di interesse generale (parr. 493-495).

[86] Corte europea dei diritti dell'uomo, Grande Camera, sentenza del 21 maggio 2021, *Big Brother Watch and Others v. the United Kingdom*, ricorsi nn. 58170/13, 62322/14 e 24960/15. Per un primo commento, v. M. MILANOVIC, *The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa, in EJIL:Talk!,* 26 maggio 2021, reperibile *online;* J. SAJFERT, *The Big Brother Watch and Centrum för Rättvisa judgments of the Grand Chamber of the European Court of Human Rights – the Altamont of privacy?*, in *European Law Blog,* 8 giugno 2021, reperibile *online*; F. BIEKER, *The State of Surveillance – An Overall Account of Surveillance?*, in M. FRIEDEWALD, S. KRENN,

necessary nor proportionate within the meaning of Article 8 of the Convention and, as such, did not fall within a State's margin of appreciation"[87].

Al contrario, il percorso argomentativo sviluppato dalla *Grand Chambre* muove proprio da un rinnovato riconoscimento del margine di discrezionalità statale nella regolamentazione di regimi di sorveglianza[88], nella consapevolezza della loro "*valuable technological capacity to identify new threats in the digital domain"*[89] e che "*bulk interception is of vital importance to Contracting States in identifying threats to their national security"*[90].

In linea con le argomentazioni della Camera, la *Grand Chambre* rimarca che "*Article 8 of the Convention does not prohibit the use of bulk interception to protect national security and other essential national interests against serious external threats"* e che *"States enjoy a wide margin of appreciation in deciding what type of interception regime is necessary"*[91]. Tuttavia, al fine di assicurare che ogni interferenza non ecceda la stretta necessità in una società democratica, la Corte ribadisce che l'intero processo di sorveglianza debba esser sottoposto dall'inizio alla fine (c.d. "*end-to-end safeguards*") a una costante valutazione sulla necessità e proporzionalità delle misure adottate[92]. Altrettanto necessaria la previsione di un'autorizzazione preventiva da parte di un organo *indipendente* dall'esecutivo (non necessariamente un organo giudiziario[93]), oltre che di un controllo successivo (c.d. "*ex post review"*) nel caso di accessi illeciti o di sorveglianze arbitrarie[94]. Con riferimento, poi, alle garanzie che la legislazione nazionale è tenuta a contemplare per rispettare il c.d. "*three-steps test"*[95] di cui all'art. 8, par. 2, CEDU, la Grande Camera rielabora i suddetti criteri Weber[96] preferendo, tuttavia, non chiarire che

---

I. SCHIERING, S. SCHIFFNER (a cura di), *Privacy and Identity Management. Between Data Protection and Security*, pp. 43-53.

[87] *Ibidem*, par. 277.

[88] *Ibidem*, par. 340. Già nel precedente par. 242 la Corte aveva evidenziato come gli ordinamenti giuridici di almeno sette Alte Parti Contraenti (Finlandia, Francia, Germania, Paesi Bassi, Svezia, Svizzera e Regno Unito) contemplino regimi di *bulk interception.*

[89] *Ibidem*, par. 323.

[90] *Ibidem*, par. 424.

[91] *Ibidem*, par. 347.

[92] *Ibidem*, par. 350.

[93] *Ibidem*, par. 358-359.

[94] *Ibidem*, par. 357.

[95] Così P. VOGIATZOGLOU, *Mass surveillance, Prective Policing and the Implementation of the CJUE and ECtHR Requirement of Objectivity*, in *European Journal of Law and Technology*, 2019, vol. 10, n. 1, in particolare par. 2. Come noto, l'art. 8, par. 2, CEDU prevede che ingerenze dell'autorità pubblica nella sfera personale dell'individuo debbano esser previste dalla legge, perseguire scopi legittimi e siano rispondenti al principio di necessità in una società democratica.

[96] *Ibidem*, par. 361. Essi concernono: 1) i motivi per i quali l'intercettazione di massa può essere autorizzata; 2) le circostanze in cui le comunicazioni di un individuo possono essere intercettate; 3) la procedura da seguire per il rilascio dell'autorizzazione; 4) le procedure da seguire per la selezione, l'esame e l'utilizzo del materiale di intercettazione; 5) le precauzioni da prendere nella comunicazione del materiale ad altri soggetti; 6) i limiti alla durata dell'intercettazione, alla conservazione del materiale intercettato e alle circostanze in cui tale materiale deve essere cancellato e distrutto; 7) le procedure e le modalità per il controllo da parte di un'autorità indipendente del rispetto delle suddette garanzie e dei suoi poteri per far fronte alle inadempienze; 8) le procedure per l'esame indipendente *ex post* di tale conformità e i poteri

tipo di vincolatività questi esplichino [97]. Ed è pertanto, alla luce di tali elementi che la Corte riscontra nel sistema britannico le seguenti criticità: "*the absence of independent authorisation, the failure to include the categories of selectors in the application for a warrant, and the failure to subject selectors linked to an individual to prior internal authorisation*"[98], accertando, dunque, la violazione dell'art. 8 CEDU.

Con riferimento all'acquisizione dei dati di comunicazione da parte di *service providers*, in linea con la sentenza del 2018, la Grande Camera rileva la violazione del criterio di legalità dal momento che la normativa inglese non risulta circoscritta ai casi di lotta alla criminalità grave, come previsto dal diritto dell'Unione, tenuto conto che all'epoca dei fatti il Regno Unito, in qualità di Stato membro dell'Unione europea, era tenuto a rispettare il principio del primato sul diritto interno[99].

Al di là del dato letterale del dispositivo, ciò che preme evidenziare è il riconoscimento di un'ampia discrezionalità degli Stati, acclarato anche dal fatto che la Corte omette di pronunciarsi tanto sulla necessità *ab origine* dei sistemi di sorveglianza di massa, quanto sull'individuazione di strumenti alternativi egualmente efficienti e meno invasivi nella vita privata dei singoli, preferendo soffermarsi esclusivamente sulle garanzie di carattere procedurale[100]. Ed è proprio sulla base di tale criticità che il giudice Pinto de Albuquerque, nella sua *Opinion*, afferma come *"with the present judgment the Strasbourg Court has just opened the gates for an electronic "Big Brother" in Europe"*[101].

Ad avviso del giudice, l'aumento esponenziale dei sistemi di conservazione dei dati per far fronte alle continue minacce alle quali gli Stati sono esposti richiede un controllo sulle prerogative dei pubblici poteri informato ai principi-valori della democrazia e dello Stato di diritto. L'utilità di tali strumenti, a detta del giudice, non deve tradursi in lesioni delle garanzie accordate dalla CEDU. "*Usefulness is not the same thing as necessity and proportionality in a democratic society"*[102].

Il giudice critica aspramente l'ammissione *in sé e per sé* della sorveglianza di massa prendendo a modello il tradizionale orientamento della Corte di giustizia sulla materia, restio ad ammettere *in via ordinaria* la legittimità di sistemi di conservazione generale e indiscriminata dei dati relativo al traffico telefonico e all'ubicazione degli utenti.

In definitiva, secondo il giudice De Albuquerque, "*the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe*"[103].

---

conferiti all'organo competente nel far fronte ai casi di non conformità.

[97] A tal riguardo, M. ZALNIERIUTE, *Procedural Fetishism and Mass Surveillance under the ECHR: Big Brother Watch v. UK, in VerfBlog,* 2 giugno 2021, reperibile *online.*

[98] *Ibidem*, par. 425.

[99] *Ibidem*, par. 518-522.

[100] Dello stesso tenore la più recente Corte europea dei diritti dell'uomo, sentenza dell'11 gennaio 2022, *Ekimdzhiev and Others v. Bulgaria,* ricorso n. 70078/12, in particolare parr. 291-293.

[101] *Ibidem*, *Partly Concurring and Partly Dissenting Opinion of Judge Pinto De Albuquerque*, par. 60.

[102] *Ibidem*, par. 58.

[103] *Ibidem*, par. 60.

Siffatta conclusione non risulta condivisa da parte della dottrina, ad avviso della quale il riconoscimento, a partire dalla sentenza *La Quadrature du Net*, della preminenza dell'obiettivo della sicurezza nazionale, letto alla luce dell'art. 4, par. 2, TUE, tale da giustificare l'adozione di misure di conservazione generalizzata ed indifferenziata dei dati, sottoponendo a controllo la totalità degli utenti di mezzi di comunicazione elettronica senza che sia necessario un collegamento tra questi ultimi e una minaccia per la sicurezza nazionale, sembra, piuttosto, indicare che "*the two Courts are converging rather than diverging in their recent jurisprudence concerning the data retention saga*"[104].

6. La sentenza della CGUE del 5 aprile 2022, C-140/20, *Commissioner of An Garda Síochána*

È in tale contesto che si colloca l'ultimo (per il momento) tassello posto dalla Corte di Lussemburgo nella saga giurisprudenziale sulla *data retention,* il quale non fa che confermare il suo recente orientamento in materia di conservazione dei metadati allo scopo di tutelare le funzioni essenziali e gli interessi fondamentali del singolo Stato da minacce reali ed attuali, o quantomeno prevedibili, alla sua sicurezza.

Con sentenza pubblicata il 5 aprile 2022[105], la Corte di Lussemburgo ha, infatti, cristallizzato i principi sin qui sanciti, ad onta delle perplessità manifestate dalla Corte suprema irlandese relative alla conservazione generalizzata, preventiva e indiscriminata delle informazioni sul traffico telefonico e telematico nelle comunicazioni elettroniche.

La domanda pregiudiziale era stata sollevata nelle more di un procedimento sulla presunta invalidità di alcune disposizioni del *Communications (Retention of data) Act 2011*, ossia della normativa irlandese che aveva recepito l'ormai abrogata direttiva 2006/24 e, ciononostante, ancora vigente nell'ordinamento interno: il ricorrente, imputato per omicidio in un procedimento penale, asseriva l'incompatibilità del regime di *data retention* contemplato dalla legislazione nazionale[106] con il diritto dell'Unione[107].

---

[104] Così 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,* 2022, vol. 28, n. 1, pp. 123-154. V. anche M. ZALNIERIUTE, *The Future of Data Retention Regimes and National Security in the EU after the Quadrature Du Net and Privacy International Judgments*, in *American Society of International Law - Insight*, 5 novembre 2020, vol. 24, n. 8, reperibile *online*.

[105] Corte di giustizia, Grande Sezione, sentenza del 5 aprile 2022, *Commissioner of An Garda Siochana*, causa C-140/20. Per un primo commento, C. BEATON, *Graham Dwyer succeeds in EU challenge to Irish data retention law*, in *Irish Legal News*, 5 aprile 2022, reperibile *online*; M. C. DALY, *Data retention rules for Europe - a headache or a vindication?*, in *Data Protection Ireland Journal*, 2022, vol. 15, n. 3, pp. 11-13; F. RESTA, *Dalla conservazione generalizzata a quella mirata e rapida: la Corte di giustizia ridelinea i contorni della data retention,* in *Giustizia insieme,* 7 aprile 2022, reperibile *online*.

[106] Il *Communications (Retention of data) Act 2011* impone ai fornitori di servizi di comunicazione elettronica di conservare i dati di telefonia e di ubicazione per un periodo di due anni (art. 3), e di comunicare tali dati alla polizia nazionale qualora essi risultino necessari alla prevenzione o all'accertamento dei reati punibili con una pena detentiva di durata pari o superiore a cinque anni o, ancora, per finalità di salvaguardia della sicurezza dello Stato e di protezione della vita umana (art. 6).

[107] Corte di giustizia, *Commissioner of An Garda Siochana,* cit., par. 24.

Il dilemma del giudice *a quo* sulla legittimità della conservazione generalizzata dei metadati muoveva da supposizioni circa una maggior efficacia di tale regime nel perseguimento di gravi fenomeni criminosi[108], a differenza della conservazione "rapida" e "mirata", ritenute potenzialmente discriminatorie, o comunque di utilità strettamente limitata ai casi in cui l'identità della persona indagata fosse già nota alle autorità competenti[109].

Alla Corte di Lussemburgo pervenivano sei lunghi e articolati quesiti, i quali, sulla scorta di un'operazione di sintesi proposta dall'Avvocato generale nelle Conclusioni rese nel caso in esame[110], venivano riformulati nelle seguenti tre questioni concernenti: "*i) la legittimità di un sistema di conservazione generalizzata e indifferenziata dei dati, di per sé e per quanto riguarda la lotta contro le forme gravi di criminalità; ii) le caratteristiche che deve soddisfare, se del caso, l'*accesso *ai dati conservati; iii) la possibilità di limitare nel tempo gli effetti di un'eventuale dichiarazione di incompatibilità con il diritto dell'Unione della normativa nazionale in materia*"[111].

Orbene, in ordine alla prima questione, in via preliminare la Corte ribadisce che i diritti sanciti dagli artt. 7, 8 e 11 della Carta dei diritti fondamentali non hanno valore assoluto, sicché eventuali restrizioni agli stessi sono conformi al diritto dell'Unione solo se poste nel rispetto della clausola generale di cui all'art. 52, par. 1 della Carta, nel contesto di un "*contemperamento equilibrato*"[112] da effettuarsi tra gli obiettivi tassativamente individuati dall'art. 15 della direttiva 2002/58 e i diritti di cui trattasi. In particolare, la Corte di giustizia rimarca come l'adozione di normative nazionali sulla memorizzazione dei metadati non possa esimersi da una previa valutazione sulla gravità dell'ingerenza subita dai singoli individui in rapporto all'obiettivo di interesse generale perseguito, alla luce del principio di proporzionalità[113]. Ed è alla luce di tale principio che nella gerarchia degli obiettivi di interesse generale elencati al suddetto art. 15, quello della sicurezza nazionale, letto alla luce dell'art. 4, par. 2, TUE, occupa una posizione preminente, in quanto "*idoneo a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare tali altri obiettivi"*[114].

---

[108] Corte suprema irlandese, decisione del 24 febbraio 2020, *Graham Dwyer and The Commissioner of An Garda Síochána, the Minister for Communications, Energy and Natural Resources, Ireland and the Attorney*, ricorso n. 2019/18, in particolare par. 5.5.

[109] Corte di giustizia*, Commissioner of An Garda Siochana,* cit., par. 26.

[110] Conclusioni dell'Avvocato generale M. C. SANCHEZ-BORDONA, presentate il 18 novembre 2021, nella causa C-140/20, *Commissioner of the Garda Síochána*, par. 23. Nel medesimo giorno l'Avvocato generale Sanchez-Bordona ha rassegnato le proprie Conclusioni nei casi *Bundesrepublik Deutschland c. SpaceNet AG (C-793/19) Telekom Deutschland GmbH (C-794/19*), cause riunite C-793/19 e C-794/19, e *VD e SR*, cause congiunte C-339/20 e C-397/20. Per un commento si rinvia a L. WOODS, *Data Retention: AG opinions on the latest CJEU cases on national laws,* in *EU Law Analysis,* 24 novembre 2021, reperibile *online;* T. WAHL*, AG: German, Irish and French Data Retention Rules Incompatible with EU Law,* in *EUcrim,* 19 gennaio 2022, reperibile *online.*

[111] Corte di giustizia*, Commissioner of An Garda Siochana,* cit., par. 23.

[112] *Ibidem*, par. 52.

[113] *Ibidem*, parr. 53-54.

[114] *Ibidem*, par. 57.

Ne consegue, ad avviso dei giudici di Lussemburgo, che esigenze di sicurezza nazionale giustificano una conservazione universale dei dati di telefonia e di ubicazione degli utenti in presenza di "*circostanze sufficientemente concrete*"[115] di minacce reali e attuali, o tantomeno prevedibili, alla sicurezza dello Stato; in tal caso, le ingiunzioni rivolte ai *service providers* devono prevedere la durata della sorveglianza e devono esser oggetto di controllo, da parte di organi amministrativi o giudiziari indipendenti, sull'esistenza della situazione di gravità descritta e sul rispetto delle condizioni previste dalla legge.

Differentemente, la lotta alla criminalità grave - per definizione, motivo "*generale e permanente*"[116] di perturbazione alla sicurezza pubblica - non giustifica una sorveglianza generalizzata e indiscriminata, in quanto tale situazione non risulta equiparabile al caso di gravi minacce alle funzioni essenziali dello Stato; ammetterne un'interpretazione contraria *"equivarrebbe a introdurre una categoria intermedia tra la sicurezza nazionale e la sicurezza pubblica per applicare alla seconda i requisiti della prima*"[117].

Dunque, nel caso di lotta a forme gravi di criminalità, la Corte esclude la conservazione generalizzata in quanto eccedente i limiti dello stretto necessario in una società democratica, dal momento che "*essa si applica […] anche a persone per le quali non vi è alcun indizio che il loro comportamento possa avere un legame, anche indiretto o remoto, con l'obiettivo di combattere gli atti di criminalità grave e, in particolare, senza che sia stabilita una correlazione tra i dati di cui è prevista la conservazione e una minaccia per la sicurezza pubblica*"[118].

Ciò detto, sulla scia del percorso logico-argomentativo già sviluppato nella sentenza *La Quadrature du Net*, la Corte di giustizia ritiene conforme al diritto dell'Unione: la conservazione "mirata" di dati di traffico e di ubicazione delimitata a una cerchia ristretta di persone individuate mediante elementi oggettivi e non discriminatori, nonché la conservazione generalizzata e indifferenziata degli indirizzi IP[119], e, infine, la conservazione "rapida" oggetto di ingiunzione da parte delle autorità competenti ai *service provider*, per un periodo di tempo limitato allo stretto necessario[120].

Ed è a tal proposito che, in risposta al dilemma del giudice irlandese, la Corte - rilevato, in via preliminare, che la garanzia dell'efficacia dell'azione penale dipende dalla

[115] *Ibidem*, par. 62.
[116] *Ibidem*, par. 62.
[117] *Ibidem*, par. 63. Si vedano anche le Conclusioni dell'Avvocato generale, cit., parr. 50-52 secondo il quale "(*introdurre un tertium genus di violazioni) estenderebbe fino a limiti imprecisati l'unica causa idonea a giustificare una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione – ossia la sicurezza nazionale – equiparando le minacce a quest'ultima quelle derivanti dalle forme gravi di criminalità"*.
[118] *Ibidem*, par. 66.
[119] *Ibidem*, parr. 73-74. La Corte ritiene giustificata la conservazione generalizzata degli indirizzi IP in quanto, in casi particolarmente delicati come l'abuso e lo sfruttamento sessuale di minori e la pornografia minorile, solo mediante il codice dell'apparecchiatura connessa ad *Internet* risulta allo stato tecnicamente possibile risalire alla persona alla quale tale indirizzo era attribuito al momento della commissione del reato. Tuttavia, aggiunge la Corte, la normativa nazionale deve prevedere rigorose condizioni sostanziali e procedurali atte a disciplinarne l'utilizzo nel procedimento penale.
[120] *Ibidem*, par. 67 che riprende la sentenza del 6 ottobre, *La Quadrature du Net.,* cit., par. 168.

pluralità degli strumenti di indagine[121] - offre alcuni chiarimenti sulle diverse modalità di conservazione precedentemente elencate e sulla loro applicazione. Con riferimento alla conservazione "mirata", la Corte riconosce esplicitamente in capo agli Stati membri la facoltà di prevedere misure di conservazione dei dati di persone "*iscritte nel casellario giudiziario nazionale ove è menzionata una condanna precedente per atti di criminalità grave che possono comportare un elevato rischio di recidiva*"[122], o, ancora, di persone situate in zone geografiche in cui vi sia "*un rischio elevato di preparazione o di commissione di atti di criminalità grave*"[123], fermo restando la possibilità per gli Stati membri di prevedere ulteriori criteri da quelli suddetti dal momento che "*è a questi ultimi e non alla Corte che spetta identificare siffatti criteri, fermo restando che non può trattarsi di reintrodurre, in tal modo, una conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione*"[124].

Anche con riferimento alla conservazione "rapida", la Corte ammette la facoltà degli Stati membri di prevedere la raccolta di dati anche per tempi superiori rispetto ai limiti tempo ordinariamente previsti dalla legge per i trattamenti commerciali dei *service providers*, al fine di indagare su reati gravi o attentati alla sicurezza nazionale[125]. Inoltre, la Corte non preclude la possibilità di un'applicazione cumulativa dei diversi regimi summenzionati[126].

Con riferimento all'accesso ai dati, in coerenza con la pronuncia *H.K. Prokuratuur*, i giudici di Lussemburgo riaffermano la necessità che la normativa nazionale preveda condizioni e circostanze rigorose in virtù delle quali le attività di *law enforcement* possano accedere ai dati di persone sospettate di commettere o aver già commesso reati gravi o, nel caso di minaccia alla sicurezza nazionale, anche di un numero superiore di individui "*qualora sussistano elementi oggettivi che permettano di ritenere che tali dati potrebbero, in un caso concreto, fornire un contributo effettivo alla lotta contro attività di questo tipo*"[127]. Anche in questo caso, la Corte rimarca la necessità di un bilanciamento tra gli interessi legittimi sottesi alle esigenze di indagini e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali da affidarsi ad un organo terzo, indipendente e imparziale[128]. Tutte condizioni, quelle elencate, che, a detta della Corte, mancano nella legislazione irlandese, in cui il trattamento delle domande di accesso ai dati conservati dai fornitori di telecomunicazione è rimesso alla discrezionalità delle stesse autorità di polizia[129].

Infine, la Corte di giustizia censura in maniera definitiva la "sopravvivenza" di una normativa, come quella irlandese sulla *data retention*, emanata in attuazione di una

[121] *Ibidem*, par. 69.
[122] *Ibidem*, par. 78.
[123] *Ibidem*, parr. 79-80.
[124] *Ibidem*, par. 83.
[125] *Ibidem,* par. 85.
[126] *Ibidem,* par. 92.
[127] *Ibidem*, par. 105.
[128] *Ibidem*, par. 107-105.
[129] *Ibidem*, par. 111-114.

direttiva dichiarata poi invalida (e dunque anch'essa contrastante con il diritto dell'Unione) ponendo al centro delle proprie argomentazioni il principio del primato del diritto dell'Unione. Ribadito che, in virtù di tale principio, il giudice nazionale è sempre tenuto a disapplicare la contraria disposizione nazionale e, in secondo luogo, che soltanto alla Corte di giustizia è consentito sospendere temporaneamente la disapplicazione della norma interna in contrasto con la norma di diritto dell'Unione per ragioni (eccezionali) di certezza del diritto, ne consegue che il procrastinare del giudice nazionale sulla disapplicazione di una normativa ormai contraria al diritto dell'Unione impatta gravemente sulla tutela dei diritti fondamentali del singolo individuo[130].

Un'ultima postilla attiene all'ammissibilità di elementi di prova acquisiti sulla base di una normativa nazionale contraria al diritto dell'Unione: sulla base del richiamato principio di autonomia procedurale e, in particolare, del principio di effettività, ad avviso della Corte, nell'ambito di un procedimento penale nei confronti di persone sospettate della commissione di reati, il giudice nazionale è tenuto a escludere dalla propria valutazione elementi di prova ricavati dall'attività di conservazione generale e indiscriminata di dati soltanto nel caso in cui la persona interessata dalla sorveglianza non sia nelle condizioni di contestare la legittimità delle prove medesime[131].

In conclusione, tale sentenza consolida il recente orientamento della Corte di Lussemburgo sulla *data retention* per finalità di sicurezza nazionale: la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione può esser giustificata, secondo la Corte, soltanto dall'obiettivo della salvaguardia della sicurezza nazionale, la cui importanza supera quella degli altri obiettivi di cui all'art. 15 della direttiva 2002/58[132].

7. Osservazioni conclusive

La costante ricerca di un adeguato bilanciamento tra la tutela dei diritti fondamentali dell'individuo e la garanzia di interessi generali parimenti meritevoli di tutela vede impegnate la Corte di giustizia dell'Unione europea e la Corte europea dei diritti dell'uomo nell'elaborazione di criteri interpretativi informati, *inter alia*, ai principi di proporzionalità e di stretta necessità, da intendersi quali principi di "minima interferenza" nei diritti fondamentali dei singoli.

Dinanzi, poi, a questioni di "ultima generazione" come quella fin qui proposta[133], entrambe le Corti non si sottraggono da interpretazioni evolutive, all'occorrenza

[130] *Ibidem*, par. 112.
[131] *Ibidem*, par. 127-128 che riprende la sentenza del 2 marzo 2022, *H.K. c. Prokuratuur*, cit., parr. 41-44.
[132] Appare difficile che le pronunce attese nei prossimi mesi sulle medesime questioni possano discostarsi dal suddetto orientamento. Cfr. Conclusioni dell'Avvocato generale M. CAMPOS SÁNCHEZ-BORDONA, presentate il 18 novembre 2021, nelle cause riunite C-793/19 e C-794/19 *Bundesrepublik Deutschland c. SpaceNet AG Telekom Deutschland GmbH*, e nelle cause riunite C-339/20 e C-397/20, *VD e SR*.
[133] L. S. ROSSI, *Brevi osservazioni sulle recenti tendenze evolutive della giurisprudenza della Corte di Giustizia dell'Unione europea sulla protezione dei dati personali,* in *Eurojus*, 2020, fasc. speciale "*Mercato*

spingendosi oltre i confini letterari della singola disposizione normativa al fine di ricomprendere, nell'ambito di applicazione della stessa, fattispecie del tutto inedite (art. 8 CEDU, emblema del "*carattere di* living instrument *della Convenzione*"[134]), o comunque riempiendo di significato norme dal contenuto piuttosto ampio (art. 15 della direttiva 2002/58/CE). In tale contesto, il riconoscimento della legittimità (di carattere generale, a Strasburgo; eccezionale, a Lussemburgo) della raccolta indiscriminata dei dati relativi al traffico telefonico e all'ubicazione degli utenti per finalità di sicurezza nazionale determina uno spostamento della linea di confine tra ciò che è "necessario in una società democratica" e ciò che costituisce un'inaccettabile compressione dei diritti fondamentali dell'individuo.

Restringendo la visuale allo spazio di libertà, sicurezza e giustizia, se da un lato si evidenzia come il diritto dell'Unione europea, come interpretato dalla Corte di Lussemburgo, continui a garantire "*una protezione più estesa*"[135] mediante la previsione di diversi regimi di conservazione dei dati da potersi applicare anche congiuntamente, dall'altro lato, la contestuale emersione di una sorta di convergenza nella giurisprudenza delle due Corti europee sembra declinare la dicotomia *privacy vs. security* in senso favorevole al secondo elemento, rafforzando altresì l'orientamento degli Stati membri teso a preservare ad ogni costo il proprio margine di apprezzamento nelle questioni attinenti la materia della sicurezza nazionale[136].

È il caso dell'ordinamento italiano, la cui disciplina sulla *data retention* prevede - anche a seguito dei recenti interventi di riforma[137] - un generale limite temporale di conservazione dei metadati pari a ventiquattro mesi per i dati relativi al traffico telefonico, dodici mesi per quelli relativi al traffico telematico[138]; nel caso di contrasto al terrorismo o ad altri gravi reati, tale limite è di ben settantadue mesi[139] (ben oltre i ventiquattro

Unico Digitale, dati personali e diritti fondamentali", pp. 51-56 in cui è definito "*multifocale"* il bilanciamento tra il diritto alla *privacy* e la pluralità di interessi e diritti spesso confliggenti con il primo.

[134] Così A. DI STASI, *Introduzione alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, III ed., Milano, 2022, p. 11.

[135] Art. 52, par. 3, della Carta dei diritti fondamentali. Cfr. Conclusioni dell'Avvocato generale M. C. SANCHEZ-BORDONA, *Commissioner of An Garda Síochána,* par. 38.

[136] Cfr. M. ZALNIERIUTE, *A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence*, in *EJIL:Talk!*, 4 giugno 2021, reperibile *online*. Si veda anche V. MITSILEGAS, E. GUILD, E. KUSKONMAZ, N. VAVOULA*, Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks,* in *European Law Journal,* 12 maggio 2022, reperibile *online* secondo cui *"Though both European courts are in principle in alignment, their interaction is much more complex, and it is hoped that the seemingly more lenient approach of the ECtHR will not lead to further downgrading of the standards of protection as elaborated by the CJEU"*.

[137] Legge 23 novembre 2021, n. 178 di conversione, con modificazioni, del decreto legge 30 settembre 2021, n. 132, *recante misure urgenti in materia di giustizia e di difesa, nonché' proroghe in tema di referendum, assegno temporaneo e IRAP.* Sull'argomento, si rinvia a CORTE DI CASSAZIONE, Ufficio del Massimario e del Ruolo, Relazione n. 67 del 2 dicembre 2021 a cura di M. ACIERNO, G. ANDREAZZA, A. NATALINI.

[138] Art. 132 del Decreto legislativo 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*.

[139] Art. 24 della Legge 20 novembre 2017, n. 167, *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea - Legge europea 2017.*

previsti nell'abrogata direttiva 2006/24)[140]. In tale scenario, è concreto il rischio di una sorta di "normalizzazione" della conservazione generalizzata, tenuto conto che i fornitori di servizi non possono, ovviamente, conoscere *a priori* il livello di gravità dei reati perseguiti[141].

Altro profilo parimenti meritevole di attenzione è il crescente contributo operativo dei *service providers*[142] anche nel *volet* della cooperazione di polizia, tenuto conto delle quantità sempre maggiori di dati personali detenute dagli stessi di potenziale rilievo per le indagini penali; in tale contesto, le recenti modifiche apportate al regolamento (UE) 2016/794 *che istituisce l'Agenzia dell'Unione europea per la cooperazione nelle attività di contrasto (Europol)* intendono intensificare la cooperazione tra l'Agenzia e le parti private, prevedendo che le stesse inviino direttamente ad Europol i dati acquisiti al fine di sostenere le azioni degli Stati membri nel contrasto a specifiche fattispecie delittuose consumatesi *online*[143]. Altro canale di cooperazione è quello instaurato dal nuovo regolamento (UE) 2021/784, mediante l'introduzione del c.d. "ordine di rimozione" che obbliga i *service providers* a rimuovere contenuti terroristici *online*[144] entro un'ora dal suo ricevimento, nonché a conservare tali contenuti per un periodo di successivi sei mesi per finalità di indagine. Inoltre, viene sancito l'obbligo per i fornitori particolarmente esposti all'utilizzo improprio da parte di terzi di adottare misure specifiche per proteggere i propri servizi dalla diffusione al pubblico di contenuti terroristici, nel rispetto dei "*diritti fondamentali degli utilizzatori e tenendo conto, in particolare, della fondamentale*

---

[140] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico* del 22 luglio 2021, reperibile qui in cui si invitano Parlamento e Governo italiano a una riforma della disciplina della *data retention* che preveda limiti temporale di conservazione dei dati compatibili con il principio europeo di proporzionalità.

[141] In dottrina, tra gli altri, 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 AIC,* 2022, n. 1, pp. 125-166; V. PALLADINI, Data retention *e privacy in rete: verso una regolazione conforme al diritto UE?,* in *Rivista italiana di informatica e diritto,* 2022, n. 1, reperibile *online*.

[142] Cfr. P. STANZIONE, *Introduzione*, in P. STANZIONE (a cura di), *I "poteri privati" delle piattaforme e le nuove frontiere della privacy*, Torino, 2022, p. 14 a proposito del confine tra *public* e *private enforcement* che, secondo l'Autore, necessita di esser chiarito *"con nettezza soprattutto rispetto all'incidenza che tali decisioni hanno sui diritti e le libertà fondamentali, distinguendo responsabilità primaria e secondaria delle piattaforme"*.

[143] Regolamento (UE) 2022/991 del Parlamento Europeo e del Consiglio, dell'8 giugno 2022, *che modifica il regolamento (UE) 2016/794 per quanto riguarda la cooperazione di Europol con le parti private, il trattamento dei dati personali da parte di Europol a sostegno di indagini penali, e il ruolo di Europol in materia di ricerca e innovazione,* in GUUE, L 169, 27 giugno 2022, pp. 1-42.

[144] Regolamento (UE) 2021/784 del Parlamento europeo e del Consiglio, del 29 aprile 2021, *relativo al contrasto della diffusione di contenuti terroristici online*, in GUUE L 172, del 17 maggio 2021, pp. 79-109, in cui per "contenuti terroristici", ai sensi dell'art. 2, n. 7), si fa riferimento a materiali pubblicati sulla Rete che possano istigare la commissione di reati terroristici da parte di singolo o di gruppi terroristici. Nella definizione rientrano, altresì, i contenuti che forniscono indicazioni per la fabbricazione o l'uso di esplosivi, armi o sostanze nocive, nonché su metodi o tecniche finalizzati alla perpetrazione di condotte terroristiche individuate dall'art. 3 della direttiva (UE) 2017/541 *sulla lotta contro il terrorismo,* in GUUE L 88, del 31 marzo 2017, pp. 6-21.

importanza che riveste la libertà di espressione e di informazione in una società aperta e democratica"[145].

Tali iniziative si inseriscono nella più ampia strategia della Commissione europea denominata "*Unione della sicurezza"* nella quale, se da un lato è ribadita la competenza esclusiva degli Stati membri in materia di sicurezza nazionale, dall'altro non si sottace la sostanziale "sovrapposizione" tra sicurezza nazionale e sicurezza interna dell'Unione[146].

Da qui, l'auspicio di uno sforzo "comune" che veda una più intensa cooperazione tra Stati membri, istituzioni dell'Unione e settore privato "*tanto più che l'industria possiede una parte importante dell'infrastruttura digitale e non digitale indispensabile per lottare efficacemente contro la criminalità e il terrorismo*"[147].

Il presupposto di tale sforzo "comune" è perfettamente intuibile, ovverosia il rispetto dei valori europei di cui all'art. 2 TUE (in particolare, democrazia, Stato di diritto, rispetto dei diritti umani), valori mediante i quali è possibile guardare alla sicurezza e al rispetto dei diritti fondamentali quali obiettivi non "*contrastanti, bensì coerenti e complementari*"[148].

Tale concetto trova efficace sintesi nelle Conclusioni generali dell'Avvocato generale Campos-Sanchez Bordona: la tutela della sicurezza "*non deve essere impostata solo pensando alla sua efficacia. Da ciò deriva la sua difficoltà, ma anche la sua grandezza quando i suoi mezzi e metodi rispettano i requisiti dello Stato di diritto, che significa anzitutto assoggettamento del potere e della forza ai limiti del diritto e, in particolare, a un ordinamento giuridico che trova nella difesa dei diritti fondamentali la ragione e il fine della sua esistenza. [...] Se si abbandonasse semplicemente alla mera efficacia, lo Stato di diritto perderebbe la qualità che lo contraddistingue e potrebbe diventare esso stesso, in casi estremi, una minaccia per il cittadino. Nulla potrebbe assicurare che, dotando il potere pubblico di strumenti esorbitanti per il perseguimento dei reati, mediante i quali esso potesse ignorare o svuotare di contenuto i diritti fondamentali, la sua azione incontrollata e totalmente libera non si risolverebbe in definitiva in un pregiudizio alla libertà di tutti*"[149].

Emerge, dunque, tutta la difficoltà di approdare a un punto di equilibrio nel contesto di nuove minacce - fisiche e digitali - che mettono in pericolo la stessa sopravvivenza della "*società europea*"[150]. In tale contesto, tanto la Corte di giustizia dell'Unione europea

[145] *Ibidem,* art. 5, par. 1.
[146] COMMISSIONE EUROPEA, Comunicazione al Parlamento europeo, al Consiglio europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni *sulla strategia dell'UE per l'Unione della sicurezza,* Bruxelles, 24 luglio 2020, COM(2020) 605 final, p. 1.
[147] *Ibidem*, p. 7.
[148] *Ibidem*, p. 2. Sulla garanzia della c.d. *human security* con particolare riguardo allo spazio di libertà, sicurezza e giustizia, A. DI STASI, *Diritti umani e sicurezza umana. Il «sistema» europeo*, Napoli, 2011, in particolare pp. 261-268.
[149] Conclusioni dell'Avvocato Generale M. CAMPOS SÁNCHEZ-BORDONA, *La Quadrature du Net*, cit. parr. 130-131.
[150] Nel senso di "*Una società priva di uno Stato, ma non priva degli Stati: gli Stati membri, infatti, con tutte le loro istituzioni, sono espressamente inclusi nella società europea*" in A. VON BOGDANDY, *La nostra società europea e la sua Conferenza sul futuro dell'Europa,* in *Quaderni costituzionali,* 2021, n. 3, pp. 699-

quanto la Corte europea dei diritti dell'uomo concorrono nella ricerca di un costante bilanciamento tra esigenze di sicurezza e diritti fondamentali, alla luce delle nuove minacce, ma anche delle nuove opportunità, del progresso tecnologico.

ABSTRACT: L'annullamento della direttiva 2006/24/CE ha innescato un fitto dialogo tra giudici nazionali e Corte di giustizia dell'Unione europea in ordine alla legittimità e proporzionalità delle misure statali in materia di *data retention* in rapporto alla tutela dei diritti fondamentali. In tale contesto la sentenza C-140/20, *Commissioner of An Garda Sìochana*, cristallizza il recente approdo della Corte teso a giustificare la conservazione generalizzata, preventiva e indiscriminata dei dati personali dei singoli dinanzi a esigenze di tutela delle funzioni essenziali e degli interessi fondamentali dello Stato rispetto a minacce reali ed attuali, o prevedibili, alla sua sicurezza.

KEYWORDS: *data retention* – art. 15 direttiva 2002/58/CE – diritti fondamentali – sicurezza nazionale – principio di proporzionalità.

THE DIFFICULT BALANCE BETWEEN NATIONAL SECURITY AND PROTECTION OF FUNDAMENTAL RIGHTS IN THE CJEU "DATA RETENTION SAGA"

ABSTRACT: The annulment of Directive 2006/24/EC has triggered a close dialogue between national courts and the Court of Justice of the European Union on the legality and proportionality of national data retention laws on the protection of fundamental rights. In this context, the judgment in case C-140/20, *Commissioner of An Garda Sìochana judgment*, crystallizes the recent position of the Court to justify the general and indiscriminate data retention vis-à-vis the need to protect the essential functions and fundamental interests of the State concerning genuine and present, or foreseeable, threats to its security.

KEYWORDS: Data Retention – Art. 15 Directive 2002/58/EC – Fundamental Rights – National Security – Principle of Proportionality.

701.