UNIVERSITÀ DEGLI STUDI DI MILANO

Facoltà di Giurisprudenza
Pubblicazioni del Dipartimento di Diritto pubblico italiano e sovranazionale

GIULIA FORMICI

LA DISCIPLINA DELLA *DATA RETENTION* TRA ESIGENZE SECURITARIE E TUTELA DEI DIRITTI FONDAMENTALI

UN'ANALISI COMPARATA

G. Giappichelli Editore

UNIVERSITÀ DEGLI STUDI DI MILANO

Facoltà di Giurisprudenza
Pubblicazioni del Dipartimento di Diritto pubblico italiano e sovranazionale

Studi di diritto pubblico

94

La Collana "Pubblicazioni del Dipartimento di Diritto pubblico italiano e sovranazionale" dell'Università degli Studi di Milano raccoglie monografie e altri risultati inediti di ricerche, individuali e collettive, di studiosi che svolgono attività di studio e ricerca nel Dipartimento.
Essa comprende Studi di Diritto costituzionale, di Diritto amministrativo, di Diritto internazionale ed europeo, di Diritto processuale civile, di Diritto comparato, di Storia del diritto, di Politica economica.
La qualità scientifica delle pubblicazioni è assicurata da una procedura di c.d. double blind peer review *ad opera di revisori esterni.*

GIULIA FORMICI

LA DISCIPLINA DELLA *DATA RETENTION* TRA ESIGENZE SECURITARIE E TUTELA DEI DIRITTI FONDAMENTALI

UN'ANALISI COMPARATA

G. Giappichelli Editore

VIA PO, 21 - TEL. 011-81.53.111 - FAX 011-81.25.100
http://www.giappichelli.it

ISBN/EAN 978-88-921-4210-7
ISBN/EAN 978-88-921-9950-7 (ebook - pdf)

Il volume è pubblicato con il contributo del Dipartimento di Diritto pubblico italiano e sovranazionale dell'Università degli Studi di Milano.

Stampa: Stampatre s.r.l. - Torino

Ai miei genitori e a mia sorella,
per il loro costante incoraggiamento.

A Stefano,
per aver reso più leggera ogni fatica.

INDICE

pag.

Introduzione 1

CAPITOLO 1

SISTEMI DI CONSERVAZIONE DEI METADATI
PER SCOPI SECURITARI E DIRITTI FONDAMENTALI
ALLA RISERVATEZZA E ALLA PROTEZIONE DEI DATI

1. I sistemi di conservazione e accesso ai metadati come strumenti di lotta alla criminalità e al terrorismo: potenzialità e rischi 19
2. I diritti fondamentali alla riservatezza e alla protezione dei dati: cenni ricostruttivi 26
   2.1. Il diritto alla riservatezza: dalle origini negli USA al riconoscimento nel continente europeo 26
   2.2. Dalla dimensione negativa a quella positiva: il progressivo affermarsi del diritto alla protezione dei dati 34
3. La *data retention* tra esigenze securitarie e tutela dei diritti fondamentali: una rinnovata sfida 45

pag.

CAPITOLO 2
LA LUNGA E ARTICOLATA *DATA RETENTION SAGA:* IL COMPLESSO DIALOGO TRA LEGISLATORE EUROPEO, CORTE DI GIUSTIZIA DELL'UE E CORTI NAZIONALI

1. La disciplina normativa della *data retention* nell'Unione europea: dalla Direttiva *e-Privacy* alla *Data Retention Directive* 56
2. Gli Stati membri e la trasposizione della DRD, tra criticità attuative e rilevanti decisioni delle Corti nazionali: un primo dibattito interno 63
3. La storica pronuncia *Digital Rights Ireland*: la CGUE invalida la DRD 68
   3.1. La significativa portata della sentenza *Digital Rights Ireland* e i primi dubbi interpretativi 76
4. Le reazioni degli Stati membri e delle Istituzioni europee all'intervento della CGUE: una situazione confusa 80
5. La CGUE chiamata nuovamente a pronunciarsi sulla conformità del regime di conservazione generalizzata rispetto alla Carta di Nizza: la sentenza *Tele2* 87
6. Una rinnovata frammentarietà di approcci all'indomani della pronuncia *Tele2*: le problematiche "interpretazioni difensive" adottate dagli Stati membri 92
7. L'art. 15 Direttiva *e-Privacy* sottoposto ancora una volta all'intervento chiarificatore della CGUE: la sentenza *Ministerio Fiscal* e i requisiti dell'accesso ai metadati conservati 98
8. Le importanti sentenze *La Quadrature du Net*, *Privacy International* e *H.K.*: la *data retention saga* al capolinea? 104
   8.1. La delicata determinazione dell'ambito di applicazione del diritto dell'UE 104
   8.2. I limiti dello strumento di conservazione generalizzata e l'inedita distinzione tra sicurezza nazionale e sicurezza pubblica 108
   8.3. Il difficile tentativo di sintesi di una "sconfitta vittoriosa" 114
   8.4. La sentenza *H.K. c. Prokuratuur* e le nuove importanti specificazioni sulla disciplina dell'accesso ai metadati 120

pag.

9. Prevedere l'imprevedibile: le profonde ed incerte conseguenze sul piano europeo e nazionale della più recente giurisprudenza della CGUE 124
9.1. L'impatto sui rinvii pregiudiziali ancora pendenti: un esito già scritto o un persistente bisogno di chiarezza? 125
9.2. Verso il risveglio del legislatore europeo da tempo silente: i rischi e le sfide di un rinnovato intervento normativo sovranazionale 130
9.3. Le attese mosse di legislatori e Corti nazionali. Prime considerazioni a partire dalle sentenze della *Cour Constitutionnelle* belga e del *Conseil d'État* francese 137

CAPITOLO 3

L'UNIONE EUROPEA SI CONFRONTA CON L'ESTERNO: LA GARANZIA EXTRA-TERRITORIALE DEGLI STANDARD EUROPEI DI PROTEZIONE DEI DATI ALLA PROVA DELLA CORTE DI GIUSTIZIA DELL'UE NEI CASI DI *DATA TRANSFER* VERSO USA E CANADA

1. La normativa europea in materia di trasferimento dati verso Stati terzi 147
2. Il trasferimento dati UE-USA al vaglio della CGUE: il caso *Schrems c. Data Protection Commissioner* 152
3. Dai principi *Safe Harbour* alle salvaguardie disposte nel *Privacy Shield*: un discusso compromesso 158
4. Un nuovo capitolo della *Schrems saga*: la sentenza della CGUE 16 luglio 2020, C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems* 164
5. Le dirompenti ripercussioni della decisione *Schrems II*: il difficile futuro del trasferimento dati UE-USA (e non solo) 170
6. La disciplina del trasferimento di PNR oltre i confini dell'UE: la bozza di accordo UE-Canada e il *Parere 1/15* della CGUE 179
7. Una ricognizione delle più significative implicazioni del *Parere 1/15* fuori e dentro i confini dell'UE 190
7.1. La necessaria rinegoziazione dell'accordo con il Canada e i dubbi quanto alla conformità alla Carta di Nizza degli accordi in materia di PNR vigenti 190

pag.

7.2. La Direttiva 2016/681 e un destino incerto: i rinvii pregiudiziali pendenti 194
8. Uno sguardo critico alla disciplina europea in materia di trasferimento dati verso Stati terzi: debolezze e successi in uno scenario in divenire 198

CAPITOLO 4

IL REGNO UNITO.
LA DISCIPLINA DELLA *DATA RETENTION*:
SPINTE CONTRAPPOSTE ALL'OMBRA DELL'INEDITA
SFIDA DELLA *BREXIT*

1. Il diverso approccio di legislatori e Corti nazionali in materia di *data retention*: una necessaria premessa sull'importanza dell'analisi comparata 218
2. Il legislatore del Regno Unito e la disciplina della *data retention* 221
2.1. Un sostanziale cambio di approccio: dalla volontarietà della conservazione dei metadati al *Data Retention (EC Directive) Regulations 2009* 221
2.2. Le rapide e dibattute reazioni del legislatore nazionale alla sentenza *DRI*: il *Data Retention and Investigatory Powers Act* (DRIPA) 226
2.3. L'adozione dell'*Investigatory Powers Act* (IPA) nelle more del caso *Tele2* 229
2.4. Le modifiche alla disciplina nazionale apportate dal *Data Retention and Acquisition Regulations 2018* 235
3. Le Corti inglesi e i principi delineati dalla giurisprudenza sovranazionale, tra divergenze e avvicinamenti 238
3.1. La decisione della *High Court* in merito alla compatibilità del DRIPA con il diritto dell'UE 238
3.2. La diversa lettura fornita dalla *Court of Appeal*: i motivi del primo rinvio pregiudiziale ai giudici di Lussemburgo 242
3.3. Le valutazioni della *Court of Appeal* a seguito della pronuncia *Tele2*: una complessa decisione tra mutamenti del quadro normativo e importanti casi giurisprudenziali pendenti 244

pag.

3.4. La sentenza della *High Court* nel caso *Liberty* avente ad oggetto la *Part 4* dell'IPA 248
3.5. Le pronunce dell'*Investigatory Powers Tribunal*: il rinvio alla CGUE nel caso *Privacy International* e la decisione finale del 22 luglio 2021 253
4. Provvisorie considerazioni sulla disciplina inglese della *data retention*: ulteriori e doverosi interventi all'orizzonte? 259
5. Garantire il flusso di dati UE-Regno Unito nello scenario *post-Brexit*: il dibattito sull'adeguatezza delle garanzie offerte Oltremanica 263
5.1. Il lento e difficile cammino verso l'adozione di una decisione di adeguatezza 263
5.2. L'auspicata – e criticata – decisione di adeguatezza del 28 giugno 2021: un instabile destino per il trasferimento dati Oltremanica? 268

CAPITOLO 5
IL BELGIO. DALLA *COUR CONSTITUTIONNELLE* AL LEGISLATORE NAZIONALE, PASSANDO PER LUSSEMBURGO

1. L'iniziale approccio "pro-securitario" del legislatore belga in materia di *data retention* e i primi dubbi sulla proporzionalità di una conservazione generalizzata 276
2. La *Cour constitutionnelle* annulla la normativa nazionale sulla conservazione dei metadati: l'unicità dell'*Arrêt* 11 giugno 2015, n. 84 286
3. La *Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques* 292
3.1. La necessaria adozione di una nuova normativa sulla conservazione e accesso ai metadati: il complesso dibattito emerso dai *Travaux préparatoires* 292
3.2. Un difficile compromesso tra efficienza ed elevata tutela dei diritti alla riservatezza e protezione dei dati 294

pag.

4. L'ulteriore intervento della *Cour constitutionnelle* e il dialogo con la CGUE: andata e ritorno 301
4.1. Il ricorso di annullamento avverso la legge del 2016: le contrastanti letture della giurisprudenza della CGUE promosse da Governo e ricorrenti 301
4.2. L'*Arrêt interlocutoire* 19 luglio 2018, n. 96: un necessario chiarimento quanto alla cumulativa sussistenza dei requisiti fissati a livello europeo 306
4.3. Di ritorno da Lussemburgo: la decisa risposta dei giudici costituzionali belgi nell'*Arrêt* 22 aprile 2021, n. 57 309
4.4. Ancora una difficile prova per il legislatore belga: cenni all'*Avant-project de loi* proposto dal Governo 313
5. Un approfondito dibattito legislativo e una attenta considerazione dei criteri enunciati dalla giurisprudenza della CGUE: ingredienti per un approccio virtuoso o per un fallimento annunciato? 316

CAPITOLO 6
L'ITALIA. I MOLTEPLICI INTERVENTI NORMATIVI E GIURISPRUDENZIALI IN MATERIA DI *DATA RETENTION*, TRA OCCASIONI PERDUTE E UN DIBATTITO CHE FATICA AD AFFERMARSI

1. La disciplina normativa in materia di *data retention* 321
1.1. Il frenetico susseguirsi di modifiche all'art. 132 Codice Privacy 321
1.2. Dalle deroghe legate ad esigenze emergenziali alla Legge Europea 2017, sino al d.lgs. 10 agosto 2018, n. 101 329
2. Le Corti italiane e la *data retention*: una lettura restrittiva dei principi e criteri definiti dalla CGUE 341
2.1. La sentenza della Corte costituzionale 14 novembre 2006, n. 372: una conferma del corretto bilanciamento tra diritti fondamentali e garanzia della sicurezza 341
2.2. La rilevante e discussa Ordinanza del Tribunale di Padova: una prima presa di posizione dei giudici italiani dinnanzi alle pronunce della CGUE 345

pag.

2.3. La costante giurisprudenza della Corte di Cassazione: un approccio "rassicurante" 349
3. Dall'impegno di riforma assunto dal Governo al rinvio pregiudiziale promosso dal Tribunale di Rieti: l'Italia verso una reale svolta? 359
3.1. Le ripercussioni della sentenza *H.K. c. Prokuratuur* nel contesto italiano 359
3.2. Il mancato dibattito sulla proporzionalità della conservazione generalizzata: necessarie riflessioni 368

Conclusioni 373

Bibliografia 395

INTRODUZIONE

«The danger threatening democratic societies (…) stems from the temptation facing public authorities to "see into" the life of the citizens» [1]: questa affermazione, scritta con lucidità e lungimiranza nel lontano 1984 da Louis-Edmond Pettiti, all'epoca giudice della Corte europea dei diritti dell'uomo, colpisce ancora oggi per la sua estrema attualità.

Nell'estate 2021, infatti, una vasta inchiesta internazionale promossa da diverse testate giornalistiche e organizzazioni non governative ha svelato l'esistenza di un insidioso *spyware* denominato Pegasus, utilizzato per estrarre dai dispositivi telefonici immagini, messaggi, e-mail, informazioni condivise nelle *app* installate ed in grado anche di registrare le telefonate e attivare il microfono. Secondo quanto riportato dalla società israeliana creatrice del sistema di sorveglianza, esso sarebbe impiegato da diversi Governi in tutto il mondo al solo fine della lotta al terrorismo e alla criminalità, soprattutto transfrontaliera; l'indagine pubblicata ha invece rivelato come destinatari di tale invasivo strumento di controllo siano in realtà anche giornalisti, politici e attivisti di organizzazioni non governative per la tutela dei diritti fondamentali [2].

---

[1] Corte europea dei diritti dell'uomo, 2 agosto 1984, *Malone v. United Kingdom*, *Application* n. 8691/79, *Concurring opinion* del Giudice Pettiti, para. 5.

[2] L'inchiesta è stata pubblicata, tra gli altri, da D. PRIEST, C. TIMBERG, S. MEKHENNET, *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, in *The Washington Post*, 1 luglio 2021; per alcuni primi commenti, si rinvia a N. KRACK, *The myth of Pegasus: journalists safety and press freedom as modern chimaera? Story of the abusive use of a military spyware*, in *CiTiP Law Blog*, 27 luglio 2021; S. WOODHAMS, *Spyware: an unregulated and escalating threat to independent media*, Center for International Media Assistence, agosto 2021.

Impossibile non leggere nelle pieghe di questa notizia l'eco delle rivelazioni di Edward Snowden, il più noto – e ancora ricercato – *whistleblower* della storia recente: nel 2013, infatti, sono stati resi noti i potenti sistemi di raccolta, intercettazione e analisi su ampia scala di dati e metadati derivanti da mezzi di telecomunicazione posti in essere dalla *National Security Agency* statunitense [3], realizzati in completa segretezza per scopi di *foreign intelligence* e subordinati a limitazioni e garanzie ampiamente criticate da studiosi e società civile per la loro parzialità e insufficienza a costituire un efficace argine alla discrezionalità delle autorità di intelligence.

Una tendenza, quella ad adottare strumenti di controllo e sorveglianza, che non risulta certamente limitata ai due esempi sin qui citati ma che si concretizza in molteplici forme, dalla diffusione di strumenti di riconoscimento facciale negli spazi pubblici fondati sulla raccolta e trattamento di dati biometrici [4], alla recente adozione di sistemi di tracciamento – *contact tracing* – promossi durante la pandemia da Covid-19 quale una delle possibili armi di difesa e prevenzione alla diffusione del virus che ha

---

[3] Il contenuto delle rivelazioni sarà oggetto di approfondita disamina nel presente lavoro. Per una ricostruzione di tali complesse vicende si rimanda preliminarmente a G. GREENWALD, *No place to hide: Edward Snowden, the NSA and the US surveillance state*, Hamish Hamilton, Londra, 2014.

[4] Questa discussa tecnologia consente, mediante l'impiego dei dati biometrici e di strumenti di Intelligenza Artificiale, di ricostruire un *template* della struttura e delle caratteristiche del viso e di compararlo con immagini contenute in una apposita banca dati di raffronto. Sul dibattito circa la proporzionalità e necessità di un simile strumento – peraltro oggetto di particolare attenzione nel contesto europeo nella Proposta di Regolamento che stabilisce regole armonizzate sull'Intelligenza Artificiale e modifica alcuni atti legislativi dell'UE, COM/2021/206final, presentata dalla Commissione il 21 aprile 2021 – si leggano, tra i molti H. RUHRMANN, *Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement,* University of California Berkeley, Berkeley, 2019; F. PAOLUCCI, *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1, 2021, p. 204 ss.; G. MOBILIO, *Tecnologie per il riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021; R. DUCATO, *Il riconoscimento facciale tra rischi di 'mitridatizzazione sociale' e prospettive di regolamentazione*, in L.E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, Napoli, 2021, p. 187 ss.

tragicamente scosso il mondo intero dal 2020[5]. Tutti i sistemi richiamati condividono comuni caratteristiche da ravvisarsi nella raccolta e disponibilità di dati – seppur di diversa natura – che, grazie a meccanismi di analisi algoritmica e di Intelligenza Artificiale[6], consentono di trarre rilevanti informazioni sulla vita privata dei target, realizzando una forma di sorveglianza pervasiva posta in essere primariamente da soggetti pubblici per perseguire l'obiettivo di una efficiente prevenzione e repressione di minacce alla sicurezza. Questa sempre più rilevante propensione ad un impiego espansivo di strumenti di controllo si mostra poi in tutta la sua complessità e delicatezza laddove inserita nel più ampio contesto storico caratterizzante i primi decenni del nuovo Millennio: l'emergenza terroristica e il cronicizzarsi delle esigenze securitarie[7] da un lato e il progresso

[5] Sul punto, G. TROPEA, *Il contact tracing digitale e l'epidemia: sindrome cinese?*, in *LaCostituzione.info*, 9 aprile 2020; M. FARINA, *La data protection ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, in *BioLaw Journal*, 20 marzo 2020; G. DELLA MORTE, *La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, in *SIDI Blog*, 30 marzo 2020; G. DE MINICO, *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *LaCostituzione.info*, 1 aprile 2020; S. CRESPI, *Applicazione di tracciamento Immuni tra normative nazionale e diritto UE in materia di protezione dei dati personali*, in *Freedom, Security & Justice*, 2, 2020, p. 20 ss. Organizzazione per la cooperazione e lo sviluppo economico (OECD), *Tracking and tracing COVID: protecting privacy and data while using apps and biometrics*, 2020.

[6] L'Intelligenza Artificiale è definibile come «un insieme di tecnologie che combina dati, algoritmi e potenza di calcolo», COMMISSIONE EUROPEA, *Libro Bianco sull'intelligenza artificiale. Un approccio europeo all'eccellenza e alla fiducia*, 19 febbraio 2020. Si leggano sul punto G. ALPA (a cura di), *Diritto e intelligenza artificiale*, Pacini Giuridica, Pisa, 2020; U. RUFFOLO (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Giappichelli, Torino, 2021, nonché la bibliografia richiamata nel Capitolo 1 del presente lavoro, in cui questa importante tecnologia viene ricostruita.

[7] G. DE VERGOTTINI, *La 'guerra' contro un nemico indeterminato*, in *Forum di Quaderni costituzionali*, 5 ottobre 2001, p. 1 ss. Il concetto di "normalizzazione dell'emergenza" viene ripreso anche, *ex multis*, da A. VEDASCHI, *A' la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Giappichelli, Torino, 2007; G.M. FLICK, *Dei diritti e delle paure*, in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, ESI, 2009; T. GROPPI, *Democrazia e terrorismo,* ESI, Napoli, 2009; G. DE MINICO*, Costituzione. Emergenza e terrorismo*, Jovene, Napoli, 2016; L. FORNI, T. VETTOR (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Giappichelli, Torino, 2018.

tecnico-scientifico [8] dall'altro, hanno infatti accelerato e rafforzato quella che è stata definita la «illusory conviction that global surveillance is the *deus ex machina* capable of combating the scourge of global terrorism» [9] e di altri pericoli per la sicurezza pubblica e nazionale.

Tale marcata deriva *pro-securitaria* ha tuttavia ben presto mostrato tutte le sue debolezze e le profonde e non più ignorabili insidie, grazie non solo all'attivismo della società civile ma anche all'attento lavoro di tante Corti nazionali e sovranazionali: soprattutto da questa giurisprudenza è emersa la ricostruzione di forme ampie di sorveglianza, capaci di interferire nella sfera privata di ciascun individuo anche a solo scopo preventivo e di controllo, ovvero in maniera sconnessa ed indipendente dalla concreta presenza di sospetti o reali minacce alla sicurezza. L'impiego di strumenti tecnologicamente avanzati di controllo dei dati produce così un forte impatto sulla effettiva garanzia e salvaguardia dei diritti fondamentali, non solo di quelli alla riservatezza e alla protezione dei dati, senza dubbio più direttamente compressi, bensì, in senso più ampio, del principio di presunzione di innocenza e delle stesse libertà personali che

---

[8] Tutti i settori, dalla sanità al lavoro, dall'istruzione alla comunicazione ed informazione, dal trasporto alle previsioni metereologiche, sono stati rivoluzionati dal mondo dei *bit*, dei *Big Data* e dei c.d. metadati, ovvero dati che non attengono al contenuto di telecomunicazioni ma che sono mediante le stesse prodotti, quali i dati di traffico ed ubicazione che forniscono informazioni sulla data e ora di una chiamata, sul mittente e destinatario di una mail, sulla geolocalizzazione al momento di una telefonata o di un accesso al Web. Anche la garanzia della sicurezza ha potuto beneficiare di strumenti sofisticati e all'avanguardia di analisi automatizzata dei dati che hanno permesso di svolgere attività di prevenzione nonché di implementare ed accrescere le capacità investigative, così da assicurare la disponibilità di un vasto insieme di informazioni in grado di creare collegamenti tra soggetti sconosciuti alle pubbliche autorità: si pensi ai nuovi – ma già ampiamente utilizzati – sistemi di riconoscimento facciale, di *predictive policing* o all'impiego di banche dati genetiche e biometriche sempre più ampie; in questo senso, quindi, la tecnologia si pone come una «nuova frontiera della sicurezza», M. BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: o dei diritti "violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 3, 2016, p. 1.

[9] *Concurring opinion* del giudice della Corte europea dei diritti dell'uomo (Corte EDU) Pinto de Albuquerque nella pronuncia 12 gennaio 2016, *Szabo e Vissy v. Hungary,* Application n. 37138/14, para. 20.

al rispetto della vita privata si collegano e alle quali si radica la stessa democraticità delle nostre società. Il pericolo, sempre più nettamente percepito, è che la diffusione di simili mezzi di sorveglianza, soprattutto se non debitamente regolati e sottoposti a limiti precisi e chiari, finisca col favorire l'affermarsi di scenari tutt'altro che fantascientifici di un *Big Brother* di orwelliana immaginazione [10] o di un Panopticon di benthamiana origine [11], facilitando la trasformazione verso una società *trasparente* [12] grazie alla realizzazione di forme di sorveglianza tecnologicamente avanzate e sempre più *liquide* [13].

A partire da simili considerazioni si è aperto un ampio dibattito che, centrato sull'esigenza di rileggere lo storico e problematico rapporto tra sicurezza e diritti fondamentali [14] nel mutato contesto della società digita-

---

[10] G. ORWELL, *1984*, Secker&Warburg, Londra, 1949.

[11] J. BENTHAM, *Panopticon or the inspection-house*, T. Payne, Londra, 1791. Si legga però anche M. FOUCAULT, M. PIERROT (a cura di), *Jeremy Bentham. Panopticon ovvero la casa d'ispezione*, nella traduzione italiana di V. Fortunati, Marsilio, Venezia, 1997. Il progetto di carcere ideato da Bentham era basato sulla realizzazione di una struttura circolare in grado di garantire un continuo e perenne controllo operato da un sorvegliante centrale, celato alla vista dei prigionieri. Il principio di fondo era quello secondo cui la convinzione della invisibile e costante sorveglianza inducesse, per sé stessa, i prigionieri – che non potevano stabilire in quale momento e se fossero sottoposti a osservazione o meno – a comportarsi sempre in maniera retta.

[12] È l'espressione utilizzata da David Brin nel suo celebre *The transparent society. Will technology force us to choose between privacy and freedom?*, Perseus Books, New York, 1998.

[13] Il termine è mutuato da Z. BAUMAN, D. LYON, *Liquid surveillance. A conversation*, Polity Press, Cambridge, 2013: l'immagine della "liquidità" ben trasmette l'idea di una sorveglianza pervasiva e dilagante in ogni ambito della vita moderna. Gli autori suggeriscono il superamento della visione Benthamiana e l'avvento di una modernità *post-panottico*, nella quale le nuove tecnologie e la loro architettura mobile, flessibile e mutevole rendono ormai superflui i muri e le strutture in mattoni ideate da Bentham.

[14] In via preliminare ma con rinvio alla bibliografia contenuta nel Capitolo 1, si consultino: G. DE VERGOTTINI, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Il Mulino, Bologna, 2004; C. WALTER (a cura di), *Terrorism as challenge for national and international law: security versus liberty?*, Springer, Berlino, 2004; V. BALDINI, *Sicurezza e libertà nello Stato di diritto in trasformazione*, Giappichelli, Torino, 2004; E. POSNER, A. VERMEULEN, *Terror in balance: security, liberty and the Courts*, Oxford Uni-

lizzata e iper-connessa, rappresenta senza dubbio una delle più grandi sfide delle democrazie stabilizzate [15] e non solo [16]. Ciò che mette alla prova legislatori e Corti è la rinnovata necessità di elaborare tutele e limiti che, rifuggendo una semplicistica visione di *trade-off* [17], giungano piuttosto a

---

versity Press, Cambridge, Massachusetts, 2007; AA.VV., *Convegno AIC, Libertà e sicurezza nelle democrazie contemporanee. Atti del Convegno annuale, Bari, 17-18 ottobre 2003: annuario 2003*, Cedam, Padova, 2008; M. CALVINO, M.G. LOSANO, C. TRIPODINA (a cura di), *Lotta al terrorismo e tutela dei diritti fondamentali*, Giappichelli, Torino, 2009; C. BASSU, *Terrorismo e costituzionalismo. Percorsi comparati*, Giappichelli, Torino, 2010. In tale contesto si inserisce anche l'ampio dibattito, apertosi nel contesto italiano, quanto alla possibilità di definire la sicurezza quale interesse collettivo, diritto soggettivo o valore superprimario: *ex multis* si rimanda a P. TORRETTA, *Diritto alla sicurezza e (altri) diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'ALOIA (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Giuffrè, Milano, 2003, p. 451 ss.; T.E. FROSINI, *Il diritto costituzionale alla sicurezza,* in *Forum di Quaderni costituzionali*, 2006, p. 1 ss.; G. CERRINA FERONI, G. MORBIDELLI, *La sicurezza: un valore super primario*, in *Percorsi Costituzionali*, 1, 2008, p. 31 ss.; T.F. GIUPPONI, *La sicurezza e le sue dimensioni costituzionali*, in S. VIDA (a cura di), *Diritti umani. Teorie, analisi, applicazioni*, Bononia University Press, Bologna, 2008, p. 1 ss.; M. RUOTOLO, *La sicurezza nel gioco del bilanciamento*, in *Astrid Rassegna*, 2009; L. LORELLO, *Il dilemma sicurezza vs. libertà al tempo del terrorismo*, in *Democrazia e Sicurezza*, 2017.

[15] M. ZALNIERIUTE, *A struggle for competence: national security, surveillance and the scope of EU law at the Court of Justice of the EU*, in *Modern Law Review*, 85, 2021, p. 1.

[16] Il riferimento è ad ordinamenti, quale quello cinese, caratterizzati dall'adozione di ampi e pervasivi sistemi di controllo dei dati da parte delle autorità pubbliche, nei quali pare sempre più importante lo sviluppo di un serio dibattito sui limiti e le salvaguardie che debbono accompagnare l'impiego di strumenti di sorveglianza. In questo senso e quale segno di un primo rilevante tentativo di innalzare il livello di attenzione posto rispetto alla garanzia dei diritti alla riservatezza e alla *data protection*, è interessante notare come proprio la Cina abbia recentemente approvato una normativa in materia di tutela della protezione dei dati che entrerà in vigore il 1 novembre 2021 (per alcuni primi approfondimenti, si rimanda a F. PIZZETTI, *Il nuovo approccio cinese e l'importanza di un mercato unico digitale globale*, in *Agenda Digitale*, 27 agosto 2021).

[17] Per *trade-off* si intende una scelta tra due opzioni desiderabili in egual misura, seppure tra loro in contrasto. Nel contesto oggetto di analisi questo termine è stato impiegato, in maniera critica, da Solove che ha ritenuto falsa e scorretta una lettura del rapporto sicurezza-diritti fondamentali in termini di reciproca esclusione (D. SOLOVE, *Nothing to hide. The false tradeoff between privacy and security*, Yale University Press, New Haven, 2011).

garantire un punto di equilibrio tra spinte differenti, permettendo in ultima istanza di ricondurre le misure volte alla garanzia della sicurezza entro l'alveo dello Stato di diritto e della tutela dei diritti fondamentali.

In questo articolato contesto, una sfida di estrema attualità e delicatezza, che si pone come chiaramente esplicativa del sopra rilevato complesso rapporto tra esigenze securitarie e salvaguardia dei diritti fondamentali, è da individuarsi nella disciplina della c.d. *data retention* che si realizza nella previsione di un obbligo di conservazione di dati finalizzato al successivo – benché eventuale – accesso a tali informazioni da parte di autorità di *law enforcement* o agenzie di intelligence per scopi di prevenzione, indagine e repressione di reati o minacce alla sicurezza. Tali operazioni di memorizzazione preventiva, quali quelle ad esempio effettuate da fornitori privati di servizi di comunicazione elettronica, possono coinvolgere – e invero nella maggior parte dei casi coinvolgono – in maniera generalizzata ed indiscriminata tutti gli utenti e tutti i mezzi di telecomunicazione, consentendo così alle autorità pubbliche di disporre di un'enorme mole di dati e di poter "andare indietro nel tempo" [18] al fine di reperire informazioni utili a scopi investigativi, anche attinenti a soggetti previamente non noti alle forze dell'ordine e rispetto ai quali pertanto non sussisteva, al momento della conservazione, nessun sospetto tale da giustificare un controllo mirato delle comunicazioni o una intercettazione diretta [19].

Per quanto ogni dato o metadato, considerato singolarmente, possa apparire del tutto innocuo e incapace di interferire in maniera significativa nella sfera privata del soggetto cui si riferisce, è stato invece ormai riconosciuto [20] come l'esame della ingente quantità di dati conservati consen-

---

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

[19] Riassuntivamente ma incisivamente, «the aim of this bulk accumulation of data is to generate useful and reliable correlations and ultimately to generate suspects», M. ANDREJEVIC, *Surveillance in the big data era. Emerging pervasive information and communications technologies*, in *Law, Governance and Technology Series*, 11, 2014, p. 55.

[20] Sul punto, per alcuni utili e chiari esempi sulle capacità sconfinate della lettura aggregata di grandi quantità di dati (*Big Data analysis*), si rimanda a V. MAYER-SCHONBERGER, K. CUKIER, *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano, 2013. Anche la Corte di giustizia dell'UE e la Corte europea dei diritti dell'uomo hanno ampiamente riconosciuto la

ta, mediante tecniche di lettura aggregata e analisi algoritmica o sistemi di Intelligenza Artificiale, di determinare abitudini, stili di vita, connessioni tra soggetti e luoghi frequentati nonché, in taluni casi, di risalire persino ad informazioni attinenti allo stato di salute o all'orientamento politico o sessuale. Alla luce di simili considerazioni non può dunque che riconoscersi come anche la sola conservazione *in bulk* ovvero ampia e generalizzata, prima ancora ed indipendentemente dal successivo accesso ai dati, si concretizzi in una tutt'altro che marginale ingerenza nella vita privata, costituendo una minaccia seria e reale per la riservatezza e la protezione dei dati e per un fattivo controllo sulle informazioni che ciascun utente – più o meno consapevolmente – produce, oltre ad aprire a concreti pericoli di abusi sui dati stessi sotto forma, ad esempio, di un illegittimo utilizzo delle informazioni per finalità differenti da quelle per le quali essi vengono originariamente conservate.

Non stupisce pertanto che la disciplina della *data retention* e dell'accesso ai dati conservati, riconosciuta come uno dei terreni più delicati sul quale esigenze securitarie e garanzia dei diritti fondamentali si sono incontrate e scontrate [21], sia divenuta oggetto di un interessante e vivace dibattito normativo e giurisprudenziale nell'Unione europea, riportato ed analizzato in chiave critica nelle pagine del presente lavoro. Da decenni, infatti, le Istituzioni europee e la Corte di giustizia dell'UE (d'ora in avanti CGUE), nonché i legislatori e le Corti degli Stati membri si sono spesso interrogati sulla determinazione di salvaguardie e limiti all'obbligo di conservazione di dati e metadati per scopi securitari, in un ricco dialogo multilivello che risulta invero ancora del tutto aperto e in continuo

possibilità, resa ormai reale dal progresso tecnico-scientifico, di risalire ad abitudini e stili di vita, preferenze e relazioni sociali degli utenti anche impiegando i soli metadati: «questi dati [di traffico e ubicazione], presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati», Corte di giustizia dell'UE, 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications e al.*, para. 27.

[21] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018, p. 1 ss.

divenire. Sin dai primi anni Duemila gli Stati membri hanno esercitato una forte spinta nella direzione dell'adozione di una normativa sovranazionale in materia di *data retention*, ritenuta uno strumento irrinunciabile nella lotta al terrorismo e alla criminalità grave che proprio agli inizi del XXI secolo si era imposta quale obiettivo centrale e prioritario delle democrazie del vecchio continente. L'adozione della Direttiva 2006/24/CE, volta ad imporre agli Stati membri l'introduzione nei propri ordinamenti di un obbligo di conservazione generalizzata di metadati in capo ai fornitori di servizi di telecomunicazione, ha tuttavia incontrato serie resistenze espresse dalle numerose autorità preposte alla tutela dei diritti alla riservatezza e alla protezione dei dati nonché da cittadini e organizzazioni non governative, che hanno promosso un attivismo interessato ed acuto a garanzia dei diritti fondamentali lesi da forme di controllo e sorveglianza digitali. I dubbi e le preoccupazioni quanto alla conformità di regimi di *data retention* tanto alle Carte costituzionali nazionali quanto alla Carta di Nizza hanno ben presto portato a significativi e storici interventi delle Corti nazionali e della CGUE. Quest'ultima, sin dalla prima e determinante pronuncia *Digital Rights Ireland*[22], ha stabilito stringenti principi e requisiti di proporzionalità e necessità finalizzati a garantire la legittimità della compressione dei diritti fondamentali perpetrata dallo strumento della conservazione ed accesso ai metadati, che hanno addirittura condotto alla invalidazione della Direttiva 2006/24/CE stessa; gli Stati membri e il legislatore europeo hanno invece manifestato una certa riluttanza e una seria difficoltà attuativa della lettura fornita dai giudici di Lussemburgo, i cui principi non sono dunque spesso stati *in toto* incorporati nelle normative nazionali o sovranazionali adottate sulla base dell'ancora oggi vigente art. 15 Direttiva 2002/58/CE che attribuisce, in termini estremamente vaghi, ai legislatori nazionali la facoltà di derogare all'obbligo generale di cancellazione dei metadati raccolti da fornitori di servizi di telecomunicazione, qualora tale deroga si renda necessaria per perseguire specifiche finalità elencate, tra cui anche la garanzia della sicurezza e la repressione dei reati. Così, quella che è divenuta nota come la *data retention saga*, correlata da diverse ma certamente connesse pronunce in mate-

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

ria di trasferimento dati verso Stati terzi [23], ha determinato la nascita di un articolato dibattito e dialogo – talvolta vero e proprio scontro dai toni accesi e aspri – tra Stati membri e Istituzioni europee, che ha in ultimo portato ad una confusa disomogeneità di approcci nazionali, espressione di un diverso equilibrio individuato tra diritti fondamentali ed esigenze di garanzia della sicurezza.

Lo strumento della *data retention* ha quindi imposto una ampia e approfondita discussione che non può che avere al suo centro quesiti complessi che mirano a comprendere se e come sia possibile conciliare, nello specifico contesto dell'Unione europea e dei suoi Stati membri, la decisa tutela di diritti fondamentali quali la riservatezza e la protezione dei dati con l'impiego di un vasto sistema di conservazione dei metadati derivanti da telecomunicazioni. Diviene dunque essenziale chiedersi se una forma di c.d. *bulk data retention*, cioè di conservazione generalizzata ed indiscriminata di metadati, rappresenti un inevitabile ed insanabile sacrificio della garanzia della vita privata e della tutela dei dati, sbilanciando definitivamente il rapporto tra diritti fondamentali ed esigenze securitarie a favore di queste ultime. Simili interrogativi affondano le proprie radici nella consapevolezza che l'impiego di strumenti invasivi, quali l'obbligo di *data retention*, si possono inverare nel concreto pericolo di «undermining or even destroying democracy on the ground of defending it» [24], risultando in una compressione dei diritti che, pur motivata da legittimi scopi di salvaguardia della sicurezza, rischia di inficiare il godimento di altri fondamentali diritti strettamente interrelati alla protezione della sfera privata, quali le libertà personali e il diritto di autodeterminazione della propria personalità e identità, volano per il riconoscimento della dignità umana. Partendo da questi presupposti è dunque necessario stabilire come sia possibile scongiurare il realizzarsi di un simile rischio e, conseguentemente, se e in quale misura possano essere adottate normative,

[23] Si fa riferimento alle sentenze Corte di giustizia dell'UE 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*; alla pronuncia 26 luglio 2017, *Parere 1/15*; alla decisione 16 luglio 2020, C-311/18, *Data Protection commissioner c. Facebook Ireland Ltd e Miximillian Schrems*.

[24] Corte europea dei diritti dell'uomo 6 settembre 1978, *Klass et al. v. Germany*, Application n. 5029/71, para. 49.

tanto sovranazionali quanto nazionali, in grado di assicurare il rispetto dei diritti fondamentali senza compromettere irrimediabilmente l'efficacia ed utilità dello strumento della *data retention* stessa.

Dinnanzi ai delicati e profondi interrogativi così delineati e nel tentativo di fornirne una chiara analisi capace di guardare anche ai potenziali sviluppi futuri, il presente lavoro intende riflettere sulla disciplina della *data retention* nel contesto dell'Unione europea e dei suoi Stati membri [25] e sulla individuazione di una possibile sintesi tra le divergenti letture emerse da un dibattito che, a distanza di più di quindici anni dal primo intervento della CGUE sul tema, non ha ancora trovato un punto di approdo condiviso e capace di superare la preoccupante disomogeneità di soluzioni normative adottate a livello nazionale.

Proprio alla luce di tali considerazioni, le discipline normative e le decisioni giurisprudenziali che si sono andate a formare nei singoli Stati, a volte prima ancora di quelle adottate a livello sovranazionale, costituiscono il punto di partenza – non solo metodologico – dal quale muovere l'analisi comparata, che rappresenta uno dei profili maggiormente innovativi di questa opera. Mentre grande rilievo è stato sino ad oggi indubbiamente attribuito alla analisi delle storiche pronunce dei giudici di Lussemburgo in materia di *data retention*, minore attenzione è stata invece dedicata a quanto ha preceduto e seguito le decisioni della CGUE nel contesto dei singoli Stati membri: ci si riferisce cioè alla disamina, da un lato, delle vicende giurisprudenziali che nella dimensione nazionale han-

[25] Benché lo strumento della *data retention*, qui brevemente descritto, possa avere ad oggetto diverse tipologie di dati, merita precisare preliminarmente come in questo lavoro verrà dedicato ampio e prioritario spazio a sistemi di conservazione dei metadati derivanti da servizi di telecomunicazione – telefonica e telematica –, imponenti obblighi di *retention* in capo a fornitori privati per finalità di salvaguardia della sicurezza. Al di là della disamina di taluni casi che si occuperanno della disciplina del trasferimento dati verso Stati terzi e che avranno ad oggetto la conservazione di dati relativi al contenuto delle comunicazioni o, ancora, i PNR, ovvero i codici di prenotazione dei passeggeri aviotrasportati, non troveranno pertanto posto nel presente studio né le forme di conservazione di dati prodotti da oggetti quali automobili senza guidatore o c.d. *wearable devices*, né la disciplina della conservazione di dati per scopi differenti da quello securitario, quali i sistemi di *data retention* riguardanti i dipendenti nell'ambito di un rapporto di lavoro o ancora i dati memorizzati da aziende e imprese per scopi commerciali.

no condotto alla promozione del rinvio pregiudiziale e delle motivazioni di una simile scelta da parte dei giudici nazionali, e dall'altro lato delle reazioni provocate entro i confini nazionali dalle sentenze della c.d. *data retention saga*, sotto il profilo politico e legislativo. In altre parole, sono sovente rimasti senza risposta i quesiti vertenti sulle modifiche normative introdotte negli ordinamenti nazionali e sull'inserimento in esse dei principi e requisiti stabiliti dalla giurisprudenza della CGUE; o ancora non hanno trovato debito approfondimento le ragioni che hanno spinto la società civile, cittadini e organizzazioni non governative a promuovere controversie dinnanzi ai giudici nazionali e come questi ultimi abbiano determinato la compatibilità o meno delle disposizioni interne in materia di conservazione e accesso ai metadati rispetto al diritto dell'UE e ai diritti sanciti nella Carte costituzionali stesse.

È allora riconoscendo l'importanza di analizzare tali interrogativi e provare a fornirne una risposta che si comprende il valore della comparazione. Se comparare significa infatti «fare i confronti, con tutte le premesse, le conseguenze, le implicazioni, i problemi e le scelte valutative che ciò comporta» [26], attraverso l'analisi delle vicende nazionali e delle diverse so-

---

[26] L. PEGORARO, A. RINELLA, *Sistemi costituzionali comparati*, Giappichelli, Torino, 2017, p. 34. O ancora «confronto tra soluzioni normative adottate da diversi ordinamenti in risposta ai problemi pratici più o meno analoghi creati dagli sviluppi sociali, economici, politici, nel seno delle rispettive collettività; al fine di rilevare in quelle soluzioni l'eventuale esistenza di reciproche affinità ovvero di divergenze», G. BOGNETTI, *L'oggetto e il metodo*, in P. CARROZZA, A. DI GIOVINE, G.F. FERRARI (a cura di), *Diritto costituzionale comparato*, Laterza, Roma-Bari, V Ed., 2014, p. 727. *Ex multis*, si rimanda a A. GAMBARO, P.G. MONATERI, R. SACCO, *Comparazione giuridica*, in *Digesto italiano*, Utet, Milano, 1989; G. BOGNETTI, *Introduzione al diritto costituzionale comparato (Il metodo)*, Giappichelli, Torino, 1994; S. GAMBINO, *Diritto costituzionale italiano e comparato. Lezioni*, Periferia, Assago, 2002; G. DE VERGOTTINI, *Diritto costituzionale comparato*, Cedam, Padova, 2004; P. RIDOLA, *Diritto comparato e diritto costituzionale europeo*, Giappichelli, Torino, 2010; G. MORBIDELLI, L. PEGORARO, A. REPOSO, M. VOLPI, *Diritto pubblico comparato*, Giappichelli, Torino, 2014; R. HIRSCHL, *Comparative matters: the renaissance of comparative constitutional law*, Oxford University Press, Oxford, 2014; G. PASCUZZI, *Conoscere comparando: tra tassonomie ed errori cognitivi*, in *Diritto pubblico comparato ed europeo*, 4, 2017, p. 1779 ss.; G. RESTA, A. SOMMA, V. ZENO-ZENCOVICH (a cura di), *Comparare. Una riflessione tra le discipline*, Mimesis, Sesto San Giovanni, 2020; T.E. FROSINI, *Il metodo del e nel diritto pubblico comparato*, in

luzioni adottate in differenti Stati – pur tenendo sempre in considerazione le peculiarità proprie dei singoli ordinamenti – è possibile accrescere il livello di conoscenza della materia oggetto del presente lavoro [27], rendendo possibile in ultimo luogo anche un raffronto tra modelli e approcci [28]. In tal modo si consente l'individuazione delle pratiche migliori, più efficaci e virtuose, delle scelte normative nazionali che determinano un punto di equilibrio più solido tra diritti fondamentali ed efficienza dello strumento della *data retention*, nonché delle decisioni giurisprudenziali maggiormente attente al difficile intreccio con quanto stabilito a livello sovranazionale e al suo impatto sulla disciplina interna. Simili esercizi di comparazione possono dunque ispirare e coadiuvare non solo i giudici chiamati a districare delicate questioni di bilanciamento, spesso rese ancor più intricate dal dialogo con la CGUE, ma anche il legislatore, tanto nazionale quanto europeo, impegnato nella determinazione di soluzioni normative condivise, ragionate e consapevoli.

Da tali valutazioni è scaturita la scelta di sviluppare uno studio comparato riguardante tre Stati membri, Belgio, Italia e Regno Unito; con riferimento a quest'ultimo, è importante premettere come l'analisi svolta nel testo abbia riguardato tanto l'evoluzione normativa e giurisprudenziale in materia di *data retention* attinente al periodo precedente al recesso dall'UE, quanto i successivi ed inediti sviluppi caratterizzanti il contesto *post-Brexit* [29].

L. LLOREDO ALIX, A. SOMMA (a cura di), *Scritti in onore di Mario G. Losano. Dalla filosofia del diritto alla comparazione giuridica*, Accademia University Press, Torino, 2021, p. 99 ss.; R. SCARCIGLIA, *Metodi e comparazione giuridica*, Cedam, Padova, 2021.

[27] «Compito della comparazione giuridica, senza il quale essa non sarebbe scienza, è l'acquisizione di una migliore conoscenza del diritto», A. GAMBARO, P.G. MONATERI, R. SACCO, *Comparazione giuridica*, in *Digesto italiano*, cit., p. 52.

[28] Del resto, lo studio delle realtà ordinamentali rappresenta «"materia prima" della comparazione e rappresenta i mattoni dai quali l'edificio del diritto comparato risulta costruito. La comparazione poi, se si vuole proseguire con il paragone, è il cemento», per citare una celebre quanto efficace metafora di Lombardi (G. LOMBARDI, *Premesse al corso di diritto pubblico comparato. Problemi di metodo*, Giuffrè, Milano, 1986, p. 26).

[29] Sulla sterminata bibliografia in materia, si rimanda, *ex multis*, a F. SAVASTANO, *Uscire dall'UE. Brexit e il diritto di recedere dai Trattati*, Giappichelli, Torino, 2019; M. ELLIOTT, J. WILLIAMS, A.L. YOUNG (a cura di), *The UK Constitution after Miller. Brexit*

Con sguardo più generale, i motivi per i quali la scelta è ricaduta sugli ordinamenti di questi tre Paesi vanno rinvenuti nel fatto che essi risultano paradigmaticamente rappresentativi di approcci differenti e, sotto taluni profili, persino divergenti, con riguardo tanto alle scelte e alle soluzioni normative adottate in materia di *data rentention* e accesso ai metadati, quanto alle decisioni giurisprudenziali pronunciate dalle rispettive Corti nazionali. La comparazione è proseguita non solo per differenze ma anche volgendo attenzione ai punti di contatto ravvisabili tra i diversi approcci seguiti, seppur nelle diversità ordinamentali di cui si è dato debitamente atto nel testo.

Sia allora qui permesso riassumere alcune "circostanze giuridiche" che evidenziano con chiarezza l'importanza – e in certo qual modo la necessità – di porre a confronto questi diversi Paesi.

Il Regno Unito è stato sin dai primi anni Duemila un protagonista importante del dibattito circa la regolamentazione dello strumento della conservazione generalizzata, avendo predisposto normative che si sono susseguite a rapido ritmo e che non sempre hanno considerato – e talvolta neppure atteso – le valutazioni ed i requisiti fissati dalla CGUE, nonché avendo promosso due rinvii pregiudiziali di enorme rilievo con i quali le Corti nazionali inglesi hanno avviato un dialogo, dai toni talvolta aspri, con i giudici di Lussemburgo. Nonostante l'orientamento brevemente tratteggiato metta in luce la difficoltà espressa dal Regno Unito di integrare nella propria disciplina nazionale i criteri definiti a livello sovranazionale dalla giurisprudenza della CGUE, va nondimeno sottolineata, soprattutto in tempi più recenti, la forte sensibilità dimostrata al tema della *data retention* e alla promozione di un dibattito serio ed approfondito sulla garanzia dei diritti fondamentali anche dinnanzi all'impiego di strumenti di sorveglianza; una discussione, questa, che è divenuta poi ancor più complessa con l'avvio dell'inedita procedura di recesso dall'UE dai significativi e dirompenti risvolti riguardanti anche la protezione dei dati e la tutela della riservatezza.

Il Belgio, diversamente dal Regno Unito, ha visto invece un interven-

---

and beyond, Hart, Londra, 2020; F. FABBRINI, *Brexit. Tra diritto e politica*, Il Mulino, Bologna, 2021, nonché a quanto più specificamente richiamato nel Capitolo 3 del presente lavoro.

to della Corte costituzionale più netto ed inizialmente quasi "ossequioso" rispetto alle decisioni della CGUE, mentre sul piano normativo il legislatore nazionale ha incontrato, sin dalla prima legge in materia di conservazione dei metadati, significative difficoltà e frizioni, anche e soprattutto con l'Autorità nazionale garante della protezione dei dati. Lo studio attento, ma anche critico, della vasta giurisprudenza europea emerge con chiarezza non solo dalle più recenti decisioni dei giudici costituzionali belgi, che per ben due volte hanno dichiarato l'incompatibilità della disciplina nazionale rispetto al diritto dell'UE, ma anche dai lavori preparatori che hanno in passato accompagnato e che stanno ancora oggi accompagnando il difficile percorso di adozione di una nuova normativa in materia di *data retention* che sappia integrare al meglio i criteri delineati dai giudici di Lussemburgo.

Una discussione profonda e ragionata sulle forti ripercussioni delle pronunce della CGUE che non si ravvisa invece – se non solo in tempi recentissimi – né nella giurisprudenza né tanto meno nel dibattito parlamentare italiano; così, le normative, approvate spesso con strumenti confusi ed inappropriati per una disciplina così delicata ed articolata, hanno finito con l'attribuire all'Italia il non invidiabile primato di un obbligo di conservazione dei metadati tra i più ampi e lunghi dell'UE – ben settantadue mesi, a fronte di Stati come Regno Unito e Belgio che prevedono termini di tempo dai dodici ai sei mesi –. Nel nostro Paese, inoltre, le Corti hanno provveduto solo nel 2021 a promuovere per la prima volta un rinvio pregiudiziale alla CGUE, dopo aver per anni negato quel dialogo che, seppur con differenti toni, molti altri Stati membri avevano da tempo proficuamente instaurato e che ha rappresentato la vera spinta alla determinazione di un corretto punto di equilibrio tra ingerenza nella sfera privata per scopi securitari e garanzia dei diritti fondamentali [30].

[30] «La comparazione è utile, anzi è spesso indispensabile, anche per studiare il diritto interno, a patto di essere consapevoli di qual è il suo uso corretto, e soprattutto la sua finalità in questo caso: una finalità che non è quella propria della nostra scienza (costruzione di modelli e classi, studio della circolazione degli istituti, esposizione critica delle analogie e delle differenze) (…), bensì quella di guardare "fuori" per capire meglio il *proprio* diritto», L. PEGORARO, *Il diritto pubblico comparato tra scienza e metodo*, in G. MORBIDELLI, L. PEGORARO, A. REPOSO, M. VOLPI, *Diritto pubblico comparato*, cit., p. 1. Sul punto si legga anche M. SMITS, *Comparative law and its influence on national legal*

Da tali valutazioni, trattate e ampiamente argomentate nelle pagine del testo, emerge pertanto come Regno Unito, Belgio e Italia raffigurino esempi estremamente emblematici dei diversi possibili orientamenti adottati dagli Stati membri, utili ad individuare convergenze e divergenze di soluzioni ed approcci determinati tra Stati stessi nonché tra contesto nazionale e quanto stabilito nell'ambito sovranazionale. Anche sviluppando una analisi comparata, dunque, il libro si propone di vagliare la *data retention* e le sfide che essa comporta sviluppando due fondamentali quanto complementari percorsi: quello discendente, che mira cioè ad analizzare la disciplina e la giurisprudenza dell'UE e le sue ripercussioni sugli Stati membri, e quello ascendente che, studiando le peculiari e spesso eterogenee dimensioni nazionali, induce a riflettere sulle differenze e sui punti di contatto riscontrabili tra gli stessi ordinamenti considerati nonché tra questi e i principi promossi a livello europeo e su come questi ultimi debbano essere posti in discussione o modificati.

La struttura del presente lavoro rispecchia le considerazioni sin qui svolte e le scelte illustrate.

Il Capitolo 1 mira a fornire le coordinate di riferimento, necessarie a guidare il lettore nel successivo cammino di analisi: prendendo avvio da una chiara descrizione dei sistemi di *data retention* e accesso ai metadati per scopi securitari, delle potenzialità nonché dei connessi rischi per i diritti fondamentali, la disamina si concentra poi sui due diritti che maggiormente e più direttamente risultano compromessi dall'impiego di simili strumenti: i diritti alla riservatezza e alla protezione dei dati. Questi ultimi vengono dunque descritti nel loro contenuto e nel loro interessante percorso evolutivo, fortemente segnato dall'inarrestabile progresso scientifico, nonché nella loro intima connessione con il godimento di altri diritti fondamentali quali libertà personali e dignità dell'uomo.

Queste essenziali valutazioni, propedeutiche ad una maggiore com-

---

systems, in M. REIMANN, M. ZIMMERMANN (a cura di), *The Oxford handbook of comparative law*, Oxford University Press, Oxford, 2006, p. 513 ss. Partendo da tale premessa, nello specifico caso italiano la comparazione proposta vuole dunque rappresentare anche uno spunto di riflessione per instaurare un più ampio e consapevole dibattito parlamentare in materia di *data retention*. Come si vedrà, infatti, tale tematica e la sua delicatezza e complessità sono risultate pressoché inosservate sia dal legislatore sia dai giudici italiani.

prensione del vasto dibattito in materia di *data retention*, consentono di muovere, nei Capitoli 2 e 3, allo studio della dimensione dell'Unione europea: seguendo un criterio cronologico, trova infatti posto una approfondita ricostruzione tanto delle principali disposizioni normative di riferimento quanto delle rilevanti pronunce della CGUE e del complesso ed intricato confronto che soprattutto l'approccio e i requisiti fissati dai giudici di Lussemburgo hanno determinato non solo tra le Istituzioni dell'UE ma anche negli Stati membri. Particolare rilievo è riservato al ruolo del legislatore europeo e alle prospettive future di azione sul fronte normativo sovranazionale, vagliando le proposte, ancora in *fieri*, di modifica dell'assetto esistente e il dibattito in seno al Comitato dei rappresentanti permanenti degli Stati membri. La proiezione verso la dimensione esterna all'UE delle criticità e dei complessi interrogativi legati alla c.d. *data retention saga* e il confronto delle Istituzioni europee stesse con ordinamenti di Stati extra-UE trova poi specifico spazio nel Capitolo 3: la disamina delle decisioni della CGUE nei casi *Schrems* e nel *Parere 1/15* relativi al trasferimento di dati verso Stati terzi consente di trarre considerazioni importanti su quanto i sistemi di raccolta e accesso a dati e metadati posti in essere per scopi securitari da ordinamenti quali quello statunitense e canadese possano incidere sulla legittimità del flusso di dati provenienti dall'UE e quanto dunque l'elevato standard di tutela fissato entro i confini europei possa realizzarsi – e, in un certo senso, imporsi – nella promozione di un più alto livello di garanzia della riservatezza e della protezione dei dati in Stati terzi.

Se anche nella dimensione esterna vengono messe in luce le oggettive difficoltà applicative e i limiti concreti dei rigidi requisiti fissati dalla giurisprudenza dei giudici di Lussemburgo, i successivi Capitoli 4, 5 e 6 delineano simili criticità e la complessità della sfida della regolamentazione della *data retention* nello specifico contesto dei tre Stati membri individuati. L'analisi degli ordinamenti nazionali risulta avere una struttura simile e condivisa: lo studio della normativa e dei diversi interventi di riforma legislativa susseguitisi nel tempo, scanditi anche dall'evolversi della disciplina e della giurisprudenza europea, viene accompagnato dalla dettagliata disamina delle più significative sentenze delle Corti nazionali relative alla compatibilità con il diritto dell'UE e con i diritti riconosciuti nelle Carte costituzionali delle disposizioni interne in materia di conser-

vazione e accesso ai metadati. In questo modo vengono evidenziate le peculiarità proprie dell'approccio seguito da ciascuno Stato, il dialogo instaurato con l'UE – tanto con la CGUE quanto in seno alle Istituzioni stesse – nonché i dibattiti ancora aperti e in fase di sviluppo.

Le Conclusioni, tirando le fila degli studi e delle considerazioni proposte nei previ Capitoli, intendono infine ragionare sul futuro della disciplina della *data retention* nel contesto europeo. Gli interrogativi in attesa di risposta da parte della CGUE e l'auspicato intervento del legislatore europeo vengono letti congiuntamente agli esiti della analisi comparata degli Stati oggetto di disamina: le convergenze, le differenze e le eterogenee soluzioni promosse a livello nazionale divengono un cruciale tassello che consente di promuovere una finale riflessione sul difficile punto di equilibrio tra impiego di strumenti di conservazione e accesso a dati e metadati e garanzia dei diritti fondamentali. Ciò pur nella consapevolezza che tale determinazione rappresenta una sfida in divenire, destinata ad impegnare ancora a lungo Corti e legislatori, europei e nazionali.

CAPITOLO 1

SISTEMI DI CONSERVAZIONE DEI METADATI PER SCOPI SECURITARI E DIRITTI FONDAMENTALI ALLA RISERVATEZZA E ALLA PROTEZIONE DEI DATI

SOMMARIO: 1. I sistemi di conservazione e accesso ai metadati come strumenti di lotta alla criminalità e al terrorismo: potenzialità e rischi. – 2. I diritti fondamentali alla riservatezza e alla protezione dei dati: cenni ricostruttivi. – 2.1. Il diritto alla riservatezza: dalle origini negli USA al riconoscimento nel continente europeo. – 2.2. Dalla dimensione negativa a quella positiva: il progressivo affermarsi del diritto alla protezione dei dati. – 3. La *data retention* tra esigenze securitarie e tutela dei diritti fondamentali: una rinnovata sfida.

1. *I sistemi di conservazione e accesso ai metadati come strumenti di lotta alla criminalità e al terrorismo: potenzialità e rischi.*

Successivamente ai drammatici attentati terroristici che hanno colpito gli Stati Uniti d'America nel 2001, seguiti dai molteplici tragici attacchi che hanno scosso il continente europeo, la garanzia della sicurezza da minacce tanto esterne quanto interne è divenuta obiettivo prioritario dei Governi nazionali. L'acceso dibattito che ne è seguito, anche nei consessi sovranazionale ed internazionale, si è essenzialmente focalizzato sulla determinazione di strategie e mezzi efficaci per raggiungere un alto livello di prevenzione e lotta al terrorismo e alla criminalità transfrontaliera. In questo contesto – quantomeno inizialmente – emergenziale, la scelta operata dalla quasi totalità degli Stati occidentali, a partire dagli USA, è stata

quella di potenziare sistemi di sorveglianza [1] – segreta e non – che hanno trovato realizzazione mediante l'implementazione di mezzi di intercettazione, controllo e accesso alla enorme mole di dati digitali (*Big Data*) [2] prodotti dal vasto e sempre più quotidiano impiego del Web, di dispositivi di telecomunicazione nonché dalla pervasiva digitalizzazione di informazioni e dati raccolti da operatori privati e pubblici nello svolgimento dei propri servizi [3].

Tra questi strumenti, in particolare, sono risultati ampiamente utilizzati sistemi di c.d. *data retention* di dati derivanti da servizi di telecomunicazione. Con tale termine, difficilmente traducibile in italiano se non con la riduttiva locuzione "conservazione dei dati", si intende indicare l'imposizione, indirizzata a fornitori privati di servizi di comunicazione

---

[1] Come ben rilevato da Ziccardi risulta chiaro come «l'attività di controllo non sia più un'esclusiva di regimi che, un tempo, comparati al nostro sistema legale e alla nostra idea di tutela dei diritti, erano definiti autoritari o fautori di politiche liberticide, ma che possa avvenire in qualsiasi contesto politico e costituzionale e, anzi, per tale motivo sia ancora più subdola e complessa da interpretare. (…) La tendenza diffusa è quella di uno Stato che sorveglia le comunicazioni elettroniche con tutti i mezzi possibili», G. ZICCARDI, *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina, Milano, 2015, p. 225.

[2] Al di là della classica definizione di *Big Data* intesi come quella enorme mole di dati caratterizzati dalle c.d. "tre V", ovvero volume, velocità e varietà (secondo quanto scritto da D. Laney e ripreso poi da F.X. DIEBOLD, *On the origin(s) and development of Big Data phenomenon, the term and the discipline*, PIER Working Paper, 13, 2012, p. 1 ss.), secondo una più moderna spiegazione dei *Big Data* tale termine «designa delle cose che si possono fare solo su larga scala» (V. MAYER-SCHONBERGER, K. CUKIER, *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano, 2013, p. 16), riferendosi dunque non solo ai dati ma anche e specificamente alle operazioni che mediante tali dati possono essere svolte (*Big Data analysis*), anche grazie a moderne tecniche di trattamento automatizzato di dati, analisi algoritmiche e di Intelligenza Artificiale, di cui si parlerà a breve.

[3] Sebbene in questo studio grande attenzione verrà primariamente attribuita ai sistemi di sorveglianza e controllo dei dati derivanti da servizi di telecomunicazione, è bene premettere come in realtà gli strumenti di *surveillance* possano avere ad oggetto le informazioni più disparate: come si avrà modo di vedere, molti Stati hanno adottato mezzi di acquisizione e analisi dei codici di prenotazione dei passeggeri aviotrasportati (i c.d. PNR); altri ancora riguardano la disponibilità e il controllo di informazioni relative alle transazioni finanziarie.

elettronica accessibili al pubblico o di reti pubbliche di comunicazione, di conservare per un determinato periodo di tempo i dati di traffico, ubicazione o identificativi dei propri utenti [4]; a tale obbligo di *retention* si accostano poi misure volte a consentire l'accesso ai dati conservati da parte di autorità pubbliche specificamente individuate, che potranno quindi trattare tali informazioni per finalità di prevenzione, indagine e contrasto alla criminalità e alle minacce alla sicurezza nazionale [5], anche attraverso

[4] Drewry definisce la *data retention* come «measures that aim at requiring (some or all) operators to retain non-content data generated or processed as a result of activities of all users of operators'communications or network services so that they can be accessed by state authorities and used for public order purposes when necessary and lawful», L. DREWRY, *Crimes without culprits: why the EU needs data retention and how it can be balanced with the right to privacy*, in *Wisconsin International Law Journal*, 4, 2015, p. 728.

[5] Pur non volendo entrare nel dettaglio del complesso dibattito definitorio avente ad oggetto il termine "sicurezza nazionale", da ritenersi distinta rispetto a quella pubblica, è nondimeno utile sottolineare come nel diritto dell'UE non siano presenti chiare definizioni di tale espressione. Ciò pare piuttosto singolare soprattutto alla luce del delicato art. 4, co. 2, Trattato sull'Unione europea (TUE), nel quale viene espressamente stabilito che la materia della garanzia della sicurezza nazionale resta di esclusiva competenza degli Stati membri: pur rappresentando una disposizione di fondamentale rilievo, capace di incidere sulla determinazione dell'ambito di applicazione del diritto dell'UE, essa non risulta accompagnata da alcuna definizione su quanto debba ricondursi alle attività volte alla tutela della sicurezza nazionale. Come si avrà modo di vedere nei prossimi Capitoli, proprio la difficoltà di circoscrivere esattamente questo ambito di intervento dello Stato – soprattutto dinnanzi alle moderne e sofisticate tecniche di indagine e repressione di reati e minacce alla sicurezza che spesso sono difficilmente riconducibili in maniera chiara e decisa alle attività di agenzie di intelligence per scopi di sicurezza nazionale o a quelle di autorità di *law enforcement* per finalità di sicurezza pubblica – assumerà grande importanza nel dibattito legislativo e giurisprudenziale in materia di *data retention*. Anche la Corte di giustizia dell'UE (d'ora in avanti CGUE) cercherà, soprattutto nelle più recenti pronunce, di proporre una definizione di sicurezza nazionale ed una distinzione rispetto agli scopi di lotta alla criminalità grave, al fine di chiarire i dubbi quanto all'ambito di applicazione del diritto dell'UE in una così complessa e fondamentale materia. Sulle possibili distinzioni tra il concetto di sicurezza nazionale e pubblica, si rimanda comunque, *ex multis*, a P. VOGIATZOGLOU, S. FANTIN, *National and public security within and beyond the Police Directive*, in A. VEDDER, J. SCHROERS, C. DUCUING, P. VALCKE (a cura di), *Security and Law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Intersentia, Bruxelles, 2019, p. 27 ss.; ma an-

lo svolgimento di analisi aggregate o automatizzate, o ancora tramite l'impiego di sofisticati sistemi di Intelligenza Artificiale e algoritmi [6].

La preliminare operazione di conservazione permette così alle autorità di intelligence e di *law enforcement* di disporre di una moltitudine di dati, che non necessariamente riguardano però il contenuto delle comunicazioni: lo strumento della *data retention* sopra descritto, infatti, nella maggioranza dei casi impone l'obbligo di trattenere e memorizzare unicamente i c.d. metadati. Questi ultimi, normalmente prodotti dal comune impiego delle telecomunicazioni – dunque dall'utilizzo di dispositivi elettronici quali telefoni e computer –, sono necessariamente raccolti dagli operatori per la corretta erogazione dei servizi e per scopi di fatturazione, venendo poi abitualmente cancellati quando non più utili per tali finalità

---

che a G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della 'emergenza normalizzata'*, in *Federalismi.it*, 4, 2019, p. 66 ss.

[6] In estrema sintesi, per Intelligenza Artificiale si intende «una famiglia di tecnologie in rapida evoluzione in grado di apportare una vasta gamma di benefici economici e sociali in tutto lo spettro delle attività industriali e sociali. L'uso dell'intelligenza artificiale, garantendo un miglioramento delle previsioni, l'ottimizzazione delle operazioni e dell'assegnazione delle risorse e la personalizzazione dell'erogazione di servizi, può contribuire al conseguimento di risultati vantaggiosi dal punto di vista sociale e ambientale nonché fornire vantaggi competitivi fondamentali alle imprese e all'economia europea», come si legge nella recente Proposta di Regolamento che stabilisce regole armonizzate sull'Intelligenza Artificiale e modifica alcuni atti legislativi dell'UE, COM/2021/206final, presentata dalla Commissione il 21 aprile 2021. Quanto agli algoritmi, invece, essi «da un punto di vista tecnico, (…) sono semplici metodi matematici che esprimono risultati entro una quantità limitata di spazio e tempo e in un linguaggio formale definito, trasformando gli input, costituiti da dati, in output sulla base di un processo di calcolo specificato; da un punto di vista sociale, tali tecnologie costituiscono processi decisionali automatizzati il cui percorso decisionale è stato programmato da uno sviluppatore. (…) In altre parole, gli algoritmi esprimono risultati che, seppur determinati dal loro codice, costituiscono determinazioni soggettive fornite da parte di sistemi automatizzati», G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy digitale*, Giuffrè, Milano, 2019, p. 450. Sul punto si leggano anche, *ex multis*, J. KAPLAN, *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, Roma, 2017; F. PIZZETTI (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018; A. D'ALOIA (a cura di), *Intelligenza artificiale (Contributi del Convegno su 'Intelligenza artificiale e diritto. Come regolare un mondo nuovo', Parma, 12 ottobre 2018),* in *BioLaw Journal*, 1, 2019.

operative. Per metadati – o dati relativi al traffico – si fa riferimento pertanto all'«involucro delle comunicazioni elettroniche» [7], cioè a tutte quelle informazioni riguardanti luogo, data, ora, durata e destinatario di una comunicazione, unitamente all'ubicazione e all'identità dell'utilizzatore di un servizio di telecomunicazione. Per questo è importante distinguere preliminarmente lo strumento della conservazione dei metadati dalle intercettazioni: queste attengono al contenuto delle comunicazioni, si svolgono in "tempo reale" e vengono poste in essere direttamente dalle autorità di intelligence o *law enforcement*; mediante la *data retention*, invece, i dati vengono conservati e trattenuti dall'operatore, ovvero dal soggetto privato e non dall'autorità pubblica, per essere poi solo eventualmente e in un secondo momento analizzati mediante accesso su richiesta avanzata dalle autorità pubbliche autorizzate [8].

Questo sistema di previa conservazione dei metadati, così descritto, è stato sin da subito percepito come una carta vincente e uno strumento di significativa efficacia nel campo delle attività investigative: esso infatti permette di effettuare controlli sui dati relativi ad individui che al momento dell'atto terroristico o della commissione di un determinato reato non risultavano essere ancora noti alle forze dell'ordine o alle agenzie di intelligence e che quindi non erano sottoposti ad alcuna forma di sorveglianza o intercettazione specifica; in questo modo, per impiegare il termine utilizzato da Cameron, la *data retention* consente di andare «indietro nel tempo» [9] durante la fase investigativa, permettendo di accedere ad

---

[7] G. CAGGIANO, *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *Medialaws*, 2, 2018, p. 65.

[8] Similmente, «l'acquisizione, necessariamente *post factum*, dei dati esterni del traffico presso il fornitore dei servizi telefonici o telematici interessati vale a marcare la distanza della *data retention* rispetto a fenomeni solo apparentemente analoghi, come il c.d. pedinamento satellitare, in cui gli organi dell'investigazione inseriscono un GPS su oggetti che la persona reca con sé e ne registrano i movimenti nel momento in cui essi avvengono o comunque quando interessi geolocalizzare la persona stessa», S. MARCOLINI, *L'istituto della DR dopo la sentenza della CGUE del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA (a cura di), *Cybercrime*, Utet, Torino, 2019, p. 1580.

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

informazioni che, qualora non preventivamente conservate, sarebbero altrimenti difficilmente reperibili. La conservazione di metadati insomma si traduce, per impiegare una nota ed efficace immagine, nella creazione di un enorme "pagliaio" di informazioni entro cui, con le moderne tecniche di indagine e di analisi automatizzata dei dati, si può essere in grado di trovare il singolo "ago" [10] di cui le autorità pubbliche necessitano al fine di svolgere efficaci attività di prevenzione e contrasto delle minacce alla sicurezza.

Le grandi potenzialità che la *data retention* rappresenta e che l'hanno portata ad essere impiegata non solo nella lotta al terrorismo ma anche nella repressione della criminalità, non hanno però impedito di osservare i profondi rischi caratterizzanti l'utilizzo di questo controverso strumento: oltre ai seri pericoli di *purpose* o *function creep* [11], nonché di *data breaches* [12], la conservazione – indipendentemente e prima ancora della

---

Murray e Fussey, «these methods of interrogating retained communications data benefit from the ability to look into the past. First, in the event of a crime, retained data allows security services to 'rewind'events, facilitating the identification of suspects and a better understanding of what happened. (…) Second, retained data allows analysts to look back and immediately identify a suspect's pre-existing network», D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, in *Israel Law Review*, 1, 2019, p. 40.

[10] Si pensi, a titolo esemplificativo, alla possibilità di analizzare l'aggancio ad una determinata cella telefonica da parte di dispositivi di telecomunicazione, nonché di risalire ai dati identificativi dei soggetti che abbiano attivato utenze telefoniche su uno specifico dispositivo, o ancora di ottenere informazioni sulla frequenza di contatti e telefonate che leghino vittime di un reato a soggetti sconosciuti alle forze dell'ordine. Queste operazioni non risulterebbero possibili se i metadati non fossero innanzitutto conservati da parte dei fornitori dei servizi.

[11] Ci si riferisce cioè alle pratiche di utilizzo di dati per finalità differenti da quelle per le quali erano stati raccolti e conservati: i dati che i servizi di telecomunicazioni sono obbligati a conservare per finalità securitarie, e dunque per consentire l'accesso alle autorità pubbliche di *intelligence* o *law enforcement*, potrebbero ad esempio essere impiegati dai soggetti privati stessi per finalità commerciali, di marketing o di profilazione del cliente.

[12] Per *data breaches* si intendono casi di furto o manomissione di dati, che costituiscono pericoli tipici ed ineludibili di sicurezza dei dati (*data security*) che divengono tanto più elevati con l'aumentare dei dati raccolti e memorizzati nonché con la crescita della dimensione delle banche dati, che peraltro rappresentano un costo economico e ge-

eventuale analisi ed accesso – di una grande quantità di informazioni, in maniera indiscriminata e generalizzata, senza che sussista cioè alcun sospetto o connessione con la commissione di un reato o una minaccia alla sicurezza (c.d. *bulk* o *blanket data retention*), provoca indubbie e forti ingerenze entro la sfera privata di tutti gli utenti. Sebbene infatti i metadati non attengano al contenuto delle comunicazioni – siano esse telefonate o messaggi di testo – e possano quindi apparire, singolarmente considerati, del tutto innocui e incapaci di rappresentare un mezzo di sorveglianza degli utenti, essi sono in realtà in grado di fornire, una volta aggregati, un'immagine completa ed ampia della vita e delle abitudini degli individui: come sarà più volte chiaramente affermato nella giurisprudenza della Corte di giustizia dell'UE (CGUE), della Corte Europea dei Diritti dell'Uomo (Corte EDU) e di numerose Corti nazionali, i metadati consentono di rivelare, non meno dei dati attinenti al contenuto, una enorme quantità di informazioni circa la vita privata di un soggetto, le sue relazioni famigliari e sociali e persino gli orientamenti politici o sessuali [13]. Potendo creare un dettagliato profilo e una ricostruzione chiara della sfera privata di ciascun consociato, gli strumenti volti a sfruttare le significative potenzialità dei metadati mediante la disposizione di obblighi di conservazione e la successiva possibilità di accesso hanno sollevato seri dubbi e perplessità quanto alla loro compatibilità con il godimento e la tutela di diritti fondamentali, in particolar modo quelli alla riservatezza e alla protezione dei dati.

Prima di muovere ad una più approfondita analisi degli interrogativi e dell'ampio dibattito scaturiti dall'impiego di sistemi di *data retention*, risulta perciò imprescindibile procedere ad una ricostruzione, seppur breve, dei diritti fondamentali sopra indicati: i diritti alla riservatezza e alla protezione dei dati, in quanto direttamente e maggiormente compressi

---

stionale di non trascurabile entità per gli operatori sui quali l'obbligo di conservazione ricade.

[13] «This information can reveal extensive insights, such as a near comprehensive record of an individual's movements, with whom he or she communicates, how frequently and for how long. Communications data is not restricted to conventional communications such as phone calls, emails or messaging, but also includes communications between computers and internet browsing histories», D. MURRAY, P. FUSSEY, *Bulk surveillance in the digital age*, cit., p. 34.

dall'impiego di regimi di conservazione dei metadati, saranno al centro di quelle valutazioni di legislatori e giudici che occuperanno i Capitoli successivi di questo lavoro e necessitano dunque di essere definiti nei loro tratti principali.

2. *I diritti fondamentali alla riservatezza e alla protezione dei dati: cenni ricostruttivi.*

2.1. *Il diritto alla riservatezza: dalle origini negli USA al riconoscimento nel continente europeo.*

Sebbene strettamente correlati tra loro, tanto da essere spesso confusi e sovrapposti, i diritti alla riservatezza e alla protezione dei dati presentano in realtà una origine ed un contenuto molto differenti.

Il diritto alla riservatezza – o diritto alla privacy [14] o alla vita privata – trova le sue radici storiche nella dottrina statunitense: Warren e Brandeis, nel celebre articolo intitolato *The right to privacy* [15], apparso nel 1890 sul-

[14] Nei Paesi anglosassoni tale termine assume in realtà spesso una accezione piuttosto ampia o vaga, intesa a ricomprendere anche il diritto alla protezione dei dati, come evidenziato da V. SALVATORE, *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, Studio Servizio di Ricerca del Parlamento europeo, PE 628.243, 2018, p. 2. In questo lavoro il termine *privacy* viene invece impiegato con riferimento esclusivo al diritto alla riservatezza, mentre quale sinonimo del diritto alla protezione dei dati viene utilizzato la più specifica e distinta espressione inglese di *data protection*. Con riferimento a quest'ultima specifica scelta terminologica, essa risulta motivata dal fatto che, come sottolineato da Gambini, l'espressione più utilizzata nel linguaggio internazionale per indicare il più recente diritto alla protezione dei dati «non è quella di privacy, ma è quella di *data protection*, proprio per sottolineare che non si discorre soltanto del diritto dell'individuo "ad essere lasciato solo", chiuso nel proprio mondo privato, ma anche del suo diritto a potersi proiettare liberamente nel mondo attraverso le proprie informazioni, mantenendo però sempre il controllo sul modo in cui queste circolano e vengono utilizzate dagli altri», M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Juridico*, 1, 2013, p. 150. Anche tale differenza lessicale dunque è finalizzata a sottolineare le peculiarità e specificità che caratterizzano i due diritti che si intende esaminare.

[15] S.D. WARREN, L.D. BRANDEIS, *The right to privacy,* in *Harvard Law Review*, 4, 1890, p. 193 ss.

la prestigiosa rivista *Harvard Law Review*, affermavano per la prima volta la necessità di riconoscere quale specifica situazione giuridica soggettiva il *right to be let alone*. Tale diritto "ad essere lasciati soli", pur nascendo dal bisogno, concretamente percepito dai due autori, di proteggere la propria vita famigliare e il proprio domicilio da invasioni perpetrate ad opera di fotografi di riviste di gossip, non si limitava ad affermare un semplice privilegio della classe borghese posto a tutela della rispettabilità ma, al contrario, esprimeva l'esigenza di salvaguardare la sfera privata da interferenze esterne come mezzo per assicurare il godimento delle libertà personali [16]. Partendo da una attenta analisi di diversi casi giurisprudenziali della *common law* – in materia ad esempio di sequestro di documenti – che tutelavano la segretezza di corrispondenza e documenti facendo riferimento alle garanzie fornite dai *property rights*, Warren e Brandeis giungevano infatti a dichiarare l'esistenza di una fattispecie giuridica autonoma, non esclusivamente legata al diritto di proprietà o di riservatezza delle comunicazioni interpersonali [17], il cui più profondo «contenuto spirituale protetto non è tutelato per il valore che esso ha o può avere nel pubblico, nei rapporti di mercato o nei traffici giuridici, ma, al contrario, riceve protezione dal *common law* unicamente per il valore intimo, privato, che esso ha per il suo titolare» [18].

Questo nuovo diritto [19], emerso in tutta la sua complessità sin dalla prima teorizzazione dei due autori, ha conosciuto un percorso di afferma-

---

[16] O. POLLICINO, M. BASSINI, *Social network e tutela dei dati personali*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, Torino, 2018, p. 66.

[17] M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws*, 2, 2018, p. 93.

[18] A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, Roma, 1974, p. 43.

[19] L'esigenza di tutela della vita privata era emersa già nel 1849 nel Regno Unito: nella decisione *Prince Albert v. Strange*, pronunciata dalla *High Court of Chancery*, era stato impiegato per la prima volta il termine *privacy* nella sua accezione di libertà da interferenze nella propria sfera privata. Come ben sottolineato da Famiglietti, la riservatezza nella concezione inglese risultava tuttavia strettamente legata al concetto di *property*, ed intesa dunque quale privilegio di classe e non come vero e proprio diritto autonomo: «la giurisprudenza inglese non ha individuato una tutela specifica della privacy,

zione graduale nella giurisprudenza delle Corti statunitensi [20]. Queste ultime hanno infatti lentamente ma progressivamente garantito il *right to be let alone* nella sua più ampia ed articolata accezione, ancorandolo a diversi principi e libertà ampiamente riconosciute nel *Bill of Rights*, quali quelle espresse dagli Emendamenti I, III, IV, V, IX e XIV [21]. Lo stratifi-

---

ma singoli rimedi per i casi concreti, i quali però avrebbero mostrato tutta la loro inadeguatezza ogniqualvolta la lesione della vita privata si fosse realizzata senza un'azione materiale o senza la violazione di un vincolo contrattuale o fiduciario», G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto*, in A. D'ALOIA (a cura di), *Bio-tecnologie e valori costituzionali. Il contributo della giustizia costituzionale*, Giappichelli, Torino, 2004, p. 299. Per maggiori approfondimenti, si legga anche F. PETRUCCO, *The right to privacy and new technologies: between evolution and decay*, in *MediaLaws*, 1, 2019, p. 148 ss.

[20] Per una dettagliata e ampia ricostruzione delle difficoltà riscontrate nel processo di affermazione del diritto alla privacy come teorizzato da Warren e Brandeis, nonché della giurisprudenza statunitense in materia, si rimanda *ex multis* a A. BALDASSARRE, *Privacy e Costituzione. L'esperienza statunitense*, cit. e a E. BLOUNSTEIN, *Privacy as an aspect of human dignity*, in *New York University Law Review*, 39, 1964, p. 962 ss.; A. DI MARTINO, *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, Napoli, 2017.

[21] «La capacità espansiva del diritto alla privacy si è rivelata [negli USA] direttamente proporzionale alla capacità delle Corti di leggerne il fondamento – anche costituzionale – nelle maglie di principi anche molto diversi fra loro», O. POLLICINO, M. BASSINI, *Social network e tutela dei dati personali*, cit., p. 68. Importanti pronunce, in questo processo di lenta affermazione del diritto alla riservatezza, vanno riscontrate nelle sentenze della Corte Suprema *Griswold v. Connecticut* (n. 381 US 479, 1965), ma anche *Kats v. United States* (n. 389 U.S. 347, 1967). In quest'ultima in particolare «la Corte offre una lettura evolutiva, e non più solo testuale, del quarto emendamento della Costituzione americana affermando che esso non protegge solo il domicilio, la corrispondenza, la persona fisica, ma anche la privacy dell'individuo contro taluni tipi di intrusione del governo. In secondo luogo, chiarisce, da un lato, che il quarto emendamento non può essere interamente ridotto al diritto alla privacy, e da un altro lato, che il diritto alla privacy trova fondamento anche in altre norme costituzionali. In particolare, la Corte osserva che una protezione della privacy può essere trovata nell'interpretazione del primo emendamento che vieta le limitazioni governative alla libertà di associazione e alla privacy dell'associazione stessa, nel divieto, di cui al terzo emendamento di acquartierare dei soldati in tempo di pace in case private senza il consenso dei proprietari e per alcuni aspetti anche nel quinto emendamento che tutela il diritto di ogni individuo a un enclave dove poter condurre una vita privata», M. OROFINO, *Diritto alla protezione dei dati personali e sicurezza*, cit., p. 92.

carsi della *common law* ha così emancipato il diritto alla riservatezza da quel più rigido e limitato binomio *privacy-property* che legava la riservatezza alle tutele civilistiche della proprietà privata, per coglierne invece la connessione con i fondamentali principi di libertà, autodeterminazione e dignità. Da "difesa della solitudine fisica" o «individual interest in avoiding disclosure of personal matters», il diritto alla privacy veniva dunque riconosciuto quale salvaguardia dell'«individual's independence in making certain kinds of important decisions» (Corte Suprema degli Stati Uniti d'America, *Whalen v. Roe* (n. 429 US 589, 1977, para. 599-600) [22]. La tutela "negativa" alla non intrusione nella sfera privata si arricchiva quindi sempre più di significati e di sfaccettature differenti: da un lato, essa giungeva a proteggere l'individuo non solo nella sua dimensione più intima ma anche nel suo riflesso verso l'esterno, nelle relazioni famigliari e nella più ampia società entro cui il soggetto è inserito, vive ed opera [23]; dall'altro lato, il diritto alla riservatezza veniva sempre più inteso quale «libertà fondamentale da esercitare nei confronti del potere pubblico» [24], come prerogativa, insomma, di una società democratica nella quale la privacy diveniva baluardo avverso forme di intrusione e controllo da parte di soggetti pubblici o privati capaci altrimenti di minacciare il reale esercizio delle libertà civili e politiche così faticosamente riconosciute nelle Carte costituzionali [25]. Proprio sotto questo profilo, anticipando rifles-

---

[22] In questa decisione dunque emerge come «the US Supreme Court derived a right to privacy from the various 'zones of privacy' emanating from several constitutional guarantees and prohibiting government intrusion into the intimate matters of married couples. (…) The US conception sees privacy as a 'right of the individual to decide for himself, found in the penumbras of several provisions of the Bill of Rights», M.J. CEPEDA ESPINOSA, *Privacy*, in M. ROSENFELD, A. SAJO (a cura di), *The Oxford handbook of comparative constitutional law*, Oxford University Press, Oxford, 2013, p. 970.

[23] T.E. FROSINI, *La tutela dei dati e il diritto all'oblio*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, cit., p. 89.

[24] F. MIDIRI, *La giuridificazione della protezione dei dati in Italia*, in *Giustamm*, 5, 2016.

[25] Westin definisce infatti la privacy come «the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others», sottolineando quindi l'aspetto relazionale e la connessione con l'autodeterminazione e la formazione della propria personalità (A. WESTIN,

sioni e problematiche che si concretizzeranno con ancor più forza a partire dall'avvento del mondo dei *bit* e della digitalizzazione, già nel 1954 il giudice della Corte Suprema Douglas, nella sua *Dissenting opinion* al caso *Irvine v. California* (347 US 128), aveva riconosciuto l'importanza della tutela della riservatezza come garanzia e precondizione per l'affermazione del diritto alla autodeterminazione, alla partecipazione libera alla vita politica e sociale, impiegando parole di grande forza e di perpetua attualità: «the right of privacy should include the right to pick and choose from competing entertainments, competing propaganda, competing political philosophies. If people are let alone in those choices, the right to privacy will pay dividends in character and integrity. The strength of our system is in the dignity, the resourcefulness, and the independence of our people. Our confidence is in their ability as individuals to make the wisest choice. That system cannot flourish if regimentation takes hold. The right of privacy, today violated, is a powerful deterrent to anyone who would control men's minds» [26].

Nella ricchezza di sfumature e nel suo esser oggetto di una continua evoluzione nel contesto giurisprudenziale statunitense, non stupisce come il diritto alla riservatezza fosse e continui ad essere un diritto difficile da definire: come affermato da Solove «currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over information about

---

Privacy and freedom, in *Washington and Lee Law Review*, 20, 1968, p. 7); Friedman poi parla di privacy come della tutela delle scelte di vita contro qualsiasi tipo di controllo pubblico, censura o discriminazione sociale (L. FRIEDMAN, *The Republic of choice, law, authority and culture*, Harvard University Press, Cambridge, Massachusetts, 1990).

[26] Non possono che riecheggiare nelle parole citate quanto già nel 1928 il giudice della Corte Suprema Brandeis, lo stesso che nel 1890 aveva teorizzato il *right to privacy* insieme a Warren, scriveva nella sua *Dissenting opinion* al caso *Olmstead v. United States* (n. 277 US 438, 1928): «The protection guaranteed by the Amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. (…) They conferred, as against the Government, the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth».

oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations» [27].

Tale diritto dalle ampie sfaccettature, dopo essersi affermato negli USA, è stato oggetto di riconoscimento anche nel continente europeo a partire dalla seconda metà del Novecento: la Convenzione europea dei diritti dell'uomo del 1950 (CEDU), infatti, diviene la prima e significativa fonte sovranazionale ad attribuire rango di diritto fondamentale alla tutela della vita privata e famigliare, ricomprendente anche domicilio e corrispondenza. A tale diritto previsto dall'art. 8, tuttavia, non è attribuito carattere assoluto ed anzi al comma 2 vengono ammesse alcune possibili restrizioni ed ingerenze, seppur accompagnate da debite limitazioni e garanzie. In tal senso l'intrusione nella sfera privata da parte di autorità pubbliche può essere legittimata solo se prevista dalla legge e se si riveli necessaria, in una società democratica, per raggiungere scopi ben specificati, per quanto ampi, quali la sicurezza nazionale, la sicurezza pubblica, il benessere economico del Paese, la difesa dell'ordine e la prevenzione di reati, la protezione della salute e della morale, la protezione dei diritti e libertà altrui (art. 8, co. 2). Certamente l'ampiezza dei termini utilizzati nel dettato della CEDU nonché i labili confini di quanto possa realmente essere considerato "necessario in una società democratica" hanno comportato non pochi dubbi interpretativi quanto alla portata dell'art. 8, cui la Corte europea dei diritti dell'uomo (Corte EDU) ha tuttavia cercato di sopperire con la sua giurisprudenza. Questa, similmente a quanto fatto dalla *case law* delle Corti statunitensi, ha gradualmente colto le molteplici sfaccettature del diritto alla privacy, inteso non solo come salvaguardia «against arbitrary interference by the public authorities in his private family life», ma anche come «right to personal development» [28]. In questa ultima e forse più complessa accezione, «Article 8 protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world» [29]. Grazie

[27] D. SOLOVE, *Conceptualizing privacy*, in *California Law Review*, 90, 2002, p. 1102.

[28] Corte EDU 9 febbraio 1967, *Case "relating to certain aspects of the laws on the use of languages in education in Belgium" v. Belgium*, Application n. 1474/62.

[29] Corte EDU 6 febbraio 2021, *Bensaid v. UK*, Application n. 44599/98.

anche all'apporto dei giudici di Strasburgo [30], dunque, si realizza progressivamente ma rapidamente anche nel continente europeo l'affermazione di quella che è stata definita «decisional privacy» ovvero la «libertà di autodeterminarsi rispetto alle scelte personali, siano esse pertinenti alla procreazione, la libertà sessuale o la libertà di organizzazione» [31], intendendo il diritto alla riservatezza come «funzionale al libero esplicarsi della persona» [32] e, dunque, «diritto della personalità» [33].

La tutela della riservatezza ha poi trovato ulteriore e significativo riconoscimento nella legislazione dell'UE, in particolare nella Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza) adottata nel 2000 e alla quale, come noto, è stato attribuito il medesimo valore giuridico dei Trattati solo nel 2009 con il Trattato di Lisbona [34]. L'art. 7 della Carta infatti prevede espressamente il diritto al rispetto della vita privata e della vita famigliare, con un dettato normativo simile a quello della CEDU: «Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni». Anche dalla garanzia offerta da questa disposizione, rafforzata dal dinamico ed attivo

[30] Come sottolineato da Tiberi, la giurisprudenza della Corte EDU ha fornito un approccio evolutivo e dinamico al concetto di "vita privata", ammettendo peraltro come «sarebbe troppo restrittivo limitare la nozione di vita privata ad una cerchia intima nella quale ciascuno può condurre la sua vita personale come crede, ed escludere completamente il mondo esterno a tale cerchia. Il rispetto alla vita privata deve perciò anche comprendere una sfera esterna del soggetto, cioè il diritto dell'individuo di stringere e sviluppare relazioni sociali con altri individui e con il mondo esterno in generale, che si tratti di sfera intima o sessuale, o che riguardi invece il campo professionale e commerciale», G. TIBERI, *Il diritto alla protezione dei dati personali nelle Carte e nelle Corti sovranazionali (in attesa del Trattato di Lisbona)*, in *Cassazione Penale*, 11, 2009, p. 4467.

[31] A. MANTELERO, *Il costo della privacy tra valore della persona e ragione dell'impresa*, Giuffrè, Milano, 2007, p. 13. In questa prospettiva si legga anche M. GAMBINI, *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *EJJL*, 1, 2013, p. 1 ss.

[32] S. BONFIGLIO, *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Diritto e Sicurezza*, 3, 2014, p. 2.

[33] L. CALIFANO, *Privacy e sicurezza*, in *Diritto e Sicurezza*, 3, 2013, p. 7.

[34] Il Trattato di Lisbona è stato sottoscritto il 13 dicembre 2007 ma è entrato in vigore il 1 dicembre 2009.

intervento della CGUE, il diritto alla privacy ha assunto sempre più un carattere trasversale [35], «accostato al valore persona come mezzo per tutelare la sua dignità e il suo sviluppo all'interno della società» [36], ben presto affermandosi anche nei singoli ordinamenti degli Stati membri [37].

---

[35] In questi termini si esprime S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006.

[36] E. BRUGIOTTI, *La privacy attraverso le generazioni dei diritti. Dalla tutela della riservatezza alla protezione dei dati personali*, in *Dirittifondamentali.it*, 2, 2013, p. 4.

[37] A livello nazionale si riscontrano differenze tra quegli ordinamenti nei quali il diritto alla vita privata ha conosciuto un'espressa previsione nel testo costituzionale e quelli invece in cui tale diritto ha trovato tutela mediante l'intervento giurisprudenziale, anche grazie al richiamo alle fonti di diritto sovranazionale e alle Carte EDU e di Nizza in particolare. Tra le Costituzioni che riconoscono espressamente, ispirandosi al testo dell'art. 8 della Convenzione EDU, il diritto alla vita privata si rinviene l'art. 18 della Costituzione spagnola del 1978, l'art. 35 della Costituzione slovena del 1991 che tutela il "diritto alla riservatezza e i diritti della personalità", o ancora l'art. 26 della Costituzione portoghese del 1976 che inserisce nella medesima disposizione il diritto alla riservatezza "dell'intimità della vita privata e famigliare" e quello all'identità personale e allo sviluppo della personalità. In Francia invece il diritto alla privacy non ha ottenuto esplicito riconoscimento nel testo costituzionale: è solo nell'art. 9 del Code Civil che viene fatto riferimento al diritto alla vita privata. In Italia la Costituzione riconosce l'inviolabilità del domicilio (art. 14) e la segretezza e libertà della corrispondenza (art. 15), mentre non trova spazio autonomo il diritto alla vita privata e famigliare; sentenze quali la n. 366 del 1991 della Corte costituzionale o la n. 5525 del 2012 della Sez. III Civ. della Corte di Cassazione hanno però attribuito rango di diritto fondamentale al diritto alla riservatezza, che trova il proprio ancoraggio costituzionale in libertà esplicitamente riconosciute quali quelle di cui agli artt. 2, 3, 13, 15, 21 e 32 (per approfondimenti sul punto, tra i tanti, si rimanda a G. ALPA, B. MARKESINIS, *Il diritto alla privacy nell'esperienza di common law e nell'esperienza italiana*, in *Rivista trimestrale di diritto civile e procedura civile*, 51, 1974, p. 417; T.M. UBERTAZZI, *Diritto alla privacy, natura e funzioni giuridiche*, Cedam, Padova, 2004; U. PAGALLO, *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè, Milano, 2008). Come sottolineato da Cepeda Espinosa, merita comunque rilevare come, similmente al legislatore nazionale, anche l'intervento giurisprudenziale sia stato portatore, nei diversi Stati membri, di diversi approcci al diritto alla privacy e alla sua definizione, risentendo anche delle differenze riscontrabili nella cultura – giuridica e non – dei diversi ordinamenti. Così «privacy in some countries is associated with specific legal ideas, such as inviolability of domicile and the secrecy of correspondence, whereas in others it is related to broad concepts such as freedom, dignity, autonomy», M.J. CEPEDA ESPINOSA, *Privacy*, cit., p. 968.

Ma la Carta di Nizza e il diritto dell'UE più in generale non si sono limitati a tutelare espressamente il solo diritto alla riservatezza: con una scelta invero fortemente innovativa, la Carta ha infatti introdotto anche il diritto alla protezione dei dati, inserendolo all'art. 8 appena successivo a quello in materia di privacy. Nonostante la vicinanza di tali disposizioni, quest'ultimo moderno diritto prevede un contenuto e un significato specifici, che meritano di essere brevemente analizzati.

2.2. *Dalla dimensione negativa a quella positiva: il progressivo affermarsi del diritto alla protezione dei dati.*

L'avvento delle nuove tecnologie, nonché l'affermarsi della digitalizzazione e della "datificazione" [38] hanno imposto, in particolare a partire dagli anni '90 dello scorso secolo, nuove esigenze di tutela, evidenziando i limiti della protezione offerta dal solo diritto alla riservatezza: mentre l'interferenza nella sfera privata subita da Warren e Brandeis da parte di fotografi e giornalisti appariva del tutto palese e manifesta nelle sue immediate conseguenze, le moderne tecnologie, attraverso l'impiego di algoritmi, sistemi di Intelligenza Artificiale, creazione di banche dati e strumenti di sorveglianza e profilazione [39], possono invece manifestarsi in

[38] Questo termine, trasposizione italiana del termine inglese *datification*, è volto a designare «la centralità acquisita dai dati personali in ogni ramo dell'attività umana, suscettibile di essere appunto "datificata" ovvero ridotta ad informazione e rappresentata mediante serie di dati; e in un'accezione più specifica indica la possibilità, attraverso analisi predittive, di estrarre nuove informazioni a carattere personale da dati già raccolti in precedenza», R. D'ORAZIO, *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, p. 67.

[39] Resa semplice dalle operazioni di c.d. *data mining* cioè di selezione ed estrazione automatizzata di informazioni tra una mola enorme di dati, la profilazione consente di ricostruire un preciso profilo degli utenti – delle preferenze, interessi, opinioni condivise, abitudini – partendo dalle diverse "tracce digitali" quotidianamente prodotte online o sui *social network*. Sui profili critici ed insidiosi di tale moderna tecnica di elaborazione dati si rimanda a O. SESSO SARTI, *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, Editoriale Scientifica, Napoli, 2017, p. 574 ss., L. MONTUORI, M. SIANO, *Evoluzione del concetto di consenso in-*

lesioni dei diritti fondamentali molto più articolate e subdole, rispetto alle quali il diritto alla riservatezza, pur nelle sue molteplici sfaccettature, non è in grado di fornire adeguata protezione e garanzia. Come le rivelazioni di Snowden e il differente ma egualmente inquietante caso *Cambridge Analytica*[40] hanno drammaticamente posto in evidenza, le minacce prodotte dal progresso tecnologico non sono infatti più unicamente legate ad una compressione della sfera più intima di ciascun consociato o, ancora, ad una limitazione del pieno ed autonomo sviluppo degli individui nella società in cui vivono: i pericoli del mondo dei *bit* e delle telecomunicazioni sono piuttosto legati alla perdita di ogni controllo sui dati che vengono quotidianamente e spesso inconsapevolmente creati dagli utenti; le "tracce digitali"[41] che lasciamo dietro di noi ogni giorno posso-

---

formato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Aracne, Roma, 2017, p. 101 ss.

[40] Questo noto e discusso scandalo, svelato dalle inchieste dei giornali *The Guardian* e *New York Times* nel marzo 2018, ha messo in luce l'impiego da parte della società di consulenza e marketing Cambridge Analytica di dati illegalmente sottratti al *social network* Facebook al fine di profilare gli utenti e predisporre messaggi mirati, facendo circolare *fake news* mediante la creazione di profili *bot* e incidendo così, mediante una selezione di messaggi e notizie targettizzate a seconda del destinatario, sui convincimenti personali – anche politici – degli ignari destinatari. Queste pratiche avrebbero comportato, sebbene con profili ancora da accertare, un significativo impatto sia sull'esito delle elezioni presidenziali americane del 2016, sia sul voto relativo alla procedura di *Brexit* nel Regno Unito. É emersa dunque una nuova consapevolezza circa i rischi e le insidie derivanti dalle pratiche di profilazione nonché dal riutilizzo da parte di soggetti terzi di dati prodotti e raccolti per diverse finalità. Su questa complessa vicenda si rinvia a E. ASSANTE, *Cosa ci può insegnare il caso Cambridge Analytica*, in *Federalismi.it*, 9, 2018, p. 1 ss.; D. MESSINA, *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Anlaytica"*, in *Federalismi.it*, 20, 2018, p. 1 ss.; A. SORO, *Democrazia e potere dei dati. libertà, algoritmi e umanesimo digitale*, Baldini Castoldi, Milano, 2019; G. ZICCARDI, *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina, Milano, 2019.

[41] Come scritto da De Minico, «sta accadendo in Internet quanto capitava a Pollicino che nell'attraversare il bosco lasciava cadere a terra briciole di pane per ritrovare la via di casa. Anche noi durante la navigazione lasciamo cadere frammenti della nostra identità, che raccolti e riorganizzati da chi verrà dopo comporranno il patrimonio virtuale della sua attività d'impresa, cioè gioveranno fondamentalmente a chi li ha raccolti», G. DE

no essere impiegate per ricostruire nel dettaglio la nostra vita, abitudini, preferenze, orientamenti politici o sessuali, fornendo informazioni estremamente delicate che rischiano di essere sfruttate per le finalità più disparate, dalla sorveglianza per scopi di garanzia della sicurezza nazionale e pubblica, al marketing o alla profilazione per fini assicurativi [42]. Proprio dinnanzi a tali ampliate insidie, si è venuto ad affermare un differente interesse da proteggere, distinto da quello posto alla base del diritto alla riservatezza: esso è stato identificato non solo nell'interesse a che «non siano raccolte e diffuse informazioni che non si intende fornire o di cui si è disposti a dare conoscenza entro ambiti limitati, ma anche nell'interesse ad impedire il collegamento di informazioni diverse che ci riguardano, anche da noi stessi fornite, al fine di evitare aggregazioni di informazioni per scopi non voluti o non previsti» [43]. Questa inedita esigenza di tutela ha dunque quale fulcro non più direttamente l'individuo bensì i dati da esso prodotti, che vanno protetti nelle diverse operazioni di raccolta, conservazione, accesso, impiego, trattamento e analisi.

È in tale mutato contesto e da questi diversi bisogni di tutela che viene così ad affermarsi lentamente ma in maniera decisa una evoluzione dal diritto alla riservatezza inteso come tutela statica e negativa, al diritto alla protezione dei dati quale dinamica e positiva proiezione del diritto alla privacy nella dimensione tecnologica [44]. La riconosciuta tutela della *data protection* si connette pertanto ad una diversa dimensione del diritto

---

MINICO, *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto pubblico*, 1, 2019, p. 90. Della stessa autrice anche *Libertà in rete. Libertà dalla rete*, Giappichelli, Torino, 2020. Similmente sul punto si leggano anche V. ZENO-ZENCOVICH, *Dati, grandi dati, dati granulari e la nuova epistemiologia del giurista*, in *MediaLaws*, 2, 2018, p. 32 ss.

[42] Vasti sono gli ambiti all'interno dei quali le tecniche di profilazione possono essere impiegate allo scopo di ricostruire preferenze ed orientamenti degli individui per indirizzare messaggi pubblicitari mirati, per svolgere previsioni di rischio nell'ambito delle assicurazioni fondate sull'elaborazione di dati in grado di stabilire gli stili di vita e persino per veicolare in maniera targettizzata messaggi elettorali attraverso tecniche di c.d. segmentazione psicografica.

[43] G. TIBERI, *Il diritto alla protezione dei dati personali*, cit., p. 4469.

[44] Per una analisi approfondita di questi interessanti profili, si rimanda a S. RODOTÀ, *Tecnologia e diritti*, Il Mulino, Bologna, 1995.

all'autodeterminazione, che non è più quella *decisional privacy* di cui si è parlato sopra, bensì diviene una *informational privacy* che si «manifesta cioè in una sorta di signoria sulle informazioni inerenti la propria persona, traducendosi in un limite non solo alla diffusione di indiscrezioni sulla vita privata, ma anche, più in generale, alla raccolta ed all'impiego arbitrario dei dati personali» [45]. Questa differente sfaccettatura del diritto allo sviluppo libero della propria personalità è stata del resto gradualmente affermata tanto dalla dottrina quanto dalla giurisprudenza: sotto il primo profilo, Frosini già nel 1981 parlava di "libertà informatica" nella sua accezione positiva, che esprime cioè «la facoltà di esercitare un diritto di controllo sui dati concernenti la propria persona che sono fuoriusciti dalla cerchia della privacy per essere divenuti input di un programma elettronico; e dunque libertà informatica positiva, o diritto soggettivo riconosciuto, di conoscere, correggere, togliere o aggiungere dati in una scheda personale elettronica» [46]. Proprio negli stessi anni si rinviene anche una storica e rilevante pronuncia del Tribunale costituzionale federale tedesco, nella c.d. "decisione sul censimento" (*Volkszahlungsentscheidung*, BVerfG 65, NJW, 15 dicembre 1983). Con tale sentenza i giudici hanno riconosciuto il diritto all'autodeterminazione informativa che, come riassunto da Di Martino, «presuppone che a ciascuno sia assicurata la libertà di decidere in ordine alle azioni da intraprendere o da omettere, per poi comportarsi di conseguenza. Chi non può valutare la diffusione delle informazioni che lo riguardano in un determinato ambiente sociale, può essere sostanzialmente dissuaso dall'intraprendere azioni che altrimenti avrebbe liberamente scelto», così che il diritto affermato viene inteso come «una concretizzazione del diritto generale della personalità di cui agli artt. 1, I co., 2, II co., GG, (…) e come potere di ciascuno di decidere sostanzialmente da sé circa la rivelazione e l'utilizzo dei propri dati personali» [47].

---

[45] A. MANTELERO, *Il costo della privacy tra valore della persona e ragione dell'impresa*, cit., p. 1.

[46] Relazione di V. FROSINI, *La protezione della riservatezza nella società informatica*, in N. MATTEUCCI, *Privacy e banche dei dati*, Il Mulino, Bologna, 1981, p. 41. Ma anche V. FROSINI, *Diritto alla riservatezza e calcolatori elettronici*, in AA. VV., *Il riserbo e la notizia*, Jovene, Napoli, 1983.

[47] A. DI MARTINO, *La protezione dei dati personali*, in S. PANUNZIO (a cura di), *I di-*

Il legame così rilevato tra libero sviluppo della personalità e adeguata protezione dei dati che ci riguardano fa sorgere la necessità del riconoscimento di un diritto al controllo sulle informazioni e sui dati prodotti: è quello che Rodotà chiamava con il suggestivo termine dell'*habeas data*, inteso come sviluppo del più antico *habeas corpus*, ovvero di una esigenza, maturata dal mutare delle circostanze e del progresso tecnico-scientifico, di passare dalla tutela della libertà del corpo, nella sua accezione fisica e di intendimento, alla tutela della libertà della persona nella sua dimensione "datizzata". Un passaggio, quello descritto da Rodotà, che «è stato colto quando ci si è resi conto che la tradizionale nozione di privacy, come diritto a essere lasciato solo, non era più in grado di comprendere una dimensione così profondamente mutata» [48].

Il sempre maggiore e più profondo riconoscimento del diritto alla protezione dei dati, così come sopra delineato, ha visto un lento e complesso percorso di affermazione nel nostro continente a livello sovranazionale. Volendo ripercorrere le tappe che hanno contrassegnato la genesi

---

ritti fondamentali e le Corti in Europa, Jovene, Napoli, 2005, p. 365. Vivarelli, a commento di tale pronuncia, sottolinea come «this result definitively marks the transition from a static view of privacy to a dynamic one known as 'informational privacy'», A. VIVARELLI, *The crisis of the rights to informational self-determination*, in *The Italian Law Journal*, 1, 2020, p. 308.

[48] S. RODOTÀ, *Il mondo nella rete. Quali i diritti, quali i vincoli,* Laterza, Roma-Bari, 2013, p. 35. Come poi ribadito e sottolineato da altri esperti in materia, il «percorso di costruzione del diritto alla protezione dei dati personali si intreccia con il crescente sviluppo dell'innovazione tecnologica delle comunicazioni elettroniche alla base della nostra società digitale e della globalizzazione delle relazioni interpersonali, economiche, finanziarie e sociali», L. CALIFANO, *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, cit., p. 2. Così, «la stessa definizione ed il contenuto essenziale della riservatezza devono allora adeguarsi, dal momento che il problema non è più soltanto quello di evitare l'ingerenza e la diffusione, che rappresentano l'aspetto primitivo della questione, essendosi il baricentro adesso spostato dall'esigenza di isolamento al potere di controllo sulle informazioni rilevanti per l'interessato, anche dopo che siano divenute conosciute all'esterno», G. FAMIGLIETTI, *Il diritto alla riservatezza o la riservatezza come diritto*, cit., p. 320. Sul punto si legga anche ampiamente G. PASCUZZI, *Il diritto alla riservatezza nell'era di Internet*, in AA. VV., *Studi in onore di Piero Schlesinger*, Giuffré, Milano, 2004, p. 337 ss.; nonché dello stesso autore *Il diritto dell'era digitale*, V Edizione, Il Mulino, Bologna, 2020.

europea di tale fondamentale diritto, non si può che prendere avvio dalla già richiamata Convenzione EDU e, in particolare, dall'analizzato art. 8: se è vero che questa disposizione risultava priva di qualsiasi cenno alla protezione dei dati [49] – con una mancanza motivata dal fatto che nel 1950 il progresso informatico era ancora agli albori e la tecnologia stessa era prevalentemente intesa come strumento volto al raggiungimento di uno scopo e «non come fattore capace di influenzare le modalità di esercizio di un diritto o addirittura capace di elaborarne di nuovi» [50] –, è altrettanto importante notare come il Consiglio d'Europa si fosse mostrato già negli anni '80 del Novecento consapevole della necessità di integrare la Convenzione con indicazioni in grado di fornire una base comune di protezione dei dati [51], anche e soprattutto per fronteggiare l'emergere confuso e disomogeneo, in quello stesso periodo, di normative nazionali in materia di *data protection* [52]. Veniva perciò adottata la Convenzione di

[49] Secondo Pollicino, infatti, il dettato dell'art. 8 CEDU è portatore di «una dimensione statica, dunque, di riservatezza e a contenuto prevalentemente negativo, non in grado di cogliere appieno il dinamismo del processo tecnologico che ha portato alla emersione di un'autonomia concettuale del diritto alla protezione del dato personale nell'ambito di quel processo, *work in progress*, che coincide con il trattamento del dato stesso», O. POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in www.forumcostituzionale.it, 31 dicembre 2013.

[50] F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016, p. 57.

[51] G. BUQUICCHIO, *Aspetti internazionali della protezione dei dati: il ruolo svolto dal Consiglio d'Europa*, in N. MATTEUCCI (a cura di), *Privacy e banche dati*, Il Mulino, Bologna, 1981. Su questa tematica si legga anche E. PAVARANI, *Diritto al rispetto della vita privata e familiare*, in C. DEFILIIPPI, D. BOSI, R. HARVEY (a cura di), *La Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, ESI, Napoli, 2006, p. 291 ss.

[52] La Germania fu il primo Stato europeo ad approvare leggi in materia di protezione dei dati personali: la prima disciplina in tema, infatti, fu quella adottata dal Land dell'Assia che nel 1970 aveva predisposto una normativa a tutela dei lavoratori e dei loro dati personali dinnanzi a forme di schedatura indebita e di conservazione di dati all'interno di banche dati create dai datori di lavoro. Risale invece al 1992 la *Ley Organica de regulacion del tratamiento automatizado de los datos de caracter personal* adottata in Spagna qualche anno prima della Direttiva 95/46/CE. Merita poi sottolineare come anche in alcuni testi costituzionali di fine anni '70 sia possibile trovare il riconoscimento di un autonomo diritto alla protezione dei dati: è il caso dell'art. 35 della Costituzione

Strasburgo n. 108/1981 *sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*, primo strumento normativo a livello internazionale che ha riconosciuto e stabilito principi nell'ambito della tutela dei dati [53]. Anche grazie a tale intervento, cui poi la stessa Corte EDU si è ispirata e ha fatto riferimento nella propria giurisprudenza [54], si è dunque potuto ampliare l'ambito di garanzia fornito

portoghese che stabilisce che «tutti i cittadini hanno il diritto di accesso ai dati informatici che li riguardano, potendone esigere la rettifica e l'aggiornamento, e il diritto di conoscere la finalità cui sono destinati, nei termini della legge. 2. La legge definisce il concetto di dati personali così come le condizioni applicabili ad essi quanto a trattamento automatizzato, connessione, trasmissione e utilizzazione, garantendone la protezione specificatamente attraverso organismi amministrativi indipendenti. 3. L'informatica non può essere utilizzata per il trattamento di dati relativi a convinzioni filosofiche o politiche, affiliazione a partiti o sindacati, fede religiosa, vita privata e origine etnica, salvo mediante consenso espresso del titolare, autorizzazione prevista per legge con garanzie di non discriminazione o nel caso di elaborazione di dati statistici non identificabili individualmente. 4. È vietato l'accesso ai dati personali di terzi, salvo in casi eccezionali previsti dalla legge. 5. È vietata l'attribuzione di un numero nazionale unico ai cittadini»; la Costituzione dei Paesi Bassi invece dispone all'art. 10, co. 2 che debba essere affidato ad una legge ordinaria il compito di determinare una disciplina normativa completa sul trattamento dei dati personali.

[53] Tale Convenzione era peraltro aperta alla firma e ratifica non solo degli Stati parte del Consiglio d'Europa bensì anche di Stati terzi.

[54] Pur non potendo, in questa sede, analizzare tutte le pronunce della Corte EDU nelle quali viene disposto un riconoscimento del diritto alla protezione dei dati come riconducibile alla tutela offerta dall'art. 8 della Convenzione, pare utile e chiara la sintesi proposta da De Hert e Gutwirth: «without having at its disposal an explicit data protection right, the Court has brought many data protection aspects under the scope of Art. 8 of the Convention. (…) The Strasbourg Court has expressed the view that the protection of personal data is fundamentally important to a person's enjoyment of his or her right to respect for private life. Through its references to the 1981 Data Protection Convention, the Strasbourg Court has endorsed and spread the idea that data protection is more than just technical regulation. (…) But we have also to underline some of the shortcomings of the Strasbourg reception of data protection: not all data are protected, the recognition of the rights to information and access is far from straightforward», P. DE HERT, S. GUTWIRTH, *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, in S. GUTWIRTH, Y. POULLET, P. DE HERT. C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing data protection?*, Springer, Berlino, 2009, p. 27.

dallo statico art. 8, estendendolo così anche ai dati ai quali deve essere assicurata una protezione specifica dinnanzi alle invasive e sempre più pregnanti nuove tecnologie. È stata quindi per la prima volta fornita, all'interno di un testo normativo di diritto internazionale, la definizione di "dato personale", inteso come «ogni informazione concernente una persona fisica identificata o identificabile» (art. 2, lett. a), e sono state riconosciute una serie di importanti tutele e principi volti a determinare la correttezza del trattamento, la liceità dello stesso nonché il divieto di trattamento di "categorie speciali di dati" [55]. Pur in una forma embrionale, ancora fortemente legata al diritto alla vita privata, il documento redatto dal Consiglio d'Europa rappresentava un importante atto capace di stabilire il «minimo comune denominatore della protezione dei dati in Europa, su cui sarà costruita la successiva normazione a livello comunitario» [56].

E sarà proprio a livello dell'Unione europea che tale diritto otterrà poi un solido ed autonomo riconoscimento [57]: «pochi altri diritti appartenenti alla c.d. nuova generazione possono vantare l'autentica e solida matrice europea che è propria del diritto alla protezione dei dati personali» [58].

Sulla scia dell'intervento del Consiglio d'Europa, infatti, l'Unione europea nel 1995 ha adottato la nota Direttiva 95/46/CE *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché al-*

---

[55] Ci si riferisce a quelli che vengono comunemente chiamati *data sensibili* ovvero i dati di carattere personale «indicanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale" che "non possono essere elaborati automaticamente a meno che il diritto interno non preveda garanzia adatte», art. 6.

[56] G. TIBERI, *Il diritto alla protezione dei dati personali*, cit., p. 360.

[57] In questo senso, e proprio riconoscendo l'importanza della dottrina, di alcuni interventi giurisprudenziali nazionali come quello tedesco sopra richiamato nonché delle disposizioni adottate dal Consiglio d'Europa, è possibile condividere l'affermazione secondo cui «le radici europee della privacy e della protezione dei dati personali non sono solo il risultato dell'evoluzione del paradigma negativo americano, ma anche di una maturazione europea avvenuta nella seconda metà del XX secolo», G. DE GREGORIO, R. TORINO, *Privacy, tutela dei dati personali e Big Data*, cit. p. 447.

[58] L. CALIFANO, *Introduzione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, cit., p. xxiii.

la libera circolazione di tali dati. Il Considerando 3 [59] di tale normativa risultava però esemplificativo dell'iniziale approccio del legislatore europeo dinnanzi all'esigenza di garantire la protezione dei dati: prendendo atto delle disomogeneità riscontrate nelle differenti normative in materia di protezione dei dati nel frattempo adottate dai vari Stati membri, che finivano col rappresentare barriere immateriali in grado di rendere difficoltosa la realizzazione di un mercato unico e libero, la Direttiva 95/46 emergeva come frutto della vocazione economica della Comunità europea ai suoi esordi nonché dell'obiettivo di realizzare il Mercato Unico, abbattendo le restrizioni alla libera circolazione di merci, servizi e persone [60].

Se la Direttiva 95/46 proponeva così un bilanciamento tra libertà e diritti fondamentali, tra cui l'affermato diritto alla vita privata da un lato e la libera circolazione dei dati dall'altro, la successiva tappa rappresentata dalla adozione della Carta di Nizza ha determinato invece una evoluzione ben più decisa e significativa nell'ottica di una espressa dichiarazione del diritto alla protezione dei dati. Con la Carta di Nizza, infatti, accanto al diritto alla riservatezza – l'art. 7 di cui si è sopra parlato –, ha trovato posto l'art. 8 nel quale viene affermato che «ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente». Questa chiara e netta distinzione tra diritto alla vita privata e diritto alla protezione dei dati è tutt'altro che una mera differenziazione di facciata, rappresentando al contrario un riconoscimento della dignità propria che il legislatore del-

[59] «L'instaurazione e il funzionamento del mercato interno, nel quale è assicurata la libera circolazione delle merci, delle persone, dei servizi e dei capitali, esigono non solo che i dati personali possano circolare liberamente da uno Stato membro all'altro, ma che siano altresì salvaguardati i diritti fondamentali della persona».

[60] Per questo la base giuridica di tale Direttiva è stata identificata nell'art. 95 TCE (Trattato che istituisce la Comunità europea) finalizzato a consentire l'adozione da parte della Comunità europea di misure di ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri aventi per oggetto appunto l'instaurazione ed il funzionamento del mercato interno.

l'UE ha voluto attribuire alla sempre più forte esigenza di controllo e tutela dei dati e delle informazioni personali; l'affermazione di una fattispecie autonoma ha dunque permesso da un lato di attribuire al diritto alla protezione dei dati un rilievo che non trovava precedenti nella Convenzione EDU, mentre dall'altro di consentire un chiaro ed espresso «recepimento di un patrimonio inestimabile costituito dalla pluridecennale giurisprudenza della Corte EDU» che aveva arricchito, insieme alla Convenzione di Strasburgo e ai principi in essa affermati, il dettato dell'art. 8 Convenzione EDU, adattandolo all'evoluzione dei tempi [61].

L'inserimento entro la Carta di Nizza non è stata comunque l'unica modifica sostanziale delle fonti di diritto dell'UE: l'art. 16 del Trattato sul Funzionamento dell'UE (TFUE) ha infatti espressamente riconosciuto il diritto di ogni individuo alla protezione dei dati di carattere personale che lo riguardano, mentre al comma 2 viene previsto che «il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti». Attribuendo così questa competenza all'UE, è stato chiaramente consentito al legislatore europeo di adottare normative che permettano una protezione attiva ed effettiva dei dati [62]. Ed è proprio con riferimento a tale disposizione che il vigente ed imponente Regolamento generale sulla protezione dei dati (c.d. GDPR, Reg. UE 2016/679) trova la propria base giuridica [63]: questa corposa e innovativa normativa ha predi-

---

[61] F. PIZZETTI, *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA, M. D'AMICO (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, Milano, 2009, p. 86.

[62] Per un commento a tale articolo si rimanda a P. PIRODDI, *Art. 16 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'Unione europea*, Cedam, Padova, II Ed., 2014, p. 189 ss.

[63] Come precisato da Finocchiaro, il Regolamento «non ha ad oggetto il diritto alla riservatezza: ha un ambito molto più ampio della riservatezza, ma che non è necessaria-

sposto una ampia disciplina aggiornata ed adeguata al mutare dei tempi, che ha sostituito l'ormai anacronistica Direttiva del 1995, pur non abbandonando del tutto quella vocazione economica che ha contraddistinto la disciplina della protezione dei dati a livello europeo sin dalla sua prima affermazione [64].

In conclusione, dalla pur breve ricostruzione elaborata in questo paragrafo, volta ad evidenziare le principali evoluzioni nonché le fonti del diritto dell'UE in tema di diritto alla protezione dei dati, è possibile cogliere l'unicità e l'importanza del cammino europeo – inteso in senso lato – di affermazione della *data protection* e del suo rilievo soprattutto dinnanzi al progresso tecnologico: tale percorso si è realizzato con chiarezza nella

---

mente connesso alla sfera più intima della persona. I dati personali costituiscono il tema disciplinato anche se non si riferiscono a vicende private, intime o familiari. Qualunque informazione, quale che sia il suo contenuto, è oggetto del Regolamento», ribadendo come «il diritto alla protezione dei dati deve essere considerato distinto dalla libertà negativa di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, costituendo invece il fondamento della libertà positiva di esercitare un controllo sul flusso delle proprie informazioni», G. FINOCCHIARO, *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quaderni costituzionali*, 4, 2018, p. 896.

[64] Al Considerando 13 GDPR si legge infatti: «per assicurare un livello coerente di protezione delle persone fisiche in tutta l'Unione e prevenire disparità che possono ostacolare la libera circolazione dei dati personali nel mercato interno, è necessario un regolamento che garantisca certezza del diritto e trasparenza agli operatori economici, comprese le micro, piccole e medie imprese, offra alle persone fisiche in tutti gli Stati membri il medesimo livello di diritti azionabili e di obblighi e responsabilità dei titolari del trattamento e dei responsabili del trattamento e assicuri un monitoraggio coerente del trattamento dei dati personali, sanzioni equivalenti in tutti gli Stati membri e una cooperazione efficace tra le autorità di controllo dei diversi Stati membri». La doppia natura ed obiettivo di tutela dei diritti fondamentali da un lato e garanzia della efficienza del Mercato Unico e della libera circolazione di merci dall'altro, resta evidente. Per ulteriori approfondimenti si rimanda, *ex multis*, a: P. PALLARO, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffrè, Milano, 2002; G. GONZALES FUSTER, *The emergence of personal data protection as a fundamental right of the EU*, Spinger, Berlino, 2014; F. BALDUCCI ROMANO, *La protezione dei dati personali nell'UE tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario,* 6, 2015, p. 1619 ss. Per uno studio approfondito del GDPR, si rimanda, tra i tanti, a L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona*, cit.; V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personale nel diritto europeo*, Giappichelli, Torino, 2019.

disposizione di obblighi legislativi e di un apparato normativo solido e articolato, anche ed in particolare a livello dell'UE, rappresentativi del «punto di approdo di una lunga evoluzione concettuale che, nelle sue varie tappe, ha arricchito di implicazioni e significati nuovi e ulteriori un concetto che si è caratterizzato e che si caratterizza ancora oggi per la sua incessante mutevolezza contenutistica e per la capacità di racchiudere in sé una serie di esigenze multiformi» [65].

3. *La* data retention *tra esigenze securitarie e tutela dei diritti fondamentali: una rinnovata sfida.*

L'analisi sin qui svolta ha permesso non solo di delineare la complessità dei diritti alla riservatezza e alla protezione dei dati ma anche di metterne in luce la forte connessione con la piena tutela di altri fondamentali diritti. Non è un caso che proprio nella già richiamata sentenza del Tribunale federale tedesco del 1983 i giudici di Karlsruhe avessero individuato il fondamento del diritto alla autodeterminazione informativa ivi riconosciuto proprio nei diritti alla dignità e alla libertà personale: il potere sui propri dati, la possibilità di decidere se diffonderli nonché di accertarne la correttezza e l'utilizzo che ne viene fatto, sono stati infatti considerati precondizioni necessarie a che la personalità possa liberamente esplicarsi nella società e nelle relazioni interpersonali, legandosi così a quella capacità di autonomia di scelta posta alla base della garanzia della dignità umana. Il fatto che proprio in Germania questa connessione tra tutela della sfera privata, protezione dei dati, libertà e dignità abbia incontrato una così importante affermazione risulta, del resto, estremamente significativo: gli orrori del totalitarismo nazista si erano realizzati anche

[65] L. MIGLIETTI, *Profilo storico-comparativi del diritto alla privacy*, in *Diritti Comparati*, 4 dicembre 2014. E similmente: «il diritto alla privacy che Warren e Brandeis immaginarono come *right to be let alone* ha conosciuto un processo di migrazione dagli USA verso l'Europa, arricchendosi progressivamente di una dimensione che non tutela esclusivamente l'aspettativa di riservatezza dell'individuo ma che vede nella definizione di un sistema di principi e regole a tutela dei dati un ulteriore momento essenziale a presidio della personalità individuale», O. POLLICINO, M. BASSINI, *Social network e tutela dei dati personali*, cit., p. 74.

grazie ad un annientamento della sfera privata e ad un controllo delle scelte individuali che perdevano così la loro stessa natura di decisioni libere, per essere invece governate dall'alto anche mediante l'impiego di forme pervasive di sorveglianza delle relazioni, delle preferenze, delle abitudini, delle opinioni politiche e degli orientamenti sessuali o religiosi di ogni cittadino. Entrando nella vita privata ed esercitando forme di sorveglianza e coazione che non conoscevano limite né nella dimensione delle abitazioni private né nella corrispondenza, il potere nazista violava la dignità umana per ammettere solo asservimento ed omologazione [66]. Non stupisce pertanto che i giudici tedeschi, consapevoli dell'impatto che la negazione della dimensione privata aveva comportato nella tragica esperienza del regime totalitario, abbiano riconosciuto con chiarezza l'intrinseco legame che la garanzia della privacy e della *data protection* intesse con l'esercizio effettivo e reale delle libertà personali e, con uno sguardo più ampio e complessivo, con la stessa democraticità delle nostre società. L'affermazione dell'identità individuale e della sua correlata autonomia e libertà, nelle sue diverse accezioni – di espressione, politica, di associazione, di pensiero –, non possono svilupparsi se non nella dimensione della sfera privata, che deve essere dunque tutelata da ingerenze esterne, e nel controllo positivo e attivo sui dati e sulle informazioni che ci definiscono

[66] Come ben sottolineato da Porcedda, «totalitarian regimes crushed private and family life, home and correspondence with the use of ideology and terror, with a view to curbing individuals'spontaneity and leeway for action, and substituted autonomy with automatic processes», M.G. PORCEDDA, *The recrudescence of 'Security v. Privacy' after the 2015 terrorist attacks and the value of privacy rights in the European Union*, in E. ORRÙ, M.G. PORCEDDA, S. WEYDNER-VOLKMANN (a cura di), *Rethinking surveillance and control: beyond the 'security versus privacy' debate*, Nomos, Baden-Baden, 2017. L'autrice fa derivare da queste considerazioni che «both rights are instrumental in fostering personhood, one's unique identity, protected as an expression of dignity and enabling autonomy as concepts emerged out of modernity». Anche Rodotà ha più volte messo in luce la correlazione tra totalitarismo e violazione della riservatezza e della protezione dei dati: «non bisogna mai perdere la memoria di quel che è avvenuto nei regimi totalitari, dove violazioni profonde dei diritti fondamentali sono state possibili proprio grazie a massicce raccolte di informazioni che hanno consentito un controllo continuo della vita quotidiana», S. RODOTÀ, *Privacy, libertà, dignità, discorso conclusivo della Conferenza internazionale sulla protezione dei dati,* disponibile all'indirizzo www.privacy.it/archivio/rodo20040916.html, 2004.

e che potrebbero, altrimenti, finire esse stesse col controllarci [67].

Si comprende pertanto come il diritto alla riservatezza e quello alla protezione dei dati rivestano un'importanza strumentale e finalistica «tale da poter compromettere, in caso di [loro] violazione, tutta un'altra serie di principi, diritti e libertà che vanno dalla libertà di espressione alla libertà religiosa, dalla libertà d'impresa al diritto di difesa, dal divieto di discriminazione a tutti quei diritti di prestazione posti a tutela dei soggetti più deboli. A fronte di un'autorevole posizione dottrinale che configura il diritto alla protezione dei dati quale presupposto della salvaguardia di ogni diritto costituzionalmente protetto [il riferimento è a F. Pizzetti, nel suo scritto *Privacy e diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016], non vi è dubbio in ogni caso che una compressione del diritto del singolo all'autodeterminazione informativa pone in discussione la salvaguardia della dignità stessa della persona, intesa quale valore costituzionale indisponibile. In questo si fonda il principale collegamento con l'intera e più complessa costellazione dei diritti fondamentali» [68]. Per usare le efficaci parole di Rodotà, dunque, la riservatezza e la protezione dei dati si presentano quali elementi imprescindibili per una società dell'eguaglianza, della partecipazione [69], della dignità [70] e della libertà [71]. Solo se si prende

---

[67] «Privacy prevents interference, pressures to conform, ridicule, punishment, unfavorable decisions, and other forms of hostile reaction. To the extent that privacy does this, it functions to promote liberty of action, removing the unpleasant consequences of certain actions and thus increasing the liberty to perform», R. GAVISON, *Privacy and the limits of law*, in *The Yale Law Journal*, 3, 1980, p. 448.

[68] L. CALIFANO, *Principi e contenuti del Regolamento UE 2016/679*, cit., p. 1.

[69] Sotto questo profilo della partecipazione alla vita politica e dunque della garanzia di una reale ed effettiva democrazia, viene affermato come «privacy and data protection regimes are not there merely to protect the best rights holders'interests, but are necessary in a democratic society to sustain a vivid democracy», A. ROUVROY, Y. POULLET, *The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy*, in S. GURTWIRTH *et al.* (a cura di), *Reinventing data protection?*, cit., p. 57.

[70] Flick giunge a sostenere che la privacy e lo spazio di intimità del singolo siano coessenziali alla stessa dignità (G.M. FLICK, *Elogio della dignità (se non ora, quando?)*, in *Rivista AIC*, 4, 2014, p. 6).

avvio da queste considerazioni si può dunque cogliere appieno l'importanza e l'articolata natura dei due diritti esaminati: la loro garanzia, lungi dal ricoprire un rilievo unicamente per il singolo, si ripercuote anche sull'intera collettività, sulla democraticità della società, sul rispetto dei diritti fondamentali di cui tutti beneficiano e dai quali anche il rapporto tra Stato e cittadino dipende [72].

---

[71] S. RODOTÀ, *Privacy, libertà, dignità*, cit. L'autorevole studioso italiano non è certo il solo ad esprimere tale posizione, che possiamo leggere anche nelle parole del Giudice Douglas della Corte Suprema USA che, nella sua *Dissenting opinion* nel caso *Public Utilities Commission v. Pollak* (US, 451, 467, 1952), ha affermato che «the right to be let alone is indeed the beginning of all freedom». In tempi più recenti e proprio sulla base di tali considerazioni, alcuni autori sono giunti a ritenere che la privacy rappresenti una vera e propria precondizione al godimento degli altri diritti fondamentali: «privacy is not only one of the core fundamental rights, but it also plays a central role for exertion of other fundamental rights and freedoms, for balancing powers between the state and citizens, for democratic development, societal and economic innovativeness or individual autonomy. Privacy is a precondition for thinking and expressing oneself freely, in general and in particular when new media or social networks come into play. (…) Whether the Internet can continue to be an infrastructure for unrestricted communication and access to information, supporting the freedom of expression and political participation or whether it is converted into an instrument of control and surveillance depends predominantly on the respect for privacy», J. CAS, R. BELLANOVA, J.P. BURGESS, M. FRIEDWALD, W. PEISSL, *Introduction: Surveillance, privacy and security*, in J. CAS, R. BELLANOVA, J.P. BURGESS, M. FRIEDWALD, W. PEISSL (a cura di), *Surveillance, privacy and security: Citizens' perspectives*, Routledge, Londra, 2017, p. 8, in cui si richiama il pensiero di D. SOLOVE, *Understanding privacy*, Harvard University Press, Cambridge, Massachusetts, 2008. Similmente, si legga anche N. RICHARDS, *The dangers of surveillance*, in *Harvard Law Review*, 126, 2013, p. 1934 ss.

[72] Regan osserva come «privacy has value beyond its usefulness in helping the individual to maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize the individual is better off if privacy exists. I maintain that the society is better off as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public and collective purposes», P.M. REGAN, *Legislating privacy, technology, social values and public policy*, University of North Carolina Press, Chapel Hill, 1995, p. 221. Parlano di «social value of privacy»: D. SOLOVE, *Nothing to hide. The false trade-off between privacy and security*, Yale University Press, New Haven, 2011 e K. HUGHES, *The social value of privacy, the value of privacy to society and human rights discourse*, in B. ROESSLER, D. MOKROSINKA (a cura di), *Social dimensions of privacy. Interdisciplinary perspectives*, Cambridge University Press, Cambridge, 2015, p. 225 ss.

Tutti questi rilievi divengono così essenziali punti di partenza per cogliere la delicatezza e la complessità delle insidie che la realizzazione di sistemi di raccolta e accesso a dati e metadati, quali quello posto in essere tramite lo strumento della *data retention*, comporta, soprattutto – ma non solo – per i diritti alla riservatezza e alla protezione dei dati: questi ultimi non debbono essere considerati diritti assoluti, ben potendo essere limitati qualora ciò si renda necessario al fine di garantire la tutela di ulteriori e differenti interessi legittimi, come del resto specificato dallo stesso art. 8 Convenzione EDU e artt. 7 e 8 della Carta di Nizza. Nonostante ciò, è innegabile come una compressione della sfera privata e del controllo sui propri dati debba essere realizzata con estrema attenzione, imponendo la determinazione di un punto di equilibrio tra una solida tutela dei diritti fondamentali alla riservatezza e alla protezione dei dati da un lato e, dall'altro, la tentazione di Governi e Istituzioni dell'UE di porre in essere regimi estensivi di conservazione ed analisi della vasta mole di dati e metadati prodotti mediante sistemi di telecomunicazione in risposta alla minaccia terroristica e a forme sempre più insidiose di criminalità. La disciplina degli strumenti di *data retention* e accesso ai metadati, descritti nel primo paragrafo e oggetto di studio nel presente lavoro, non può quindi che tradursi in una seria e difficile sfida per legislatori e Corti, tanto nazionali quanto sovranazionali, resa ancor più complessa nell'ormai affermato contesto di «emergenza normalizzata»: il cronicizzarsi delle esigenze securitarie[73] venutosi a creare a seguito degli attentati alle Torri Gemelle ha infatti acuito la difficoltà del già complicato bilanciamento

[73] M. ROSENFELD, *Judicial balancing in times of stress: comparing diverse approaches to the war of terror*, Benjamin N. Cardozo School of Law Working Paper, 5, 2005, p. 2079. Flick, parla di «una sorta di cronicizzazione e di normalizzazione dell'emergenza, idonee a trasformare il ricorso a misure eccezionali – quali ad esempio, la limitazione o la sospensione dei diritti fondamentali – in una sorta di prevenzione senza fine, giustificata dal pericolo del terrorismo», G.M. FLICK, *Dei diritti e delle paure*, in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, ESI, Napoli, 2009; ma anche, tra i tanti: G. AGAMBEN, *Stato di eccezione,* Bollato-Boringhieri, Torino, 2003; P. BONETTI, *Terrorismo, emergenza e costituzioni democratiche,* Il Mulino, Bologna, 2006; T. GROPPI, *Democrazia e terrorismo,* ESI, Napoli, 2009; A. CARDONE, *La "normalizzazione" dell'emergenza*, Giappichelli, Torino, 2011; G. DE MINICO, *Costituzione. Emergenza e terrorismo*, Jovene, Napoli, 2016.

tra salvaguardia della sicurezza e garanzia dei diritti fondamentali[74]. In un simile scenario, il rischio che giudici e legislatori hanno dovuto e debbono ancora scongiurare è che l'obbiettivo della sicurezza «divenga l'esclusivo criterio di riferimento, finendo così con l'autorizzare ingerenze nella nostra sfera privata e con il trasformare le nostre organizzazioni sociali, il modo in cui ci rapportiamo con i pubblici poteri ma anche il modo in cui possiamo realmente godere delle nostre libertà»[75] e che, in altre parole, «il bene della sicurezza, a mo' di buco nero, finisca con l'attrarre a sé e fagocitare ogni altro bene costituzionalmente protetto»[76].

---

[74] G. DE VERGOTTINI, *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Il Mulino, Bologna, 2004; C. WALTER (a cura di), *Terrorism as challenge for national and international law: security versus liberty?*, Springer, Berlino, 2004; V. BALDINI, *Sicurezza e libertà nello Stato di diritto in trasformazione*, Giappichelli, Torino, 2004; A. VEDASCHI, *A' la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Giappichelli, Torino, 2007; E. POSNER, A. VERMEULEN, *Terror in balance: security, liberty and the Courts*, Oxford University Press, Cambridge, Massachusetts, 2007; AA.VV., *Convegno AIC, Libertà e sicurezza nelle democrazie contemporanee. Atti del Convegno annuale, Bari, 17-18 ottobre 2003: annuario 2003*, Cedam, Padova, 2008; M. CALVINO, M.G. LOSANO, C. TRIPODINA (a cura di), *Lotta al terrorismo e tutela dei diritti fondamentali*, Giappichelli, Torino, 2009; C. BASSU, *Terrorismo e costituzionalismo. Percorsi comparati*, Giappichelli, Torino, 2010; F. CLEMENTI, G. TIBERI, *Sicurezza interna, diritti e cooperazioni internazionale nella lotta al terrorismo*, in *Astrid-online.it*, 1, 2013; L. SCAFFARDI, *Nuove tecnologie, prevenzione del crimine e privacy, alla ricerca di un difficile bilanciamento*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli, Santarcangelo di Romagna, 2013, p. 245 ss.; M. BARBERIS, *Liberté, égalité, sécurité. Gli equivoci della guerra al terrore*, in *Il Mulino*, 4, 2016.

[75] S. RODOTÀ, *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012, p. 325.

[76] A. RUGGERI, *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)*, in *Consulta Online*, III, 2016. Del resto «le tradizionali libertà negative sono i primi diritti fondamentali dell'uomo a risultare potenzialmente compressi dall'inasprimento delle misure di sicurezza», M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi),* in *federalismi.it*, 23, 2016, p. 3. Come riassunto da Sartoretti, che riprende il pensiero di Foucault, «la ragione di fondo della accettazione ad essere sorvegliati è, nella modernità, la ricerca di sicurezza, che porta a rinunciare a porzioni di libertà in cambio di rassicurazioni sulla propria vita e il proprio benessere», C. SARTORETTI, *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web,* in *federalismi.it*, 13, 2019, p. 9.

Una deriva insidiosa, quella appena delineata, che si è del resto rivelata tutt'altro che meramente teorica: la concreta ed inquietante ampiezza e diffusione di strumenti di lotta alla criminalità e al terrorismo, fortemente invasivi della sfera privata [77], è emersa grazie alle rivelazioni del più noto *whistleblower* della storia moderna, Edward Snowden, che nel 2013 ha svelato l'esistenza di strumenti di sorveglianza massiva posti in essere dalla *National Security Agency* degli USA [78]. Questi sistemi, quali Prism e Upstream, fondati sulla raccolta, conservazione, analisi automatizzata e generalizzata ed accesso ai dati provenienti da telecomunicazioni dirette o uscenti dagli USA [79], hanno nuovamente posto all'attenzione del dibatti-

[77] «La percezione del concetto di sorveglianza, che ha avuto un picco negli ultimi vent'anni appoggiandosi alla giustificazione della lotta al terrorismo, non viene più considerata, in molti casi, quale evento eccezionale ma come fenomeno normale, quotidiano, che è rivolto alla massa, a tutte le persone e non a uno in particolare, sino a dar vita, come ricorda Rodotà, all'ombra del cosiddetto uomo di vetro», G. ZICCARDI, *Internet, controllo e libertà*, cit., p. 92.

[78] Questa autorità di intelligence, regolata dal *Patriot Act* del 2001, si occupa di attività di prevenzione e lotta alle minacce alla sicurezza nazionale provenienti dall'esterno, quindi al di fuori dei confini degli USA, diversamente invece dal *Federal Bureau of Investigation* (FBI) cui sono attribuiti compiti di *domestic surveillance*. Per approfondimenti, A. SERENA, *The leviathan, the chains, the lock: dynamics of power in the digital surveillance state*, in *MediaLaws. Law and Media Working Papers Series*, 8, 2017, p. 1 ss.

[79] In estrema sintesi e per quanto risulterà utile anche nelle analisi svolte nei successivi Capitoli, Snowden, ex dipendente di un *contractor* esterno fornitore di servizi per la NSA, oggi ancora ricercato dagli USA e accusato di spionaggio e furto di proprietà governative, ha rilasciato documenti classificati, pubblicati il 5 giugno 2013 dal giornale *The Guardian*, aventi ad oggetto *tools* di sorveglianza elettronica di massa delle comunicazioni riguardanti soggetti americani connessi ad un target esterno o soggetti unicamente stranieri; restano dunque escluse le comunicazioni *wholly domestic* ovvero svolte solo tra cittadini statunitensi entrambi presenti sul territorio degli USA al momento della raccolta dei dati. Il programma Upstream ha certamente destato maggiore preoccupazione e sgomento poiché consente alla NSA di effettuare intercettazioni dirette – riguardanti sia il contenuto che i metadati – delle telecomunicazioni veicolate mediante reti di telecomunicazione americane – la c.d. dorsale, ossia la rete di commutatori e cavi su cui "viaggiano" le comunicazioni sia telefoniche che telematiche –, senza che i *service providers* ne siano a conoscenza o offrano il loro attivo apporto. La NSA dunque accede a determinati dati di traffico ritenuti di interesse per le operazioni di *Foreign Intelligence*; successivamente, attraverso l'uso di marcatori (c.d. *selectors*), viene svolto un primo fil-

traggio delle comunicazioni da sottoporre a più approfondito vaglio. Il programma Prism, invece, è caratterizzato dall'accesso da parte dell'NSA ai dati conservati nelle banche dati dei fornitori di servizi telecomunicazioni (Google, Youtube, Facebook, Microsoft, Skype, etc.): questi ricevono specifici *selectors* dalla NSA (ad esempio riguardanti parole chiave, contenuti o soggetti specifici) e sono conseguentemente tenuti a garantire all'autorità pubblica l'accesso a tutti dati risultanti dall'analisi automatizzata svolta. Le informazioni così ottenute vengono poi trattenute per 5 anni in un database dell'NSA stessa e utilizzate mediante ricerche "targetizzate", cioè svolte attraverso l'introduzione di target e obiettivi specifici: ciò, tuttavia, si traduce nell'analisi di un numero estremamente ampio di dati correlati (le ricerche svolte possono infatti includere anche l'esame di comunicazioni di/con individui correlati ai target – c.d. *contact chaining method* –, ampliando così la cerchia di soggetti interessati dalle analisi). Questi programmi si fondano sulla normativa *Patriot Act* del 2001, sul FISA (*Foreign Intelligence Surveillance Act*) *Amendments Act* del 2008 e sul controllo di un tribunale segreto *ad hoc*, il Tribunale FISA, istituito nel 2006. In particolare, grande rilievo, come si vedrà più avanti, assume la Sezione 702 del FISA, in cui viene previsto il potere dell'*Attorney General* e del Direttore della *National Intelligence* di autorizzare la sorveglianza di soggetti specifici, ritenuti presumibilmente al di fuori dai confini degli USA, qualora ciò si riveli utile per scopi di *foreign intelligence*. Una volta avviate tali procedure, non è richiesto nessun ulteriore controllo da parte dei giudici, neppure per giustificare l'eventuale successivo ampliamento dei target stessi. La sezione 702 quindi è stata la base giuridica che ha consentito lo sviluppo dei programmi quali Prism e Upstream e per tale ragione è stata indicata come una delle disposizioni più controverse del FISA. Fondamentale per la realizzazione di sistemi di sorveglianza poi è l'ulteriore strumento dell'*Executive Order 12333* che autorizza la NSA a svolgere operazioni di *foreign intelligence* oltre i confini territoriali degli USA accedendo cioè direttamente ai cavi posti sotto l'Oceano Atlantico e attraverso i quali i dati vengono trasferiti negli USA; tali *Orders* saranno oggetto di alcune limitazioni normative introdotte proprio a seguito delle rivelazioni di Snowden, di cui si parlerà nel Capitolo 3 di questo lavoro. Sui programmi di sorveglianza di massa utilizzati dagli USA ed emersi in occasione del *datagate*, si rinvia a C. BOWDEN, *The US Surveillance programmes and their impact on EU citizens' fundamental rights. Note to the European Parliament*, 2013, p. 1 ss.; F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra una nuova grande guerra cibernetica e controllo globale*, in *Federalismi.it*, 13, 2013, p. 1 ss.; F. BIGNAMI, G. RESTA, *Transatlantic privacy regulation: conflict and cooperation*, in *Law and Contemporary Problems*, 4, 2015, p. 231 ss.; L.P. VANONI, *Il IV emendamento della Costituzione americana tra terrorismo internazionale e datagate: security v. privacy*, in *Federalismi.it*, 1, 2015, p. 1 ss.; A. BUTLER, F. HIDVEGI, *From Snowden to Schrems: how the surveillance debate has impacted US-EU relations and the future of international data protection*, in *Seton Hall Journal of Diplomacy and International Relations*, Special Issue 2015/2016, p. 1 ss.; S. MITSILEGAS, *Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime*, in *Columbia Human Rights Law Re-*

to legislativo e giurisprudenziale i rischi concreti ed attuali di una sistematica e incontrollata sorveglianza di dati e metadati e delle pericolose tensioni che dall'utilizzo di tali strumenti invasivi possono derivare. Così, se l'11 settembre 2001 è stato definito come il «momento che ha segnato un cambiamento radicale nella percezione del rapporto tra sicurezza e privacy» [80] a favore di una tendenza maggiormente pro-securitaria, il c.d. *datagate* provocato da Snowden ha invece contribuito all'affermarsi di una più solida consapevolezza della necessità di bilanciare l'impiego di sistemi di sorveglianza e accesso alle informazioni con una più attenta tutela dei diritti alla privacy e alla protezione dei dati, così fortemente colpiti dalla descritta tendenza pro-securitaria [81]. Una consapevolezza che, come si vedrà, ha generato forti ripercussioni negli Stati membri e nell'UE, portando ad un deciso attivismo da parte di ONG e cittadini dal quale sono poi derivate fondamentali pronunce giurisprudenziali – e correlate reazioni politiche e normative –. È in questo articolato contesto, caratterizzato da spinte differenti, che il dibattito sulla *data retention* deve dunque essere inserito: le considerazioni svolte sulle insidie e le potenzialità rappresentate da questo invasivo strumento di lotta alla criminalità e alle minacce alla sicurezza nazionale, nonché quelle sull'importanza dei diritti fondamentali in gioco, sino ad ora svolte, serviranno quali rilevanti coordinate di riferimento dalle quali prenderanno avvio gli studi che occuperanno il prosieguo del presente lavoro. I prossimi Capitoli e l'analisi delle evoluzioni giurisprudenziali e normative tanto a livello nazionale quanto sovranazionale in essi proposte, serviranno pertanto a tratteggiare una possibile risposta alla delicata sfida, qui delineata, della determinazione di un punto di equilibrio tra esigenze securitarie e diritti fondamentali. E la posta in gioco non è di poco conto: scongiurare il rischio di

---

view, 3, 2016, p. 1 ss.; R.A. MILLER, *Privacy and power: a transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, Cambridge, 2017.

[80] G. ZICCARDI, *Internet, controllo e libertà*, cit., p. 31.

[81] «The classical national security v. civil liberties debate was brought back to life by Snowden's disclosures and the resulting broader awareness of the global mass surveillance measures», A. DIMITROVA, M. BRKAN, *Balancing national security and data protection: the role of the EU and US policy-makers and Courts before and after NSA affair*, in *Journal of Common Market Studies*, 4, 2018, p. 764.

una società della sorveglianza e di una sproporzionata ingerenza e compressione della sfera privata in grado di minare la democrazia e le libertà fondamentali, per evitare di cedere sia alla tentazione di una garanzia della sicurezza a tutti i costi, sia al pericolo di divenire schiavi di un incontrollato e rapido progresso tecnico-scientifico [82].

[82] Per usare le parole di Soro, «se la tecnologia sconvolge l'antropologia, al diritto spetta ricomporne i frantumi, governare l'evoluzione perché l'uomo non ne sia sopraffatto», Intervento dell'allora Presidente del Garante all'incontro *Verso una nuova privacy?*, 6 ottobre 2017, disponibile all'indirizzo: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6937167.

CAPITOLO 2

LA LUNGA E ARTICOLATA *DATA RETENTION SAGA:* IL COMPLESSO DIALOGO TRA LEGISLATORE EUROPEO, CORTE DI GIUSTIZIA DELL'UE E CORTI NAZIONALI

SOMMARIO: 1. La disciplina normativa della *data retention* nell'Unione europea: dalla Direttiva *e-Privacy* alla *Data Retention Directive*. – 2. Gli Stati membri e la trasposizione della DRD, tra criticità attuative e rilevanti decisioni delle Corti nazionali: un primo dibattito interno. – 3. La storica pronuncia *Digital Rights Ireland*: la CGUE invalida la DRD. – 3.1. La significativa portata della sentenza *Digital Rights Ireland* e i primi dubbi interpretativi. – 4. Le reazioni degli Stati membri e delle Istituzioni europee all'intervento della CGUE: una situazione confusa. – 5. La CGUE chiamata nuovamente a pronunciarsi sulla conformità del regime di conservazione generalizzata rispetto alla Carta di Nizza: la sentenza *Tele2*. – 6. Una rinnovata frammentarietà di approcci all'indomani della pronuncia *Tele2*: le problematiche "interpretazioni difensive" adottate dagli Stati membri. – 7. L'art. 15 Direttiva *e-Privacy* sottoposto ancora una volta all'intervento chiarificatore della CGUE: la sentenza *Ministerio Fiscal* e i requisiti dell'accesso ai metadati conservati. – 8. Le importanti sentenze *La Quadrature du Net*, *Privacy International* e *H.K.*: la *data retention saga* al capolinea? – 8.1. La delicata determinazione dell'ambito di applicazione del diritto dell'UE. – 8.2. I limiti dello strumento di conservazione generalizzata e l'inedita distinzione tra sicurezza nazionale e sicurezza pubblica. – 8.3. Il difficile tentativo di sintesi di una "sconfitta vittoriosa". – 8.4. La sentenza *H.K. c. Prokuratuur* e le nuove importanti specificazioni sulla disciplina dell'accesso ai metadati. – 9. Prevedere l'imprevedibile: le profonde ed incerte conseguenze sul piano europeo e nazionale della più recente giurisprudenza della CGUE. – 9.1. L'impatto sui rinvii pregiudiziali ancora pendenti: un esito già scritto o un persistente bisogno di chiarezza? – 9.2. Verso il risveglio del legislatore europeo da tempo silente: i rischi e le sfide di un rinnovato intervento normativo sovranazionale. – 9.3. Le attese mosse di legislatori e Corti nazionali. Prime considerazioni a partire dalle sentenze della *Court constitutionnelle* belga e del *Conseil d'État* francese.

1. *La disciplina normativa della* data retention *nell'Unione europea: dalla Direttiva* e-Privacy *alla* Data Retention Directive.

La grande sensibilità ed interesse che sin dagli ultimi decenni dello scorso secolo erano stati riservati, a livello comunitario, alla tutela della *privacy* e della protezione dei dati, trovavano una chiara concretizzazione nella Direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (c.d. Direttiva *e-Privacy*). In questa normativa, oggi ancora vigente – sebbene, come si dirà, sottoposta ad un lungo e travagliato procedimento di modifica –, si collocavano alcune importanti disposizioni riguardanti la disciplina della *data retention*: cogliendo le potenzialità ma anche i pericoli che le nuove tecnologie e i servizi di comunicazione elettronica comportavano, il legislatore europeo stabiliva quale regola generale il divieto di memorizzazione di dati e metadati prodotti dai servizi di telecomunicazione (art. 5). L'art. 6 della Direttiva *e-Privacy* imponeva di conseguenza l'obbligo in capo ai *service providers* di cancellare o rendere anonimi tutti i dati sul traffico relativi ai propri abbonati ed utenti, non appena tali informazioni si fossero rivelate non più necessarie ai fini di trasmissione della comunicazione stessa o di fatturazione e pagamenti – si parla in questo caso di memorizzazione tecnica –.

Se le richiamate disposizioni risultavano ispirate dall'obiettivo di una solida tutela della riservatezza e della protezione dei dati, la Direttiva in esame non mancava però di prevedere anche una disciplina eccezionale: l'art. 15, co. 1 della Direttiva 2002/58/CE, infatti, attribuiva agli Stati membri la facoltà di adottare normative volte a limitare i diritti e gli obblighi dell'art. 6, «qualora tale restrizione costituisca, ai sensi dell'art. 13, co. 1 della Direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri *possono* tra l'altro *adottare misure legislative che prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo*». Il dettato normativo dell'art. 15 lasciava così agli Stati membri una vasta autonomia quanto

alla determinazione degli obblighi di conservazione, in assenza di specifiche e rigide condizioni e limitazioni – neppure temporali – volte a circoscrivere la disciplina derogatoria della *data retention*: in tal modo, ciò che traspare è l'accettazione da parte del legislatore europeo del 2002 di un certo stemperamento della *data protection* a favore dell'impiego di forme di *data surveillance* generalizzata per scopi securitari [1].

Dinnanzi alla sempre più concreta minaccia terroristica, non stupisce dunque il rapido avvicendarsi di normative nazionali che, basandosi proprio sulla disposizione derogatoria sopra descritta, imponevano in capo ai gestori di servizi di telecomunicazione un obbligo di conservazione dei metadati e regolavano la successiva possibilità di accesso da parte delle autorità di *law enforcement* [2]. Tali leggi, però, potevano essere anche molto differenti da Stato a Stato, causando difficoltà applicative di non poco conto, oltre a notevoli costi in capo agli attori privati operanti nel settore delle telecomunicazioni: quello che si era dunque venuto a creare era un panorama normativo estremamente frammentario [3] che, a causa dell'ampia discrezionalità lasciata ai legislatori nazionali dal vago dettato normativo dell'art. 15 Direttiva *e-Privacy*, sollevava significative problematiche politiche, economiche e giuridiche.

Dinnanzi a questa complessa situazione, si veniva così ad imporre con forza nel dibattito sovranazionale la necessità di un intervento legislativo comunitario volto a predisporre una normativa armonizzata *ad hoc* in materia di conservazione dei dati derivanti dalle telecomunicazioni elettroniche, in grado sia di incrementare l'efficacia di tale strumento [4], sia di

---

[1] In questi termini, si legga E. SPILLER, *La sentenza Tele2 Sverige: verso una* digital rule of law *europea?*, in *IANUS*, 15, 2017, p. 283.

[2] Si pensi al *Criminal Justice Terrorist Offenses Act* n. 64 del 2005, adottato in Irlanda, che imponeva ai *service providers* la conservazione, per un periodo di tre anni, di tutti i metadati derivanti da comunicazioni elettroniche; o ancora, in Italia, al d.lgs. n. 196/2003 che fissava, all'art. 132, un obbligo di conservazione generalizzata della durata di trenta mesi.

[3] Sul punto si legga la ricostruzione del frastagliato quadro di soluzioni normative nazionali in materia di *data retention* riportato nell'*Extended Impact Assessment* elaborato il 21 settembre 2005 dalla Commissione europea e relativo alla proposta di Direttiva in materia di *data retention* (SEC(2005)1131), di cui si parlerà a breve.

[4] Nella Comunicazione *Migliorare l'accesso all'informazione da parte delle autorità incaricate del mantenimento dell'ordine pubblico e del rispetto della legge* (COM(2004)429def), 16 giu-

superare quella disomogeneità di regole che impattava seriamente sul funzionamento del mercato unico interno e sulla libera circolazione di merci e servizi. L'urgenza di una simile disciplina, acuita dai drammatici attacchi che avevano colpito Madrid e Londra negli anni 2004 e 2005, facendo (ri)affiorare l'esigenza di un intervento comune europeo in materia di lotta al terrorismo [5], trovava risposta nella *Direttiva 2006/24/CE riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la Direttiva 2002/58/CE* (c.d. *Data Retention Directive*, d'ora in avanti DRD), datata 15 marzo 2006 [6]. Nonostante i dubbi e i timori espressi da più parti quanto alla compatibi-

gno 2004, la Commissione affermava che la maggiore interazione tra Stati membri nella lotta al terrorismo poteva essere raggiunta anche mediante la predisposizione di misure volte a garantire la raccolta, conservazione e disponibilità di dati e metadati. Anche il Consiglio dell'UE, nella *Dichiarazione sulla lotta al terrorismo* del 25 marzo 2004, attribuiva peso prioritario all'adozione di un quadro normativo comunitario in materia di *data retention*.

[5] Per una accurata ricostruzione dell'impatto degli attentati terroristici sulle politiche europee in materia securitaria, si legga F. BIGNAMI, *Privacy and law enforcement in the European Union: the Data Retention Directive*, in *Chicago Journal of International Law*, 1, 2007, p. 233 ss.; ma anche T. KONSTADINIDES, *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, in *European Current Law Issue*, 1, 2012, p. I ss.

[6] La proposta di adozione di una direttiva in materia giungeva a seguito del naufragato tentativo di approvazione di una Decisione Quadro regolante la *data retention*, promossa da Francia, Irlanda, Svezia e Regno Unito nell'aprile 2004. L'idea sottesa a tale Decisione era quella di imporre agli Stati membri l'adozione di normative interne volte ad introdurre l'obbligo in capo ai *service providers* di conservazione di tutti i metadati relativi alle comunicazioni svolte dai propri utenti. Questa spinta verso l'armonizzazione aveva però incontrato dubbi tanto sotto il profilo della base giuridica scelta – il Terzo Pilastro –, quanto sotto quello sostanziale con riguardo alla proporzionalità e necessità della *data retention* generalizzata e della sua compatibilità con l'art. 8 della Convenzione EDU e con il principio di presunzione di non colpevolezza, come sottolineato anche dal relatore della Commissione per la libertà pubbliche, giustizia e affari interni del Parlamento europeo. Per una analisi dei profili problematici che hanno portato all'insuccesso di tale proposta di Decisione Quadro, si rimanda a S. SAXBY, *European Parliament says 'No!' to Member States'data retention proposal*, in *Computer Law & Security Report*, 21, 2005, p. 279 ss.; E. KOSTA, P. VALCKE, *Retaining the data retention directive*, in *Computer Law & Security Report*, 22, 2006, p. 370 ss.

lità di un obbligo di conservazione generalizzata (c.d. *bulk* o *blanket data retention*) con i diritti sanciti agli artt. 52, 7 e 8 della Carta di Nizza[7], l'adozione della DRD segnava senza dubbio un «vero e proprio *revirement* securitario, passando da una politica volta ad incoraggiare la *data protection* (segnatamente con le dir. 95/46 e 2002/58) alla graduale legittimazione della *data retention*»[8].

Riconoscendo dunque «l'importanza dei dati relativi al traffico e dei dati relativi all'ubicazione per l'indagine, l'accertamento e il perseguimento dei reati, come dimostrato da lavori di ricerca e dall'esperienza

---

[7] Il Garante Europeo della Protezione dei Dati (GEPD) – nominato dal Parlamento europeo e dal Consiglio, ha il compito di promuovere la cooperazione tra le autorità competenti in materia di protezione dei dati nell'UE e di fornire indicazioni e pareri sulla corretta e coerente applicazioni delle norme sulla *data protection* – nonché il Gruppo di Lavoro Art. 29 – un organo indipendente istituito sulla base dell'art. 29 della Direttiva 95/46/CE, al quale era attribuita la funzione di controllo e analisi di questioni connesse alla protezione della vita privata e alla tutela dei dati personali, poi sostituito dal Comitato europeo per la protezione dei dati (CEPD) a seguito dell'entrata in vigore del GDPR – avevano espresso forti perplessità quanto alla proporzionalità della *data retention* (si legga ad esempio il documento redatto dal GEPD *Parere sulla proposta di Direttiva relative alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazion elettronica pubblici e recande modifica della Dir. 2002/58/CE*, 26 settembre 2005); 80 *service providers* e 90 ONG, tra cui Privacy International e Digital Rights Ireland, che troveremo qualche anno dopo protagoniste degli interventi giurisprudenziali promossi a livello nazionale ed approdati poi dinnanzi alla CGUE, avevano scritto un accorato appello al Parlamento europeo affinché quest'ultimo respingesse la direttiva proposta, sottolineando come «The European Parliament now faces a crucial decision. Is this the type of society we would like to live in? A society where all our actions are recorded, all of our interactions may be mapped, treating the use of communications infrastructures as criminal activity; just in case that it may be of use at some point in the future by countless agencies in innumerable countries around the world with minimal oversight and even weaker safeguards», come riportato da C. JONES, B. HAYES, *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, in *Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness – Paper*, 2013, p. 1 ss.

[8] E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, cit., p. 283. Anche Vedaschi e Lubello mettevano in luce come la DRD avesse segnato una «transition from a fundamental concern with protection to the pragmatic desire for retention», A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy*, in *Tilburg Law Review*, 20, 2015, p. 19.

pratica di diversi Stati membri» [9], a scapito della – ritenuta – meno efficace soluzione della *data preservation* [10], la disciplina europea sanciva l'onere in capo agli Stati membri – anche quelli che non avevano ancora adottato nessuna normativa specifica in materia di *data rentention* sulla base dell'art. 15 della Direttiva *e-Privacy* – di «adottare misure per garantire che i dati [relativi al traffico, all'ubicazione e quelli necessari per identificare l'abbonato o l'utente], qualora generati o trattati nel quadro della fornitura dei servizi di comunicazione interessati (…), siano conservati conformemente alle disposizioni della presente direttiva» (art. 3, co. 1), allo scopo di assicurarne la disponibilità a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale (art. 1, co. 1). Non veniva quindi prevista una delimitazione dei soggetti i cui metadati dovevano essere sottoposti a conservazione [11], così che la memorizzazione imposta ai fornitori di servizi di telecomunicazione doveva riguardare tutti gli utenti e tutte le comunicazioni elettroniche aventi luogo nel territorio europeo, coinvolgenti cittadini europei o non, senza che dovesse sussistere alcun collegamento tra *data retention* e indagini in corso e senza richiedere un legittimo sospetto o un previo ordine da parte di un giudice. La conservazione doveva riguardare unicamente i metadati espressamente indicati all'art.

[9] Considerando 11, Direttiva 2006/24/CE.

[10] La *data preservation* consente alle autorità di *law enforcement* di richiedere agli operatori privati la conservazione dei soli metadati relativi a determinate persone; meno invasiva della *data retention* generalizzata, la *data preservation* risulta però efficace solo per il futuro, non consentendo un'indagine del passato ovvero riguardante i metadati prodotti quando ancora non vi era alcun sospetto nei confronti di un soggetto; in altre parole, come affermato dalla Commissione nell'*Impact assessment* predisposto con riferimento alla Direttiva in esame, «data preservation is only useful as of the moment when suspects have been identified; data retention is indispensable in many cases to actually identify suspects», p. 5.

[11] In altre parole, «cette conservation se fait, a priori, pour l'ensamble des citoyens sans distinction d'aucune sorte. Ni entre ceux qui font l'object d'enquetes judiciaires et ceux qui n'en font pas l'objet, ni entre ceux qui sont tenus d'un secret professionnel et ceux qui ne sont pas tenus d'une telle obligation», A. CASSART, J-F. HENROTTE, *L'invalidation de la directive 2006/24 sur la conservation des données de communication èlectronique ou la chronique d'une mort annoncée*, in *Jurisprudence de Liege, Mons et Bruxelles*, 20, 2014, p. 955.

5[12], mentre risultavano in ogni caso esclusi i dati relativi al contenuto delle comunicazioni; la *data retention* poi poteva avere una durata stabilita dai legislatori nazionali entro una forbice temporale, individuata dalla DRD stessa, tra i sei mesi e i due anni[13]. Era infine lasciata ampia discrezionalità ad ogni Stato membro quanto alla definizione delle «procedure da seguire e le condizioni da rispettare per aver accesso ai dati conservati, in conformità dei criteri di necessità e di proporzionalità», «con riserva delle disposizioni in materia del diritto dell'Unione europea o del diritto pubblico internazionale e in particolare della CEDU, secondo l'interpretazione della Corte europea dei diritti dell'uomo» (art. 4).

L'assenza di definizione precisa quanto al concetto di "reati gravi", la mancata indicazione delle autorità nazionali deputate all'accesso ai metadati – non essendo peraltro prevista alcuna limitazione alle sole autorità

[12] Essi riguardavano sostanzialmente le informazioni volte a rintracciare la fonte di una comunicazione (numero telefonico o identificativo dell'utente di un servizio Internet o di posta elettronica), la destinazione di una comunicazione (ad esempio il numero del destinatario di una telefonata), la data, ora e durata della comunicazione (telefonata o accesso Internet), il tipo di comunicazione e l'attrezzatura utilizzata (comprensiva di codice IMEI cioè identificativo del cellulare impiegato dal chiamante), nonché i dati determinanti l'ubicazione delle apparecchiature di comunicazione mobile. Per una completa e dettagliata analisi dei diversi metadati oggetto di conservazione ai sensi della DRD, si rimanda a L. FEILER, *The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection*, in *European Journal of Law and Technology*, 3, 2010, p. 1 ss.

[13] Con riferimento a tale scelta temporale, il GEPD non riteneva i dati presentati a sostegno di questa decisione come sufficienti a dimostrare la necessità di una conservazione di durata superiore ad un anno (GEPD, *Parere sulla proposta di Direttiva relativa alla conservazione dei dati trattati in relazione alla fornitura di servizi di comunicazione elettronica pubblici e recante modifica della Direttiva 2002/58/CE*, cit., para. 17). È interessante rimarcare come su questo punto il dibattito tra le stesse Istituzioni europee fosse stato ampio: mentre la Commissione aveva inizialmente proposto un termine fisso di dodici mesi di conservazione, ridotto a sei mesi per i dati legati all'uso di Internet, il Parlamento europeo aveva richiesto invece la restrizione di tale periodo a tre mesi, con una possibile estensione massima di sei mesi. Il Consiglio propendeva invece per l'opzione di una forbice temporale che lasciasse maggiore discrezionalità agli Stati membri, similmente a quanto era stato proposto nella bozza di Decisione Quadro sopra richiamata, che prevedeva però un intervallo temporale ben più esteso, da uno a tre anni.

di *law enforcement*[14] –, la carenza di specifiche condizioni sul fronte della *data security*, nonché la mancata restrizione dell'obbligo di conservazione unicamente al territorio europeo, insieme al silenzio quanto alle condizioni di accesso da parte delle autorità preposte[15], erano solo alcuni dei molteplici profili critici che avevano destato sin da subito non poche preoccupazioni circa l'impatto di tale disciplina sui diritti fondamentali e alla proporzionalità delle misure disposte[16]. La discrezionalità ampia lasciata agli Stati membri quanto alla determinazione della durata della conservazione o alla possibilità di rimborsare ai *service providers* i costi sostenuti per la conservazione imposta, rischiavano inoltre di condurre nuovamente a differenze anche significative tra le diverse discipline statuali di trasposizione, con la conseguenza di impedire il raggiungimento

[14] La mancata specificazione di cosa dovesse intendersi per "reato grave" e di quali elementi fossero tali da determinare il carattere di gravità apriva al rischio che tale importante requisito venisse interpretato in maniera eccessivamente estensiva da parte degli Stati membri: ne è chiara esemplificazione il fatto che nelle normative nazionali di attuazione della DRD ben 14 dei 28 Stati membri avessero incluso nella definizione di "autorità competenti" anche i servizi di intelligence nazionali, come riportato dallo studio di C. JONES, B. HAYES, *The EU Data Retention Directive*, cit.

[15] Il GEPD aveva posto in evidenza, nel già richiamato parere, come la delicata regolamentazione dell'accesso non dovesse essere totalmente lasciata alla determinazione discrezionale degli Stati membri, criticando così le vaghe ed ampie disposizioni stabilite nella DRD, che proponeva solo un generico riferimento ai principi di necessità e proporzionalità, senza richiedere specifiche garanzie quali la previa autorizzazione di un'autorità giudiziaria.

[16] Altro profilo problematico che poco convinceva il GEPD era da rinvenirsi nella necessità ed efficacia dello strumento della *data retention* stessa: «in his opinion on the Commission proposal of 2005, the EDPS (European Data Protection Supervisor) said that he was not convinced by the assumption of its necessity and called for further evidence. In the opinion published in May 2011 on the Commission evaluation report, the EDPS concluded that on the basis of the available quantitative findings it remained doubtful whether the European Commission could conclude that data retention was considered necessary for law enforcement by most member states and there is still a problematic lack of evidence substantiating its value», E. GUILD, S. CARRERA, *The political and judicial life of metadata: Digital Rights Ireland and the trial of the Data Retention Directive*, CEPS Paper in Liberty and Security in Europe, 65, 2014, p. 7. Sul punto si legga anche M. TAYLOR, *The EU Data Retention Directive*, in *Computer Law & Security Report*, 22, 2006, p. 309 ss.

di quella armonizzazione che era stata posta quale obiettivo della DRD stessa, volta ad eliminare gli ostacoli al corretto funzionamento del mercato interno e le possibili distorsioni concorrenziali derivanti dalla presenza di legislazioni fortemente disomogenee.

2. *Gli Stati membri e la trasposizione della DRD, tra criticità attuative e rilevanti decisioni delle Corti nazionali: un primo dibattito interno.*

L'obbligo posto in capo agli Stati membri di trasporre nel proprio ordinamento interno quanto previsto dalla Direttiva 2006/24/CE entro il 15 settembre 2007 [17], era stato accolto, sin dall'inizio, da accese discussioni a livello nazionale: in taluni contesti, infatti, il complesso dibattito parlamentare sorto in materia giungeva a sollevare significativi dubbi quanto alla legittimità costituzionale di un regime di conservazione generalizzata. Tali interrogativi, che non mancavano di essere rilevati anche dalla stessa società civile e da ONG attive nell'ambito della tutela dei diritti fondamentali, erano sfociati in importanti interventi dei giudici nazionali: ci si riferisce alle sentenze della *Varhoven administrativen sad* (Corte suprema amministrativa bulgara) del 11 dicembre 2008, della *Curtea Constituțională a României* (Corte costituzionale romena) del 8 ottobre 2009 [18], del *Bundesverfassungsgerich* (Tribunale costituzionale federale tedesco) del 2 marzo 2010 [19], della *Ústavní soud České republiky*

[17] È bene sottolineare come, con riferimento alla sola disciplina della conservazione di dati derivanti dall'utilizzo di Internet, la DRD offrisse la possibilità, accolta da 16 Stati membri, di posporre il termine di trasposizione nell'ordinamento nazionale al 15 marzo 2009.

[18] Corte cost. romena, 8 ottobre 2009, n. 1258. Per la presente analisi è stata impiegata una traduzione inglese della sentenza disponibile all'indirizzo http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention. pdf. Si è inoltre fatto ampiamente riferimento all'approfondita analisi svolta da C.C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, in *Common Market Law Review*, 3, 2010, p. 933 ss.

[19] BVerfG, *Vorratsdatenspeicherung*, BvR 256/08, 2 marzo 2010. Lo studio di tale pronuncia è basato sulla traduzione ed analisi di A. DI MARTINO, *Bundesverfassungsgeri-*

(Corte costituzionale della Repubblica Ceca) del 1 febbraio 2011, nonché della *Ανώτατο Δικαστήριο της Κυπριακής Δημοκρατίας* (Corte suprema cipriota) del 22 marzo 2011. Nonostante in tutti questi casi l'analisi della questione fosse unicamente incentrata sulle disposizioni interne attuative della DRD, senza così giungere alla promozione di rinvii pregiudiziali aventi direttamente ad oggetto l'interpretazione della fonte normativa europea, gli interventi delle Corti nazionali risultano nondimeno ricchi di rilevanti considerazioni anticipatrici del futuro intervento della CGUE e rappresentative, seppure in forma ancora embrionale, di quelle difficoltà attuative e di quel complesso bilanciamento tra diritti fondamentali ed esigenze securitarie che caratterizzano ancora oggi il dibattito sulla *data retention*.

In particolare, gli interventi della Corte romena e del Tribunale tedesco si rivelano esemplificativi di due diversi approcci, sotto taluni profili addirittura divergenti, avverso la materia della conservazione dei metadati, prefigurando già una diversità di reazioni e scelte a livello nazionale poi acuitesi nel corso del tempo. La Corte costituzionale romena [20], infatti, facendo ampio e continuo riferimento alla giurisprudenza dei giudici

---

cht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza, in *Giurisprudenza costituzionale*, 5, 2010, p. 4059 ss. Per un approfondimento sulle ulteriori decisioni nazionali richiamate, nonché per un ampio studio delle normative di recepimento della DRD, si rimanda a: T. KONSTADINIDES, *Destroying democracy on the ground of defending it?*, cit.; E. KOSTA, *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, in *SCRIPTed*, 3, 2013, p. 339 ss.; J. DURICA, *Directive on the retention of data on electronic communication in the rulings of the Constitutional Courts of EU Member States and efforts for its renewed implementation*, in *The Lawyer Quarterly*, 2, 2013, p. 143 ss.; L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, in *German Law Journal*, 6, 2015, p. 1727 ss.; L. CURICCIATI, *Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della Data Retention Directive*, in *Democrazia e Sicurezza*, 2, 2017, p. 89 ss.

[20] Il caso giunto dinnanzi alla Corte costituzionale trovava origine nel ricorso promosso dalla ONG romena *Civil Society Commissariat* dinnanzi al Tribunale di Bucharest, nel quale veniva citato in causa un operatore di telecomunicazione che, sulla base della normativa romena in materia di *data retention*, conservava i metadati relativi alle comunicazioni degli attivisti della ONG.

di Strasburgo [21], aveva dichiarato l'illegittimità costituzionale della legge n. 298/2008 di trasposizione della DRD non solo perché eccessivamente vaga quanto alle finalità di conservazione e accesso ai dati (genericamente indicate con il termine «minacce alla sicurezza nazionale») e carente sotto il profilo delle salvaguardie poste in essere, ma anche sulla base di una decisa dichiarazione di incompatibilità con il diritto alla riservatezza – tutelato dall'art. 26 della Costituzione romena e dall'art. 8 Convenzione EDU – di forme di conservazione generalizzata, obbligatoria e permanente [22]. Diviene chiaro dunque come la posizione della Corte costituzionale romena, pur senza mai – piuttosto sorprendentemente – citare la DRD, si fosse concretizzata in una forte critica dello strumento di conservazione generalizzata *per se* considerato nonché della sua necessità e proporzionalità in una società democratica: così facendo, i giudici ponevano il Parlamento nella difficile condizione di non poter approvare una normativa nazionale che prevedesse forme di *bulk data retention* [23].

---

[21] In particolare, veniva ampiamente richiamata la sentenza Corte EDU 6 settembre 1978, ricorso n. 5029/71, *Klass v. Germania*. Per una ricostruzione della casistica e della posizione della Corte EDU in materia di sorveglianza massiva, si rimanda a: S. O'LEARY, *Balancing rights in a digital age*, in *Irish Jurist*, 59, 2018, p. 82 ss.; V. RUSINOVA, *A European perspective on privacy and mass surveillance at the crossroad*, Working Papers HSE, 2019; sia consentito il rimando a G. FORMICI, *La* digital mass surveillance *al vaglio della Corte Europea dei Diritti dell'Uomo: da* Zakharov *a* Big Brother Watch, in *Federalismi.it – Focus Human Rights*, 23, 2020, p. 44 ss.

[22] Come affermato da Murphy nella sua accurata analisi, «the Court held that the data retention legislation reverses the presumption that the rights to privacy and free expression are only subject to limited interference as all electronic communication is targeted for surveillance. (…) By applying the data retention to all electronic communications users, the rights in question – to privacy and freedom of expression – become theoretical and illusory and the legislation may overturn the presumption of innocence», C.C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, cit., p. 936. Sul punto, si legga anche C. JONES, B. HAYES, *The EU Data Retention Directive*, cit., p. 22 ss.

[23] Come acutamente osservato da Murphy, neppure una modifica della Costituzione nazionale avrebbe potuto rendere l'attuazione di forme di conservazione generalizzata compatibile alla garanzia dei diritti fondamentali: «given that the Romanian Constitutional Court invokes the ECHR in addition to the domestic Constitution, an amendm-

Anche il Tribunale federale tedesco si era pronunciato sulla normativa nazionale in materia di conservazione dei dati [24], ritenendo le disposizioni in essa contenute non conformi all'art. 10, co. 1 della *Grundgesetz* (GG) posto a tutela dei diritti alla riservatezza e alla segretezza delle comunicazioni. Diversamente dai colleghi romeni, tuttavia, ciò che in questo caso veniva considerato contrastante rispetto alla legge fondamentale era il mancato rispetto del principio di proporzionalità riscontrato in diversi punti della normativa nazionale, nelle parti in cui, ad esempio, non risultavano disposte adeguate garanzie avverso l'ingerenza nella sfera privata, soprattutto nella fase di accesso ai dati raccolti [25]. I giudici di Karlsruhe, dunque, pur evidenziando che regimi di *data retention* generalizzata po-

---

ent to the latter may not suffice to protect any implementing law», C.C. MURPHY, *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, cit., p. 940.

[24] Il caso era stato promosso dalla ONG *Working Group on Data Retention*, sostenuta poi da ben 34.000 cittadini: tale vasto numero evidenzia senza dubbio l'attenzione sempre maggiore mostrata dalla società civile rispetto a temi complessi e delicati quali la tutela della riservatezza dinnanzi all'ingerenza delle autorità pubbliche. Per chiarezza, è utile rilevare come questo vasto attivismo e partecipazione fosse stato certamente incentivato, a livello procedurale, dalla previsione, contenuta nella *Grundgesetz* all'articolo 93(4a), dello strumento del *Verfassungsbeschwerde*, ovvero del ricorso diretto individuale dinnanzi al Tribunale costituzionale federale, per finalità di tutela dei diritti fondamentali.

[25] Veniva infatti criticato il periodo di memorizzazione che, per considerarsi necessario e proporzionato, avrebbe dovuto prevedere una durata massima di 6 mesi; ma anche l'assenza di idonee tutele nella fase di accesso ai dati, che avrebbero dovuto restringere tale ingerenza solo in presenza di un sospetto di reato grave o di un pericolo concreto per la vita o per la sicurezza; a ciò si aggiungevano la mancanza di un obbligo di notificazione o informazione al soggetto interessato nonché la carenza di solide salvaguardie tecnico-informatiche sulla sicurezza dei dati. Per un ampio studio di tale pronuncia si rimanda a: C. DE SIMONE, *Pitting Karlsruhe against Luxembourg? German data protection and the contested implementation of the EU Data Retention Directive*, in *German Law Journal*, 11, 2010, p. 291 ss.; K. DE VRIES, R. BELLANOVA, P. DE HERT, S. GUTWIRTH, *The German Constitutional Court judgement on data retention: proportionality overrides unlimited surveillance (doesn't it?)*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, R. LEENS (a cura di), *Computers, privacy and data protection: an element of choice*, Springer, Berlino, 2011, p. 3 ss.; D. WESTPHAL, *German federal constitutional Court delivers roadmap for national data retention laws – without transferral to ECJ*, in *Vienna Journal on International Constitutional Law*, 5, 2011, p. 222 ss.

tevano «ingenerare un sentimento diffuso e minaccioso dell'essere osservati, che può pregiudicare in molti settori un libero esercizio dei diritti fondamentali» (para. 212), non giungevano a ritenere la conservazione in blocco e generalizzata per sua natura in contrasto con l'art. 10 GG [26]. Così, usando le parole di Konstadinides, mentre il Tribunale tedesco adottava una decisione «simply related to the extent of state discretion implied in the implementation of the Directive», comportando così una sospensione dell'efficacia della normativa interna in attesa di appropriati emendamenti stabiliti dal Parlamento nazionale, la Corte romena «rejected altogether the obligation of data rentention. Thus, the Romanian Constitutional Court's attack was not limited to the relevant implementation process but to the Europeanisation of the system of data retention» [27].

Andando oltre queste pur rilevanti diversità, il comune denominatore della prima ricca giurisprudenza nazionale in materia di conservazione dei metadati per scopi securitari, qui brevemente delineata, è certamente da individuarsi in un ampio riconoscimento dell'importanza dei diritti alla *privacy* e alla protezione dei dati, che non potevano essere considerati sempre remissivi dinnanzi al pur legittimo compito dello Stato di garantire la sicurezza [28]. Le difficoltà attuative riscontrate dagli Stati membri,

---

[26] Come ben evidenziato da Flor, per i giudici costituzionali tedeschi la «verifica di legittimità costituzionale riguarda non le disposizioni della Direttiva europea, ma le soluzioni legislative adottate dal legislatore tedesco per raggiungere gli scopi prefissati dall'Unione. La questione della prevalenza del diritto comunitario e della sua eventuale incidenza sui diritti fondamentali non è stata, dunque, posta in discussione o, almeno, non direttamente», R. FLOR, *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constitutionala*, in *Cassazione Penale*, 5, 2011, p. 1953.

[27] T. KONSTADINIDES, *Destroying democracy on the ground of defending it?*, cit., p. XX.

[28] «Nel susseguirsi di pronunce [dei giudici nazionali] la complessa natura della disciplina era stata dunque messa in forte discussione. Si è avvertita così l'esigenza di ridefinire i valori in gioco, non limitandosi a considerare i meri interessi economici della prima ora, ma estendendo l'analisi anche ai profili fino a quel momento trascurati, in primis la tutela dei diritti», E. SPILLER, *La sentenza Tele2 Sverige: verso una digital rule of law europea?*, cit.

pertanto, non solo riflettevano e confermavano i dubbi e timori già espressi in fase di approvazione della DRD, ma mettevano anche sempre più in luce l'esigenza di un intervento della CGUE capace di andare alla "fonte" delle criticità rilevate e dunque alla Direttiva stessa. Così, non si può che concordare con l'affermazione di Jones e Hayes, risalente al 2013, secondo cui già a pochi anni dalla sua entrata in vigore, «the DRD ranks among the most controversial pieces of counter-terrorism legislation the EU has ever adopted and fierce debate as to its legitimacy and effectiveness has raged since the earliest stages of its drafting to the present day» [29].

3. *La storica pronuncia* Digital Rights Ireland*: la CGUE invalida la DRD.*

Le criticità sottolineate sin dalla adozione della DRD nonché il dibattito dottrinario [30] ma anche normativo e giurisprudenziale successivamen-

---

[29] Così C. JONES, B. HAYES, *The EU Data Retention Directive*, cit., p. 10. Similmente e con efficacia di immagini, Markou: «by imposing an obligation to retain data but excluding from its scope the issue of access to it – a closely inter-related step capable of affecting the privacy related acceptability of data retention –, the [Data Retention] Directive has placed a bomb in the privacy of European citizens and has allowed the Member States alone to take measures to prevent it from exploding. Several Member States did not do well on this task and the bomb has exploded as has the negativity surrounding the particular measure», C. MARKOU, *The Cyprus and other EU Courts rulings on data retention: the Directive as a privacy bomb*, in *Computer Law & Security Review*, 28, 2012, p. 475.

[30] Anche la dottrina, infatti, non aveva mancato di interrogarsi sulla validità della DRD e sulla sua conformità rispetto alla Carta di Nizza. Gran parte degli studiosi rispondeva negativamente a tale questione, ritenendo sproporzionata l'interferenza nella sfera privata provocata da una conservazione generalizzata, considerando eccessiva la durata della *data retention* nel suo massimo di due anni nonché criticando la carenza di misure adeguate ed efficaci contro il rischio di abusi da parte di autorità pubbliche o soggetti terzi. Di questa opinione, ad esempio, L. FEILER, *The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection*, cit. Merita, per completezza, rilevare come alcuni autori, tra cui F. BIGNAMI, *Protecting privacy against the Police in the European Union: the Data Retention Directive,* in AA. VV., *Me-*

te sviluppatosi a livello nazionale, avevano reso ben presto chiara la necessità di un intervento della CGUE [31]. Non deve stupire quindi che la delicatezza e complessità della disciplina della conservazione dei dati abbiano portato i giudici di Lussemburgo a pronunciarsi numerose volte, a partire dal 2009, in materia di *data retention*, due delle quali aventi ad oggetto la Direttiva 2006/24/CE. Mentre la prima di tali decisioni verteva su una questione prettamente formale, riguardando la correttezza della base giuridica della DRD [32], quanto in questa sede assume fondamentale rilievo è

---

langes en l'honneur de Philippe Léger, Editions Pedone, Parigi, 2006, p. 109 ss., avessero invece espresso una opinione differente, ritenendo nel complesso la DRD conforme alla Carta di Nizza, grazie alle limitazioni e condizioni presenti nella normativa.

[31] La situazione, del resto, risulta ancor più caotica e problematica se si osserva la posizione all'epoca tenuta dalla Commissione europea: quest'ultima, all'indomani – e nonostante – delle pronunce delle Corti nazionali, aveva deciso di avviare numerose procedure di infrazione a carico di quegli Stati membri, quali Grecia, Irlanda, Olanda, Svezia, Austria e Germania, che avevano mancato di trasporre la DRD nell'ordinamento nazionale entro i termini imposti. A nulla erano valse le motivazioni espresse da taluni Governi nazionali, quali quello svedese ed austriaco, il cui ritardo nella predisposizione della disciplina nazionale era stato addotto proprio ai dubbi circa la compatibilità della *data retention* generalizzata disposta dalla DRD rispetto ai diritti fondamentali sanciti nella Carta di Nizza, nella Convenzione EDU o nell'ordinamento nazionale. Considerando la delicatezza delle questioni poste e il profondo dibattito sorto a livello nazionale, alcuni autori avevano denunciato come «hazardous for the Commission to rule with an iron fist by forcing Member States to adopt data retention legislation that is incompatible with their Constitutions», T. KONSTADINIDES, *Destroying democracy on the ground of defending it?*, cit., p. 733.

[32] Si fa riferimento alla pronuncia CGUE 25 febbraio 2009, C-301/06, *Irlanda c. Parlamento europeo e Consiglio*, promossa mediante ricorso di annullamento *ex* art. 230, co. 2, TCE dal Governo irlandese che riteneva erronea la base giuridica della DRD, individuata nel Primo Pilastro e, in particolare, nell'art. 95 TCE. Secondo la ricorrente, infatti, obiettivo primario della disciplina europea in materia di *data retention* era da rinvenirsi nella garanzia della sicurezza e nella lotta al crimine, mentre risultava solo secondario l'impatto sul funzionamento del mercato interno. Con una argomentazione che verrà più volte riproposta anche in tempi recenti, il Governo irlandese richiamava quanto deciso dai giudici di Lussemburgo nella sentenza CGUE 30 maggio 2006, C-317/04 e 318/04, *Parlamento europeo c. Consiglio e Commissione*, avente ad oggetto la Decisione del Consiglio 2004/496 relativa alla conclusione di un accordo con gli USA in materia di trattamento e trasferimento dei dati PNR – cioè dei codici di prenotazione di passeggeri aviotrasportati, in partenza dall'UE e diretti verso gli Stati Uniti – da parte

la seconda decisione della CGUE, la nota *Digital Rights Ireland* (d'ora in avanti *DRI*) [33], che, traendo origine dai due attesi rinvii pregiudiziali della *High Court* irlandese e dalla *Verfassungsgerichtshof* (Corte costituzionale) austriaca [34], si concentrava invece sulla compatibilità della Direttiva ri-

---

dei vettori aerei al *Bureau of Customs and Border Protection* statunitense. In quel caso infatti i giudici di Lussemburgo avevano annullato la Decisione del Consiglio, ritenendola erroneamente fondata sul Primo Pilastro, rinvenendo lo scopo del *data transfer* non nella prestazione di servizi bensì nella salvaguardia della sicurezza pubblica degli USA (para. 57). I parallelismi tra i due casi, evidenziati dalla ricorrente, venivano però negati dalla CGUE nella sentenza del 2009, che faceva salva la DRD. Questo perché la direttiva, secondo il ragionamento dei giudici di Lussemburgo, si limitava esclusivamente a disciplinare la *data retention* e non la fase dell'accesso: regolando primariamente l'operato e gli obblighi posti in capo ai *service providers*, essa non poteva che trovare quale unica e corretta base giuridica il Primo Pilastro, non sconfinando nelle competenze degli Stati membri in materia di repressione della criminalità. Se da un lato tale argomentazione aveva certamente il merito di confermare la correttezza della base giuridica e, di riflesso, la partecipazione del Parlamento europeo e del GEPD al processo di approvazione di una disciplina così delicata (in questi termini F. FABBRINI, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quaderni costituzionali*, 2, 2009, p. 422), d'altro lato essa era all'origine di quella marcata vaghezza dei termini impiegati per definire scopi e limiti dell'obbligo di conservazione generalizzata nonché di quella ampia discrezionalità lasciata agli Stati membri quanto alla regolamentazione dell'accesso che avevano poi finito col tradursi nella persistente disomogeneità di discipline che la Direttiva intendeva invece scongiurare. Proprio questa sottile linea di demarcazione tra disciplina della conservazione e regolamentazione dell'accesso, tra finalità di armonizzazione e scopi securitari, continuerà ad essere oggetto di ampi dibattiti. Per una approfondita ricostruzione di questa pronuncia e dei suoi discussi profili, si leggano E. HERLIN-KARNELL, *Annotation of Ireland v. Parliament and Council*, in *Common Market Law Review*, 46, 2009, p. 1667 ss.; T. KONSTADINIDES, *Wavering between Centres of Gravity: comment on Ireland v. Parliament and Council*¸ in *European Law Review*, 35, 2010, p. 88 ss.; S. POLI, *The legal basis of Internal market measures with a security dimension: comment on case C-301/06, Ireland vs. Parliament/Council*, in *European Constitutional Law Review*, 6, 2010, p. 135 ss.; C.C. MURPHY, *Fundamental rights and security: the difficult position of the European judiciary*, in *European Public Law*, 16, 2010, p. 289 ss.

[33] CGUE 8 aprile 2014, Cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e al.* e *Karntner Landesregierung e al.*

[34] Il rinvio promosso dalla *High Court* irlandese trovava origine nel ricorso elaborato dall'organizzazione *Digital Rights Ireland* che riteneva illegittimi il trattamento, conser-

spetto ai diritti fondamentali sanciti agli artt. 7, 8, 11 e 52 della Carta di Nizza. In un mutato contesto politico-sociale ma anche istituzionale e delle fonti [35], più lontano da quel clima fortemente segnato dalla emer-

vazione e accesso ai dati relativi alle proprie comunicazioni telefoniche, imposti dalla normativa interna *Criminal Justice Terrorist Offences Act 2005*. In Austria invece erano stati il Governo del Land della Carinzia prima e il sig. Seitlinger poi, seguito da un ricorso promosso da ben 11.130 cittadini, a lamentare l'incostituzionalità – nonché l'incompatibilità con l'art. 8 della Carta di Nizza – dell'art. 102-*bis* della legge austriaca sulle telecomunicazioni, introdotto quale trasposizione della DRD. Le questioni pregiudiziali sollevate muovevano dall'impossibilità riscontrata dai giudici di risolvere le questioni attinenti alle normative nazionali in materia di *data retention* senza che prima fosse valutata la validità della DRD da cui esse discendevano. In ciò dunque le considerazioni promosse dalle Corti irlandese e austriaca differivano rispetto a quanto deciso in precedenza da altre Corti nazionali; e proprio per tale ragione questi rinvii «were welcomed with relief as they gave the CJEU the chance to revisit the fundamental rights questions left open in its initial (competency) judgement on the DRD», F. BOEHM, M. COLE, *Data retention after the judgement of the Court of Justice of the EU*, The Greens in the EP Working Paper, 2014, p. 19. L'importanza e la delicatezza di tali rinvii era peraltro testimoniata anche dalle decisioni di altre Corti nazionali similmente chiamate a pronunciarsi sulla legittimità costituzionale delle normative interne in materia di *data retention*: la *Ústavný súd Slovenskej republiky* (Corte costituzionale slovacca) ad esempio aveva deciso di sospendere l'applicazione della legislazione di trasposizione della DRD nelle more del giudizio pendente dinnanzi ai giudici di Lussemburgo. Sul punto si rimanda a M. DICOSOLA, *La data retention directive e il dialogo tra Corti costituzionali e Corte di giustizia nel sistema multilivello europeo*, in *Diritti Comparati*, 20 febbraio 2014.

[35] Ci si riferisce innanzitutto al Trattato di Lisbona, adottato nel 2007 ed in entrato in vigore nel 2009, che aveva comportato, oltre al superamento della ormai troppo rigida suddivisione in Pilastri, anche l'inserimento nel Trattato sul Funzionamento dell'UE (TFUE) dell'art. 16 che, pur rassomigliando al previo art. 286 del TCE, fornisce ora una più ampia e completa tutela del diritto alla protezione dei dati, rappresentando la base giuridica per l'adozione di qualsiasi normativa relativa alla privacy e *data protection*. L'art. 6 del Trattato sull'Unione europea (TUE), come modificato nel 2007, ha riconosciuto poi alla Carta di Nizza lo stesso valore giuridico dei Trattati, facendola divenire fonte vincolante del diritto europeo e parametro che la CGUE può utilizzare per vagliare la validità e conformità al diritto dell'UE degli atti sopposti al suo controllo. Sotto il profilo sociale e politico, poi, le rivelazioni di Edward Snowden avevano ancor più accresciuto, a partire dal 2013, la sensibilità dell'opinione pubblica verso tematiche quali l'ingerenza nella sfera privata da parte delle autorità pubbliche, perpetrata – anche – mediante strumenti di raccolta e conservazione massiva di dati e metadati. Merita inoltre rilevare come, nel frattempo, anche la Commissione europea si fosse interrogata sulla

genza securitaria e dalla minaccia del terrorismo che aveva caratterizzato l'adozione della DRD, la CGUE nella storica sentenza dell'8 aprile 2014 esprimeva principi e considerazioni di estrema novità e dagli effetti dirompenti, imponendo un vero e proprio ripensamento del bilanciamento tra garanzia della sicurezza e diritti fondamentali alla *privacy* e alla protezione dei dati.

Innanzitutto, per la prima volta, venivano espressamente riconosciuti, con grande consapevolezza e lucidità, i rischi rappresentati dalla disponibilità e dal trattamento dei metadati: indipendentemente dal contenuto delle comunicazioni, infatti, «questi dati, presi nel loro complesso, possono permettere di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini quotidiane, i luoghi di soggiorno permanente o temporaneo, gli spostamenti giornalieri e non, le attività svolte, le relazioni sociali di queste persone e gli ambienti sociali da esse frequentati», para. 27. La sola conservazione dunque, nel suo complesso, era in grado di comportare una lesione della sfera privata di vasta portata e particolarmente grave, tale peraltro da «ingenerare nelle persone interessate (...) la *sensazione che la loro vita privata sia oggetto di costante sorveglianza*», para. 37; ciò a prescindere dal successivo ed eventuale accesso da parte delle autorità di *law enforcement*, che costituiva una ingerenza supplementare (para. 35). Al fine di essere giustificato e legittimo, un obbligo di conservazione dei metadati quale quello disposto dalla DRD, doveva pertanto possedere tutti i requisiti indicati dall'art. 52 della Carta di Nizza, quali il rispetto del contenuto essenziale dei diritti, nonché la conformità al principio di proporzionalità secondo cui le misure determinanti una ingerenza nei diritti fondamentali debbo-

---

efficacia e proporzionalità della DRD stessa, riconoscendo, nel documento *Valutazione dell'applicazione della Direttiva sulla conservazione dei dati (Direttiva 2006/24/CE)*, COM (2011) 225 def, 18 aprile 2011, il fallimento della DRD che non solo non aveva raggiunto quell'obiettivo di armonizzazione parziale della materia cui tendeva, ma aveva anche determinato un impatto non più trascurabile sui diritti fondamentali, come ribadito anche dalle posizioni espresse da ONG, Gruppo di Lavoro Art. 29 e GEPD e riportate nel documento di valutazione. Per una analisi della posizione della Commissione in questa fase valutativa, si rimanda a M. COLE, F. BOEHM, *EU Data Retention – Finally abolished? Eight years in light of Article 8*, in *Critical Quarterly for Legislation and Law*, 1, 2014, p. 58 ss.

no essere necessarie e rispondere a finalità di interesse generale riconosciute dell'UE o all'esigenza di proteggere diritti e libertà altrui.

Affermando che la conservazione generalizzata di metadati non era tale da pregiudicare il nucleo essenziale dei diritti fondamentali alla protezione dei dati e alla vita privata poiché non riguardava il contenuto delle comunicazioni, nonché riconoscendo la legittimità dell'interesse generale perseguito dalla DRD, individuato nell'obiettivo sostanziale della lotta contro la criminalità grave e, di conseguenza, della garanzia alla sicurezza pubblica (para. 41), la CGUE si concentrava poi sul controllo di proporzionalità. Sotto il profilo dell'idoneità al raggiungimento dell'obiettivo, la valutazione della Corte si presentava in realtà piuttosto sbrigativa: i metadati conservati rappresentavano, a parere dei giudici, una fonte supplementare di informazioni utili per l'accertamento di reati gravi, così che la *data retention* non poteva che essere considerata idonea al conseguimento dello scopo securitario posto alla base della DRD.

Se fino a qui nessuna lacuna o incompatibilità con la Carta di Nizza emergeva dall'analisi promossa dalla CGUE, ciò che veniva invece rilevato come problematico era il requisito della stretta necessità: la Direttiva 2006/24, infatti, avrebbe dovuto «prevedere regole chiare e precise che disciplinino la portata e l'applicazione della misura e impongano requisiti minimi in modo che le persone i cui dati sono stati conservati dispongano di garanzie sufficienti che permettano di proteggere efficacemente i loro dati personali contro il rischio di abusi nonché contro eventuali accessi e usi illeciti dei suddetti dati», para. 54. Ebbene, la DRD veniva ritenuta carente e non limitata a quanto strettamente necessario sotto quattro differenti aspetti: la disciplina della conservazione, l'accesso, la durata della conservazione, le condizioni di sicurezza e protezione dei dati. Con riferimento al primo profilo, i giudici osservavano come la Direttiva obbligasse gli operatori ad una conservazione generalizzata, comportante una «ingerenza nei diritti fondamentali della quasi totalità della popolazione europea, (…) senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo di lotta contro i reati gravi», para. 57. La conservazione così come disciplinata dalla DRD non veniva subordinata alla sussistenza di un legame o una relazione tra i dati conservati e una minaccia per la sicurezza pubblica e non veniva neppure richiesto che i soggetti i cui dati erano sottoposti a conservazione si trovassero «anche indiretta-

mente, in una situazione che po[tesse] dar luogo ad indagini penali», para. 59. Non era prevista, in altre parole, la necessaria presenza di un indizio a carico dei soggetti i cui dati venivano conservati, «tale da far credere che il loro comportamento possa avere un *nesso, anche indiretto o lontano*, con reati gravi», para. 58. Una *retention* legittima e proporzionata, dunque, doveva concretizzarsi in una forma di conservazione limitata (o *targeted*) ad un determinato periodo di tempo e/o ad un'area geografica determinata e/o ad una cerchia di persone «che possano essere coinvolte, in un modo o nell'altro, in un reato grave, o alle persone la conservazione dei cui dati, per altri motivi, potrebbe contribuire alla prevenzione, accertamento o perseguimento di reati gravi», para. 59.

Ma la Corte, piuttosto singolarmente, non si limitava al vaglio di proporzionalità della disciplina della *data retention*, che la DRD regolava espressamente: lo scrutinio veniva infatti esteso anche alla successiva ed eventuale fase dell'accesso, la cui regolamentazione era lasciata al legislatore nazionale, per espressa indicazione della Direttiva. I giudici avevano rilevato, anche sotto tale profilo, la mancanza di criteri oggettivi capaci di limitare «l'accesso delle autorità nazionali competenti ai dati e il loro uso ulteriore ai fini di prevenzione, di accertamento o di indagini penali riguardanti reati che possano, con riguardo alla portata e alla gravità dell'ingerenza nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, essere considerati sufficientemente gravi da giustificare siffatta ingerenza. Al contrario, la Direttiva 2006/24 si limita invece a rinviare in maniera generale ai reati gravi come definiti da ciascuno Stato membro nel proprio diritto interno», para. 60 [36]. La Corte, pertanto, riteneva necessaria la previsione, in maniera chiara e precisa, di criteri oggettivi tali da permettere una limitazione del numero di soggetti autorizzati ad accedere e ad usare i dati conservati; l'accesso, inoltre, doveva essere preceduto e subordinato ad uno specifico controllo svolto da un giudice o da un'entità amministrativa indipendente (para. 62).

I giudici di Lussemburgo, infine, ritenevano da un lato la forbice

[36] «L'art. 4 della Direttiva, che regola l'accesso di tali autorità ai dati conservati, non stabilisce espressamente che tale accesso e l'uso ulteriore dei dati di cui trattasi debbano essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative», para. 61.

temporale di conservazione fissata dal legislatore europeo come del tutto priva di criteri obiettivi in grado di limitare la durata della conservazione allo stretto necessario [37], dall'altro le norme disposte dalla DRD sotto il profilo della sicurezza dei dati non erano considerate tali da garantire tutele sufficienti contro eventuali accessi ed usi illeciti dei dati, non disponendo neppure la distruzione irreversibile dei metadati al termine della conservazione, né tantomeno l'obbligo di *retention* limitato al solo territorio dell'UE [38].

Alla luce di tutte queste considerazioni, i giudici di Lussemburgo dichiaravano la DRD eccedente i limiti indicati dal principio di proporzionalità e dunque invalida con effetto immediato, senza accogliere la proposta dell'Avvocato generale di sospendere gli effetti di tale decisione «per dar tempo al legislatore dell'Unione di adottare le misure necessarie per porre rimedio all'invalidità accertata, restando inteso che tali misure devono essere adottate entro un lasso di tempo ragionevole» [39].

---

[37] Ad esempio non veniva stabilita una distinzione della durata della conservazione in base alla tipologia dei dati, nonché «a seconda della loro eventuale utilità ai fini dell'obiettivo perseguito o a seconda delle persone interessate», para. 63.

[38] La possibilità che i metadati venissero trasferiti e conservati in Paesi extra-UE comportava una seria restrizione del controllo effettuato da autorità indipendenti, riconosciuto come essenziale al fine di garantire un effettivo rispetto della tutela del diritto alla protezione dei dati personali. Sotto questo profilo «the EU judges display an acute awareness of today's global data flows and the possibility for data to reside in cloud services worldwide», M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review,* 6, 2014, p. 849. Del resto già in precedenza il Gruppo di Lavoro Art. 29, nel *Parere 5/2012* del 1 luglio 2012 aveva evidenziato i pericoli derivanti da una conservazione dei dati provenienti dall'UE in uno Stato terzo, come riportato e analizzato da X. TRACOL, *Legislative genesis and judicial death of a directive: the European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it*, in *Computer Law & Security Review*, 30, 2014, p. 736 ss.

[39] Para. 158, Conclusioni dell'Avvocato generale Cruz Villalon, 12 dicembre 2013.

3.1. *La significativa portata della sentenza* Digital Rights Ireland *e i primi dubbi interpretativi.*

La decisione descritta, che ispirerà non solo la successiva giurisprudenza della CGUE ma che anche quella delle Corti nazionali, ha sicuramente rappresentato un primo significativo momento di riflessione sull'impatto dei Big Data e del loro utilizzo massivo rispetto ai diritti fondamentali, in particolare quelli alla riservatezza e alla protezione dei dati [40]. In questa pronuncia i giudici europei hanno affermato con forza come anche discipline volte alla garanzia della sicurezza non possano sottrarsi ad uno stretto esame di proporzionalità, necessità e compatibilità con la Carta di Nizza [41]. In questo senso, se l'adozione della DRD aveva segnato un passaggio dalla *data protection* alla *data collection* e *retention*, la sentenza *DRI* ha rappresentato invece una sorta di inversione di rotta, da un approccio spiccatamente pro-securitario ad uno invece connotato da un più attento bilanciamento tra tutela della vita privata e protezione dei dati da un lato e raccolta e conservazione massiva dei dati dall'altro [42]. Ecco allora che al-

[40] In questa pronuncia alcuni autori hanno anche rilevato un importante momento di affermazione di un più netto approccio *human rights-oriented* della giurisprudenza della CGUE: «Until DRI, with few exceptions, the Court had been overall deferential towards EU framework laws, even when directives and framework decisions left room for serious interference with human rights. (...) In contrast, in DRI, the Court of Justice shifts the responsibility to protect human rights onto the EU legislator. When EU legislative acts themselves impose serious interference with human rights, they must, simultaneously, provide for necessary safeguards, expressed in a clear and precise way, to prevent the interference from going beyond what is strictly necessary», M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland*, cit., p. 845.

[41] «The DRD case has posed a milestone for the future developments of EU legislation in two key areas of recent emergence: EU anti-terrorism and security legislation and fundamental rights in the framework of new technologies», L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights*, cit., p. 1768.

[42] Come rilevato da alcuni autori «In fact, the core of the Court's decision lies in the rejection of mass surveillance and in particular indiscriminate monitoring of the entire European population», A. VEDASCHI, V. LUBELLO, *Data Retention and its implications for the fundamental right to privacy*, cit., p. 27; della stessa autrice anche A. VEDASCHI, *I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Diritto pubblico comparato ed europeo*, 3, 2014, p. 1224 ss.

cuni commentatori hanno letto nella pronuncia analizzata la testimonianza della «ritrovata vocazione costituzionale della Corte di giustizia. Scegliendo di far propri gli argomenti con cui i giudici tedeschi, cechi, bulgari e rumeni hanno a vario titolo bloccato i provvedimenti nazionali di attuazione, i giudici del Lussemburgo non hanno soltanto eliminato una delle più importanti cause di attrito con le giurisdizioni nazionali, ma hanno anche posto le basi per il superamento di una pratica pericolosamente lesiva di basilari libertà individuali e fissato dei limiti precisi per l'eventuale futura adozione di testi normativi in materia di sicurezza» [43]. Così facendo, è stato dato ampio rilievo ai diritti alla riservatezza e alla protezione dei dati, colti nella loro dimensione di forte interconnessione con la tutela di altri diritti fondamentali nonché con la garanzia stessa di valori e principi democratici [44].

Con questa importante decisione, poi, i giudici fornivano un vero e proprio vademecum di principi e requisiti che avrebbero dovuto ispirare il legislatore europeo nei suoi successivi interventi in materia: in questo senso, «the decision is not only important in terms of the balance of powers in a horizontal perspective, strenghening the power of the ECJ in relation to the European legislature, but also in a vertical perspective: the normative setting has to be more detailed at a supranational level» [45].

---

[43] F. VECCHIO, *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*, 12 giugno 2014. Per Granger e Irion la pronuncia in esame contribuisce alla «redefinition of the basis of the European integration in favour of constitutionalism and human rights», M. GRANGER, K. IRION, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland*, cit., p. 840. Similmente si legga M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Diritto dell'Unione europea*, 4, 2014, p. 803 ss.

[44] I giudici di Lussemburgo hanno stabilito una posizione forte «in favor of strengthening privacy protections in the digital age and abandoning sweeping programs of data retention that alter at their roots the relationship between citizens and government in a democratic society», 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*, 28, 2015, p. 65 ss.

[45] J. KUHLING, S. HEITZER, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in

Nonostante questi profili certamente di grande rilievo, che hanno permesso alla sentenza *DRI* di essere accolta come una storica e profonda vittoria per i diritti fondamentali nell'era digitale[46], non possono tuttavia essere taciute alcune persistenti zone grigie ed interrogativi aperti, destinati a condizionare il successivo e ancora lungo dibattito in materia di *data retention*. Alcuni specifici profili della pronuncia esaminata, infatti, sono parsi problematici o poco chiari: nel delineare ad esempio precise condizioni e requisiti con riferimento tanto alla fase di conservazione dei metadati quanto a quella del successivo ed eventuale accesso – la cui regolamentazione, è bene ricordarlo, non era contenuta nella DRD –, la Corte ha *de facto* sfumato il più netto confine tra armonizzazione della materia della *data retention* e quella di ai dati accesso per scopi securitari tracciato in precedenza nella pronuncia *Irlanda c. Parlamento europeo e Consiglio*. Mentre in quel caso la distinzione tra le due fasi era servita a validare la scelta della base giuridica della DRD (l'allora Primo Pilastro), ritenendo unico oggetto della direttiva la disciplina della conservazione e l'armonizzazione di regole attinenti al funzionamento del mercato unico, nella sentenza *DRI* invece i giudici di Lussemburgo hanno identificato nell'ampio margine di discrezionalità riconosciuto in capo agli Stati membri quanto alla disciplina dell'accesso un serio rischio per la garanzia e il rispetto della Carta di Nizza e dei diritti fondamentali, così che compito del legislatore europeo dove-

---

European Law Review, 2, 2015, p. 266. Sul punto si legga anche S. CRESPI, *Diritti fondamentali, Corte di Giustizia e riforma del Sistema UE di protezione dei dati*, in *Rivista italiana di Diritto Pubblico Comparato*, 3, 2016, p. 834 ss., nonché T. OJANEN, *Rights-based review of electronic surveillance after DRI and Schrems in the European Union*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, Londra, 2017, p. 13 ss. Quest'ultimo ha riconosciuto nella sentenza *DRI* «an instance of a constitutional dialogue between the CJEU and the EU legislature in which the CJEU does not only invalidate a legal measure but also indicates how the legislator could enact valid legislation accomplishing the main objective of the invalidated law», p. 27.

[46] Sul punto si legga L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the UK after the European Data Retention Directive*, in R.A. MILLER (a cura di), *Privacy and power. A transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, Cambridge, 2017, p. 564 ss., che riporta l'entusiastica reazione e le dichiarazioni della ONG Privacy International.

va essere anche quello di fissare garanzie minime contro il rischio di abusi nella successiva fase di trattamento dei dati conservati.

Altre criticità sono state poi rinvenute sia nella frettolosa distinzione tra contenuto delle comunicazioni e metadati quali elementi determinanti per stabilire l'avvenuta lesione del nucleo essenziale del diritto alla vita privata, sia nella valutazione sbrigativa e poco motivata circa l'idoneità del regime di conservazione generalizzata al raggiungimento dell'obiettivo posto, ovvero quello della garanzia della sicurezza e di un più efficiente contrasto alla criminalità: «the Court's failure to rigorously assess the suitability of data retention as a measure to tackle serious crime is regrettable, given the increasingly prevalent use of mass surveillance techiniques by governments and private entities» [47].

Particolarmente problematici e dibattuti, anche in ambito nazionale, sono stati poi i requisiti specificamente fissati in materia di *data retention*: la richiesta sussistenza di un nesso, anche solo indiretto, tra conservazione dei dati e minaccia per la sicurezza pubblica, ha infatti portato alla nascita di considerevoli dubbi quanto alla conformità alla Carta di Nizza di una forma di conservazione generalizzata in quanto tale, *per se* incompatibile con la preventiva determinazione di indizi a carico dei soggetti i cui dati venivano sottoposti a conservazione. Alcuni autori hanno così sul punto rilevato come «from the wording of the judgement, it is not fully clear what the position of the Court was: there was indeed the option to think that bulk data retention was prohibited unless it was paired with a strict access regime providing the necessary guarantees» [48]; in altre parole, una lettura meno rigida della pronuncia della Corte avrebbe potuto evitare di giungere ad una netta esclusione della possibilità di ricorrere allo strumento della *bulk data retention*, ritenendo invece un simile regime di conservazione compatibile con il diritto dell'UE solo in presenza di ido-

---

[47] O. LYNSKEY, *The DRD is incompatible with the rights to privacy*, in *Common Market Law Review*, 2014, p. 1799; sul punto anche E. GUILD, S. CARRERA, *The political and judicial life of metadata*, cit., p. 1 ss.

[48] E. CELESTE, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019, p. 134. Similmente anche J. KUHLING, S. HEITZER, *Returning through the national back door?*, cit., p. 266.

nee e stringenti salvaguardie relative alla fase di accesso.

Come si vedrà, queste incertezze interpretative ed applicative, insieme agli ulteriori profili poco chiari o coerenti sopra rilevati, hanno contribuito sin da subito all'affermarsi di criticità attuative e disomogeneità di reazioni tanto negli Stati membri quanto nelle Istituzioni europee stesse: il ruolo di giudice (para-)costituzionale assunto dalla CGUE e l'approccio orientato ad una decisa garanzia dei diritti fondamentali si sono infatti ben presto scontrati con le esigenze concrete delle autorità statali e con la difficoltà di conciliare un elevato standard di tutela della privacy e protezione dei dati con l'efficacia degli strumenti di conservazione e accesso ai dati, nonché con i limiti segnati dalla divisione di competenze tra Unione e Stati membri che, come si è già in parte visto nella discussa distinzione tra disciplina della conservazione e quella dell'accesso, emergono con particolare forza in un'area normativa di estrema delicatezza e complessità quale quella esaminata, che tocca tanto l'operato di *service providers* privati quanto l'intervento di autorità pubbliche [49].

4. *Le reazioni degli Stati membri e delle Istituzioni europee all'intervento della CGUE: una situazione confusa.*

La storica pronuncia *DRI*, che per certe realtà statuali si poneva in perfetta continuità e coerenza rispetto alla giurisprudenza nazionale in materia di *data retention* [50], ha presto mostrato i propri dirompenti effetti: la dichiarazione di invalidità della DRD ha imposto, infatti, un ripensamento della disciplina della conservazione dei dati e una seria riflessione sui successivi passi da intraprendere si è quindi resa necessaria sia da parte delle Istituzioni europee, chiamate a valutare se e come colmare il vuoto

---

[49] Sul punto si legga R. FLOR, *Dalla 'data retention' al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de jure condendo'*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, Roma, 2015, p. 223 ss.

[50] Si veda M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE*, cit., p. 826.

normativo lasciato dalla decisione della CGUE, sia da parte degli Stati membri – legislatori e Corti nazionali – con riferimento alla sorte delle legislazioni statali attuative della disciplina europea invalidata.

Sul versante sovranazionale, sebbene numerosi Stati membri e gran parte della dottrina avessero richiesto con decisione e urgenza l'avvio di una nuova iniziativa legislativa *ad hoc* in materia di *data retention*[51], si è registrata una completa inazione delle Istituzioni europee; un immobilismo che, come si vedrà nel prosieguo di questo Capitolo, perdura sino ad oggi nonostante alcuni più recenti tentativi di promuovere un serio dibattito sull'opportunità di una nuova disciplina armonizzata. La pronuncia *DRI* ha poi determinato importanti riverberi non solo rispetto alla disciplina della conservazione di metadati bensì anche con riferimento a tutte quelle normative sovranazionali che implicavano – ed implicano tutt'ora – operazioni di raccolta, conservazione e trattamento di ingenti quantità di dati personali in forma generalizzata. Si pensi, ad esempio, alla disciplina europea del trasferimento di dati verso Stati terzi, nonché al trasferimento, per scopi securitari, di dati PNR relativi a tutti i passeggeri di voli aerei in partenza dall'UE e diretti verso Stati terzi. In questo ambito, proprio le considerazioni sulla proporzionalità e legittimità di strumenti invasivi della sfera privata promosse dai giudici di Lussemburgo nella pronuncia sin qui esaminata hanno portato, come si avrà modo di vedere nel prossimo Capitolo, a ripetuti e nuovi interventi della CGUE finalizzati a determinare l'estensione, anche al di là dei confini europei, dei principi sanciti in materia di *data retention* dinnanzi a quello che alcuni autori hanno definito, con una immagine d'impatto, il «Trojan horse effect» della sentenza *DRI*[52].

---

[51] Si legga a tal proposito F. GALLI, *Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions*, in *Maastricht Journal of European and Comparative Law*, 3, 2016, p. 460 ss.

[52] Tale efficace espressione è stata utilizzata da Celeste che ha evidenziato come la c.d. *data retention saga* si sia poi espansa in due direzioni, orizzontale e verticale, come meglio si vedrà nel Capitolo 3: «in the first case [horizontally] the requirements developed by the Court of Justice could potentially apply to EU acts implying forms of data retention. In the second case [vertically] there is the possibility that the Court's prescriptions will eventually affect other branches of member states'law that presuppose a system of bulk data retention, and in particular those regulating national security au-

Giungendo all'analisi degli effetti prodotti dall'intervento dei giudici di Lussemburgo sul fronte nazionale, è necessario premettere che la dichiarazione di invalidità di una Direttiva non produce ripercussioni, se non indirette, sulla legislazione di recepimento a livello nazionale [53]. Di conseguenze, viene lasciato all'iniziativa dei singoli Stati membri il compito di valutare la legittimità delle discipline interne e la loro compatibilità tanto ai diritti garantiti dal proprio ordinamento quanto al diritto dell'UE, così come interpretato dalla giurisprudenza della CGUE.

Ebbene, dinnanzi a questo scenario, le risposte degli Stati membri alla invalidazione della DRD hanno presentato caratteristiche anche molto differenti tra loro: seguendo una utile ripartizione in tre gruppi delle reazioni registratesi a livello nazionale [54], un primo insieme risultava composto da tutti quegli ordinamenti che avevano cercato di incorporare nella normativa interna i principi e requisiti emersi dalla sentenza *DRI* mediante un nuovo intervento normativo, su iniziativa talvolta del Governo e talaltra del Parlamento. È il caso di Regno Unito [55], Lussemburgo [56] e Germania [57], nei quali comunque, è bene premetterlo, le rinnovate disci-

---

thorities», E. CELESTE, *The Court of Justice and the ban on bulk data retention*, cit., p. 135.

[53] Questo profilo è stato espressamente precisato anche dalla Commissione europea nelle FAQs relative alla disciplina della *data retention*, aggiornate nell'aprile 2014 a seguito della pronuncia della CGUE (consultabili all'indirizzo: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_14_269).

[54] Elaborata da J. KUHLING, S. HEITZER, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, cit.

[55] Come si vedrà ampiamente nel Capitolo 4, dinnanzi alla pronuncia della CGUE, il legislatore inglese aveva reputato opportuno superare la previa normativa di trasposizione della DRD, adottando con un rapido e discusso procedimento normativo il *Data Retention and Investigatory Powers Act* (c.d. DRIPA) del 17 luglio 2014.

[56] L'iniziativa normativa era stata promossa del Ministro della Giustizia nel 2015.

[57] La normativa tedesca adottata nel dicembre 2015 (*Gesetz zur Einfuhrung einer Speicherflicht und einer Hochstspeicherfrist fur Verkehsdaten*) rappresentava, a parere di molti commentatori, uno dei più seri tentativi di trasposizione, nel contesto nazionale, delle indicazioni espresse dai giudici di Lussemburgo nella sentenza *DRI*: il periodo di conservazione era stato così limitato ad una forbice temporale da quattro a dieci settimane a seconda della tipologia di dati interessati; era stato previsto un previo vaglio ef-

pline nazionali non escludevano interamente il ricorso ad una forma di conservazione dei metadati generalizzata ed indiscriminata, pur introducendo più stringenti tutele e salvaguardie nella fase di accesso.

Il secondo insieme di Stati si caratterizzava per il superamento della normativa di recepimento della DRD mediante un procedimento che, diversamente dal primo gruppo descritto, aveva visto nell'intervento delle Corti nazionali il motore propulsivo del cambiamento. Ci si riferisce ad Austria, Belgio, Olanda, Polonia, Romania e Slovenia [58], le cui Corti, la

---

fettuato da un giudice volto ad autorizzare l'accesso ai metadati da parte di autorità pubbliche; le categorie di dati conservati erano state ristrette mediante l'esclusione dei dati derivanti da e-mail; erano state inoltre introdotte nuove misure a garanzia della sicurezza dei dati, per esempio limitando i soggetti terzi abilitati all'accesso o imponendo l'obbligo di conservazione unicamente nel territorio tedesco. Merita sin da ora sottolineare però come questa normativa sembrasse «at first glance, to be a serious effort to meet the requirements set by the Karlsruhe and Luxembourg Courts. It does not however, address the major issue raised by the CJEU in paras. 57-59 of *DRI*: blanket retention of all users of telecommunication without any limitation based on suspicion, geography, time or group», N. VAINIO, *Fundamental rights compliance and the politics of interpretation: explaining Member State and Court reactions to Digital Rights Ireland*, in T. BRAUTIGAM, S. MIETTINEN (a cura di), *Data protection, privacy and European regulation in the digital age*, Unigrafia, Helsinki, 2016, p. 245. Per approfondimenti su tale normativa, si rimanda più ampiamente a S. SCHWEDA, *Germany: Parliament adopts new data retention law*, in *European Data Protection Law Review*, 1, 2015, p. 223 ss.

[58] La Corte costituzionale austriaca si era pronunciata nel caso G 47/2012-49, il 27 giugno 2014, dichiarando l'illegittimità della normativa in materia di *data retention*; la Corte costituzionale belga era intervenuta l'11 giugno 2015 annullando la *Loi du 30 juillet 2013* in materia di conservazione dei metadati per scopi securitari; la normativa olandese veniva invalidata da una ordinanza di un tribunale olandese nel 2015; il Tribunale costituzionale polacco si era pronunciato, nello stesso senso, il 30 luglio 2014 (caso K 23/11); la Corte costituzionale romena con decisione n. 40 del 8 luglio 2014 si era nuovamente pronunciata sulla normativa nazionale attinente alla conservazione dei dati, ritenendo tale regime ancora una volta incostituzionale; la Corte costituzionale slovena, nel caso U-I-65/13-19, del 3 luglio 2014 – dopo la già richiamata sospensione volta ad attendere l'esito della sentenza della CGUE sulla DRD – aveva dichiarato l'illegittimità costituzionale delle disposizioni regolanti la conservazione generalizzata di metadati, ordinando anche la cancellazione di tutti i dati conservati sulla base di tale normativa. Per approfondimenti su tali pronunce e sulle reazioni degli Stati membri, si rimanda a: L. BENEDIZIONE, E. PARIS, *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data*

maggior parte delle volte costituzionali, avevano affermato l'incostituzionalità – totale o parziale – delle disposizioni statali in materia di *data retention*, rendendo così necessaria l'adozione di una nuova disciplina nazionale ad opera del legislatore.

L'ultimo insieme di Stati riuniva invece quegli ordinamenti nei quali non si era provveduto, in alcun modo, alla modifica della normativa interna: salvo alcune eccezioni [59], negli ordinamenti rientranti in questo gruppo la scelta di mantenere intatta la legislazione di recepimento della DRD si era registrata a seguito di una forma di controllo della compatibilità della normativa esistente rispetto ai criteri indicati dalla giurisprudenza europea in materia, esercitata mediante l'intervento dei giudici nazionali o di soggetti o organismi *ad hoc* cui veniva specificamente affidata tale valutazione. Al termine del controllo e diversamente da quanto accaduto nel primo e nel secondo gruppo, in Stati quali Danimarca, Svezia [60], Ungheria, Spagna e Cipro, le autorità preposte erano giunte ad una dichiarazione di legittimità della disciplina interna sulla conservazione dei

---

Retention Directive, cit., p. 1764 ss.; ma anche N. VAINIO, S. MIETTINEN, *Telecommunications data retention after DR: legislative and judicial reactions in the Member States*, in *International Journal of Law and Information Technology*, 23, 2015, p. 290 ss.

[59] Merita infatti rilevare come in alcuni degli Stati rientranti in questo ultimo gruppo, quali Croazia, Italia e Portogallo, non si fosse registrato alcun intervento – né da parte dei giudici nazionali né del legislatore o del Governo – finalizzato a vagliare, ed eventualmente modificare, la normativa esistente in materia di *data retention*. Il risultato di mantenere immutata la disciplina nazionale era stato pertanto ottenuto non da una decisione attestante la legittimità e compatibilità della regolamentazione statale bensì da una totale inazione di tutte le autorità nazionali e da una mancata attivazione del controllo giudiziario.

[60] Con riferimento alla Svezia ad esempio è interessante notare come «In a first response to the annulment of the DRD, the Swedish Post and Telecom Authority stopped enforcing their implementation law and apparently tacitly approved the Swedish internet service provider deleting all data that has been stored on the grounds of data retention law. However, after scrutinizing more precisely the requirements determined by the ECJ in *DRI*, the Swedish authorities changed course. In August 2014, they started to enforce unaltered data retention law and instructed providers to start retaining data again», J. KUHLING, S. HEITZER, *Returning through the national back door?*, cit., p. 275. Come vedremo, proprio tale decisione del Governo svedese sarà alla base del successivo ed ulteriore intervento della CGUE in materia di conservazione dei dati.

metadati e dunque al suo mantenimento in vita, senza bisogno di alcun intervento o modifica.

Dalla ricognizione sin qui svolta emerge così, da un lato, la difficoltà e, per certi versi, la reticenza espressa dalle autorità governative nazionali ad applicare *in toto* le garanzie e limitazioni stabilite nella *DRI*; garanzie che, qualora interamente attuate, avrebbero finito inevitabilmente col comprimere l'utilità dello strumento della *data retention*[61]. Dall'altro lato, sul fronte giurisprudenziale, si registra una disomogenea risposta delle Corti nazionali: queste infatti hanno mostrato approcci fortemente diversi, talvolta in linea con l'indirizzo dei giudici di Lussemburgo, come in Belgio, talaltra invece adottando una lettura meno rigida rispetto a quella fornita a livello europeo, giungendo così a far salve, *in toto* o in parte, le normative nazionali adottate sulla base della DRD. Sotto questo profilo, si venivano quindi a distinguere quelle che Vanio e Miettenin hanno descritto efficacemente come «permissive interpretation» e «strict interpretation» di quanto sancito nella sentenza *DRI*[62]: mentre la prima tipologia mirava a far salva la conservazione generalizzata purché essa fosse accompagnata da idonee garanzie nella fase di accesso successiva, ritenendo

---

[61] Come emerso dal Report redatto da Eurojust all'esito del *Consultative forum of Prosecutors General and Directors of Public Prosecutors of the MSs of the EU* e del *Workshop on data retention in the fight against serious crime: the way forward*, tenutisi il 11 dicembre 2015, «data retention must be carried out in a generalized manner as it is impossible to know beforehand whose data will be relevant in the course of a specific criminal investigation prosecution. Generalised data retention is not only a useful tool to link suspects to an offence, but also to delink suspects from an offence. There are no equally effective alternatives to data retention», p. 5. Sulla base di queste considerazioni si comprende quindi la resistenza mostrata avverso l'attuazione delle limitazioni indicate dalla CGUE nella sua sentenza.

[62] Secondo l'approccio "permissivo", «the observations Court makes in paragraphs 57-68 are a checklist of changes that would make the law proportionate, but it is not an absolute list. (…) According to the strict interpretation, the ruling in practice forbids any indiscriminate blanket data retention per se by requiring that the retained data must have a connection to serious crime and terrorism», N. VAINIO, S. MIETTINEN, *Telecommunications data retention after DRI*, cit., p. 300. In questo senso gli autori hanno ritenuto generalmente – anche se non sempre – le Corti degli Stati membri più inclini ad una interpretazione "rigida", mentre quella "permissiva" era tendenzialmente adottata dai Governi e dai legislatori nazionali.

quindi i criteri delineati dalla Corte come non cumulativi e non necessari nella loro totalità, l'interpretazione restrittiva invece riscontrava nella posizione dei giudici di Lussemburgo una chiara dichiarazione di invalidità *tout court* della conservazione generalizzata che, per sua natura, non poteva essere considerata compatibile con il principio di proporzionalità e stretta necessità, mentre unica forma di conservazione conforme al diritto dell'UE veniva rinvenuta nella *targeted data retention*.

Infine, in questo già complesso e frammentario panorama di soluzioni e approcci, reso possibile proprio da quelle incertezze e zone grigie rinvenibili nella sentenza *DRI* e sottolineate nei paragrafi precedenti [63], un ulteriore aspetto è da tenere in considerazione: venendo meno l'imposizione derivante dalla Direttiva DRD, l'introduzione di un obbligo di *data retention* da parte degli Stati membri tornava ad essere uno strumento di lotta alla criminalità volontariamente adottabile dai singoli Stati membri sulla base del "redivivo" art. 15 della Direttiva *e-Privacy*. Proprio quest'ultimo diveniva, in assenza di una nuova normativa *ad hoc*, l'unica disposizione europea in materia di conservazione di metadati per scopi securitari. Tale articolo, tuttavia, era stato, come si ricorderà, sin dall'inizio considerato estremamente vago e generico, così come eccessivamente ampio era stato ritenuto il richiamo ai limiti derivanti dai principi generali del diritto comunitario. Sebbene i requisiti e le condizioni sancite dalla pronuncia *DRI* ben avrebbero potuto aiutare a "riempire di significato" il succinto dettato normativo dell'art. 15, le incertezze e gli interrogativi ancora aperti riscontrati nella posizione espressa dai giudici di Lussemburgo erano inevitabilmente destinati a riflettersi anche sull'interpretazione della Direttiva *e-Privacy* stessa, facilitando così il riproporsi di una nuova situazione di incertezza e di disomogeneità nel panorama europeo,

[63] «Vagueness of the judgement leaves these MSs room to argue their implementation is proportionate because it addresses some of the worries the Court listed», N. VAINIO, *Fundamental rights compliance and the politics of interpretation*, cit., p. 249. Proprio di una situazione di "grave incertezza giuridica" parla F. VECCHIO, *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*, cit. Sul punto anche A. ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014, p. 723 ss.

proprio come avvenuto prima della adozione della DRD. Anche all'indomani della pur rilevante sentenza *DRI*, dunque, la determinazione di una forma di conservazione dei dati conforme al diritto dell'UE e alla Carta di Nizza risultava ancora priva di un chiaro punto risolutivo. Come Rauhofer e Sithigh avevano preannunciato, l'intervento della CGUE e la "riespansione" dell'ambito di applicazione dell'art. 15 Direttiva *e-Privacy* avevano infatti portato ad un nuovo «sustained period of legal uncertainty», con l'avvertimento che «the prudent MSs should hesistate before readopting provisions along the lines of the now invalid Directive» [64].

5. *La CGUE chiamata nuovamente a pronunciarsi sulla conformità del regime di conservazione generalizzata rispetto alla Carta di Nizza: la sentenza* Tele2.

Ecco perché, dinnanzi a questa situazione piuttosto confusa, una strada percorribile diveniva quella di chiedere nuovamente l'intervento della CGUE al fine di ottenere chiarimenti, questa volta attinenti all'interpretazione ed applicazione dell'art. 15 Direttiva *e-Privacy*: in tal modo si sarebbe offerta ai giudici di Lussemburgo la possibilità di spiegare se e come i criteri indicati nella *DRI* con riferimento alla DRD dovessero essere applicati – cumulativamente o meno – anche alle normative nazionali adottate in attuazione della facoltà derogatoria garantita dall'art. 15 stesso.

È in questo contesto che le Corti nazionali di Regno Unito e Svezia promuovevano due importanti rinvii pregiudiziali alla CGUE, poi riuniti e sfociati nella rilevante pronuncia c.d. *Tele2* del 21 dicembre 2016 [65], avente ad oggetto l'interpretazione dell'art. 15 della Direttiva e-*Privacy* letto alla luce degli artt. 7, 8 e 52 della Carta di Nizza [66]. In tale storica

---

[64] J. RAUHOFER, D. MAC SITHIGH, *The data retention directive never existed*, in *Scripted* n. 118, 2014, citato da L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the UK after the European Data Retention*, in R.A. MILLER, *Privacy and power. A transatlantic dialogue in the shadow of the NSA-affair*, cit.

[65] CGUE 21 dicembre 2016, Cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB eScretary of State c. Post-och telestyrelsen (PTS) e Tom Watson e al.*

[66] Come ben riassumeva l'Avvocato generale Henrik Saugmandsgaard Øe nelle sue

sentenza, dal forte impatto e dalle enormi conseguenze, i giudici di Lussemburgo chiarivano innanzitutto una questione preliminare di estremo rilievo, viste anche le incertezze emerse dalla previa giurisprudenza: una normativa nazionale che regoli, ai sensi dell'art. 15 Direttiva *e-Privacy*, la conservazione ed accesso ai metadati per scopi securitari, rientra, *in toto*, nell'ambito di applicazione del diritto dell'UE. Nonostante le opposte considerazioni espresse dai Governi degli Stati membri intervenuti [67], la CGUE giungeva ad affermare con chiarezza come anche la fase di accesso fosse da ritenersi attuativa dell'art. 15 della Direttiva richiamata: l'accesso infatti prevedeva un intervento da parte dei fornitori privati, chiamati ad accordare alle autorità nazionali la possibilità di ottenere i dati, operando quindi un trattamento rientrante nell'ambito di applicazione della normativa europea.

Appurato questo profilo estremamente delicato – e invero ancora discusso –, capace di incidere sulla difficile determinazione dei confini tra competenze dell'UE e quelle proprie degli Stati membri, i giudici poi si erano ancora una volta concentrati sul vaglio di proporzionalità delle normative in materia di conservazione e accesso ai metadati. Ribadendo come la facoltà di derogare all'obbligo generale di cancellazione ed ano-

---

conclusioni del 19 luglio 2016, «la Corte dovrà segnatamente precisare quale interpretazione occorra dare in un contesto nazionale alla sentenza *DRI*», para. 7. Brevemente si vuole sottolineare come il rinvio pregiudiziale proveniente dalla Svezia fosse scaturito dall'azione della società Tele2 Sverige fornitrice di servizi di telecomunicazione con sede nel territorio svedese: quest'ultima, dopo la pronuncia *DRI*, aveva interrotto la conservazione dei metadati prodotti dai propri utenti e imposta dalla *Lagen om Elektronisk Kommunikation* (c.d. LEK, ovvero la legge nazionale sulle comunicazioni elettroniche), ritenendo tale disposizione normativa non più applicabile alla luce della posizione espressa dalla CGUE; questo nonostante tale normativa fosse stata dichiarata, come si è detto, conforme al diritto dell'UE e alla Convenzione EDU a seguito dello scrutinio svolto da un relatore speciale incaricato dal Ministro della Giustizia. Per quanto attiene invece all'ulteriore rinvio promosso dai giudici della *Court of Appeal* inglesi, si rimanda alla ampia ricostruzione svolta nel Capitolo 4, specificamente dedicato al Regno Unito.

[67] Questi, infatti, individuando l'obiettivo della disciplina dell'acceso ai metadati nella lotta alla criminalità, ritenevano tali previsioni rientranti nelle competenze proprie degli Stati membri, sfuggendo all'ambito di applicazione del diritto europeo. In quest'ultimo dovevano piuttosto ricadere solo le disposizioni nazionali attinenti alla *data retention* e dunque agli obblighi di conservazione posti in capo agli operatori economici.

nimizzazione dei dati dovesse essere considerata una eccezione da interpretarsi quindi in maniera restrittiva [68], i giudici riproponevano *de facto* i medesimi requisiti indicati nella sentenza *DRI* tra i quali, per quanto attiene alla disciplina della conservazione, la sussistenza di un nesso, «sia pure indiretto o remoto», tra *data retention* e violazioni penali gravi (para. 105), rilevando inoltre la necessaria presenza di peculiari tutele stabilite a garanzia delle comunicazioni sottoposte a segreto professionale. Veniva così riaffermata quale forma di conservazione compatibile con la Carta di Nizza «una normativa la quale consenta, a titolo preventivo, la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione, per finalità di lotta contro la criminalità grave, a condizione che la conservazione dei dati sia, per quanto riguarda le categorie di dati da conservare, i mezzi di comunicazione interessati, le persone riguardate nonché la durata di conservazione prevista, limitata allo stretto necessario», para. 108. Alla luce di tali considerazioni, «l'art. 15 della Direttiva 2002/58, letto alla luce degli artt. 7, 8 e 11 nonché 52, par. 1, della Carta, deve essere interpretato nel senso che esso osta ad una normativa nazionale la quale preveda, per finalità di lotta contro la criminalità, una conservazione generalizzata e indifferenziata dell'insieme dei dati relativi al traffico e dei dati relativi all'ubicazione di tutti gli abbonati e utenti iscritti riguardante tutti i mezzi di comunicazione elettronica» (para. 112). Come si avrà modo di vedere, questa forte affermazione volta nella direzione di un abbandono totale dei sistemi di conservazione generalizzata, aprirà le porte a notevoli difficoltà attuative da parte dei legislatori nazionali e delle autorità di *law enforcement*, restii a sacrificare definitivamente uno strumento ritenuto così importante per la garanzia della sicurezza e dunque decisi a promuovere, anche in questo caso, una lettura più flessibile della posizione espressa dalla Corte.

La seconda questione affrontata dai giudici di Lussemburgo riguardava poi la disciplina dell'accesso: quest'ultimo poteva essere consentito solo se motivato da finalità di lotta alla criminalità di carattere *grave*. Que-

[68] I giudici riproponevano piuttosto rapidamente le stesse valutazioni svolte nella precedente sentenza *DRI* quanto ai requisiti del rispetto del contenuto essenziale dei diritti fondamentali in gioco, della sussistenza di un interesse legittimo e della idoneità della misura incidente sui diritti fondamentali al raggiungimento dell'obiettivo.

sto punto, lo si vuole premettere, non è da sottovalutare e anzi merita appropriato rilievo per la portata innovativa rispetto al dettato normativo dell'art. 15: quest'ultimo, infatti, a differenza dell'art. 1 della DRD, non svolgeva alcun richiamo al criterio della gravità del reato, che veniva quindi stabilito in via interpretativa dalla CGUE stessa. Nelle parole dei giudici di Lussemburgo, tuttavia, risultava comunque del tutto assente qualsiasi qualificazione o indicazione capace di stabilire il significato e gli elementi determinanti la "gravità" dei reati, la cui definizione era quindi ancora una volta lasciata interamente ai legislatori nazionali.

Oltre alla limitazione derivante dallo scopo, l'accesso poteva poi essere effettuato solo entro i limiti di stretta necessità: dovevano quindi essere stabilite norme chiare e precise sulle condizioni alle quali gli operatori economici che avevano conservato i dati erano tenuti a concederne l'accesso alle autorità pubbliche. Così, nell'interpretazione dei giudici di Lussemburgo, l'art. 15 attribuiva a ciascuno Stato membro il compito di stabilire una normativa interna che prevedesse requisiti sostanziali e procedurali in materia di accesso, nonché criteri oggettivi in grado di determinare una connessione, anche indiretta, tra accesso e finalità di repressione del crimine. Ne derivava che «un accesso può essere consentito (…) soltanto per i 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», para. 119. Unica eccezione prevista a tali restrizioni era individuabile in caso di sussistenza di una minaccia agli interessi vitali della sicurezza nazionale, difesa o sicurezza pubblica, come nel caso di attività terroristiche (para. 119). Ulteriore criterio necessario per la disciplina dell'accesso veniva individuato nel controllo preventivo di un giudice o di una entità amministrativa indipendente, subordinato alla presentazione di una richiesta motivata da parte delle autorità di *law enforcement* nell'ambito di una procedura di prevenzione, accertamento o esercizio dell'azione penale, salvo casi di urgenza debitamente giustificati. A ciò si aggiungeva anche la previsione di una notifica alle persone interessate, a partire dal momento in cui tale comunicazione non era più suscettibile di compromettere le indagini condotte dalle autorità summenzionate, allo scopo di consentire al soggetto cui i dati appartenevano la possibilità di esercitare eventualmente il diritto di ricorso.

La CGUE infine precisava come sussistesse in capo ai fornitori l'obbligo di stabilire misure tecniche ed organizzative appropriate a garanzia della protezione dei dati. La disciplina interna doveva a tal fine prevedere l'obbligo di conservazione nel solo territorio dell'Unione, nonché la distruzione irreversibile dei dati alla scadenza del termine fissato, come già enunciato nella precedente sentenza *DRI*, oltre alla determinazione di controlli da parte di autorità indipendenti circa il rispetto «del livello di protezione garantito dal diritto dell'Unione in materia di tutela delle persone fisiche riguardo al trattamento dei dati personali», para. 123.

La sentenza *Tele2*, quindi, «richiama a fondamento del percorso interpretativo della diversa Direttiva del 2002 numerosi passaggi della sentenza *Digital Rights* qualificando espressamente l'opportunità argomentativa di tali richiami in una logica "per analogia". Sebbene la Grande Sezione del 2014 non abbia inteso enunciare prescrizioni imperative applicabili alle normative nazionali, nella pronuncia *Tele2* del 2016 rileva quindi come il ragionamento da svolgere rispetto alla Direttiva 2002 – che continua a fissare i confini dell'autonomia procedurale degli Stati membri in materia – sia strettamente legato all'obiettivo perseguito dalla Direttiva invalidata» [69]. In questo senso, quindi, l'intervento dei giudici risultava indirizzato verso il consolidamento e l'integrazione dell'interpretazione promossa nella sentenza *DRI*, in tal modo estendendo anche alle discipline nazionali attuative dell'art. 15 Direttiva *e-Privacy* quanto in essa statuito, nonché fugando taluni di quei dubbi interpretativi emersi a seguito della giurisprudenza precedente e posti alla base dei divergenti approcci riscontratisi a livello nazionale [70].

---

[69] 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*, 2, 2017, p. 353.

[70] La diversa lettura maggiormente flessibile dei criteri sanciti nella sentenza *DRI*, adottata da numerosi Governi nazionali e da taluni Corti, era stata peraltro in parte seguita anche dall'Avvocato generale Saugmandsgaard Øe nelle sue Conclusioni. Egli infatti riteneva che la *bulk data retention* non fosse da considerarsi *per se* eccedente i limiti di quanto strettamente necessario e dunque, per sua stessa natura, incompatibile con il diritto dell'UE: «secondo la mia lettura della sentenza *DRI*, la Corte ha dichiarato che un obbligo generale di conservazione dei dati eccede i limiti dello stretto necessario qualora esso non sia accompagnato da garanzie rigorose riguardanti l'accesso ai dati, la du-

6. *Una rinnovata frammentarietà di approcci all'indomani della pronuncia* Tele2*: le problematiche "interpretazioni difensive" adottate dagli Stati membri.*

Se a seguito della sentenza *DRI* si era registrato, come si è visto, il tentativo di far salve le normative statali che sancivano un obbligo di conservazione generalizzato purché fossero accompagnate da tutele specifiche sulla sicurezza dei dati e sull'accesso ad essi, la decisa posizione espressa nella pronuncia *Tele2* aveva provocato invece una più netta chiusura verso l'adozione di forme di *bulk data retention*, bocciando quella interpretazione maggiormente flessibile che molti Governi nazionali avevano abbracciato a seguito della invalidazione della DRD. In questo senso pare condivisibile l'affermazione secondo cui «if the judgement in *DRI* was far-reaching, the Court of Justice's judgement in *Tele2* was even more radical in a number of important respects» [71].

Così, all'indomani di tale importante intervento della CGUE, erano emerse significative prese di posizione da parte degli Stati membri: i legislatori nazionali avevano infatti sin da subito manifestato profonde difficoltà nel predisporre discipline in materia di conservazione dei metadati per scopi securitari che fossero in tutto conformi ai principi delineati dalla giurisprudenza della CGUE e, al contempo, capaci di garantire l'utilità ed efficacia di tale strumento di indagine.

In questo contesto, significative perplessità erano state mosse avverso la soluzione della *targeted data retention* individuata dai giudici di Lussemburgo quale unica possibile e legittima forma di conservazione dei metadati. Ebbene, rispetto ad essa, i Governi degli Stati membri, la dottrina [72] e molte autorità europee [73] avevano da tempo manifestato – in-

---

rata di conservazione nonché la protezione e la sicurezza dei dati. (…) A questo proposito sottolineo che i punti da 56 a 59 della sentenza *DRI* non contengono alcuna dichiarazione della Corte nel senso che un obbligo generale di conservazione di dati ecceda, di per sé, i limiti dello stretto necessario», para. 193.

[71] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018, p. 16.

[72] Secondo Cameron, ad esempio, una *targeted data retention* posta in essere sulla base di criteri soggettivi o geografici avrebbe finito col porre problemi in termini di rispetto del diritto di non discriminazione: «while this power [to use the geographic cri-

vero anche prima della sentenza *Tele2* – profondi dubbi e resistenze, evidenziando come la *targeted data retention* fosse stata ideata dalla Corte stessa senza che alcuna parte nel corso del giudizio ne avesse mai menzionato l'opportunità e realizzabilità e senza che una tale soluzione

terion] would enable temporary monitoring of large public gatherings (such as sporting events), it also raises the spectre of permanent monitoring of, not simply zones surrounding government offices and other obvious terrorist targets, or even targets of organized crime, such as concentrations of banks, but, more disturbingly, large urban areas with marginalized populations, such as immigrants communities», I. CAMERON, *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 54, 2017, p. 1489.

[73] Come si legge nel *Report of the Consultative forum of Prosecutors General and Directors of Public Prosecutors of the MSs of the EU and of the Workshop on data retention in the fight against serious crime: the way forward*, datato 11 dicembre 2015 e radatto dai rappresentanti delle autorità di *law enforcement* degli Stati membri, la soluzione della conservazione mirata promossa dalla CGUE nella sentenza *DRI* era stata oggetto di aspre critiche: «while it is possible to differentiate technically and legally between categories of data, limiting retention to specific categories or particular persons reduces the effectiveness of investigations and may apply nebulous distinctions, leading to allegations of prejudice, profiling and unlawful discrimination. Moreover, as a matter of law, limited data retention constitutes surveillance or preservation of data (not 'data retention' as such)». Tale ragionamento aveva spinto ad indicare quale unica soluzione percorribile una forma di conservazione generalizzata accompagnata da maggiori e più profonde tutele relative alla fase successiva ed eventuale dell'accesso ai metadati. Nella stessa direzione si poneva anche Europol a seguito della pronuncia *Tele2*: nel documento *Proportionate data retention for law enforcement purposes* e riportato dalla dottrina, emerge come «a data retention measure that is "targeted", as CJEU provides in the Digital Rights Ireland and Tele 2 Sverige rulings, is practically impossible, since the "potential relevance amongst data and the purposes pursued cannot be foreseen in advance". In this way, EUROPOL seems to provide for an interpretation that would "fit for law enforcement reality", where "restricted" data retention may still be considered to abide by the CJEU requirement as discussed above, since, in the opinion of EUROPOL, the subsequent access to the retained data must always be "targeted"», P. VOGIATZOGLOU, *Mass surveillance, predictive policing and the implementation of the CJEU and ECtHR requirement of objectivity*, in *European Journal of Law and Technology*, 1, 2019, p. 8. Come si richiamerà anche in seguito, la lettura di Europol portava ad identificare una "terza via", quella della conservazione "limitata" o "ristretta", dai connotati più ampi di quella "mirata" proposta dalla CGUE ma al contempo maggiormente garantista rispetto ad un regime di *bulk data retention*.

fosse stata considerata sotto il profilo della efficacia [74].

Accanto a questo dibattuto aspetto, si riproponevano poi, anche a seguito della sentenza *Tele2*, talune delle problematiche già emerse in passato: la difficile ricostruzione dei netti confini tra competenze proprie degli Stati membri, rispetto alle quali dunque non dovevano essere applicati i criteri individuati dalla giurisprudenza della CGUE, e ciò che invece rientrava nell'ambito di applicazione dell'UE; la rapida valutazione dell'idoneità dello strumento della *data retention* al raggiungimento dell'interesse legittimo – individuato nella lotta alla criminalità grave – [75]; la distinzione tra lesione del contenuto essenziale dei diritti in gioco a seconda che il trattamento dei dati riguardi il contenuto o i meri metadati, considerata piuttosto labile, se non incongruente, rispetto alla riconosciuta capacità di una lettura aggregata di metadati di fornire con precisione informazioni sulla vita privata degli utenti; la difficile determinazione del carattere di gravità dei reati, rispetto ai quali nulla veniva specificato da

[74] Cioè «without referring to any evidence which supported either the feasibility or utility of targeted retention», D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, cit., p. 14. Del resto, sullo specifico aspetto della legittimità ed utilità di una conservazione targettizzata, anche l'Avvocato generale Saugmandsgaard Øe nelle proprie Conclusioni relative al rinvio *Tele2* aveva mostrato significative perplessità: «Una limitazione sostanziale della portata di un obbligo generale di conservazione dei dati rischia di ridurre considerevolmente l'utilità offerta da tale regime nella lotta contro i reati gravi. Da una parte, diversi governi hanno sottolineato la difficoltà o addirittura l'impossibilità di determinare in anticipo i dati che possano presentare un collegamento con un reato grave. Pertanto, una siffatta limitazione rischia di escludere la conservazione di dati che potrebbero rivelarsi rilevanti ai fini della lotta contro i reati gravi. Dall'altra, come ha sostenuto il Governo estone, la criminalità grave è un fenomeno dinamico, capace di adattarsi agli strumenti investigativi di cui dispongono le autorità di contrasto. Pertanto, una limitazione a un'area geografica o a un mezzo di comunicazione determinati rischierebbe di provocare un trasferimento delle attività legate ai reati gravi verso un'area geografica e/o un mezzo di comunicazione non coperti da detto regime», para. 213-214.

[75] Sul punto, alcuni studiosi ritenevano preoccupante la sbrigativa analisi della CGUE: quest'ultima «did not base its ruling on evidence relating to the effectiveness of the instrument of the data retention. The ruling is rather based on a theoretical reasoning that data retention genuinely satisfies an objective of general interest», H. HIJMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 116 TFEU*, PHD Thesis, 2016, p. 223, disponibile all'indirizzo https://pure.uva.nl/ws/files/2676807/169421_DEFINTIEF_ZELF_AANGEPAS_full_text_.pdf.

parte dei giudici di Lussemburgo; o ancora, l'impatto di una pronuncia di incompatibilità con il diritto dell'UE delle normative nazionali in materia di conservazione dei metadati sulla validità degli elementi di prova ottenuti mediante tale strumento.

Dinnanzi a queste persistenti perplessità, le forti critiche riguardanti la più netta posizione della CGUE con riferimento ai regimi di *bulk data retention* nonché la rilevata difficoltà da parte degli Stati membri di inserire e rispettare i criteri indicati dalla giurisprudenza sovranazionale esaminata, avevano nuovamente portato all'emergere di una frammentarietà di approcci e reazioni a livello nazionale. Nella perdurante assenza di una normativa europea *ad hoc* in materia di conservazione e accesso ai metadati, il panorama venutosi a creare all'indomani della sentenza *Tele2* ben poteva essere così sintetizzato: «the vast majority of the Countries do not have targeted data retention rules within categories of location/traffic data, users/subscribers and means of communication (internet/telephone); one Country (DE) reported that it excludes some targeted users/subscribers from the retention obligation in the legislation that is to come into force in July 2017 (…); finally some countries reported that they do not have data retention laws for law enforcement purposes only, following the annulment of their previous laws by their constitutional/high courts in accordance with the DRD judgement (…). It can be concluded that none of the Countries have national legislation that obliges the targeted retention of data linked to specific persons or geographical locations» [76].

Similmente a quanto accaduto successivamente alla decisione *DRI* e nonostante le precisazioni e chiarimenti forniti nella sentenza *Tele2*, taluni Stati membri avevano dunque optato per non adottare una nuova disciplina normativa *ad hoc* in materia di *data retention* [77]; altri ancora

---

[76] EUROJUST, *Data retention regimes in Europe in light of the CJEU ruling of 21 December in Joined Cases C-203/15 and C-698/15*, 6 novembre 2017, reso parzialmente accessibile il 6 giugno 2019 (10098/17 Eurojust 91), p. 6.

[77] L'Austria, ad esempio, a seguito della dichiarazione di incostituzionalità della normativa di trasposizione della DRD da parte della *Verfassungsgerichtshof* (Corte costituzionale) del 27 giugno 2014 (sul punto si rimanda a M. FLORA, *The unlawfulness of data retention confirmed by the Court of Justice of the European Union and the Austrian*

avevano assistito ad un ulteriore intervento delle Corti nazionali volto a determinare la compatibilità con il diritto dell'UE o con la Costituzione nazionale delle disposizioni regolanti la conservazione e accesso ai metadati: è il caso di Francia, Belgio, Regno Unito, Estonia ma anche Italia, Repubblica Ceca e Portogallo; ciò che però consente di individuare ulteriori sottocategorie all'interno di questo folto gruppo è il diverso esito dell'intervento giurisprudenziale. Per i primi quattro Stati membri citati – seguiti poi anche da Germania e Irlanda – le perplessità e i dubbi interpretativi ed attuativi relativi ai principi delineati dalla CGUE avevano portato i giudici nazionali a formulare ulteriori rinvii pregiudiziali: riconoscendo la sussistenza di criticità nell'assetto normativo esistente, le Corti ritenevano di non poter risolvere le questioni ad esso presentate se non ottenendo chiarimenti dai giudici di Lussemburgo. Pur con talune differenze, che saranno più avanti oggetto di attenta analisi, i rinvii promossi giungevano tutti al medesimo esito, quello cioè di riconoscere da un lato l'esistenza di diverse possibili interpretazioni della sentenza *Tele2* e dall'altro la necessità che una univoca e decisa posizione dirimente venisse espressa a livello sovranazionale.

In Italia, Repubblica Ceca e Portogallo, invece, le Corti nazionali avevano riconosciuto la disciplina interna conforme al diritto dell'UE e alla Costituzione nazionale; in Italia, come si avrà modo di vedere, la Corte di Cassazione e alcune Corti di merito hanno più volte, negli ultimi anni, considerato le disposizioni in materia di *data retention* e accesso ai metadati compatibili con la Carta di Nizza e con l'interpretazione di essa fornita dalla giurisprudenza europea; similmente, in Repubblica Ceca la *Ústavní soud České republiky* (Corte costituzionale) aveva respinto il ricorso promosso dalla ONG Iuridicum Remedium volto ad ottenere la dichiarazione di illegittimità costituzionale della disciplina nazionale in materia di *data retention*[78]: sebbene già nel 2011 la medesima Corte avesse statuito l'incostituzionalità della normativa all'epoca vigente e adottata quale trasposizione nell'ordinamento interno della DRD, le stesse considerazioni non erano poi state ripetute con riferimento alla normativa

Constitutional Court, in *Journal of European Consumer and Market Law*, 3, 2015, p. 102 ss.) non si era poi dotata di una nuova legislazione specifica in materia.

[78] Si fa riferimento al caso P.US 45/17 del 14 maggio 2019.

successivamente adottata nel 2012, ritenuta invece proporzionata allo scopo di indagine e prevenzione del crimine, nonostante la natura indiscriminata e generalizzata della conservazione. Ancora, nel 2017, il *Tribunal Constitucional* portoghese aveva ritenuto la normativa nazionale n. 32/2008 del 17 giugno 2008, adottata quale implementazione della DRD, conforme ai diritti fondamentali tutelati dalla Costituzione portoghese [79].

Ciò che è possibile rilevare da tutte le reazioni nazionali sopra richiamate è una diffusa interpretazione c.d. "difensiva" della giurisprudenza delle CGUE finalizzata, cioè, ancora una volta, a far salva la compatibilità con la Carta di Nizza di una forma di conservazione generalizzata, alla quale nessuno Stato pareva disposto a rinunciare. Anche le Corti nazionali avevano infatti dimostrato di adottare un approccio cauto e "difensivo", appunto, laddove chiamate a vagliare le normative nazionali, talvolta non rilevando criticità o incompatibilità con il diritto dell'UE, talaltra invece rimettendo le delicate questioni emerse ai giudici di Lussemburgo, suggerendo a questi ultimi, come si vedrà nei casi inglese e belga, di rivedere o mitigare il proprio orientamento e i principi delineati, tenendo conto delle reali e ben evidenziate difficoltà applicative che le concrete reazioni degli Stati membri avevano posto in luce.

In conclusione, senza dubbio la giurisprudenza della CGUE sin qui analizzata «is increasingly building up a real and effective privacy shield to protect European values which are increasingly eroded by domestic legislation of Member States aiming to organize the fight against serious crime and terrorism» [80]. Nonostante questo positivo risultato nella dire-

---

[79] Sentenza 13 luglio 2017, n. 420/2017. Per una dettagliata analisi, si rimanda a T. VIOLANTE, *Data retention in Portugal*, in M. ZUBIK, J. PODKOWIK, R. RYBSKI (a cura di), *European Constitutional Courts towards data retention laws*, Springer, Berlino, 2020, p. 175 ss.

[80] X. TRACOL, *The judgement of the Grand Chamber dated 21 December 2016 in the two joint Tele2Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level*, in *Comupter Law & Security Review*, 33, 2017, p. 552. Similmente, vi era chi ravvisava nella pronuncia *Tele2* la volontà della CGUE di «prendere davvero sul serio l'esigenza di tutelare un nuovo *digital right to privacy*» (O. POLLICINO, *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*,

zione di un più attento bilanciamento tra esigenze securitarie e diritti fondamentali, non può tuttavia ignorarsi come, nel fornire dettagliati criteri e una sorta di vademecum per la regolamentazione dello strumento della *data retention*, «the Court of Justice is arguably engaging in an excercise which would appear more legislative than judicial in its character (…). The Court in effect constitutionalizes these detailed requirements. If such an approach was intended to serve as guidance for the legislature, this might be understandable. However, in the case of data retention, it appears to have had the contrary effect, inhibiting legislative action at EU and nation level» [81]. Ed è dunque da queste complesse ed articolate considerazioni che si comprende come il dibattito sulla disciplina della conservazione e accesso ai metadati fosse da ritenersi, anche all'indomani dell'importante sentenza *Tele2*, tutt'altro che concluso.

7. *L'art. 15 Direttiva* e-Privacy *sottoposto ancora una volta all'intervento chiarificatore della CGUE: la sentenza* Ministerio Fiscal *e i requisiti dell'accesso ai metadati conservati.*

Il primo rinvio pregiudiziale nel quale la CGUE, successivamente alla sentenza *Tele2*, si è nuovamente trovata a doversi pronunciare sull'in-

---

Roma TrE-Press, Roma, 2015, p. 7), tanto da giungere, secondo alcuni commentatori, all'esito di attribuire ai diritti alla riservatezza e alla protezione dei dati il rango di *super-rights.* Sul punto, come rilevato da O'Leary, «it could be asked whether arts 7 and 8 of EU Charter have emerged as the most powerful and far-reaching EU Charter tools in the ECJ's post-Lisbon armament? No other EU Charter provisions, not even the defense rights enshrined in arts 47 and 48 which had been the subject of extensive case law via the EU general principles route pre-Lisbon, seem to have had an equivalent impact. Some commentators refer critically to the ECJ's elevation of these rights into 'super-rights'while others appear to applaud this nomenclature», S. O'LEARY, *Balancing rights in a digital age*, cit., p. 87. Si pensi, ad esempio, all'approccio critico di Kuner avverso l'attribuzione di una eccessiva rilevanza ai diritti in analisi (C. KUNER, *A super right to data protection? The Irish Facebok case and the future of EU data transfer regulation*, in *LSE Blog*, 24 giugno 2014), mentre di opposto avviso è Scheinin (si legga M. SCHEININ, *Towards evidence-based discussion on surveillance*, in *European Constitutional Law Review*, 12, 2016, p. 347 ss.).

[81] D. FENNELLY, *Data retention: the life, death and afterlife of a directive*, cit., p. 17.

terpretazione dell'art. 15 Direttiva *e-Privacy*, è da ravvisarsi nel caso *Ministerio Fiscal*[82], avente ad oggetto primariamente la determinazione del carattere di gravità del reato, inteso quale requisito di grande rilievo per la garanzia della proporzionalità delle operazioni di accesso. Come già sottolineato, infatti, nel testo dell'art. 15 Direttiva *e-Privacy* si parlava ben più genericamente dello scopo di prevenzione, ricerca, accertamento e perseguimento dei reati, senza alcun accenno al carattere di gravità del reato, che veniva invece individuato unicamente dalla giurisprudenza della CGUE. Quest'ultima tuttavia non stabiliva indicazioni utili a determinare gli elementi da considerare al fine di affermare il carattere di gravità, così che tale profilo rimaneva alquanto problematico ed indefinito. Il giudice spagnolo sottoponeva per questo alla CGUE due questioni pregiudiziali, chiedendo *in primis* se la soglia di gravità potesse essere «individuata prendendo in considerazione unicamente la pena irrogabile per il reato oggetto di indagine o se sia inoltre necessario rilevare nella condotta criminosa particolari livelli di lesività nei confronti dei beni giuridici individuali e/o collettivi», para. 25; in secondo luogo, nel caso in cui la determinazione della gravità del reato sulla sola base della durata della pena fosse risultata conforme ai principi dell'UE, il giudice del rinvio chiedeva se essa fosse compatibile con il limite di tre anni di reclusione indicato dalla dibattuta normativa spagnola in materia[83].

---

[82] CGUE 2 ottobre 2018, C-207/16, *Ministerio Fiscal*.

[83] Anche ai fini di una corretta comprensione della pronuncia della CGUE, pare utile ricostruire brevemente i fatti che avevano condotto alla questione pregiudiziale promossa dall'*Audiencia Provincial de Tarragona* il 6 aprile 2016. Essa trae origine da un caso di rapina ai danni di un cittadino spagnolo che in quella occasione subiva anche il furto del proprio cellulare. Per risalire all'autore del reato, la polizia giudiziaria decideva di seguire proprio le tracce del telefono. Al fine di attivare una SIM e dunque aprire una utenza presso un fornitore di servizi di telecomunicazione, è necessario infatti fornire al *service provider*, oltre alle informazioni relative alla propria identità, anche il codice relativo all'identificatore internazionale di apparecchiature mobili, c.d. codice IMEI, che individua univocamente il dispositivo sul quale si intende attivare l'utenza stessa. La polizia pertanto decideva di ingiungere a tutte le maggiori compagnie telefoniche di verificare se nei propri *database*, contenenti i dati di attivazione di SIM, vi fosse un'utenza aperta utilizzando il codice IMEI del dispositivo rubato. Così facendo, la polizia avrebbe potuto risalire al numero telefonico e all'identità del soggetto che aveva attivato l'utenza sul telefono oggetto di furto e che poteva essere, presumibilmente, l'autore stesso del

Dinnanzi a tali precisi quesiti, la CGUE, con la decisione relativamente breve del 2 ottobre 2018, affrontava dapprima la preliminare questione dell'ambito di applicazione della Direttiva *e-Privacy.* Mentre i governi intervenuti ritenevano che la domanda di accesso ai dati, promossa da autorità nazionali di *law enforcement* avverso i fornitori di servizi di comunicazione elettronica rientrasse nell'esercizio dello *ius puniendi*, ricompreso nel novero delle attività escluse dalla disciplina della Direttiva 2002/58, ai sensi del suo art. 1, co. 3, i giudici di Lussemburgo scioglievano ancora una volta questo delicato e dibattuto nodo con grande velocità, riproponendo lo stesso ragionamento seguito nella pronuncia *Tele2*: le normative nazionali adottate sulla base della deroga sancita dall'art. 15 Direttiva *e-Privacy* vengono per questo stesso fatto "attirate" nell'ambito di applicazione della Direttiva, anche nel caso in cui esse «rimandino ad attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati» (para. 34) e persino quando le finalità perseguite dalle leggi interne coincidano sostanzialmente con quelle indicate nel citato art. 1, co. 3. Le operazioni di accesso, poi, al pari di quelle di conservazione, prevedono un trattamento dei dati da parte degli operatori dei servizi di telecomunicazione e sono pertanto da considerarsi come attività svolte da attori privati e regolate dal diritto dell'UE. Viene, in altre parole, riconfermata la «concezione unitaria che considera i due momenti della "conservazione" e dell'"accesso" come espressione di un atto invero complessivamente unitario» [84], ribadendo così quella interpretazione – da alcuni autori [85] ritenuta estensiva – dell'art. 15 già proposta sin dalla *Tele2*, senza aggiungere peraltro ad essa ulteriori elementi chiarificatori rispetto al passato [86].

---

furto o comunque una persona a conoscenza di informazioni utili alle indagini. Proprio dai dubbi e dalle divergenti interpretazioni circa la sussistenza e la correttezza del requisito di "gravità" del reato, necessario al fine di legittimare la richiesta di accesso ai metadati conservati, traeva origine il rinvio pregiudiziale in esame.

[84] O. POLLICINO, M. BASSINI, *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 9 gennaio 2017, p. 5.

[85] D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* cit., p. 10.

[86] L'Avvocato generale aggiungeva sul punto un ulteriore spunto di riflessione di

A seguito di queste pur rilevanti preliminari questioni che, come si vedrà, saranno nuovamente oggetto di rinvio pregiudiziale da parte del Regno Unito, la CGUE provvedeva a riformulare il quesito proposto dai giudici spagnoli: in particolare, prima di stabilire quali elementi – materiali o formali – dovessero essere utilizzati per determinare il carattere di gravità del reato, secondo i giudici risultava necessario valutare se, al fine di essere considerata giustificata, l'ingerenza nei diritti fondamentali fosse tale da richiedere il perseguimento di un reato di carattere grave [87].

---

grande rilievo, per quanto non seguito poi dalla CGUE: Saugmandsgaard Øe, infatti, aveva affermato nelle sue Conclusioni la necessità di distinguere da una parte i dati personali trattati «*direttamente* nell'ambito delle attività – di natura sovrana – dello Stato in un settore rientrante nel diritto penale e, dall'altra, quelli trattati nell'ambito delle attività – di natura commerciale – di un fornitore di servizi di comunicazione elettronica che sono *successivamente* utilizzati dalle autorità statali competenti», para. 47. Riferendosi dunque ad attività sovrane dello Stato come a quelle che si «riferiscono alle funzioni riservate allo Stato o ai suoi apparati, che esso non può delegare ad enti privati, in particolare, quelle relative alla giustizia, alla polizia o alle forze armate» (nota 43), l'Avvocato generale riteneva tra di esse rientranti il trattamento dei dati da parte di «autorità di polizia o giudiziarie al fine di ricercare gli autori di reati, ad esempio i dati raccolti e analizzati durante un'intercettazione di conversazioni telefoniche effettuata da agenti di polizia su richiesta di un giudice istruttore», nota 44. Ciò che risulta chiaro, in ogni caso, anche dal ragionamento seguito dall'Avvocato generale, è la complessità e delicatezza di tale profilo e delle conseguenze che ne derivano. Da un lato, ricomprendere le attività riguardanti l'accesso all'interno dell'ambito di applicazione della Direttiva *e-Privacy* permette alla Corte di pronunciarsi sul punto e di estendere il bilanciamento con i diritti fondamentali anche sul fronte di una operazione certamente invasiva dei diritti alla riservatezza e alla protezione dei dati, quale l'accesso. Dall'altro, pare altrettanto vero che il confine tra le attività ricomprese nella Direttiva e quelle invece escluse si presenta come estremamente sottile ed incerto, tanto da spingere il Regno Unito a promuovere un apposito rinvio sul tema, soprattutto con riferimento alla materia della sicurezza nazionale e delle operazioni di raccolta, conservazione e trattamento di dati svolte da agenzie di intelligence.

[87] «Con le sue due questioni (…) il giudice del rinvio chiede, in sostanza, se l'articolo 15, par. 1, della Direttiva 2002/58, letto alla luce degli articoli 7 e 8 della Carta, debba essere interpretato nel senso che l'accesso delle autorità pubbliche ai dati che mirano all'identificazione dei titolari di carte SIM attivate con un telefono cellulare rubato, come il cognome, il nome e se del caso l'indirizzo di tali titolari, comporta un'ingerenza nei diritti fondamentali di questi ultimi, sanciti dai suddetti articoli della Carta, che presenta una gravità tale da dover limitare il suddetto accesso, in materia di prevenzione,

Veniva così stabilito come, sulla base del principio di proporzionalità, solo la lotta alla criminalità connotata da gravità fosse in grado di legittimare un'ingerenza significativa nei diritti alla riservatezza e alla protezione dei dati. Ne derivava, ragionando a contrario, che, in caso di intrusione non grave nella sfera privata, l'accesso non doveva considerarsi vincolato alla sola repressione di crimini gravi. Ebbene, se nel caso *Tele2* la Corte aveva ritenuto sussistente una ingerenza profonda nei diritti fondamentali poiché l'accesso promosso aveva ad oggetto una mole indiscriminata di dati che «considerati nel loro insieme, consentono di trarre conclusioni precise sulla vita privata delle persone i cui dati sono oggetto di attenzione» (para. 99); nel caso in esame, invece, le operazioni di accesso riguardavano solo un ristretto numero di dati – quelli riferibili all'utenza telefonica attivata usando il codice IMEI del telefono rubato – ed una limitata tipologia di dati, cioè unicamente i dati identificativi – e non anche quelli di traffico o ubicazione –, peraltro riferiti ad uno specifico e breve periodo di tempo di dodici giorni. Un siffatto accesso – che si poteva quasi definire *targettizzato* e mirato quanto alla quantità, tipologia dei dati e arco temporale coperto dall'accesso – non era in grado di consentire una precisa ricostruzione della vita privata dei soggetti interessati e finiva dunque col rappresentare una ingerenza di carattere solo lieve nei diritti fondamentali di cui agli artt. 7 e 8 della Carta di Nizza. Giunta a tale conclusione ed applicando quel principio di proporzionalità prima individuato, la Corte arrivava a ritenere che l'intrusione lieve rilevata nel caso specifico in esame non fosse tale da richiedere, al fine di essere giustificata, il perseguimento di un crimine grave (para. 63). Alla luce di queste considerazioni, i giudici concludevano così la loro pronuncia e non procedevano ulteriormente alla determinazione dei criteri volti a stabilire la natura grave del reato, come richiesto dal giudice del rinvio.

Ebbene, pur facendo attenzione a non individuare nella pronuncia analizzata una sorta di *revirement* o di passo indietro della Corte rispetto al requisito della gravità del reato [88], è evidente che la riformulazione dei

---

ricerca, accertamento e perseguimento dei reati, alla lotta contro la criminalità grave e, in caso affermativo, sulla base di quali criteri dovrebbe essere valutata la gravità dell'infrazione in questione», para. 48.

[88] Bisogna infatti tenere in considerazione le differenze che distinguono i due casi

quesiti pregiudiziali promossi ha di fatto portato la Corte ad esimersi, secondo alcuni autori con una scelta "tattica" [89], dal prendere una posizione sulla ben più delicata e complessa questione dell'individuazione dei criteri determinanti la gravità del reato [90]. Con la pronuncia *Ministerio Fiscal* i giudici di Lussemburgo non hanno dunque risolto gli interrogativi emersi nell'era post-*Tele2* relativamente alla gravità del reato come requisito per l'accesso ai dati [91], pur chiarendo taluni aspetti di rilievo e slegando

giurisprudenziali, con particolare riferimento alle diverse tipologie di accesso e al grado di invasività che esse comportano, tali da non consentire una equiparazione e un pieno parallelismo. Sul punto si rimanda a D. DEL VESCOVO, *L'accesso delle autorità pubbliche a dati personali di natura meramente identificativa non costituisce ingerenza grave nei diritti fondamentali degli interessati*, in *Amministrativamente – Rivista di diritto amministrativo*, 11-12, 2018, p. 12 ss.

[89] L. WOODS, *Mobile phone theft and EU e-privacy law: the CJEU clarifies police powers*, in *EU Law Analysis*, 4 ottobre 2018. Della stessa opinione Tracol, che afferma: «through its re-phrasing of the questions posed by the referring Court, the Grand Chamber carefully avoided and quite notably sidestepped the tricky issues of defining the notion of serious crime and determining whether it is an autonomous concept of EU law», X. TRACOL, *Ministerio Fiscal: access of public authorities to personal data retained by providers of electronic communications services*, in *European Data Protection Law Review*, 1, 2019, p. 134. L'Avvocato generale, nelle sue Conclusioni, invece, entrava più nello specifico sotto questo profilo, proponendo risposte alle questioni promosse dai giudici del rinvio quanto al criterio di gravità del reato; per una analisi di tali considerazioni, sia consentito il rimando a G. FORMICI, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, in *Osservatorio AIC*, 3, 2018, p. 433 ss.

[90] Secondo Celeste, il fatto che i giudici non abbiano potuto spingersi a vagliare alcuni aspetti di grande rilievo quali la legittimità della disciplina sulla conservazione dei dati spagnola o gli elementi che determinano il carattere di gravità di un reato, dovendosi attenere al *petitum*, è diretto derivato della «very architecture of the European judicial system, which does not allow the Court of Justice to go beyond the questions referred by national courts and prevents it from quashing national legislation, slows down ad fragments the effective application of the data retention principles within the member states. This situation increases the state of uncertainty at national level, amplifies national divergences, and ultimately appears to be in contrast with the proactive approach that the Court adopted so far in the data retention saga», E. CELESTE, *The Court of Justice and the ban on bulk data retention*, cit., p. 145.

[91] Tale era l'auspicio di alcuni autori: non a caso Artemiou sceglieva emblematicamente e forse provocatoriamente di titolare il proprio commento alle Conclusioni del-

dal rispetto di tale criterio "rafforzato" alcune tipologie di indagini ristrette nel tempo e limitate a particolari categorie di dati. Bisognerà quindi attendere i successivi rinvii pregiudiziali promossi dai giudici inglese, belga, francese, estone, tedesco e irlandese – solo più recentemente da quello italiano – per vedere la Corte nuovamente impegnata a fornire importanti e più precise indicazioni utili a chiarire il difficile bilanciamento tra interessi securitari e tutela dei diritti fondamentali.

8. *Le importanti sentenze* La Quadrature du Net, Privacy International *e* H.K.*: la* data retention saga *al capolinea?*

8.1. *La delicata determinazione dell'ambito di applicazione del diritto dell'UE.*

Le concrete e significative difficoltà attuative nonché i dubbi interpretativi già emersi all'indomani della sentenza *Tele2* erano ben presto sfociati, come si è anticipato, in numerosi rinvii pregiudiziali susseguitisi a partire dal 2017: si tratta dei rinvii promossi dall'*Investigatory Powers Tribunal* del Regno Unito, dal *Conseil d'État* francese (Consiglio di Stato), dalla *Cour constitutionnelle* belga (Corte costituzionale), dalla *Riigikohus* estone (Corte Suprema), dalla *Bundesverwaltunsgericht* tedesca (Corte amministrativa federale), dalla *Supreme Court* irlandese e, solo in tempi estremamente recenti, dal Tribunale di Rieti italiano. I quesiti promossi, pur nelle loro differenti sfumature ed accenti, erano tutti attinenti all'interpretazione dell'art. 15 della Direttiva *e-Privacy* e si ponevano qua-

---

l'Avvocato generale nel caso *Ministerio Fiscal* "The way out of Digital Rights Ireland" (E. ARTEMIOU, *The way out of Digital Rights Ireland*, in *CiTiP Law Blog*, 19 giugno 2018). In tale rinvio pregiudiziale l'autrice intravedeva l'occasione per la Corte di poter indicare alle autorità nazionali un modo legittimo per accedere ai dati conservati dai fornitori di servizi di comunicazione, fornendo criteri chiari e concretamente realizzabili: «In conclusion, it is safe to say that the Court of Justice of the European Union has raised the bar in terms of protection of personal data, to a point where it seemed impossible to process such data for prosecution purposes lawfully. This is a unique opportunity to illustrate practically if the police can request access to personal data retained by telecommunication service providers for the purposes of criminal investigation but should without a doubt be framed carefully by the Court».

le riflesso della forte preoccupazione – quando non vera e propria resistenza – che i Governi degli Stati membri dai quali i rinvii provenivano avevano espresso rispetto ad una integrale e letterale attuazione dei requisiti affermati nelle sentenze *DRI*, *Tele2* e *Ministerio Fiscal*, che avrebbero finito col privare le autorità nazionali di uno strumento di fondamentale rilievo per la garanzia della sicurezza nazionale e la lotta alla criminalità grave. Per questo, come ben riassunto dall'Avvocato generale Campos Sanchez-Bordona nelle sue Conclusioni del 15 gennaio 2021, relative ai rinvii promossi dalle Corti francese e belga, «la maggioranza degli Stati membri che hanno presentato osservazioni invitano la Corte a chiarire, temperare o addirittura riconsiderare vari aspetti della sua giurisprudenza in materia (...). Sarebbero sufficienti norme rigorose sull'accesso ai dati conservati dai fornitori di servizi di comunicazione elettronica, che possano compensare, in qualche modo, la gravità dell'ingerenza che la conservazione generalizzata e indifferenziata di tali dati comporta», para. 70-71 [92].

Di fronte a queste chiare e decise posizioni, da più parti espresse, la CGUE ha pronunciato nel medesimo giorno, il 6 ottobre 2020, due importanti sentenze, *La Quadrature du Net* [93] e *Privacy International* [94], rela-

---

[92] Del resto, è interessante notare come nel corso dell'udienza pubblica tenutasi il 9 settembre 2019 con riferimento ai rinvii inglese, francese e belga, anche il GEDP, piuttosto sorprendentemente, avesse espresso perplessità e dubbi quanto alla concreta realizzabilità di forme di conservazione mirata: nelle *Pleading notes* si legge infatti come «in the specific context of retention of electronic communications data, it might not be possible to identify in advance those data subjects (or categories of data subjects) whose information may at some point in the future become part of a criminal investigation, for example victims of serious crime», p. 11. Così, pur negando la compatibilità di un regime di *bulk data retention* con il diritto dell'UE, il GEPD suggeriva l'adozione di una forma di conservazione «limited yet effective», identificata in una conservazione circoscritta a specifiche categorie di dati ed accompagnata da rafforzate salvaguardie attinenti all'accesso ai dati medesimi. In questo punto, dunque, venivano in parte riprese quelle considerazioni espresse da Europol all'indomani della sentenza *Tele2* circa la già richiamata possibilità di addivenire ad una "terza via" intermedia tra conservazione mirata e generalizzata.

[93] CGUE 6 ottobre 2020, C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs e al.*

[94] CGUE 6 ottobre 2020, Cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net e al. c. Premier Ministre e al.*

tive rispettivamente ai rinvii pregiudiziali promossi dai giudici francese e belga, la prima, e da quello inglese, la seconda.

Mentre le vicende che hanno condotto le Corti nazionali alla formulazione dei rinvii verranno ampiamente trattate nei Capitoli specificamente dedicati alle vicende normative e giurisprudenziali che hanno segnato Belgio e Regno Unito, particolare attenzione vuole invece ora essere assegnata agli esiti del tanto auspicato intervento chiarificatore della CGUE che possono essere utilmente ricondotti a quattro argomenti principali: la determinazione dell'ambito di applicazione del diritto dell'UE – in particolare della Direttiva *e-Privacy* –; la possibilità da parte degli Stati membri di adottare normative che autorizzino una *blanket data retention* per scopi di sicurezza nazionale; la possibilità di prevedere una conservazione generalizzata per finalità di sicurezza pubblica – nello specifico si fa riferimento alla lotta alla criminalità grave –; la determinazione delle categorie di dati che debbono sottostare al rispetto dei criteri stabiliti nella sentenza *Tele2* (c.d. requisiti *Tele2*).

Prendendo dunque abbrivio dal primo degli argomenti trattati dalla CGUE, la questione relativa all'ambito di applicazione della Direttiva *e-Privacy* risultava, come si ricorderà, essere oggetto di un acceso scontro tra Stati membri e CGUE, trascinatosi sin dalla pronuncia *DRI*. I Governi intervenuti nella causa *La Quadrature du Net* – nello specifico quello francese, ceco, estone, irlandese, cipriota, polacco, svedese, ungherese, inglese – avevano infatti con forza sostenuto come la Direttiva richiamata – e dunque anche le relative limitazioni e criteri ad essa connessi – non potesse applicarsi a normative, come quelle oggetto dei rinvii, finalizzate alla salvaguardia della sicurezza nazionale: quest'ultima materia era del resto chiaramente assegnata alla competenza esclusiva degli Stati membri ai sensi dell'art. 4, co. 2, TUE. Ne derivava, a parere dei Governi intervenuti, che in tale ambito una forma di conservazione dei metadati dovesse risultare libera dal rispetto dei rigidi requisiti *Tele2*, pur dovendo comunque sottostare ai limiti dettati dalla Convenzione EDU e dall'interpretazione di essa fornita dalla Corte EDU.

I giudici di Lussemburgo, nel chiarire in maniera definitiva questo primo e dibattuto punto, non si sono limitati a citare solo le considerazioni già espresse nella previa giurisprudenza ma hanno anche chiarito, per la prima volta ed espressamente, la questione attinente allo specifico

ambito della sicurezza nazionale. Nel fare questo, la CGUE ha innanzitutto respinto quella lettura della Direttiva *e-Privacy* – nonché dello stesso art. 4 TUE – che mirava ad escludere dall'ambito di applicazione del diritto dell'UE qualsiasi normativa nazionale che facesse richiamo a scopi di tutela della sicurezza nazionale [95]. In particolare, le "attività dello Stato" nei settori del diritto penale, della difesa, della sicurezza dello Stato, che venivano escluse dall'ambito di applicazione della Direttiva 2002/58 ai sensi del suo art. 1, co. 3, dovevano intendersi come riferite unicamente ad «attività proprie degli Stati o delle autorità statali, estranee ai settori di attività dei privati», para. 92. Poiché dunque le normative nazionali adottate in deroga all'obbligo generale di cancellazione dei metadati disciplinavano l'attività di fornitori di servizi di telecomunicazione, imponendo loro una forma di conservazione o trasmissione dei dati raccolti nell'erogazione del proprio servizio, esse non potevano essere considerate rientranti nella definizione di «attività proprie dello Stato» [96]. Nella sentenza *Privacy International* poi i giudici di Lussemburgo precisavano anche che costituisce una operazione di trattamento dei dati ad opera di *service providers* sia una misura che impone la conservazione dei metadati sia una misura che impone di accordare alle autorità nazionali competenti la trasmissione e l'accesso ai dati stessi; «ne consegue che una comunicazione di dati personali mediante trasmissione, così come una conservazione di dati o qualsiasi altra forma di messa a disposizione, configura un trattamento ai sensi dell'art. 3 della Direttiva 2002/58 e, di conseguenza, rientra nell'ambito di applicazione di tale direttiva», para. 41. Questo profilo rappresenta uno degli aspetti maggiormente innovativi della pronuncia richiamata, se non altro per la chiarezza delle affermazioni promosse che non lasciano adito a differenti interpretazioni: l'obbligo di tra-

[95] «La mera circostanza che una misura nazionale sia stata 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», para. 99.

[96] «Quando gli Stati membri adottano direttamente misure che derogano alla riservatezza delle comunicazioni elettroniche, senza imporre obblighi di trattamento ai fornitori di servizi di tali comunicazioni, la tutela dei dati delle persone interessate rientra non già nell'ambito di applicazione della direttiva 2002/58 ma in quello del solo diritto nazionale», para. 48, sentenza *Privacy International*.

smissione di dati – quale quello imposto dalla normativa inglese oggetto del rinvio promosso – veniva per la prima volta parificato alla conservazione, tanto sotto il profilo della determinazione dell'ambito di applicazione, quanto sotto quello della applicazione ad essa dei requisiti *Tele2*.

8.2. *I limiti dello strumento di conservazione generalizzata e l'inedita distinzione tra sicurezza nazionale e sicurezza pubblica.*

I giudici di Lussemburgo si sono poi più ampiamente dedicati all'interpretazione dell'art. 15 Direttiva *e-Privacy* e alla possibilità di imporre, sulla base di tale disposizione, forme di conservazione generalizzata ed indiscriminata di metadati.

Pur ribadendo concetti già ampiamente espressi nella previa giurisprudenza, sin dalla *DRI*, attinenti alla invasività della conservazione di metadati nonché all'idoneità dello strumento della conservazione al raggiungimento dell'interesse legittimo, è proprio con riguardo al vaglio di proporzionalità che emerge una rilevante novità: veniva infatti stabilita una inedita distinzione tra disciplina della *data retention* volta alla garanzia della sicurezza nazionale e conservazione finalizzata invece alla salvaguardia della sicurezza pubblica e lotta alla criminalità. Mentre nelle previe sentenze *Tele2* e *Ministerio Fiscal* la CGUE non aveva mai specificamente o approfonditamente trattato il tema [97], nella pronuncia in esame i giudici paiono in parte accogliere le forti istanze avanzate dagli Stati membri e dalle autorità di *law enforcement*, che avevano ribadito più volte e in maniera decisa l'importanza dello strumento della *data retention* generalizzata ed indiscriminata ai fini di garanzia della sicurezza nazionale. È proprio unicamente con riferimento a quest'ultima finalità che i giudici di Lussemburgo hanno previsto una eccezione, pur circostanziata,

[97] È la stessa CGUE ad ammetterlo: «l'obiettivo di salvaguardia della sicurezza nazionale, evocato dai giudici del rinvio e dai governi che hanno presentato osservazioni, non è ancora stato specificamente esaminato dalla Corte nelle sentenze che interpretano la direttiva 2002/58», para. 134. L'unico accenno svolto dalla CGUE alla possibilità di adozione di un regime derogatorio per finalità di sicurezza nazionale può essere rinvenuto solo nella pronuncia *Tele2* al para. 119, nel quale viene considerato legittimo un accesso più ampio e meno targettizzato laddove sussista l'esigenza di proteggere gli interessi vitali della sicurezza nazionale minacciati da attività di terrorismo.

alla dichiarata incompatibilità della *bulk data retention* con la Carta di Nizza e il diritto dell'UE. Se la garanzia della sicurezza nazionale, di competenza esclusiva degli Stati membri, veniva così considerata corrispondente «all'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» (para. 135 della sentenza *La Quadrature du Net*), questo obiettivo risultava superiore rispetto a quello della lotta alla criminalità grave e di tutela della sicurezza pubblica in generale. Dalla superiorità e maggiore importanza di questo scopo derivava pertanto «l'idoneità a giustificare misure che comportino ingerenze nei diritti fondamentali più gravi di quelle che potrebbero giustificare altri obiettivi», para. 136. Pertanto, l'art. 15 Direttiva *e-Privacy* non veniva considerato contrario «in linea di principio, a una misura legislativa che autorizzi le autorità competenti ad imporre ai fornitori di servizi di comunicazione elettronica di procedere alla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione di *tutti gli utenti dei mezzi di comunicazione elettronica per un periodo limitato, se ricorrono circostanze sufficientemente concrete che consentono di ritenere che lo Stato membro affronti una minaccia grave per la sicurezza nazionale che si rivela reale e attuale o prevedibile*. Anche se una misura siffatta riguarda, in maniera indifferenziata, tutti gli utenti di mezzi di comunicazione elettronica senza che questi ultimi sembrino, a prima vista, presentare alcun collegamento (…) con una minaccia per la sicurezza nazionale di tale Stato membro, si deve tuttavia considerare che l'esistenza di una simile minaccia *è idonea, di per sé, a stabilire detto collegamento*», para. 137, enfasi aggiunta. Il citato paragrafo, che si è voluto riportare integralmente per la sua centrale importanza, fissava dunque la possibilità di impiegare strumenti di *bulk data retention* per le specifiche necessità di tutela della sicurezza nazionale, pur stabilendo limiti e condizioni ben precise: l'obbligo di conservazione in capo a fornitori privati può assumere carattere generalizzato e indiscriminato purché tale ingiunzione a) sia temporalmente limitata allo stretto necessario, ovvero non superi un termine di tempo prevedibile, pur potendo essere soggetta a rinnovo in caso di persistenza

della minaccia; b) sia accompagnata da garanzie rigorose finalizzate a proteggere i dati dal rischio di abusi; c) non abbia carattere sistematico; d) sia oggetto di un controllo effettivo da parte di un giudice o di un organo amministrativo indipendente «la cui decisione sia dotata di efficacia vincolante, diretto ad accertare la sussistenza di una delle suddette situazioni nonché il rispetto delle condizioni e della garanzie che devono essere previste», para. 139.

I giudici di Lussemburgo si sono concentrati poi sull'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati. Ebbene sotto questo profilo sono state sostanzialmente confermate le condizioni già espresse nella previa giurisprudenza, che ben possono essere riassunte in questa chiara affermazione: «una normativa nazionale che prevede la conservazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione, ai fini della lotta alle forme gravi di criminalità, travalica i limiti dello stretto necessario e non può essere considerata giustificata in una società democratica, così come richiede l'art. 15 della direttiva 2002/58 letto alla luce degli artt. 7, 8, 11 e 52 della Carta», para. 141. La *bulk data retention* rimaneva, dunque, per queste finalità, una misura eccessivamente invasiva e non limitata allo stretto necessario, così che l'unica forma di conservazione in grado di superare il vaglio di proporzionalità veniva nuovamente individuata nella *conservazione mirata* (*targeted* o *ciblée*) ovvero in quella forma di conservazione di metadati ristretta e delimitata sotto il profilo delle categorie di dati interessati, dei mezzi di comunicazione, delle persone coinvolte e della durata della conservazione stessa (para. 147), nonché motivata da una connessione, almeno indiretta, tra i dati conservati e gli atti di criminalità grave (para. 148). Nonostante le critiche e i dubbi avanzati dal GEPD e dall'Avvocato generale quanto all'impiego di forme di *targeted data retention* e al rischio che ciò risulti in forme di discriminazione, i giudici confermavano il criterio geografico quale elemento cardine per l'attuazione di una conservazione mirata: esso deve essere determinato valutando il livello di rischio di preparazione o commissione di atti di criminalità grave in uno specifico luogo – caratterizzato ad esempio da un numero elevato di atti di criminalità o esposto a tale rischio in quanto luogo o infrastruttura frequentata da molte persone o perché luogo strategico quale aeroporti e stazioni –; anche il criterio temporale ovvero la previsione di una durata limitata allo

stretto necessario – salvo possibilità di rinnovo in caso di persistente necessità di procedere a conservazione – veniva riconosciuto quale ulteriore importante elemento chiave per garantire una conservazione mirata [98].

Sebbene il profilo di maggior interesse e novità delle pronunce in esame sia certamente da ravvisarsi nella distinzione, sopra analizzata, dell'esito del vaglio di proporzionalità a seconda della finalità perseguita, si vogliono comunque sinteticamente richiamare ulteriori profili di rilievo affrontati dalla CGUE. Concentrando l'attenzione sulla disciplina dell'accesso, accanto alla riconferma dei criteri e requisiti già individuati nella previa giurisprudenza, i giudici di Lussemburgo hanno svolto, in particolar modo nella sentenza *Privacy International*, una considerazione importante: la disciplina del Regno Unito – da cui il rinvio traeva origine – stabiliva l'obbligo in capo ai fornitori di servizi di telecomunicazione di trasmettere i metadati in maniera generalizzata ed indiscriminata alle agenzie di sicurezza e di *intelligence* nazionali, le quali poi raccoglievano e conservavano le informazioni in apposite banche dati finalizzate allo svolgimento di trattamenti ed analisi di massa automatizzate. In tale contesto la CGUE ha affermato l'equivalenza tra accesso e trasmissione, così che «una normativa che consente una trasmissione generalizzata e indifferenziata dei dati alle autorità pubbliche implica un accesso generale» para. 80. Un simile regime di accesso, anche qualora si sostanzi in analisi meramente automatizzate, era stato considerato privo di qualsiasi nesso, indiretto o remoto, con l'obiettivo perseguito, nonché di criteri oggettivi e condizioni sostanziali e procedurali in grado di disciplinare l'utilizzo delle informazioni così ottenute: ne derivava che un simile accesso generalizza-

[98] Non veniva pertanto accolta, né in realtà veniva svolto alcun riferimento in merito alla possibilità di adottare una "terza via" tra quella *mirata* e quella *generalizzata*, individuata nella già richiamata conservazione *limitata* (*restricted* o *limitée*) prospettata da Europol e ribadita dal Consiglio nell'ambito della rinnovata discussione sulla adozione di una normativa europea *ad hoc* in materia di *data retention*, di cui si dirà in seguito. Questa ulteriore tipologia intermedia risultava fondata su una limitazione della conservazione a specifiche categorie di dati, oggettivamente necessarie per la salvaguardia della sicurezza, nonché a certi tipi di fornitori e di servizi, individuati sulla base di una connessione tra *retention* e obiettivo da raggiungere: una simile forma di conservazione sarebbe così stata in grado di escludere dall'obbligo di conservazione piccoli fornitori di servizi o ancora i dati di soggetti le cui attività risultavano coperte da segreto professionale.

to non poteva essere considerato limitato a quanto strettamente necessario. Se questa equivalenza "trasmissione-accesso" rappresenta una precisazione dagli attesi effetti dirompenti sulle discipline nazionali, soprattutto quelle regolanti l'attività di autorità di intelligence, un ulteriore profilo di maggiore chiarezza e specificazione rispetto alla previa giurisprudenza è emerso con riferimento a due particolari categorie di dati: gli indirizzi IP e i dati relativi all'identità civile degli utenti (c.d. dati identificativi). A parere dei giudici di Lussemburgo, infatti, queste informazioni presentano un grado di sensibilità inferiore rispetto agli altri metadati (quali i dati di traffico e di ubicazione), poiché non consentono di ricostruire, da soli, abitudini o relazioni sociali degli utenti. Sulla base di tali considerazioni dunque, una normativa nazionale che prevede la conservazione generalizzata di indirizzi IP non può considerarsi, in linea di principio, contraria all'art. 15 Direttiva *e-Privacy* purché questa possibilità sia limitata alla sola lotta avverso forme gravi di criminalità, abbia una durata limitata e sia oggetto di rigorose garanzie. Quanto ai dati relativi all'identità, conformemente a ciò che era stato affermato nella sentenza *Ministerio Fiscal*, essi risultano in una ingerenza lieve nella sfera privata tale da non richiedere che normative nazionali disciplinanti la loro conservazione siano limitate al rispetto dei criteri stabiliti nella pronuncia *Tele2*, ben potendosi così prevedere per tali sole informazioni una *bulk data retention* anche finalizzata alla repressione di reati non gravi.

Infine, l'ultimo profilo di grande interesse che si vuole qui evidenziare[99] è da rilevarsi nella posizione espressa dalla CGUE circa la questione,

[99] Merita comunque sottolineare come la sentenza *La Quadrature du Net* abbia trattato anche l'ulteriore tema dell'analisi automatizzata di metadati e della raccolta in tempo reale di dati relativi a traffico ed ubicazione, che pare tuttavia di minor interesse nel contesto della presente disamina. Riassuntivamente, comunque, si può evidenziare come la tematica dell'analisi automatizzata e della raccolta in tempo reale fosse attinente prevalentemente al rinvio francese, nel quale il giudice chiedeva se l'art. 15 Direttiva 2002/58 dovesse essere letto nel senso di ostare ad una normativa nazionale che imponeva ai fornitori di servizi di telecomunicazione l'attuazione sulle proprie reti di misure volte a consentire l'analisi automatizzata e la raccolta in tempo reale di metadati senza che le persone interessate ne fossero a conoscenza. Tali norme comunque non prevedevano obblighi di conservazione in capo ai fornitori di servizi: mentre l'analisi automatizzata era volta ad individuare, mediante filtraggio con parametri prestabiliti, una connes-

posta dalla *Cour Constitutionnelle* belga, relativa alla possibilità di limitare nel tempo gli effetti della dichiarazione di illegittimità di una normativa in materia di *data retention* (para. 213). Tale questione è estremamente delicata: nella maggior parte dei casi, infatti, i dati conservati rappresentano elementi di prova di grande rilievo nei processi penali, così che l'illegittimità della normativa sulla cui base i dati stessi sono stati raccolti o ottenuti potrebbe compromettere gravemente procedimenti di estrema importanza per la sicurezza pubblica. Sotto questo profilo la CGUE ha stabilito che il giudice nazionale non può limitare nel tempo gli effetti di una dichiarazione di incompatibilità delle normative nazionali in materia di *data retention* rispetto al diritto dell'UE; ciò implicherebbe infatti la persistenza dell'obbligo di conservazione in capo ai fornitori di servizi e dunque il protrarsi di ingerenze gravi nei diritti fondamentali degli utenti (para. 219). I giudici di Lussemburgo hanno nondimeno precisato che la determinazione dell'ammissibilità di informazioni ed elementi di prova ottenuti mediante una conservazione contraria al diritto dell'UE spetta unicamente al diritto nazionale. Ciò, pur precisando che il giudice nazionale, dinnanzi ad un procedimento penale basato su elementi di prova ottenuti in violazione della Direttiva *e-Privacy*, non potrà tenere conto di

---

sione in grado di rivelare una minaccia terroristica, la raccolta in tempo reale riguardava solamente una o più persone già individuate come potenzialmente connesse ad una minaccia terroristica. Tali normative dunque si distinguevano chiaramente e significativamente da una forma di *bulk data retention* pur fondandosi comunque sull'obbligo di trattamento generalizzato tramite l'uso di un processo automatizzato. Per tale ragione e in considerazione della gravità dell'ingerenza perpetrata, i giudici di Lussemburgo ritenevano un simile trattamento come proporzionato solo: a) laddove finalizzato a fronteggiare una minaccia grave per la sicurezza nazionale, reale e attuale o prevedibile; b) limitato allo stretto necessario sotto il profilo temporale; oggetto di controllo di un giudice o di un organo amministrativo indipendente; c) laddove i modelli e criteri prestabiliti per il trattamento automatizzato fossero affidabili, specifici, non discriminatori e non fondati sull'utilizzo di dati sensibili; d) qualsiasi risultato positivo fosse sottoposto a riesame individuale con strumenti non automatizzati (para. 180-182). Quanto poi alla raccolta di dati di traffico e di ubicazione in tempo reale, essa poteva essere effettuata solo per scopi di prevenzione del terrorismo e solo nei confronti di persone rispetto alle quali esisteva già un sospetto validamente motivato da criteri oggettivi; tali operazioni dovevano poi risultare sottoposte al controllo preventivo di un giudice o di un organo amministrativo indipendente.

queste informazioni qualora i sospettati non siano in grado di «dedurre efficacemente in merito a un mezzo di prova che rientra in un settore che esula dalla competenza del giudice e che è fondamentale per la ricostruzione dei fatti», para. 226. Su tale punto, la CGUE non ha affatto considerato quegli elementi che invece l'Avvocato generale aveva mostrato di tenere fortemente in conto, quali le difficoltà riscontrate da tanti legislatori nazionali nell'adeguare le proprie normative ai requisiti indicati dalla giurisprudenza europea, l'impegno mostrato da taluni Stati membri ad operare nella direzione di un adeguamento il più possibile completo ai requisiti indicati nella sentenza *Tele2*, nonché gli effetti estremamente pregiudizievoli che potrebbero prodursi sulla effettiva tutela della sicurezza pubblica e dello Stato in caso di annullamento o disapplicazione immediata di una normativa sulla *data retention* adottata *ex* art. 15 Direttiva *e-Privacy*.

8.3. *Il difficile tentativo di sintesi di una "sconfitta vittoriosa".*

L'analisi dei precedenti paragrafi impone ora un tentativo di sintesi, in grado di trarre un bilancio finale della posizione espressa dalla CGUE nelle pronunce *Privacy International* e *La Quadrature du Net*, strettamente connesse tra loro e fortemente attese da Stati membri, autorità di *law enforcement*, giuristi, ONG e società civile.

Svolgere una tale operazione risulta tuttavia esercizio quanto mai complesso: se da un lato infatti la CGUE, attingendo ampiamente alla propria giurisprudenza[100], ha riconfermato alcuni principi e criteri in precedenza affermati e maggiormente orientati verso un'ampia tutela dei diritti fondamentali alla *privacy* e alla protezione dei dati, dall'altro lato è pur vero che sono chiaramente emersi profili di grande novità e rilievo in grado di aprire le porte ad alcune significative deroghe rispetto al divieto di conservazione generalizzata ed indiscriminata per scopi securitari. Identificare nell'orientamento della CGUE una prevalenza netta degli interessi alla sicurezza o della garanzia dei diritti fondamentali non pare

[100] La CGUE peraltro ha attinto non solo alle pronunce più direttamente riguardanti la disciplina della *data retention* bensì anche a quelle attinenti al trasferimento di dati verso Stati terzi, come il *Parere 1/15* e sentenza *Schrems* e *Schrems II*, di cui si parlerà nel Capitolo 3.

quindi possibile, tanto che le prime reazioni di ONG e Stati membri sono state estremamente caute e timide[101], riconoscendo alcuni aspetti di apertura rispetto al passato ed altri profili invece di solida conferma dei limiti già espressi.

Partendo da quest'ultimo profilo e volendo sottolineare *in primis* le "vittorie" per la *privacy* e la protezione dei dati ottenute dalle ONG e dai ricorrenti promotori delle controversie dalle quali i rinvii hanno avuto origine, sono almeno quattro i punti nei quali la CGUE riafferma con forza un alto livello di tutela dei diritti fondamentali, anche dinnanzi alle esigenze securitarie: a) la determinazione dell'ambito di applicazione del diritto dell'UE e, in particolare, della Direttiva *e-Privacy*; b) il mancato accoglimento della proposta di una "terza via" in materia di *data retention* e la conseguente conferma della conservazione targettizzata come unica forma compatibile con il diritto dell'UE; c) l'equiparazione delle operazioni di trasmissione massiva di metadati ad un trattamento da parte dei fornitori di servizi di telecomunicazione e ad un accesso da parte delle autorità riceventi; d) la predisposizione di tutele sia nei casi eccezionali in cui la *bulk data retention* viene legittimata, sia nei casi di analisi automatizzata e raccolta in tempo reale di dati relativi a traffico ed ubicazione.

Rispetto a tutti i profili citati, quanto deciso dalla CGUE si allontana, in maniera anche profonda, dalla posizione espressa dai governi degli Stati membri intervenuti e da quanto auspicato dalle autorità di *law enforcement* nonché, in taluni punti, anche dalle Conclusioni dell'Avvocato generale. Ad esempio, stabilendo che, indipendentemente dalla finalità, sono il coinvolgimento e la previsione di obblighi in capo a fornitori di servizi di telecomunicazione a ricondurre entro l'ambito di applicazione del diritto dell'UE la disciplina della *data retention* e dell'accesso successi-

[101] Non è un caso che la ONG Statwatch abbia titolato il suo commento alle sentenze *Privacy International* e *La Quadrature du Net*: «a victory and a defeat for privacy» (https://www.statewatch.org/news/2020/october/bulk-data-interception-retention-judgments-of-the-cjeu-a-victory-and-a-defeat-for-privacy/, 27 ottobre 2020), similmente alla ONG La Quadrature du Net che ha significativamente utilizzato l'espressione «a victorious defeat» per descrivere le pronunce della CGUE (https://www. laquadrature.net/_en/2020/10/06/surveillance-victory-in-defeat/, 6 ottobre 2020). Dello stesso avviso anche J. SAJFERT, *Bulk data interception/retention judgements of the CJEU. A victory and a defeat for privacy*, in *European Law Blog*, 26 ottobre 2020.

vo, la CGUE riduce così significativamente le aree e le attività rispetto alle quali può essere fatta valere la competenza esclusiva degli Stati membri in materia di *data retention*. Considerando infatti che le moderne tecnologie rendono spesso complesso tracciare una netta linea di confine tra operazioni che richiedono l'intervento di soggetti privati e quelle che invece prevedono solo un coinvolgimento di autorità pubbliche, secondo il ragionamento seguito dalla Corte paiono ora potersi con certezza ricondurre alla definizione di "attività dello Stato" solo le operazioni di intercettazione diretta da parte di autorità di *law enforcement*. Anche le operazioni di trasmissione e di analisi automatizzata, sul modello di quelle effettuate dalle *Security and Intelligence Agencies* inglesi, costituiscono infatti attività che non rientrano in quelle proprie dell'art. 4 TUE, così che la lettura fornita dai giudici di Lussemburgo produce un effetto espansivo dell'ambito di applicazione della Direttiva *e-Privacy* e, conseguentemente, della Carta di Nizza e dei criteri e limiti stabiliti dalla giurisprudenza della CGUE [102].

In tal modo, riportando sotto l'"ombrello" del diritto dell'UE anche trattamenti di dati operati per finalità di sicurezza nazionale, nonché negando la proporzionalità di un obbligo generalizzato di trasmissione di

---

[102] Sulla definizione di "attività dello Stato" fornita dai giudici di Lussemburgo, taluni autori hanno espresso critiche e perplessità: «The way the Court defines "activities of the state" (Art. 1(3) E-Privacy Directive) as activities "unrelated to the fields in which individuals are active" further begs the question if such a field can ever exist in a state and what is left of the exception of national security, as enshrined in the TEU», P. VOGIATZOGLOU, J. BERGHOLM, *Privacy International and La Quadrature du Net: the latest on data retention in the name of national and public security*, in *CITIP Law Blog*, 27 ottobre 2020. Come rilevato da Zalnieriute, «the positive answer to the first question in all four cases shows that the CJEU has become an important actor in regulating national security and intelligence activities in EU member states», M. ZALNIERIUTE, *The future of data retention regimes and national security in the EU after the Quadrature du Net and Privacy International judgments*, in *Insights*, 28, 2020, p. 2; il sempre maggiore e più influente intervento del diritto dell'UE nell'ambito delle attività di intelligence è stato rilevato anche da Cameron: «For intelligence agencies, the emergence of European actors that are capable of seriously influencing matters that are central for them, in particular their powers of surveillance, is something relatively new», I. CAMERON, *European Union Law restraints on intelligence activities*, in *International Journal of Intelligence and Counter-Intelligence*, 3, 2020, p. 453.

metadati da parte dei servizi di telecomunicazioni verso le autorità di intelligence, la CGUE ha certamente confermato quell'approccio *human-rights oriented* che la giurisprudenza sin qui analizzata ha così tanto rafforzato negli ultimi decenni, trasformando l'UE in quella che è stata definita una fortezza della privacy digitale anche dinnanzi alle importanti esigenze securitarie. Ribadendo il divieto di *bulk data retention* per scopi di sicurezza pubblica nonché stabilendo precisi e rigidi limiti alla disciplina della conservazione generalizzata concessa per finalità di sicurezza nazionale, la CGUE ha poi fugato i dubbi interpretativi espressi dagli Stati membri, andando nella chiara direzione di un ampliamento dello standard di tutela dei diritti fondamentali dinnanzi alle esigenze securitarie nel campo della *data retention* e dell'accesso e trasmissione di metadati. Sicuramente la lettura netta dei giudici di Lussemburgo, che hanno rifiutato l'approccio per certi profili più compromissorio promosso dall'Avvocato generale [103], non mancherà di destare perplessità e dibattiti vivaci anche e soprattutto dinnanzi ad una espansione dell'ambito di applicazione del diritto dell'UE che, pur avendo il pregio di ampliare le garanzie previste dalla Carta di Nizza, rischia di mettere significativamente in ombra quelle che dovrebbero essere competenze esclusive degli Stati membri.

Se quanto esaminato sino ad ora potrebbe far propendere per l'affermazione di una netta vittoria della privacy e protezione dei dati, ad indirizzare invece l'ago della bilancia verso una forte tutela delle esigenze securitarie sono le posizioni, più innovative, assunte dai giudici di Lussemburgo con riferimento a talune importanti questioni: tra queste, i minori limiti previsti quanto all'impiego di indirizzi IP e di dati identificativi di un utente, o ancora la chiara ammissione della possibilità di prevedere una conservazione generalizzata ed indiscriminata per scopi di sicurezza nazionale, sebbene limitatamente ad occasioni del tutto eccezionali e residuali e nonostante l'imposizione di stringenti tutele e salvaguardie. Con

[103] Come si è detto, l'Avvocato generale promuoveva una posizione meno restrittiva di quella promossa dalla CGUE, sia con riferimento alla possibilità di adottare una forma di *restricted data retention*, sia per quanto atteneva alla modulazione nel tempo degli effetti di una dichiarazione di incompatibilità di una normativa nazionale rispetto al diritto dell'UE.

riferimento a tutti questi profili, la CGUE va in una direzione senza dubbio maggiormente pro-securitaria rispetto al passato, anche se sarebbe eccessivo e, anzi, fuorviante considerare la posizione espressa come un significativo passo indietro rispetto alle tutele stabilite nelle previe pronunce: da un lato la bassa ingerenza nella sfera privata rappresentata dai meri dati identificativi dell'utente, ad esempio, era già stata riconosciuta nel caso *Ministerio Fiscal* e dall'altro, sotto il profilo della eccezione prevista con riferimento alla sicurezza nazionale, questa maggiore apertura è stata nondimeno accompagnata da specifiche condizioni restrittive. Insomma, quella che prima era rimasta un'area grigia ed incerta, ora diviene più chiaramente esplicitata dai giudici che, senza dubbio, mostrano di concedere agli Stati membri la tanto auspicata possibilità di ricorrere alla conservazione generalizzata almeno per finalità di tutela della sicurezza nazionale, sebbene circondandola di garanzie ed evidenziandone la natura residuale, circostanziata e non sistematica. Questa apertura, che pure non giunge a sconvolgere o ribaltare totalmente l'approccio della giurisprudenza precedente [104], è stata nondimeno oggetto di critiche e preoccupazioni da parte delle ONG che hanno visto in questa concessione maggiormente pro-securitaria una possibile fonte di abusi da parte delle pubbliche autorità: in effetti, la terminologia impiegata dai giudici per stabilire le condizioni alle quali una forma di *bulk data retention* può essere legittimamente realizzata resta piuttosto vaga ed ampia, lasciando una

[104] Non si vuole accogliere una lettura troppo drastica ed espansiva dell'apertura maggiormente pro-securitaria concessa dalla CGUE nelle pronunce in esame. Sebbene opinioni quale quella proposta da Zalnieriute, che ha affermato come «In *Quadrature du Net* and *Privacy International* the Court demanded procedural safeguards, yet this approach is very different from that in *Tele 2 Sverige* where the CJEU had insisted that to be proportionate, data retention had to be targeted» (M. ZALNIERIUTE, *The future of data retention regimes*, cit., p. 4), paiano sotto taluni profili condivisibili, esse scontano nondimeno il fatto di non tenere in debito conto le rigide condizioni e limitazioni previste dalla Corte, volte a restringere fortemente la possibilità di ricorrere allo strumento eccezionale della *bulk data retention*. Non a caso, il Garante per la protezione dei dati personali italiano ha letto le sentenze in esame come una «coerente conclusione del percorso iniziato con le sentenze Digital Rights e Tele2 Sverige» (Comunicato del 6 ottobre 2020, disponibile all'indirizzo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9464165) non ravvisandovi dunque un netto stravolgimento della previa giurisprudenza.

certa discrezionalità agli Stati membri nella determinazione puntuale dei criteri indicati [105]. Viene dunque rimessa ai legislatori o ai Governi nazionali l'individuazione delle circostanze "concrete" tali da rappresentare una minaccia grave, reale, attuale o prevedibile per la sicurezza nazionale, così come la previsione delle tutele da apprestare – ad esempio i giudici o l'autorità amministrativa indipendente deputata alla funzione di controllo, nonché i poteri e le informazioni da fornire a tali autorità al fine di garantire un vaglio effettivo ed efficace –. Sarà sul terreno delle condizioni più o meno ampie stabilite dai legislatori nazionali nonché dell'impiego più o meno frequente e precisamente regolamentato di tale disciplina eccezionale che si giocherà la partita fondamentale del futuro della *data retention* per scopi di sicurezza nazionale.

In conclusione, alla luce delle posizioni qui ricostruite, diviene particolarmente difficile giungere ad un bilancio chiaro e netto della giurisprudenza della CGUE: taluni aspetti scontentano e lasciano perplessi sia le ONG promotrici delle controversie nei casi nazionali – che avrebbero preferito un più rigido rifiuto della *bulk data retention* ma che restano soddisfatte dalla riconduzione all'ambito di applicazione del diritto dell'UE di normative che coinvolgono anche autorità di intelligence per finalità di sicurezza nazionale nonché del confermato divieto di conservazione generalizzata per scopi di sicurezza pubblica –, sia i Governi degli Stati membri intervenuti che, accogliendo favorevolmente l'apertura – pur condizionata – ad una forma di conservazione generalizzata nei casi di minacce gravi alla sicurezza nazionale, osservano invece con preoccupazione la riaffermazione della conservazione targettizzata quale unico strumento compatibile con il diritto dell'UE per finalità di repressione dei reati gravi. Come a dire che entrambi gli schieramenti risultano vittoriosi e sconfitti al tempo stesso [106].

---

[105] «The burning question here is: what constitutes a foreseeable threat to national security? For example, do threats, such as the continuous contemporary threat of terrorism, fulfil this condition? In that regard, it is worth remembering the Advocate General Opinion on how difficult it may be to distinguish between public and national security in relation to terrorist threats», P. VOGIATZOGLOU, J. BERGHOLM, *Privacy International and La Quadrature du Net*, cit.

[106] Come sottolineato da Zalnieriute, «while *Privacy International* is an unequivocal

8.4. *La sentenza* H.K. c. Prokuratuur *e le nuove importanti specificazioni sulla disciplina dell'accesso ai metadati.*

A pochi mesi dalle importanti sentenze dell'ottobre 2020, la CGUE è nuovamente tornata a pronunciarsi sull'interpretazione dell'art. 15 Direttiva *e-Privacy* nel caso *H.K. c. Prokuratuur*[107]. A differenza delle decisioni sopra analizzate, però, il rinvio pregiudiziale promosso dalla Corte Suprema estone atteneva principalmente alle condizioni e ai requisiti riguardanti l'accesso ai metadati conservati: i quesiti infatti vertevano sia sui criteri da valutare al fine di determinare la gravità dell'ingerenza nei diritti fondamentali, sia sullo specifico requisito del controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente e, in particolare, se esso potesse considerarsi legittimamente assolto nel caso in cui la funzione di controllo fosse attribuita ad un pubblico ministero che dirige la fase istruttoria ma al quale è assegnato anche il compito di rappresentare la pubblica accusa nel corso del procedimento giudiziario eventualmente avviato.

Ripercorrendo i principi delineati nella propria giurisprudenza in tema di *data retention*, i giudici di Lussemburgo hanno riaffermato il necessario il parallelismo tra gravità dell'ingerenza nella sfera privata e gravità del reato che si intende perseguire[108], giungendo a ribadire che, qualora oggetto di trattamento siano i dati relativi al traffico e all'ubicazione, solo la lotta alla criminalità grave o la presenza di gravi minacce alla sicurezza pubblica sono in grado di giustificare l'accesso da parte di autorità di *law*

---

assertion of CJEU's authoritiy in the area of national security and a victory for data protection, *Quadrature du Net* does not oppose indiscriminate data retention in principle and is an ambivalent response by the CJEU in the face of political pressure», M. ZALNIERIUTE, *A struggle for competence: national security, surveillance and the scope of EU law at the Court of Justice of the EU*, in corso di pubblicazione in *Modern Law Review*, 85, 2021, p. 1.

[107] CGUE 2 marzo 2021, C-746/18, *H.K. c. Prokuratuur*.

[108] I giudici di Lussemburgo hanno poi preliminarmente chiarito che le operazioni di accesso possono essere consentite solo qualora la conservazione dei metadati stessi sia conforme all'art. 15 Direttiva *e-Privacy*; come a dire, nuovamente, che è la conservazione, intesa quale strumento prodromico e funzionale all'accesso, a dover essere in primo luogo legittima.

enforcement o di intelligence ai metadati conservati [109].

Definito questo fondamentale primo punto, è stata poi esaminata l'ulteriore questione posta dal giudice estone, riguardante la determinazione della natura "indipendente" dell'autorità deputata a svolgere il controllo di legittimità preventivo all'accesso. Se questo vaglio rappresenta uno dei requisiti ormai cristallizzati nella giurisprudenza della CGUE, le qualità e la definizione della "indipendenza" richiesta non erano mai state analizzate dai giudici di Lussemburgo: in questo rinvio dunque viene offerta l'occasione di entrare ulteriormente nel dettaglio di tale criterio e di fornire una lettura ancor più approfondita della disciplina dell'accesso. Nello specifico, la normativa estone, similmente a quella italiana, identi-

[109] Ciò indipendentemente dal periodo di tempo per il quale viene chiesto l'accesso e dalla quantità di dati interessati: anche il trattamento di un quantitativo limitato di dati relativi al traffico o di dati relativi all'ubicazione, o un accesso ai dati di breve durata possono infatti essere in grado di fornire precise informazioni sulla vita dell'utente, rappresentando così una ingerenza non lieve nella sfera privata, tale da richiedere necessariamente un obiettivo "rafforzato", da indentificarsi appunto nella repressione dei soli reati o minacce di carattere grave. Seguendo questo ragionamento, la CGUE ripropone quella distinzione tra dati di traffico e di ubicazione e dati invece meramente identificativi dell'utente già statuita nelle previe sentenze dell'ottobre 2020 e in *Ministerio Fiscal*. È stato così ribadito come «le misure legislative riguardanti il trattamento dei dati relativi all'identità civile degli utenti dei mezzi di comunicazione elettronica come tali, e segnatamente la conservazione di tali dati e l'accesso agli stessi, al solo scopo di identificare l'utente interessato, e senza che tali dati possano essere associati ad informazioni relative alle comunicazioni effettuate, possono essere giustificate dall'obiettivo di prevenzione, ricerca, accertamento e perseguimento di reati in generale, al quale fa riferimento l'articolo 15, paragrafo 1, prima frase, della direttiva 2002/58», para. 34. Alla luce di questi principi, la normativa estone è risultata particolarmente problematica e lacunosa: secondo tale legislazione, infatti, l'accesso ai dati poteva essere richiesto per qualsiasi tipo di reato, senza specificazione alcuna circa la gravità dell'obiettivo perseguito. Ciò apre inevitabilmente, nello specifico caso da cui il rinvio origina, a questioni riguardanti l'ammissibilità dei processi verbali redatti basandosi sui metadati raccolti e trattati grazie ad una disposizione nazionale contrastante con l'art. 15 Direttiva *e-Privacy*. Su questo fronte, la CGUE ha ribadito quanto già emerso nella pronuncia *La Quadrature du Net*: spetta al solo diritto nazionale il compito di stabilire regole relative all'ammissibilità di informazioni ed elementi di prova ottenuti nell'ambito di un procedimento penale mediante forme di conservazione o accesso non conformi al diritto dell'UE. Ciò a condizione che tali regole rispettino però il principio di effettività, il principio del contraddittorio e il diritto all'equo processo.

ficava nel pubblico ministero l'autorità preposta al controllo preventivo: tale soggetto, pur essendo sottoposto solo alla legge e avendo l'obbligo di esaminare nel corso del procedimento istruttorio sia gli elementi a carico sia quelli a discarico dell'indagato, assumeva su di sé il compito di raccogliere elementi di prova per lo svolgimento, eventuale, di un futuro processo, al quale avrebbe poi partecipato in qualità di pubblica accusa. Date tali caratteristiche, alcuni dubbi erano sorti quanto all'indipendenza del pubblico ministero e, in particolare, se esso godesse di uno status tale da consentirgli di agire nell'assolvimento dei propri compiti in modo obiettivo, imparziale e al riparo da qualsiasi influenza esterna. Secondo la CGUE, il requisito dell'indipendenza richiede che l'autorità incaricata del controllo preventivo sia «in grado di garantire un giusto equilibrio tra gli interessi connessi alle necessità dell'indagine nell'ambito della lotta contro la criminalità e i diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali delle persone i cui dati sono interessati dall'accesso», para. 52. Ne deriva che l'autorità alla quale è affidato il delicato compito del controllo preventivo deve necessariamente essere terza rispetto a quella incaricata di formulare la richiesta di accesso ai dati, in modo che il vaglio esercitato possa essere realmente imparziale ed oggettivo. Il requisito di terzietà dunque impone che l'autorità di controllo non sia coinvolta nella conduzione dell'indagine penale e si trovi così in una posizione di neutralità rispetto a tutte le parti del procedimento. Poste queste stringenti condizioni, un sistema di controllo quale quello stabilito dalla normativa estone poneva non pochi problemi, essendo affidato ad un pubblico ministero che, a causa della natura stessa dell'incarico assegnatogli – quello cioè di valutare, a seguito di una istruttoria penale, se sottoporre o meno al giudice una controversia – e del cumulo di posizioni ricoperte – anche quella cioè di vera e propria parte che esercita l'azione penale nell'eventuale processo –, non poteva soddisfare il requisito di terzierà ed indipendenza. La CGUE ha precisato inoltre, sul punto, un aspetto di grande rilievo: all'assenza di un vaglio preventivo non può in alcun modo sopperire un controllo successivo da parte di un giudice. Un tale intervento postumo infatti non riuscirebbe a garantire il perseguimento del medesimo obiettivo al quale il controllo preventivo è preposto, ovvero impedire che l'accesso ai dati – e dunque l'invasione nella sfera privata – ecceda i limiti dello stretto necessario. Viene respinta, in

sostanza, la correttezza di una lettura complessiva e globale delle tutele, fondata cioè sull'idea di poter compensare, con altre e diverse garanzie, il mancato rispetto delle salvaguardie fissate dalla CGUE.

Nel riaffermare poi la necessaria sussistenza di un collegamento, almeno indiretto, tra accesso e finalità perseguita e dunque una limitazione dell'ingerenza solo ai dati di persone sospettate di progettare, di aver commesso o di essere implicate in un reato grave, viene ancor meglio specificato il divieto di un accesso generalizzato ed "esplorativo", che trova l'unica eccezione possibile nel caso in cui gli interessi vitali della sicurezza nazionale, difesa e sicurezza pubblica siano soggetti alla minaccia terroristica: solo in tali circostanze eccezionali, l'accesso può essere concesso anche in assenza di un sospetto specifico, potendo dunque riguardare persone diverse dai sospettati e laddove comunque vi siano elementi oggettivi che consentano di ritenere l'accesso utile nel caso concreto. Viene pertanto riconfermato quell'allentamento – pur condizionato – delle stringenti condizioni fissate dalla CGUE qualora entri in gioco la finalità di garanzia della sicurezza nazionale, del tutto similmente a quanto le sentenze dell'ottobre 2020 hanno precisato con riferimento alla disciplina della conservazione.

In conclusione, come alcuni primi commenti della pronuncia esaminata hanno posto in rilievo [110], la decisione qui esaminata, inserendosi perfettamente nel solco già tracciato della previa giurisprudenza della CGUE, contribuisce a chiarire quel complesso quadro di limiti, criteri e condizioni che i giudici di Lussemburgo, ormai da un decennio, stanno tratteggiando e dal quale affiora un'immagine dai contorni via via sempre più netti e precisi. Fornendo in particolare importanti chiarimenti quanto al requisito di indipendenza dell'autorità deputata al controllo preventivo, la pronuncia inoltre non mancherà di produrre rilevanti conseguen-

[110] Si rimanda a E. CELESTE, *Commission v. Spain and H.K. v. Prokuratuur: taking the plank out of EU's own eye*, in *Bridge Blog*, 15 marzo 2021; S. ROYER, S. CAREEL, *Access denied. The CJEU raffirms la Quadrature du Net and clarifies requirements for access to retained data*, in *CiTiP Law Blog*, 23 marzo 2021; S. ROVELLI, *Case Prokuratuur: proportionality and the independence of authorities in data retention*, in *European Papers*, 6, 2021, p. 199 ss. Sia consentito anche il rimando a G. FORMICI, *L'incerto futuro della data retention saga nell'Unione europea: osservazioni a partire dalla sentenza H.K. v. Prokuratuur*, in *SIDI Blog*, 27 aprile 2021.

ze negli Stati membri che presentano similitudini con il sistema estone oggetto del rinvio, tra cui può essere annoverata certamente l'Italia, che non a caso è stata citata dall'Avvocato generale Pitruzzella nelle sue Conclusioni sul rinvio estone. Non stupisce pertanto come proprio in Italia si siano manifestati con chiarezza e rapidità gli effetti della sentenza *H.K.*: il Tribunale di Rieti ha infatti recentemente promosso un rinvio pregiudiziale alla CGUE – il primo avanzato dai giudici italiani in materia di *data retention* e accesso ai metadati – avente ad oggetto il requisito di indipendenza dell'autorità preposta al previo vaglio all'accesso ai metadati [111]. Sebbene questo ulteriore e ancora pendente rinvio sia oggetto di approfondita analisi nel Capitolo 6 dedicato alla disciplina, il breve cenno qui svolto costituisce una chiara dimostrazione dell'importanza degli interventi della CGUE e delle dirompenti ripercussioni che esse provocano sugli ordinamenti nazionali. Del resto, l'ampio dibattito venutosi ad instaurare a seguito della sentenza *H.K.* e la difformità di interpretazioni avanzate sul punto da diverse Corti italiane che hanno determinato ancora una volta la necessità dell'intervento chiarificatore della CGUE, testimoniano quanto, nonostante il celere avvicendarsi di pronunce dei giudici di Lussemburgo e i chiarimenti man mano forniti, la materia della *data retention* e dell'accesso ai metadati per scopi securitari resti ancora estremamente controversa, in attesa di giungere a quel punto conclusivo di arrivo che l'apertura di un rinnovato dialogo tra Corti nazionali e sovranazionale continua invece a spostare in avanti.

9. *Prevedere l'imprevedibile: le profonde ed incerte conseguenze sul piano europeo e nazionale della più recente giurisprudenza della CGUE.*

Il complesso panorama apertosi a seguito delle pronunce *Privacy International*, *La Quadrature du Net* e *H.K.* richiede una seria riflessione sui possibili sviluppi e sul futuro della *data retention* nell'UE. La difficoltà di

[111] Causa C-334/21 derivante dalla domanda di pronuncia pregiudiziale proposta dal Tribunale di Rieti il 26 maggio 2021 nel procedimento penale a carico di G.B. e R.H.

trarre un definitivo bilancio dalle importanti sentenze dell'ottobre 2020, gli innovativi principi sanciti, tra cui la possibilità di ricorso eccezionale allo strumento della conservazione generalizzata per scopi di garanzia della sicurezza nazionale, unitamente al continuo dialogo con la CGUE venutosi ad instaurare anche a seguito della sentenza *H.K.*, ricostruiscono un panorama dai tratti ancora in parte incerti, che non consente di considerare la *data retention saga* definitivamente conclusa e chiarita. Se è vero che gli ultimi interventi dei giudici di Lussemburgo devono ancora dispiegare del tutto i propri effetti, così che risulta al momento piuttosto difficile svolgere previsioni in un ambito così "magmatico" e dai molteplici risvolti, pare nondimeno possibile ed utile proporre alcune considerazioni critiche sull'impatto che la più recente giurisprudenza della CGUE è destinata a produrre rispetto a tre profili di rilievo, che qui si vogliono approfondire: a) i rinvii pregiudiziali ancora pendenti in materia; b) la posizione che il legislatore europeo deciderà di tenere con riferimento sia all'adozione del Regolamento *e-Privacy* sia all'eventuale predisposizione di una normativa *ad hoc* in materia di conservazione; c) le reazioni delle Corti e dei legislatori degli Stati membri a seguito dei principi stabiliti dalla CGUE.

9.1. *L'impatto sui rinvii pregiudiziali ancora pendenti: un esito già scritto o un persistente bisogno di chiarezza?*

La CGUE vede al momento ancora pendenti i rinvii pregiudiziali *SpaceNet AG c. Repubblica federale di Germania*, C-793/19 e *Repubblica Federale di Germania c. Telekom Deutschland GmbH*, C-794/19, entrambi promossi dal *Bundesverwaltungsgericht* tedesco il 29 ottobre 2019, il rinvio *G.D. c. The Commissioner of the Garda Siochana e al.*, C-140/20 avanzato dalla *Supreme Court* irlandese il 25 marzo 2020, oltre al più recente rinvio, sopra richiamato, del Tribunale di Rieti risalente al 26 maggio 2021. Tralasciando l'analisi di quest'ultimo procedimento, intervenuto successivamente alla pronuncia *H.K.* e strettamente correlato ad essa[112], i quesiti contenuti nei tre rinvii citati e risalenti ad un momento

[112] Come anticipato, ampio spazio all'analisi di questo rinvio e delle considerazioni svolte dai giudici italiani verrà dedicato nel Capitolo 6.

antecedente alle chiarificatrici sentenze dell'ottobre 2020 presentano forti somiglianze con quelli promossi in precedenza dai giudici inglese, belga e francese e risultano accumunati, ancora una volta, dal tentativo di promuovere una modulazione dei rigidi criteri indicati nella sentenza *Tele2*.

La Corte amministrativa federale tedesca[113], infatti, nei due rinvii proposti non ha mancato di svolgere un interessante ed approfondito esame della giurisprudenza europea all'epoca disponibile, mettendone in luce i limiti argomentativi e le concrete difficoltà attuative. Dopo aver sollevato dubbi quanto alla correttezza di una rigida lettura della pronuncia *Tele2* volta a ritenere una conservazione generalizzata sempre, in tutte le circostanze e per sua stessa natura, incompatibile con il diritto dell'Unione, il giudice del rinvio è giunto a chiedere se debba risultare non conforme alla Carta di Nizza e ai requisiti stabiliti dalla CGUE anche una normativa, come quella tedesca, che, pur prevedendo una conservazione ampia e non fondata su un indizio di connessione ad una minaccia per la sicurezza pubblica o nazionale, stabiliva precisi e dettagliati limiti e ampie garanzie tanto nella fase di *retention* quanto in quella di accesso. Il discusso art. 113b del *Telekommunikationsgesetz* (c.d. TKG), infatti, disponeva

[113] I giudici tedeschi erano stati chiamati a pronunciarsi sulla conformità al diritto dell'UE dell'art. 113b del *Telekommunikationsgesetz* (c.d. TKG). Come già brevemente riportato in questo Capitolo, tale disposizione normativa, che introduceva un obbligo generale di conservazione dei metadati in capo ai fornitori di servizi di telecomunicazione per scopi securitari, era stata modificata dalla legge del 10 dicembre 2015, come reazione sia alla sentenza *DRI* sia alla decisione del Tribunale costituzionale federale del 2010, che aveva dichiarato, come si ricorderà, l'incostituzionalità della previa legislazione in materia di *data retention*. La normativa modificata, pur integrando numerosi requisiti fissati dalla giurisprudenza della CGUE, non rinunciava comunque ad una forma di conservazione generalizzata: proprio per questo aspetto, considerato in contrasto con la normativa dell'UE, la fornitrice di servizi di telecomunicazione SpaceNet AG aveva promosso azione avverso il Tribunale amministrativo federale che, in primo grado, aveva ritenuto la ricorrente non obbligata alla memorizzazione dei metadati; dinnanzi a questa pronuncia, dai prorompenti e rischiosi effetti, capaci di incidere fortemente sull'efficacia dello strumento della *data retention* per scopi securitari, la Repubblica federale tedesca aveva proposto ricorso di annullamento; per risolvere tale delicata questione, il giudice amministrativo di secondo grado ha tuttavia ritenuto imprescindibile un chiarimento da parte della CGUE sull'interpretazione dell'art. 15 della Direttiva *e-Privacy*.

una durata dell'obbligo di conservazione estremamente ridotta e differenziata a seconda della categoria dei dati – quattro settimane per i dati relativi all'ubicazione e dieci settimane per tutte le altre tipologie –, escludendo peraltro dalla conservazione non solo il contenuto delle comunicazioni, ma anche i dati relativi alle pagine Internet visitate, i collegamenti effettuati a linee Internet in ambito religioso nonché i dati sul traffico di soggetti tenuti al segreto professionale. Alla luce di queste significative salvaguardie, in grado di ridurre considerevolmente l'invasività della conservazione stessa, i giudici tedeschi hanno così suggerito un'interpretazione dell'art. 15 della Direttiva *e-Privacy* che non escluda a priori la compatibilità col diritto dell'UE di qualsiasi forma di conservazione ingiustificata – cioè non targettizzata [114] –; questo anche perché «il concetto alla base della conservazione dei dati non è conciliabile con la richiesta formulata dalla Corte di distinguere, nei dati oggetto di memorizzazione, in base alle persone, ai periodi e alle aree geografiche» [115], respingendo dunque l'utilità e la fattibilità di una rigida forma di conservazione mirata [116]. Così, secondo l'analisi svolta dai giudici del rinvio «non può desumersi dalla giurisprudenza della Corte [di giustizia dell'UE] il fatto che ai legislatori nazionali non sia più concessa la possibilità, sulla base di una valutazione globale, di introdurre la conservazione ingiustificata dei dati, eventualmente integrata da rigorose norme di accesso, al fine di tener conto dello

[114] Con tale termine i giudici tedeschi hanno inteso operare una distinzione rispetto ad una conservazione *in toto* generalizzata: ciò è motivato dal fatto che alcune categorie di metadati e alcuni utenti risultavano esclusi dalla disciplina della *data retention* che non coinvolgeva dunque l'interezza dei dati e degli utenti. Nonostante ciò, comunque, è bene sottolineare come anche una simile tipologia di conservazione resti priva di quegli elementi e criteri oggettivi che permettono, anche solo indirettamente, di collegare la conservazione dei metadati di un soggetto alla minaccia di reati gravi.

[115] Para. 25, *Sintesi della domanda di pronuncia pregiudiziale ai sensi dell'art. 98, par. 1, del Regolamento di procedura della CGUE.*

[116] Una lettura eccessivamente rigida della giurisprudenza dei giudici di Lussemburgo porterebbe, secondo i giudici tedeschi, ad una notevole restrizione del margine di discrezionalità ed autonomia lasciato ai legislatori nazionali nell'ambito della tutela della sicurezza, ai sensi dell'art. 4, co. 2, TUE. Ciò che è stato posto in luce dunque è la necessità di trovare un equilibrio tra il rispetto dei diritti fondamentali e l'obbligo degli Stati membri di garantire il diritto alla sicurezza dei propri cittadini.

specifico potenziale di rischio associato ai nuovi mezzi di telecomunicazione», para. 27.

Del tutto similmente, anche Corte Suprema irlandese nel rinvio richiamato [117] ha evidenziato forti perplessità quanto ad una rigida lettura dei requisiti stabiliti dalla CGUE: ponendo grande enfasi sugli studi e sulle considerazioni riportate da vari esperti, tra cui l'ex *UK Independent Reviewer of Terrorism Legislation*, i giudici irlandesi hanno non solo ribadito l'importanza e l'efficacia della conservazione generalizzata e dell'analisi dei metadati nella lotta alla criminalità grave e al terrorismo [118],

[117] La Corte Suprema irlandese ha interrogato la CGUE quanto alla compatibilità di un regime generale o universale di conservazione dei metadati con il diritto dell'Unione anche qualora: (a) esso preveda rigorose limitazioni e salvaguardie sulla sicurezza dei dati e sulla fase di accesso; (b) la *data retention* sia finalizzata alla garanzia della sicurezza nazionale; (c) la conservazione sia indispensabile e strettamente necessaria al raggiungimento dell'obiettivo di lotta contro reati gravi. Il giudice irlandese, inoltre, similmente a quanto già svolto dalla Corte costituzionale belga nel suo rinvio, ha posto un quesito relativo agli effetti nel tempo di una dichiarazione di incompatibilità con il diritto dell'UE della normativa nazionale sulla conservazione dei dati e alla possibilità di limitarne le conseguenze laddove una mancata modulazione temporale sia tale da portare ad un serio disordine e ad un danno all'interesse pubblico. Proprio quest'ultimo aspetto è stato evidenziato con grande decisione dai giudici nazionali, anche in considerazione dello specifico caso concreto dal quale il rinvio ha avuto origine: il signor Graham Dwyer, accusato dell'omicidio di una donna sulla base delle informazioni dedotte dai metadati telefonici conservati dalle compagnie di telecomunicazione, aveva ritenuto inammissibili le prove addotte a suo carico promuovendo un procedimento nel quale ad essere contestata era la legittimità della legge irlandese, il *Communications Data Retention Act* del 2011, adottata in attuazione della DRD. A seguito dell'accoglimento del ricorso da parte della *High Court* nel 2018, il Governo aveva impugnato tale decisione dinnanzi alla *Supreme Court*, che ha poi ritenuto fondamentale ottenere un chiarimento da parte della CGUE circa la corretta interpretazione dell'art. 15 Direttiva *e-Privacy*.

[118] Viene in particolare riportata una analisi statistica elaborata dalla Germania, presentata alla Commissione europea nel 2013, secondo cui «in 44,5% of the cases involving requests for retained traffic data, there were no other means of conducting the investigation», para. 4.3 della sentenza n. 2019/18 della *Supreme Court*, nel caso *Graham Dwyer v. The Commissioner of An Garda Siochana, the Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General*, del 24 febbraio 2020. Al successivo para. 4.4. si legge come «the expert witnesses also gave evidence that they considered that there were no equally effective alternatives to a universal regime of data retention. The "quick-freeze" system, under which preservation orders relating to par-

ma ne hanno anche affermato l'insostituibilità con altri strumenti quali la *data preservation* o la conservazione targettizzata. Per questi motivi la Corte ha invitato i giudici di Lussemburgo a considerare con attenzione «the fact that many serious crimes against vulnerable people are most unlikely, on the undisputed evidence, to be capable of successful prosecution in the absence of a system of universal retention. In that context, I would consider that considerable weight must be attached to the undoubted rights of the victims of such crime, which rights will be impaired to a very significant degree indeed if it should prove impossible to detect or successfully prosecute the perpetrators of crimes against them. I would suggest that the rights of such persons need to be kept very much in mind in determining any appropriate balance» [119].

La breve ricostruzione dei rinvii richiamati, nonché le posizioni espresse dai giudici nazionali, rivelano ancora una volta quell'approccio "difensivo" tenuto dagli Stati membri, nel tentativo di preservare una forma di conservazione generalizzata, pur corredandola di profonde tutele e salvaguardie, e di fornire così un'interpretazione dei criteri sanciti dalla sentenza *Tele2* più flessibile e meno stringente.

Un approccio, questo, che pare ormai risultare superato dalle più recenti sentenze *Privacy International*, *La Quadrature du Net* e *H.K.*, che rendono piuttosto prevedibile, almeno sotto taluni profili più generali, l'esito finale dei rinvii tedeschi e irlandese: i giudici di Lussemburgo, salvo imprevedibili rovesciamenti dell'orientamento sino ad ora tenuto, provvederanno ad una riconferma del divieto di conservazione generalizzata ed indiscriminata per scopi di sicurezza pubblica e alla riproposizione della conservazione mirata come unica soluzione percorribile. Se tale approccio fosse confermato, si rivelerebbe ancora una volta inutile il richiamo, operato anche dai giudici del rinvio tedesco ed irlandese, alla

---

ticular individuals can be served on service providers after those individuals came under suspicion, would have limited efficacy in the context of the investigation of crime, as the majority of data regarding the suspect's conduct prior to their identification would be unavailable. (…) Further, this system would be of no utility in identifying persons who are unknown to law enforcement authorities at the time of the offence».

[119] Para. 6.18 della sentenza n. 2019/18 della *Supreme Court*, nel caso *Graham Dwyer v. The Commissioner of An Garda Siochana, the Minister for Communications, Energy and Natural Resources, Ireland and the Attorney General*, del 24 febbraio 2020.

presenza di elevate salvaguardie previste tanto nella fase di conservazione quanto di accesso, così come pure l'affermata inconciliabilità del concetto stesso di conservazione dei dati con una forma di *data retention* targettizzata. Anche rispetto al quesito posto dal giudice irlandese circa la modulazione degli effetti nel tempo della dichiarazione di incompatibilità con il diritto dell'UE di una normativa nazionale in materia di *data retention*, pare che nella sostanza le sentenze dell'ottobre 2020 abbiano già fornito una risposta piuttosto chiara e in senso prevalentemente negativo, pur in parte rimandando, come si è detto, al giudice nazionale le delicate valutazioni quanto alla validità degli elementi di prova.

Con queste considerazioni sul possibile e prevedibile epilogo dei rinvii pendenti non si vuole però certamente negare l'interesse e il rilievo delle future pronunce dei giudici di Lussemburgo: sebbene molti dei profili problematici rilevati nei rinvii verranno con grande probabilità risolti in maniera coerente con la previa giurisprudenza, la CGUE potrà certamente sfruttare questa utile occasione per ribadire, rafforzare o meglio esplicitare quanto già emerso dalla stratificata *data retention saga* sin qui analizzata.

9.2. *Verso il risveglio del legislatore europeo da tempo silente: i rischi e le sfide di un rinnovato intervento normativo sovranazionale.*

Il secondo scenario in attesa di determinazione e rispetto al quale le decisioni *Privacy International*, *La Quadrature du Net* e *H.K.* produrranno – e in parte hanno già iniziato a produrre – certamente un grande impatto è quello riguardante le possibili reazioni del legislatore sovranazionale e, più in generale, delle Istituzioni dell'UE chiamate a contribuire alla determinazione della complessa disciplina della *data retention*.

In questo articolato panorama, un primo fronte aperto è senza dubbio da individuarsi nelle soluzioni normative che potrebbero essere adottate nel prossimo futuro e che sono da lungo tempo attese e da più parti invocate: dinnanzi al forte attivismo della CGUE pare ancor più assordante il silenzio del legislatore dell'UE che solo negli ultimi anni ha mostrato di voler – non senza grande fatica e difficoltà – superare la lunga fase di immobilismo apertasi a seguito dell'invalidazione della DRD. Il primo tentativo, ancora tutto in divenire, di colmare il vuoto normativo lasciato

dalla sentenza *DRI* è stato infatti promosso nel 2019 dal Consiglio che, all'indomani della sentenza *Tele2*, aveva avviato un lento processo di riflessione culminato nel documento *Conclusioni sulla conservazione dei dati per finalità di lotta contro la criminalità*, n. 9336/19 del 27 maggio 2019. Con questo succinto elaborato, il Consiglio affidava alla Commissione il compito di avviare iniziative per procedere a consultazioni e studi approfonditi sulle possibili soluzioni da adottare in materia di conservazione dei dati, compresa l'opportunità di avviare una specifica ed apposita iniziativa legislativa *ad hoc* in tale ambito. Nell'attribuire alla Commissione questo delicato e arduo incarico, il Consiglio invitava quest'ultima a valutare i concetti di conservazione «generale, mirata e limitata e il concetto di accesso mirato ai dati conservati, nonché ad esaminare in che misura l'effetto cumulativo di forti garanzie e possibili limitazioni a entrambi i livelli di interferenza possa contribuire ad attenuare l'impatto complessivo della conservazione dei dati sulla protezione dei diritti fondamentali», para. 2. Così facendo, il Consiglio pareva suggerire quindi sia di tenere in considerazione il possibile contemperamento tra le salvaguardie disposte all'accesso e quelle previste nel campo della mera conservazione, sia di approfondire le caratteristiche, la fattibilità e la legittimità di quella nuova forma di conservazione limitata (*restricted data retention*) emersa dal dibattito sorto in seno ad Europol [120].

Ebbene, queste soluzioni alternative rispetto a quanto prospettato dalla CGUE nelle sentenze *DRI* e *Tele2* e che promuovevano una lettura meno stringente della giurisprudenza sino ad allora disponibile, sembrano doversi ora ritenere respinte alla luce delle chiare considerazioni svolte dai giudici di Lussemburgo nelle pronunce dell'ottobre 2020: come si è visto, infatti, nei casi *Privacy International* e *La Quadrature du Net* non solo è stato avversato il ragionamento che vede nella predisposizione di condizioni di accesso più limitate un contraltare in grado di consentire una conservazione più ampia, ma è stata anche espressamente riconosciu-

[120] Per ulteriori approfondimenti sulla già esaminata conservazione "limitata" proposta da Europol si rimanda al documento, solo in parte accessibile, EUROPOL, *Proportionate data retention for law enforcement purposes*, WK 9957/2017, 21 settembre 2017, nonché a P. VOGIATZOGLOU, *Data retention tales: the Council of the EU strickes back?*, in *CiTiP Law Blog*, luglio 2019.

ta quale unica forma di conservazione conforme al diritto dell'UE quella di tipo targettizzato laddove l'obiettivo sia quello di salvaguardia della sicurezza pubblica. Dinnanzi a queste nette posizioni, sembra pertanto difficile che ora la Commissione possa procedere nella direzione suggerita dal Consiglio, anche qualora dovesse ritenere opportuno proporre l'adozione di una nuova normativa *ad hoc* in materia di *data retention*. Le articolate e recenti sentenze della CGUE, insomma, paiono restringere significativamente il margine di azione del legislatore europeo e il tentativo di predisporre una disciplina che possa da un lato risultare efficace ed ottenere l'approvazione dei rappresentanti degli Stati membri e dall'altro rispettare i criteri stabiliti dalla giurisprudenza della Corte appare ora ancor più complessa. Sebbene molti studiosi abbiano individuato proprio nell'intervento del legislatore sovranazionale l'unica soluzione concreta e definitiva alle criticità derivanti dal panorama frammentario e confuso che caratterizza le normative degli Stati membri in materia e che ha portato – in passato e ancora oggi – al succedersi di così tanti rinvii pregiudiziali alla CGUE, una proposta legislativa *ad hoc* in materia di *data retention* sembra oggi rappresentare uno sviluppo estremamente delicato e difficile, che richiede una ponderazione molto attenta da parte della Commissione. Queste considerazioni paiono del resto trovare conferma nelle statuizioni del Commissario per la Giustizia Didier Reynders che, in occasione di un incontro con i Ministri della Giustizia degli Stati membri, tenutosi l'11 marzo 2021, ha cautamente ribadito l'impegno della Commissione a fornire indicazioni utili all'implementazione di una forma di *data retention* compatibile con le indicazioni della CGUE, peraltro evidenziando la vincolatività delle decisioni dei giudici di Lussemburgo quale monito rivolto in particolare a quegli Stati membri che invece, come si vedrà, stanno cercando, anche a seguito delle più recenti pronunce dell'ottobre 2020, di sfuggire ai limiti fissati da queste ultime e di preservare forme di conservazione generalizzata. Al contrario, nel medesimo incontro, l'esigenza di approvare soluzioni di compromesso condivise a livello sovranazionale, che non lascino cioè ai singoli Stati il difficile compito di adeguarsi a requisiti complessi e rigidi fissati dalla giurisprudenza della CGUE, è emersa con chiarezza dalle parole del Ministro della Giustizia del Portogallo – Stato cui all'epoca era affidata la presidenza del Consiglio dell'UE –: quest'ultimo infatti ha ribadito il bisogno di definire uno strumento re-

golatorio comune europeo, che possa stabilire in maniera netta e quanto più possibile definitiva le condizioni e l'impiego dello strumento della *data retention* e che consenta così di evitare il continuo intervento dei giudici di Lussemburgo e il susseguirsi di difficili vicende giurisprudenziali, anche a livello nazionale, che rappresentano una insidiosa fonte di instabilità e incertezza in una disciplina invece di estremo rilievo per la garanzia della sicurezza.

Mentre sotto il profilo di un intervento normativo sovranazionale *ah hoc* il futuro resta dunque ancora estremamente confuso e nebuloso, caratterizzato da spinte in direzioni opposte da parte dei diversi attori in gioco, un altro fronte sul quale le sentenze *Privacy International* e *La Quadrature du Net* sembrano avere già, nel frattempo, sortito effetto è quello della proposta di Regolamento *e-Privacy*, volto ad abrogare e sostituire l'ormai vetusta Direttiva *e-Privacy* 2002/58, contenente, lo si ricorda, le uniche disposizioni ad oggi esistenti a livello sovranazionale che attribuiscono ai legislatori nazionali la facoltà di prevedere obblighi di conservazione per finalità securitarie.

La proposta di Regolamento ha sin dall'inizio incontrato proprio nella determinazione della materia della *data retention* un terreno di scontro e di acceso dibattito, che ha peraltro contribuito a rallentare l'approvazione di un testo finale. Pur non proponendosi come obiettivo quello di prevedere una normativa specifica sulla conservazione dei dati, nel discusso testo del Regolamento si sono infatti avvicendate diverse versioni delle disposizioni riguardanti tale materia che hanno comunque in gran parte ricalcato l'esistente art. 15 della Direttiva, proponendo una disciplina ancora vaga e generica circa la possibilità per i legislatori nazionali di disporre deroghe all'obbligo di cancellazione o anonimizzazione dei metadati. Questo è ciò che in sostanza si rinviene nella proposta di Regolamento approvata dal Comitato dei rappresentanti permanenti (COREPER) il 10 febbraio 2021 (doc. 6087/21), sulla base della quale sono state avviate le negoziazioni tra Parlamento europeo, Commissione e Consiglio stesso: questa versione finale, frutto di sostanziali e complessi compromessi tra differenti visioni degli Stati membri in seno al Consiglio [121],

[121] A seguito delle sentenze del 6 ottobre 2020 della CGUE, la Presidenza tedesca del Consiglio aveva proposto di evitare l'inserimento all'interno del Regolamento *e-Privacy*

stabilisce all'art. 7, co. 4, che «Union or Member states'law may provide that the electronic communications metadata is retained, including under any retention measure that respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society, in order to safeguard the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the safeguarding against and the prevention of threats to public security, for a limited period. The duration of the retention may be extended if threats to public security of the Union or of a Member State persists» [122]. Se questa disposizione sembra riproporre le problem-

di qualsiasi riferimento specifico alla disciplina eccezionale della *data retention*, eliminando così l'art. 7, co. 4 dalla bozza. Questa posizione era stata tuttavia accolta con disappunto da taluni Stati membri che ritenevano preferibile, invece, la previa versione dell'art. 7, co. 4, promossa dalla antecedente Presidenza finlandese. L'attuale reintroduzione di una specifica disposizione sulla *data retention*, pur con un dettato estremamente ampio e che poco aggiunge rispetto a quanto in precedenza stabilito nell'art. 15 Direttiva *e-Privacy*, è da leggersi quindi come una soluzione di compromesso tra posizioni prosecuritarie, non disposte a perdere qualsiasi riferimento alla possibilità di adottare discipline nazionali in materia di conservazione dei metadati, e altre invece maggiormente inclini ad adottare più rigide disposizioni in materia atte ad adeguarsi all'interpretazione della CGUE – in questo senso va letta la posizione della Germania che, non a caso, si è astenuta nell'ultima votazione di approvazione della bozza proposta –.

[122] Al considerando 26 viene inoltre precisata «the possibility for the Union or Member States under specific conditions to restrict by law certain obligations and rights, including by way of derogations, when such a restriction constitutes a necessary and proportionate measure in a democratic society to safeguard specific public interests, including public security and the prevention, investigation, detection or prosecution of criminal offences, or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests»; in tutti questi casi, dunque, resta concessa agli Stati membri la facoltà di adottare misure, «such as legislative measures, providing for the retention of data for a limited period of time, if necessary and proportionate to safeguard the public interests mentioned above, in accordance with the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, as interpreted by the Court of Justice of the European Union and of the European Court of Human Rights».

atiche già rilevate nell'attuale dettato dell'art. 15 Direttiva *e-Privacy*, ciò che pare ancora più problematico è invece quanto previsto all'art. 2, co. 2, lett. a: «the Regulation does not apply to activities, which fall outside the scope of Union law, and in any event measures, processing activities and operations concerning national security and defence, regardless who is carrying out those activities whether it is a public authority or a private operator acting at the request of a public authority». Questa disposizione risulta particolarmente critica e discutibile nonché in aperto contrasto con la recente lettura promossa dalla CGUE che ha invece ampiamente chiarito come, indipendentemente dalla finalità di sicurezza nazionale o sicurezza pubblica, la disciplina della conservazione e accesso ai metadati rientra nell'ambito di applicazione del diritto dell'UE ogni qual volta sia previsto un intervento – un trattamento – da parte di soggetti privati – i fornitori di servizi di telecomunicazione –, mentre ne restano escluse unicamente le attività proprie dello Stato, quali le intercettazioni dirette svolte da parte di autorità pubbliche. Questa previsione normativa, unitamente alla riproposizione della disciplina derogatoria dell'art. 15 Direttiva *e-Privacy* senza alcuna specificazione o limitazione chiara e precisa che rimandi ai principi delineati dalla CGUE, sono evidenza lampante del tentativo di taluni Stati membri di "smarcarsi" dai limiti stabiliti dai giudici di Lussemburgo e di non rinunciare allo strumento della conservazione generalizzata, soprattutto nel delicato ambito della garanzia della sicurezza nazionale. Non è un caso che il Comitato europeo per la protezione dei dati [123], nello *Statement 3/2021 on the e-Privacy Regulation* del 9 marzo 2021, abbia espresso preoccupazione quanto alla disciplina inserita nella proposta esaminata, ritenendo che il futuro Regolamento «cannot derogate from the application of the latest CJEU case law. (…) With regard to the exclusion from the scope of application of the Regulation of processing activities by providers, the EDPB considers that such exclusion runs against the premise for a consistent EU data protection framework».

In conclusione, sotto il profilo normativo permane l'incertezza e la

[123] Un organo europeo indipendente, composto dai rappresentati delle autorità nazionali per la protezione dei dati e dal Garante europeo della protezione dei dati, che ha sostituito il Gruppo di Lavoro Art. 29 istituito dalla previa Direttiva 95/46.

difficoltà di determinare un punto di equilibrio tra quanto promosso dagli Stati membri e quanto invece disposto dalle pronunce della CGUE che, pur con le innovazioni previste quanto allo scopo di sicurezza nazionale, pare andare in una direzione ben più garantista dei diritti fondamentali [124]. Nel frattempo, la reiterata assenza di armonizzazione delle normative in materia di *data retention* e la mancanza di una normativa sovranazionale precisa e chiara, contribuiscono al perdurare di un panorama frammentario all'interno dell'UE che continua e continuerà a dare adito a continui dubbi di conformità tra normative nazionali e diritto dell'UE, così da alimentare incertezze e disomogeneità di approcci che vedono nella promozione di rinvii ai giudici di Lussemburgo l'unica via percorribile per ottenere risposte. Se l'intervento del legislatore sovranazionale con una normativa *ad hoc* sembra ancora ben lontano dall'avverarsi, gli ultimi sviluppi giurisprudenziali sono certamente destinati a rendere ancora più complessa la determinazione di una soluzione – anche politica – condivisa, che sia in grado di incontrare il favore degli Stati membri e al contempo di resistere al vaglio della CGUE, evitando di subire la stessa drammatica sorte della DRD.

Infine, un ulteriore profilo in attesa di determinazione a seguito delle sentenze più recenti della CGUE è quello che attiene alla specifica posizione che la Commissione vorrà adottare nel prossimo futuro: se infatti quest'ultima ha mantenuto, anche all'indomani della sentenza *Tele2*, un atteggiamento piuttosto cauto ed attendista [125], ci si chiede ora se e come essa deciderà di porsi nei confronti di quegli Stati membri che hanno

---

[124] Per una approfondita disamina del percorso e del dibattito in seno al Consiglio che ha portato all'approvazione della bozza di Regolamento qui analizzata, si rimanda a M. ROJSZCZAK, *The uncertain future of data retention laws in EU: is a legislative reset possible?*, in *Computer Law and Security Review*, 41, 2021, p. 1 ss.

[125] Precedentemente alle pronunce *Privacy International* e *La Quadrature du Net*, dinnanzi alle interrogazioni che chiedevano chiaramente «When will [the Commission] launch infringement proceedings against those Member States that have breached the provisions of the ePrivacy Directive?», la Commissione rispondeva in maniera tutt'altro che incisiva: «The Commission is monitoring developments at the Court of Justice of the EU on a number of legal frameworks and will assess the need for further action once the judgments in the relevant pending cases are delivered», interrogazione E-000389/2020 del 23 gennaio 2020.

adottato e continueranno a mantenere normative *ex* art. 15 Direttiva *e-Privacy* non conformi al diritto dell'UE e alla Carta di Nizza. L'appello di 40 ONG, in una lettera indirizzata proprio alla Commissione a seguito delle pronunce *Privacy International* e *La Quadrature du Net*, spinge infatti nella direzione di evitare qualsiasi futuro tentativo di reintrodurre a livello dell'UE obblighi di conservazione dei metadati per scopi securitari [126], chiedendo allo stesso tempo di avviare «infringement procedures to ensure that national data retention laws are repealed in all member states concerned. Furthermore, we appeal to you to work towards an EU-wide ban on blanket and indiscriminate data retention practices that capture people's activities. We call on you to develop the European way so that it leads to an EU free of invasive surveillance» [127]. Diviene dunque chiaro, anche dinnanzi a tali richieste, come l'intervento della Commissione o la sua reiterata inerzia giocheranno un ruolo fondamentale per comprendere l'approccio che l'UE vorrà tenere in tale delicato ambito, anche nel rapporto con gli Stati membri che potrebbero, come si dirà in seguito, decidere di non intervenire e dunque mantenere in essere normative nazionali dissonanti ed incompatibili con la –ancor più chiara – posizione della CGUE.

9.3. *Le attese mosse di legislatori e Corti nazionali. Prime considerazioni a partire dalle sentenze della* Cour Constitutionnelle *belga e del* Conseil d'État *francese*.

Gli effetti delle sentenze *Privacy International* e *La Quadrature du Net*, infine, non possono che essere esaminati sotto un ulteriore quanto fondamentale profilo: quello delle attese reazioni degli Stati membri.

Come già avvenuto a seguito delle sentenze *DRI* e *Tele2*, la rilevante giurisprudenza della CGUE non ha mai mancato di produrre forti ricadute a livello nazionale, incidendo sia sulle scelte normative di Governi e

---

[126] Il riferimento qui è chiaramente al delicato e discusso compito affidato alla Commissione di valutare l'opportunità di adozione di una nuova normativa *ad hoc* in materia di *data retention*.

[127] Così si legge nella lettera disponibile all'indirizzo: https://www.statewatch.org/news/2020/october/joint-ngo-letter-no-data-retention-in-the-eu/.

Parlamenti, sia sulle decisioni delle Corti statali. Ed è proprio nel contesto nazionale che il dibattito sulla complessa disciplina della *data retention* ha trovato la sua più forte spinta, dinnanzi al silenzio del legislatore europeo e all'immobilismo della Commissione. Le più recenti decisioni della CGUE non possono dunque che rappresentare nuova linfa per quelle discussioni ed interrogativi che già da decenni sfociano in un serrato ma tutt'altro che risolutivo dialogo tra giudici nazionali e sovranazionali: nonostante i dubbi e le difficoltà interpretative poste alla base dei quesiti promossi nei numerosi rinvii pregiudiziali esaminati abbiano certamente trovato una risposta nelle sentenze *Privacy International* e *La Quadrature du Net*, le concrete conseguenze di simili pronunce non devono per questo essere considerate certe e necessariamente omogenee. Al contrario, quello che si è già in parte verificato e che sicuramente continuerà ad osservarsi anche in futuro, è il riproporsi di una problematica frammentarietà di soluzioni e approcci che difficilmente, a parere di chi scrive, troverà una composizione definitiva in tempi rapidi.

Questo del resto emerge con evidenza da alcune prime reazioni registratesi in Belgio e Francia: la Corte costituzionale belga da un lato e il Consiglio di Stato francese dall'altro, riprendendo nelle proprie mani i casi dai quali i rinvii pregiudiziali avevano tratto origine ed attuando così nel contesto interno i principi e i criteri indicati dalla CGUE, hanno promosso due differenti interpretazioni della medesima pronuncia, giungendo a due diversi esiti, già esemplificativi e premonitori di una difformità di soluzioni – e dunque anche di normative nazionali in materia – destinata a permanere nel prossimo futuro.

La Corte costituzionale belga, nell'*Arrêt* 22 aprile 2021, n. 57, ha dichiarato l'incompatibilità con il diritto dell'UE della normativa nazionale disciplinante la conservazione e l'accesso ai metadati per finalità di repressione dei reati, con una decisione che ha individuato con chiarezza nel regime di conservazione generalizzata ed indiscriminata un ineludibile elemento di contrasto con quanto affermato dalla giurisprudenza della CGUE. Il legislatore nazionale, dunque, si è rapidamente mosso, con un procedimento ancora in corso, per colmare il vuoto normativo creatosi e per disporre una nuova legge in materia di *data retention* che, sulla base dei testi disponibili, si fonderebbe, per la prima volta, sulla previsione di una conservazione mirata mediante l'impiego di criteri prettamente geo-

grafici. Sebbene tale pronuncia e i suoi effetti verranno ampiamente analizzati nel Capitolo 5, la sintetica descrizione dell'approccio tenuto da giudici e legislatore belgi qui tratteggiata è utile per comprendere la diversa interpretazione fornita invece dai giudici francesi.

Ad un solo giorno di distanza rispetto ai giudici belgi, il 21 aprile 2021, il *Conseil d'État* francese ha adottato una importante decisione, destinata a fare a lungo discutere: con la pronuncia n. 393099 i giudici francesi hanno ritenuto legittima e compatibile con il diritto dell'UE la normativa nazionale in materia di *bulk data retention* per scopi di garanzia della sicurezza nazionale [128]. Sul punto i giudici francesi hanno rinvenuto nel perdurante stato di emergenza, dovuto principalmente al pericolo di fenomeni terroristici, la sussistenza di quel requisito, specificato nella sentenza *La Quadrature du Net*, che condiziona la possibilità di adottare un regime eccezionale di conservazione generalizzata alla presenza di una minaccia reale e grave alla sicurezza nazionale. Unici profili problematici, rispetto ai quali è stato attribuito al legislatore nazionale un termine di tempo di sei mesi per l'introduzione di debite modifiche, sono stati individuati innanzitutto nell'assenza di un vaglio prevenivo vincolante da parte di un'autorità indipendente: la normativa esaminata dispone infatti solo l'obbligo per il Primo Ministro di ottenere il previo parere della *Commission Nationale de Contrôle des Techniques de Renseignement*, che non assume tuttavia carattere vincolante per le scelte del Governo; ulteriore profilo di incompatibilità con il diritto dell'UE è stato poi ravvisato nella mancata previsione di un periodico controllo volto ad accertare la persistenza di una minaccia grave per la sicurezza nazionale tale da giustificare il ricorso alla *bulk data retention*. Nel delineare però i pericoli concreti ed attuali che determinano un rischio per la sicurezza nazionale, la suprema Corte amministrativa francese ha richiamato non

[128] Si fa riferimento, in particolare, all'art. 34, co. 1, del *Code des postes et des communications électroniques*, nonché al *Code de la sécurité intérieure* e ai decreti 28 settembre 2015, n. 2015-1185 e 11 dicembre 2015, n. 2015-1639 che stabilivano un regime di conservazione generalizzata dei metadati della durata di un anno. Per una analisi della normativa, si rimanda a L. AZOULAI, D. RITLENG, M. BONINI, *L'État, c'est moi: il Consiglio di Stato francese, fra salvaguardia della sicurezza nazionale e protezione dei dati*, in *CERIDAP*, 26 luglio 2021.

solo la minaccia terroristica bensì ha fornito una definizione ampia e composita, comprensiva anche dei «risque d'espionnage et d'ingérence étrangère», l'«espionnage industriel ou scientifique» o ancora «menace graves pour la paix publique, liées à une augmentation de l'activité d groupes radicauzx et extrémistes» (para. 44), proponendo così una interpretazione piuttosto estensiva di quei criteri e limiti che la CGUE ha invece posto al fine di circoscrivere il ricorso a regimi eccezionali e fortemente invasivi della sfera privata.

Sotto il profilo poi della garanzia della sicurezza pubblica e dunque della repressione di reati, i giudici francesi hanno proposto ancora una volta un approccio complesso: pur riaffermando quanto sancito nella pronuncia *La Quadrature du Net*, con riferimento alla mancata proporzionalità di forme di conservazione generalizzata nell'ambito del contrasto alla criminalità grave, il Consiglio di Stato si è però poi allontanato nuovamente dalla posizione espressa dalla CGUE, ritenendo una forma di *targeted data retention* concretamente impraticabile ed inefficace, non potendosi in anticipo e *a priori* determinare i luoghi o i soggetti da sottoporre a regime di conservazione [129].

Insomma, pur rifiutando di seguire quanto suggerito dal Governo francese, che aveva richiesto ai giudici nazionali di ricorrere alla dottrina degli atti *ultra vires* e al concetto di *identité constitutionnelle* [130] al fine di

---

[129] «Il est impossible de définir par avance des zones géographiques où, par nature, aucun acte de criminalité grave susceptible de justifier la conservation des données de connexion ne pourrait survenir. Une obligation de conservation des données de connexion limitée à certaines zones géographiques, à supposer même qu'elle soit techniquement envisageable, ferait ainsi obstacle à l'action des services d'enquête dans les autres parties du territoire national lorsque de telles infractions y seraient commises. Enfin, aucune présomption de dangerosité ne saurait être légalement retenue à l'encontre de personnes en fonction de leur lieu de résidence ou d'activité professionnelle pour justifier la conservation de leurs données de trafic et de localisation. Une différence de traitement instaurée sur ces fondements serait contraire au principe constitutionnel d'égalité devant la loi», para. 54.

[130] Questo concetto era già stato in precedenza – sebbene piuttosto raramente – impiegato dalle Corti nazionali francesi quale limite all'applicazione del diritto dell'UE nel contesto interno nel caso in cui una fonte sovranazionale si fosse rivelata in contrasto con un principio inerente all'identità costituzionale della Francia (si legga sul punto D. ROUSEAU, *L'identité constitutionnelle, bouclier de l'identité nationale ou branche de l'etoile*

europeenne?, in L. BURGORGUE-LARSEN (a cura di), *L'identité constitutionnelle saisie par les Juge en Europe*, Edition Pedone, Parigi, 2011, p. 89 ss.). La richiesta avanzata dal Governo francese e il richiamo alla teoria degli atti *ultra vires*, ha catturato l'attenzione di molti studiosi per la potenziale riproposizione di una nuova *saga Taricco*: come ben riassunto da Perlo, «nella memoria difensiva depositata tra il gennaio e l'aprile 2021, il governo si è dichiarato contrario all'applicazione del diritto dell'Unione poiché "la risposta della Corte di giustizia dell'Unione europea alle questioni pregiudiziali che le erano state poste ha manifestamente violato il principio di attribuzione previsto dall'articolo 5 del TUE e, in tal modo, la Corte si è intromessa nelle competenze degli Stati membri, secondo quanto è previsto dall'articolo 4 par. 2 TUE". Inoltre, tale risposta "non permette di garantire l'effettività degli obiettivi di valore costituzionale che sono la salvaguardia degli interessi fondamentali della Nazione, la prevenzione dei reati e la ricerca degli autori di reati, e la lotta contro il terrorismo"», N. PERLO, *La decisione del Consiglio di Stato francese sulla data retention: come conciliare l'inconciliabile*, in *Rivista di Diritti Comparati*, 2, 2021, p. 168. In questa sede non si intende tuttavia entrare nel dettaglio della teoria del controlimite promossa dal Governo, che, come si è detto, non ha peraltro avuto seguito nella decisione dei giudici (per analisi specifiche e dettagliate su tale specifico profilo, si rimanda a J. ZILLER, *Il Conseil d'Etat si rifiuta di seguire il pifferaio magico di Karlsruhe*, in *CERIDAP*, 2, 2021; V. SIZAINE, J.-P. FOEGLE, *Les fausses notes du souverainisme juridique*, in *La Revue des Droits de l'Homme*, giugno 2021, p. 1 ss.; L. AZOULAI, D. RITLENG, *L'État c'est moi. Le conseil d'État, la sécurité et la conservation des données*, in *Revue Trimestrielle de Droit Européen*, 2, 2021, p. 349 ss.; M. AUDIBERT, *Conservation des données de connexion. Comment le Conseil d'État a sauvé la majorité des enquête judiciaires*, in *Vielle Juridique*, 96, 2021, p. 16 ss.). Quanto invece pare utile rilevare, in maniera funzionale alle riflessioni che si intendono svolgere, è come la posizione del Governo francese risulti paradigmatica della resistenza mostrata dinnanzi alle pronunce della CGUE e del tentativo, anche mediante tale discusso richiamo alla teoria degli atti *ultra vires*, di scongiurare gli effetti dirompenti di una possibile dichiarazione di incompatibilità della normativa nazionale in materia di *data retention* rispetto al diritto dell'UE. Del resto un simile approccio del Governo sul fronte interno risulta del tutto coerente con le iniziative promosse nell'ambito del procedimento di adozione del nuovo Regolamento *e-Privacy*: come si ricorderà, è stato proprio il Governo francese a proporre con grande forza e decisione il discusso e largamente criticato art. 2 (a) che esclude dall'ambito di applicazione della normativa qualsiasi attività di trattamento di dati o metadati derivanti da telecomunicazioni finalizzata alla garanzia della sicurezza nazionale. Una simile disposizione, ponendosi in forte contrasto con la più recente giurisprudenza della CGUE, rappresenta un evidente «example of Member States attempting to invalidate a CJEU ruling unfavourable to them by changing the provisions that constitute its basis», M. ROJSZCZAK, *The uncertain future of data retention laws in EU*, cit., p. 2. Ben può dirsi, dunque, che il Governo francese ha operato, all'indomani delle pronunce *Privacy International* e *La Quadrature du Net*, su due differenti fronti: "a

dichiarare non applicabile nel contesto nazionale il diritto dell'UE come interpretato dalla CGUE, ciò che emerge dalla sintetica analisi della sentenza francese è come il Consiglio di Stato abbia adottato una decisione controversa, che presenta taluni punti di distanza, se non di vero e proprio contrasto, rispetto a quanto affermato dai giudici di Lussemburgo nelle più recenti pronunce [131]. La ritenuta inefficacia e irrealizzabilità pratica nonché le possibili derive discriminatorie rilevate con riferimento alla soluzione di una conservazione mirata, insieme ad una estensiva lettura dei requisiti posti alla base dell'adozione di una forma di conservazione generalizzata per scopi di sicurezza nazionale, non possono che porsi in contrapposizione con quanto invece statuito con grande chiarezza dai giudici di Lussemburgo. Per questo, il complesso ed articolato – quanto innovativo – approccio dei giudici francesi ha sin da subito scatenato reazioni diverse: mentre vi è chi ha ravvisato nelle considerazioni e nelle soluzioni promosse dal Consiglio di Stato l'utile tentativo di fornire «a concrete shape to the challenging balance between national security and rights, which otherwise risks remaining relegated to a theoretical and abstract dimension», anche laddove l'interpretazione prospettata si distanzi da quella della giurisprudenza della CGUE [132], altri hanno invece criticato le posizioni della suprema Corte amministrativa francese, rappresentative di una «disingenous misinterpretation of the CJEU ru-

monte" nel dibattito normativo di adozione del Regolamento *e-Privacy*, e "a valle" nella posizione tenuta dinnanzi al Consiglio di Stato; in entrambi i casi, tali interventi mirano a frenare la forza espansiva dei requisiti fissati dalla giurisprudenza della CGUE in materie delicate e di grande rilievo per lo Stato quale la difesa della sicurezza.

[131] Un ulteriore punto controverso è ravvisato nell'interpretazione del requisito della gravità del reato: a parere del Consiglio di Stato «il ne résulte pas des énonciations de l'arrêt de la Cour de justice de l'Union européenne que le législateur serait tenu d'énumérer les infractions relevant du champ de la criminalité grave en se référant à des catégories strictement prédéfinies en droit interne. Le rattachement d'une infraction pénale à la criminalité grave a donc vocation à s'apprécier de façon concrète, sous le contrôle du juge pénal, au regard de la nature de l'infraction commise et de l'ensemble des faits de l'espèce», para. 38. I giudici francesi dunque parlano non di reati gravi, intesi in "termini assoluti", bensì di reati che presentino, proporzionalmente all'ingerenza perpetrata, un "sufficiente grado di gravità", valutato caso per caso.

[132] A. VEDASCHI, *Customizing La Quadrature du Net: the French Council of State, national security and data retention*, in *Bridge Blog*, 5 maggio 2021.

ling» [133], che rischia di alimentare, anziché sopire, il dibattito sulla conformità delle normative nazionali ai rigidi requisiti stabiliti a livello sovranazionale. Al di là delle valutazioni circa la correttezza o l'opportunità di tale decisione, comunque, quel che impone una seria riflessione è certamente il fatto che l'approccio seguito «sembra discostarsi dal parere del governo solo per quel che riguarda la strategia giurisprudenziale scelta per salvaguardare la normativa nazionale, a fronte di una sentenza europea di sostanziale condanna. Relativamente al merito, in effetti, il giudice amministrativo difende gli interessi e condivide le ragioni governative» [134]. I dubbi e le resistenze espresse dal Governo francese all'indomani della sentenza *La Quadrature du Net* sono stati così in parte ascoltati ed accolti dal Consiglio di Stato, che ha promosso una lettura dei requisiti stabiliti dalla giurisprudenza della CGUE lontana da quella registratasi invece, quasi contemporaneamente, in Belgio: qui, a seguito della sentenza della Corte costituzionale che ha quasi pedissequamente riproposto le considerazioni svolte dai giudici di Lussemburgo, il legislatore nazionale sta tentando, non senza difficoltà, di adottare una normativa che introduca per la prima volta una forma di conservazione *targeted*, fondata proprio su quei criteri geografici e soggettivi fortemente osteggiati invece dai giudici francesi.

Le rilevanti e così particolari differenze riscontratesi all'indomani delle sentenze *La Quadrature du Net* e *Privacy International* non possono che essere fortemente indicative da un lato di una persistente diversità di reazioni da parte degli Stati membri e della reticenza di alcuni di essi a rinunciare allo strumento della *data retention*, e dall'altro dell'importanza dell'intervento dei giudici nazionali; questi, laddove chiamati a pronunciarsi, avranno nei prossimi anni, il fondamentale compito di applicare

---

[133] I. BROWN, D. KORFF, *Exchanges of personal data after the Schrems II Judgement*, PE 694.678, luglio 2021, p. 40. Similmente Rojszczak: «in its argumentation, the Conseil therefore decided that the exception could become the norm. However, not only is such a concept not in line with the CJEU's position, it is also threatening to establish permanent restriction of fundamental rights under the pretext of combating a persistent terrorist threat», M. ROJSZCZAK, *The uncertain future of data retention laws in EU*, cit., p. 12.

[134] N. PERLO, *La decisione del Consiglio di Stato francese sulla data retention*, cit., p. 172.

nel contesto interno la giurisprudenza della CGUE e, conseguentemente, di valutare la compatibilità della disciplina normativa con i delicati principi fissati a livello sovranazionale. Come ben riassunto da Rojszczak, «just two days apart, the highest national courts of two Member States came to fundamentally different conclusions interpreting the same judgement of the CJEU. This situation is the best illustration that, despite the existence of a clear interpretation of the Court of Justice, it is still not possible to say that a universally accepted standard for the application of national retention regulations has yet been established» [135].

Proprio alla luce di queste prime reazioni degli Stati membri risulta chiaro come svolgere previsioni sul futuro della *data retention* rappresenti un esercizio alquanto difficile: seguendo pedissequamente la posizione espressa dalla CGUE, i legislatori nazionali non potrebbero ora che rinunciare definitivamente allo strumento della *bulk data retention* per finalità di garanzia della sicurezza pubblica. A seguito della sentenza *Tele2* rimanevano ancora taluni dubbi interpretativi quanto ad un divieto totale di conservazione generalizzata ed indiscriminata, dubbi sui quali i rinvii pregiudiziali susseguitisi negli ultimi anni si fondavano e rispetto ai quali i legislatori nazionali hanno ritenuto di poter riproporre forme di conservazione generalizzata, sebbene, come si è visto, meglio regolamentate e circostanziate rispetto al passato. Ebbene, simili interrogativi, che avevano anche spinto alla adozione di letture "difensive" della giurisprudenza della CGUE, paiono ora definitivamente risolti e chiariti in una direzione fortemente garantista, che ammette una forma di *bulk data retention* solo ed esclusivamente per scopi di sicurezza nazionale.

I legislatori degli Stati membri – e le Corti qualora tenute a pronunciarsi su tale materia – dovranno allora impegnarsi, nel prossimo futuro, a delineare regimi di conservazione mirata, superando quelle resistenze ma anche quelle concrete difficoltà e perplessità da più parti rilevate; avranno poi anche il compito di stabilire le condizioni e i precisi requisiti che devono necessariamente accompagnare strumenti di *bulk data retention* per finalità di tutela della sicurezza nazionale. I criteri e la terminologia ampia e vaga utilizzata dalla CGUE su questo delicato profilo dovranno essere così riempiti di significato dalle normative nazionali, chia-

[135] M. ROJSZCZAK, *The uncertain future of data retention laws in EU*, cit., p. 12.

mate a stabilire, ad esempio, i limiti temporali e le circostanze che consentono di considerare realizzata una minaccia reale alla sicurezza nazionale tale da giustificare l'impiego dei più invasivi sistemi di conservazione generalizzata; o ancora a definire le garanzie e i controlli posti a salvaguardia dell'eccezionalità di tale misura. Sarà quindi anche dall'esercizio di questa discrezionalità lasciata ai legislatori nazionali che si potranno valutare i risultati concreti della giurisprudenza sovranazionale degli ultimi anni: se gli Stati membri dovessero impiegare definizioni ampie, in grado di far rientrare nell'ambito della garanzia della sicurezza nazionale un gran numero di situazioni e dunque di attività di indagine, così da ampliare la possibilità di ricorrere alla *bulk data retention*, si potrebbero venire a creare nuove e complesse problematiche quanto alla compatibilità con il diritto dell'UE di simili misure [136]. Il percorso di allineamento alla giurisprudenza della CGUE nel contesto nazionale dipenderà poi senza dubbio anche da quanto la società civile, i pubblici ministeri o i giudici nel corso dei procedimenti penali sapranno rilevare eventuali difformità tra la disciplina interna e il diritto dell'UE. In questo contesto delicato, nel quale tante sono le variabili e gli attori da considerare, la posizione espressa dal Consiglio di Stato francese, così diversa da quella belga, è senz'altro indicativa di quanto, a livello nazionale, sia ancora possibile giungere a reazioni e soluzioni anche molto dissimili ed eterogenee.

In conclusione, nonostante la direzione del cammino risulti sempre più definita dalla giurisprudenza della CGUE, che nel corso dei decenni è intervenuta con decisione nell'assenza di una chiara normativa sovranazionale, la difficile sfida della *data retention* non può al momento dirsi completamente risolta e un rapido superamento delle attuali criticità e

[136] Una netta distinzione in termini di strumenti e regimi di conservazione impiegati a seconda delle finalità – sicurezza nazionale o pubblica – perseguite rappresenta peraltro una operazione tutt'altro che semplice. Questo perché «these two areas of state activity largely overlap. While there is no doubt that, for example, the foreign intelligence or gathering information relevant to the economic interests of the state are not linked to those concerning criminal law, the fight against terrorism is a task carried out by both law enforcement authorities (criminal procedure) and security services (national security). Furthmore, the legislation of some Member State salso gives national intelligence services powers to conduct criminal proceedings», M. ROJSZCZAK, *The uncertain future of data retention laws in EU*, cit., p. 12.

della frammentarietà di soluzioni nazionali sembra da escludersi. I rinvii ancora pendenti, le risposte attese dal legislatore europeo e le reazioni degli Stati membri delineeranno nei prossimi anni il futuro della *data retention* nell'UE: se le pronunce analizzate hanno stabilito e confermato alcuni punti saldi e certezze, saranno ora gli approcci tenuti dagli attori nazionali e sovranazionali a determinare una concreta assonanza con i principi delineati dalla giurisprudenza della CGUE o una rinnovata e continua distonia di scelte e di orientamenti, che potrebbe esasperare un dibattito e un dialogo già articolato e dai toni talvolta aspri.

CAPITOLO 3

L'UNIONE EUROPEA SI CONFRONTA CON L'ESTERNO: LA GARANZIA EXTRA-TERRITORIALE DEGLI STANDARD EUROPEI DI PROTEZIONE DEI DATI ALLA PROVA DELLA CORTE DI GIUSTIZIA DELL'UE NEI CASI DI *DATA TRANSFER* VERSO USA E CANADA

SOMMARIO: 1. La normativa europea in materia di trasferimento dati verso Stati terzi. – 2. Il trasferimento dati UE-USA al vaglio della CGUE: il caso *Schrems c. Data Protection Commissioner*. – 3. Dai principi *Safe Harbour* alle salvaguardie disposte nel *Privacy Shield*: un discusso compromesso. – 4. Un nuovo capitolo della *Schrems saga*: la sentenza della CGUE 16 luglio 2020, C-311/18, *Data Protection commissioner c. Facebook Ireland Ltd e Miximillian Schrems*. – 5. Le dirompenti ripercussioni della decisione *Schrems II*: il difficile futuro del trasferimento dati UE-USA (e non solo). – 6. La disciplina del trasferimento di PNR oltre i confini dell'UE: la bozza di accordo UE-Canada e il *Parere 1/15* della CGUE. – 7. Una ricognizione delle più significative implicazioni del *Parere 1/15* fuori e dentro i confini dell'UE. – 7.1. La necessaria rinegoziazione dell'accordo con il Canada e i dubbi quanto alla conformità alla Carta di Nizza degli accordi in materia di PNR vigenti. – 7.2. La Direttiva 2016/681 e un destino incerto: i rinvii pregiudiziali pendenti. – 8. Uno sguardo critico alla disciplina europea in materia di trasferimento dati verso Stati terzi: debolezze e successi in uno scenario in divenire.

1. *La normativa europea in materia di trasferimento dati verso Stati terzi.*

L'immagine complessa ed articolata della disciplina della raccolta, conservazione, accesso e trattamento di metadati per scopi securitari, così come tratteggiata nel previo Capitolo, non può dirsi completa senza la

disamina di un ulteriore ma imprescindibile profilo legato alla tutela della riservatezza e protezione dei dati, che tanto ha impegnato – e impegna tutt'ora – i giudici di Lussemburgo e le Istituzioni europee: il trasferimento di dati e metadati al di fuori dei confini dell'UE [1].

In un mondo sempre più globalizzato e digitalizzato, il valore economico dei dati elettronici risiede proprio nella loro "volatilità" e "aterritorialità" [2], cioè nella loro intrinseca propensione ad essere facilmente trasferiti in qualsiasi parte del mondo, in qualunque momento [3]. Ecco allora che l'enorme rilevanza economica, nonché la quotidianità ed automaticità delle operazioni di scambio e trasmissione di dati e metadati, hanno fatto ben presto sorgere complesse problematiche giuridiche: legislatori e giudici, nazionali ed europei, sono infatti stati posti dinnanzi alla moderna esigenza di garantire una tutela dei dati di tipo transfrontaliero, che sappia cioè travalicare i confini territoriali sovranazionali mediante la predisposizione di specifiche regole volte a disciplinare il trasferimento di dati verso Stati terzi – nell'ottica della presente disamina, "terzo" rispetto all'UE – e ad assicurare così un livello elevato di protezione dei diritti dei cittadini europei anche quando i dati non si trovino più ad essere sottoposti alla normativa europea o a quella dei suoi Stati membri.

Partendo dunque dalla consapevolezza della inevitabilità ed ineliminabilità del flusso transfrontaliero di dati [4], nonché dall'idea secondo cui

---

[1] Alcuni autori considerano i casi *Schrems* e il *Parere 1/15*, che verranno qui analizzati, come complementari rispetto alle previe decisioni *DRI* e *Tele2*: sul punto si veda S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, 3, 2016, p. 689. Altri, tra cui E. CELESTE (in *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019, p. 134 ss.), parlano significativamente di "effetto domino" della giurisprudenza della CGUE in materia di *data retention* nella dimensione esterna all'UE.

[2] Sul punto si legga J. DASKAL, *The un-territoriality of data*, in *Yale Law Journal*, 2, 2015, p. 326 ss.

[3] Per alcune interessanti riflessioni sull'importanza dello scambio di dati sotto il profilo economico ma anche geopolitico, si rimanda a M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, in *Rivista di Diritti Comparati*, 2, 2017, p. 187 ss.

[4] Mantelero evidenzia infatti il rapporto di «dipendenza reciproca esistente fra imprese commerciali europee ed imprese dei Paesi terzi, in un contesto di economia

«nell'era digitale, la promozione di standard elevati di protezione dei dati e la facilitazione del commercio internazionale devono necessariamente andare di pari passo» [5], il legislatore dell'UE ha inserito nel proprio apparato normativo – poi integrato e arricchito dalla giurisprudenza della CGUE – apposite rigide disposizioni in materia di *data transfer*. Sia il vigente GDPR sia la previa Direttiva 95/46/CE [6] hanno infatti previsto quale regola generale il divieto di trasferimento dati verso un Paese terzo, salvo stabilire poi alcune deroghe tassativamente elencate: tra queste, quella sicuramente più rilevante è la possibilità di trasmissione dei dati personali al di fuori del territorio UE nel caso in cui il Paese di destinazione garantisca un "livello di protezione adeguato" (art. 25 Direttiva 95/46/CE ed ora art. 45 GDPR). In altre parole, prendendo atto che nella maggior parte dei casi la transizione delle informazioni ha luogo «da un'area giuridica ad elevato grado di protezione per il diritto alla riservatezza verso ordinamenti ove il *right of privacy* non è circondato dalle medesime garanzie» [7], l'UE ha imposto quale condizione per il trasferimento di dati la garanzia, da parte dei Paesi destinatari, di una certa continuità del livello di tutela dei dati e della riservatezza offerto entro i confini europei, così che tale standard diviene il vero punto di riferimento e di raffronto [8]. Impiegando il concetto di "adeguatezza" della protezione dei diritti fondamentali, il legislatore europeo si è però espresso in maniera

---

dell'informazione», A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, p. 241.

[5] COMMISSIONE EUROPEA, *Comunicazione della Commissione al PE e al Consiglio: Scambio e protezione dei dati personali in un mondo globalizzato*, COM (2017) 7 final, 10 gennaio 2017.

[6] Mentre quest'ultima dedicava al trasferimento di dati personali verso Paesi terzi il Capo IV, che conteneva una disciplina piuttosto scarna – solo due disposizioni e pochi Considerando –, il Capo V del GDPR riserva invece a questa materia ben 8 articoli e 19 Considerando.

[7] S. SICA, V. D'ANTONIO, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, cit., p. 138.

[8] Si legga al proposito il Considerando 101, GDPR.

piuttosto vaga, destando sin da subito rilevanti perplessità. Sotto questo profilo, è dunque venuta in soccorso la giurisprudenza della CGUE: nella sentenza *Schrems*, di cui si parlerà a breve, è stato specificato che il termine "adeguato" implica che «non possa esigersi che un Paese terzo assicuri un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione. Tuttavia, (…) l'espressione deve essere intesa nel senso che esige che tale Paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali *sostanzialmente equivalente* a quello garantito all'interno dell'Unione in forza della Direttiva 95/46, letta alla luce della Carta» [9]. Il livello di tutela offerto dallo Stato terzo deve essere pertanto comparabile ma non identico a quello garantito nell'UE: ciò deve essere attestato mediante una «valutazione globale dei sistemi del Paese terzo, compresa la normativa sull'accesso ai dati personali da parte di pubbliche autorità preposte alle attività di contrasto, alla sicurezza personale o ad altro scopo d'interesse pubblico» [10]. Questa interpretazione giurisprudenziale del fondamentale concetto di adeguatezza è stata peraltro chiaramente e pedissequamente recepita dal legislatore europeo all'interno del GDPR, nel Considerando 104 [11].

Sotto il profilo procedurale, il GDPR attribuisce esclusivamente alla Commissione – e non più anche agli Stati membri, come previsto dalla

---

[9] CGUE 6 ottobre 2015, C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, para. 73, enfasi aggiunta. La Commissione sul punto ha affermato che «il livello di adeguatezza non comporta necessariamente una duplicazione pedissequa delle norme dell'UE. La prova consiste, piuttosto, nel determinare se, con la sostanza dei diritti alla riservatezza e rendendone l'attuazione, l'azionabilità e il controllo effettivi, il sistema estero in questione, nel suo insieme, offre il necessario livello elevato di protezione», COMMISSIONE EUROPEA, *Scambio e protezione dei dati personali in mondo globalizzato*, cit., p. 7.

[10] *Ibidem.*

[11] Nel Regolamento attualmente vigente sono inoltre specificati con maggiore precisione i criteri determinanti l'adeguatezza; l'art. 45, co. 2, in particolare, riconosce tra gli elementi da valutare al fine di determinare la sostanziale equivalenza: lo stato di diritto; il rispetto di diritti e libertà fondamentali, delle normative generali e settoriali, della giurisprudenza e dei diritti effettivi e azionabili; l'esistenza e l'effettività di una o più autorità di controllo indipendenti nel Paese terzo; gli impegni internazionali assunti.

previa Direttiva [12] – il compito di rilevare l'adeguatezza o meno della protezione assicurata dallo Stato terzo, mediante l'adozione di un atto di esecuzione [13]. Nel caso in cui venga rilevata la mancata adeguatezza [14], la Commissione dovrà avviare consultazioni con lo Stato terzo stesso, al fine di superare la problematica situazione (art. 45, co. 6): tali negoziati, che possono concretizzarsi in veri e propri accordi internazionali o nella determinazione di condizioni e principi specifici finalizzati a regolare il trasferimento dei dati verso un Paese terzo, sono volti a consentire l'adozione di una decisione di adeguatezza di carattere parziale cioè vertente su determinate categorie di dati – come nel caso della valutazione di Accordi di *data transfer* aventi ad oggetto i PNR, ovvero i codici di prenotazione dei passeggeri aviotrasportati –, oppure fondata sulle particolari condizioni di trasferimento e trattamento dei dati negoziate – come nel caso della Decisione riguardante il *data transfer* verso gli USA basata, come si dirà, sul rispetto dei requisiti fissati nel meccanismo *Safe Harbour* prima e *Privacy Shield* successivamente –.

---

[12] Nella Direttiva 95/46/CE veniva però prevista una differenza tra la decisione assunta dalla Commissione e quella invece adottata dagli Stati membri: solo la prima infatti assumeva efficacia vincolante per tutti gli Stati membri (art. 25, co. 6). Un ulteriore elemento di novità e discontinuità rispetto alla previa disciplina va ravvisato nel fatto che la capacità valutativa centralizzata attribuita alla Commissione si estende all'adeguatezza garantita non più unicamente dagli Stati al di fuori dell'UE bensì anche dalle organizzazioni internazionali, oltre a riferirsi espressamente anche ai trasferimenti successivi di dati personali verso ulteriori organizzazioni o Stati terzi.

[13] Si tratta cioè di atti unilaterali della Commissione che non devono essere confusi con gli accordi internazionali che possono – ma non necessariamente devono – porsi alla base delle valutazioni svolte nelle decisioni di adeguatezza. Sul punto si legga F. BORGIA, *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in *Il mercato unico digitale*, in *Diritto Mercato e Tecnologia, Numero Speciale*, 2017, p. 140 ss.

[14] Tale "inadeguatezza" può essere ravvisata anche in un momento successivo alla adozione della Decisione stessa, che non risulta dunque fissata una volta per tutte: al contrario, come indicato nel GDPR e come già in precedenza suggerito nella sentenza *Schrems*, viene previsto un riesame periodico delle decisioni adottate – almeno ogni quattro anni –, in modo da tenere debitamente conto degli sviluppi normativi, giurisprudenziali o di prassi eventualmente intercorse nel Paese terzo e tali da incidere sulle valutazioni di adeguatezza precedentemente effettuate (art. 45, co. 3, GDPR).

Pur prevedendo strumenti alternativi, per lo più adottati da singoli soggetti privati interessati a porre in essere le operazioni di *data transfer*[15], la Decisione di adeguatezza adottata dalla Commissione era e rimane certamente lo strumento maggiormente rilevante per la sua capacità di attestare in maniera generale l'adeguatezza dei trasferimenti verso uno Stato terzo. Ed è proprio con riferimento a questo controverso strumento di garanzia che la CGUE è stata più volte chiamata a pronunciarsi con decisioni storiche e dalla portata dirompente.

2. *Il trasferimento dati UE-USA al vaglio della CGUE: il caso* Schrems c. Data Protection Commissioner.

Le vicende giurisprudenziali che hanno fortemente impegnato la CGUE nella c.d. *Schrems saga* prendono avvio dalla Decisione 520/2000 adottata il 26 luglio 2000 dalla Commissione: quest'ultima, in assenza di una legislazione generale sulla protezione dei dati che consentisse di considerare l'ordinamento degli USA "adeguato" nel suo complesso[16], aveva

---

[15] Il GDPR, in maniera più puntuale rispetto alla previa Direttiva del 1995, istituzionalizza infatti anche altre modalità alternative di trasferimento dei dati da impiegarsi in assenza di una decisione di adeguatezza della Commissione. L'art. 46 stabilisce così la possibilità di trasferimento nel caso in cui il titolare o il responsabile del trattamento forniscano «garanzie adeguate e gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi», che si sostanziano nell'impiego di strumenti giuridicamente vincolanti quali norme vincolanti d'impresa, clausole tipo di protezione dei dati adottate da Commissione o autorità di controllo, codici di condotta e clausole contrattuali tipo stabilite tra le parti (art. 46, co. 2, c.d. *Standard Contractual Clauses*, che saranno oggetto poi di approfondimento anche giurisprudenziale) o, ancora, disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici. Per approfondimenti sugli interessanti strumenti alternativi di trasferimento dei dati, si rimanda a M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE,* cit., ma anche P. PIRODDI, *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo Regolamento generale sulla protezione dei dati,* in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015, p. 827 ss.; più ampiamente: C. KUNER, *Transborder data flows and data privacy law*, Oxford University Press, Oxford, 2013.

[16] Riflessioni sul diverso livello di tutela della riservatezza e della protezione dei dati garantito Oltreoceano negli USA possono essere ritrovate nei contributi di J. WHIT-

però ritenuto adeguate le tutele sancite dai principi del c.d. Approdo sicuro (o *Safe Harbour*), posto alla base – e quale precondizione – del trasferimento Oltreoceano dei dati raccolti per fini commerciali da società aventi sede nel territorio UE. Il meccanismo di *data transfer* così stabilito prevedeva sette principi e 15 FAQ (redatte dalla *Federal Trade Commission*) [17] cui le aziende importatrici stabilite in USA erano tenute ad attenersi al fine di poter ricevere, e quindi poi conservare e trattare, i dati provenienti dal continente europeo; l'adesione ed il rispetto dei requisiti individuati dall'Approdo sicuro aveva carattere puramente volontario – sebbene indispensabile per poter procedere al trasferimento – e si basava sull'autocertificazione delle aziende stesse, con un controllo meramente successivo ed eventuale da parte della *Federal Trade Commission*. Accanto a queste misure poste a garanzia dei diritti alla protezione dei dati e alla riservatezza, venivano però anche previste disposizioni di natura eccezionale in grado di consentire una deroga al rispetto dei *Safe Harbour principles* nel caso in cui fosse emersa la necessità di «soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia degli Stati Uniti»; per questi scopi, determinati in maniera estremamente ampia, le autorità pubbliche statunitensi avevano la possibilità di accedere ai dati provenienti dall'UE e conservati dalle aziende importatrici, senza essere vincolate al rispetto delle condizioni e delle tutele indicate dai principi dell'Approdo sicuro, che si applicavano dunque solo ai soggetti privati.

A seguito delle già richiamate importanti rivelazioni di Snowden, che avevano messo in luce l'invasività e la carenza di rigidi controlli e limitazioni ai meccanismi di sorveglianza massiva esercitata negli USA dalla NSA e dai servizi di intelligence nazionali, molti dubbi e preoccupazioni erano ben presto emersi tanto nella società civile quanto nelle Istituzioni

---

MAN, *The two Western culture of privacy: dignity versus liberty*, in *Yale Law Journal*, 113, 2004, p. 1151 ss.; P.M. SCHWARTZ, D. SOLOVE, *Reconciling personal information in the United States and European Union*, in *California Law Review*, 102, 2014, p. 1 ss.

[17] Per una approfondita analisi del contenuto dello strumento di Approdo sicuro, si legga, tra gli altri: M. P. QUEK, *Personal data privacy protection in an age of globalization: the UE-USA Safe Harbour compromise*, in *Journal of European Public Policy*, 3, 2002, p. 325 ss.; S. SICA, V. D'ANTONIO, *I Safe Harbour privacy principles: genesi, contenuti, criticità,* in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015, p. 801 ss.

europee: se inizialmente il meccanismo di tutele fornito dall'Approdo sicuro era stato accolto con entusiastica fiducia, tanto da spingere alcuni autori a ritenere l'innalzamento del livello di protezione dei dati trasferiti dall'UE agli USA come una conquista tutta europea, a testimonianza di un positivo *Brussels effect* [18], le dichiarazioni sui vasti programmi Prism e Upstream, che potevano interessare anche i dati provenienti dall'UE sulla base delle previsioni derogatorie inserite nei *Safe Harbour principles*, svelavano debolezze ed incertezze – se non addirittura le falle – circa la reale adeguatezza delle tutele offerte Oltreoceano [19].

In questo delicato e complesso contesto si inserisce la vicenda *Schrems*, originata proprio dai timori del cittadino austriaco Maximillian Schrems, che si era rivolto, senza successo, all'autorità garante della protezione dei dati irlandese al fine di ottenere una pronuncia di divieto di trasferimento dei propri dati personali da Facebook Ireland Ltd a Facebook Inc. con sede negli USA. Il caso, giunto dinnanzi alla *High Court*, veniva inviato alla CGUE tramite rinvio pregiudiziale vertente principalmente sull'interpretazione degli art. 25 e 28 della Direttiva 95/46/CE disciplinanti, come si è visto, il trasferimento di dati verso Paesi terzi e, in particolare, il ruolo delle autorità nazionali garanti della protezione dei dati [20].

---

[18] A. BRADFORD, *The Brussels effect*, in *Northwestern University Law Review*, 1, 2012, p. 1 ss.

[19] Del resto la stessa Commissione, nella Comunicazione al Parlamento e al Consiglio (COM (2013) 846 final del 27 novembre 2013),emblematicamente titolata *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, riconosceva come «l'accesso su larga scala, da parte dei servizi di intelligence, ai dati trasferiti negli USA da imprese certificate nell'ambito dell'Approdo sicuro solleva gravi problemi riguardanti la continuità dei diritti dei cittadini europei in materia di protezione in caso di invio dei loro dati negli Stati Uniti», para. 7 e 8. Precisando poi che i sistemi di sorveglianza massiva adottati negli USA non erano conosciuti né prevedibili all'epoca dell'approvazione del regime dei *Safe Horbour principles*, la Commissione reputava comunque eccessivamente negativo l'impatto – soprattutto economico – che l'abrogazione della Decisione di adeguatezza avrebbe provocato, preferendo dunque come miglior soluzione percorribile quella della apertura di un dialogo e di una discussione con le autorità americane finalizzata a risolvere le carenze e le problematicità emerse.

[20] Veniva chiesto in particolare se, sulla base della normativa indicata, le autorità di garanzia nazionali avessero l'obbligo di adeguarsi alla decisione della Commissione o se dovesse invece considerarsi sussistente in capo a tali autorità un potere autonomo di in-

I giudici di Lussemburgo, riformulando però i quesiti posti dai giudici del rinvio [21], giungevano ad occuparsi della validità della decisione 520/2000 della Commissione e dunque della sua conformità rispetto alla Direttiva 95/46/CE nonché ai diritti fondamentali tutelati dalla Carta di Nizza. Così, concentrando l'analisi sul contenuto dell'Approdo sicuro, la CGUE ravvisava nelle disposizioni di carattere eccezionale, già sopra richiamate, che consentivano alle autorità pubbliche statunitensi di accedere ai dati trasferiti dall'UE, l'affermazione della primazia delle esigenze di sicurezza nazionale, interesse pubblico e amministrazione della giustizia sul rispetto dei *Safe Harbour principles* e quindi sulla garanzia di quell'elevato standard di tutela della riservatezza e protezione dei dati valutato come adeguato dalle Istituzioni europee. Ciò che veniva messo in discussione dalla Corte non era la legittimità dell'interesse "sicurezza nazionale", considerato certamente capace, entro precisi limiti, di giustificare la compressione e l'interferenza nei diritti fondamentali: quanto veniva ritenuto problematico era piuttosto il carattere incondizionato e generalizzato delle operazioni di conservazione, accesso ed utilizzo di dati e metadati che le pubbliche autorità statunitensi potevano porre in essere, in assenza di regole chiare, prevedibili e conformi al principio di proporzionalità e necessità. Con un evidente richiamo ai requisiti e principi già stabiliti sul fronte interno all'UE nella sentenza *DRI*, di poco precedente, i giudici stabilivano dunque con forza come non potesse ritenersi limitata

dagine e di messa in discussione della valutazione svolta dall'organo europeo. Più ampiamente sul rinvio pregiudiziale e sulle questioni promosse dai giudici irlandesi si legga M. TZANOU, *EU regulation of transatlantic data transfers and online surveillance*, in *Human Rights Law Review*, 17, 2015, p. 545 ss.

[21] «Al fine di fornire una risposta completa a detto giudice, occorre verificare se tale decisione sia conforme ai requisiti risultanti da detta Direttiva, letta alla luce della Carta», para. 67. La CGUE si è comunque pronunciata anche con riferimento ai poteri delle autorità garanti nazionali attribuiti dalla Direttiva 95/46/CE: pur affermando, in estrema sintesi e per quanto qui interessa, l'effetto vincolante prodotto dalla Decisione di adeguatezza adottata dalla Commissione e dunque l'impossibilità di adottare atti in diretto contrasto con le valutazioni svolte a livello centralizzato europeo, le autorità di garanzia nazionali devono però sempre disporre del potere di sollevare questioni di legittimità della Decisione di adeguatezza per via indiretta dinnanzi ai giudici nazionali, i quali poi, mediante rinvio pregiudiziale, possono attivare il ruolo esclusivo di controllo della CGUE.

«allo stretto necessario una normativa che autorizza in maniera generale la conservazione di tutti i dati personali di tutte le persone i cui dati sono stati trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito e senza che sia previsto alcun criterio oggettivo che permetta di delimitare l'accesso delle autorità pubbliche ai dati e il loro uso ulteriore a fini precisi, rigorosamente ristretti ed idonei a giustificare l'ingerenza che sia l'accesso sia l'utilizzazione di tali dati comporta», para. 93. Un dettagliato vaglio di proporzionalità delle misure disposte dall'Approdo sicuro, sulla base dei criteri indicati all'art. 52 della Carta di Nizza e similmente a quanto svolto rispetto alla DRD, non si era tuttavia reso necessario nel caso *Schrems*: la CGUE affermava infatti preliminarmente che «una normativa che consente alle autorità pubbliche di accedere in maniera generalizzata *al contenuto* di comunicazioni elettroniche pregiudica il *contenuto essenziale* del diritto fondamentale al rispetto della vita privata», para. 94, enfasi aggiunta. Veniva poi riconosciuta anche la violazione del nucleo essenziale del diritto ad una tutela giurisdizionale effettiva: l'assenza di rimedi e di un controllo giurisdizionale effettivo nonché la mancanza di misure volte a garantire la possibilità di rettifica o la cancellazione dei dati, erano stati considerati elementi sufficienti a pregiudicare il contenuto essenziale del diritto tutelato all'art. 47 della Carta di Nizza. Tali considerazioni venivano ritenute sufficienti per dichiarare la decisione di adeguatezza esaminata non conforme ai criteri indicati all'art. 25 della Direttiva 95/46/CE e dunque invalida.

La relativamente breve decisione della CGUE, dagli effetti, come si vedrà, dirompenti su entrambe le sponde dell'Oceano Atlantico, presenta dunque importanti elementi di novità quanto alla determinazione della legittimità di sistemi di sorveglianza, nonché rilevanti spunti di riflessione sullo strumento della decisione di adeguatezza. Sotto il primo profilo, i giudici di Lussemburgo proponevano una inedita valutazione del requisito della lesione del nucleo essenziale dei diritti fondamentali [22], stabilendo

[22] In questa pronuncia, peraltro, per la prima volta la CGUE affermava «the idea that fundamental rights must be understood as having a 'hard core' that should remain outside the scope of application of the balancing test», T. OJANEN, *Making the essence of*

per la prima volta una netta distinzione tra l'ingerenza nei diritti fondamentali provocata dalle operazioni di accesso e trattamento di dati relativi al contenuto delle comunicazioni, e l'invasione nella sfera privata causata invece dalla conservazione ed accesso ai soli metadati che non assume, coerentemente con quanto stabilito nella sentenza *DRI*, gravità tale da incidere sul nucleo essenziale dei diritti fondamentali in gioco. Una distinzione, quella proposta, che, come già richiamato anche nel Capitolo 2, non ha mancato di far discutere: la riconosciuta capacità dei soli metadati di fornire una precisa ed accurata descrizione di abitudini e stili di vita degli utenti ha fatto sorgere significativi dubbi quanto alla correttezza e coerenza di una rigida distinzione tra contenuto delle comunicazioni e metadati nella determinazione del grado di ingerenza nella sfera personale [23].

Sotto il secondo profilo, quello cioè relativo al vaglio che la Commissione è chiamata a svolgere al fine di verificare l'adeguatezza delle tutele offerte nello Stato terzo, risulta chiaro dalla disamina dei giudici di Lussemburgo come il controllo di adeguatezza non possa limitarsi ai soli

fundamental rights real: the Court of Justice of the EU clarifies the structure of fundamental rights under the Charter, in *European Constitutional Law Review*, 12, 2016, p. 325.

[23] Ciò che è stato oggetto di critica e di perplessità, oltre al ragionamento seguito dalla CGUE nel caso specifico, è la mancanza di chiarimenti quanto all'esatto significato del "contenuto essenziale" di un diritto fondamentale: come rilevato da Tzanou, «it has been ambiguous as to whether the essence of fundamental rights under art. 52, para. 1 refers to the common and universal essence of a fundamental right or whether it can have a different meaning in each particular case», M. TZANOU, *EU regulation of transatlantic data transfers and online surveillance*, cit., p. 558. Riconoscendo questa incertezza, Pfisterer ha suggerito che «the Court should move beyond what was stated and implied in the Digital Rights and Schrems cases and provide a more in-depth rationale as to why the measures in dispute compromise the respective essence of the right to privacy and right to protection of personal data», V. PFISTERER, *The right to privacy. A fundamental right in search of its identity: uncovering the CJEU's flawed concept of the right to privacy*, in *German Law Journal*, 20, 2019, p. 733. Sul punto anche Lenaerts ha messo in evidenza come, in assenza di una definizione che permetta di comprendere il concetto di "contenuto essenziale" in maniera univoca, tale requisito vada interpretato caso per caso, a seconda della intensità e dell'estensione della "compressione" del diritto in gioco (così K. LENAERTS, *Limits on limitations: the essence of fundamental rights in the EU*, in *German Law Journal*, 20, 2019, p. 781 ss.).

principi e requisiti disciplinanti le operazioni poste in essere da soggetti privati bensì debba estendersi anche alle condizioni e alle garanzie regolanti il trattamento dei dati svolto dalle autorità pubbliche, ad esempio di *law enforcement* o intelligence, nel loro complesso [24]. Questo perché la necessaria sussistenza della sostanziale equivalenza delle salvaguardie disposte dallo Stato ricevente rispetto a quanto stabilito nell'UE non può conoscere deroghe ed eccezioni neppure quando l'adozione di sistemi di accesso e trattamento di dati (contenuto e metadati) sia motivata da esigenze securitarie e neppure quando le operazioni rappresentanti una forma di ingerenza nella sfera privata degli utenti europei siano svolte da autorità pubbliche dello Stato terzo ricevente [25].

3. *Dai principi* Safe Harbour *alle salvaguardie disposte nel* Privacy Shield*: un discusso compromesso.*

La decisa sentenza della CGUE aveva sin da subito comportato rilevanti conseguenze, innanzitutto in ambito economico: le imprese stanzia-

---

[24] Questo aspetto è stato peraltro chiaramente accolto dal legislatore europeo che nel GDPR, all'art. 45, co. 3, lett. a), include espressamente tra gli elementi che la Commissione è tenuta a considerare nella sua valutazione di adeguatezza anche «la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali)».

[25] Per una più ampia analisi di questa rilevante pronuncia, si legga, tra i molti: S. PEYROU, *La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques*, in *Journal de Droit Européen*, 2, 2015, p. 395 ss.; P. FALLETTA, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c. DPC, C-362/14)*, in *Federalismi.it*, 24, 2015, p. 1 ss.; S. CARRERA, E. GUILD, *The end of Safe Harbour: what future for EU-US data transfers?,* in *Maastricht Journal of European and Comparative law*, 3, 2015, p. 651 ss.; 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'informazione e dell'informatica*, 4, 2015, p. 755 ss.; R. DE SIMONE, *Corte di giustizia dell'UE, Grande Sezione, sentenza 6 ottobre 2015, in causa C-362/14, Maximillian Schrems c. Data Protection Commissioner,* in *Rivista italiana di diritto pubblico comunitario*, 4, 2015, p. 1793 ss.; X. TRACOL, *"Invalidator" strikes back: the harbour has never been* safe, in *Computer Law and Security Review*, 3, 2016, p. 1 ss.

te nell'UE potevano infatti legittimamente trasferire dati verso gli USA solo mediante l'impiego dei complessi ed onerosi strumenti di *data transfer* alternativi alla Decisione di adeguatezza della Commissione [26], determinando così il venirsi a creare di una situazione di forte confusione ed incertezza dovuta alle disomogenee – e talvolta poco attente – soluzioni adottate dai singoli operatori privati. La prioritaria necessità di addivenire rapidamente ad una chiara via d'uscita da tale problematica *empasse*, era così sfociata, in – relativamente – poco tempo e grazie a colloqui intensificati, nella predisposizione di nuovi principi inseriti nello strumento *Privacy Shield* (o Scudo per la privacy), volti ad assicurare l'adeguatezza delle tutele garantite nelle operazioni di trasferimento e trattamento dei dati indirizzati negli USA [27]. Tale nuovo meccanismo regolante il flusso dei dati UE-USA si presentava senza dubbio maggiormente garantista rispetto al previo assetto dell'Approdo sicuro: pur mantenendo il sistema di autocertificazione, i controlli circa il rispetto dei requisiti dello Scudo per la privacy venivano sensibilmente rafforzati [28], anche mediante l'introduzione della figura dell'*Ombudsperson* – di nomina presidenziale ma indipendente rispetto ai servizi di intelligence – e alla previsione di possibili ri-

[26] Si fa riferimento agli strumenti elencati all'art. 16 della Direttiva 95/46/CE, poi confermati e arricchiti da quanto disposto agli artt. 46 e 47 del GDPR, più sopra richiamati. Il mancato rispetto di tali meccanismi alternativi e dunque la disposizione di forme di trasferimento dati verso gli USA non conformi alla normativa europea vigente esponeva i *data exporters* al rischio di incorrere in significative sanzioni economiche, dovendo rispondere dei danni causati da illegittime operazioni di *data transfer* (per alcuni esempi, si leggano S. CARRERA, E. GUILD, *Safe Harbour or into the Storm? EU-US Data transfer after Schrems Judgement*, CEPD Liberty and Security in Europe Papers, novembre 2015, p. 1 ss.).

[27] Sulla base del meccanismo *Privacy Shield* la Commissione ha poi adottato la Decisione di esecuzione COM (2016)1250 *sull'adeguatezza della protezione offerta in ragione dello Scudo UE-USA per la privacy*, 12 luglio 2016.

[28] Per approfondimenti sul contenuto di questo accordo, si rimanda più ampiamente a S. CRESPI, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo scudo UE/USA per la privacy*, cit.; G. VERMEULEN, *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities*, in G. VERMEULEN, E. LIEVENS (a cura di), *Data protection and privacy under pressure. Transatlantic tensions, EU serveillance and Big Data*, Maklu, Anversa, 2017, p. 49 ss.

medi giurisdizionali accessibili dai cittadini europei che avessero ritenuto illegittimo il trattamento dei propri dati Oltreoceano; tutte queste tutele poi erano accompagnate, per la prima volta, dall'espresso impegno delle autorità pubbliche statunitensi di accedere e trattare i dati provenienti dall'UE solo in casi eccezionali e per specifiche finalità di interesse generale, secondo quanto previsto nella *Presidential Policy Directive*, c.d. PPD-28, del 17 gennaio 2014 che regolava la raccolta e l'accesso ai dati da parte delle autorità di intelligence [29] e nel *Judicial Redress Act* [30], entrambi introdotti nell'ordinamento statunitense proprio quale risposta all'acceso dibattito sorto a seguito del *datagate*.

Nonostante le richiamate e certamente rilevanti novità inserite nel

---

[29] Per una panoramica delle modifiche normative che il Congresso si era apprestato, non senza difficoltà, ad approvare a seguito delle rivelazioni di Snowden, si leggano A. BUTLER, F. HIDVEGI, *From Snowden to Schrems: how the surveillance debate has impacted US-EU relations and the future of international data protection*, in *Seton Hall Journal of Diplomacy and International Relations*, Special Issue 2015/2016, p. 1 ss. In estrema sintesi (e come richiamato anche nell'analisi effettuata dalla Commissione all'interno della Decisione di esecuzione COM (2016)1250, Allegato VI), la PPD-28, introdotta nel 2014 dall'allora Presidente Obama, prevedeva in capo ai membri della *Intelligence Community* l'onere di implementare nuove misure e *policies* volte a rafforzare la tutela della privacy all'interno dei programmi di sorveglianza. In questa *Directive* sono dunque fissati i principi che devono essere rispettati dalle agenzie di intelligence nelle operazioni di raccolta dati (quali: *executive branch authorization, purpose limitation, prohibition on collecting foreign private commercial information for competitive advantage, narrow tailoring of collection activities*) nonché gli scopi specifici – seppure estremamente ampi – per i quali un accesso ed analisi generalizzata dei dati può essere effettuato: combattere le minacce derivanti da attività di spionaggio, combattere il terrorismo, combattere la produzione e il commercio di armi di distruzione di massa, contrastare le minacce alla sicurezza informatica, le minacce alle forze armate o al personale militare e le minacce transnazionali inerenti una o più delle altre cinque finalità.

[30] Il *Judicial Redress Act*, approvato nel dicembre 2015, amplia anche ai cittadini stranieri le protezioni e garanzie giurisdizionali riconosciute in capo ai cittadini statunitensi (ad esempio il risarcimento dei danni da trattamento illecito dei dati). La portata garantista e innovativa di questa misura viene comunque da molti autori largamente critica e ridimensionata poiché gli oneri imposti per poter accedere a tali rimedi giudiziari risultano ancora estremamente pesanti, rendendo difficile la realizzazione di un effettivo accesso alla giustizia. Sul punto si legga: D. BENDER, *The Judicial Redress Act: A Path to Nowhere,* in *Privacy Advisor*, Issue 17, 2015.

Privacy Shield, le valutazioni espresse dalla Commissione quanto all'adeguatezza delle tutele disposte avevano sin da subito destato forti perplessità e critiche: in capo alle autorità statunitensi di *law enforcement* e intelligence permaneva infatti un'ampia facoltà di imporre alle aziende private con sede negli USA la trasmissione e messa a disposizione dei dati raccolti e conservati nello svolgimento delle attività commerciali. Le formule ambigue e i poteri fortemente discrezionali previsti dalle disposizioni normative statunitensi emergevano con chiarezza sia nella richiamata PPD-28, che prevedeva in maniera solo estremamente generica l'obbligo in capo alle autorità pubbliche di provvedere ad un accesso «quanto più possibile mirato» [31], sia nelle vaste finalità che consentivano operazioni di accesso e trattamento di dati in blocco (*in bulk*) [32]. Insomma i rilievi critici riportati e da più parti evidenziati [33] avevano fatto sorgere, già all'indomani del-

[31] Para. 71, Decisione di esecuzione COM (2016)1250.

[32] Para. 65, Decisione di esecuzione COM (2016)1250.

[33] Il Gruppo di lavoro Art. 29, ad esempio, aveva espresso, ai sensi dell'art. 30 Direttiva 95/46/CE, la propria opinione non vincolante sulla bozza di decisione di adeguatezza presentata dalla Commissione nel febbraio 2016. Nella *Opinion 01/2016 on the draft EU-US Privacy Shield adequacy decision* (WP 238, 13 aprile 2016) venivano dunque messe in luce le criticità e le lacune ravvisabili sia nei principi stabiliti nello Scudo per la privacy, sia nelle tutele offerte dall'ordinamento statunitense nel suo complesso. Particolarmente problematiche erano state ad esempio considerate le previsioni della PPD-28 che «has not removed the possibility for the indiscriminate collection of personal data in bulk and that the scale of such collection possibilities remains unclear and potentially broad» o ancora nel fatto che «the committment of the Office of the Director of National Intelligence not to conduct mass and indiscriminate collection of personal data (…) lacks of concrete assurances that such practice does not take place». Anche la dottrina aveva ampiamente espresso dubbi quanto alla reale adeguatezza del sistema di *data transfer* UE-USA: della stessa opinione di Vermeulen e Mantelero – che, nelle opere già citate in questo Capitolo, avevano manifestato profondi interrogativi quanto alla correttezza delle valutazioni svolte dalla Commissione – erano Brkan (M. BRKAN, *The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning,* in *German Law Journal,* 20, 2019, p. 876 ss.) e Tracol. Quest'ultimo aveva ribadito come «the Commission has relied on letters from various authorities of the US government appended as annexes 1 to 7 to the decision and not on relevant US law. These letters may however not shield US law from the application of the findings made by the Grand Chamber in the Schrems judgment. The latter implies substantial changes to the US law. The legal system of the

l'adozione della Decisione di adeguatezza della Commissione significativi dubbi quanto alla idoneità del meccanismo disposto a garantire un livello adeguato di tutela dei diritti fondamentali, nonché alla capacità dello stesso di superare illeso il rigido vaglio di proporzionalità e legittimità della CGUE.

Sulla base di tali considerazioni e similmente a quanto avvenuto con riferimento al sistema di *Safe Harbour principles*, anche le disposizioni dello Scudo per la privacy venivano così dopo poco tempo sottoposte all'attenzione dei giudici di Lussemburgo: oltre a due differenti ricorsi di annullamento azionati rispettivamente dalle ONG *Digital Rights Ireland*[34] e *La Quadrature du Net*[35] insieme ad altre associazioni e ONG francesi[36], un ulteriore importante rinvio era stato azionato dalla *High*

US has however not changed», X. TRACOL, *EU–U.S. Privacy Shield: The saga continues*, in *Computer Law and Security Review*, 32, 2016, p. 777. Similmente Terpan: «one major shortcoming is that the adequacy decision as regards Privacy Shield, like its predecessor, does not meet the CJEU requirement that the Commission should make an evaluation of US rules and guarantees. As these guarantees continue to be mostly based on declarations of intent, there are sufficient reasons to believe that the legality of the new regime is fragile», F. TERPAN, *EU-US data transfer from Safe Harbour to Privacy Shield: back to square one?*, in *European Papers*, 3, 2018, p. 1058. Perplessità erano state espresse anche con riferimento alla efficacia della figura dell'*Ombudsperson*, sia perché la procedura per accedere al vaglio di quest'ultimo risultava estremamente lunga e complessa, sia perché anche al termine del procedimento non veniva comunque mai confermato l'assoggettamento del ricorrente ad operazioni di sorveglianza (così M. TZANOU, *European Union regulation of transatlantic data transfers and online surveillance*, cit., in particolare p. 563).

[34] CGUE, T-670/16, *Digital Rights Ireland c. Commissione,* promossa il 16 settembre 2016: tale ricorso tuttavia è stato dichiarato, per ragioni formali, inammissibile con ordinanza del 22 novembre 2017. Il Tribunale ha infatti ritenuto insussistenti i requisiti di cui all'art. 263 TFEU, vista l'impossibilità di rinvenire in capo alla ricorrente un interesse all'annullamento della misura contestata.

[35] CGUE, T-738/16, *La Quadrature du Net e altri c. Commissione*, promossa il 25 ottobre 2016.

[36] Entrambi i ricorsi citati si fondavano sulla tesi secondo cui il carattere generalizzato della raccolta ed accesso ai dati per scopi securitari disciplinati dalla normativa statunitense fosse tale da pregiudicare il contenuto essenziale del diritto fondamentale al rispetto della vita privata (art. 7, Carta di Nizza), con la conseguenza che le considerazio-

Court irlandese. Il caso che i giudici irlandesi erano stati chiamati a dirimere, promosso dall'*Irish Data Protection Commissioner* (DPC) sulla base di un nuovo ricorso dell'attivista Maximillian Schrems [37], aveva imposto ancora una volta la necessità di un intervento chiarificatore della CGUE [38]: a quest'ultima veniva chiesto innanzitutto di accertare l'adeguatezza del livello di protezione offerto dalle c.d. *Standard Contractual Clauses* (d'ora in avanti SCC) definite dalla Commissione nella Decisione 2010/87, mentre solo secondariamente e funzionalmente al quesito richiamato veniva posta la questione della conformità alla Carta di Nizza della Decisione di adeguatezza adottata dalla Commissione sulla base delle condizioni dello Scudo per la privacy [39].

---

ni della Commissione sul livello adeguato di tutela assicurato dal *Privacy Shield* erano da ritenersi erronee.

[37] Il caso dinnanzi alla *High Court* risulta essere una diretta conseguenza della decisione *Schrems*: a seguito dalla invalidazione del sistema *Safe Harbour*, infatti, il DPC irlandese aveva chiesto all'attivista austriaco di riformulare la propria originaria doglianza, fondata sull'ormai annullata decisione 2000/520/CE. Schrems individuava così la fonte del flusso di dati tra la sede irlandese e quella americana di Facebook nell'accordo c.d. *Data transfer processing Agreement*, concluso tra le due aziende nel 2015 ed integrante le *Standard Contractual Clauses* indicate dalla Commissione nella Decisione 2010/87, modificata dalla Decisione 2016/2297 (c.d. *SCC decisions*). Ebbene Schrems aveva ritenuto le clausole contrattuali così disposte ed impiegate da Facebook per le operazioni di *data transfer* non idonee a garantire la sostanziale equivalenza alle tutele stabilite nel territorio dell'UE. Il DPC, vagliando le doglianze dell'attivista, aveva espresso dubbi circa l'adeguatezza della protezione garantita dalle SCCs disposte dalla Commissione nelle sue Decisioni, così da promuovere sul punto ricorso alla *High Court*.

[38] C-311/18, *Data Protection Commissioner v Facebook Ireland Limited e Maximillian Schrems*, promossa dalla *High Court* irlandese il 4 maggio 2018.

[39] Nella sentenza della *High Court* 4 maggio 2018, 4809/2018 dalla quale il rinvio pregiudiziale alla CGUE ha preso avvio, i giudici irlandesi rilevavano come «the issue whether the protections afforded to EU citizens whose data is transferred to the US are protected as required by Union law following the adoption of the Privacy Shield Decision and the establishment of the Privacy Shield ombudsperson requires to be determined by the Court in order to determine the validity of the SSC decisions», para. 45. Sul punto, poi, i giudici del rinvio avevano svolto uno studio approfondito dell'apparato normativo statunitense, ritenendo infine come programmi quali Prism e Upstream prevedessero sì una ricerca generalizzata, in grado di creare uno scenario di sorveglianza di massa, ma non indiscriminata grazie alla natura targettizzata della ricerca, che punta-

4. *Un nuovo capitolo della* Schrems saga*: la sentenza della CGUE 16 luglio 2020, C-311/18,* Data Protection Commissioner c. Facebook Ireland Ltd e Maximillian Schrems.

Dinnanzi alle continue critiche e alle perplessità mostrate avverso la reale adeguatezza delle tutele stabilite dai principi *Privacy Shield*, la risposta dei giudici di Lussemburgo al rinvio promosso dai giudici irlandesi risultava ancora una volta fortemente attesa e di fondamentale rilievo per determinare il futuro del *data transfer* tra UE e USA ma anche, più in generale, dello stesso strumento dell'adeguatezza [40]. Ecco allora che con la

va cioè ad individuare una cerchia di obiettivi determinati. Nonostante questo, però, simili programmi finivano col concretizzarsi, nel complesso, in un trattamento dei dati di natura massiva, in contrasto con il diritto dell'UE e con i rilievi e l'interpretazione fornita dalla CGUE nella sua ampia giurisprudenza sul punto. Anche sulla base di queste considerazioni, i giudici irlandesi ritenevano necessario l'intervento della CGUE.

[40] Questo complesso e delicato rinvio si inseriva peraltro in un contesto estremamente articolato e caratterizzato da posizioni contrastanti anche all'interno delle stesse Istituzioni dell'UE: la Commissione anche nella *Relazione sul terzo riesame annuale del funzionamento dello Scudo UE-USA per la privacy* (COM(2019)495 final, 23 ottobre 2019) confermava l'adeguatezza delle tutele poste in campo dagli USA e la corretta attuazione del meccanismo *Privacy Shield*, pur riconoscendone alcune criticità quali la carenza di efficaci controlli circa l'effettivo rispetto delle condizioni fissate nello Scudo per la privacy. Il Parlamento europeo nella Risoluzione del 5 luglio 2018 sull'adeguatezza della protezione offerta dallo Scudo UE-USA per la privacy (2018/2645 (RSP)), metteva invece in luce la sussistenza di ben più profonde lacune nell'ordinamento statunitense e nel meccanismo stesso di *data transfer* disposto dalla Commissione, fra cui spiccavano la rilevata assenza di una chiara e precisa definizione di "sicurezza nazionale" in grado di circoscrivere l'intervento delle autorità pubbliche, ma anche «i persistenti ostacoli in materia di ricorso per i cittadini non statunitensi soggetti a una misura di sorveglianza», para. 25, oltre alla problematicità del *Clarifying Overseas Use of Data* (c.d. CLOUD) *Act*, approvato il 23 marzo 2018 dal Congresso statunitense, con cui viene concesso alle autorità di *law enforcement* di accedere più facilmente ai contenuti delle comunicazioni, anche nel caso in cui esse siano conservate al di fuori dei confini degli USA; sulla portata di tale atto si rimanda a S.W. SMITH, *Clouds on the horizon: cross-border surveillance under the US CLOUD Act*, in F. FABBRINI, E. CELESTE, J. QUINN (a cura di), *Data protection beyond borders: transatlantic perspectives on extraterritoriality and sovereignity*, Hart, Oxford, 2021, p. 119 ss. Simili critiche erano peraltro state avanzate nuovamente dal Gruppo di Lavoro Art. 29 nel documento *EU-US Privacy Shield – First Annual Joint Review*, 17/EN WP 255, 28 novembre 2017, nel quale peraltro veniva contestato il

lunga e complessa sentenza del 16 luglio 2020 ribattezzata *Schrems II*, la CGUE ha innanzitutto considerato il quesito attinente alla validità del trasferimento dati UE-USA fondato sullo strumento delle SCCs [41]. È stato così sin da subito chiarito come l'obbligo di garantire la sostanziale equivalenza dell'elevato livello di protezione dei dati tutelato entro i confini dell'UE debba essere rispettato sia nel caso in cui il trasferimento verso Stati terzi avvenga sulla base di una decisione di adeguatezza, sia qualora esso si verifichi mediante utilizzo delle clausole contrattuali tipo (para. 96). Ne consegue che tra gli elementi da vagliare al fine di dichiarare la validità di un trasferimento dati verso Stati terzi sulla base di SCCs deve essere ricompreso non solo quanto disposto dalle clausole contrattuali convenute tra titolare o responsabile del trattamento (*data exporter*) e destinatario nel Paese terzo (*data importer*), ma anche gli «elementi rilevanti del sistema giuridico di quest'ultimo», con particolare riferimento alla possibilità di accesso da parte delle autorità pubbliche ai dati trasferiti dall'UE (para. 104). In tale delicato contesto un importante compito è attribuito alle autorità nazionali di controllo che devono verificare la correttezza delle operazioni di *data transfer* verso Stati terzi e il rispetto dei requisiti e principi fissati dal diritto dell'UE, disponendo peraltro di significativi poteri tra cui quello di sospensione o divieto di *data transfer* qualora «le clausole tipo di protezione dei dati non siano o non possano essere rispettate in tale Paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'UE non possa essere garantita con altri mezzi», para. 113.

---

mancato avvio da parte della Commissione di nuovi negoziati – o quanto meno di un rinnovato dibattito – circa il sistema di trasferimento dati UE-USA.

[41] Preliminarmente la CGUE ha anche riconosciuto come, sulla base della definizione di trattamento dei dati personali fornita dall'art. 4, punto 2 del GDPR, anche le operazioni consistenti nel trasferimento di dati personali da uno Stato membro verso uno Stato terzo rappresentino un trattamento di dati personali effettuato nel territorio dello stesso Stato europeo "di partenza" (para. 83); a tale trattamento deve conseguentemente essere applicato il GDPR e, più in generale, il diritto dell'UE. La possibilità che i dati trasferiti tra operatori economici (quali appunto Facebook Ireland e Facebook Inc.) subiscano nello Stato di destinazione un trattamento da parte di autorità pubbliche per scopi di tutela della sicurezza pubblica, difesa o sicurezza nazionale, durante o successivamente alle operazioni di trasferimento, «non può escludere detto trasferimento dall'ambito di applicazione del GDPR», para. 86.

Sulla base di queste importanti spiegazioni quanto ai parametri da valutare, la CGUE è quindi passata a determinare la validità della Decisione SCCs 2010/87 alla luce della Carta di Nizza e, in particolare, degli artt. 7, 8 e 47. È stato così precisato come le clausole tipo indicate dalla Commissione nella richiamata decisioni «mirino unicamente a fornire ai titolari o responsabili del trattamento stabiliti nell'Unione garanzie contrattuali che si applicano in modo uniforme in tutti i Paesi terzi e pertanto indipendentemente dal livello di protezione garantito in ciascuno di essi» (para 132), assumendo pertanto una valenza generale e standard, indipendentemente dalle specificità dell'ordinamento dello Stato terzo destinatario. Ne deriva dunque che le SCCs previste nella Decisione della Commissione abbisognano di essere integrate da misure suppletive disposte dal titolare del trattamento qualora ciò si renda necessario in considerazione delle peculiarità dell'ordinamento dello Stato terzo ricevente e delle tutele da esso offerte (para. 133). È quindi posto in capo all'operatore privato interessato ad effettuare il *data transfer* il difficile compito di verificare, caso per caso, ed eventualmente in collaborazione con il destinatario del trasferimento, «se il diritto del Paese terzo di destinazione garantisca una protezione adeguata, alla luce del diritto dell'UE, dei dati personali trasferiti sulla base di clausole tipo di protezione dei dati, fornendo, se necessario, garanzie supplementari rispetto a quelle offerte da tali clausole», para. 134. Laddove poi il titolare del trattamento che opera il trasferimento dei dati non adempia a tale delicato onere, saranno chiamate ad intervenire in subordine le autorità nazionali di controllo che potranno anche decidere di sospendere o vietare il *data transfer*: «tale ipotesi ricorre in particolare nel caso in cui il diritto del Paese terzo imponga al destinatario di un trasferimento di dati personali proveniente dall'UE obblighi in contrasto con dette clausole e, pertanto, atti a rimettere in discussione la garanzia contrattuale di un livello di protezione adeguato contro l'accesso delle autorità pubbliche di detto paese terzo a tali dati», para. 135.

Alla luce della responsabilità di integrazione posta in capo agli operatori privati e fondata su una valutazione caso per caso di quanto stabilito dall'ordinamento dello Stato ricevente, il solo fatto che le SCCs previste nella *SSCs Decision* non vincolino le autorità pubbliche degli Stati terzi verso i quali i dati personali provenienti dall'UE possono essere trasferiti,

non determina di per sé l'invalidità della Decisione SCCs della Commissione. Ciò che la CGUE individua piuttosto come elemento fondamentale per il vaglio di validità è la presenza di «meccanismi efficaci che consentano, in pratica, di garantire che sia rispettato il livello di protezione richiesto dal diritto dell'UE e che i trasferimenti di dati personali, fondati su siffatte clausole, siano sospesi o vietati in caso di violazione delle clausole o di impossibilità di rispettarle», para. 137. Tali meccanismi vengono individuati dai giudici sia nell'obbligo imposto ai *data exporter* e al *data importer* di verificare che le normative dell'ordinamento dello Stato terzo di destinazione consentano il rispetto del livello di protezione richiesto dal diritto dell'UE, sia nell'ulteriore obbligo in capo al *data importer* di «informare il titolare del trattamento della sua eventuale impossibilità di conformarsi a tali clausole», ed infine anche nel compito di controllo attribuito all'autorità garante nazionale. La presenza di simili oneri, salvaguardie e misure correttive è stata ritenuta dalla CGUE sufficiente per dichiarare la conformità della Decisione SCCs al diritto dell'UE: quest'ultima, prevedendo gli specifici meccanismi ed obblighi sopra citati, è in grado di assicurare il rispetto degli standard di tutela garantiti nel territorio europeo.

Chiarito questo punto di estremo rilievo, la CGUE ha poi valutato l'ulteriore e forse più attesa e delicata questione: quella della validità della Decisione di adeguatezza basata sui principi *Privacy Shield* relativa al trasferimento dati UE-USA. Nonostante l'opposta opinione espressa dall'Avvocato generale nelle sue Conclusioni, i giudici di Lussemburgo hanno considerato la valutazione di tale Decisione come dirimente e fondamentale per poter rispondere ai quesiti del giudice del rinvio [42]. È stata

[42] Sul punto la CGUE ha affermato come, «sebbene il ricorso del DPC nel procedimento principale metta in dubbio la validità della sola Decisione SCCs, tale ricorso è stato proposto dinnanzi al giudice del rinvio prima dell'adozione della decisione "scudo per la privacy". Nei limiti in cui (…) detto giudice interroga la Corte sulla tutela che deve essere garantita (…) nel contesto di un siffatto trasferimento, *l'esame della Corte deve prendere in considerazione le conseguenze derivanti dall'adozione della decisione "scudo per la privacy", occorsa nel frattempo*», para. 151, enfasi aggiunta. L'Avvocato generale Saugmandsgaard Øe, nelle sue Conclusioni del 19 dicembre 2020, aveva al contrario messo in guardia i giudici di Lussemburgo dai rischi di un simile vaglio, definito precipitoso e prematuro, non essendo peraltro chiara la rilevanza di una tale analisi ai fini della risoluzione del caso concreto.

così innanzitutto rilevata nelle disposizioni del *Privacy Shield*, similmente a quelle dell'Approdo sicuro, la presenza di una deroga al rispetto dei principi in essa stabiliti «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione di giustizia»: questa ampia eccezione consente dunque lo svolgimento di invasive operazioni di raccolta, accesso e trattamento dei dati da parte di autorità pubbliche statunitensi, che rischiano di inficiare e restringere le tutele offerte dal meccanismo dello Scudo per la privacy. Riprendendo i principi affermati nella propria consolidata giurisprudenza in materia di *data retention*, la CGUE ha esaminato – invero con una analisi più rapida e concisa di quella svolta dai giudici irlandesi del rinvio [43] – i programmi di sorveglianza di massa statunitensi. Ponendo particolare attenzione alle disposizioni della Sezione 702 del FISA, la CGUE ha affermato come la Corte FISA – l'autorità giudiziaria chiamata a valutare la legittima attuazione dei programmi di sorveglianza – non provveda ad autorizzare singole misure di controllo delle telecomunicazioni e dei dati personali quanto più ad approvare interi e complessi programmi di sorveglianza, *in toto* considerati, quali ad esempio i già citati Prism e Upstream. Non vengono pertanto effettuati da parte di tale organo giurisdizionale veri e propri controlli sulla legittimità e necessità delle operazioni di sorveglianza nonché sulla sussistenza di un nesso causale che legittimi l'ingerenza nella sfera privata disposta dai sistemi di accesso ai dati personali. Non emerge, dunque, da tali analisi l'esistenza nell'ordinamento statunitense di stringenti condizioni di autorizzazione dei programmi di sorveglianza attuati ai fini di intelligence esterna – cioè attinenti a dati provenienti dall'esterno dei confini USA –, così come non risultano neppure essere previste rigide garanzie per i cittadini stranieri i cui dati sono oggetto di siffatte operazioni di accesso e trattamento: l'intervento giudiziario posto in essere dalla Corte FISA, in altre parole, non assicura un livello di tutela che possa dirsi sostanzialmente equivalente a quello previsto entro il terri-

[43] Critiche alla brevità ed eccessiva rapidità – e financo superficialità – dello scrutinio della CGUE su tale punto, sono state mosse nel commento *National Security Law — Surveillance — Court of Justice of the European Union invalidates the EU-U.S. Privacy Shield. — Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd., ECLI:EU:C:2020:559 (July 16, 2020)*, in *Harvard Law Review*, 134, 2020, p. 1567 ss.

torio dell'UE. Sebbene poi i programmi azionati sulla base della Sezione 702 del FISA debbano essere attuati nel rispetto della PPD-28, la CGUE rileva come i requisiti fissati in tale *Directive* non «conferiscano agli interessati diritti nei confronti delle autorità statunitensi azionabili dinnanzi ai giudici. Pertanto, essa non è idonea a garantire un livello di protezione sostanzialmente equivalente a quello risultante dalla Carta, contrariamente a quanto richiesto dall'art. 45, co. 2, lett. a) GDPR, secondo il quale la constatazione di tale livello dipende dall'esistenza dei diritti effettivi e azionabili di cui godono le persone i cui dati sono stati trasferiti verso il Paese terzo di cui trattasi», para. 181. Passando poi al vaglio dei programmi di sorveglianza fondati sull'*Executive Order 12333*, che autorizza la NSA ad accedere direttamente ai cavi posti sotto l'Oceano Atlantico e attraverso i quali i dati vengono trasferiti dall'UE agli USA, operando dunque una raccolta ed un accesso diretto alle informazioni provenienti dall'UE, i giudici hanno rilevato come tali *Orders* non siano sottoposti ad un previo controllo giudiziario e non siano previsti neppure rimedi giurisdizionali successivi attivabili dai soggetti sorvegliati. I limiti posti all'impiego di tali misure, stabiliti dalla già richiamata PPD-28, non sono dunque tali da impedire lo svolgimento di operazioni di raccolta in blocco di un volume consistente di dati provenienti dall'esterno dei confini statunitensi nei casi in cui non sia possibile provvedere ad una raccolta mirata finalizzata al perseguimento di uno specifico obiettivo. Le normative in essere nell'ordinamento statunitense, proponendo criteri e condizioni estremamente vaghi, non risultano in grado di circoscrivere in maniera sufficientemente chiara e precisa la portata ed i limiti della raccolta in blocco operata dalle autorità di intelligence [44].

[44] La CGUE ha anche operato un vaglio sulla base di quanto disposto dall'art. 45, co. 2, lett. a) del GDPR che richiede, ai fini della valutazione di adeguatezza, un accurato controllo circa l'esistenza nell'ordinamento dello Stato terzo ricevente di mezzi di ricorso effettivo in sede amministrativa e giudiziaria. Allontanandosi da quanto espresso dalla Commissione nella Decisione di adeguatezza, i giudici di Lussemburgo hanno ritenuto che l'istituzione dell'*Ombudsperson*, disposta dal meccanismo *Privacy Shield*, non possa colmare le lacune che attengono alla tutela giurisdizionale dei diritti dei cittadini europei i cui dati sono stati oggetto di trasferimento verso gli USA. Le possibilità di ricorso predisposte dallo Scudo per la privacy, infatti, non si applicano alle operazioni di raccolta e accesso ai dati poste in essere dalle autorità di intelligence sulla base dell'im-

Sulla base di queste rapide considerazioni, la Corte ha concluso che la disciplina statunitense regolante l'accesso e trattamento da parte di autorità pubbliche di dati e metadati derivanti da Paesi esterni ai confini statunitensi non è in grado di superare il vaglio di proporzionalità e di stretta necessità, così che il livello di protezione dei dati fornito non può essere considerato sostanzialmente equivalente a quello garantito nell'UE. Con un esito finale del tutto simile a quello della prima sentenza *Schrems*, quindi, i giudici hanno dichiarato l'invalidità della Decisione di adeguatezza fondata sulle condizioni stabilite nel *Privacy Shield* con effetto immediato, rifiutando così di stabilire una modulazione nel tempo dell'efficacia della pronuncia che sarebbe stata invece certamente vantaggiosa per gli operatori commerciali e per le Istituzioni – europee e statunitensi – chiamate ora a trovare ancora una volta una difficile soluzione ad una situazione confusa e dalle conseguenze complesse e articolate [45].

5. *Le dirompenti ripercussioni della decisione* Schrems II: *il difficile futuro del trasferimento dati UE-USA (e non solo).*

La sentenza analizzata ha evidenziato la forte attenzione dedicata dalla CGUE alla tutela dei diritti fondamentali alla privacy, alla protezione dei dati e all'accesso alla giustizia, anche dinnanzi alle possibili interferenze

portante strumento dell'*Executive Order 12333*, così che non può ritenersi garantito un livello di protezione sostanzialmente equivalente a quello stabilito all'art. 47 della Carta di Nizza. L'*Ombudsperson* poi, pur essendo descritto come una figura indipendente dalle autorità di intelligence statunitensi, riferisce direttamente al Segretario di Stato da cui viene designato, risultando così parte integrante del Dipartimento di Stato degli USA; la revoca o l'annullamento della nomina di tale soggetto non sono accompagnate da specifiche e particolari salvaguardie volte a garantirne l'indipendenza dal potere esecutivo. Sui diversi profili di fragilità ed instabilità di questa figura di controllo si rimanda a F. BIGNAMI, *Schrems II: the right to privacy and the new illiberism*, in *MediaLaws*, 3, 2020, p. 311.

[45] L'annullamento della Decisione di adeguatezza di valenza generale non comporta un blocco del flusso di dati, vista la sussistenza di una serie di strumenti alternativi disposti dal GDPR e adottabili dai singoli *data exporter*: per queste ragioni la CGUE ha ritenuto di non dover sospendere l'efficacia temporale della propria dichiarazione di invalidità.

poste in essere per finalità securitarie da autorità pubbliche di Paesi terzi. Il rigido vaglio di proporzionalità e necessità e la stringente interpretazione del criterio di "adeguatezza" indicato dal legislatore europeo, pur risultando in linea di continuità con le previe decisioni in materia di *data retention* entro i confini dell'UE, impongono serie riflessioni sugli effetti e sulle reazioni prodotte nonché sui possibili sviluppi futuri.

Una simile analisi non può che prendere avvio dalle composite posizioni espresse dalla CGUE quanto all'impiego di clausole contrattuali tipo come strumento di trasferimento dati verso Stati terzi. Se da un lato infatti la *SSCs Decision* esaminata dai giudici non è stata dichiarata invalida, dall'altro rimangono in capo ai *data exporters*, ai *data importers* e, in via suppletiva, alle autorità nazionali di controllo, due obblighi estremamente onerosi e dagli esiti incerti: richiedere la predisposizione di ulteriori e specifiche clausole che, diversamente da quelle generali e standard previste dalla Decisione della Commissione 2010/87, sappiano tenere in considerazione le peculiarità dell'ordinamento dello Stato terzo ricevente, impone anche e innanzitutto l'onere in capo agli operatori privati di svolgere una complessa e preliminare valutazione circa la sussistenza nel Paese del *data importer* di normative volte a consentire la raccolta, accesso e trattamento di dati e metadati da parte di autorità pubbliche per finalità securitarie. Dovrà quindi essere esaminata la possibilità che tali disposizioni nazionali possano contrastare con la corretta applicazione delle clausole contrattuali tipo stabilite, determinando così la necessità di disporre ulteriori e più stringenti clausole aggiuntive; nel caso in cui si ravveda l'impossibilità da parte dell'operatore ricevente i dati di rispettare le SCCs anche addizionali, saranno gli stessi *data exporters* a dover provvedere alla sospensione delle operazioni di *data transfer*. Come ben può comprendersi, l'attribuzione a soggetti privati di un compito di controllo così delicato e complesso, ha destato non poche preoccupazioni: da un lato, gli operatori commerciali possono non disporre[46] delle specifiche conoscenze giuridiche – o di uffici legali

[46] «Whatever happens, big US internet industry are well placed to react to the ECJ decision through high resources and a lot of solicitor's capability. The real question is what will happen to SMEs and small businesses alike. With the 'new' SCC scheme, they will have to personally invest a lot of resources on appropriate legal assessment of

in house o, ancora, di risorse economiche tali da consentire il pagamento di servizi di consulenza legale esterna – necessarie per esaminare le discipline previste nell'ordinamento degli Stati terzi verso cui i dati sono diretti; le normative da controllare, inoltre, sono spesso difficili da individuare e comprendere, soprattutto se riguardanti attività di intelligence o di lotta alla criminalità grave; tali disposizioni, inoltre, non sono sempre di pubblico dominio, come le rivelazioni di Snowden hanno evidenziato. A tali difficoltà oggettive e concrete è poi da aggiungere il fatto che il titolare del trattamento e il ricevente hanno entrambi evidenti interessi economici nel garantire la continuità del flusso di dati e nel promuovere dunque una valutazione dell'adeguatezza del livello di tutele offerto dallo Stato terzo più flessibile e meno stringente di quella promossa dalla CGUE [47]. Dall'altro lato, se è certamente vero che un compito di controllo ed intervento "sussidiario" deve essere assegnato alle autorità garanti nazionali, va nondimeno detto come appaia piuttosto difficile ed improbabile che tali autorità possano svolgere una analisi della validità di ogni trasferimento dati verso qualsiasi Stato terzo e sulla base di clausole contrattuali che possono essere anche molto differenti

---

third-countries'rule of law, a responsibility which could indirectly become a deterrent for global trade and SMÈs extra-EU business», S. FANTIN, *The impact of Schrems II: a list of homeworks*, in *CiTiP Law Blog*, 23 luglio 2020.

[47] In altre parole, viene richiesto agli operatori commerciali di provvedere preventivamente ad un vaglio «of the law of a foreign country as a first step and then compare it against the EU data protection standard. Such an assessment goes beyond purely legal analysis and must take account of multiple factors (…). Normally this evaluation takes several months or even years and requires consultations with experts in the field. It is unrealistic to expect private entities to invest financial and human resources into a thorough analysis of the legal framework in the first place and then come up with some as of yet unclear "additional safeguards" to correct all the identified deficiencies», J. MIADZVETSKAYA, *Schrems II: on appropriate safeguards and risks of divergent application of EU law*, in *CiTiP Law Blog*, 29 settembre 2020. Come rilevato poi da Kuner, «the obligations that the Court puts on data controllers to investigate the level of protection will be even more difficult for transfers to countries such as China, where legislation dealing with law enforcement and the security services may be difficult to obtain or non-existent», C. KUNER, *The Schrems II judgement of the Court of Justice and the future of data transfer regulation*, in *European Law Blog*, 17 luglio 2020.

da operatore a operatore: per questo molti studiosi [48] hanno considerato del tutto irrealistico pensare che una singola autorità garante nazionale abbia la capacità – in termini di tempo, risorse umane ed economiche – di controllare l'adeguatezza delle salvaguardie predisposte dalle SCCs adottate da tutti gli operatori economici con riferimento a tutti i *data transfer* effettuati [49]. In ultima analisi, il sistema decentrato di controllo, scelto dall'UE per garantire localmente il rispetto delle normative in materia di protezione dei dati, potrebbe facilitare la creazione di un panorama estremamente frammentario e disomogeneo di approcci e reazioni, da quella maggiormente interventista a quella invece più immobilista, che potrebbe addirittura tradursi in una sorta di *forum shopping*, cioè nella decisione degli operatori economici di trasferire la propria sede in uno Stato membro in cui, ad esempio, vengano presentati meno ricorsi o vengano effettuati minori controlli in materia di *data transfer* [50].

Pur facendo salva la Decisione 2010/87, quindi, la stabilità e la concreta affidabilità delle SCCs come strumento di trasferimento dati escono piuttosto compromesse dal vaglio della CGUE: gli oneri posti in capo agli operatori privati nonché alle autorità garanti nazionali hanno creato certamente una situazione confusa, nella quale i *data exporters* si trovano,

---

[48] Bignami si chiede «How exactly is the relatively small Irish DPA supposed to monitor the third-country transfers of the disproportionate number of digital multinationals that have established their EU internal market presence via Ireland?», F. BIGNAMI, *Schrems II: the right to privacy and the new illiberism*, cit., p. 309.

[49] Il fatto che talune ONG stiano adottando, proprio a seguito della pronuncia *Schrems II*, una strategia di ricorsi "a tappeto" dinnanzi alle autorità nazionali di controllo, aventi in particolare ad oggetto le condizioni di trasferimento dati verso Stati terzi ad opera di giganti del web (sul punto si veda la strategia intrapresa dalla ONG NOYB, come si legge in https://noyb.eu/en/101-complaints-eu-us-transfers-filed), sta ponendo e sicuramente porrà anche in futuro una pressione notevole sulle spalle delle singole autorità garanti.

[50] «La sentenza in commento potrebbe addirittura essere all'origine di rischi di una frammentazione della tutela o, meglio ancora, di una tutela a macchia di leopardo, legata alle specificità ordinamentali e alla maggiore sensibilità di qualche autorità di controllo di uno Stato membro rispetto ad altre», R. BIFULCO, *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno*, in *Diritto Pubblico Europeo Rassegna Online*, 2, 2020, p. 2.

ancora una volta, ad operare "tra l'incudine e il martello", dovendo valutare se interrompere il *data transfer* o proseguirlo correndo il rischio di essere sanzionati nel territorio dell'UE nel caso in cui l'adempimento degli obblighi normativi imposti nello Stato terzo ricevente venga considerato incompatibile con la garanzia di un adeguato livello di protezione dei dati [51].

È proprio in questo panorama articolato ed incerto che il CEPD, ri-

[51] Con riferimento al trasferimento dati verso gli USA, le conseguenze della decisione della CGUE paiono dunque ancora incerte e indefinite: alla luce delle considerazioni svolte rispetto al meccanismo *Privacy Shield*, è possibile presumere che gli operatori privati (esportatori o riceventi i dati) o le autorità di controllo nazionali possano giungere a ritenere le SCCs stabilite come non realmente e concretamente applicabili da parte del *data importer* negli USA, in considerazione degli obblighi di trattamento e trasmissione imposti dalle autorità pubbliche statunitensi. Da ciò potrebbe quindi derivare la decisione di sospendere o vietare il flusso di dati fondato sulle SCCs. Questa lettura sembra supportata dalle interessanti ed articolate vicende registratesi in Irlanda: a seguito della pronuncia della CGUE passava infatti all'autorità garante irlandese l'arduo compito di determinare la necessità o meno di adottare specifiche salvaguardie aggiuntive rispetto a quelle previste nella Decisione SCCs, nonché di valutare il rispetto da parte dei *data importers* delle clausole stesse anche dinnanzi agli obblighi imposti dalle autorità pubbliche statunitensi. Nello svolgere tale vaglio, il DPC irlandese ha notificato il 28 agosto 2020 a Facebook Ireland Ltd una *Preliminary Draft Decision* volta ad intimare il blocco del trasferimento dati verso gli USA basato sulle SCCs identificate dalla Decisione della Commissione, affermando che l'ordinamento statunitense – e in particolare le normative attinenti ai sistemi di sorveglianza – non consente di considerare concretamente applicabili le salvaguardie predisposte dalle clausole contrattuali. Tale prima notifica del DPC è stata oggetto di impugnazione da parte di Facebook Ireland dinnanzi alla *High Court* irlandese, secondo taluni con un intento dilatorio volto a concedere alla Commissione il tempo necessario per negoziare un nuovo accordo sostitutivo dell'invalidato *Privacy Shield* (come sostenuto dalla ONG NOYB nel comunicato disponibile all'indirizzo https://noyb.eu/en/irish-high-court-judicial-review-against-dpc-admitted). I giudici irlandesi, con sentenza del 14 maggio 2021 *Facebook Ireland Limited c. Data Protection Commission and Maximilian Schrems*, 2020 No. 126 COM., hanno respinto il ricorso del colosso dei *social network*, ritenendo infondate ed erronee le accuse di quest'ultimo circa l'illegittimità della decisione del DPC e il mancato rispetto di specifiche regole procedurali disposte dalla normativa irlandese sulla protezione dei dati e sui poteri attribuiti all'autorità garante. La DPC dunque può ora procedere nelle proprie attività di valutazione delle tutele offerte da *Facebook Ireland Ltd* nelle operazioni di trasferimento dati a *Facebook Inc* negli USA. Questa decisione, così come quelle delle autorità di controllo operanti negli Stati membri dell'UE, saranno determinanti per comprendere il reale impatto della sentenza *Schrems II*.

conoscendo la complessità del compito attribuito ai singoli operatori e la difficoltà del vaglio da effettuare caso per caso, ha predisposto alcune linee guida quali le Raccomandazioni 1/2020 del novembre 2020, aggiornate poi il 18 giugno 2021, accompagnate dalle Raccomandazioni 2/2020 del 10 novembre 2020, relative rispettivamente alle possibili clausole suppletive volte ad integrare le SCCs disposte dalla Decisione della Commissione e alle garanzie essenziali che devono accompagnare le misure di sorveglianza poste in essere da Stati terzi al fine di assicurare la sostanziale equivalenza delle tutele disposte con il livello di protezione dei dati previsto entro i confini dell'UE. Questi documenti hanno lo scopo di coadiuvare i *data exporters* fornendo indicazioni sulle procedure da seguire [52], sulle fonti di informazioni da considerare e sui possibili esempi di misure supplementari da adottare [53], nonché predisponendo elementi utili «a valutare se misure di sorveglianza che consentono l'accesso ai dati personali da parte delle autorità pubbliche di un paese terzo, siano esse agenzie di sicurezza nazionale o autorità incaricate dell'applicazione della legge, possano configurare un'ingerenza giustificabile o meno» [54].

Tali documenti e i complessi requisiti e controlli che essi richiedono non hanno però mancato di provocare la decisa reazione del Governo statunitense: questo, infatti, ha significativamente sottolineato come, sulla base delle indicazioni suggerite dal CEPD, «each data exporter would be responsible, under extremely challenging conditions, for issuing its own

---

[52] Alcune utili fonti sono state identificate nella «giurisprudenza della CGUE o della Corte EDU, nelle decisioni di adeguatezza ove presenti, risoluzioni e relazioni di organizzazioni intergovernative, altri organismi regionali e organi e agenzie dell'ONU, nella giurisprudenza nazionale o nelle decisioni prese da autorità giudiziarie o amministrative indipendenti; nelle relazioni di istituzioni accademiche o organizzazioni della società civile», p. 41.

[53] Ad esempio inserire clausole che obblighino l'importatore a fornire informazioni, «sulla base dei suoi migliori sforzi, sull'accesso ai dati da parte delle autorità pubbliche, anche nel campo dell'intelligence», oppure clausole che stabiliscano l'obbligo di effettuare verifiche costanti in grado di determinare se i dati siano stati divulgati o trattati dalle autorità pubbliche e a quali condizioni. Altre clausole aggiuntive potrebbero vertere sulla comunicazione precisa e tempestiva delle richieste di accesso avanzate da autorità pubbliche a carico del *data importer* (pp. 30-40).

[54] Raccomandazioni 2/2020, p. 5.

individualized adequacy determination for each non-EU country in which it does business – the kind of determination that the Commission issues only after receiving information directly from, and conducting months of direct consultations with, the non-EU government concerned» [55]. Insomma, gli oneri posti sulle spalle di operatori privati vengono ritenuti eccessivi ed insostenibili, così che le autorità americane hanno chiesto al CEPD e alle Istituzioni europee in generale di adottare non solo un'interpretazione maggiormente flessibile e concretamente attuabile dei requisiti stabiliti dalla normativa e dalla giurisprudenza europea, bensì anche fissare criteri certi che guidino le autorità di controllo nazionali europee nella valutazione della condotta dei *data exporters*, evitando – o quanto meno limitando – la comminazione di sanzioni nei casi in cui le scelte operate da tali operatori privati siano «based on reasonable conclusions drawn when analyzing the available information on foreign law and practice» [56].

L'analisi delle criticità e delle problematiche applicative derivanti dalla decisione *Schrems II* non può però limitarsi alle considerazioni attinenti allo strumento delle SCCs: una delle più attese e dirompenti conseguenze della decisione analizzata è senza dubbio da rinvenirsi nella invalidazione della Decisione di adeguatezza 2016/1250. Dinnanzi al riproporsi della

---

[55] *Comments on proposed EDPB Reccomandations* 1/2020, 21 dicembre 2020.

[56] Toni estremamente critici rispetto ai requisiti e principi stabiliti nelle Raccomandazioni citate sono stati impiegati anche da alcuni studiosi, quali Rubinstein e Margulies: a loro parere, il CEPD «claims to offer a roadmap for data transfer, but actually supplies a road to nowhere with no workable options», I. RUBINSTEIN, P. MARGULIES, *Risk and rights in transatlantic data transfers: EU privacy law, US surveillance and the search for common ground*, in *LawFare Blog*, 10 marzo 2021; similmente sul punto si legga T. CHRISTAKIS, *'Schrems III'? First thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers*, in *European Law Blog*, 13 novembre 2020. Tali obiezioni e criticità sono peraltro state ribadite anche con riferimento alla Decisione di esecuzione (UE) 2021/914 del 4 giugno 2021, relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso Stati terzi: a seguito della sentenza *Schrems II*, che pure non aveva invalidato le *SSCs Decisions*, la Commissione ha infatti sentito l'esigenza di adottare una nuova decisione in materia di SCCs in grado di tenere conto delle specificazioni e precisazioni fornite dalla CGUE nella sua giurisprudenza. Sono state così inserite in tale decisione talune delle discusse condizioni fornite dal CEPD nelle Raccomandazioni prima esaminate.

medesima situazione già in passato verificatasi a seguito della prima pronuncia *Schrems*[57], anche a seguito della sentenza del 2020 gli operatori privati che avevano aderito volontariamente al meccanismo di *data transfer* del *Privacy Shield* hanno dovuto adottare e porre rapidamente in essere gli alternativi strumenti previsti dal GDPR al fine di poter proseguire le operazioni di trasferimento dati verso gli USA. Non stupisce, dunque, che dinnanzi a tale difficile ed incerta situazione sia stata a gran voce invocata la rapida adozione di una nuova Decisione di adeguatezza da parte della Commissione. Quest'ultima, come già avvenuto in passato e per la seconda volta nel corso di soli cinque anni, si trova ora dinnanzi all'arduo compito di rinegoziare con gli Stati Uniti un nuovo insieme di principi e condizioni che, similmente al *Safe Harbour* e al *Privacy Shield*, fissino specifiche salvaguardie in materia di protezione dei dati in grado di consentire l'approvazione di una Decisione di adeguatezza. Così, con il comunicato stampa congiunto, rilasciato il 10 agosto 2020 dal Commissario europeo per la giustizia Didier Reynders e dal *US Secretary of Commerce* Wilbur Ross, è stato annunciato l'avvio di un nuovo percorso di negoziazione che, pur volto al raggiungimento di un «enhanced EU-US Privacy Shield framework to comply with 16 July judgment of the CJEU»[58], si presenta caratterizzato da profonde difficoltà ed ostacoli[59]. Viene evidenziata dunque, sin da subito, l'esigenza di non ripetere gli errori del passato, affrettando le trattative con gli USA ed accettando solu-

[57] È bene sottolineare come la decisione *Schrems II* abbia avuto anche ripercussioni sul fronte giurisprudenziale: il richiamato ricorso di annullamento promosso nel caso *La Quadrature du Net c. Commissione europea*, T-738/16 si è infatti concluso con ordinanza del Tribunale europeo del 14 dicembre 2020, nella quale è stato riconosciuto che non vi era più luogo a statuire sul ricorso poiché «l'invalidité de la décision attaquée, produit, en l'espèce, des effets équivalents à ceux d'un arret d'annulation», para. 31.

[58] Come si legge in https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836.

[59] Non a caso lo stesso Reynders, in occasione di un incontro dinnanzi al Comitato LIBE del Parlamento europeo, il 3 settembre 2020, ha affermato che «There will be no quick fix. What we need are sustainable solutions that deliver legal certainty, in full compliance with the judgment of the Court», https://multimedia.europarl.europa.eu/en/committee-on-civil-liberties-justice-and-home-affairs_20200903-1345-COMMITTEE-LIBE_vd?auth_cloudf=c3e8a8d1-e536-ac08-b5a9-1a4fbc1f3951.

zioni di compromesso che rischiano di dimostrarsi poi deboli alla prova dei giudici di Lussemburgo. Del resto, come già da più parti rilevato, salvo il caso di una – al momento improbabile [60] – riforma dei discussi programmi Prism, Upstream e degli strumenti di regolamentazione dei sistemi di sorveglianza quali gli *Executive Order 12333*, pare del tutto plausibile ritenere che le criticità rilevate dalla CGUE nella pronuncia *Schrems II* ben potrebbero ripresentarsi anche rispetto ad una nuova Decisione di adeguatezza e ad un aggiornato Scudo per la privacy [61]. Alla luce di tali rilevate complessità, il dibattito per una composizione tra tutela dei diritti fondamentali e garanzia della circolazione dei dati tra UE e USA si presenta quindi come un processo lungo, travagliato, dagli esiti incerti [62], che spingono inevitabilmente a riflettere tanto sulla efficacia del

---

[60] Di tale opinione J. DASKAL, *What comes next: the aftermath of European Court's blow to transatlantic data transfers*, in *Just Security*, 17 luglio 2020. Ciò appare improbabile anche se si legge il *White Paper: Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S. Data Transfers after Schrems II*, elaborato nel settembre 2020 dal *Department of Commerce* statunitense, nel quale viene affermato come molte delle considerazioni espresse dai giudici di Lussemburgo sui rischi di accesso ai dati trasferiti negli USA risultino solo teoricamente fondate ma non rappresentanti la realtà dei fatti e delle pratiche concrete poste in essere dalle autorità di intelligence.

[61] Come ben affermato da Guido Scorza in un'intervista rilasciata ad Agenda Digitale il 17 novembre 2020, un problema di disallineamento tra due ordinamenti si risolve solo intervenendo su uno o entrambi gli ordinamenti, tanto che, in assenza di un intervento diplomatico o tecnico che riesca in questo arduo compito, ci saranno sempre ipotesi nelle quali i dati personali non potranno circolare. I rimedi contrattuali da soli non potranno risolvere il problema, così che «l'unica possibile conclusione è che è urgente che le diplomazie europea e statunitense si mettano alla ricerca di una soluzione più definitiva – anche se difficilmente sarà possibile identificarne una solida nel breve periodo come insegna la brevissima storia di Privacy Shield – mentre la comunità scientifica e quella degli addetti ai lavori (…) cerca rimedi e soluzioni capaci di identificare il maggior numero di possibili soluzioni temporanee e parziali».

[62] Dinnanzi alla improbabile adozione da parte degli USA di sostanziali riforme dei sistemi di sorveglianza e delle normative in materia, alcuni autori come Ian Brown e Douwe Korff nello studio *Exchanges of personal data after the Schrems II Judgement*, PE 694.678, luglio 2021 hanno individuato una più plausibile, per quanto complessa, soluzione nella promozione da parte degli Stati membri di accordi multilaterali finalizzati a limitare le attività di intelligence e a riportare le spinte pro-securitarie entro un rigido schema di tutela dei diritti fondamentali. Per Rubinstein e Margulies «a more ambitious

requisito di adeguatezza quanto sulle ripercussioni del rigido vaglio di proporzionalità e necessità svolto dalla CGUE anche rispetto a sistemi di raccolta, conservazione e accesso a dati e metadati posti in essere da autorità di *law enforcement* e di intelligence in Stati terzi.

6. *La disciplina del trasferimento di PNR oltre i confini dell'UE: la bozza di accordo UE-Canada e il* Parere 1/15 *della CGUE.*

Il lungo percorso verso la determinazione di un delicato punto di equilibrio tra tutela dei diritti fondamentali alla riservatezza e alla protezione dei dati da un lato ed esigenze securitarie dall'altro che ha impegnato la CGUE e le Istituzioni europee anche nella dimensione esterna ai confini dell'UE ha conosciuto una ulteriore importante tappa nel *Parere 1/15* pronunciato dai giudici di Lussemburgo il 26 luglio 2017.

Diversamente dalle sentenze già analizzate in materia di trasferimento dati, aventi ad oggetto primariamente dati e metadati raccolti da operatori commerciali privati nello svolgimento dei loro servizi, il Parere citato riguarda il trasferimento di una specifica categoria di dati, i *Passenger Name Records* (c.d. PNR) ovvero i codici di prenotazione relativi ai passeggeri aviotrasportati [63]. Gli operatori aerei, nel normale e corretto svol-

approach would entail a multilateral group of countries to identify and agree upon criteria for understanding "the rule of law" and "respect for human rights and fundamental freedoms" in the context of surveillance law. Reaching consensus on these criteria would in turn facilitate reviews of third county foreign surveillance laws and possibly incentivize legal reforms in countries that fall short of these multilateral standards», I. RUBINSTEIN, P. MARGULIES, *Risk and rights in transatlantic data transfers: EU privacy law, US surveillance and the search for common ground*, in *Roger Williams University Legal Studies Paper*, 18 febbraio 2021, p. 39. Sul punto si legga anche T. CHRISTAKIS, *Squaring the circle? International surveillance, underwater cables and EU-US adequacy negotiations*, in *European Law Blog*, 12 aprile 2021. Anche Scorza, nella richiamata intervista ha affermato come «l'unica vera possibile risposta sta nell'avvio di una discussione spedita, nella comunità internazionale, per l'identificazione di uno strumento pattizio capace di garantire la libera circolazione globale dei dati nel rispetto di poche ma insuperabili garanzie per gli interessati».

[63] I PNR contengono un elevato numero di informazioni: indirizzo, dati personali identificativi, forma di pagamento, itinerario di viaggio, numero di biglietto, informa-

gimento delle proprie attività, infatti, raccolgono e conservano nei sistemi automatizzati di controllo delle partenze un ampio numero di dati personali (i PNR appunto), rilasciati dai passeggeri al momento della prenotazione [64]. Soprattutto a seguito degli attentati alle Torri Gemelle, che hanno messo in luce la necessità di garantire una maggiore sicurezza dei trasporti aerei, questa tipologia di informazioni ha assunto un'enorme importanza nel campo della prevenzione e della lotta al crimine grave, dal terrorismo alle attività criminali di natura transfrontaliera (tratta di esseri umani, traffico di sostanze stupefacenti, etc.), grazie anche all'impiego di tecniche di intelligenza artificiale che rendono possibile la preventiva e sistematica analisi dei dati di passeggeri di voli internazionali, fornendo informazioni sui percorsi di viaggio ma anche creando connessioni tra una persona sconosciuta alle forze dell'ordine e un criminale noto.

Sulla base di queste enormi potenzialità, molti Stati hanno deciso di adottare normative che obbligano gli operatori aerei a fornire, a specifiche autorità di *law enforcement* o doganali, i PNR dei passeggeri per voli con destinazione o partenza o anche solo sorvolanti il proprio territorio nazionale. Gli Stati Uniti si sono per primi muniti di tale tipologia di legislazione, immediatamente dopo gli attacchi terroristici dell'11 settembre 2001, e sono stati seguiti in breve tempo da Regno Unito, Australia e Canada. Simili imposizioni avevano però sin dall'inizio creato non pochi problemi ai vettori aerei operanti nell'UE: come si è ampiamente visto, infatti, la Direttiva 95/46/CE stabiliva un divieto generale di trasferimen-

---

zioni relative al bagaglio ma anche alla frequenza dei viaggi (*frequent flyer information*); i PNR possono inoltre rivelare informazioni sensibili: esprimendo preferenze su un pasto o richiedendo la presenza di particolari apparecchiature mediche a bordo (*Special Service Request* o *Special Service Information*), vengono indirettamente fornite informazioni circa la religione o lo stato di salute del passeggero che rientrano appunto nella categoria di dati sensibili o 'categoria particolare di dati personali', secondo la denominazione utilizzata dal GDPR all'art. 9. Una utile definizione di PNR può essere quella fornita dalla *International Civil Aviation Organization* (ICAO), nelle sue *Guidelines on the PNR data* (2010).

[64] Per approfondimenti sulla storia e sul funzionamento dei sistemi di controllo basati sull'utilizzo dei PNR, si rimanda a G.A. CANNETTI, *Passenger Name Records tra istanze di sicurezza globale e tutela dei dati personali*, in *I quaderni europei. Il diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, 63, 2014, p. 86 ss.

to di dati provenienti dall'UE se non in presenza di una decisione di adeguatezza o di altre misure alternative. In assenza di tali disposizioni, gli operatori aerei si trovavano a dover scegliere se rispettare l'obbligo di trasmissione dei PNR imposto dallo Stato terzo verso il quale il volo era diretto, violando così il divieto di trasferimento dati stabilito a livello dell'UE o, viceversa, rifiutare di trasmettere i dati alle autorità straniere rischiando di perdere così le proprie rotte da e verso tali Stati [65]. Di fronte a questa situazione così problematica diventava dunque sempre più urgente il raggiungimento di accordi internazionali tra Paesi terzi e UE in materia di PNR, al fine di stabilire condizioni e tutele specifiche per i dati trasferiti e garantire così un livello adeguato di protezione dei dati e della privacy tale da consentire lo svolgimento di legittime operazioni di *data transfer*.

Da questa esigenza hanno così avuto origine diversi importanti accordi siglati tra UE e USA [66], nonché con Australia [67] e Canada. Ed è proprio

---

[65] A. VEDASCHI, G.M. NOBERASCO, *From DRD to PRN: looking for a new balance between privacy and security*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and trans-Atlantic relations*, Hart Publishing, Oxford, 2015, p. 67 ss.

[66] Si fa riferimento all'accordo e alla relativa Decisione di esecuzione della Commissione 2004/535/CE del 14 maggio 2004. Tale disposizione non ha avuto tuttavia vita lunga: con sentenza 30 maggio 2006, Cause riunite C-317/04 e C-138/04, *Parlamento europeo c. Consiglio e Commissione*, la CGUE aveva infatti annullato la richiamata decisione per carenza di una corretta base giuridica e senza dunque addentrarsi nella valutazione del contenuto delle previsioni inserite nell'accordo. Il trattamento dati disciplinato dall'accordo non era volto, secondo lo scrutinio dei giudici, a garantire la prestazione di un servizio ma risultava piuttosto finalizzato a contribuire alla pubblica sicurezza e allo svolgimento di attività dello Stato terzo in materia di diritto penale. Considerando che, ai sensi dell'art. 3, co. 2, Direttiva 95/46/CE erano esclusi dall'ambito di applicazione di tale normativa i dati correlati allo svolgimento di attività proprie degli Stati o delle autorità statali estranee ai settori di attività dei singoli, ne derivava che, nel caso di trasferimento di PNR oggetto di esame, la Direttiva in materia di protezione dei dati non poteva essere applicata e che, conseguentemente, l'art. 95 CE non costituiva base giuridica corretta della Decisione, che andava piuttosto individuata nel Terzo Pilastro di cooperazione di polizia e giudiziaria in materia penale. Sebbene la problematica della base giuridica sarà poi in parte superata dall'abbandono della divisione in Pilastri, questa decisione verrà più volte richiamata, come già emerso nel Capitolo 2, dai Governi nazionali nelle diverse controversie in materia di *data retention*; ciò al fine di supportare la tesi secondo cui le operazioni di accesso ai dati svolte da autorità pubbliche debbono

con riferimento a tale ultimo Stato terzo che prende origine il rilevante *Parere 1/15*. Dopo la scadenza del primo accordo [68], infatti, il Consiglio dell'UE aveva avviato nuovi negoziati con le autorità canadesi, conclusisi il 25 giugno 2014 con la firma di una bozza di accordo; tale documento veniva dunque inviato per la definitiva approvazione al Parlamento europeo [69]. Quest'ultimo però, trovandosi a decidere in un momento in cui il livello di attenzione per la tutela della vita privata e la protezione dei dati

essere considerate escluse dall'ambito di applicazione del diritto dell'UE e dunque sottratte al vaglio e ai rigidi requisiti stabiliti dalla giurisprudenza della CGUE (per approfondimenti su tale discussa pronuncia, si rimanda, *ex multis*, a G. TIBERI, *L'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura elettronica dei passeggeri aerei al vaglio della Corte di giustizia*, in *Quaderni costituzionali*, 2006, p. 824 ss.; E. PEDILARCO, *Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione europea-Stati Uniti sul trasferimento dei dati dei passeggeri aerei*, in *Diritto Pubblico comparato ed europeo*, 2006, p. 1225 ss.; M. MENDEZ, *Passenger Name Record Agreement*, in *European Constitutional Law Review*, 3, 2007, p. 127 ss. ma anche F. ROSSI DAL POZZO, *Servizi di trasporto aereo e diritti dei singoli nella disciplina comunitaria*, Giuffrè, Milano, 2008 e E. LEHNER, *Democrazia e tutela dei dati personali nell'UE: l'evoluzione nella negoziazione sul PNR dopo il Trattato di Lisbona*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli Editore, Santarcangelo di Romagna, 2013, p. 941 ss.). A seguito di tale pronuncia, un secondo accordo tra USA e UE è stato approvato il 16 ottobre 2006 (Decisione del Consiglio 2006/729/PESC/GAI, c.d. *interim agreement*, dalla natura temporanea), sostituito da un ulteriore accordo il 23 luglio 2007 a seguito di nuovi negoziati (decisione del Consiglio 2007/551/PESC/GAI). Nel 2011, sulla base di nuove trattative richieste in particolare dal Parlamento europeo, si è giunti alla versione, ancora in vigore, approvata nell'aprile 2012. Per interessanti approfondimenti sulla evoluzione delle tutele inserite nei diversi accordi, si rimanda a M. BOTTA, M. VIOLA DE AZEVEDO CUNHA, *La protezione dei dati personali nelle relazioni tra UE e USA, le negoziazioni sul trasferimento dei PNR*, in *Il Diritto dell'Informazione e dell'Informatica*, 2, 2010, p. 315 ss. e M. SPATTI, *Il trasferimento dei dati relativi ai PNR: gli accordi UE con Australia e USA*, in *Diritto del commercio internazionale*, 3, 2013, p. 683 ss.

[67] L'ultimo accordo è stato adottato con Decisione del Consiglio 2012/380/UE, 22 settembre 2011.

[68] La previa Decisione della Commissione 2006/253/CE basata sull'Accordo UE-Canada in materia di trasferimento di PNR era infatti scaduta il 22 settembre 2009.

[69] Si ricorda infatti che ai sensi dell'art. 218 TFUE talune tipologie (indicate al co. 6) di accordi internazionali – che non devono dunque essere confusi con le Decisioni di esecuzioni di cui si è parlato nei previ paragrafi – necessitano della previa approvazione del Parlamento europeo.

era estremamente elevato a causa delle significative rivelazioni di Snowden nonché della importante prima pronuncia della CGUE in materia di *data retention*, reputava opportuno rivolgersi ai giudici di Lussemburgo chiedendo il loro previo intervento al fine di verificare la compatibilità rispetto all'*acquis communautaire* – comprensivo della Carta di Nizza – della bozza di nuovo accordo UE-Canada. L'art. 218 co. 11 TFUE, infatti, attribuisce al Parlamento europeo, al Consiglio, alla Commissione e a ciascuno Stato membro la possibilità di ottenere un parere di carattere preventivo da parte della CGUE circa la compatibilità di un accordo internazionale con i Trattati [70]; questa facoltà, assolutamente utile e dai positivi risvolti [71], prevede tuttavia una conseguenza tutt'altro che trascurabile in caso di parere negativo: quest'ultimo infatti ha l'effetto di impedire l'entrata in vigore dell'accordo così come stabilito, imponendo o l'appro-

[70] Non sono mancati autori che hanno letto nell'attivazione di tale strumento di controllo preventivo da parte del Parlamento la volontà di "scaricare" sulla Corte il peso di una decisione di estrema delicatezza in un frangente storico-politico e giudiziario fortemente articolato. Si legga sul punto A. VEDASCHI, *Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement*, in *International Data Privacy Law*, 2, 2018, p. 124 ss. e della stessa autrice anche A. VEDASCHI, G.M. NOBERASCO, *From DRD to PRN: looking for a new balance between privacy and security*, cit., nel quale viene comunque affermato che: «While seemingly giving up its 'responibility to decide' to a judicial body, in fact the EP made a reasonable choice», p. 87. Mentre per Tracol la richiesta avanzata dal Parlamento era da considerarsi tardiva, intervenendo in un momento in cui l'accordo già era stato siglato dal Consiglio dell'UE e dal Canada e facendo così sorgere dubbi in capo agli interlocutori internazionali quanto alla stabilità e opportunità delle lunghe e complesse negoziazioni con l'UE, minando peraltro credibilità e affidabilità delle Istituzioni di quest'ultima (X. TRACOL, in *Opinion 1/15 of the Grand Chamber date 26 July 2017*, cit., p. 840), Mendez ha espresso grande apprezzamento per la decisione del Parlamento di azionare il meccanismo del previo parere, ritenendo che «we should be grateful for the presence of the opinion procedure which not only allows for review to take place, but allows it to take place in an arguably less charged political setting than would be the case if we were to allow exclusively ex post review», in M. MENDEZ, *Opinion 1/15: the Court of Justice meets PNR data (again!),* in *European Papers*, 3, 2017, p. 812.

[71] Come già rilevato dalla CGUE nel *Parere 1/09* del 8 marzo 2011, non vi è dubbio che tale procedimento *ex ante* «mira a prevenire le complicazioni che deriverebbero da controversie giudiziarie riguardanti la compatibilità con i Trattati di accordi internazionali che impegnino l'Unione», para. 47-48.

vazione di modifiche al testo posto al vaglio dei giudici o la revisione dei Trattati.

La Corte, incaricata di sciogliere tale nodo, ha dunque svolto una analisi estremamente precisa della bozza di accordo, vagliando la proporzionalità e necessità di ogni singola misura inserita nel testo della bozza, a partire dalla base giuridica. Questa viene correttamente rinvenuta nell'art. 87, co. 2 TFUE in materia di cooperazione di polizia e giudiziaria, nonché nell'art. 16 TFUE sulla garanzia del diritto alla protezione dei dati personali [72]: già da queste affermazioni viene rilevata la natura peculiare dell'accordo che persegue due obiettivi, entrambi essenziali e dunque parimenti rilevanti al fine di valutare la proporzionalità e necessità delle misure disposte [73]. Dopo aver rapidamente valutato l'idoneità del sistema di trasferimento, trattamento e conservazione dei PNR al fine del raggiungimento dello scopo securitario [74], nonché avendo appurato che simili in-

[72] Viene invece escluso quale base giuridica l'art. 82, co. 2, lett. d) TFUE poiché l'accordo non prevede in alcun modo una facilitazione della cooperazione tra autorità giudiziarie in relazione all'azione penale e all'esecuzione delle decisioni.

[73] Come rilevato dall'Avvocato generale Mengozzi nelle sue Conclusioni dell'8 settembre 2016, nessuno dei due scopi perseguiti può essere considerato prevalente sull'altro (sul punto si legga ampiamente F. COUDERT, *The legitimacy of bulk transfers of PNR data to law enforcement authorities under the strict scrutiny of AG Mengozzi*, in *European Data Protection Law Review*, 4, 2016, p. 596 ss.). Questo importante chiarimento, dal valore tutt'altro che meramente formale, segna una significativa distanza rispetto alla rigida distinzione tra finalità di regolamentazione delle attività di soggetti privati da un lato e garanzia della sicurezza dall'altro promossa nella previa decisione della CGUE *Parlamento europeo c. Consiglio e Commissione*, sopra richiamata; «the ruling in Opinion 1/15 thus marks a complete departure from the limited EC-US PNR ruling in 2006. It illustrates the impact of the Lisbon Treaty, its consolidation of the former First and Third Pillars of the Maastricht Treaty, and the strength that the new Treaty provides to the Court», C. DOCKSEY, *Opinion 1/15: privacy and security, finding the balance*, in *Maastricht Journal of European and Comparative Law*, 6, 2017, p. 771.

[74] Questa valutazione è stata svolta in maniera molto concisa nei para. 152-153, nei quali viene fatto rimando ai dati forniti dalle autorità canadesi nel corso del processo, con un approccio che è stato da taluni giudicato discutibile e sotto alcuni profili persino deficitario. Il GEPD, ad esempio, nella propria *Opinion on the Proposal for Council decisions on the conclusion and signature of the Agreement between Canada and the EU on the transfer and processing of PNR data*, del 30 settembre 2013, aveva espresso perplessità sia quanto alla reale utilità del meccanismo di trasferimento generalizzato di PNR, sia

gerenze nella sfera privata non sono tali da pregiudicare il nucleo essenziale dei diritti tutelati agli artt. 7 e 8 della Carta di Nizza [75], i giudici di

quanto alla sua concreta idoneità a contribuire alla sicurezza pubblica. Del resto anche il Parlamento europeo, richiedendo l'intervento della Corte, aveva sottolineato come Consiglio e Commissione non avessero dimostrato, sulla base di elementi obiettivi, la necessità effettiva della conclusione dell'Accordo ai sensi dell'art. 52, co. 1 della Carta di Nizza. Tale aspetto è peraltro emerso anche in occasione della proposta di Direttiva europea in materia di conservazione e trattamento di PNR, di cui si parlerà più avanti: rispetto ad essa non è stato ritenuto «chiaro perché sia stato escluso a priori un approccio più selettivo, che limitasse la portata delle misure di controllo ad alcuni Paesi, ad alcune categorie di voli, ad alcune categorie di passeggeri, o ad un arco temporale definito» (F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella Direttiva PNR?*, in *Diritti Umani e Diritto Internazionale*, 1, 2017, p. 224), riproponendo così quelle restrizioni emerse dalla giurisprudenza della CGUE in materia di *data retention*. Lo stesso Di Matteo peraltro sottolineava come l'adozione di sistemi di trasferimento massivo dei PNR avesse incontrato forti avversioni in chi vedeva in tali strumenti un vero e proprio passo in avanti verso la sorveglianza globale (E. BROUWER, *Ignoring Dissent and Legality. The EU's Proposal to Share the Personal Information of All Passengers*, in *CEPS Paper in Liberty and Security in Europe* 2011, p. 1 ss.), mentre posizioni più moderate erano state promosse da chi proponeva soluzioni di compromesso in grado di assicurare al tempo stesso la tutela dei diritti fondamentali e la sicurezza delle persone (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Twelve Operational Fundamental Rights Considerations for Law Enforcement When Processing Passenger Name Record (PNR) Data*, gennaio 2015). Anche Tracol, pur riconoscendo che alla CGUE non è attribuito il potere e la funzione di spingersi a considerazioni o valutazioni circa l'opportunità delle misure legislative o degli accordi internazionali adottati, essendo questa funzione unica prerogativa del legislatore europeo, ha nondimeno ritenuto eccessivamente sbrigativo e poco motivato il vaglio svolto dai giudici quanto all'idoneità delle disposizioni rispetto al raggiungimento del fine stabilito, come previsto dall'art. 52 della Carta di Nizza (X. TRACOL, *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the Eu and Canada,* cit., p. 836).

[75] Sul punto la CGUE ha affermato come «anche se i dati PNR possono, eventualmente, rivelare informazioni molto precise sulla vita privata di una persona, la natura di dette informazioni è limitata ad alcuni aspetti di tale vita privata, relativi in particolare ai viaggi aerei tra il Canada e l'Unione. Quanto al contenuto essenziale del diritto alla protezione dei dati di carattere personale, sancito all'articolo 8 della Carta, l'accordo previsto circoscrive, al suo articolo 3, le finalità del trattamento dei dati PNR e stabilisce, al suo articolo 9, norme destinate a garantire, in particolare, la sicurezza, la riservatezza e l'integrità di tali dati, nonché a tutelare dagli accessi e dai trattamenti illegali»,

Lussemburgo hanno svolto poi un accurato test di proporzionalità inteso *stricto sensu*, dal quale sono emersi profili problematici, individuati ad esempio nella definizione di PNR, considerata non sufficientemente chiara e precisa[76], o ancora nella possibilità di trasferimento e trattamento di dati "sensibili"[77]. Accanto a queste criticità, l'aspetto sicuramente più delicato emerso dalla dettagliata e lunga analisi della CGUE[78] è però quello attinente al vaglio di proporzionalità del regime di conservazione dei PNR trasferiti alle autorità canadesi: rilevando come la bozza di accordo non proponga alcuna differenziazione a seconda dei diversi momenti del viaggio – prima della partenza, durante la permanenza in Canada e successivamente all'uscita dal territorio canadese –, i giudici affermano come, a seconda della distinzione temporale, la necessità di con-

---

para. 150. Questo profilo risulta di grande interesse poiché mette in luce la differenza di un trattamento avente ad oggetto PNR rispetto a quello attinente invece al contenuto di dati derivanti da servizi di telecomunicazione, come rilevato nella sentenza *Schrems*.

[76] In particolare l'utilizzo di termini quali "etc." è stato criticato dalla Corte in quanto «non determina a sufficienza la portata dei dati da trasferire» (para. 157); questo nonostante la definizione riportata nell'accordo corrispondesse a quanto contenuto nell'Allegato 1 delle Linee Guida ICAO.

[77] L'art. 8 della bozza di accordo includeva nella definizione di PNR anche i dati "sensibili" – o, impiegando la terminologia oggi prevista nel GDPR, "categorie particolari di dati" –. La CGUE ha affermato con chiarezza come gli artt. 7, 8, 21 e 52 della Carta di Nizza precludano la possibilità di adottare disposizioni concernenti il trasferimento di detta categoria di dati, richiamando peraltro l'esempio positivo della Direttiva UE 2016/681 in materia di PNR – su cui si rifletterà in seguito –, che esclude e proibisce *tout court* il trasferimento, conservazione e accesso a dati idonei a rivelare informazioni sulla salute, origine razziale o etnica, orientamento e vita sessuale, opinioni politiche, convinzioni religioso o filosofiche o appartenenza sindacale.

[78] Si vuole solo marginalmente rilevare come ulteriori criticità siano emerse con riferimento all'analisi automatizzata dei dati PNR svolta prima che il passeggero cui il dato afferisce arrivi sul suolo canadese: su tale delicata forma di accesso ai dati non è stato infatti imposto né l'utilizzo di modelli e criteri prestabiliti specifici ed affidabili, privi di qualsiasi carattere discriminatorio, né il riesame umano nel caso in cui l'analisi automatizzata rilevi la presenza di sospetti o criticità particolari rispetto ad uno specifico passeggero. Anche l'individuazione delle autorità competenti a ricevere i dati inviati dai vettori aerei è stata ritenuta parzialmente vaga e non sufficientemente chiara poiché vengono indicate genericamente, quali possibili destinatari dei dati, una molteplicità di autorità governative canadesi o addirittura autorità situate in Stati terzi.

servare i PNR e dunque la proporzionalità dell'ingerenza nei diritti fondamentali debbano essere diversamente valutate. Ecco quindi che, partendo dalla fase antecedente all'arrivo dei passeggeri in Canada, la CGUE riconosce la legittimità del meccanismo di invio sistematico e generalizzato dei PNR mediante un ragionamento di grande rilevanza: nonostante il trasferimento e la prima analisi automatizzata dei dati avvengano «indipendentemente da qualsiasi elemento obiettivo che consenta di ritenere che i passeggeri possano rappresentare un rischio per la sicurezza pubblica in Canada» (para. 186), il criterio di stretta necessità risulta rispettato poiché «la conservazione e l'uso a tal fine non possono, per loro stessa natura, essere limitati a una cerchia determinata di passeggeri aerei né essere oggetto di una previa autorizzazione di un giudice o di un ente amministrativo indipendente», para. 197. Anche durante il soggiorno i dati PNR possono essere conservati in maniera generalizzata purché le successive ed eventuali operazioni di accesso vengano svolte solo in presenza di condizioni sostanziali e procedurali basate su criteri oggettivi. In questo modo, la CGUE ammette, nella fase precedente all'arrivo e durante il soggiorno, l'impiego di una forma di raccolta e conservazione sistematica, slegata da quei caratteri di oggettività che richiederebbero invece una conservazione targettizzata a taluni soggetti appartenenti a determinati gruppi sociali o provenienti da specifiche aree geografiche.

Questa posizione solleva immediatamente evidenti dubbi di compatibilità con quanto affermato nelle sentenze in materia di *data retention*, nelle quali la Corte ha espressamente ritenuto non conformi alla Carta di Nizza forme generalizzate ed indiscriminate di conservazione dei metadati provenienti dalla totalità degli utenti di servizi di telecomunicazione e riguardanti i metadati di tutti i mezzi di telecomunicazione[79], se non a specifiche e determinate condizioni laddove a dover essere tutelata sia la

[79] Del resto il GEPD nella sua *Opinion 5/2015*, seppur vertente sulla proposta di Direttiva europea in materia di PNR, ha ribadito con forza come «the non-targeted and bulk collection and processing of the PNR scheme amount to a measure of general surveillance» (para. 63), suggerendo come l'unico utilizzo dei PNR conforme ai principi di proporzionalità debba ravvisarsi in un impiego «on a case-by-case basis but only in case of a serious and concrete threat established by more specific indicators», para. 64.

sicurezza nazionale. Ebbene su questo problematico profilo e cogliendo la delicatezza di queste considerazioni, l'Avvocato generale Mengozzi nelle sue Conclusioni ha espressamente delineato una distinzione tra il sistema PNR e quello oggetto dei precedenti giudizi: l'utilizzo dei codici di prenotazione dei voli e le informazioni in esse contenute, pur rappresentando certamente una invasione della sfera personale del passeggero, rappresenta una ingerenza minore e più ristretta rispetto alla forma di *bulk data retention* prevista dalla Direttiva 2006/24 e dai sistemi adottati sulla base dell'art. 15 Direttiva *e-Privacy*[80]. Pur ammettendo che la «natura indifferenziata e generalizzata [del sistema di raccolta e conservazione PNR] suscita interrogativi» (para. 240), l'Avvocato rileva come «l'interesse stesso dei regimi PNR è di garantire la trasmissione massiccia di dati che consenta alle autorità competenti di identificare, mediante strumenti di trattamento automatizzato e di scenari o di criteri prestabiliti, individui fino a quel momento sconosciuti ai servizi di polizia», para. 241; inoltre, «contrariamente alle persone i cui dati formavano oggetto del trattamento di cui alla Direttiva 2006/24, tutte quelle cui si riferisce l'accordo in materia di PNR prendono volontariamente un volo internazionale diretto o proveniente da un Paese terzo», impiegando peraltro un mezzo di trasporto che è stato, purtroppo in modo ricorrente, impiegato per perpetrare atti di terrorismo o reati gravi di natura transnazionale, così da richiedere la garanzia di un livello di sicurezza elevato (para. 242).

Insomma sulla base di queste valutazioni, l'Avvocato generale, seguito poi dalla Corte stessa, ha precisato le molteplici differenze sussistenti tra il sistema di trasferimento massivo di dati PNR e quello invece oggetto della *data retention saga*, così che nessuna difformità o incoerenza è da ravvisarsi rispetto al filone giurisprudenziale precedente.

La continuità con quanto previamente statuito dalla CGUE è chiaramente individuabile poi nella posizione espressa dai giudici con riferimento alla disciplina della conservazione dei dati dei passeggeri dopo che

---

[80] Sul punto si legga l'analisi di L. WOODS, *Trasnferring personal data outside the EU: clarification from the ECJ?*, in *EU Law Analysis*, 4 agosto 2017; P. VOGIATZOGLOU, *Mass surveillance, predictive policing and the implementation of the CJEU and the ECtHR requirment of objectivity*, in *European Journal of Law and Technology*, 1, 2019, p. 1 ss.

questi ultimi abbiano lasciato il Canada: «i passeggeri aerei che hanno lasciato il Canada sono stati, di norma, oggetto di controlli all'entrata e all'uscita da tale Paese. Parimenti, i loro dati PNR sono stati verificati prima del loro arrivo in Canada e, eventualmente, durante il loro soggiorno nonché all'uscita da tale Paese terzo. In dette circostanze, si deve ritenere che tali passeggeri non presentino, in linea di principio, un rischio in materia di terrorismo o di reati gravi di natura transnazionale» (para. 204), così che si rende necessaria la presenza di elementi obiettivi che determinino l'esigenza di trattenere il dato e che siano idonei a comprovare la sussistenza di un rischio nei confronti di uno specifico soggetto. La mancata previsione di tali elementi oggettivi in grado di legare l'obiettivo di lotta al terrorismo e crimini gravi al soggetto "in uscita" rende dunque ingiustificata e sproporzionata una archiviazione continua e prolungata dei PNR.

Esaminando infine la disciplina dell'accesso da parte delle autorità di *law enforcement* ai dati dei passeggeri aviotrasportati durante il loro soggiorno, viene rilevata la necessità di istituire un legame tra l'accesso al dato e una determinata indagine: debbono pertanto sussistere comprovate esigenze, subentrate in un momento successivo all'ingresso nel Paese del passeggero, in grado di giustificare l'ulteriore ingerenza nella sfera privata. In questo caso, la Corte ha pertanto ribadito e riconfermato i criteri già individuati nelle sue previe pronunce, in particolare nella *Tele2*, prevedendo inoltre la necessaria presenza sia di un controllo preventivo effettuato da un giudice o da un soggetto amministrativo che gode del carattere di indipendenza, sia del diritto d'informazione, di accesso e rettifica per il passeggero.

La carenza di tali tutele nella bozza di accordo esaminata, insieme alle ulteriori criticità prima rilevate, ne rendono il testo incompatibile con il diritto dell'UE ed in particolare con gli artt. 7, 8, 21 e 52 comma 1 della Carta di Nizza, costituendo ingerenze sproporzionate e non limitate a quanto strettamente necessario nei diritti fondamentali alla riservatezza e alla protezione dei dati.

7. *Una ricognizione delle più significative implicazioni del* Parere 1/15 *fuori e dentro i confini dell'UE.*

7.1. *La necessaria rinegoziazione dell'accordo con il Canada e i dubbi quanto alla conformità alla Carta di Nizza degli accordi in materia di PNR vigenti.*

Da quanto emerso dall'analisi svolta, nel *Parere 1/15* i giudici di Lussemburgo non si sono limitati a negare la conformità della bozza di Accordo UE-Canada rispetto ai diritti tutelati dalla Carta di Nizza: similmente a quanto avvenuto anche nelle sentenze *DRI* e *Tele2* – quest'ultima intercorsa nelle more del giudizio in esame –, la CGUE ha indicato una serie molto precisa e dettagliata di condizioni e requisiti necessari al fine di garantire la compatibilità con il diritto dell'UE di accordi in materia di trasferimento di PNR [81]. Tale articolato elenco di criteri, pur essendo certamente utile per le Istituzioni europee impegnate nelle operazioni di negoziazione con Stati terzi, ha nondimeno fatto sorgere alcune serie perplessità quanto alla sua reale e concreta attuazione nel contesto delle relazioni internazionali e dunque quanto alla possibilità che uno Stato terzo possa approvare ed accettare di vincolarsi al rispetto di condizioni di trasferimento e tutela dei dati così stringenti [82]. È proprio da tali prime

---

[81] Si vuole infatti sin da ora far notare come alcuni autori abbiano parlato di un approccio para-legislativo del giudice di Lussemburgo «che esalta la dimensione costruttiva dell'attività del giudice, laddove non si limita ad invalidare (o censurare) le norme che è chiamato a vagliare, ma nell'intento di concretizzare principi espressi dalla pregressa giurisprudenza tenda a riscriverne di nuove, anche con il piglio tipico del comitato di tecnica legislativa», A. VEDASCHI, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione Europea*, in *Giurisprudenza Costituzionale*, 4, 2017, p. 1925; sul punto anche H. HIJMANS, *PNR Agreement EU-Canada scrutinised: CJEU gives very precise guidance to negotiators*, in *European Data Protection Law Review*, 3, 2017, p. 406 ss.

[82] Come ben sottolineato da Vedaschi, la CGUE, pur ammettendo in linea generale la legittimità del sistema di scambio di PNR, ha stabilito condizioni talmente stringenti da rendere, nella pratica, quasi impossibile delineare un accordo in grado di rispettarle e racchiuderle tutte, così che «la legittimità di tale operazione resta meramente teorica, poiché il legislatore, a giudizio della Corte, non ha ancora trovato, sul piano pratico, una realizzazione compatibile con la Carta dei diritti», A. VEDASCHI, *L'accordo interna-*

incertezze attuative che derivano alcune importanti riflessioni sull'impatto della pronuncia esaminata non solo sul fronte esterno, quello cioè delle conseguenze per le negoziazioni in corso o per gli accordi già conclusi, bensì anche sul fronte interno, con riferimento alle ripercussioni prodotte sulla Direttiva 2016/681 in materia di PNR.

Iniziando dunque ad analizzare il primo profilo, è utile sottolineare come a seguito dell'autorizzazione del Consiglio, ricevuta dalla Commissione nel dicembre 2017, i nuovi negoziati con il Canada hanno preso avvio nel giugno 2018 e si sono poi conclusi, in tempi relativamente brevi, nel luglio 2019: la rinnovata bozza di accordo al momento risulta ancora in fase di riesame giuridico e approvazione politica da parte del Canada. Nel frattempo, però, in attesa del raggiungimento di una aggiornata e modificata regolamentazione delle operazioni di trasferimento e trattamento dei PNR in grado di rispettare i requisiti fissati dalla CGUE, è bene precisare come i vettori aerei stiano ancora continuando a trasferire i dati dei propri passeggeri europei alle autorità canadesi: in particolare, il trattamento dei dati risulta ad ora essere disciplinato da un *Committment* elaborato della *Border Service Agency* canadese che altro non è se non un allegato alla superata Decisione della Commissione 2006/253/EC. Tale documento, ormai datato, presenta un livello di garanzia del diritto alla protezione dei dati e alla riservatezza di gran lunga inferiore a quanto previsto nella bozza di accordo bloccata dall'intervento della CGUE [83]: questa situazione, per quanto temporanea, deve pertanto da un lato far riflettere sulle difficoltà che il rispetto di standard elevati di tutela dei dati pone, rendendo i negoziati ancor più lunghi, complessi e dagli incerti risvolti, ben potendo incontrare la resistenza dello Stato terzo che potrebbe essere riluttante ad approvare accordi dalle condizioni restrittive e stringenti [84]; dall'altro lato, il vuoto regolatorio e la fase prolungata di stallo

---

zionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di Giustizia dell'Unione Europea, cit., p. 1927.

[83] Per una analisi delle tutele predisposte dal *Committment* attualmente utilizzato per il trasferimento dei dati PNR verso il Canada, si legga X. TRACOL, *Opinion 1/15 of the Grand Chamber*, cit., p. 841.

[84] L'accettazione degli standard di tutela europei e la loro garanzia all'interno dell'ordinamento nazionale possono infatti comportare la necessità di modifiche com-

venutasi a creare a seguito del *Parere 1/15*, continuando comunque ad esporre i dati dei passeggeri europei a rischi in termini di ridotte garanzie e tutele, inducono a chiedersi se un accordo pur imperfetto e perfezionabile non sia in realtà più apprezzabile e maggiormente garantista rispetto all'assenza totale di accordi. Su questi profili problematici di tutt'altro che semplice risoluzione le Istituzioni dell'UE dovranno necessariamente confrontarsi al fine di giungere all'approvazione di soluzioni condivise e coerenti che, come detto anche con riferimento alle decisioni di adeguatezza attinenti al flusso di dati UE-USA, siano in grado sia di superare l'eventuale vaglio, preventivo o successivo della CGUE, sia di essere accettate dallo Stato terzo. Simili considerazioni risultano di fondamentale rilievo anche per il futuro dei negoziati al momento in corso con Messico e Giappone [85].

Oltre che per gli accordi non ancora conclusi, una seria valutazione dell'impatto e delle conseguenze dei requisiti e criteri fissati dai giudici di Lussemburgo in materia di trasferimento di PNR deve riguardare anche gli accordi attualmente in vigore, quali quello con gli USA e quello con l'Australia, sopra richiamati: ciò che viene posto in discussione è la capacità di tali accordi di superare il medesimo vaglio di proporzionalità utilizzato dai giudici di Lussemburgo nel *Parere 1/15*. Non può infatti essere ignorata la somiglianza di molte delle disposizioni contenute negli accordi di PNR vigenti a quelle inserite nella bozza esaminata dalla CGUE, sotto il profilo ad esempio della definizione di PNR impiegata, della possibilità di trattamento dei dati sensibili [86] o della mancata distinzione delle tutele

---

plesse e di non poco rilievo nell'assetto normativo vigente nello Stato terzo ricevente i PNR.

[85] Mentre il 18 febbraio 2020 la Commissione è stata autorizzata dal Consiglio ad avviare negoziati con il Giappone finalizzati alla conclusione di un accordo in materia di trasferimento di dati PNR, le trattative con il Messico, iniziate nel 2015, sono ora in una fase di stallo.

[86] L'art. 8 della bozza di accordo con il Canada e l'art. 6 dell'accordo vigente con gli USA sono molto simili tra loro, prevedendo entrambi la possibilità di trasferimento di dati sensibili, pur con l'adozione di specifiche tutele. Dinnanzi al chiaro e netto divieto, emerso dal vaglio di proporzionalità promosso dalla CGUE nel *Parere 1/15*, di trasferimento e trattamento di dati sensibili, pare dunque innegabile come tali accordi non rispettino i criteri stabiliti dalla giurisprudenza della Corte, prevedendo misure simili, se

e limitazioni poste alla raccolta, conservazione e accesso ai codici di prenotazione a seconda delle diverse scansioni temporali – prima, durante o dopo il soggiorno del passeggero – secondo quanto indicato nel Parere [87].

La possibilità di rilevare dunque anche negli accordi con gli USA e l'Australia le medesime criticità evidenziate dai giudici di Lussemburgo nella bozza con il Canada [88], ben potrebbe, con alte probabilità, condurre ad una dichiarazione di invalidità di tali vigenti accordi e della connessa decisione di adeguatezza da parte della CGUE, il cui vaglio potrebbe essere attivato da un rinvio pregiudiziale promosso dalle Corti nazionali [89].

---

non persino più problematiche di quelle inserite nella cassata bozza di accordo con il Canada.

[87] L'accordo con gli USA, ad esempio, pare stabilire sotto taluni profili regole meno rigide e meno garantiste dei diritti alla privacy e protezione dei dati rispetto alla bozza di accordo con il Canada, facendo dunque dubitare della possibilità di ritenere tali misure conformi alla Carta di Nizza e al principio di proporzionalità; basti pensare al fatto che i PNR trasferiti negli USA non vengono mai distrutti: per quanto venga previsto l'obbligo di anonimizzazione dei dati, in modo da impedire qualsiasi possibilità di ripersonalizzarli, è chiaro che una conservazione illimitata dei dati, anche dopo che il passeggero abbia lasciato il territorio statunitense, rappresenta una invasione nei diritti fondamentali difficilmente considerabile come limitata allo stretto necessario. Il medesimo ragionamento può essere esteso anche alle disposizioni che nell'accordo vigente con gli USA regolano la possibilità, da parte delle autorità statunitensi, di trasferire i PNR ad ulteriori Stati terzi: anche in questo caso infatti le previsioni della bozza di accordo con il Canada, ritenute eccedenti i limiti di quanto strettamente necessario, risultano maggiormente tutelanti. Per approfondimenti su questi profili critici e per un raffronto tra le disposizioni contenute negli accordi UE-USA e nella bozza UE-Canada, sia concesso di rimandare a G. FORMICI, *The external dimension of the European rule of law in the digital age: an analysis through the lens of the ECJ case-law on data transfer*, in *Cahiers Jean Monnet n. 6/2020, Actes des ateliers doctoraux 2019 "L'État de droit" de l'Université degli Studi di Milano et de la European School of Law Toulouse, Centre d'excellence Europe Capitole*, Lextenso, Toulouse, 2020, p. 215 ss.

[88] Di tale opinione X. TRACOL, *Opinion 1/15 of the Grand Chamber date 26 July 2017*, cit., ma anche Mendez che afferma con chiarezza come «there is no difficulty in establishing that the two existing PNR agreements do not meet the privacy and data protection standards outlined in Opinion 1/15», M. MENZED, *Opinion 1/15: the Court of Justice meets PNR data (again!)*, cit., p. 816.

[89] La possibilità di portare all'attenzione della CGUE, mediante rinvio pregiudiziale, la validità di un accordo internazionale, anche dopo il decorso dei termini di annulla-

Anche sotto tale profilo, estremamente problematico e fonte di preoccupazione quanto alla stabilità degli accordi esistenti, si dovranno quindi osservare con grande attenzione i possibili sviluppi futuri, sia da parte delle Istituzioni europee, che potrebbero valutare l'opportunità di rinegoziare nuovi accordi con USA e Australia [90], sia da parte dei giudici di Lussemburgo, che potrebbero essere chiamati ad intervenire ancora una volta in materia di trasferimento di PNR.

7.2. *La Direttiva 2016/681 e un destino incerto: i rinvii pregiudiziali pendenti.*

Il *Parere 1/15* infine non ha mancato di provocare reazioni anche sul fronte interno ai confini dell'UE, inducendo in particolare a riflettere sulla compatibilità con la Carta di Nizza della Direttiva 2016/681 del 27 aprile 2016 *sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi*. Se alcune disposizioni di tale normativa sono state infatti addirittura elogiate dai giudici di Lussemburgo, che ne hanno citato il contenuto quale esempio positivo e modello cui ispirarsi [91], altre

---

mento, è stata chiaramente statuita dai giudici di Lussemburgo nella pronuncia del 27 febbraio 2018, C-266/16, *The Queen, Western Sahara Campaign Uk c. Commissioners for Her Majesty's Revenue and Customs and Secretary of State for Environment, Food and Rural Affairs*.

[90] È quanto peraltro sembra potersi dedurre dal Report elaborato della Commissione (COMMISSIONE EUROPEA, *Report on the joint evaluation of the Agreement between the USA and the EU on the use and transfer of PNR to the US Department of Homeland Security*, COM(2021)18 final, del 12 gennaio 2021) nel quale viene riconosciuto come «despite the numerous safeguards contained therein, several aspects of the Agreement are not fully in line with Opinion 1/15 of the Court of Justice on the envisaged PNR Agreement with Canada (…).crime for cross-checking of PNR data». La Commissione dunque prosegue impegnandosi ad «assess the necessary follow-up action also taking into account the feedback received by the European Parliament and Council on this Evaluation», nonché a provvedere ad una «review of the EU external strategy towards PNR transfers to third countries next year», p. 4.

[91] Si richiama in questo senso il riferimento svolto dalla Corte alla corretta disciplina in materia di dati "sensibili" contenuta nella Direttiva stessa (para. 166).

invece non hanno mancato di destare perplessità e dubbi proprio alla luce dei principi e requisiti stabiliti dalla giurisprudenza sovranazionale.

In estrema sintesi e per quanto qui rileva [92], la Direttiva avente ad oggetto la disciplina del trasferimento ad opera di vettori aerei di dati PNR relativi a passeggeri di voli internazionali da e per l'UE [93] è stata adottata nel 2016 ma ha previsto un termine di tempo più ampio, scaduto il 25 maggio 2018, per l'attuazione a livello nazionale. Essa impone agli Stati membri di istituire delle *Passenger Information Unit* (PIU) incaricate della conservazione e trattamento dei PNR, del loro trasferimento alle competenti autorità nazionali di *law enforcement* nonché dello scambio di informazioni con altri Stati membri e con Europol, mentre significativi poteri di controllo sono attribuiti alle Autorità nazionali garanti della protezione dei dati. I dati raccolti dalle PIU vengono conservati per un periodo di 5 anni, al termine del quale ne viene imposta la cancellazione, stabilendo però una prima procedura di anonimizzazione da effettuarsi dopo sei mesi dalla raccolta. Emerge dunque come, anche nella normativa dell'UE, non siano previste differenziazioni nella disciplina della conservazione ed accesso ai dati sulla base della scansione temporale – prima, durante o dopo l'arrivo dei passeggeri nel territorio europeo –: proprio questa mancanza rappresenta uno dei profili maggiormente problematici della Direttiva. Nonostante infatti siano riscontrabili molti punti rispetto ai quali il legislatore europeo ha dimostrato di tenere in considerazione i rilievi emersi dalla giurisprudenza della CGUE – che al momento dell'adozione della Direttiva erano rappresentati dalla sentenza *DRI* e dal ca-

---

[92] Per un'analisi approfondita della normativa, si rimanda a E. SAULNIER-CASSIA, *La Directive (UE) 2016/681: miscellanies sur l'utilisation des données des dossier passagers dans l'Union Européenne*, in C. CHEVALLIER GOVERS (a cura di), *L'èchange des données dans l'Espace de liberté, de sécurité et de Justice de l'Union Européenne*, Mare & Martin, 2017, p. 21 ss.; nonché a F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella Direttiva PNR?*, cit., che mette in evidenza il lungo e dibattuto iter normativo che, risalente al 2007, ha ricevuto una forte spinta propulsiva a seguito della nuova ondata di attentati terroristici registratasi nel 2015.

[93] Restano quindi esclusi dalla disciplina in esame i voli meramente infra-UE, che possono però essere sottoposti agli obblighi e alla regolamentazione enucleata nella normativa europea sulla base di una decisione, eventuale e discrezionale, adottata da ciascuno Stato membro nella propria normativa interna di recepimento.

so *Schrems* –, ad esempio vietando la raccolta e l'utilizzo di dati "sensibili", o predisponendo una anonimizzazione e una successiva cancellazione dei dati (art. 9) o ancora imponendo un intervento umano dinnanzi ai risultati di analisi automatizzate (art. 12), non possono essere ignorate anche talune carenze sotto il profilo della base giuridica [94], nonché della proporzionalità e stretta necessità della conservazione dei PNR, che fanno dubitare della legittimità della Direttiva e della sua capacità di resistere indenne al vaglio della CGUE [95].

Alla luce di queste considerazioni, alcune ONG nonché taluni cittadini europei, si sono attivati dinnanzi alle Corti statali per contestare la legittimità della normativa nazionale adottata in attuazione della Direttiva in materia di PNR, con l'obiettivo ultimo di ottenere dai giudici interni un rinvio pregiudiziale alla CGUE in grado di condurre ad una valutazione della compatibilità della Direttiva PNR rispetto al diritto dell'UE e alla Carta di Nizza. Queste azioni si sono ben presto rivelate effi-

---

[94] Questa è stata individuata negli artt. 82 e 87 TFEU: i dubbi quindi sorgono con riferimento alla correttezza dell'art. 82 che nel *Parere 1/15* è stato invece ritenuto una erronea base giuridica dell'accordo UE-Canada.

[95] Di tale opinione, tra i molti, E. CARPANELLI, N. LAZZERINI, *PNR: problems not resolved? The EU PNR conundrum, after Opinion 1/15 of the CJEU*, in *Air and Space Law*, 42, 2017, p. 377 ss.; C. GRAZIANI, *PNR EU-Canada, la Corte di giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali,* in *DPCE Online*, 4, 2017, p. 959 ss., ma anche M. ZALNIERIUTE, *Developing a European standard for international data trasnfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *Modern Law Review*, 6, 2018, p. 1046 ss.; X. TRACOL, *Opinion 1/15 of the Grand Chamber dated 26 July 2017 about the agreement on Passenger Name Record data between the EU and Canada,* cit; S. RODA, *Shortcomings of the PNR Directive in light of Opinion 1/15 of the Court of Justice of the European Union*, in *European Data Protection Law Review*, 6, 2020, p. 66 ss. Interessante sul punto è notare come, già prima del *Parere 1/15*, si fosse aperta una accesa discussione circa la legittimità della Direttiva in materia di PNR, letta alla luce delle sentenze *DRI* e *Schrems*: posizioni discordanti si rinvenivano tra chi, come Di Matteo (in *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella Direttiva PNR?*, cit.) rinveniva la mancata conformità della normativa rispetto al diritto dell'UE e chi invece considerava la Direttiva del tutto legittima e le sue disposizioni proporzionate e limitate allo stresso necessario (D. LOWE, *The European Union's passenger name record data Directive 2016/681: is it fit for the purpose?*, in *International Criminal Law Review*, 16, 2016, p. 856 ss.).

caci: sono infatti cinque i rinvii pregiudiziali al momento pendenti dinnanzi alla CGUE ed aventi ad oggetto proprio la Direttiva 2016/681, su rinvio della *Cour constitutionnelle* belga (C-817/19, *Lingue des droits humains c. Conseil des Ministres*, promosso il 31 ottobre 2019) [96], del *Amtsgericht* di Colonia, il 20 gennaio 2020 (C-148/20, *AC c. Deutsche Lufthansa AG*) e il 17 marzo 2020 (C-150/20, *BD c. Deutsche Lufthansa AG*) [97] e del *Verwaltungsgericht* di Wiesbaden, il 19 maggio 2020 (C-215/20, *JV c. Repubblica federale di Germania*) e il 27 maggio 2020 (C-222/20, *OC c. Repubblica federale di Germania*). Questi rinvii, pur con differenti sfumature, presentano elementi comuni: tutti i giudici nazionali infatti hanno messo in evidenza significative problematiche circa la compatibilità rispetto alla Carta di Nizza della disciplina nazionale in materia di trasferimento, raccolta, conservazione e accesso ai PNR e dunque della stessa disciplina dell'UE. Ricostruendo con grande attenzione la giurisprudenza della CGUE, le Corti nazionali hanno rinvenuto numerosi parallelismi tra quanto affermato dai giudici di Lussemburgo con riferimento alla bozza di accordo UE-Canada e quanto contenuto nella Direttiva PNR, ad esempio con riferimento alla definizione di PNR o alla durata della conservazione e alla mancata differenziazione della disciplina di conservazione e accesso a seconda dei diversi momenti – prima, durante e dopo il volo del passeggero –. Inoltre, per quanto attiene al bilanciamento tra esigenze securitarie e tutela della sfera privata, le Corti nazionali hanno richiesto di chiarire un punto di estremo rilievo: se cioè un sistema di raccolta, trasferimento e trattamento generalizzato di PNR,

[96] Il caso è stato promosso mediante ricorso di annullamento presentato dinnanzi alla Corte costituzionale belga dalla ONG Ligue des droits humains avverso la *Loi du 25 décembre 2016, relative au traitement des données des passegers*, adottata in attuazione della Direttiva 2016/681.

[97] La controversia dinnanzi al Tribunale circoscrizionale di Colonia ha avuto origine da una azione inibitoria promossa dal ricorrente AC avverso la compagnia aerea Lufthansa: l'obiettivo del ricorrente era quello di impedire al vettore aereo il trasferimento dei propri dati PNR all'ufficio federale tedesco della polizia, sulla base della ritenuta incompatibilità con il diritto dell'UE e la Carta di Nizza della normativa tedesca in materia di trattamento dei dati dei passeggeri aviotrasportati (*Gesetz uber die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie EU 2016/681* del 10 giugno 2017), adottata in attuazione alla Direttiva PNR.

che riguarda tutti i passeggeri che si servono di un determinato mezzo di trasporto a prescindere da elementi obiettivi che consentano di creare una connessione tra il soggetto cui i dati si riferiscono e un rischio per la sicurezza pubblica, sia da ritenersi compatibile agli artt. 7, 8 e 52 della Carta di Nizza. Con tale quesito i giudici hanno in sostanza domandato se i principi e i requisiti sanciti nella *data retention saga* con riferimento all'impiego di strumenti di conservazione generalizzata di metadati derivanti da telecomunicazioni siano applicabili e trasponibili anche ai regimi di trasferimento e trattamento, del pari generalizzati ed indiscriminati, aventi ad oggetto i PNR; la distinzione, evidenziata dall'Avvocato generale e sopra richiamata, tra sistemi di *bulk data retention* riguardanti i metadati e regimi che pure impongono un trasferimento, conservazione e analisi della totalità dei dati ma che, come nel caso dei PNR, risultano unicamente limitati ai passeggeri aviotrasportati e non alla totalità della popolazione e riguardano dati idonei a rivelare aspetti più limitati della vita privata dei soggetti coinvolti, non ha dunque risolto tutti i dubbi e le perplessità sorte dinnanzi alla legittimazione del sistema di trasferimento generalizzato dei PNR affermata nel *Parere 1/15*. La delicatezza e il rilievo dei quesiti rivolti alla CGUE rendono la risoluzione dei rinvii qui esaminati estremamente attesa e da osservare con grande attenzione: le risposte che i giudici di Lussemburgo forniranno, contribuiranno certamente a definire un quadro più completo e dettagliato dei sistemi di conservazione e trasferimento dati in grado di superare il vaglio di proporzionalità stabilito dalla Carta di Nizza, aiutando a definire le caratteristiche e le restrizioni che consentono di ritenere tali regimi limitati a quanto strettamente necessario.

8. *Uno sguardo critico alla disciplina europea in materia di trasferimento dati verso Stati terzi: debolezze e successi in uno scenario in divenire.*

Volendo ora trarre un conclusivo bilancio sull'efficacia e sul più sostanziale e profondo portato della normativa e della giurisprudenza sin qui analizzate, non si può che rilevare sin da subito come tale operazione sia tutt'altro che semplice e scontata.

La garanzia della continuità del livello di tutela stabilito nell'UE anche

oltre i suoi confini territoriali persegue senza dubbio il virtuoso scopo di scongiurare i rischi derivanti da operazioni di *data transfer* verso quelli che potrebbero essere definiti, parafrasando la terminologia usata in ambito fiscale, "paradisi dei dati", ovvero verso Paesi terzi nei quali la normativa in materia di riservatezza e *data protection* risulta essere più blanda e meno garantista rispetto a quella stabilita nell'UE; se così fosse, infatti, il trasferimento dati si potrebbe pericolosamente inverare non solo in una lesione dei diritti fondamentali riconosciuti dall'UE, ma anche, in ultimo, in una distorsione della concorrenza e della competizione, a scapito di quelle aziende o *data exporters* che attuano rigorose *privacy policies* rispettose di elevati standard di tutela e che per questo sostengono costi ed investimenti considerevoli in termini di gestione, controllo, strumentazione e formazione del personale addetto.

Se questo obiettivo primario è certamente condivisibile e di estremo rilievo, ciò che risulta essere oggetto di grande discussione è la modalità con la quale l'UE sta cercando di garantire il raggiungimento di tale risultato. Da un lato, infatti, la previa valutazione di adeguatezza quale requisito fondamentale per la trasmissione dei dati verso Stati terzi ha certamente consentito di ribadire l'importanza della tutela della privacy e della protezione dei dati come diritti non sacrificabili né dinnanzi ai forti interessi del settore privato – dettati dalla interdipendenza economica con Stati quali gli USA e dall'elevato valore di mercato dei dati –, né di fronte ad una crescente "securitarizzazione"[98] che ha portato all'adozione di normative tese a garantire una prioritaria salvaguardia della sicurezza dei consociati anche mediante l'impiego di strumenti in grado di comprimere in misura significativa i diritti fondamentali[99].

---

[98] Come mette in luce Zalnieriute, del resto, «a great deal of far-reaching 'pro-security' legislation and numerous data-sharing agreements were implemented without any serious democratic debate during the decade following 9/11, and only some received a post factum attention by raising suspicions about their constitutional legitimacy in the US and EU»; in tale contesto dunque, secondo l'autrice, è da leggere positivamente la posizione espressa dalla CGUE: «at least the CJEU will no longer accept the rules of the game for data-sharing modelled around security interests in the previous decades», M. ZALNIERIUTE, *Developing a European standard for international data transfers after Snowden: Opinion 1/15 on the EU-Canada PNR agreement*, cit., p. 1055-1056.

[99] Mendez ad esempio ritiene che «we should praise it [la CGUE] for seeking to ensure

Dall'altro lato, però, il rigido scrutinio adottato dalla CGUE e la lettura da essa fornita del requisito di adeguatezza hanno finito col tradursi, nella concretezza delle relazioni e negoziazioni con Stati terzi, in una oggettiva impossibilità – o quantomeno in una seria difficoltà – applicativa ed attuativa dei principi stabiliti [100]: ciò pare trovare chiara dimostrazione nell'incapacità della Commissione di giungere ad accordi e decisioni stabili e in grado di superare il vaglio dei giudici di Lussemburgo. La più recente pronuncia *Schrems II* ha del resto confermato queste criticità: sconfessando le valutazioni promosse dalla Commissione quanto alla sostanziale equivalenza delle salvaguardie disposte negli USA, è stata nuovamente posta in evidenza non solo la profonda discordanza tra le Istituzioni dell'UE [101] ma anche i limiti stessi dello strumento di adeguatezza,

---

that privacy and data protection standards in the Charter are taken seriously and that, despite the very real threat of terrorism and serious crime, international agreements cannot simply be used in a manner that rides roughshod over these fundamental rights», M. MENDEZ, *Opinion 1/15: the Court of justice meets PNR data (again!)*, cit., p. 811.

[100] Si legga in questo senso la veemente critica rivolta alla CGUE da Espstein il quale considera la giurisprudenza europea erronea non solo sotto il profilo sostanziale della valutazione della ingerenza nei diritti fondamentali perpetrata dal sistema statunitense, ma anche sotto quello della interpretazione del termine stesso di adeguatezza: «It was therefore incorrect, in my view, for the European Court of Justice to take the position that the American statutory framework had to offer protection 'essentially equivalent'to that supplied under exacting European standards, which started from the assumption that the privacy right in data-apparently even that which has been previously publicly posted on Facebook-was a fundamental interest deserving the highest protection». Ciò che viene poi fortemente condannato dall'autore è il peso attribuito nella sentenza *Schrems* alle rivelazioni di Snowden: così facendo la CGUE si è rifiutata di «look closely at the general agreement by which data passed from the EU to the United States. It takes years to put into place successful complex systems of data transmission. It takes only one errant complaint and a dubious decision of the European Court of Justice to rip it all apart», R. EPSTEIN, *The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European Constitutional Law Review*, 12, 2016, p. 339.

[101] Ad esempio, la Commissione, anche all'indomani delle rivelazioni di Snowden e pur avendo dimostrato piena consapevolezza delle debolezze e criticità del meccanismo *Safe Harbour*, aveva preferito lavorare a stretto contatto con le Istituzioni americane al fine di rivedere i principi di Approdo sicuro ed incentivare una loro corretta e concreta attuazione da parte delle aziende e delle autorità pubbliche statunitensi, anziché mettere in discussione la validità

che si rivela così «più debole di quanto appare, incapace in concreto di difendere nella sostanza i confini dello standard di tutela [garantito dall'UE] in un mondo globale e interconnesso» [102]. Una debolezza, quella rilevata, che affonda secondo taluni le proprie radici nella "esaltante illusione" [103] dell'UE di poter proteggere i propri valori e tutelare i diritti dei propri cittadini anche oltre i confini europei mediante l'impiego di quelle che sono state definite forzature unilaterali [104] frutto di una discutibile forma di moderno «imperialismo normativo» [105]. Le critiche alla disciplina normativa in materia di *data transfer* non si sono però limitate ad evidenziare l'illusoria efficacia e le problematiche rinvenute nella concreta attuazione degli strumenti predisposti, bensì hanno anche messo in luce un ulteriore significativo rischio e "malfunzionamento": quello di una deriva "ipocrita" [106] da parte delle Istituzioni europee, che finiscono con il voler imporre, *de facto*, nelle relazioni con Stati terzi la garanzia di livelli di tutela che non sono però spesso concretamente rispettati neppure nel contesto interno all'Unione stessa [107]. Un rischio, questo, che si è rivelato

della decisione di adeguatezza stessa. Più nel dettaglio si legga sul punto F. COUDERT, *Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for Data Protection Authorities,* in *European Law Blog,* 15 ottobre 2015.

[102] A. MANTELERO, *I flussi di dati transfrontalieri*, cit., p. 262.

[103] Per usare una espressione impiegata da C. KUNER, *Reality and Illusion in the EU data transfer regulation post Schrems,* in *German Law Journal*, 4, 2017, p. 898.

[104] Usa questo termine L. ZAGATO, *Il trasferimento di dati personali verso Stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*, in *Diritto del commercio internazionale*, 2, 2008, p. 297 ss., giungendo però alla conclusione secondo cui tale modello di imposizione unilaterale è da considerarsi vincente ed efficace. Anche Kuner parla di «unilateral application» della disciplina europea che non può, però, ad opinione dell'autore, rappresentare uno strumento utile a garantire una completa protezione dei dati e della riservatezza una volta operato il trasferimento (così C. KUNER, *Reality and Illusion in the EU data transfer regulation post Schrems*, cit., p. 910).

[105] Espressione mutuata da M. LEFFI, *I trasferimenti di dati terzi nel nuovo Regolamento UE,* cit., p. 203.

[106] C. KUNER, *Reality and Illusion,* cit., p. 898.

[107] Sul punto si legga anche S. CRESPI, *The applicability of Schrems principles to the Member States: national security and data protection within the EU context,* in *European Law Review*, 43, 2018, p. 669 ss.

ancor più concreto a seguito della lettura combinata della pronuncia *Schrems II* e delle sentenze in materia di *data retention* dell'ottobre 2020: in queste ultime, come si ricorderà, tutte le operazioni di conservazione e trasmissione che implicano un obbligo in capo ad operatori privati sono state considerate riconducibili sotto l'"ombrello" del diritto dell'UE e dunque sottoposte ai limiti disposti dalla CGUE nella sua ampia giurisprudenza; le attività dello Stato, ovvero quelle, quali le intercettazioni dirette, che non richiedono un intervento o un trattamento da parte di operatori privati, sono rimaste invece escluse dall'ambito di applicazione del diritto dell'UE, essendo riconducibili a quelle competenze ancora esclusivamente poste nelle mani degli Stati membri *ex* art. 4 co. 2, TUE: simili attività risultano pertanto svincolate dagli standard fissati dai giudici di Lussemburgo e sottoposte al rispetto dei diritti costituzionali riconosciuti negli ordinamenti nazionali nonché nella giurisprudenza della Corte EDU, che stabilisce però condizioni di legittimità meno stringenti e rigide rispetto a quelle stabilite dalla CGUE [108]. Proprio in questa deli-

[108] La minore tutela offerta dalla Convenzione EDU, così come interpretata dai giudici di Strasburgo è stata peraltro ribadita dal CEPD nelle richiamate Raccomandazioni del 10 novembre 2020. Sebbene non sia possibile, in questa sede, provvedere ad una ricostruzione completa della ampia giurisprudenza della Corte EDU in materia di sorveglianza massiva, pare tuttavia opportuno sottolineare come, soprattutto nelle più recenti pronunce, i giudici di Strasburgo abbiano promosso un vaglio di conformità alla Convenzione EDU dei sistemi di raccolta, conservazione e accesso di dati e metadati per scopi securitari più flessibile rispetto a quello disposto dalla CGUE. La Grande Camera, infatti, nelle attese sentenze del 25 maggio 2021 *Big Brother Watch and others v. UK*, Applications n. 58170/13, 62322/14 e 24960/15 e *Centrum for Rattvisa v. Sweden*, Applications n. 35252/08, ha analizzato rispettivamente la normativa inglese *Regulation Investigatory Powers Act* del 2000, in materia di intercettazioni di telecomunicazioni, *intelligence sharing* e acquisizione di metadati per scopi di sicurezza pubblica e nazionale, nonché la normativa svedese relativa alle operazioni di *Foreign Intelligence* poste in essere per finalità di tutela della sicurezza nazionale (legge 2000:130). Pur premettendo che queste pronunce hanno avuto ad oggetto normative differenti e non esattamente sovrapponibili a quelle analizzate dalla CGUE nella sua *data retention saga*, riguardando operazioni di intercettazione di contenuti e metadati ad opera di autorità di intelligence e riguardanti prevalentemente comunicazioni dirette o provenienti dall'esterno dei confini nazionali (*foreign intelligence*), merita rilevare come la Corte EDU non abbia ritenuto *per se* incompatibili con i diritti tutelati dalla Convenzione EDU forme di intercettazione e trattamento generalizzato (*bulk interception*) di dati (intesi anche come contenu-

to delle comunicazioni), lasciando un ampio «*margin of appreciation*» ai legislatori statali nella determinazione di limiti e condizioni all'impiego di simili sistemi. Nonostante siano stati rilevati tanto nella normativa inglese quanto in quella svedese taluni profili critici e in violazione dell'art. 8 Convenzione EDU, queste ultime sentenze sono state viste da molti studiosi come portatrici di criteri e principi distanti da quelli affermati dai giudici di Lussemburgo, proponendo ad esempio una lettura "globale" delle normative nazionali, valutando così in maniera complessiva e cumulativa la presenza di idonee tutele e salvaguardie. Anche taluni requisiti, quali la notifica ai soggetti interessati o il previo vaglio di una Corte o di una autorità indipendente, sono stati ridimensionati e ristretti, ritenuti non del tutto compatibili con la natura stessa di legittime forme di sorveglianza massiva. Lo stesso dicasi per il requisito del *reasonable suspicion*: «the requirement of "reasonable suspicion", which can be found in the Court's case-law on targeted interception in the context of criminal investigations is less germane in the bulk interception context, the purpose of which is in principle preventive, rather than for the investigation of a specific target and/or an identifiable criminal offence. Nevertheless, the Court considers it imperative that when a State is operating such a regime, domestic law should contain detailed rules on when the authorities may resort to such measures. In particular, domestic law should set out with sufficient clarity the grounds upon which bulk interception might be authorised and the circumstances in which an individual's communications might be intercepted», para. 348. Per questi motivi, rapidamente richiamati, il Giudice De Albuquerque nella sua *Partly concurring and partly dissenting opinion* alla sentenza *Big Brother Watch*, ha sottolineato i potenziali problematici effetti di queste decisioni: «this judgement fundamentally alters the existing balance in Europe between the right to respect for private life and public security interests, in that it admits non-targeted surveillance of the content of electronic communications and related communications data and even worse, the exchange of data with third countries which do not have comparable protection to that of the Council of Europe States. This conclusion is all the more justified in view of the CJEU's peremptory rejection of access on a generalised basis to the content of electronic communications, its manifest reluctance regarding general and indiscriminate retention of traffic and location data and its limitation of exchanges of data with foreign intelligence services which do not ensure a level of protection essentially equivalent to that guaranteed by the Charter of Fundamental Rights. On all these three counts, the Strasbourg Court lags behind the Luxembourg Court, which remains the lighthouse for privacy rights in Europe», para. 59. La distanza tra i principi delineati dalla giurisprudenza delle due Corti europee non può che divenire problematica: le materie escluse dall'ambito di applicazione del diritto dell'UE, infatti, restano soggette al rispetto della Convenzione EDU, come interpretata dai giudici di Strasburgo, così che un differente livello di tutela e una minore rigidità dei requisiti disposti potrebbe finire col creare due diversi standard di tutela dei diritti alla vita privata e alla protezione dei dati dinnanzi all'adozione di sistemi di sorveglianza per scopi securitari. Per una ricostruzione ed analisi critica della giurisprudenza della Corte EDU e

mitazione dell'ambito di applicazione del diritto dell'UE è stata ravvisata una forte incongruenza ed "ipocrisia" rispetto al vaglio di adeguatezza svolto con riferimento al trasferimento dati verso Stati terzi, che, come si è ben visto nella più recente sentenza *Schrems II*, ha avuto ad oggetto anche sistemi di sorveglianza posti direttamente in essere dalle autorità di intelligence – quali l'accesso ai dati operato mediante *Executive Order 12333* –, non limitandosi dunque solo a quelli che rientrerebbero invece, nel contesto interno all'UE, nelle competenze di quest'ultima. Con grande chiarezza, infatti, alcuni autori hanno sottolineato come «in the EU different standards apply to surveillance carried out by Member States under orders issued to prividers of communication services (the standards set by the CJEU in *Schrems II* and *La Quadrature du Net*) and to surveillance carried out by their national security agencies through direct, surreptitious 'hacking' into the providers'systems (the ECHR standards), while surveillance laws and practices of third countries have to "essentially" meet the CJEU standards in relation to both kinds of surveillance if a third country is to be held to provide "essentially equiva-

---

delle sue conseguenze nel panorama europeo (inteso in senso lato) di tutele, si rimanda *ex multis* a T. CHRISTAKIS, K. BOUSLIMANI, *National security, surveillance and human rights*, in R. GEISS, N. MELZER (a cura di), *Oxford handbook on the International Law of global security*, Oxford University Press, Oxford, 2020 (in corso di pubblicazione); N. NI LOIDEAIN, *The approach of the ECtHR to the interception of communications*, nel volume in corso di pubblicazione della medesima autrice dal titolo *EU data privacy law and serious crime. Data retention and policymaking*, Oxford University Press, Oxford, e della stessa autrice *Not so grand: the Big Brother Watch ECtHR Grand Chamber judgement*, in *Information Law and Policy Centre Blog*, 28 maggio 2021; M. MILANOVIC, *The Grand normalization of mass surveillance: ECtHR Grand Chamber judgments in Big Brother Watch and Centrum for Rattvisa*, in EJIL:Talk!, 26 maggio 2021; E. CELESTE, *From the UK adequacy decision to Big Brother Watch: increasingly divergent approaches to mass surveillance in Europe*, in *DCU Brexit Insititute news*, 28 maggio 2021; O. POLLICINO, F. PAOLUCCI, *Big Brother (cannot) watch: the Grand Chambeer ruled against surveillance in the Snowden revelation's aftermath*, in *EULawLive*, 31 maggio 2021; J. SAJFERT, *Big Brother Watch and Centrum for Rattvisa judgements of the Grand Chamber of the European Court of Human Rights: the altamount of privacy?*, in *European Law Blog*, 8 giugno 2021. Sia consentito anche il rinvio a G. FORMICI, *La* digital mass surveillance *al vaglio della Corte Europea dei Diritti dell'Uomo: da* Zakharov *a* Big Brother Watch, in *Federalismi.it – Focus Human Rights*, 23, 2020, p. 44 ss.

lent/adequate" protection in relation to data transfer» [109]. Oltre al differente standard di tutele, l'ipocrisia è stata rilevata anche nel fatto che «EU Member States have been reluctant to come up with laws that actually meet the CJEU standards laid down in its *DRI* and *Tele2* judgements (…). The current laws in the EU Member States have also not yet been brought into line with CJEU judgements in *Privacy International* and *La Quadrature du Net*. And the surveillance laws and practices in many EU Member States would clearly fail the tests applied to the laws and practices of the USA in *Schrems II*» [110]. Sulla base di queste valutazioni e per evitare un approccio incoerente e ipocrita, dovrebbero essere conseguentemente escluse dal vaglio di adeguatezza della Commissione – e dunque anche del successivo eventuale esame della CGUE – tutte quelle operazioni di acquisizione e accesso a dati e metadati che, entro i confini europei e rispetto agli Stati membri, risultano essere poste al di fuori dell'ambito di applicazione del diritto dell'UE. Dinnanzi a simili problematiche riflessioni, che impongono un serio ripensamento dei confini del controllo stesso di adeguatezza e che si scontrano con il vaglio più estensivo sino ad ora svolto dalla CGUE nei casi *Schrems*, la Commissione sarà ora chiamata a prendere una decisa posizione nel corso delle negoziazioni con gli USA, dovendo quindi valutare quali tipologie di norme e sistemi di sorveglianza considerare nel proprio vaglio e quali livelli di protezione individuare a seconda dei diversi mezzi di sorveglianza considerati. Da questo delicato punto emerge con evidenza il significativo intreccio venutosi a creare tra principi stabiliti dalla giurisprudenza in materia di conservazione dei metadati e pronunce nell'ambito del *data transfer*: i

[109] I. BROWN, D. KORFF, *Exchanges of personal data after the Schrems II judgement*, cit., p. 32. In tale elaborato viene ampiamente richiamata la posizione espressa dal Governo statunitense nel già citato documento *Comments on the proposed EDPB Recommendations 1/2020*. Anche Christakis e Propp hanno rilevato come «EU law provides no national security exemption that may be invoked on behalf of third-state intelligence services. The US, as well as other third countries, will remain under the close scrutiny of the CJEU in *Schrems*-like cases addressing their "adequacy" and "essential equivalence"», T. CHRISTAKIS, K. PROPP, *How EU's intelligence services aim to avoid the EU's highest Court and what it means for the US*, in *LawFare*, 8 marzo 2021.

[110] I. BROWN, D. KORFF, *Exchanges of personal data after the Schrems II judgement*, cit., p. 56.

futuri sviluppi, anche legislativi, della disciplina della *data retention* dovranno dunque essere osservati con attenzione anche al fine di determinare quegli standard di protezione dei diritti fondamentali che costituiscono il parametro di riferimento per stabilire la sostanziale equivalenza delle tutele offerte dagli Stati terzi riceventi dati dall'UE [111].

Se dunque anche da tali profonde critiche e dai rilevati effetti negativi e "distorsivi" del meccanismo del trasferimento dati emergono le debolezze e le inefficienze tanto dell'operato della Commissione quanto della rigidità della giurisprudenza della CGUE e delle sue discrepanze, è necessario ora interrogarsi sulle ragioni più profonde delle problematiche riscontrate: se i fatti hanno dimostrato, nelle vicende giudiziarie della *Schrems saga*, l'incapacità della Commissione di negoziare accordi e decisioni di adeguatezza in grado di integrare i limiti e le salvaguardie fornite dal diritto dell'UE come interpretato dai giudici di Lussemburgo, tale incapacità non pare però semplicisticamente riconducibile solo ed unicamente ad una limitata attenzione da parte della Commissione stessa ai principi e requisiti sanciti dalla giurisprudenza sovranazionale; essa va piuttosto identificata anche nelle carenze e nel "malfunzionamento" intrinseco del meccanismo di adeguatezza e, in particolare, nella sua interpretazione da parte della CGUE che, fissando standard elevati di tutela e imponendo una sostanziale equivalenza delle garanzie predisposte [112], si scontra con

[111] Non bisogna poi dimenticare come tutte le osservazioni sin qui proposte debbano indurre a riflettere anche sul destino della discussa Decisione di adeguatezza adottata dalla Commissione nel giugno 2021 e avente ad oggetto il trasferimento dati verso il Regno Unito, divenuto uno Stato terzo a seguito del percorso di recesso dall'UE (c.d. *Brexit*). Sebbene su questo punto specifico si concentrerà il Capitolo 4, ampiamente dedicato al Regno Unito, diviene chiaro come tutte le criticità e le fragilità sino ad ora evidenziate ben possano riverberarsi anche sulla regolamentazione del trasferimento dati Oltremanica: già da più parti, come si dirà, sono state infatti evidenziate le debolezze delle tutele offerte dall'ordinamento inglese, soprattutto rispetto all'impiego di sistemi di sorveglianza quali quelli posti in essere direttamente dalle autorità di intelligence Oltremanica, così che il dibattito sulla correttezza delle valutazioni della Commissione e la "stabilità" della Decisione di adeguatezza risulta ancora, similmente a quanto avvenuto rispetto agli USA, del tutto aperto.

[112] Criticamente, si legga Dhont: «There are no easy answers as to how personal data should be protected when it leaves the EU. However, a legal regime which structurally adversely impacts international trade in virtue of protecting a human right seems difficult

quelle concrete difficoltà che la Commissione si trova invece a dover affrontare nei rapporti con Stati terzi caratterizzati da tradizioni giuridiche e tutele normative anche molto differenti da quelle europee [113]. È dinnanzi a questa situazione fattuale e mossa dalla volontà di evitare una inutile posizione di rigido scontro con i Paesi riceventi i dati, che la Commissione si è trovata a dover adottare Decisioni di adeguatezza ed accordi "di compromesso", fondati su una lettura del requisito di adeguatezza certamente più flessibile rispetto a quella fornita dalla giurisprudenza della CGUE ma che ha al contempo concesso di addivenire a soluzioni accettabili anche dagli Stati terzi.

Ecco allora che le inefficienze e le criticità riscontrate nella pratica attuazione della disciplina del trasferimento dati debbono essere ricondotte ad un "concorso di colpa" tra Commissione e CGUE e non unicamente agli erronei approcci dell'una o dell'altra: parafrasando la massima latina *errare humanum est, perseverare autem diabolicum*, Pollicino ha efficacemente riassunto la situazione descritta come «the diabolical persistence of the European Commission and the judicial manipulation as the original sin of the CJEU and its (not so hidden) ambitions and frustrations» [114].

---

to justify. To put it somewhat dramatically: not only would it not be sustainable in the long term, it would, in essence, constitute a threat to the values on which it is based, that is, economic prosperity and peace», J.X. DHONT, *Schrems II. The EU adequacy regime in existential crisis?*, in *Maastricht Journal of European and Comparative Law*, 5, 2019, p. 601.

[113] Secondo alcuni autori, infatti, la tutela della continuità degli standard europei si ridurrebbe, nella realtà dei fatti, ad una discutibile valutazione unilaterale del sistema giuridico straniero dello Stato terzo ricevente i dati. Se nella sentenza *Schrems* era stato specificato come il termine "adeguatezza" non dovesse essere interpretato nel senso di "eguaglianza", non rilevando dunque ai fini di tale valutazione il fatto che gli strumenti normativi impiegati da Paesi terzi fossero differenti da quelli europei, nella stessa pronuncia però i giudici erano poi entrati «eccome nel merito degli strumenti normativi che assicurano la protezione dei dati personali nell'ordinamento (…) E lo fa con un approccio che è inedito, almeno per quanto riguarda le decisioni che più direttamente vertono in materia di diritti fondamentali, e non di libertà economiche: con uno sguardo pragmatico e un'attenzione particolare per il soddisfacimento dell'obiettivo di tutela sotteso alle misure in questione», giungendo così a manipolare il più flessibile significato del termine "sostanziale equivalenza"», O. POLLICINO, M. BASSINI, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo,* cit., p. 87.

[114] O. POLLICINO, *Diabolical persistence. Thoughts on the Schrems II decision*, in *Me-*

Una "perseveranza diabolica" e un "peccato originale", quelli descritti, che possono risultare in altrettanto "diaboliche" conseguenze: il rischio infatti è che lo strumento della decisione di adeguatezza, da meccanismo volto a garantire un elevato livello di tutela della privacy e della protezione dei dati, finisca con l'assumere il ruolo di uno strumento meramente dilatorio, con il quale cioè stabilire soluzioni e condizioni di trasferimento consapevolmente non del tutto conformi ai principi stabiliti dalla giurisprudenza europea ma che raggiungono nondimeno l'obiettivo di garantire, almeno sino all'eventuale – ma altamente probabile – intervento della CGUE, un più agile flusso dei dati verso Stati terzi. Se questa diventasse realmente la prassi, la disciplina in materia di *data transfer* predisposta dal GDPR e, prima ancora, dalla Direttiva 95/46, verrebbe privata, alla radice, della sua capacità ed aspirazione alla garanzia di un elevato livello di protezione dei dati e della riservatezza anche al di là dei confini dell'UE.

Il pericolo che le più flessibili valutazioni di adeguatezza svolte dalla Commissione e la loro successiva invalidazione da parte della CGUE divengano la prassi, ripetendosi in un vizioso circolo di instabilità che rischia di svuotare del suo significato e scopo sostanziale il meccanismo di adeguatezza, va dunque scongiurato: sarà per questo sempre più fondamentale per il futuro elaborare una linea di azione coerente e condivisa tra tutte le Istituzioni europee, al fine di individuare un punto di equilibrio che risulti in valutazioni e condizioni di trasferimento dati stabili e concretamente realizzabili nei rapporti con gli Stati terzi, pur senza sacrificare la garanzia di un elevato livello di tutela dei diritti fondamentali. Ciò richiede non solo un maggior dialogo tra Istituzioni ma anche una coerente lettura del portato normativo in materia di *data transfer* rispetto ai principi stabiliti in altri ambiti ad esso strettamente connessi, quale

---

diaLaws, 3, 2020, p. 315. Come anticipato nella previa nota, secondo l'autore, la "manipolazione" operata dalla CGUE può essere individuata nel suo discostarsi dal concetto di adeguatezza per promuovere invece una "sostanziale equivalenza": mentre la prima non implica una comparazione tra il livello di protezione garantito nell'UE e quello dello Stato terzo, la seconda al contrario impone un raffronto ben più delicato e problematico tra ordinamenti. In questo senso quindi la CGUE manipola il dato normativo della Direttiva 95/46 prima e del GDPR poi, per innalzare lo standard di garanzia dei diritti fondamentali.

quello della *data retention*, evitando così pericolosi dubbi interpretativi ed incertezze attuative. Come ben riassunto da Celeste, allora, «certainly, the persistence of issues related to the application of the EU data protection framework should not let us desist from adopting a strict approach when it comes to assessing the adequacy of the level of protection offered by third countries. Yet, this must remind us to take a humbler and self-critical attitude when looking at our neighbours' eyes» [115].

Se tutte le significative criticità e i limiti sino ad ora riportati e dimostrati dalle complesse vicende giurisprudenziali analizzate mostrano certamente l'imperfezione della disciplina europea in materia di *data transfer* e la necessità di ripensare tale strumento nella sua concreta attuazione, non si può tuttavia mancare di sottolineare anche l'altro lato della medaglia, per fornire una analisi obiettiva e completa della materia: nell'approccio adottato dall'Unione, infatti, può essere individuata non solo quella richiamata volontà di esportare e imporre il modello normativo europeo ai legislatori stranieri, bensì anche l'intenzione di esercitare una positiva influenza nel contesto internazionale, volta a contribuire alla costruzione di un «regime internazionale di tutela della vita privata e delle informazioni di natura personale» [116]. In questo senso, e non solo in quel-

[115] E. CELESTE, *Commission v. Spain and H.K. v. Prokuratuur: taking the plank out of EU's own eye*, in *Bridge Blog*, 15 marzo 2021. Il rischio è peraltro quello di creare una situazione di isolamento dell'UE, data dalla difficoltà da parte degli Stati terzi di negoziare accordi conformi agli standard europei o derivante dalla reticenza e diffidenza degli Stati terzi stessi: questi, pur interessati ad attivare lunghi e costosi procedimenti di negoziazione con l'UE, potrebbero risultare scoraggiati dal timore dell'instabilità dell'accordo ottenuto o della relativa decisione di adeguatezza, che potrebbero essere entrambi suscettibili di invalidazione da parte della CGUE, come le vicende della *Schrems saga* e del *Parere 1/15* hanno ampiamento dimostrato. Di fronte a questa consapevolezza e vedendo nel raggiungimento di un accordo internazionale che fissi livelli globali di tutela della *privacy* e di protezione dei dati l'unica possibile soluzione per ovviare ai pericoli insiti nella sussistenza di differenti standard di garanzia nazionale, alcuni autori, come Reidenberg, ritengono che l'UE debba rassegnarsi ad accettare l'idea che il proprio livello di tutela non venga adottato in Stati terzi (J. REIDENBERG, *The transparent citizen,* in *Loyola University Chicago Law Journal*, 47, 2015, p. 437).

[116] «L'Unione può svolgere un ruolo chiave e di guida, valorizzando siffatto modello [frutto dei principi delineati nella giurisprudenza della CGUE e nella normativa GDPR] nell'ambito di fora internazionali, nella prospettiva della costruzione di un re-

lo di un già richiamato di «imperialismo normativo europeo», può essere letto l'art. 50 del GDPR in materia di cooperazione internazionale per la protezione di dati personali, che prevede in capo alla Commissione e alle autorità di controllo nazionali il compito di sviluppare meccanismi di collaborazione con Stati terzi o con organizzazioni internazionali volti a facilitare una efficace applicazione di elevati standard di protezione dei dati e a prestare assistenza a livello internazionale. Così, questa previsione normativa «potrebbe incarnare uno Zeitgeist europeo in una materia ancora in bilico fra resistenza ad ogni cedimento sul piano della tutela del diritto, e volontà di aprire strade nuove, che comunque non facciano della protezione dei dati un ostacolo insormontabile allo sviluppo» [117].

Se si osserva sotto questo ulteriore profilo la discussa disciplina e giurisprudenza europea in materia di *data transfer*, può essere allora riconosciuta all'UE la capacità di utilizzare efficacemente il necessario e ormai irrinunciabile flusso di dati oltre i confini europei come mezzo per porsi quale «fortress of digital privacy» [118] nel panorama internazionale, trasformando, mediante il meccanismo dell'adeguatezza, i propri standard interni di tutela in «*de facto* standard» [119] internazionali a garanzia di una

---

gime internazionale di tutela della vita privata e delle informazioni personali, sia che si scelga la strada della conclusione di un trattato internazionale, sia che gli Stati stabiliscano un modello giuridico internazionale sulla falsariga del modello UNCITRAL», M. NINO, *Le prospettive internazionali ed europee della tutela della privacy*, cit., p. 785. Questo interessante profilo della opportunità e importanza di raggiungimento di accordi internazionali sarà oggetto di considerazioni specifiche nelle Conclusioni di questo lavoro.

[117] M. LEFFI, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, cit., p. 203.

[118] Così F. FABBRINI, *The EU Charter of Fundamental Rights and the rights to data privacy: the EU Court of Justice as a Human Rights Court*, in S. DE VRIES et al. (a cura di), *The EU Charter of Fundamental Rights as a binding instrument: five years old and growing*, Bloomsbury, Londra, 2015, p. 261; e similmente W.B. WRAY, *A European approach to the United States Constitutional privacy*, in *Craighton International and Comparative Law Review*, 51, 2015, p. 51 e L.P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of the Eu and US constitutional systems*¸ in L. VIOLINI, A. BARAGGIA (a cura di), *The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and non-Judicial Actors*, Elgar Publish, Cheltenham, 2018, p. 114 ss.

[119] M. BRKAN, *The unstoppable expansion of the EU fundamental right to data protec-*

maggiore salvaguardia dei diritti fondamentali alla riservatezza e alla protezione dei dati. Pur con tutti i limiti riscontrati nella ricostruzione critica sopra svolta, un tale approccio ha avuto effetti innegabilmente positivi sul fronte delle scelte adottate tanto dagli operatori privati quanto dalle autorità pubbliche di Stati terzi. Con riferimento ai primi, ed in particolare alle aziende operanti nel settore digitale aventi sede al di fuori del territorio europeo ma riceventi dati dall'UE, molte di esse hanno già allineato o stanno allineando quanto più possibile le proprie *policies* in materia privacy e *data protection* ai principi e criteri indicati dalla normativa e giurisprudenza europea, reputando tale scelta più conveniente e meno rischiosa – per quanto almeno inizialmente più onerosa – al fine ultimo di scongiurare il pericolo di vedere il flusso di dati interrotto e quindi subire un forte svantaggio competitivo ed economico [120]. Oltre a predisporre politiche interne o ad utilizzare strumenti alternativi in grado di garantire la sostanziale equivalenza delle tutele offerte, in caso di assenza di una decisione di adeguatezza della Commissione i soggetti privati possono poi utilmente fare pressione sui legislatori nazionali degli Stati terzi affinché

tion. little shop of horrors?, in *Maastricht Journal of European and Comparative Law*, 5, 2016, p. 812 ss.

[120] «Multinational corporations have adjusted their global data management systems to reduce their compliance costs with multiple regulatory regimes», A. BRADFORD, *The Brussels effect*, cit., p. 25. «In the short term, organisations may consider keeping personal data in the EU and avoiding transfers to the US. Some US companies offer cloud customers the option to store personal data in Europe so that it is not sent for storage elsewhere. For instance, Amazon announced on 6 November 2015 that it would be building data centres in the UK in 2016. A few days later, the CEO of Microsoft, Satya Nadella, also announced that Microsoft was opening data centres in the UK for the first time. The new data centres will enable UK users of Microsoft's cloud services, Azure and Office 365, to keep their data within Europe at all times. Companies that provide cloud services within the EU and rely on data centres in the US may invest in data centres within the EU provided they sign contracts with European companies only. European based cloud providers that ensure compliance with EU law could thus benefit from the situation», X. TRACOL, *"Invalidator" strikes back: the harbour has never been safe*, cit., p. 360. Sin dal 2000, inoltre, non si è mancato di sottolineare come i principi *Safe Harbour* avessero contribuito ad innalzare gli standard di protezione dei dati e di tutela della riservatezza negli USA: sul punto si legga G. SHAFFER, *Globalization and social protection: the impact of EU and International Rules in the ratcheting up of US data privacy standards*, in *Yale Journal of International Law,* 25, 2000, p. 1 ss.

approvino normative a tutela della riservatezza e protezione dei dati capaci di consentire un maggior avvicinamento agli standard europei [121], promuovendo questo obiettivo e ponendolo all'attenzione del dibattito politico del Paese terzo in cui operano. Anche grazie a tali interventi, trend positivi nella direzione di più elevate garanzie si riscontrano dunque nelle scelte normative adottate dai legislatori di Stati terzi: basti pensare allo Stato della California che, in assenza di una normativa federale statunitense in materia di protezione dei dati, ha elaborato nel 2018 il *California Consumer Privacy Act* (CCPA), chiaramente ispirato alla disciplina del GDPR [122], a dimostrazione di quanto la necessità di garantire la continuità del flusso di dati con l'UE, particolarmente importante per le aziende operanti nella c.d. *silicon valley*, abbia incentivato i legislatori statali ad incrementare e migliorare le proprie normative in materia di *data protection*. È quello che Bradford ha definito *Brussels effect*, considerando «the unprecedented and deeply underestimated global power that the European Union is exercising through its legal institutions and standards, and how it successfully exports that influence to the rest of the world» e che si esplica anche attraverso le azioni esterne dell'UE sino ad ora descritte nell'ambito della tutela della privacy e protezione dei dati [123]. La disciplina europea in materia di *data transfer* e la sua interpretazione da parte dei giudici di Lussemburgo ben può essere iscritta, quindi, «all'interno della dinamica di competizione regolatoria (…), dove ai ripetuti fenomeni di violazione transfrontaliera dei diritti fondamentali – resi possibili dallo sviluppo delle tecnologie dell'informazione e della comunicazione – corrispondono puntualmente meccanismi di reazione a carat-

[121] Si legga ampiamente sul punto UNCTAD, *Data protection regulations and international data flows: implications for trade and development*, 2016.

[122] L'atto è entrato in vigore nel gennaio 2020; alcune disposizioni di questo testo normativo sono molto simili a quanto stabilito nel GDPR: sono incluse previsioni circa il diritto di accesso, il diritto di *opt-out*, il diritto di azione in caso di *data-breach*, sanzioni amministrative, diritto all'oblio (tale diritto presenta però notevoli differenze rispetto alla versione europea, facendo emergere quell'innegabile distanza insita nelle peculiarità dei diversi ordinamenti). Sul punto si legga L. DETERMANN, *California Privacy Law. Practical guide and commentary*, IAPP, Portsmouth, 2020.

[123] Utilizzando il termine impiegato da A. BRADFORD, *The Brussels effect*, cit., p. 1.

tere dichiaratamente "nazionalistico". Tale termine [in questo contesto] non è impiegato in un'accezione dispregiativa, bensì per denotare l'impronta tipicamente "locale" del modello di disciplina (e di bilanciamento degli interessi) che si intende proteggere, a fronte dei rischi di aggiramento derivanti dall'utilizzo delle tecnologie informatiche e dalla de-localizzazione dei dati su server remoti» [124]. Ecco allora che, sotto questo profilo, non può essere negato all'azione dell'UE il riconoscimento di un positivo riflesso e ripercussione sugli Stati terzi, sia mediante il requisito dell'adeguatezza, utilizzato quale moderna forma di «gunboat diplomacy» [125] per indurre ad una modifica ed innalzamento del livello di tutela offerto dallo Stato terzo ricevente, sia attraverso azioni promosse a livello delle organizzazioni internazionali, incoraggiando ad esempio l'adesione alla Convenzione del Consiglio d'Europa n. 108 [126].

Da questi innegabili profili positivi, si può certamente comprendere come una corretta analisi della materia del *data transfer* debba essere svolta valutando la complessità delle diverse sfaccettature della disciplina normativa sovranazionale e della sua concreta attuazione. Gli effetti indubbiamente virtuosi che il meccanismo dell'adeguatezza e le pronunce dei giudici di Lussemburgo hanno comportato, imponendo una maggiore attenzione alle condizioni del trasferimento e ponendosi alla base di evoluzioni e sviluppi migliorativi delle normative adottate in Stati terzi [127], hanno spinto il dialogo e il dibattito politico e legislativo, anche a

---

[124] G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE,* in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, p. 45.

[125] M. TZANOU, *European Union regulation of transatlantic data transfers and online* surveillance, cit., p. 552.

[126] Oppure adottando, in sede dell'ICAO, una posizione unitaria tra tutti gli Stati membri finalizzata a promuovere una modifica a livello internazionale degli standard in materia di PNR che vada nella direzione di una maggiore garanzia dei diritti fondamentali (COM(2019) 416 final).

[127] Indiscutibilmente i principi disposti nel meccanismo *Privacy Shield* ponevano tutele ben più significative rispetto a quelle del previo *Safe Harbour*, così come nella medesima direzione si sono indirizzate le riforme adottate dal legislatore statunitense a seguito delle rivelazioni di Snowden e della sentenza *Schrems*, portando all'introduzione di maggiori garanzie nei sistemi di sorveglianza segreta.

livello internazionale, in una direzione maggiormente *human rights-oriented*, anche dinnanzi alle stringenti esigenze securitarie. Nonostante questo, le difficoltà attuative di tali principi e le continue invalidazioni delle decisioni adottate dalla Commissione fanno inevitabilmente sorgere interrogativi che mettono in dubbio tanto l'efficacia effettiva dello strumento impiegato quanto la posizione della CGUE che, nel valutare la dimensione esterna della tutela dei dati e della privacy, sembra aver fissato l'asticella delle garanzie ad un livello troppo elevato per essere raggiunto correttamente nella concretezza degli accordi e delle condizioni regolanti i *data transfer*, favorendo così il continuo ripetersi di situazioni altamente problematiche che, al momento, non sono ancora riuscite a trovare soluzione definitiva e certa. Se quindi è vero che «protecting privacy and facilitating data flows has to go hand in hand» [128], pare altrettanto corretto asserire che questo percorso condiviso non è ancora giunto al traguardo.

In queste riflessioni e considerazioni non può non essere chiaramente rinvenuta una sostanziale similitudine e connessione con quanto analizzato nel Capitolo precedente con riferimento alla disciplina della *data retention* entro i confini dell'UE: su entrambi i fronti infatti la situazione si pone aperta e in attesa di importanti sviluppi che ne determineranno il destino nel prossimo futuro; in entrambe le dimensioni, interna ed esterna all'UE, si ravvede poi la difficoltà di porre concretamente in essere discipline normative capaci di integrare gli elevati standard di garanzia dei diritti fondamentali alla riservatezza e alla vita privata così come fissati dalla giurisprudenza della CGUE [129]. Sebbene quest'ultima, anche nell'ambito del trasferimento dati, abbia contribuito ad innescare un positivo processo di innalzamento delle tutele offerte non solo dagli Stati membri ma anche da ordinamenti di Stati terzi, resta evidente come le esigenze securitarie spingano Governi e legislatori nazionali – tanto di

[128] *Joint Statement by Vice-President Jourova and Commissioner Reynders ahead of Data Protection Day*, 27 gennaio 2021, disponibile all'indirizzo https://ec.europa.eu/commission/presscorner/detail/en/statement_21_208.

[129] Una tendenza che Christakis e Propp definiscono «judicialization of the fundamental right to data protection in all settings», T. CHRISTAKIS, K. PROPP, *How EU's intelligence services aim to avoid the EU's highest Court and what it means for the US*, cit.

Stati membri quanto di Stati terzi – verso l'adozione di sistemi di sorveglianza che sfruttino appieno le potenzialità delle nuove tecnologie. Il processo per la determinazione di un concreto e raggiungibile bilanciamento tra queste due differenti spinte appare, così, dinnanzi a tutte le criticità e le attese evoluzioni, ancora in divenire.

CAPITOLO 4

IL REGNO UNITO. LA DISCIPLINA DELLA *DATA RETENTION*: SPINTE CONTRAPPOSTE ALL'OMBRA DELL'INEDITA SFIDA DELLA *BREXIT*

SOMMARIO: 1. Il diverso approccio di legislatori e Corti nazionali in materia di *data retention*: una necessaria premessa sull'importanza dell'analisi comparata. – 2. Il legislatore del Regno Unito e la disciplina della *data retention*. – 2.1. Un sostanziale cambio di approccio: dalla volontarietà della conservazione dei metadati al *Data Retention (EC Directive) Regulations 2009*. – 2.2. Le rapide e dibattute reazioni del legislatore nazionale alla sentenza *DRI*: il *Data Retention and Investigatory Powers Act* (DRIPA). – 2.3. L'adozione dell'*Investigatory Powers Act* (IPA) nelle more del caso *Tele2*. – 2.4. Le modifiche alla disciplina nazionale apportate dal *Data Retention and Acquisition Regulations 2018*. – 3. Le Corti inglesi e i principi delineati dalla giurisprudenza sovranazionale, tra divergenze e avvicinamenti. – 3.1. La decisione della *High Court* in merito alla compatibilità del DRIPA con il diritto dell'UE. – 3.2. La diversa lettura promossa dalla *Court of Appeal*: i motivi del primo rinvio pregiudiziale ai giudici di Lussemburgo. – 3.3. Le valutazioni della *Court of Appeal* a seguito della pronuncia *Tele2*: una complessa decisione tra mutamenti del quadro normativo e importanti casi giurisprudenziali pendenti. – 3.4. La sentenza della *High Court* nel caso *Liberty* avente ad oggetto la *Part 4* dell'IPA. – 3.5. Le pronunce dell'*Investigatory Powers Tribunal*: il rinvio alla CGUE nel caso *Privacy International* e la decisione finale del 22 luglio 2021. – 4. Provvisorie considerazioni sulla disciplina inglese della *data retention*: ulteriori e doverosi interventi all'orizzonte? – 5. Garantire il flusso di dati UE-Regno Unito nello scenario *post-Brexit*: il dibattito sull'adeguatezza delle garanzie offerte Oltremanica. – 5.1. Il lento e difficile cammino verso l'adozione di una decisione di adeguatezza. – 5.2. L'auspicata – e criticata – decisione di adeguatezza del 28 giugno 2021: un instabile destino per il trasferimento dati Oltremanica?

1. *Il diverso approccio di legislatori e Corti nazionali in materia di* data retention*: una necessaria premessa sull'importanza dell'analisi comparata.*

L'analisi svolta nei precedenti Capitoli ha contribuito a ricostruire il complesso quadro normativo europeo in materia di *data retention* e accesso ai metadati per scopi securitari, unitamente alla lunga giurisprudenza della CGUE, che ha stabilito importanti principi anche sul fronte esterno all'UE, con riferimento alle operazioni di *data transfer*.

Mentre sino ad ora lo studio delle vicende caratterizzanti gli Stati membri è stato affrontato in maniera funzionale alla comprensione piena delle decisioni dei giudici di Lussemburgo e delle scelte del legislatore europeo, in un gioco di continui rimandi e dialoghi tra livelli, in questo e nei prossimi Capitoli, invece, al centro dell'analisi vogliono essere specificamente posti gli approcci e le valutazioni di legislatori e Corti nazionali. Questo risulta essere senz'altro il punto prospettico meno esplorato della materia in esame: più spesso, infatti, la tendenza è quella di investigare poco e in maniera limitata il dibattito legislativo e giurisprudenziale interno agli Stati membri, per prestare maggiore attenzione alle pronunce della CGUE, con esse arrestando l'analisi. In tale contesto, la disamina puntuale e sistematica del livello nazionale si pone dunque come portato maggiormente innovativo ed originale del presente lavoro: il motto europeo volto a sottolineare l'importanza dell'unità nella diversità, viene così calato nella concreta operatività dell'interazione multilivello con riferimento alla peculiare materia della conservazione e accesso ai metadati.

Il risultato di un simile studio, lungi dall'essere fine a sé stesso, vuole costituire la base per osservare appieno e più approfonditamente, in chiave comparata, quanto l'esperienza propria di un Stato si distingua o converga da quella di un altro: l'analisi delle scelte e del bilanciamento tra esigenze securitarie e diritti fondamentali svolti dai legislatori nazionali, unitamente alle posizioni espresse dai giudici nazionali, consentirà di muovere osservazioni e riflessioni sugli aspetti che distanziano o accumunano i diversi approcci nonché sulle motivazioni di simili o differenti soluzioni, identificando possibili convergenze, differenze o, ancora, esempi e *trend* virtuosi, tra realtà statuali stesse ma anche tra queste e il livello sovranazionale, pur tenendo sempre in debita considerazione le peculiarità

che contraddistinguono gli ordinamenti e che non possono che essere considerate ai fini di un corretto raffronto [1].

Su tali premesse poggia dunque la decisione di dedicare ampio spazio a tre Stati membri – sebbene per il primo di essi tale qualifica non sia più attuale –: Regno Unito, Belgio e Italia. Se, anche a seguito della costante e copiosa giurisprudenza della CGUE, permane ancora nel territorio dell'UE un panorama frammentario e variegato di soluzioni statuali in tema di *data retention*, l'individuazione proprio di questi tre Stati, come anticipato nell'Introduzione, è motivata dal fatto che essi risultano essere paradigmatica espressione di approcci diversi alla materia in esame, pur dimostrando punti in comune, come evidenziato dalle simili problematiche affrontate e rilevate anche in occasione dei molteplici interventi della CGUE. Il Regno Unito ha conosciuto una parabola normativa che, pur caratterizzata da rapidi interventi che non sempre hanno atteso le valutazioni dei giudici di Lussemburgo su vicende rilevanti, si è comunque mossa nella direzione di una sempre maggiore garanzia della proporzionalità dell'ingerenza nella sfera privata rappresentata dalla disciplina della

[1] Con riferimento ai tre Stati membri scelti, ad esempio, gli strumenti di accesso alla giustizia e, ancora, l'attivazione dell'intervento dei giudici costituzionali, risultano estremamente diversi: pur rimandando ai singoli Capitoli per analisi più dettagliate, merita sin da ora sottolineare come nel Regno Unito sia stato predisposto un apposito organo giurisdizionale, l'*Investigatory Powers Tribunal*, deputato a decidere nei casi di illegittimo trattamento dei dati da parte di autorità pubbliche quali agenzie di intelligence, polizia e autorità locali, nell'esercizio di azioni di sorveglianza per scopi securitari. In Belgio, la Costituzione prevede la possibilità di richiedere un controllo astratto di legittimità alla Corte costituzionale mediante ricorso per annullamento, attivabile anche da persone fisiche e giuridiche. Strumenti di accesso alla giustizia costituzionale quale quello belga o organi giurisprudenziali *ad hoc* quale quello inglese, non sono invece presenti nell'ordinamento italiano: una simile considerazione delle caratteristiche dell'ordinamento italiano rispetto agli altri Stati analizzati aiuta a meglio comprendere il perché le pronunce rilevanti in materia di *data retention* in Italia si riscontrino quasi unicamente nell'ambito di procedimenti giudiziari di natura penale; ciò contribuisce inoltre a valutare più correttamente il diverso vaglio effettuato dagli organi giurisdizionali nei tre Stati: quello in astratto svolto da giudici costituzionali è necessariamente differente da quello elaborato da giudici penali all'interno di una controversia o ancora da quello sviluppato da una Corte specificamente deputata a dirimere controversie attinenti a strumenti di sorveglianza. Una appropriata considerazione di questi aspetti risulta fondamentale al fine di proporre una lucida e corretta disamina e comparazione.

data retention e accesso ai metadati per scopi securitari; una direzione che, seguita anche dalla giurisprudenza nazionale, non ha però mancato di alimentare un dialogo con i giudici di Lussemburgo dai toni talvolta aspri, finalizzato a determinare con chiarezza i confini tra competenze nazionali e dell'UE, con un approccio che ha visto poi, senza dubbio, nella procedura di c.d. *Brexit* una più netta esplicitazione. Pur non rinunciando del tutto, come si dirà, a forme di *bulk acquisition* o *bulk data retention*, il percorso seguito dal Regno Unito è stato certamente indirizzato ad un innalzamento dei limiti al ricorso a strumenti di sorveglianza.

Diverse invece sono le vicende che hanno caratterizzato il Belgio: a seguito del netto intervento della *Cour constitutionnelle* che, per ben due volte, all'indomani delle pronunce della CGUE, ha dichiarato l'incompatibilità della normativa nazionale rispetto al diritto dell'UE, il legislatore nazionale si è avviato verso la complessa adozione di una disciplina di *targeted data retention*, nel tentativo di conformarsi quanto più possibile alla giurisprudenza sovranazionale. Anche la Corte costituzionale belga, da un iniziale atteggiamento considerato quasi ossequioso, si è fatta promotrice di rinvii ai giudici di Lussemburgo basati sul riconoscimento di diverse possibili interpretazioni dei principi fissati dalla giurisprudenza della CGUE e su talune persistenti criticità bisognose di chiarimenti. Un dialogo multilivello che invece è stato solo in tempi estremamente recenti avviato dall'Italia, che non ha saputo promuovere, neppure dinnanzi alle dirompenti sentenze della CGUE, un profondo e consapevole dibattito in materia di *data retention*; al contrario, anzi, il legislatore italiano ha sempre introdotto, in maniera piuttosto confusa, normative che, lungi dal considerare elementi di conservazione mirata, hanno sollevato, soprattutto in dottrina, significativi dubbi di conformità al diritto dell'UE. Similmente, le Corti italiane hanno quasi sempre risolto con grande rapidità e semplicità di motivazioni e analisi le complesse questioni che erano invece confluite in numerosi rinvii pregiudiziali da parte di altre Corti nazionali, quali quelle belga e inglese.

Tre approcci, quelli qui sinteticamente tratteggiati, che, nel rivelarsi esemplificativi di divergenze e convergenze, mostrano dunque la ricchezza e l'importanza delle riflessioni che proprio dalla analisi comparata di diversi ordinamenti nazionali possono scaturire.

2. *Il legislatore del Regno Unito e la disciplina della* data retention.

2.1. *Un sostanziale cambio di approccio: dalla volontarietà della conservazione dei metadati al* Data Retention (EC Directive) Regulations 2009.

Il primo ordinamento ad essere esaminato è quello del Regno Unito.

Volendo prendere avvio – con uno schema che verrà riproposto anche nei successivi Capitoli – dalla ricostruzione dell'evoluzione normativa, è necessario sottolineare come nel Regno Unito non fosse presente, sino al 2007, un obbligo di conservazione dei metadati in capo ai fornitori di servizi di telecomunicazione. Vigeva dunque inizialmente la regola generale secondo cui i metadati dovevano essere cancellati dai *service operators* quando non più utili per finalità commerciali – ad esempio per scopi di fatturazione –. Solo nel 2001, con il *Anti-terrorism, Crime and Security Act* (ATCSA), era stato introdotto un sistema di conservazione di tipo volontario: i fornitori potevano cioè scegliere di conservare i metadati al fine di renderli disponibili alle autorità pubbliche per scopi di salvaguardia della sicurezza nazionale o di prevenzione dei crimini. Il *Secretary of State*[2] aveva il compito di elaborare uno specifico *Code of pratice* (CoP) che, fissando le regole e le condizioni della *data retention*, avrebbe dovuto essere seguito dagli operatori interessati[3]. A dimostrazione però della complessità della materia e di quanto la *data retention* non rappresentasse, quantomeno nei primi anni duemila, uno strumento prioritario per il Regno Unito, il primo CoP veniva approvato dal Parlamento solo nel novembre 2003, a distanza di quasi tre anni dall'entrata in vigore della normativa richiamata. Tale documento prevedeva un periodo di conser-

---

[2] Il *Secretary of State for the Home Department*, anche noto come *Home Secretary*, svolge sostanzialmente le funzioni attribuite al Ministro dell'Interno nell'ordinamento italiano: gestisce e controlla le attività svolte dalle autorità di *law enforcement* e di intelligence (in particolare il *National Security Council* e il *Military Intelligence*) e si occupa di tutte le questioni attinenti all'ordine pubblico.

[3] Viene tuttavia specificato come «A failure by any person to comply with a code of practice or agreement under this section which is for the time being in force shall not of itself render him liable to any criminal or civil proceedings», ATCSA, art. 102, para. 4.

vazione di dodici mesi per i dati relativi ai servizi telefonici, di sei mesi per SMS e dati telematici nonché quattro giorni per le attività svolte sul web – quali la cronologia dei siti visitati –, predisponendo inoltre forme di rimborso da parte del Governo dei costi sostenuti dagli operatori privati che si fossero impegnati alla conservazione.

Sotto il profilo della successiva acquisizione e trattamento dei metadati, invece, la disciplina era fornita dal *Regulation of Investigaroty Powers Act 2000* (RIPA): innanzitutto essa elencava espressamente i soggetti ai quali l'accesso era consentito, da individuarsi in «designated persons within relevant public authorities», tra cui, a titolo esemplificativo, la polizia, la *Serious Organised Crime Agency* e i servizi di intelligence; questi necessitavano comunque e sempre di una previa approvazione all'accesso da parte di un *Senior Officer*, con il limite però per le sole autorità locali di non poter accedere in nessun caso ai dati di traffico o di ubicazione bensì unicamente ai dati volti ad individuare l'utente – nome e indirizzo relativi ad una specifica utenza – o i numeri chiamati da un determinato soggetto. Venivano inoltre specificati gli scopi per i quali l'accesso poteva essere consentito, ovvero qualora i dati si fossero resi necessari «in the interests of national security; for the purpose of preventing or detecting crime or preventing disorder; in the interests of the economic well-being of the UK; in the interests of public safety; for the purpose of protecting public health; for the purpose of assessing or collecting any tax, duty or levy or other imposition, contribution or charge payable to a government department; for the purpose, in an emergency, of preventing death or injury or any damage to a persons physical or mental health», ma anche per scopi identificativi di vittime di reati o soggetti che avessero perso la memoria o incapaci di identificarsi per malattia, anche mentale. Sebbene una simile restrizione a finalità specifiche fosse volta a limitare l'ingerenza nella sfera privata rappresentata dalle operazioni di accesso a dati e metadati, l'elencazione promossa risultava nei fatti piuttosto ampia, nonché caratterizzata da voci facilmente interpretabili in maniera estensiva – basti pensare all'uso di termini vaghi quali *sicurezza nazionale*, *pubblica sicurezza* o *salute pubblica* –. Un controllo sulle attività di accesso ai metadati e sulla loro correttezza e legittimità veniva comunque affidato tanto al *In-*

terception of Communications Commissioner[4], cui veniva attribuito il ruolo di vigilare in maniera indipendente sull'attuazione dei poteri e doveri stabiliti nel RIPA, quanto all'*Investigatory Powers Tribunal* (IPT)[5].

Dalla ricostruzione sin qui svolta si può subito notare come inizialmente nessun obbligo di *data retention* fosse previsto dalla normativa del Regno Unito, neppure sulla base della facoltà concessa dall'art. 15 Direttiva *e-Privacy*; anche la disciplina sulla conservazione avente carattere unicamente volontario aveva poi incontrato significativi ritardi attuativi. Tale approccio pare sorprendente e singolare se lo si raffronta sia all'evoluzione normativa e alle strategie securitarie promosse dal Governo del Regno Unito nei decenni successivi, sia all'orientamento seguito, in quei medesimi anni, da altri Stati membri, quali il Belgio e l'Italia, che avevano attuato invece un regime obbligatorio di conservazione dei metadati.

L'approccio inglese avverso lo strumento della *data retention* subiva però un mutamento sostanziale a seguito tanto dei drammatici attentati terroristici di Londra del 2005, quanto dell'entrata in vigore della DRD, la cui adozione era stata peraltro fortemente sostenuta dal governo del Regno Unito. In adempimento a quanto stabilito da tale Direttiva, veniva quindi adottato, il 1 ottobre 2007, il *Data Retention (EC Directive) Regulations* che disciplinava però unicamente la conservazione di metadati derivanti da telecomunicazioni telefoniche: bisogna ricordare infatti che la DRD attribuiva agli Stati membri un termine più lungo – sino al 15 marzo 2009 – per trasporre gli obblighi attinenti ai metadati relativi alle comunicazioni telematiche. Tale disciplina veniva così inserita nel successivo *Data Retention (EC Directive) Regulations* del 6 aprile 2009, che sostituiva sia la previa normativa del 2007, sia il più risalente regime di carattere volontario previsto dal ATCSA del 2001.

---

[4] Questa figura, istituita dalla *Section 57* del RIPA e nominata direttamente dal *Prime Minister*, è stata successivamente sostituita dall'*Investigatory Powers Commissioner* con l'adozione del *Investigatory Powers Act 2016*, di cui si parlerà in seguito.

[5] «This Tribunal has full powers to investigate and decide any case within its jurisdiction, which includes the acquisition and disclosure of communications data under the Act. The Tribunal is made up of senior members of the judiciary and the legal profession and is independent of Government», SECRETARY OF STATE FOR THE HOME DEPARTMENT, *Protecting the Public in a changing communications environment*, 2009, p. 16.

Di conseguenza, come ben sottolineato da Walker, «between October 2007 and March 2009 the UK thus had a two-tier regime, with fixed and mobile data governed by the mandatory regime and Internet and email data by the voluntary code under ATCSA» [6], così che solo nel 2009 veniva introdotto per la prima volta Oltremanica un obbligo generalizzato di conservazione riguardante tutte le tipologie di metadati. Con una affermazione di grande impatto, l'allora *Secretary of State*, Jacqui Smith, aveva riconosciuto come «governed by a strict regulatory framework, communications data is routinely used to investigate terrorist plots, to bring to justice those guilty of serious crimes, to seize illegal drugs and to protect the vulnerable in our society. It is no exaggeration to say that information gathered in this way can mean the difference between life and death» [7]. Ciò a evidenziare un significativo cambio di approccio: a seguito dell'entrata in vigore della DRD e del determinarsi di un più marcato contesto emergenziale, anche il Regno Unito dimostrava di porre grande attenzione allo strumento della *bulk data retention* e alle sue significative potenzialità nella lotta al crimine e al terrorismo internazionale. La normativa del 2009 dunque stabiliva l'obbligo in capo a tutti i *communications providers* di conservare tutti i c.d. *communications data* [8] per un periodo di dodici mesi, senza alcuna differenziazione quanto alla tipologia dei metadati interessati. Era poi riconfermato il compito di controllo indipendente posto in capo all'*Interception of Communications Commissioner*, con riferimento alle attività svolte dalle autorità pubbliche, e al IPT con riguardo invece alle doglianze avanzate dai singoli utenti in caso di ritenuta violazione delle disposizioni del RIPA. A tale più risalente legislazione veniva effettuato rinvio per quanto concerneva la regolamentazione della fase di accesso, la cui disciplina dunque non conosceva mutamenti rispetto al passato.

L'introduzione di una forma di conservazione generalizzata ed indi-

---

[6] C. WALKER, *Data retention in the UK: pragmatic and proportionate or a step too far?*, in *Computer Law and Security Review*, 25, 2009, p. 326.

[7] SECRETARY OF STATE, *Protecting the Public in a changing communications environment*, cit., p. 2.

[8] Intesi come la totalità dei metadati prodotti dalle comunicazioni, ivi compresi i dati di traffico, i dati di ubicazione e le chiamate senza risposta.

scriminata non era però risultata esente da critiche e perplessità, soprattutto quanto alla proporzionalità di una misura così invasiva. Le posizioni emerse dal dibattito nazionale e dalla consultazione pubblica che aveva preceduto l'adozione della disciplina stessa, non si erano infatti rivelate pacificamente concordi e condivise: al contrario, mentre il Governo aveva presentato studi [9] volti a dimostrare la correttezza delle proprie scelte normative [10], confermando anche la proporzionalità e necessità della durata di conservazione fissa di un anno [11], numerose ONG attive nell'ambito della tutela dei diritti alla riservatezza e protezione dei dati avevano invece presentato opinioni e studi di segno avverso, secondo cui «practical experience indicates that most requests are for data of relatively recent origin, typically one to two months old» [12], rilevando così, anche sotto tale profilo, l'eccessiva lesione della sfera privata rispetto all'obiettivo perseguito. Critiche e riflessioni, queste, che avevano avviato sin dall'inizio un'acceso discussione sulla delicata disciplina della *data retention*, che vedrà, di lì a pochi anni, alcuni primi evidenti risultati concreti nei ricorsi promossi dinnanzi alle Corti nazionali e sovranazionali.

---

[9] Per una ampia analisi di tale documentazione, tra cui lo studio *Home Office consultation paper: 'Regulation of Investigatory Powers Act 2000: consolidating orders and codes of practice*, del 17 aprile 2009, si rimanda a C. WALKER, *Data retention in the UK: pragmatic and proportionate or a step too far?*, cit.

[10] Fondando i propri studi sulle informazioni derivanti dalla concreta pratica operativa delle autorità pubbliche, il Governo mirava così a supportare le proprie scelte e la proporzionalità delle disposizioni normative adottate: sulla base di tali analisi, «communications data is used as important evidence in 95% of serious crime cases and in almost all Security Service operations since 2004», secondo i dati riportati dall'allora *Home Secretary* Jacqui Smith, nel discorso tenuto presso l'*Institute for Public Policy Research Commission on National Security*, del 15 ottobre 2008, disponibile all'indirizzo http://press.homeoffice.gov.uk/Speeches/speech-to-ippr.

[11] Il Governo riteneva che la maggior parte dei casi per i quali i metadati si erano rivelati decisivi fossero «predominantly for long-running serious crime investigations, which without mandatory retention [of more than six months] is more at risk of deletion», HOME OFFICE, *Consultation Paper – Transposition of Directive 2006/24/EC*, agosto 2008, p. 10.

[12] È quanto riportato dall'esperto Peter Milford, nello studio *The retention of communications data: a view from industry*, in *Practical Law IP & IT*, 19 novembre 2008.

2.2. *Le rapide e dibattute reazioni del legislatore nazionale alla sentenza* DRI*: il* Data Retention and Investigatory Powers Act (DRIPA).

Le preoccupazioni e i dubbi relativi alla proporzionalità dello strumento della *data retention*, sopra richiamati, mostravano la loro fondatezza alla luce della sentenza *DRI* della CGUE. Dinnanzi ai dirompenti effetti di tale decisione che, pur riguardando specificamente la DRD, sanciva importanti principi anche per le discipline nazionali in materia di conservazione dei metadati, il Governo d'Oltremanica reputava necessario un intervento di adeguamento dell'assetto normativo esistente. Così, il Regno Unito risultava il primo Stato membro a dotarsi di una nuova normativa in materia di *data retention* in risposta all'intervento dei giudici di Lussemburgo [13]: se l'invalidazione della DRD risaliva infatti all'aprile 2014, la nuova normativa inglese in materia di conservazione dei metadati veniva adottata a soli pochi mesi di distanza, il 17 luglio 2014, con un percorso peraltro estremamente rapido che aveva portato all'approvazione del nuovo *Data Retention and Investigatory Powers Act* (DRIPA) a soli tre giorni dalla prima lettura in Parlamento, utilizzando la procedura di *emergency legislation*; tale scelta era stata motivata dall'esigenza di colmare con rapidità il vuoto lasciato dalla DRD e contenere le sue potenziali conseguenze, sebbene indirette, sulla disciplina nazionale di trasposizione, evitando eventuali e problematiche controversie aventi ad oggetto la legittimità delle prove derivanti da metadati conservati sulla base della previa normativa [14]. Una decisione, quella di affrettare i tempi e

[13] Il Belgio, ad esempio, aveva adottato il 29 maggio 2016 una nuova normativa in materia, finalizzata a 'correggere' ed adeguare il regime precedente alla giurisprudenza della CGUE. Il legislatore tedesco invece era intervenuta il 1 luglio 2017.

[14] Riconoscendo la necessità di un intervento a modifica della legislazione del 2009, nonché prendendo atto delle richieste pervenute dai fornitori di servizi di telecomunicazione, che chiedevano chiarezza quanto ai propri obblighi di conservazione dinnanzi alla invalidazione della normativa europea, l'*Home Office* aveva infatti affermato come «without this legislation, we face the very prospect of losing access to this data overnight, with the consequence that police investigations would suddenly go dark and criminals would escape justice. (…) We need to act immediately. If we do not, criminals and terrorists will go about their work unimpeded and innocent lives will be lost», HOUSE OF COMMONS, *Briefing Papers*, SN06934, 2014.

velocizzare l'iter approvativo, che aveva tuttavia destato non poche critiche e perplessità: la ONG The Law Society sosteneva, con toni accesi, come «the passage of DRIPA as emergency legislation was an affront to parliamentary sovereignty and the rule of law on the grounds that there was insufficient time for parliamentary scrutiny and debate and insufficient consideration of a relevant judgement of the CJEU» [15]. I dubbi espressi, oltre che al piano procedurale di approvazione della normativa, si estendevano però anche al contenuto stesso del DRIPA [16]. Quest'ulti-

[15] Come riportato da A. MUNIR, S. YASIN, S. BAKAR, *Data retention rules: a dead end*, in *European Data Protection Law Review*, 3, 2017, p. 76, facendo riferimento al documento redatto da *Law Society* dal titolo *Regulation of Investigatory Powers Act consultation: acquisition and disclosure of communications data and retention of communications data codes of practice: Law Society response*, 2015. Similmente, Zedner aveva sottolineato: «The exceptionally short timetable did not allow for the public consultation and debate that ordinarily precedes the legislative process. The usual rounds of prelegislative scrutiny were ruled out and the time available for parliamentary debate was so severely curtailed as to make review, amendment or opposition impossible. (…) Certainly no sufficiently grave emergency had arisen in July 2014 to justify overriding the ordinary legislative process. (…) The threat that companies would otherwise start deleting data, concern about the emergence of the so called "dark net" and fear of "safe spaces" in which terrorists communicate unmonitored, served to silence opposition and garner unusual all-party support», L. ZEDNER, *Why blanket surveillance is no security blanket. Data retention in the United Kingdom after the European Data Retention Directive*, in R.A. MILLER (a cura di), *Privacy and Power. A transatlantic dialogue in the shadow of the NSA-Affair*, Cambridge University Press, Cambridge, 2017, p. 565. Tale rapida procedura normativa era stata fortemente criticata anche da Boehm e Cole: «The bill was introduced just shortly before the summer recess and Members of Parliament did not have time to scrutinise the law in detail and propose possible changes. Due to the untypical emergency procedure, there was not much time for other critical voices to be heard», F. BOEHM, M. COLE, *Data retention after the judgement of the CJEU*, 2014.

[16] Diciotto Professori appartenenti a diverse Università del Regno Unito, con una *Open Letter* datata 14 luglio 2014, avevano messo in guardia il Parlamento quanto ai rischi derivanti dalla disciplina prevista nel DRIPA e all'impatto della stessa sui diritti fondamentali, auspicando un maggiore dibattito e una più cauta procedura legislativa: «DRIPA is far more than an administrative necessity; it is a serious expansion of the British surveillance state. We urge the British Government not to fast track this legislation and instead apply full and proper parliamentary scrutiny to ensure Parliamentarians are not mislead as to what powers this Bill truly contains», non mancando peraltro di sottolineare le criticità della normativa proposta rispetto ai criteri indicati dalla CGUE nel-

mo, riproponendo l'obbligo di conservazione, introduceva una sostanziale differenza rispetto al passato: anziché disporre una imposizione di carattere generale, veniva attribuito al *Secretary of State* il potere di ordinare ai fornitori di servizi di telecomunicazione, mediante una c.d. *retention notice*, la conservazione di determinate tipologie di metadati – anche la totalità di essi –, qualora ciò si rendesse necessario e proporzionato al raggiungimento di uno degli scopi specificati nel RIPA del 2000, che rimaneva ancora una volta la normativa di riferimento quanto alla disciplina dell'accesso. Rispetto alla precedente legislazione del 2009, inoltre, il periodo di *data retention* non era fissato a dodici mesi bensì poteva durare *al massimo* dodici mesi, prevedendo quindi la possibilità da parte del *Secretary of State* di stabilire un obbligo di durata inferiore laddove appropriato all'ottenimento dello scopo. Nelle disposizioni finali era stata inserita poi una *sunset clause*, una clausola di scadenza[17], nella quale si stabiliva il venir meno della validità della normativa il 31 dicembre 2016.

Ecco dunque che l'iniziale reazione del Regno Unito al primo decisivo intervento della CGUE in materia di conservazione dei metadati si presentava caratterizzata dalla predisposizione di nuove limitazioni e restrizioni, quali l'intervento del *Secretary of State* o la possibilità di modulare la durata della conservazione, accompagnate da ulteriori e più specifiche salvaguardie attinenti alla sicurezza dei dati conservati previste in maniera completa all'interno del *Data Retention Regulations 2014*, adottato sulla base del DRIPA. Così, come ritenuto da alcuni studiosi, «the concept of *retention notices* constitutes an approach worth considering»[18], ben potendo rappresentare una alternativa interessante ad un obbligo generalizzato di conservazione; nonostante questa innovazione di segno maggiormente garantista, tuttavia, l'ampiezza delle finalità per le quali l'ordine del *Secretary of State* poteva essere emanato, unitamente alla grande di-

---

la sentenza *DRI*. La lettera è reperibile all'indirizzo: https://paulbernal.wordpress.com/2014/07/15/open-letter-from-uk-legal-academic-experts-re-drip/.

[17] Per una ampia analisi di tale strumento, si rimanda a S. RANCHORDAS, *Constitutional sunsets and experimental legislation*, Elgar, Cheltenham, 2014.

[18] S. HEITZER, J. KULHING, *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in *European Law Review*, 2, 2015, p. 269.

screzionalità lasciata a tale soggetto quanto alla determinazione dei dati e dei servizi cui imporre la *data retention*, rendevano, secondo alcuni, il risultato finale non molto dissimile da quello della previa normativa del 2009: «to date, the UK legislature has not gone far enough in limiting the retention of data to very specific objects of public safety and security, as required by the more convincing narrow understanding of the ECJ decision» [19]. Con riferimento alla disciplina dell'accesso, poi, non erano stati introdotti mutamenti sostanziali al RIPA, che non veniva dunque adeguato ai precisi criteri indicati dai giudici di Lussemburgo, quali il previo controllo da parte di un giudice o di una autorità amministrativa indipendente – un vaglio preventiva era infatti svolto solamente da *Senior Officers* che non potevano però essere considerati organi "indipendenti" dal potere esecutivo – o ancora la determinazione di specifici reati gravi limitatamente ai quali le operazioni di accesso erano consentite.

2.3. *L'adozione dell'*Investigatory Powers Act *(IPA) nelle more del caso* Tele2.

Il mancato corretto inserimento della totalità degli importanti requisiti stabiliti nella pronuncia *DRI* all'interno della nuova disciplina normativa inglese non erano sfuggiti a critiche e preoccupazioni da parte di società civile e ONG [20]. Non stupisce dunque che i cittadini Brice, Lewis,

---

[19] S. HEITZER, J. KULHING, *Returning through the national back door?*, cit., p. 269.

[20] Si leggano sul punto le forti critiche mosse da Bunyan, all'epoca direttore della ONG Statewatch, reperibili in T. BUNYAN, *Analysis mass surveillance of communications in the EU: CJEU Judgement and DRIPA 2014/RIPA 2000 in the UK*, Statewatch, 2014, https://www.statewatch.org/media/documents/analyses/no-252-mand-ret-dripa-ripa.pdf. Come sottolineato da Vainio, poi, «The new law was basically an attempt to maintain data retention, just under a different name. The system enacted by the new law is similar to the one that was implemented under the Directive, except that it does not use the same language as in the Directive. (…) According to critics, DRIPA actually went further than merely maintaining the data retention regime and fails to meet the requirements of the CJEU judgment. The civil rights organisation Liberty used strong language in its critique of the bill—according to Liberty, the bill "doesn't even pretend to comply with the CJEU judgment"», N. VAINIO, *Fundamental rights compliance and the politics of interpretation: explaining Member State and Court reactions to Digital Rights*

Davis e Watson (questi ultimi due anche membri della *House of Commons*) avessero deciso di presentare nel 2015 ricorso dinnanzi alla *High Court of Justice, Divisional Court*, al fine di accertare la compatibilità con gli artt. 7 e 8 della Carta di Nizza e con l'art. 8 della CEDU del regime di conservazione dei metadati disciplinato dal DRIPA. La decisione che ne era derivata, successivamente impugnata dinnanzi alla *Court of Appeal*, aveva dato origine al fondamentale rinvio pregiudiziale alla CGUE, fonte della sentenza *Tele2*. Sebbene l'analisi di tale primo articolato intervento giurisprudenziale occuperà il prossimo paragrafo, ciò che qui merita rilevare è, ancora una volta, il "tempismo" del legislatore inglese: mentre ancora pendeva il rinvio pregiudiziale *Tele2*, che avrebbe chiarito l'impatto e l'estensione della decisione *DRI* rispetto alle normative nazionali in materia di conservazione e accesso ai metadati, nonché la sua incidenza rispetto alla facoltà prevista dall'art. 15 Direttiva *e-Privacy*, il legislatore d'Oltremanica si trovava dinnanzi all'imminente scadenza della validità del DRIPA, la cui vigenza era per legge stata limitata, come si è detto, sino al 31 dicembre 2016; anche per tale motivo e senza potersi dunque basare sulle considerazioni finali della CGUE, bensì solo su quelle espresse dall'Avvocato generale nelle sue Conclusioni, il legislatore inglese decideva di non optare per una proroga della validità del DRIPA, che gli avrebbe concesso di poter meglio strutturare una nuova normativa conforme alla più aggiornata giurisprudenza europea, bensì di adottare direttamente una nuova legge deputata a regolare tale delicata materia: l'*Investigatory Powers Act* (IPA), che riceveva il *Royal Assent* il 29 novembre 2016, entrando in vigore il 30 dicembre 2016.

Ebbene, in tale normativa erano stati sostanzialmente mantenuti i tratti fondamentali che già caratterizzavano il DRIPA, pur predisponendo un testo maggiormente comprensivo, completo e dettagliato, composto da ben 272 articoli. La *Section 87*, riguardante la *data retention*, attribuiva nuovamente in capo al *Secretary of State* non solo il potere di richiedere ai fornitori di servizi di telecomunicazione la conservazione di metadati per un periodo massimo di dodici mesi, bensì anche la facoltà di emanare *bulk acquisition warrants* in grado di consentire l'acquisizione

---

Ireland, in T. BRAUTIGAM, S. MIETTINEN (a cura di), *Data protection, privacy and European regulation in the digital age*, Unigrafia, Helsinki, 2016, p. 238.

della generalità dei metadati conservati dagli operatori, a favore però delle sole agenzie di intelligence, che avrebbero poi potuto svolgere operazioni di controllo automatizzato dei dati (*Section 136*). Entrambe le decisioni emanate dal *Secretary of State* dovevano tuttavia essere approvate da un *Judicial Commissioner*[21], cui era assegnato il compito di effettuare un vaglio sulla proporzionalità e necessità delle misure richieste, nonché sul rispetto dei diritti fondamentali alla riservatezza e alla protezione dei dati. Nonostante l'importanza di questa innovativa e ulteriore salvaguardia, denominata *double lock system*[22], non veniva però introdotta nessuna forma di *targeted data retention* sulla base di criteri geografici o soggettivi, come suggerito dalla giurisprudenza europea. Similmente, sul fronte dell'accesso ai metadati, non si registrava l'approvazione di disposizioni pienamente conformi ai criteri ribaditi nella sentenza *Tele2*: la *Section 61*, infatti, consentiva l'accesso ai metadati ad un elenco predefinito ma ampio di autorità pubbliche, senza prevedere un previo controllo da parte di un giudice o di una autorità indipendente. Era tuttavia inserita, nella *Section 67*, la possibilità, per i *Senior Officers*, di stabilire dei c.d. *filtering arrangements* relativi all'accesso: «such arrangements could be seen as forms of internal authorisation, but they aim to establish safeguards against abuse and minimise the volume of metadata accessed»[23]. Questi *arrangements*, dunque, potevano specificare i soggetti autorizzati a svolgere

[21] Agli artt. 227 e 228 venivano indicate le modalità di nomina e le caratteristiche che tale soggetto doveva possedere. In termini generali, i *Judicial Commissioners*, nominati dal Primo Ministro, potevano essere «a serving or retired member of the senior judiciary in the UK. JCs provide independent authorisation of applications for the use of certain investigatory powers. The Investigatory Powers Act sets out that a JC must hold or have held a high judicial office», secondo la definizione fornita nel sito dell'*Investigatory Powers Commissioner's Office*, all'indirizzo https://www.ipco.org.uk/default.aspx?mid=21.19.

[22] Secondo Theresa May – *Home Secretary* al momento della presentazione del *Draft Investigatory Powers Bill* e Primo Ministro all'epoca della entrata in vigore di tale normativa – tale disciplina rappresentava «one of the strongest authorisation regimes anywhere in the world» (discorso di Theresa May del 4 novembre 2015, reperibile sul sito www.gov.uk/government/speeches/home-secretary-publication-of-draft-investigatory-powers-bill).

[23] W.R. MBIOH, *Post-Och Telestyrelsen and Watson and the Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017, p. 279.

l'accesso, i parametri da impiegare per porre in essere operazioni di filtraggio e analisi automatizzata dei metadati, nonché disciplinare le condizioni di conservazione o cancellazione dei risultati delle operazioni di filtraggio, quando non più necessari per finalità di indagine. Prima dell'accesso, inoltre, i *Senior Officers* erano generalmente chiamati a confrontarsi con i *Single Points of Contacts*, cioè funzionari pubblici cui era specificamente assegnato il compito di verificare la legittimità, necessità e proporzionalità delle operazioni di accesso. Nessuna restrizione era stata inserita poi quanto alle finalità dell'accesso e, in particolare, alla gravità dei reati da perseguire e per i quali l'accesso poteva essere richiesto: gli scopi restavano infatti ampi, andando dal «purpose of preventing or detecting crime or of preventing disorder», al «purposes of protecting public health», ad «assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a Government Department», art. 61. Sebbene, come noto, la CGUE non avesse fornito un elenco di reati da considerarsi gravi o di criteri volti a definire la serietà di un reato, nondimeno essa aveva sempre richiamato crimini quali il terrorismo o la criminalità organizzata, così che le finalità delineate dall'IPA risultavano piuttosto ampie e generiche e non sempre in grado di riflettere pienamente quel carattere di gravità cui la giurisprudenza europea faceva e fa tuttora riferimento [24].

Infine, sotto il profilo dei rimedi, l'IPA, oltre a ribadire il ruolo attribuito all'apposito IPT [25], aveva anche assegnato al *Investigatory Powers*

---

[24] Si pensi allo scopo di *collecting tax* che non pare paragonabile alla repressione del terrorismo indicata quale reato grave a titolo esemplificativo dai giudici di Lussemburgo.

[25] Sul punto, l'IPA introduceva comunque una rilevante novità, prevedendo per la prima volta la possibilità di promuovere appello alla *Court of Appeal* o alla *Court of Session* avverso le decisioni dell'IPT, che non risultavano invece precedentemente impugnabili dinnanzi a nessun giudice. Tale importante possibilità veniva tuttavia sottoposta a restrittive condizioni: «An appeal under this section: (a) is to be heard by the relevant appellate court, but (b) may not be made without the leave of the Tribunal or, if that is refused, of the relevant appellate court. The Tribunal or relevant appellate court must not grant leave to appeal unless it considers that— (a) the appeal would raise an important point of principle or practice, or (b) there is another compelling reason for granting leave», art. 242. Tali requisiti sono stati oggetto di critiche, anche in fase di consultazione, in quanto ritenuti eccessivamente restrittivi e passibili di divenire un vero e proprio ostacolo alla efficacia di tale rimedio.

Commissioner non solo il compito di controllare il corretto impiego da parte delle autorità pubbliche dei poteri di sorveglianza, operando unitamente ai *Judicial Commissioners*, bensì anche il potere di informare gli utenti nel caso in cui si fosse verificato un «serious error» nello svolgimento delle operazioni di conservazione, accesso e trattamento dei dati e solo nel caso in cui «it is in the public interest for the person to be informed of the error», art. 231. Sul fronte poi della sicurezza dei metadati conservati, nulla veniva specificato quanto all'obbligo di limitare la *data retention* al territorio dell'UE.

Il quadro che risulta dall'analisi delle principali caratteristiche del IPA aiuta a comprendere le ragioni dei dubbi e delle critiche manifestate già all'indomani della adozione della nuova normativa: con riferimento, ad esempio, al ruolo dei *Judicial Commissioners* l'indipendenza e il rigore dei controlli da essi effettuati risultavano in gran parte dipendenti «on the personality of the Commissioner, as well as on the information to which they have access. Furthermore, while a Judicial Commissioner should have regard to privacy rights, they must not act in a way "contrary to the public interest or prejudicial to national security, the prevention or detection of serious crime or the economic well-being of the UK". These limitations (…) may limit the Judicial Commissioners'effectiveness» [26]. Anche il meccanismo di controllo in materia di accesso aveva posto serie perplessità sotto il profilo della sua reale efficacia: alcuni autori avevano sul punto evidenziato come un vero e proprio «external check» non fosse individuabile nel ruolo assegnato ai *Single Points of Contact*; questi ultimi infatti erano composti da funzionari appartenenti ad autorità pubbliche e sottoposti gerarchicamente ai *Senior Officers* con i quali erano chiamati a collaborare, così che una loro qualifica come organi indipendenti pareva da escludersi [27]. Una ulteriore critica veniva poi mossa con riferimento

[26] L. WOODS, *The Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017, p. 104. L'autrice inoltre rilevava come il vaglio effettuato da tale autorità fosse fondato solo sulle considerazioni conclusive redatte dal *Secretary of State*: la profondità e dunque l'efficacia stessa del controllo erano strettamente dipendenti dalla quantità e dalla precisione delle informazioni messe a disposizione del *Judicial Commissioner*.

[27] L. WOODS, *The Investigatory Powers Act 2016*, cit., p. 104.

alla facoltà assegnata all'*Investigatory Powers Commissioner* di informare gli utenti non quanto all'avvenuto accesso bensì unicamente in caso di errori nel trattamento dei metadati: «this obligation is very limited, applying only where there is a serious error which has caused significant prejudice or harm to the person concerned and it is in the public interest for the person to be informed» [28]; in questo senso, se è vero che veniva concessa al ricorrente la possibilità di adire l'*Investigatory Powers Tribunal* anche in assenza della prova di essere stato assoggettato a forme di sorveglianza, questa opportunità non sembrava sufficiente a sopperire alla mancanza di informazioni dirette ed esplicite circa l'avvenuto trattamento dei propri metadati: in altre parole, è più difficile che un utente si attivi dinnanzi all'IPT laddove non gli venga concesso di sapere se e in quali modalità i propri dati siano stati oggetto di controllo da parte di autorità pubbliche. Pur non costituendo quindi un ostacolo in termini assoluti all'accesso a rimedi giurisdizionali, le restrittive condizioni di attuazione dell'obbligo di notifica finivano col rappresentare una forte limitazione dell'utilità del potere assegnato all'*Investigatory Powers Commissioner*.

La possibilità della riproposizione di un sistema di *bulk data retention* restava, infine, uno dei profili maggiormente problematici e dibattuti: secondo taluni infatti permaneva in capo al *Secretary of State* l'opportunità di emanare *retention notices* di carattere generalizzato o comunque estremamente ampio: «to make the IPA acceptable, the retention notices would need to relate to specific investigations, rather than be general in scope» [29]; solo una forma di conservazione mirata, che pure non era stata prevista, avrebbe dunque potuto limitare il potere altamente discrezionale e vasto lasciato al *Secretary of State* nella determinazione dei confini e del contenuto del *retention notice*. Nonostante quindi l'IPA avesse portato da

---

[28] L. WOODS, *The Investigatory Powers Act 2016*, cit., p. 104.

[29] L. WOODS, *The Investigatory Powers Act 2016*, cit., p. 105. Similmente White sosteneva che l'unico modo per rendere legittimo il sistema di conservazione previsto dal IPA fosse quello di far sì che «retention notices or obligations must be used for a specific purpose, not as a general fishing exercise to bring in information, based on verifiable reasonable suspicion that is necessary and proportionate», M. WHITE, *Protection by judicial oversight or an oversight in protection?*, in *Journal of Information Rights, Policy and Practice*, 2, 2017, p. 41.

un lato a profondi miglioramenti, quali «sicuro portato delle maggiori garanzie richieste in questi processi di sorveglianza massiva, dall'altro [tale normativa] presenta[va] alcune disposizioni che ancora non soddisfa[va]no i criteri posti dalla Corte di giustizia» [30].

2.4. *Le modifiche alla disciplina nazionale apportate dal* Data Retention and Acquisition Regulations 2018.

Alla luce delle riflessioni e delle criticità rilevate, il dibattito sulla disciplina della *data retention* non aveva trovato una conclusione definitiva neppure con l'adozione dell'IPA. Al contrario, le debolezze che avevano caratterizzato tale normativa sin dalla sua origine si erano successivamente accentuate a causa dei rilevanti sviluppi giurisprudenziali in materia, registratisi a livello tanto europeo quanto nazionale: il 21 dicembre 2016 era stata infatti pubblicata l'attesa sentenza *Tele2* che aveva subito prodotto un forte impatto sulla discussione interna relativa alla compatibilità del regime nazionale con il diritto dell'UE. Proprio la richiamata sopravvenuta pronuncia dei giudici di Lussemburgo, giunta a pochissima distanza di tempo dall'approvazione dell'IPA, aveva stimolato non solo la presentazione di numerosi ricorsi da parte di cittadini e ONG dinnanzi alle autorità giudiziarie del Regno Unito, aventi proprio ad oggetto le disposizioni dell'IPA, ma anche un significativo intervento da parte del legislatore che aveva deciso di avviare, nuovamente, un percorso di riforma dell'assetto normativo esistente, riconoscendone i limiti e le criticità alla luce dei principi stabiliti dalla CGUE. Ne è riprova la consultazione pubblica avviata dal Governo il 30 novembre 2017, a meno di un anno dall'entrata in vigore dell'IPA e dalla sentenza *Tele2*: in tale consultazione emergeva con chiarezza come «the Government considers that some aspects of our current regime for the retention of and access to communications data do not satisfy the requirements of the CJEU's judgement» [31], cogliendo quindi la necessità di svolgere una dettagliata analisi

[30] L. SCAFFARDI, *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016: una legge per il futuro troppo legata al passato*, in *Quaderni costituzionali*, 2, 2017, p. 414.

[31] Così si legge nel documento redatto dal *Home Office* nel novembre 2017, titolato

dell'impatto della decisione *Tele2* rispetto alla disciplina all'epoca vigente e aprendo ad una valutazione approfondita circa la concreta fattibilità e applicabilità dei criteri indicati dai giudici di Lussemburgo.

Il processo di modifica e di riflessione promosso dal Governo subiva poi una significativa accelerazione grazie all'intervento della *High Court*: quest'ultima, a seguito di taluni ricorsi volti ad accertare la conformità dell'IPA al diritto dell'UE, aveva dichiarato, il 27 aprile 2018, l'incompatibilità di alcune sezioni del IPA (*Part 3, 4*), nonché di alcune disposizioni del RIPA nella parte attinente all'accesso ai metadati (*Chapter 2*, *Part 1*). Ne derivava, come si analizzerà meglio nel prosieguo di questo Capitolo, la richiesta rivolta al legislatore di emendare entro il 1 novembre 2018 le disposizioni interessate dalla pronuncia.

L'ultima modifica apportata all'IPA è stata così approvata il 31 ottobre 2018, mediante il *Data Retention and Acquisition Regulations 2018*, che ha introdotto notevoli innovazioni al testo normativo originario. Innanzitutto merita rilevare come le disposizioni in materia di accesso e acquisizione dei dati contenute nel RIPA del 2000, cui l'IPA faceva riferimento, siano state interamente sostituite. Sotto tale profilo, i principali aspetti sui quali il legislatore è intervenuto sono da individuarsi nella predisposizione di una soglia di gravità dei reati per i quali l'accesso è consentito, nonché nella determinazione di una previa autorizzazione all'accesso ai metadati predisposta da una autorità indipendente. Quanto a quest'ultimo profilo, tale potere è stato attribuito all'*Investigatory Powers Commissioner*, che può inoltre delegare la funzione ad un apposito ufficio, denominato *Office for Communications Data Authorisations* (OCDA): come si legge nell'*Explanatory Memorandum*, il «OCDA will report directly to the IPC, and will be responsible for considering the vast majority of requests to access communications data made by public authorities» [32]. È stata inoltre prevista, in casi di particolare urgenza, una procedura più snella e rapida, fondata cioè su un sistema di «internal authorisation by designated senior officer in a public authority», ad esclusione delle *local*

Consultation on the Government's proposed response to the ruling of the Court of Justice of the EU on 21 December 2016 regarding the retention of communications data.

[32] Documento redatto dal *Home Office* nel 2018, titolato *Explanatory memorandum to "The data retention and acquisition Regulations 2018"*, p. 4.

authorities, alle quali tale prerogativa non viene invece concessa. Viene poi effettuata una significativa modifica quanto alle finalità per le quali l'accesso viene autorizzato: mentre prima era effettuato un generico riferimento al «purpose of preventing or detecting crime or of preventing disorder», ora viene invece specificato che l'analisi di metadati può avvenire solo per scopi di lotta alla criminalità di carattere grave («the purpose of preventing or detecting serious crime», art. 60A, *Subsection 8*). Tale gravità viene identificata in «all offences for which an adult is capable of being sentenced to twelve months or more in prison, any offence involving violence, any offence which involves a large number of people acting in pursuit of a common purpose, any offence committed by a body corporate, any offence which involves the sending of a communication or a breach of privacy, or any offence involving a significant financial gain» [33]. Sempre allo scopo di limitare e rendere sempre più proporzionata l'ingerenza nella sfera privata, sono state eliminate alcune delle generiche e vaste finalità autorizzative dell'accesso, precedentemente previste nel RIPA ed oggetto, sin dall'inizio, di forti critiche legate proprio all'ampiezza ed indeterminatezza dei termini [34].

Una rilevante modifica ha poi interessato anche la disciplina della conservazione dei dati: sono stati infatti meglio precisati i criteri che il *Secretary of State* è chiamato a valutare nel momento in cui deve considerare l'opportunità e il contenuto di un *retention notice*. Vengono così specificati importanti fattori da considerare, quali la possibilità di restringere l'ordine di conservazione a determinate aree geografiche o di escludere gruppi di utenti, nonché la necessità di operare una chiara e puntuale indicazione dei servizi e degli operatori cui la conservazione deve riferirsi. Sulla base di queste specificazioni e condizioni introdotte dalla nuova normativa, il Governo ha affermato con decisione che «considering the necessity and proportionality considerations that must be taken into account, and the resulting practical effect of the regime to limit data reten-

[33] HOME OFFICE, *Explanatory memorandum*, cit., p. 4.

[34] Si tratta degli scopi di «public health; collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; exercising functions relating to the regulation of financial services and markets, or financial stability», previamente previsti dal RIPA.

tion by telecommunications operators or postal operators, services and data types, we do not consider that the existing data retention regime is general and indiscriminate» [35]. In queste parole è certamente da rilevare lo sforzo del legislatore di proporre innovazioni in senso restrittivo quanto alla disciplina della *data retention*, capaci di delimitare con maggior chiarezza e trasparenza la discrezionalità attribuita al *Secretary of State* nel suo delicato compito di emanazione dei *retention notice*. Se tale sforzo sia sufficiente per ritenere la disciplina esaminata e tuttora vigente come conforme ai principi delineati dalla CGUE e ulteriormente definiti nelle pronunce *La Quadrature du Net* e *Privacy International* dell'ottobre 2020, rimane però un profilo ancora dibattuto e meritevole di attenzione. Prima di addivenire a più specifiche riflessioni sui possibili sviluppi della disciplina normativa inglese, risulta necessario ricostruire le vicende giurisprudenziali al fine di offrire un quadro completo delle complesse questioni che hanno caratterizzato e che tutt'ora caratterizzano la regolamentazione della *data retention* nel Regno Unito.

3. *Le Corti inglesi e i principi delineati dalla giurisprudenza sovranazionale, tra divergenze e avvicinamenti.*

3.1. *La decisione della* High Court *in merito alla compatibilità del DRIPA con il diritto dell'UE.*

La giurisprudenza delle Corti inglesi in materia di *data retention* e accesso ai metadati è vasta ed articolata, resa complessa sia dal continuo intreccio con le pronunce della Corte EDU e della CGUE, sia dal rapido avvicendarsi di interventi di riforma della disciplina normativa, non sempre coordinati e conformi ai principi stabiliti dalla giurisprudenza nazionale e sovranazionale. Tutti questi elementi hanno fortemente inciso sull'orientamento seguito dalle Corti inglesi, caratterizzato da una lenta ma significativa evoluzione nel corso del tempo: se da un lato, infatti, si è as-

[35] HOME OFFICE, *Consultation on the Government's proposed response to the ruling of the Court of Justice of the EU on 21 December 2016 regarding the retention of communications data*, cit., p. 14.

sistito ad una sempre maggiore attenzione ed attuazione dei c.d. criteri *Tele2*, dall'altro i giudici nazionali non hanno mancato di mettere in discussione alcuni dei rilievi svolti dalla CGUE o di proporne una interpretazione elastica, chiedendo anche l'intervento chiarificatore dei giudici di Lussemburgo al fine di meglio delineare i confini e l'ambito di applicazione del diritto dell'UE.

Procedendo cronologicamente, prima rilevante tappa di questo percorso evolutivo, nonché "motore propulsivo" dell'iniziale momento di dialogo con la CGUE, è da individuarsi nel richiamato ricorso promosso dinnanzi alla *High Court* da alcuni cittadini inglesi: Brice, Lewis, Davis e Watson – poi sostenuti dalle ONG Open Rights Group, Privacy International e The Law Society –, fondando le proprie posizioni sui principi delineati dalla giurisprudenza della CGUE nella sentenza *DRI*, avevano richiesto ai giudici di dichiarare il regime nazionale di *data retention* e accesso ai metadati non conforme al diritto dell'UE [36]. Con sentenza del 17 luglio 2015 [37], la Corte concludeva a favore dei ricorrenti, ritenendo la *Section 1* del DRIPA incompatibile con i requisiti fissati all'art. 15 della Direttiva *e-Privacy*, nella misura in cui non venivano previste regole chiare e precise a disciplina dell'accesso ai metadati, non si limitava lo scopo dell'accesso e dell'ordine di conservazione al solo perseguimento di reati gravi e non veniva stabilito un controllo preventivo da parte di una Corte o di un'autorità amministrativa indipendente. Sebbene queste considerazioni avessero portato a ritenere tale pronuncia una vittoria significativa

[36] Come ben specificato anche dalla *High Court*, «at common law, Acts of the UK Parliament are not open to challenge in the Courts. But the position under EU law is different. Decisions of the CJEU as to what EU law is, are binding on the legislatures and Court of all Member States», para. 4. In tal senso, dunque, la controversia era attinente alla compatibilità della normativa interna rispetto ai diritti tutelati agli artt. 7 e 8 della Carta di Nizza, come interpretati dalla CGUE. Partendo poi dal presupposto secondo cui la Carta di Nizza vincolava gli Stati membri solo in caso di implementazione del diritto dell'UE, il giudice inglese aveva sin da subito chiarito come la normativa nazionale dovesse essere considerata rientrante nell'ambito di applicazione del diritto dell'UE, essendo attinente alla materia della protezione dei dati.

[37] *David Davis, Tom Watson, Peter Brice, Geoffrey Lewis v. The Secretary of State for the Home Department*, [2015] EWHC 2092, Case no. CO/3665/2014; CO/3667/2014; CO/3794/2014.

per i diritti alla riservatezza e alla protezione dei dati, uno sguardo più attento deve indurre, al contrario, a ridimensionare tale ottimistica visione. La *Divisional Court*, infatti, non era giunta – come invece aveva fatto la Corte costituzionale belga di cui si parlerà nel successivo Capitolo – ad affermare l'incompatibilità col diritto dell'UE e con la Carta di Nizza di una forma di conservazione generalizzata ed indiscriminata quale quella prevista dal DRIPA. La motivazione di una tale posizione non era da rinvenirsi solo nelle peculiarità della normativa esaminata: certo, quest'ultima, diversamente dalle discipline adottate da altri Stati membri, non prevedeva direttamente un obbligo di conservazione in capo a tutti i fornitori di servizi di telecomunicazione bensì stabiliva tale imposizione solo a seguito di un *retention notice* emanato dal *Secretary of State*, il quale poteva quindi disporre una *data retention* limitata solo ad alcuni fornitori, tipologie di metadati o utenti; nonostante queste considerazioni, la Corte stessa riconosceva come l'ordine di conservazione ben potesse assumere un carattere di generalità ed indeterminatezza, coinvolgendo la totalità degli utenti, dei metadati e dei *service providers*: «we should test the validity of DRIPA on the assumption that the retention notices issued under it may be as broad in scope as the statute permits, namely a direction to each communications service provider (CSP) to retain all communications data for a period of 12 months. (…) We shall refer in this judgment to a system under which the State may require CSPs to retain all communications data for a period as a general retention regime», para. 65.

Pur affermando dunque il potenziale carattere indiscriminato del regime di *data retention* nazionale [38], la *High Court* proseguiva però fornendo una lettura della sentenza *DRI* piuttosto restrittiva, che ne circoscriveva significativamente la portata con riferimento alla disciplina della conservazione dei metadati: secondo i giudici inglesi, infatti, la CGUE «was not indicating that communications data can only be retained if they relate to particular geographical areas, or to a particular individuals likely to be involved in serious crime. It was identifying the width of the Directive [DRD], which imposed no limits on the power to retain», para. 85. Ne derivava, significativamente, che «the solution to the conundrum,

[38] Per una ricostruzione dei punti fondamentali di tale pronuncia, si rimanda a M. SENOR, *Un altro 'tango down' in tema di data retention*, in *MediaLaws*, 22 luglio 2015.

in our view, is that the legislation establishing a general retention regime for communications data infringes rights under Articles 7 and 8 of the EU Charter *unless* it is accompanied by an access regime (laid down at national level) which provides adequate safeguards for those rights», para. 89. Una posizione, questa, di estremo rilievo, che sarà determinante per comprendere l'approccio dei giudici inglesi alla giurisprudenza della CGUE: non veniva cioè riconosciuta nella sentenza *DRI* una dichiarazione di incompatibilità assoluta di forme di conservazione generalizzata rispetto al diritto dell'UE e il ricorso ad una *targeted data retention* rappresentava solo una – e non l'unica – delle possibili soluzioni da adottare; in altre parole, un regime di conservazione risultava legittimo anche qualora generalizzato purché la normativa in materia fosse in grado di stabilire adeguate salvaguardie nella fase di accesso. Ed è proprio unicamente sotto tale ultimo profilo che il DRIPA veniva considerato incompatibile con il diritto dell'UE.

Una simile interpretazione dei principi stabiliti dalla CGUE – che non aveva mancato di sollevare sin da subito alcune perplessità [39] – risultava agli occhi dei giudici inglesi assolutamente coerente, tanto da giustificare il respingimento della richiesta dei ricorrenti di provvedere ad un rinvio pregiudiziale alla CGUE volto a chiarire taluni aspetti della pronuncia *DRI* ritenuti dibattuti ed oggetto di differenti e opposte visioni. Pur prendendo atto del rinvio pregiudiziale nel frattempo promosso dalla Corte amministrativa svedese nel caso *Tele2* (C-203/2015), nonché riconoscendo che le Corti costituzionali di tre Stati membri (Slovenia, Romania e Belgio) avevano già all'epoca dichiarato l'invalidità della normativa nazionale a seguito della sentenza *DRI* basandosi anche sulla valutazione delle criticità che il carattere generalizzato della conservazione comportava, la *High Court* aveva comunque reputato inopportuno richiedere l'intervento della CGUE [40].

---

[39] Secondo Woods questa pronuncia «seems to downplay the extent of the concerns the ECJ expressed about data retention as well as the concerns of the Advocate General as to the complete and accurate picture of users being created», L. WOODS, *High Court strikes down data retention laws in ruling on DRIPA*, in *European Data Protection Law Review*, 3, 2015, p. 239.

[40] Ciò sia perché i criteri delineati nella pronuncia *DRI* risultavano totalmente chiari, sia perché le conclusioni cui i giudici di Lussemburgo erano giunti non dovevano essere

Sulla base delle considerazioni richiamate, dunque, i giudici inglesi giungevano a dichiarare un ordine di disapplicazione della *Section 1* del DRIPA poiché incompatibile con il diritto dell'UE; tale ordine tuttavia risultava sospeso sino al 31 marzo 2016, allo scopo di fornire un adeguato intervallo di tempo al legislatore per poterne correggere gli aspetti problematici, senza creare pericolosi vuoti normativi in un settore estremamente delicato e dagli impatti determinanti per la garanzia della sicurezza [41].

3.2. *La diversa lettura fornita dalla* Court of Appeal: *i motivi del primo rinvio pregiudiziale ai giudici di Lussemburgo.*

Dinnanzi alla decisione della *High Court*, tuttavia, il *Secretary of State* decideva di proporre appello dinnanzi alla *Court of Appeal*, ritenendo erronea la lettura della giurisprudenza della CGUE fornita dai giudici di primo grado. Secondo l'appellante, infatti, i requisiti fissati dai giudici di Lussemburgo, relativi tanto alla disciplina della conservazione quanto a quella dell'accesso, erano da ritenersi meramente «descriptive and not prescriptive» [42], oltre a non essere automaticamente applicabili nella valu-

---

necessariamente le stesse cui i giudici nazionali dovevano pervenire, essendo questi ultimi chiamati a valutare normative nazionali, ciascuna differente e con le proprie peculiarità rispetto alla DRD. Infine il rinvio pregiudiziale veniva escluso anche sulla base del fatto che il DRIPA prevedeva una *sunset clause* tale da rendere concretamente inutile una pronuncia della CGUE: «the CJEU typically takes two years or more to answer to a question referred to it for a preliminary ruling. It is most unlikely that an answer to a reference made now would be received before DRIPA has expired, or has been repealed and replaced by a new statute. Either way, the answer would have become academic», para. 113.

[41] La motivazione espressa dalla *High Court* a giustificazione del prolungato lasso di tempo concesso al Parlamento per addivenire ad una modifica della normativa esistente, dimostrava una certa consapevolezza della complessità della materia, giungendo a mettere in guardia il legislatore quanto ai pericoli di una normativa adottata in maniera troppo affrettata – come accaduto per il DRIPA –: «The Court do not presume to tell Parliament for how long and in what detail Bills should be scrutinised, but it is right to say (to put it no higher) that legislation enacted in haste is more prone to error, and it would be highly desirable to allow the opportunity of thorough scrutiny in both Houses», para. 121.

[42] Secondo il *Secretary of State*, infatti, «The CJEU in *DRI* did not impose mandatory requirements which must to be applied to national legislation. It simply held that the

tazione della conformità al diritto dell'UE di una normativa nazionale.

Ebbene, con una fondamentale sentenza del 20 novembre 2015 [43], la *Court of Appeal* ribaltava la posizione espressa dalla Corte di primo grado, accogliendo gran parte delle osservazioni mosse dal Governo. Secondo i giudici di seconda istanza, infatti, la sentenza *DRI* non escludeva totalmente la possibilità di ricorrere a regimi di conservazione generalizzata né obbligava gli Stati membri ad adottare discipline che limitassero l'accesso alla sola finalità di lotta alla criminalità grave; una diversa e più restrittiva interpretazione avrebbe contrastato con l'ampia discrezionalità garantita ai legislatori nazionali dall'art. 15 della Direttiva *e-Privacy* nonché con lo stesso dettato della invalidata DRD che lasciava chiaramente in capo ai legislatori nazionali il compito di determinare la disciplina dell'accesso. Per questo motivo, i giudici di seconda istanza affermavano che nella sentenza *DRI* «the ECJ was not laying down specific mandatory requirements of EU law but was simply identifying and describing protections that were entirely absent from the harmonised EU regime. The Court's conclusion that the DRD was unlawful was compelled by the cumulative effect of what was not in the DRD», para. 73 [44].

La posizione della *Court of Appeal* dunque divergeva nettamente da quanto sostenuto dalla *High Court*: ed è proprio sulla base di questa riconosciuta divergenza interpretativa che i giudici dell'appello decidevano di promuovere

---

harmonized EU scheme for data retention failed to incorporate any safeguards and therefore was not compliant with EU fundamental rights. (…) The EU Charter does not apply to national rules concerning access by law enforcement bodies to communications data. The judgement cannot, therefore, be read as imposing substantive requirements on national law based on the EU Charter in areas where the Charter does not apply», para. 54.

[43] *The Secretary of State for the Home Department v. David Davis, Tom Watson, Peter Brice, Geoffrey Lewis*, [2015]EWCA Civ 1185, Case no. C1/2015/2612.

[44] È importante precisare che la *Court of Appeal* non avesse accolto la posizione del Governo secondo cui «when adopting domestic legislation relating to access and use of communications data by police or other law enforcement bodies, Member States are not implementing EU law», para. 98. I giudici infatti avevano riconosciuto come rientrante nell'ambito di applicazione del diritto dell'UE tanto la disciplina della conservazione quanto quella dell'accesso ai metadata (para. 102). Questa affermazione non aveva tuttavia impedito alla Corte di considerare quanto statuito dalla CGUE in materia di accesso come non obbligatorio per il legislatore nazionale.

un rinvio pregiudiziale alla CGUE: rispetto alla sentenza *DRI* erano, infatti, emersi «considerable doubts as to the effect of its decision. On this, we have the misfortune to have come to a provisional view which differs from that of the Divisional Court» [45]. Considerando anche la giurisprudenza di altri Stati membri, che avevano invalidato le normative nazionali in materia – nel frattempo erano divenute sei le Corti nazionali che si erano in tal senso pronunciate, ovvero Austria, Slovenia, Romania, Belgio, Olanda e Slovacchia –, la *Court of Appeal* proponeva così un rinvio pregiudiziale volto a stabilire se i requisiti posti dalla sentenza *DRI* avessero o meno carattere obbligatorio, soprattutto con riferimento alla disciplina dell'accesso.

Sin da queste prime sentenze, risalenti al periodo immediatamente successivo alla sentenza *DRI*, emerge pertanto un quadro piuttosto complesso della giurisprudenza inglese in materia di *data retention* e accesso ai metadati. I giudici nazionali non avevano mostrato un orientamento condiviso ed uniforme in materia: se da un lato, infatti, con riferimento alla disciplina della conservazione, entrambe le Corti di primo e secondo grado avevano letto la decisione dei giudici di Lussemburgo come non determinante *tout court* l'incompatibilità di un regime di *bulk data retention* rispetto al diritto dell'UE, dall'altro lato, sotto il profilo dell'accesso si è verificata una netta divergenza di vedute nell'interpretazione della vincolatività e cumulabilità dei requisiti fissati dalla giurisprudenza della CGUE.

3.3. *Le valutazioni della* Court of Appeal *a seguito della pronuncia* Tele2*: una complessa decisione tra mutamenti del quadro normativo e importanti casi giurisprudenziali pendenti.*

Sarà necessario attendere il 30 gennaio 2018 [46] per vedere la conclusione del caso sopra esaminato: a seguito della pronuncia *Tele2*, con la

[45] Para. 117. La Corte poi proseguiva riconoscendo che «This is an issue of general and wide-reaching importance. Notwithstanding the expiry of DRIPA on 31 December 2016 it will not become academic. On the contrary, the true effect of the judgement in DRI will remain central to the validity of all future legislation enacted by the Member States in this field», para. 117, ribaltando dunque le considerazioni svolte precedentemente dalla *High Court*.

[46] *The Secretary of State for the Home Department v. David Davis, Tom Watson, Peter Brice, Geoffrey Lewis*, [2018]EWCA Civ 70, Case no. C1/2015/2612&2613.

quale la CGUE aveva risposto ai quesiti posti dai giudici inglese, la *Court of Appeal* era stata chiamata a riprendere le redini del c.d. caso Watson (C1/2015/2612 & 2613) che, iniziato nel 2015 con la sentenza della *High Court*, si trovava ora ad essere deciso in un contesto estremamente complesso e fortemente mutato. Nelle more del giudizio dinnanzi ai giudici di Lussemburgo, infatti, si era verificato un rilevante avvicendamento normativo: mentre oggetto della disamina della Corte di secondo grado era il DRIPA, quest'ultima disciplina era stata nel frattempo superata mediante l'adozione del IPA, avvenuta, come si è visto, alla fine del 2016. Anche sul fronte giurisprudenziale poi si erano succeduti diversi e importanti interventi; sebbene su questi casi si tornerà nel dettaglio in seguito, è fondamentale ricostruire sin da ora l'articolato contesto entro cui la *Court of Appeal* ha dovuto operare il proprio vaglio: l'*Investigatory Powers Tribunal* era stato chiamato in quegli anni a pronunciarsi sulla legittimità della *Section 94* del *Telecommunications Act 1984* in materia di acquisizione di dati e metadati da parte di servizi di intelligence per finalità di sicurezza nazionale, da cui aveva tratto origine il rinvio pregiudiziale alla CGUE nel caso *Privacy International*, mentre la ONG Liberty aveva promosso dinnanzi alla *High Court* un ricorso avente ad oggetto la conformità della *Part 4* dell'IPA ai requisiti indicati dalla giurisprudenza della CGUE. A ciò era da aggiungersi anche il procedimento di modifica dell'IPA avviato nel novembre 2017 dal *Secretary of State*, mediante la pubblicazione del documento di consultazione e di proposta di emendamenti finalizzati ad adeguare la normativa interna al diritto dell'UE, come interpretato dalla giurisprudenza della CGUE.

Ecco quindi che proprio alla luce di tale composito contesto, caratterizzato da forti cambiamenti già avvenuti o ancora in corso sul fronte normativo e da rilevanti aspetti in attesa di chiara definizione da parte della giurisprudenza nazionale o sovranazionale, è possibile comprendere la scelta della *Court of Appeal* di non pronunciarsi su talune questioni delicate e di rimettere invece la soluzione di tali profili aperti da un lato ai giudici europei nel rinvio *Privacy International* all'epoca ancora pendente e alla *High Court* nella vertenza *Liberty* dall'altro, decidendo quindi di occuparsi solo degli aspetti legati alla normativa previgente, rispetto alla quale il rinvio pregiudiziale nel caso Watson era stato promosso.

Queste premesse non devono però far ritenere la pronuncia della *Court of Appeal* priva di rilievo. Al contrario, i giudici inglesi aprivano la sentenza con una iniziale affermazione di grande importanza: «I regret to say that the task now facing this Court is far from easy in view of the fact that the preliminary ruling from the CJEU is lacking in clarity. This is apparent from the disputes between the parties before us as to its effect and from the fact that it has already given rise to a further reference by the IPT», para. 8. Veniva dunque riconosciuta la persistenza, anche a seguito della pronuncia *Tele2*, di "zone grigie" e diverse possibili interpretazioni della medesima giurisprudenza europea. L'unico punto rispetto al quale era stata riscontrata chiarezza atteneva ai requisiti in materia di accesso ai metadati: escludendo di occuparsi della questione, sottoposta a rinvio nel caso *Privacy International*, circa l'estensione dei c.d. *Tele2 requirements* anche alle attività poste in essere dalle agenzie di intelligence per finalità di sicurezza nazionale, la *Court of Appeal* giungeva piuttosto rapidamente a considerare il DRIPA in contrasto con il diritto dell'UE nella parte in cui, per scopi di sicurezza pubblica, consentiva l'accesso ai metadati conservati per obiettivi non circoscritti ai reati gravi e nella parte in cui l'accesso non veniva sottoposto ad un previo controllo da parte di una Corte o di una autorità amministrativa indipendente (para. 13).

Se i giudici nazionali avevano mostrato di condividere ed applicare i principi indicati dalla giurisprudenza della CGUE quanto alla disciplina dell'accesso, ben più problematica appariva invece la lettura ed attuazione di quanto disposto dai giudici sovranazionali in materia di *data retention*[47]. Sul punto infatti il Governo inglese sosteneva che il re-

[47] Si vuole rilevare come anche rispetto ad altri criteri stabiliti dalla CGUE la *Court of Appeal* avesse mostrato dubbi e perplessità: con riferimento ad esempio al requisito della conservazione nel solo territorio dell'UE, i giudici inglesi si chiedevano se esso fosse da intendersi come assoluto, imponendo dunque l'obbligo di memorizzare dati unicamente entro i confini europei, o se invece fosse da riferirsi solo ai metadati e non alle informazioni prodotte ed elaborate partendo da essi, le quali ben potevano essere conservate in Stati terzi. Ne conseguiva, significativamente, che «in these circumstances remains considerable uncertainty in relation to this further requirement for which the Respondents and the Interveners contend. It is to be hoped that these uncertainties, which inevitably affect the vital interests of MSs, will be clarified by the CJEU when it considers the reference made by the IPT. However, as matters stand, I do not consider that

quisito della necessaria sussistenza di un criterio oggettivo capace di istituire un collegamento, anche indiretto, tra i dati da conservare e l'obiettivo perseguito, fosse da riferirsi unicamente alle questioni rinviate dai giudici svedesi, così risultando applicabile solo ad una disciplina in materia di conservazione simile a quella disposta dalla normativa svedese, sensibilmente differente da quella inglese. La posizione espressa dalla CGUE nella sentenza *Tele2*, inoltre, doveva essere interpretata ancora una volta nel senso che il diritto dell'UE consente a che gli Stati membri adottino regimi di *data retention* generalizzata purché accompagnati da appropriate salvaguardie nella fase dell'accesso, mentre la soluzione della forma di conservazione targettizzata veniva valutata dal Governo del tutto impraticabile. Ebbene, la *Court of Appeal* decideva di non prendere una netta posizione sulla correttezza di tale lettura: pur ritenendo condivisibile quanto sostenuto dal Governo, i giudici di seconda istanza consideravano tale delicata questione pendente dinnanzi alla *High Court* nel già richiamato caso *Liberty c. Secretary of State*, attinente al vigente IPA [48].

Diversamente dalla reazione provocata in altri Stati membri, quali il Belgio e la Francia che avevano promosso un ulteriore rinvio alla CGUE vertente proprio sulla disciplina della conservazione, nel Regno Unito dunque la sentenza *Tele2* non aveva portato né ad una dichiarazione di illegittimità e incompatibilità del regime generalizzato della *data retention*, né alla apertura di un nuovo dialogo con i giudici di Lussemburgo, nonostante la riconosciuta incertezza interpretativa di talune posizioni

---

this Court should make a definitive statement on this issue in the form of a declaration», para. 19. In presenza di diverse possibili vedute e limitandosi a rilevare la mancata chiarezza sul punto, i giudici inglesi decidevano di non prendere una posizione interpretativa. Del tutto similmente, rispetto al requisito della notifica agli utenti i cui metadati erano stati oggetto di accesso da parte delle autorità di *law enforcement*, veniva rilevato innanzitutto come tale motivo di invalidità del DRIPA non fosse stato avanzato nel 2015 da parte dei ricorrenti dinnanzi alla *High Court* e come esso non comparisse neppure tra i *Tele2 requirements* inseriti nel dispositivo della sentenza *Tele2*; non risultando pertanto chiara la portata di tale salvaguardia, i giudici inglesi ritenevano appropriato non pronunciarsi su di essa.

[48] Per una analisi di tale profilo, si legga I. LLOYD, *Data retention*, in *Computer Law & Security Review*, 34, 2018, p. 407 ss.

espresse dalla CGUE attinenti tanto alla disciplina della *data retention* quanto ad altri requisiti come la notifica o la conservazione nel territorio dell'UE. Se certamente i quesiti avanzati dal IPT nel caso *Privacy International* assumevano grande importanza, riguardando sostanzialmente l'ambito di applicazione dei *Tele2 requirements*, essi non erano comunque destinati a risolvere i dubbi e le perplessità con riferimento alla materia della conservazione generalizzata. Nonostante questo, i giudici dell'appello avevano preferito lasciare che fosse il giudice nazionale, impegnato nel caso *Liberty*, a risolvere la questione.

Dalla analisi proposta, emerge in sostanza come la trasposizione entro il contesto nazionale dei requisiti stabiliti dalla giurisprudenza della CGUE avesse portato unicamente alla dichiarazione di incompatibilità della disciplina del DRIPA relativamente alla materia dell'accesso. Per questo «careful analysis of the judgement of the Court of Appeal illustrated that it was actually a pyrrhic victory, as the Court avoided a conclusive answer on crucial issues (…), not establishing requirements according to which retained data should remain in the EU or that such data should be destroyed at the end of the retention period, nor a requirement for ex post facto notification, and refused to declare inconsistency of DRIPA with fundamental rights» [49].

3.4. *La sentenza della* High Court *nel caso* Liberty *avente ad oggetto la* Part 4 *dell'IPA.*

Il caso *Liberty*, più volte richiamato dalla *Court of Appeal* nella analizzata pronuncia del 2018, è stato deciso dalla *High Court* il 27 aprile 2018 [50]: la ONG Liberty, all'indomani della sentenza *Tele2*, aveva infatti presentato dinnanzi ai giudici inglesi un ricorso volto a determinare l'incompatibilità della *Part 4* dell'IPA con il diritto dell'UE e la Convenzione EDU. Del tutto similmente a quanto statuito dai giudici dell'appello

---

[49] E. KOSTA, *SSHD v. Watson and Others: a thin nail on the coffin of UK data retention legislation*, in *European Data Protection Law Review*, 4, 2018, p. 524.

[50] *The National Council for Civil Liberties (Liberty) v. Secretary of State for the Home Department and Secretary of State for Foreign and Commonwealth Affairs*, [2018]EWHC 975 (Admin).

con riferimento alla disciplina del previo DRIPA [51], anche i giudici della *High Court* nella loro pronuncia giungevano a riconoscere nell'IPA e, nello specifico, nella disciplina attinente all'accesso, criticità e lacune tali da renderla incompatibile con quanto stabilito dalla giurisprudenza della CGUE. In questo caso, il compito della Corte era stato facilitato dal Governo stesso che, come analizzato precedentemente in questo Capitolo, aveva ammesso, sin dal luglio 2017, la necessità di un intervento normativo a riforma della vigente disciplina. Così, sulla base di tali condivise e pacifiche considerazioni, la *High Court* dichiarava l'incompatibilità del IPA nelle parti in cui «(1) access to retained data is not limited to the purpose of combating "serious crime"; and (2) access to retained data is not subject to prior review by a court or an independent administrative body» [52]. Rilevando poi nel caso in esame un «very important constitutional case» e ritenendo che una mera disapplicazione della normativa avrebbe potuto tradursi in una pericolosa situazione di caos, a danno del pubblico interesse alla sicurezza (para. 46), i giudici assegnavano al legislatore nazionale un termine – considerato ragionevole – di tempo di sei mesi, dunque sino al 1 novembre 2018, al fine di apportare le necessarie modifiche al testo normativo. Così facendo, questa decisione ha rappresentato il motore propulsivo per velocizzare quel processo di modifica del IPA che era già stato in precedenza promosso dal Governo e che ha poi portato alla adozione del *Data Retention and acquisition regulations 2018*.

---

[51] I numerosi rimandi alla sentenza della *Court of Appeal* relativa al DRIPA sono indicativi di come le considerazioni svolte relativamente alla previa normativa potessero essere validamente applicate anche all'IPA: «the judgement of the Court of Appeal is still a significant one declaring DRIPA incompatible with EU law, especially as Part 4 of IPA in essence contains relevant and similar provisions on data retention and the Court's findings will be crucial in the assessment of these provisions», E. KOSTA, *SSHD v. Watson and Others*, cit., p. 527.

[52] La Corte riconosceva dunque che le finalità previste alla *Section 61*, co. 7 (*public health, tax matters, regulation of financial services/markets and financial stability*), volte a legittimare l'accesso ai metadati conservati, non potevano dirsi compatibili al diritto dell'UE, che limitava invece tale facoltà alla repressione dei soli reati gravi. Già all'epoca del processo, comunque, il Governo aveva evidenziato tale problematico aspetto e aveva proposto di restringere gli ampi scopi previsti nell'IPA in occasione del procedimento di riforma già all'epoca avviato.

Sebbene le posizioni sino ad ora esaminate paiano del tutto in linea con la giurisprudenza della CGUE, ciò che, ancora una volta, rappresenta il punto maggiormente problematico è da individuarsi nella disciplina della conservazione dei metadati. Ribadendo quanto già espresso nelle previe pronunce della *High Court* e della *Court of Appeal*, i requisiti stabiliti nella sentenza *Tele2* in materia di *data retention* venivano considerati ancora una volta come principalmente riferiti alla normativa svedese. Quest'ultima, diversamente da quella inglese, prevedeva un obbligo generalizzato di conservazione dei metadati, secondo quanto già disposto dalla DRD: per i giudici inglesi, invece, «the IPA does not contain a blanket requirement requiring the general retention of communications data. The Act does not itself impose any requirement on telecommunications operators to retain data. Instead, the Secretary of State is given a power to require retention of data by serving a notice to an operator», para. 127. La determinazione, alla *Section 88* dell'IPA, di precisi elementi che il *Secretary of State* era chiamato a valutare prima di emanare il *retention notice*, unitamente alla previsione di un controllo preventivo operato dal *Judicial Commissioner*, venivano considerate tutele idonee e sufficienti a determinare la compatibilità dell'IPA con il diritto dell'UE, nonché tali da scongiurare i rischi di una conservazione generalizzata [53]. A nulla era valsa la posizione, di segno opposto, espressa dai ricorrenti, che ricalcava peraltro quelle obiezioni e timori già espressi all'indomani dell'adozione dell'IPA stesso: la *retention notice* emanata dal *Secretary of State*, benché condizionata a specifiche valutazioni e controlli, poteva comunque assumere carattere generalizzato e riguardare cioè tutti i metadati, tutti gli utenti e tutti i fornitori di servizi di telecomunicazione; le garanzie predisposte dalla normativa, in altre parole, non permettevano di escludere totalmente l'adozione di una forma di *bulk data retention*.

[53] Ciò appare in tutta chiarezza dalle parole della *High Court*: «in the light of this analysis of the structure and content of Part 4 of the IPA we do not think it could possibly be said that the legislation requires, or even permits, a general and indiscriminate retention of communications data. The legislation requires a range of factors to be taken into account and imposes controls to ensure that a decision to serve a retention notice satisfies the tests of necessity in relation to one of the statutory purposes, proportionality and public law principles», para. 135.

In conclusione, la sentenza analizzata si pone di fatto in linea di continuità rispetto alla di poco precedente decisione della *Court of Appeal* relativamente al DRIPA: le lacune e le incompatibilità individuate nelle due normative infatti sono identiche ed entrambe attinenti alla disciplina dell'accesso, mentre nessuna dichiarazione o presa di posizione è stata svolta con riferimento agli ulteriori e diversi requisiti emersi dalla giurisprudenza della CGUE [54]. Per quanto riguarda la disciplina della conservazione dei metadati, invece, è stata affermata con decisione la compatibilità del regime disposto nell'IPA rispetto ai requisiti indicati nelle sentenze *DRI* e *Tele2*, nonostante l'assenza sia di criteri oggettivi volti creare una connessione, anche indiretta, tra conservazione e atti di criminalità grave, sia di quelle restrizioni sulla base di criteri geografici o soggettivi indicate dai giudici di Lussemburgo. Questo centrale quanto delicato punto ha scatenato un profondo dibattito e molteplici critiche: White e Cobbs hanno in particolare sottolineato come il ragionamento della Corte fosse fondato sul presupposto, invero tutto da verificarsi, secondo cui nella pratica il *Secretary of State* non avrebbe alcun vantaggio o intenzione di emanare *retention notices* di carattere generalizzato ed indiscriminato. Questo assunto tuttavia dimostra di non considerare il fatto che non esistono, a parere di molti, nella normativa vigente, limiti e divieti precisi volti ad impedire il ricorso a forme di *bulk data retention*, che rimangono quindi, nella teoria ma anche nella pratica, del tutto attuabili [55]. Per ques-

[54] Anche nel caso in analisi, la *High Court* decideva di non prendere posizione sui requisiti della conservazione nel territorio dell'UE e della notifica all'interessato in caso di avvenuto accesso ai metadati conservati, ritenendo che simili questioni fossero già state poste alla CGUE mediante il rinvio pregiudiziale promosso dal IPT nel caso *Privacy International*, dovendosi quindi attendere la pronuncia dei giudici di Lussemburgo per veder chiariti tali controversi aspetti.

[55] Sul punto si legga M. WHITE, *Is the incompatibility of UK data retention law with EU law really a victory?*, in *Legal Studies*, 41, 2021, p. 130 ss. Anche Cobbe ha affermato come «retention notices may be tailored to an extent, including by requiring that only data which meets a certain description or is from a certain time period is retained. But Section 87 does allow for service providers to be required to retain all data indiscriminately, without differentiation, limitation or exception and without clear safeguards for data subject to professional confidentiality», J. COBBE, *Casting the dragnet: communications data retention under the Investigatory Powers Act*, in *Public*

ti motivi vi è chi ha messo in dubbio la reale portata della pronuncia esaminata: «The first phase of Liberty's challenge to the IPA may have been successful – however, the real practical impact of this case remains to be seen» [56]. Così, se questa decisione ha senz'altro avuto il merito di accelerare la già avviata procedura di modifica al testo dell'IPA, è altrettanto vero però che le riforme introdotte nel 2018, pur essendosi positivamente indirizzate verso un rafforzamento delle tutele nella fase di accesso, secondo le indicazioni fornite sia dalla *High Court*, sia dalla CGUE, hanno mancato di affrontare in maniera precisa e puntuale i timori relativi alla ampiezza dei *retention notice* e dei limiti alla possibilità di addivenire ad una *bulk data retention* [57].

Law, 2018, p. 5, disponibile all'indirizzo: https://pureadmin.qub.ac.uk/ws/portalfiles/portal/153330583/Casting_the_Dragnet.pdf.

[56] C. GILMARTIN, *Privacy Rights: how should a Court remedy legislative incompatibility with EU law?*, in *UK Human Rights Blog*, 8 maggio 2018.

[57] La legittimità della disciplina dell'IPA veniva confermata peraltro dalla stessa *High Court* anche nella successiva pronuncia *Liberty v. Secretary of State for Home Department and Secretary of State for Foreign and Commonwealth Affairs* [2019]EWHC2057, del 29 luglio 2019. Su ricorso della medesima ONG Liberty, i giudici inglesi erano stati chiamati a valutare questa volta la compatibilità dell'IPA rispetto allo *Human Rights Act* (HRA) del 1998, atto con cui il Regno Unito ha recepito e riconosciuto la Convenzione EDU quale fonte del proprio ordinamento. Svolgendo considerazioni del tutto simili a quelle già evidenziate nelle sentenze sino ad ora analizzate, i giudici rilevavano la compatibilità dell'IPA con gli artt. 8 e 10 della Convenzione EDU, ritenendo che la disciplina predisposta dal legislatore inglese comportasse una ingerenza nei diritti alla vita privata e alla libertà di espressione proporzionata e necessaria in una società democratica, stabilendo salvaguardie sufficienti a prevenire il rischio di abusi e di interferenze arbitrarie da parte dei pubblici poteri. Le innovazioni introdotte dall'IPA e dalle modifiche del 2018 – quali il sistema di *double-lock* – portavano inoltre la *High Court* a ritenere non applicabili a tale disamina le considerazioni critiche svolte dalla Corte EDU nella già richiamata controversia *Big Brother Watch*. I rilievi mossi dai giudici di Strasburgo, infatti, erano riferiti in quel caso alla previa normativa RIPA e non erano automaticamente trasponibili alla innovativa e maggiormente garantista disciplina del 2018. Per approfondimenti, si veda I. TRUMMER, *Liberty v. SSHD & SSFCA: you have the right to remain silent; anything you say will be gathered and retained by the Government*, in *Tulane Journal of International and Comparative Law*, 28, 2020, p. 388 ss.

3.5. *Le pronunce dell'*Investigatory Powers Tribunal*: il rinvio alla CGUE nel caso* Privacy International *e la decisione finale del 22 luglio 2021.*

Prima di avviarsi ad alcune considerazioni critiche quanto all'evoluzione normativa e giurisprudenziale caratterizzante il Regno Unito e alle prospettive future, la ricostruzione degli interventi delle Corti inglesi deve essere completata dall'analisi di alcune ulteriori rilevanti decisioni: quelle dell'*Investigatory Powers Tribunal*. Nonostante quest'ultimo, nel ricorso promosso dalla ONG Privacy International che in questa sede si vuole esaminare, si sia pronunciato su una disciplina differente rispetto a quella che aveva interessato in precedenza la *High Court* e la *Court of Appeal*, la giurisprudenza che ne è derivata risulta di estrema importanza ed interesse anche per l'ulteriore momento di dialogo instaurato con la CGUE mediante lo strumento del rinvio pregiudiziale.

Nella controversia promossa dinnanzi al IPT [58], la ricorrente Privacy International aveva ritenuto incompatibile con la Convenzione EDU e con il diritto dell'UE il *Telecommunications Act 1984* regolante l'acquisizione, utilizzo, conservazione, memorizzazione e cancellazione di metadati da parte delle agenzie di intelligence, ovvero le *Security and Intelligence Agencies* (SIAs) che ricomprendevano i *Government Communications Headquarters* (GCHQ) e il *Security Service*. Questa normativa, vigente all'epoca del ricorso e successivamente sostituita dall'IPA nel 2016, prevedeva – anche – la possibilità da parte del *Secretary of State* di autorizzare, qualora necessario ai fini della salvaguardia della sicurezza nazionale, forme di trasmissione generalizzata di metadati alle autorità di intelligence le quali poi potevano svolgere analisi automatizzate e filtrare così l'enorme mole di dati ricevuti, accedendo poi più approfonditamente solo a quelle informazioni rispondenti ai *selctors* individuati. In una prima parziale pronuncia del 17 ottobre 2016, l'IPT si era concentrato sul primo quesito posto dalla ricorrente, valutando cioè la legittimità e compatibilità della disciplina sopra indicata unicamente alla luce dell'art. 8 della Convenzione EDU; nella seconda decisione del 8 settembre 2017 il Tri-

[58] *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, [2016]UKIPTrib15_110-CH, Case no. IPT/15/110/CH.

bunale, a seguito di ulteriori e più approfondite udienze, si era invece occupato di vagliare la conformità al diritto dell'UE dei poteri di raccolta, conservazione e accesso di metadati attribuiti alla agenzie di intelligence. Sebbene tale ultima pronuncia risulti certamente di maggiore interesse ai fini della presente disamina, pare nondimeno di rilievo premettere come nella prima sentenza del 2016[59] l'IPT avesse considerato compatibile con l'art. 8 della Convenzione EDU il potere attribuito ai *Home and Foreign Secretaries* di imporre ai fornitori di servizi di comunicazione il trasferimento generalizzato di metadati (c.d. *Bulk Communications Data*, BCD) alle autorità di intelligence per scopi di sicurezza nazionale; i giudici avevano infatti ritenuto proporzionate ed adeguate tante le salvaguardie predisposte dalla normativa nazionale e volte a scongiurare il rischio di abusi nella fase di trattamento dei metadati, quanto la supervisione garantita dall'*Independent Intelligence Service Commissioner*[60].

Nella successiva pronuncia del 2017, avente più specificamente ad oggetto la conformità rispetto al diritto dell'UE del sistema di raccolta e analisi dei metadati utilizzato dalle SIAs, l'IPT svolgeva poi una premessa di rilievo: «the context of the issues before us has been as to the balance between the steps taken by the State, through the SIAs, to protect its population against terror and threat to life against the protection of privacy of the individual», para. 6. Questa affermazione quindi mirava a chiarire come il bilanciamento che il legislatore era stato chiamato a svolgere e che i giudici dovevano vagliare vedesse lo scontro tra, da un lato, un interesse collettivo e, dall'altro, un diritto di dimensione meramente indivi-

[59] Come ben spiegato da Woods, «this judgement effectively dealt with questions of lawfulness, as understood in the light of art. 8 ECHR. (…) The difficult topics regarding proportionality and the impact of *Tele2* remain to be dealt with», L. WOODS, *Investigatory Powers Tribunal (IPT): Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, in *European Data Protection Law Review*, 3, 2017, p. 248.

[60] Merita precisare come la compatibilità con l'art. 8 della Convenzione EDU fosse stata dichiarata unicamente con riferimento alla disciplina nazionale predisposta a seguito dell'anno 2015, cioè da quando, successivamente alla pubblicizzazione dei regimi di sorveglianza, si era provveduto ad una modifica della disciplina previgente nonché all'inserimento di maggiori tutele e salvaguardie che venivano considerate, da quel momento, realmente efficaci.

duale: una lettura che pareva voler mettere, sin dall'inizio, in evidenza la maggior rilevanza della garanzia della sicurezza rispetto ad una prerogativa riconosciuta al singolo [61]. A conferma e rafforzamento di quella premessa, poi, i giudici del IPT sottolineavano l'importanza da attribuire ai sistemi di *bulk acquisition* di metadati, cioè di trasferimento massivo di informazioni dai *service providers* alle agenzie di intelligence: «the use of bulk data capabilities is critical to the ability of the SIAs to secure national security; a fundamental feature of many of the SIAs'techniques of interrogating Bulk Data is that they are non-targeted, not directed at specific targets», para. 10. Dal riconoscimento del fondamentale ruolo svolto da tali regimi derivava che imporre il rispetto dei requisiti stabiliti nelle sentenze *DRI* e *Tele2* – quest'ultima peraltro pubblicata nelle more del giudizio in esame – anche alle attività di tutela della sicurezza nazionale avrebbe comportato una forte diminuzione in termini di efficacia dell'azione delle SIAs. Secondo il Report presentato da Anderson, *Independent Reviewer of Terrorism Legislation*, e richiamato dai giudici, emergeva come «bulk acquisition has been demonstrated to be crucial, in a variety of fields (…). The SIAs'ability to interrogate the aggregated data obtained through bulk acquisition cannot, at least with currently available technology, be matched through the use of data obtained by targeted means», para. 14; una forma di raccolta, conservazione e accesso targettizzato ai metadati non sarebbe stata così in grado di garantire il medesi-

[61] In questo i giudici hanno dimostrato di non riconoscere nella tutela della privacy una rilevanza capace di andare oltre l'interesse del singolo: come affermato anche dalla giurisprudenza della Corte EDU, sistemi di *bulk trasfer, collection* e *retention*, privi di appropriati limiti e salvaguardie, rischiano di compromettere i valori fondamentali sui quali la stessa società democratica poggia, creando quella sensazione di diffusa sorveglianza che incide sul godimento di altri diritti fondamentali quali la libertà di espressione e di associazione o il principio di presunzione di innocenza. Ignorando questi profili, il bilanciamento svolto dal giudice inglese appare già "sbilanciato" in partenza laddove viene affermato che la sicurezza rappresenta comunque un interesse superiore, mentre la privacy viene considerata un mero diritto del singolo il cui mancato rispetto su null'altro incide. Su questo profilo si leggano M. WHITE, *The Privacy International case in the IPT: respecting the right to privacy?*, in *EU Law Analysis*, 14 settembre 2017; T. QUINTEL, *Investigatory Powers Tribunal: Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Ors Part II*, in *European Data Protection Law Review*, 3, 2017, p. 393 ss.

mo livello di efficacia e di garanzia della sicurezza. I giudici inglesi avevano poi messo in evidenza come le SIAs non esaminassero tutti i dati loro trasferiti *in bulk* dai fornitori privati: «by process of elimination, and with minimal intrusion, [the SIAs] obtain access only to the data of persons whose activities may constitute a threat to national security» (para. 16), in modo tale che solo una ristretta porzione dei dati raccolti diveniva effettivo oggetto di trattamento e successivo vaglio. Insieme a tutte queste considerazioni, che miravano a confermare la necessità di sistemi di *bulk transfer* e la loro limitata invasività nella sfera privata, il Governo, parte resistente nel procedimento, aveva sostenuto che i requisiti enunciati nella pronuncia *Tele2* non dovevano essere applicati alla disciplina in esame: innanzitutto poiché la finalità perseguita dal regime regolato dalla normativa del 1998 era quella di tutela della sicurezza nazionale, una materia che, ai sensi dell'art. 4 TUE, non rientrava nell'ambito di applicazione del diritto dell'UE; inoltre i principi stabiliti dalla giurisprudenza europea prendevano avvio da un caso avente ad oggetto la disciplina del DRIPA, che riguardava però non il trasferimento di metadati alle agenzie di intelligence e la loro diretta conservazione da parte di esse, bensì la conservazione da parte di fornitori privati di metadati riguardanti i propri utenti al fine di rendere disponibili tali informazioni alle autorità di *law enforcement*. Per queste ragioni e peraltro richiamando ampiamente la sentenza *Parlamento c. Consiglio*, per il Governo la disciplina posta all'attenzione dell'IPT non doveva essere vagliata alla luce del diritto dell'UE ma unicamente sulla base della Convenzione EDU, rispetto alla quale il Tribunale aveva già pronunciato la compatibilità della disciplina in esame nella previa sentenza del 2016. Per Privacy International, al contrario, la posizione espressa dal Governo si fondava su erronee considerazioni, quali la convinzione secondo cui una acquisizione generalizzata e un trattamento automatizzato dei metadati rappresentassero una invasione più limitata della sfera privata rispetto ad una forma di conservazione e accesso targettizzati; o ancora la ritenuta preminenza dell'interesse alla tutela della collettività rispetto al diritto del singolo e la supposta incompatibilità di forme di salvaguardia più stringenti con un efficace ed efficiente sistema di protezione della sicurezza nazionale.

I giudici dell'IPT non potevano quindi che prendere atto della divergenza di posizioni espresse dalle parti del processo, ritenendo imprescin-

dibile un intervento della CGUE volto a chiarire i confini del diritto dell'UE e dunque l'ambito di applicazione dei c.d. requisiti *Tele2*. Ciò che qui risulta di estremo interesse è evidenziare come il Tribunale, nel rinvio pregiudiziale promosso, non abbia mancato di rivelare posizioni concordi a quanto espresso dal Governo: le salvaguardie indicate dalla CGUE risultano incompatibili con strumenti di garanzia della sicurezza nazionale che richiedono necessariamente forme di «bulk and unspecific processing of data», para. 55; requisiti quali il previo controllo indipendente o la notifica ai soggetti i cui dati vengono vagliati da autorità pubbliche possono minare seriamente l'efficacia e l'utilità delle attività poste in essere dalle SIAs. Per questo l'IPT concludeva sostenendo che «we are persuaded that if the Watson requirements do apply to measures taken to safeguard national security, in particular the BCD regime, they would frustrate them and put the national security of the UK, and, it may be, other Member States, at risk», para. 69. Una considerazione forte, con la quale i giudici inglesi – in una certa misura – ammonivano la CGUE, ribadendo il peso e le conseguenze potenzialmente devastanti di un necessario adeguamento delle attività delle SIAs ai requisiti *Tele2*.

Tali posizioni, come si è ampiamente visto nel Capitolo 2, non sono state però condivise della CGUE che, rispondendo ai quesiti posti dall'IPT, ha al contrario ribadito come qualsiasi forma di trattamento che implichi un intervento in capo a *service operators* – dunque anche la sola trasmissione di dati – sia da ritenersi rientrante nell'ambito di applicazione del diritto dell'UE, indipendentemente dalla finalità – sicurezza nazionale o sicurezza pubblica – cui il trattamento è preposto; una forma di *bulk acquisition* è stata inoltre equiparata ad una forma di accesso illimitato ai dati da parte delle autorità di intelligence, anche laddove esso avvenga mediante analisi meramente automatizzate di screening e di filtraggio, che si svolgono comunque in assenza di un nesso tra accesso e minaccia di reato. Anche alle operazioni di trasferimento e acquisizione di metadati da parte di autorità di intelligence, debbono pertanto essere applicati quei limiti e salvaguardie sancite dall'art. 15 Direttiva *e-Privacy*, così come interpretato dalla giurisprudenza della CGUE. Quest'ultima poi, aveva chiaramente delineato, in maniera, come si è detto, piuttosto innovativa, anche le condizioni che legittimano il ricorso a forme di *bulk data retention* per il solo scopo di tutela della sicurezza nazionale.

L'IPT, di conseguenza, a seguito della pronuncia dei giudici di Lussemburgo e riprendendo il caso dinnanzi a sé, ha riconosciuto, nella sentenza del 22 luglio 2021 [62], l'incompatibilità con il diritto dell'UE della controversa *Section 94* del *Telecommunications Act 1984*, pur affermando come «we [i giudici] have not today decided what the consequences of that declaration are. That remains a matter of dispute between the parties and will be considered at a later stage», para. 29. Pur rimanendo in attesa dunque di ulteriori fondamentali sviluppi, che definiranno ulteriormente le conseguenze e l'impatto di tale pronuncia, non può non essere dichiarata sin da ora l'importanza di questa prima posizione espressa dal IPT, peraltro conforme a quanto già rilevato da entrambe le parti del procedimento a seguito della decisione della CGUE: unitamente alla ricorrente Privacy International, infatti, anche il Governo inglese ha ammesso le criticità e la non conformità della normativa oggetto di disamina rispetto ai criteri indicati dalla giurisprudenza della CGUE nelle pronunce dell'ottobre 2020 e applicabili anche alle attività dei servizi di intelligence quali quelle operate dalle SIAs inglesi. Il carattere generalizzato ed indiscriminato dell'obbligo di trasmissione dei metadati imposto agli operatori dei servizi di comunicazione non poteva ritenersi conforme a quei requisiti ribaditi nelle pronunce *Privacy International* e *La Quadrature du Net* della CGUE: non sussisteva infatti nella normativa nazionale del 1984 né una limitazione dell'obbligo di trasmissione – e dunque del potere di acquisizione dei metadati da parte delle SIAs – a situazioni di seria minaccia alla sicurezza nazionale, reale, attuale o prevedibile, né una restrizione temporale di tale imposizione che, secondo i giudici di Lussemburgo, non può superare un termine di tempo prevedibile e limitato a quanto strettamente necessario. La previsione poi dell'intervento del *Secretary of State*, membro del potere esecutivo, non è stata considerata rispondente al richiesto criterio del previo controllo da parte di un giudice o di una autorità amministrativa indipendente. Il Governo non ha tuttavia mancato di precisare nel corso del processo come la CGUE, nelle sentenze del 6 ottobre 2020, non si sia pronunciata né sulla legittimità «in the abstract» di un sistema di acquisizione generalizzata per finalità di si-

[62] *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs*, [2021]UKIPTribIPT_15_110_CH, Case No. IPT/15/110/CH.

curezza nazionale, né sulla necessità di non valutare gli elementi di prova derivanti da metadati ottenuti, nel contesto di un procedimento penale, sulla base di una normativa interna incompatibile con il diritto dell'UE. La determinazione di questi delicati punti restano, a parere del Governo, di sola pertinenza dei giudici nazionali. La correttezza di tale interpretazione, che peraltro propone – pur in maniera sintetica e quasi apodittica, senza fornire alcun dettaglio sul punto – una distinzione tra *bulk powers* e *general and indiscriminate powers* (para. 23), resta in attesa di una ulteriore pronuncia del IPT. Pur non riguardando direttamente la normativa vigente dell'IPA, la più recente – per quanto breve e concisa – sentenza dell'IPT riapre senza dubbio il dibattito, mai sopito, sulla proporzionalità della disciplina della *data retention* e accesso ai metadati stabilita dalla normativa inglese, che deve oggi essere riletta anche alla luce dei più recenti sviluppi giurisprudenziali a livello sovranazionale, tanto della CGUE quanto della Corte EDU.

4. *Provvisorie considerazioni sulla disciplina inglese della* data retention*: ulteriori e doverosi interventi all'orizzonte?*

L'analisi dell'evoluzione normativa e giurisprudenziale, sopra svolta, induce a muovere alcune considerazioni sull'approccio del Regno Unito in materia di *data retention* e accesso ai metadati: non si può infatti non porre in evidenza come il percorso seguito, costellato da molteplici interventi legislativi e sentenze delle Corti nazionali, unitamente agli sviluppi della giurisprudenza europea, abbia condotto ad una maggiore consapevolezza dei rischi legati all'impiego di invasivi strumenti di indagine e, dunque, della necessità di stabilire idonee salvaguardie e tutele, tanto nella fase di conservazione quanto in quella di accesso.

Ciò è chiaramente visibile dalla ricostruzione della disciplina normativa e delle sue riforme nel corso del tempo: l'iniziale tendenza ad interventi di adeguamento e modifica della regolamentazione interna – peraltro rapidi e poco coordinati, nella sostanza e nella scelta temporale, rispetto alla giurisprudenza nazionale e soprattutto sovranazionale – pareva motivata più dal timore di perdere la possibilità di utilizzare i metadati conservati, che da una reale e sentita volontà di innalzare il livello di tutela

dei diritti fondamentali e addivenire ad un più corretto bilanciamento con le esigenze securitarie. Una volontà, questa, che sembra invece essere maggiormente sottesa alle più recenti modifiche legislative, in particolare quella del 2018, frutto di una più seria riflessione del legislatore, spinto anche dalle critiche e dalle analisi mosse dalla dottrina nonché dall'attenzione manifestata dalla società civile e da numerose ONG, oltre che da una posizione espressa dalle Corti nazionali – in taluni punti – maggiormente convergente con quella della CGUE. Gli sviluppi normativi più recenti, pur essendo ancora lontani da quella forma di conservazione targettizzata, per scopi di sicurezza pubblica, promossa dalla CGUE come unico strumento compatibile al diritto dell'UE e alla Carta di Nizza, nonché restando privi di alcune delle salvaguardie attinenti alla fase dell'accesso [63] e alla sicurezza dei metadati indicate dai giudici di Lussemburgo, consentono di registrare una più decisa svolta verso l'attuazione dei principi di proporzionalità e necessità, che rimangono comunque assegnati in gran parte alle valutazioni di membri del potere esecutivo – quale il *Secretary of State* –.

In maniera simile, anche la giurisprudenza nazionale è stata testimone di un percorso evolutivo di lento, seppur non totale, avvicinamento alla giurisprudenza sovranazionale: dichiarando l'incompatibilità della disciplina nazionale rispetto al diritto dell'UE, nelle sentenze *Watson*, *Liberty* e nella più recente *Privacy International*, le Corti hanno seguito ed applicato al regime interno il ragionamento sviluppato dai giudici di Lussemburgo, imponendo così al legislatore di ripensare alla normativa adottata o imprimendo una spinta nella direzione di un rapido intervento di ri-

[63] Un ulteriore profilo problematico e di complessità è da rilevarsi nella concreta efficacia delle tutele e salvaguardie predisposte dal legislatore. Basti pensare al rimedio giurisdizionale rappresentato dalla possibilità di promuovere ricorso avverso l'IPT: «this extensive jurisdiction has received 2140 complaints from its inception (since 2000) to 2015 and it was only in February 2015 that the IPT found its first finding against the Government. From 2000 to 2015 there has been total of 16 successful complaints out of 2140, making a success rate of around 0.9%», M. WHITE, *Protection by judicial oversight or an oversight in protection?*, cit., p. 14. Questi interessanti dati aiutano a comprendere come un'analisi completa della disciplina della *data retention*, dell'accesso e dei rimedi previsti debba spingersi a considerarne non solo la previsione normativa ma anche la sua efficacia ed applicazione concreta.

forma. Non è però da sottovalutare come, anche con riferimento alle richiamate decisioni, il vaglio dei giudici si sia concentrato essenzialmente sulle lacune legate alla disciplina dell'accesso: non stupisce dunque che il ragionamento seguito dalla *High Court* e dalla *Court of Appeal*, fondato sulla individuata differenziazione tra la disciplina inglese e quella svedese valutata dai giudici di Lussemburgo nella pronuncia *Tele2*, abbia sin da subito attirato forti critiche, imponendo così di ridimensionare sensibilmente quelle che potevano, a primo impatto, sembrare vittorie piene per i sostenitori dei diritti fondamentali [64]. Del resto anche il rinvio pregiudiziale promosso dall'IPT mirava ad ottenere una delimitazione dell'ambito di applicazione del diritto dell'UE con riferimento alle attività e ai compiti delle agenzie di intelligence; i giudici hanno pertanto mostrato, in quella occasione, di voler «opporre una sorta di resistenza statuale che mira ad ampliare i margini di discrezionalità possibili nelle operazioni di raccolta, conservazione ed analisi dei dati relativi alle comunicazioni elettroniche» [65] in materie così fondamentali e delicate quali la sicurezza nazionale, rispetto alle quali il Regno Unito vuole mantenere un saldo ed esclusivo controllo.

Un percorso quindi, quello qui ricostruito, che, come una medaglia, non ha mancato di rivelare le sue duplici facce: da un lato l'evoluzione registratasi va letta positivamente, soprattutto se paragonata a quanto avve-

---

[64] Molti commenti alle più recenti pronunce della *High Court* hanno segnalato proprio la mancata considerazione, da parte dei giudici e, ancor prima, del legislatore, di molti degli requisiti delineati dalla giurisprudenza europea in materia di conservazione dei metadati: «Part 4 of the IPA 2016 is neither consistent with the ECHR or EU law. The High Court have fallen into the same trap as the Court of Appeal did earlier this year when distinguishing a catch all power, and a power that can catch all», M. WHITE, *Data Retention incompatible with EU law: Victory? Victory you say?*, in *EU Law Analysis*, 24 maggio 2018; similmente Trummer ha sottolineato come «the Court followed precedent, but throughout its analysis, it erred on the side of caution and decided the case with the threat of terrorist attack, hostile actors and national security weighing heavily on its mind. The lack of focus on the fundamental rights at risk of being encroached upon, resulted in a balancing test that simply lacked balance», I. TRUMMER, *Liberty v. SSHD & SSFCA*, cit., p. 396.

[65] L. SCAFFARDI, *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016*, cit., p. 415.

nuto in altri Stati membri, quali l'Italia, nei quali ancora fatica ad affermarsi un dibattito approfondito sull'esigenza di un corretto adeguamento della normativa nazionale a quanto emerso dalla giurisprudenza della CGUE; dall'altro lato però alcuni fondamentali punti rimangono ampiamente controversi e dagli sviluppi ancora incerti: la legittimità del regime nazionale di conservazione dei metadati, sin qui avvallato dagli interventi delle Corti inglesi, deve ora confrontarsi con quanto emerso tanto dalla sentenza *Privacy International* della CGUE, quanto dalla decisione della *Grand Chamber* della Corte EDU nella controversia *Big Brother Watch*. L'esito del travagliato ed intricato cammino che ha condotto alla riforma dell'IPA nel 2018 non sembra pertanto potersi ritenere risolutivo punto di arrivo ma pare al contrario destinato ad essere nuovamente al centro del dibattito politico nel prossimo futuro, sotto i colpi del continuo avvicendarsi di pronunce giurisprudenziali. Anche se la sentenza dell'ottobre 2020 dei giudici di Lussemburgo ha avuto ad oggetto una normativa differente da quella ad oggi vigente, similmente alla decisione dei giudici di Strasburgo del maggio 2021 che ha riguardato il previo RIPA, tali rilevanti sviluppi non possono non indurre a riflettere sulla conformità della normativa inglese ai principi in essi sviluppati. Tanto il legislatore quanto le Corti ben potrebbero essere dunque, nei prossimi anni, chiamati a rileggere e rivalutare la disciplina nazionale in materia di conservazione e di accesso o acquisizione dei metadati stessi: alcune ONG, tra cui Liberty, hanno già espresso l'intenzione di promuovere ricorsi dinnanzi alla Corti nazionali avverso la disciplina vigente, ritenuta non conforme ai criteri indicati dalla Corte EDU nonché – soprattutto – ai principi ben più stringenti e garantisti elaborati dalla CGUE nelle sue ultime decisioni in materia. Una giurisprudenza che, come si analizzerà nel prossimo paragrafo, è destinata a mantenere il proprio fondamentale rilievo nel conteso inglese anche a seguito della procedura di c.d. *Brexit*.

5. *Garantire il flusso di dati UE-Regno Unito nello scenario* post-Brexit*: il dibattito sull'adeguatezza delle garanzie offerte Oltremanica.*

5.1. *Il lento e difficile cammino verso l'adozione di una decisione di adeguatezza.*

A seguito del referendum del 23 giugno 2016, il Regno Unito ha notificato in data 29 marzo 2017 la propria decisione di recedere dall'Unione europea e dalla Comunità europea dell'energia atomica, sulla base della facoltà garantita dall'art. 50 TUE. L'intenso dibattito, sviluppatosi sia in seno all'UE che Oltremanica e che ha portato a complesse negoziazioni, continui rinvii e battute d'arresto, si è infine concluso con l'approvazione dell'*Accordo sul recesso del Regno Unito di Gran Bretagna e Irlanda del Nord dall'Unione europea e dalla Comunità europea dell'energia atomica* L 29/7, del 31 gennaio 2020 (conosciuto anche come *Withdrawal Agreement*) [66], determinante le modalità e gli effetti del recesso.

Questo percorso senza precedenti nella storia dell'UE non ha mancato di produrre rilevanti conseguenze anche sotto il profilo della disciplina della protezione dei dati: primo e più evidente portato è senz'altro da ravvisarsi nella assunzione da parte del Regno Unito della qualifica di Stato terzo ai sensi dell'art. 45 GDPR. Il trasferimento dati Oltremanica diviene perciò vincolato alla capacità dell'ordinamento inglese di garantire un livello di protezione dei dati sostanzialmente equivalente a quello stabilito entro i confini europei. Sebbene, come già emerso nel Capitolo 3, esistano diversi strumenti, individuati nel Capo V del Reg. UE 2016/679, atti a consentire il flusso di dati, il più importante di essi è certamente rappresentato dalla decisione di adeguatezza adottata dalla Commissione, avente valenza generale.

Tale decisione, da più parti fortemente auspicata ed attesa, è giunta il

---

[66] Sul punto si rimanda, *ex multis*, a F. JACOBS, *The EU after Brexit. Institutional and policy implications*, Palgrave, Londra, 2018; F. SAVASTANO, *Uscire dall'UE. Brexit e il diritto di recedere dai Trattati*, Giappichelli, Torino, 2019; M. ELLIOTT, J. WILLIAMS, A.L. YOUNG (a cura di), *The UK Constitution after Miller. Brexit and beyond*, Hart, Londra, 2020; F. FABBRINI, *Brexit. Tra diritto e politica*, Il Mulino, Bologna, 2021; B. PONTIN, *The environmental case for Brexit. A socio-legal perspective*, Hart, Oxford, 2021.

28 giugno 2021 [67] al termine di un procedimento travagliato e difficile, caratterizzato da continui rinvii e disposizioni transitorie, volte essenzialmente ad assicurare la continuità del flusso di dati UE-Regno Unito. L'art. 127 dell'Accordo di recesso del gennaio 2020 indicava, infatti, un primo periodo di transizione, utile ad assicurare un sufficiente lasso di tempo per la definizione dei molteplici e delicati nodi risultanti dalla procedura di *Brexit*: sino al 31 dicembre 2020 il diritto dell'Unione doveva pertanto essere applicato al e nel Regno Unito. All'interno del medesimo atto, poi, l'art. 71 meglio specificava che, in materia di *data protection*, a partire dal 1 gennaio 2021, nel Regno Unito avrebbe trovato attuazione unicamente il diritto interno inglese, determinando così il definitivo passaggio, anche sotto tale profilo, dell'isola da Stato membro a Stato terzo. Dinnanzi a queste chiare disposizioni, numerosi operatori economici privati nonché studiosi avevano tempestivamente sottolineato la fondamentale importanza dell'adozione da parte della Commissione di una decisione di adeguatezza entro la scadenza del periodo transitorio, così da scongiurare il ricorso da parte dei singoli *data exporters* agli ulteriori complessi ed onerosi strumenti di *data transfer* disposti dalla normativa europea [68]. Non mancava tuttavia in questi appelli la chiara consapevolezza

[67] *Commission implementing decision pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom*, 28 giugno 2021, C(2021)4800 final.

[68] Come già ricordato nel Capitolo 3, un blocco del trasferimento di dati avrebbe infatti comportato profonde conseguenze per le aziende operanti nel Regno Unito, imponendo a queste ultime l'adozione degli onerosi strumenti alternativi previsti nel GDPR. Queste preoccupazioni erano particolarmente sentite da taluni settori economici, quali quello finanziario, bancario e soprattutto quello dei servizi di telecomunicazione e digitali più in generale (sul punto K. WIMMER, J. JONES, *Brexit and implications for privacy*, in *Fordham International Law Journal*, 5, 2017, p. 1554 ss.; ma anche ASSOCIATION FOR FINANCIAL MARKETS IN EUROPE, *Effective flow of personal data post-Brexit. Implications for capital markets*, 2018). Per una analitica disamina delle proporzioni del potenziale danno economico causato dall'assenza di una decisione di adeguatezza – e dunque dalla mancata continuità o dalla maggiore difficoltà di garantire il flusso di dati Oltremanica –, si rimanda a K. MACASKILL, *Brexit: potential trade and data implications for digital and fintech industries*, in *International Data Privacy Law*, 1, 2017, p. 3 ss.; P. DE HERT, V. PAPAKONSTANTINOU, *The UK contribution to the field of EU data protection: let's not go for 'third country' status after Brexit*, in *Computer Law and Security Review*, 33,

della difficoltà di addivenire a tale vantaggiosa soluzione, come le faticose negoziazioni con altri Stati terzi, quali ad esempio gli USA, avevano in passato già dimostrato, unitamente alle note vicende giurisprudenziali della c.d. *Schrems saga* che più volte avevano portato la CGUE a smentire le valutazioni di adeguatezza svolte dalla Commissione, rendendo altamente instabile ed incerta la continuità delle operazioni di *data transfer*.

Del resto, incertezza sulla possibilità di giungere ad una decisione di adeguatezza *post-Brexit* era stata sin dall'inizio manifestata anche dal GEPD, che sul punto si era pronunciato in maniera critica [69]. Certamente veniva riconosciuta la peculiare ed unica posizione del Regno Unito: il trascorso da Stato membro dell'UE aveva comportato il recepimento nell'ordinamento inglese delle Direttive in materia di protezione dei dati, così come la diretta applicazione del GDPR sino alla conclusione del periodo di transizione; il legislatore inglese inoltre aveva adottato in tempi recenti una normativa, il *Data Protection Act 2018* [70], volta a "trasferire" la disciplina del Reg. UE 2016/679 in una fonte primaria interna e a sopperire dunque alla perdita di vincolatività del diritto dell'UE e del GDPR stesso al termine del percorso di recesso. Se queste particolari caratteristiche del Regno Unito facevano ottimisticamente propendere per la possibilità di adottare in tempi più celeri e con minori difficoltà una decisione di adeguatezza [71], dall'altro lato il GEPD evidenziava come «any

---

2017, p. 354 ss.; A.D. VANBERG, M. MAUNICK, *Data protection in the UK post-Brexit: the only certainty is uncertainty*, in *International Review of Law, Computers and Technology*, 1, 2018, p. 190 ss.

[69] GEPD, *Opinion 2/2020 on the opening of negotiations for a new partnership with the UK*, 24 febbraio 2020.

[70] Il *Data Protection Act* ha ottenuto il *Royal Assent* il 23 maggio 2018. Come si legge nelle *Explanatory Notes*, questa normativa «helps prepare the UK for a future outside the EU. The new Act replaces the 1998 Act to provide a comprehensive legal framework for data protection in the UK, in accordance with the General Data Protection Regulation (EU) 2016/679)». Per una analisi più dettagliata: L. WOODS, *UK: heading towards Brexit but with Data Protection Bill implementing GDPR*, in *European Data Protection Law Review*, 3, 2017, p. 500 ss.

[71] Lo stesso Primo Ministero Boris Johnson aveva messo in luce le peculiari caratteristiche del regime di protezione dei dati vigente nel Regno Unito, dovute proprio alla previa appartenenza all'UE; da ciò derivava l'auspicio di una procedura rapida e snella

substantial deviation that would result in lowering the level of protection would constitute an important obstacle to a finding of adequacy»[72], rilevando la necessità di svolgere comunque una profonda e seria riflessione sul livello di protezione offerto dal Regno Unito, che avrebbe dovuto necessariamente andare oltre la mera analisi delle tutele fornite dal *Data Protection Act 2018*. Uno degli ulteriori aspetti sui quali, infatti, la Commissione avrebbe dovuto, a parere del Garante, prestare particolare attenzione era da individuarsi nella disciplina del IPA e dunque nelle garanzie stabilite dalla normativa inglese in materia di raccolta, conservazione e accesso da parte della autorità pubbliche ai dati o metadati derivanti da servizi di telecomunicazioni, ottenuti direttamente mediante sistemi di sorveglianza da parte di agenzie di intelligence oppure conservati da soggetti privati. Proprio questo specifico profilo era parso sin da subito piuttosto problematico: non erano mancate perplessità e timori quanto alla sostanziale equivalenza della disciplina nazionale rispetto al livello di tutela e alle salvaguardie imposte dal diritto dell'UE e dalla consolidata giurisprudenza della CGUE in materia, soprattutto con riferimento alla possibilità di utilizzare forme di *bulk acquisition* o *bulk retention* nonché di trasferire dati, anche provenienti dall'UE, ad autorità pubbliche di ulteriori Stati terzi (*data sharing*). Tali dubbi si erano peraltro acuiti in seguito alla stipula dell'*Agreement on Access to Electronic Data for the Purpose of Countering Serious Crime*, siglato tra Regno Unito e USA in data 3 ottobre 2019, finalizzato a regolare il trasferimento di dati e la possibilità di accesso ad essi da parte di autorità di *law enforcement* inglesi e statunitensi, per scopi securitari[73].

Anche il Parlamento europeo, con *Risoluzione sulla Proposta di manda-*

---

di riconoscimento dell'adeguatezza del livello di protezione garantito Oltremanica (*Statement n. UIN HCWS86* del 3 febbraio 2020).

[72] GEPD, *Opinion 2/2020*, cit., p. 10.

[73] Sul punto, anche il Comitato europeo per la protezione dei dati (CEPD) aveva indirizzato una lettera al Parlamento europeo: «when it comes to a possible adequacy decision for the UK, the EDPB considers that the agreement concluded between the UK and the US will have to be taken into account by the European Commission in its overall assessment of the level of protection of personal data in the UK, in particular as regards the requirement to ensure continuity of protection in case of "onward transfers" from the UK to another third country», doc. OUT 2020-0054 del 15 giugno 2020.

to per i negoziati per un un nuovo partenariato con il Regno Unito di Gran Bretagna e Irlanda del Nord (2020/2557(RSP)) del 12 febbraio 2021, aveva messo in evidenza i delicati risvolti della procedura di *Brexit* con riferimento alla disciplina della *data protection*, ribadendo con forza l'importanza di considerare attentamente la disciplina della conservazione e accesso ai metadati per scopi di lotta alla criminalità. Proprio dall'analisi di tale normativa, il Parlamento giungeva alla significativa conclusione secondo cui «il quadro giuridico del Regno Unito relativo alla conservazione dei dati sulle telecomunicazioni elettroniche non soddisfi le condizioni del pertinente *acquis* dell'UE così come interpretato dalla CGUE, e non possa essere pertanto considerato attualmente adeguato», para. 32. La disciplina in materia di *data retention* si rivelava dunque, alla luce delle analisi sopra richiamate, un aspetto estremamente problematico, capace di insidiare seriamente il raggiungimento di una decisione di adeguatezza[74].

[74] Perplessità e timori che proprio l'IPA potesse rappresentare un ostacolo all'ottenimento di una decisione di adeguatezza erano stati espressi, sin dall'inizio del percorso di *Brexit*, anche dallo stesso Parlamento del Regno Unito. Nel Report disposto dal *European Committee della House of Lords* (*Brexit: trade in non-financial services. 18th Report of Session 2016/2017*, HL Paper 35, 22 marzo 2017), si legge come «Preserving the free flow of data across borders is seen by industry as critical to the future of UK digital services. An 'adequacy decision' by the European Commission, recognising that the UK had adequate data protection standards (as well as reciprocal arrangements), would be needed to preserve this flow of data. We note concerns that certain provisions of the Investigatory Powers Act 2016, relating to the collection and storage of personal data by security services, could stand in the way of the Commission granting such a decision», para. 159. Della stessa opinione, in quel periodo, era anche parte della dottrina: «even if the UK Government adopts standards similar or equivalent to the GDPR, there is still no clarity as to the future of the relationship between UK and the EU. Securing and adequacy decision from the EC could be difficult for the UK in the light of the current case law coupled with the extensive surveillance law in the UK such as the recently introduced IPA», così A. VANBERG, M. MAUNICK, *Data protection in the UK post-Brexit: the only certainty is uncertainty*, cit., p. 202. Sebbene queste considerazioni fossero risalenti ad un periodo antecedente alle modifiche apportate nel 2018 al testo legislativo dell'IPA, i dubbi che nei precedenti paragrafi sono stati sottolineati con riferimento alla situazione vigente inducono comunque a riflettere sull'impatto della disciplina inglese in materia di *data retention* nella valutazione sulla sostanziale equivalenza delle tutele disposte.

Anche sulla spinta dei rilevati timori e perplessità emersi nel corso del dibattito *post-Brexit*, il 24 dicembre 2020 veniva approvato l'*Accordo sugli scambi e la cooperazione tra l'UE e il Regno Unito*, entrato in vigore il 1 gennaio 2021: tale documento introduceva un'ulteriore disciplina provvisoria in materia di *data transfer*. Per un periodo massimo di sei mesi, dunque fino al 30 giugno 2021, infatti, «la trasmissione di dati personali dall'Unione al Regno Unito non è considerata un trasferimento a un paese terzo ai sensi del diritto dell'Unione, a condizione che si applichi la normativa del Regno Unito in materia di protezione dei dati al 31 dicembre 2020, quale mantenuta e integrata nel diritto del Regno Unito dalla legge *European Union (Withdrawal) Act 2018* e modificata dalla legge *Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019* ("regime di protezione dei dati applicabile")», art. FINPROV.10-*bis*. Veniva così approvata l'ennesima disposizione mitigatrice degli altrimenti complessi e onerosi effetti legati alla procedura di *Brexit*, concedendo alla Commissione un ulteriore periodo di tempo per valutare la sostanziale equivalenza delle tutele garantite Oltremanica ed addivenire alla auspicata ma discussa decisione di adeguatezza.

5.2. *L'auspicata – e criticata – decisione di adeguatezza del 28 giugno 2021: un instabile destino per il trasferimento dati Oltremanica?*

Sfruttando così l'ulteriore disciplina transitoria e riconoscendo la priorità di un sicuro mantenimento del flusso di dati con il Regno Unito, il 19 febbraio 2021 la Commissione europea pubblicava la bozza di decisione di adeguatezza: in questo importante documento, veniva affermata in maniera netta e incondizionata la sostanziale equivalenza del livello di protezione dei dati assicurato dall'ordinamento inglese, inteso nel suo complesso, dunque anche con riferimento alle norme in materia di conservazione e accesso per scopi securitari ai metadati trasferiti dall'UE. Queste considerazioni risultavano invero piuttosto inaspettate, anche alla luce di quelle puntuali osservazioni di senso opposto che in precedenza altre autorità ed Istituzioni europee avevano espresso. Così, tenendo conto anche dei principi emersi dall'attento vaglio promosso dalla CGUE nella sentenza *Schrems II*, il CEPD, chiamato dalla Commissione stessa a rendere un proprio parere sulla bozza di decisione presentata, si era e-

spresso nuovamente in termini piuttosto critici. Nel Parere 14/2021[75] grande attenzione era stata rivolta ancora una volta alla disciplina della *data retention* e dell'accesso ai dati e metadati da parte delle autorità di *law enforcement* o di intelligence: sotto questo profilo il Comitato aveva sì rilevato taluni aspetti positivi, quali la funzione di controllo garantita dal sistema di *double-lock* o dalla figura del *Judicial Commissioner*, ma aveva anche sottolineato alcuni aspetti problematici e meritevoli di ulteriore attenta analisi da parte della Commissione. Tra questi vi erano la disciplina eccezionale che consente alle autorità pubbliche di provvedere, in casi di urgenza, ad intercettazione o acquisizione di metadati senza la previa approvazione dell'*Investigatory Powers Commissioner* o del *Judicial Commissioner*; la possibilità di trasferire dati e metadati, anche provenienti dall'UE, a Stati terzi per finalità securitarie; o ancora, «the EDPB considers that there is a need for further clarification and assessment of bulk interceptions, in particular on the selection and application of the selectors, in order to clarify the extent to which access to personal data meets the threshold set by the CJEU and which safeguards are in place to protect the fundamental rights of individuals whose data are intercepted in this context, including concerning the retention periods of data», para. 29.

Similmente, anche il Parlamento europeo esprimeva parere negativo sulla bozza di decisione di adeguatezza[76]. Non stupisce come, ancora una volta, uno degli elementi maggiormente critici rilevati fosse rappresentato proprio dagli strumenti di sorveglianza di massa[77] e dalla normativa IPA

---

[75] CEPD, *Opinion 14/2021 regarding the European Commission Draft Implementing Decision pursuant to Regulation (EU) 2016/679 on the adequate protection of personal data in the United Kingdom*, 13 aprile 2021.

[76] Si fa riferimento alla *Risoluzione sull'adeguata protezione dei dati personali da parte del Regno Unito*, 2021/2594(RSP), 21 maggio 2021.

[77] Nella Risoluzione, il Parlamento dedica grande attenzione ai sistemi di sorveglianza vigenti nell'ordinamento inglese, ritenendo particolarmente problematici alcuni interessanti profili: «l'ICO o gli organi giurisdizionali non effettuano un controllo sostanziale efficace sul ricorso all'esenzione per la sicurezza nazionale prevista dalla legislazione del Regno Unito relativa alla protezione dei dati; le restrizioni di utilizzo dei poteri su dati in blocco da parte del Regno Unito non sono previste dalla legge stessa, come richiesto dalla CGUE (ma sono invece lasciate alla discrezione dell'esecutivo soggetta a un "rispettoso" controllo giurisdizionale); la descrizione di "dati secondari" (metadati) nei

in particolare; pur riconoscendo le importanti tutele introdotte dalla disciplina inglese vigente sotto il profilo dei controlli, soprattutto nella fase di accesso, il Parlamento, con una affermazione di grande forza, dichiarava di deplorare «il fatto che l'IPA continui a consentire la pratica conservazione in blocco dei dati», para. 27. Quanto sostenuto da Governo e *High Court* inglese, che, come si è visto nei previ paragrafi, negavano con decisione la possibilità da parte del *Secretary of State* di autorizzare forme di conservazione generalizzata, ritenute impraticabili grazie alle restrizioni e specifiche condizioni introdotte dall'IPA e dalla successiva modifica alla stessa, veniva pertanto smentito dalla valutazione del Parlamento, che attestava invece la persistente sussistenza – o quantomeno la pratica possibilità – di simili pericolosi sistemi di *data retention*. A seguito di tali considerazioni, la Commissione veniva pertanto invitata a modificare il progetto di decisione, ritenuto non conforme al diritto dell'UE: le criticità evidenziate dovevano essere affrontate quale presupposto necessario per l'adozione di una decisione di adeguatezza legittima e in grado di superare illesa il vaglio dei giudici di Lussemburgo. Sul punto, il riferimento alle precedenti negative vicende giurisprudenziali in materia appare lampante: il monito rivolto alla Commissione era quello di «imparare dai suoi errori del passato prestando attenzione agli inviti del Parlamento e degli esperti (...) e a non lasciare che sia la CGUE, sulla base delle denunce presentate dai singoli, ad occuparsi dell'adeguata applicazione della legislazione dell'UE in materia di protezione dei dati», para. 40.

---

progetti di decisione è gravemente fuorviante e non precisa che tali dati possono contenere molte informazioni ed essere altamente invasivi, e che sono soggetti a sofisticate analisi automatizzate (come dichiarato dalla CGUE nella causa *Digital Rights Ireland*) ma che tuttavia, ai sensi della legislazione britannica, i metadati non sono adeguatamente protetti dall'accesso indebito, dalla raccolta in blocco e dall'analisi basata sull'intelligenza artificiale da parte delle agenzie di intelligence del Regno Unito; le "*Five Eyes Agencies*" [un'alleanza tra le agenzie di intelligence di Regno Unito, USA, Canada, Nuova Zelanda e Australia, volta a facilitare lo scambio di informazioni], in particolare il GCHQ e la NSA, condividono nella pratica tutti i dati di intelligence», para. 16. Il Parlamento, sulla base di tali critiche considerazioni, «invita la Commissione a utilizzare i suoi scambi con le controparti britanniche per trasmettere il messaggio che, se le leggi e le pratiche di sorveglianza del Regno Unito non verranno modificate, l'unica opzione percorribile per facilitare le decisioni di adeguatezza sarebbe la conclusione di accordi di "non spionaggio" con gli Stati membri», para. 17.

Nonostante le opinioni – pur non vincolanti – espresse dal CEPD e dal Parlamento, nonché le critiche avanzate da molti commentatori ed esperti[78], la Commissione ha però mantenuto pressoché invariata la bozza, adottando, come anticipato, una decisione di adeguatezza nel giugno 2021, a pochi giorni dalla scadenza della disciplina transitoria. Dopo la riproposizione della lunga analisi della normativa inglese, la Commissione è infatti giunta a concludere che «any interference with the fundamental rights of the individuals whose personal data are transferred from the EU to the UK by UK public authorities for public interests purposes, in particular law enforcement and national security purposes, will be limited to what is strictly necessary to achieve the legitimate objective in question and that effective legal protection against such interferences exists», para. 275.

[78] Si richiama, a titolo esemplificativo, quanto affermato da Burns a seguito della sentenza *Schrems II*: «if you send EU data to the UK, I would strongly advise securing standard contractual clauses ahead of the Brexit transition deadline. You can no longer assume the UK will be granted data protection adequacy», H. BURNS, *What the Schrems II ruling means for Brexit*, in *AfterBrexit Blog*, 16 luglio 2020; ma anche Korff e Brow, che avevano rilevato come, sulla base della normativa inglese in materia di *data sharing*, «the adoption of the decision would lead to serious risks that the UK will become a data protection-evasion haven for personal data from the EU/EEA to countries that are not held to provide adequate protection by the EU; that the UK will allow for undue direct access to data (including data on EU persons) by US authorities under the UK-US Agreement», oltre a sottolineare come la bozza «completely fails to assess (or even note) the UK's intelligence agencies'actual surveillance practices», D. KORFF, I. BROWN, *The inadequacy of the EU Commission's draft GDPR adequacy decision on the UK*, in *Data protection and digital competition Blog*, 3 marzo 2021. Similmente, dello stesso avviso critico, anche: J. SAJFERT, *Bulk data interception/retention judgements of the CJEU. A victory and a defeat for privacy*, in *European Law Blog*, 26 ottobre 2020; E. CELESTE, *Cross-border data protection after Brexit*, in *Brexit Institute Working Paper Series*, 4, 2021, p. 1 ss.; O. LYNSKEY, *The extraterritorial impact of data protection law through an EU law lens*, in F. FABBRINI, E. CELESTE, J. QUINN (a cura di), *Data protection beyond borders: transatlantic perspectives on extraterritoriality and sovereignity*, Hart, Londra, 2021, p. 191 ss.; H. PEARCE, *Brexit-update: UK-EU data transfers in anticipation of an adequacy decision*, in *University of Portsmouth Blog*, 9 marzo 2021. Per completezza, è bene però riportare come si siano registrate anche opinioni divergenti di studiosi che hanno invece ritenuto la valutazione di adeguatezza operata dalla Commissione in grado di sostenere illesa il vaglio della CGUE (sul punto L. WOODS, *Data protection, the UK and the EU: the draft adequacy decisions*, in *EU Law Analysis*, 24 febbraio 2021).

Questa attesa decisione, favorevolmente accolta dagli operatori economici quotidianamente impegnati in operazioni di *data transfer* con il Regno Unito nonché dalla numerose aziende che Oltremanica fondano le proprie attività sull'impiego dei dati provenienti dall'UE, pare comunque non potersi considerare un granitico e solido punto di arrivo: innanzitutto, piuttosto singolarmente, il documento presenta una *sunset clause* che ne fissa la scadenza al 27 giugno 2025 [79], oltre a prevedere l'obbligo di costante monitoraggio e controllo da parte della Commissione di qualsiasi mutamento nella disciplina inglese che possa incidere sulla valutazione di adeguatezza; inoltre, le perplessità e le criticità già da tempo espresse e qui ampiamente sottolineate quanto alla sostanziale equivalenza del livello di protezione dei dati fornito Oltremanica, soprattutto con riferimento ai sistemi di sorveglianza per scopi securitari, hanno già posto in rilievo l'instabilità e l'incerto destino di tale decisione, che potrebbe pericolosamente seguire la stessa sorte dell'omologa riguardante il flusso di dati con gli USA. Vi è già infatti chi ritiene altamente probabile un ricorso dinnanzi alla CGUE, sulla scia di quanto già avvenuto nel caso *Schrems* [80], facilitato anche delle attività di controllo che le Autorità ga-

[79] La scelta di introdurre questa scadenza rappresenta un profilo innovativo e di rilievo, soprattutto se si considera che il GDPR, all'art. 45, co. 3, già prevede un obbligo di monitoraggio e riesame continuo circa la persistenza del livello adeguato di protezione fornito dallo Stato terzo beneficiario di una decisione di adeguatezza. Per questo motivo, la scelta di indicare una scadenza vera e propria della decisione stessa è stata ritenuta da Woods una risposta al timore che il legislatore britannico possa, nei prossimi anni, modificare in senso meno garantista la disciplina nazionale in materia di protezione dei dati (L. WOODS, *Data protection, the UK and the EU: the draft adequacy decisions*, cit.).

[80] Si legga sul punto quanto chiaramente scritto da Celeste, poco prima dell'adozione della Decisione di adeguatezza da parte della Commissione: «In conclusion, the UK adequacy decision is subject to a time bomb. Over the past few years, the case law of the CJEU has become more solid and clear in relation to the incompatibility of various practices adopted by national security authorities involving personal data. This makes the general EU-UK data transfer mechanism based on the adequacy decision unstable and unreliable. If, once again, the EU Commission finds a way to reach a compromise between commercial interests and fundamental rights, it is only a question of time before the CJEU will intervene. (…) The likelihood is high that the CJEU will soon again 'put asunder' what the EU Commission has 'joined together' in the name of

ranti nazionali sono tenute ad operare in materia di *data transfer*.

Anche sul fronte della garanzia di un continuo e stabile flusso di dati tra UE e Regno Unito, dunque, tanto le future scelte del legislatore inglese in materia di conservazione e trattamento di dati e metadati a fini di garanzia della sicurezza quanto le pronunce delle Corti inglesi assumeranno rilievo fondamentale. Così, una certa interdipendenza ed influenza reciproca tra le due sponte della Manica, è destinata a persistere anche a seguito della *Brexit*: da un lato Commissione europea e Autorità garanti nazionali e sovranazionali dovranno osservare con attenzione quanto avverrà nel Regno Unito sul fronte della *data protection* allo scopo di verificare la sussistenza dell'adeguatezza delle tutele; dall'altro, anche Governo, Parlamento e Corti inglesi dovranno continuare a seguire le prossime pronunce della CGUE e la possibile evoluzione della normativa dell'UE in materia di *data retention*: questi infatti saranno punti di riferimento di estrema importanza per determinare il livello di garanzia dei diritti alla riservatezza e alla *data protection* assicurato nel territorio dell'UE, che funge, come si è visto, da fondamentale parametro per la determinazione dell'adeguatezza delle tutele offerte dallo Stato terzo ricevente [81]. La spada

---

EU trade», in E. CELESTE, *Cross-border data protection after Brexit*, cit., p. 13. Nel caso in cui l'eventuale – ma probabile – vaglio della CGUE si concludesse con una invalidazione della decisione di adeguatezza, ciò potrebbe indurre ad un ulteriore intervento di riforma della disciplina vigente nella direzione di una introduzione di maggiori salvaguardie, come già gli USA avevano tentato di fare a seguito della prima sentenza *Schrems*. Svolgere previsioni su tale punto risulta però al momento operazione piuttosto ardua: da un lato si è visto come, con riferimento alla disciplina inglese vigente in materia di *data retention* e accesso ai metadati, sussistano visioni divergenti quanto alla compatibilità con i principi delineati dai giudici di Lussemburgo nelle più recenti pronunce; dall'altro, è difficile prevedere se e come il legislatore Oltremanica possa agire dinnanzi ad una potenziale decisione avversa della CGUE in materia di *data transfer*: pur riconoscendo l'importanza – anche economica – di una decisione di adeguatezza, il Regno Unito potrebbe comunque ritenere irriformabili i propri sistemi di sorveglianza, non inserendo dunque quelle modifiche altrimenti necessarie per ottenere una valutazione di sostanziale equivalenza stabile e "resistente" al controllo dei giudici europei.

[81] Sotto questo profilo, dunque, proprio la volontà – se non necessità, anche economica – di ottenere una riconferma della decisione di adeguatezza e dei suoi vantaggiosi effetti per un semplice e rapido trasferimento dei dati, ben potrebbe rappresentare una virtuosa spinta verso il mantenimento di elevati livelli di tutela della protezione dei dati

di Damocle del possibile ripetersi della *Schrems saga*, questa volta con accento britannico, continua dunque a pendere minacciosa tanto sulle Istituzioni europee quanto su quelle inglesi.

Una situazione, quella *post-Brexit*, che si rivela, in conclusione, ancora fortemente dibattuta ed incerta: futuri sviluppi su entrambi i fronti potrebbero significativamente incidere sulla continuità del trasferimento dati e sui rapporti – anche economici – tra UE e Regno Unito.

nel Regno Unito anche successivamente alla procedura di *Brexit*. In altre parole, come già evidenziato con riferimento alle vicende che hanno interessato gli USA, l'ormai irrinunciabile sistema di *data transfer* oltre i confini dell'UE e il beneficio di una decisione di adeguatezza potrebbero rappresentare il grimaldello per l'ottenimento di un condiviso e più elevato standard di garanzia dei diritti fondamentali. Questo profilo, tuttavia, rimane altamente dibattuto e criticato, come si è ampiamente rilevato nel Capitolo 3, cui si rimanda per più generali osservazioni sull'efficacia dello strumento della decisione di adeguatezza.

CAPITOLO 5

IL BELGIO. DALLA *COUR CONSTITUTIONNELLE* AL LEGISLATORE NAZIONALE, PASSANDO PER LUSSEMBURGO

SOMMARIO: 1. L'iniziale approccio "pro-securitario" del legislatore belga in materia di *data retention* e i primi dubbi sulla proporzionalità di una conservazione generalizzata. – 2. La *Cour constitutionnelle* annulla la normativa nazionale sulla conservazione dei metadati: l'unicità dell'*Arrêt* 11 giugno 2015, n. 84. – 3. La *Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques*. – 3.1. La necessaria adozione di una nuova normativa sulla conservazione e accesso ai metadati: il complesso dibattito emerso dai *Travaux préparatoires*. – 3.2. Un difficile compromesso tra efficienza ed elevata tutela dei diritti alla riservatezza e protezione dei dati. – 4. L'ulteriore intervento della *Cour constitutionnelle* e il dialogo con la CGUE: andata e ritorno. – 4.1. Il ricorso di annullamento avverso la legge del 2016: le contrastanti letture della giurisprudenza della CGUE promosse da Governo e ricorrenti. – 4.2. L'*Arrêt interlocutoire* 19 luglio 2018, n. 96: un necessario chiarimento quanto alla cumulativa sussistenza dei requisiti fissati a livello europeo. – 4.3. Di ritorno da Lussemburgo: la decisa risposta dei giudici costituzionali nell'*Arrêt* 22 aprile 2021, n. 57. – 4.4. Ancora una difficile prova per il legislatore belga: cenni all'*Avant-project de loi* proposto dal Governo. – 5. Un approfondito dibattito legislativo e una attenta considerazione dei criteri enunciati dalla giurisprudenza della CGUE: ingredienti per un approccio virtuoso o per un fallimento annunciato?

1. *L'iniziale approccio "pro-securitario" del legislatore belga in materia di* data retention *e i primi dubbi sulla proporzionalità di una conservazione generalizzata.*

Il legislatore e i giudici costituzionali belgi hanno affrontato con grande attenzione e approfondito dibattito la complessa sfida della adozione di una adeguata disciplina in materia di *data retention*. L'avvicendarsi delle pronunce della CGUE hanno infatti rivelato nel contesto belga i propri rilevanti e dirompenti effetti, tanto sotto il profilo legislativo quanto giurisprudenziale. Tali ripercussioni sono ancora oggi pienamente visibili se si considera il difficile tentativo, in atto, di addivenire alla predisposizione di una disciplina nazionale sulla conservazione e accesso ai metadati che possa dirsi compatibile con il diritto dell'UE e superare illesa il rigido vaglio dei giudici costituzionali, ormai più volte intervenuti. Al fine di comprendere appieno il peculiare approccio che caratterizza le decisioni del legislatore e delle Corti belghe e che lo distingue da quanto registratosi in altri Stati membri quali Regno Unito e Italia, è necessario innanzitutto procedere con la ricostruzione dell'evoluzione normativa in materia, mettendone in evidenza così il forte intreccio con le vicende giurisprudenziali tanto nazionali quanto sovranazionali.

Il primo obbligo di conservazione dei metadati imposto dallo Stato belga in capo agli operatori di servizi di telecomunicazione è da individuarsi già nell'anno 2000, in particolare con la legge 28 novembre 2000 [1] che modificava la previa legge 21 marzo 1991 [2]: dinnanzi all'aumentare di reati legati al mondo digitale e delle telecomunicazioni, perpetrati mediante l'impiego di Internet o di servizi di telefonia, la normativa richiamata era intervenuta in materia penale e di procedura penale allo scopo di adattare a tale contesto le disposizioni esistenti e di inserirne di nuove [3]. Ai fornitori di mezzi di comunicazione elettronica veniva così impo-

---

[1] *Loi du 28 novembre 2000 relative à la criminalité informatique, M.B., 3 février 2001, p. 02909.*

[2] *Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, M.B., 27 mars 1991, p. 6155.*

[3] Per una analisi dettagliata dei reati introdotti da tale normativa, tutti legati al progresso tecnologico e all'affermarsi dell'utilizzo massiccio di sistemi di telecomunicazio-

sto di conservare i dati relativi alle chiamate nonché i dati identificativi degli utenti per un periodo minimo di dodici mesi. Questa disposizione prevedeva tuttavia che la determinazione esatta dei dati da sottoporre a *retention* nonché delle diverse tempistiche di conservazione fosse predisposta da un *arrêté royal* (regio decreto), elaborato dal Governo a livello federale e poi formalmente emanato dal Re. La scelta di lasciare esclusivamente nelle mani del potere esecutivo la definizione di aspetti così rilevanti – quali la specifica durata della conservazione e i dati interessati –, in grado di incidere in maniera significativa sulla portata dell'ingerenza nella sfera privata, era stata però oggetto di forti critiche e preoccupazioni espresse peraltro dalla *Commission de la protection de la vie privée*[4] nel

ne, si rimanda a F. DE VILLENFAGNE, S. DUSSOLIER, *La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique*, in *A&M*, 1, 2001, p. 71 ss.

[4] La *Commission de la protection de la vie privée* era stata istituita con *Loi 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (*M.B. 18 mars 1993*). A tale autorità pubblica indipendente era stato attribuito il compito di vigilanza quanto al rispetto dei diritti alla vita privata e alla protezione dei dati, oltre alla funzione di controllo, nel territorio nazionale, circa la corretta applicazione delle disposizioni di attuazione della Direttiva 95/46/CE – questa normativa europea infatti imponeva all'art. 28 la creazione, presso ciascuno Stato membro, di una apposita autorità statale indipendente di controllo –. La *Commission* è rimasta operativa sino al 2017, quando la *Loi 3 décembre 2017portant création de l'Autorité de protection des données* ha provveduto alla istituzione presso la *Chambre des Représentants* della *Autorité de protection des données* che ha sostituito la *Commission* quale organo di controllo indipendente (per approfondimenti si legga N. RAGHENO, *Data protection: la future nouvelle Autorité dee protection des données*, in *Cahier du Juriste*, 2, 2017, p. 29). Con riferimento alla funzione e composizione della *Commission de la protection de la vie privée*, la cui opinione sulle normative in materia di *data retention* verrà più volte richiamata nel corso di questa analisi, si rimanda, *ex multis*, a E. DEGRAVE, *La Commission de la protection de la vie privée: l'Autorité de régulation du secteur des traitements de données à caractère personnel*, in *Revue du Centre d'étude et de recherches en administration publique*, 26, 2016, pp. 37-70. Per completezza, merita sottolineare infine come la *Loi 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel* abbia attribuito al *Comité permanent de controle des services des reinsegnement* il compito specifico di vigilare sul rispetto da parte dei servizi di intelligence (*Service général du renseignement*) delle norme – nazionali ed europee – in materia di privacy e protezione dei dati, laddove tali autorità pongano in essere trattamenti dei dati nell'ambito di attività di garanzia della sicurezza nazionale (art. 95). Il *Comité* (c.d.

Doc. parl. Chambre 0213/004 [5]. Come osservato anche dalla dottrina, la vaghezza del dettato normativo, la carenza di precisi limiti e salvaguardie e la discrezionalità lasciata all'organo esecutivo rischiavano di facilitare l'affermarsi di un sistema di "sorveglianza esplorativa" nelle mani delle autorità pubbliche, capace di inficiare fortemente il corretto godimento del diritto alla riservatezza [6] e finanche il rapporto tra potere pubblico e cittadini [7].

Comité R) è un organo pubblico permanente ed indipendente, istituito con legge del 18 luglio 1991 e il cui ruolo e composizione è stato poi inserito nella legge organica *30 novembre 1998 des services de renseignement et de sécurité*.

[5] *Doc. Parl. Chambre*, 1999-2000, 0213/011. In tale documento si legge come: «Le projet de loi belge ne contient aucune indication relative aux personnes susceptibles de faire l'objet de cette mesure de surveillance, aux circonstances dans lesquelles elle peut être ordonnée, aux moyens à employer ou aux procédures à observer. Il semble donc que l'article 14 du projet de loi belge relatif à la criminalité informatique ne pourrait pas être considéré comme suffisamment clair et détaillé pour assurer une protection appropriée contre les ingérences des autorités dans le droit des citoyens au respect de leur vie privée et à la confidentialité de leurs communications. La Commission est en outre préoccupée par le fait que le projet de loi puisse être disproportionné et onéreux de façon non nécessaire à charge des opérateurs», p. 18.

[6] L'art. 22 della Costituzione belga del 1994 stabilisce che: «Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi. La loi, le décret ou la règle visée à l'article 134 garantissent la protection de ce droit». Viene dunque tutelato il diritto alla vita privata nella sua accezione più classica, inteso come «protéger l'individu contre les excès de pouvoir de l'autorité publique, mais également de lui permettre de développer librement et pleinement sa personnalité, ses relations avec ses semblables, le tout dans une perspective d'autonomie individuelle». B. DOCQUIR, *Droit du numérique*, Larcier, Bruxelles, 2018, p. 347. Pur non prevedendo una specifica ed autonoma disposizione in materia di protezione dei dati, come invece stabilito nella Carta di Nizza, la giurisprudenza belga ha avuto modo di chiarire come il diritto tutelato all'art. 22 del testo costituzionale comprenda al suo interno anche il diritto alla protezione dei dati personali. In una recente decisione della Corte costituzionale (*Arrêt n. 29/2018*) viene espresso, infatti, con grande chiarezza, come «le droit au respect de la vie privée, tel qu'il est garanti par les dispositions constitutionnelles et conventionnelles précitées, a pour but essentiel de protéger les personnes contre les ingérences dans leur vie privée. Ce droit a une portée étendue et englobe notamment la protection des données à caractère personnel et des informations personnelles», para. B.11. Oltre alla Costituzione, tale diritto viene tutelato da una pluralità di normative settoriali e specifiche, tra cui la *Loi 8 décembre 1992 relative à la protection de la vie privée à l'égard des traite-*

A distanza di pochi anni e in un clima di forte paura caratterizzante il primo decennio del XXI secolo, scandito dagli attentati terroristici negli Stati Uniti d'America nel 2001 e nell'Unione europea stessa nel 2004, il legislatore belga decideva di intervenire nuovamente sulla regolamentazione delle comunicazioni elettroniche, risentendo anche della spinta marcatamente pro-securiataria proveniente dal rinnovato dibattito a livello europeo. Così la legge del 13 giugno 2005 relativa alle comunicazioni elettroniche [8], dando attuazione alla facoltà derogatoria concessa dall'art. 15 Direttiva *e-Privacy*, stabiliva all'art. 126, co. 3 l'obbligo di conservazione dei metadati nonché dei dati identificativi di tutti gli utenti di servizi di telecomunicazione, per un periodo compreso tra i dodici e i trentasei mesi e per scopi estremamente ampi, individuati nella: «investigation and prosecution of criminal acts, for the tracking of malicious calls to emergency services and to enable the research of the Ombudsman for Telecommunications in revealing the identity of people making improper use of electronic communications services or networks» [9]. Similmente alle disposizioni del 2000, anche questa disciplina, dai contorni estremamente vaghi e che demandava ad un regio decreto la determinazione di alcuni specifici aspetti, era stata accolta negativamente da parte della

ments de données à caractère personnel, più volte modificata e adeguata al progredire della tecnologia, all'evolvere delle minacce e al susseguirsi delle normative europee in materia. Per una ampia ricostruzione del tema si rimanda a K. LEMMENS, *Respect de la vie privée et de la personnalité*, in M. VERDUSSEN, N. BONBLED (a cura di), *Les droits constitutionnels en Belgique*, Bruylant, Bruxelles, 2011, pp. 901-931 e nello stesso Volume, E. DEGRAVE, Y. POULLET, *Le droit au respect de la vie privée face aux nouvelles technologies*, pp. 1001-1035 ; SERVICE DE RECHERCHE DU PARLEMENT EUROPÉEN, *Le droit au respect de la vie privée: les défis digitaux, une perspective de droit comparé. Belgique*, Bruxelles, 2018 ; C. DE TERWANGNE, E. DEGRAVE (a cura di), *La protection des données à caractère personnel en Belgique: manuel de base*, Politeia, Bruxelles, 2019.

[7] Poullet, leggendo criticamente la normative belga, ha sottolineato come «there is no worse danger than this cyber-surveillance, which hunts a man down in his most intimate space and raises within him a perpetual and haunting fear of exposure», Y. POULLET, *The fight against crime and/or the protection of privacy: a thorny debate!*, in *International Review of Law, Computers and Technology*, 2, 2004, p. 264.

[8] *Loi du 13 juin 2005 relatives aux communications électroniques, M.B., 20 juin 2005*.

[9] E. KOSTA, P. VALCKE, *Retaining the data retention directive*, in *Computer law and Security Report*, 22, 2006, p. 377.

Commission de la protection de la vie privée; quest'ultima aveva in particolare mostrato, per la prima volta, dubbi quanto alla compatibilità con i diritti fondamentali dello strumento della *data retention*, considerato *per se* e dunque nella sua natura di misura preventiva, slegata cioè dalla presenza di una indagine penale in corso tale da giustificare l'ingerenza nella sfera privata [10].

È importante evidenziare, tuttavia, come le discusse disposizioni introdotte nel 2000 e nel 2005, non divennero mai operative: non vennero mai approvati, infatti, i relativi regi decreti che, essendo chiamati a determinare le categorie di dati da sottoporre a conservazione, la durata della conservazione stessa e le condizioni circa la *data security* da garantire nel periodo di *data retention*, risultavano imprescindibili strumenti per la concreta attuazione della disciplina, senza i quali l'obbligo imposto non poteva trovare esecuzione [11].

La *de facto* mancata attuazione della legislazione nazionale in materia di conservazione dei metadati per scopi securitari diveniva poi fortemente problematica a seguito della adozione, a livello dell'UE, della Direttiva 2006/24: questa, come noto, aveva introdotto l'onere in capo agli Stati membri di adottare normative che stabilissero l'obbligo di *data retention* per scopi di repressione e lotta alla criminalità grave, lasciando peraltro ai legislatori nazionali il compito di individuare apposite regole attinenti alla fase di accesso da parte delle autorità di *law enforcement*. Ebbene, proprio nell'articolato percorso di trasposizione di tale normativa europea nell'ordinamento nazionale belga può ravvedersi tutta la complessità della disciplina della *data retention* e la difficoltà di addivenire ad una soluzione normativa condivisa: bisognerà attendere sino al 30 luglio 2013 per vedere l'approvazione di una apposita legge di attuazione della DRD, frutto di un lungo e travagliato procedimento legislativo [12] che, avviatosi

---

[10] *Avis n. 08/2004, 14 juin 2004 sur l'avant-projet de loi relatif aux communiations èlectroniques*.

[11] A. CASSART, J-F. HENROTTE, *L'invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée*, in *Jurisprudence de Liege*, 20, 2014, p. 954.

[12] Tale percorso aveva conosciuto una significativa spinta acceleratrice ad opera della Commissione europea, che nel maggio 2013 aveva intimato al Belgio di adeguare la

all'indomani dell'entrata in vigore della disciplina europea, aveva però incontrato diversi ostacoli e battute d'arresto. Il primo progetto di legge volto alla trasposizione della Direttiva 2006/24 era infatti naufragato nel 2008, dinnanzi al parere negativo espresso dalla *Commission de la protection de la vie privée* (*Avis n. 24/2008 du 2 juillet 2008*). Il testo proposto era stato ritenuto, come già in passato, eccessivamente vago, col rischio di attribuire prerogative e discrezionalità troppo ampie al potere esecutivo, soprattutto con riferimento alle condizioni di accesso ai dati conservati; questi ultimi, nella prima versione proposta, dovevano essere memorizzati da parte dei fornitori di servizi di telecomunicazione per ben due anni – ovvero il termine massimo di durata concesso dalla DRD stessa –: tale scelta non risultava ancorata a nessun appropriato vaglio di necessità né tantomeno ad alcuna valutazione concreta quanto alla reale utilità di una durata così estesa, mentre risultavano mancanti anche appropriate disposizioni sulla sicurezza dei dati conservati. Il secondo progetto di legge, risalente al 2009, aveva mostrato di tenere in debita considerazione le osservazioni che avevano portato al respingimento della previa proposta, limitando la durata di conservazione ad un massimo di dodici mesi e stabilendo la necessità che la durata della *data retention*, variabile a seconda delle categorie di dati interessati, fosse contenuta nella legge e non, come

---

propria disciplina interna all'obbligo di *data retention* imposto a livello sovranazionale: «The European Commission has asked Belgium to bring its laws into line with EU legislation on data retention, after the country failed to inform the Commission of adequate measures to transpose the rules in national law. The Commission's request takes the form of a reasoned opinion (the second step in the three-step EU infringement process). (…) Belgium has failed so far to transpose fully. In particular, the Belgian authorities still need to bring national legislation in line with the EU rules on requiring companies to retain data for between 6 months and 2 years with appropriate data security and data protection safeguards. Belgium now has two months to comply with European Union rules. If Belgium does not comply, the Commission may decide to refer the case to the EU's Court of Justice», Commissione europea, MEMO/13/470 del 30 maggio 2013. Nel Doc. Parl. Chambre, 2012-2013, DOC 53-2921/001, pp. 3-4, sulla legge 30 giugno 2013, veniva parimenti riconosciuto come «Fin septembre 2012, la Commission européenne a mis la Belgique en demeure de transposer la directive et a attiré l'attention de la Belgique sur les sanctions pécuniaires que la Cour de justice pourrait lui infliger pour transposition incomplète de la directive. Il est donc exclu d'attendre encore plus longtemps et, à plus forte raison, d'attendre un amendement éventuel de la directive».

proposto in passato, in un regio decreto, assicurando così la determinazione di tali importanti dettagli al dibattito parlamentare. Pur avendo ottenuto parere positivo da parte della *Commission de la protection de la vie privée* (*Avis n. 20/2009 du 1 juillet 2009*), anche questo progetto di legge aveva però seguito il medesimo destino del suo predecessore, questa volta per ragioni di instabilità politica, a causa della caduta del Governo in carica, il 26 aprile 2010, con il successivo scioglimento del Parlamento e indizione di nuove elezioni [13].

Solo dunque con la legge del 30 luglio 2013 [14], che modificava gli articoli 2, 126 e 145 della richiamata legge 13 giugno 2005 nonché l'articolo 90 *decies* del *Code d'instruction criminelle* (M.B. 23 agosto 2013), la DRD veniva finalmente trasposta nell'ordinamento nazionale. Le disposizioni della legge del 2013 erano poi integrate dall'*Arrêté royal* del 19 settembre 2013, che dava esecuzione all'art. 126 della legge 13 giugno 2005 (M.B. 8 ottobre 2013, n. 70828) [15] e che conteneva indicazioni di grande rilievo per l'attuazione della normativa stessa, determinando ad esempio con precisione la tipologia e la definizione dei dati da conservare, le categorie di servizi di telecomunicazione interessati nonché le misure tecniche ed amministrative che i fornitori di servizi dovevano adottare per garantire un adeguato livello di protezione dei dati conservati.

La normativa del 2013 stabiliva, in sintesi, un obbligo di conservazione di dati di localizzazione, comunicazione e identificazione [16], per una

---

[13] Come sottolineato da C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, in *Journal des Tribunaux*, 13, 2017, p. 237.

[14] *Loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle, M.B., 23 aout 2013, p. 56109.*

[15] Per una analisi approfondita si rimanda a: M. VAN BELLINGHEN, T. ZGAJEWSKI, *Les enjeux de la transposition en Belgique des nouvelles directives européennes sur les communications électroniques*, Academia Press, Gent, 2012, p. 39 ss.

[16] Per dati di localizzazione si intendevano le informazioni relative al luogo dal quale era partita o si era svolta la comunicazione e la durata della stessa; i dati di comunicazione si riferivano invece a quelle informazioni che permettevano di individuare i destinatari di una comunicazione, mentre con dati identificativi si faceva riferimento a quelli che consentivano di identificare i titolari di un numero o di un indirizzo IP, nonché tut-

durata di dodici mesi, pur prevedendo alcune possibili eccezioni in grado di prolungare sensibilmente il periodo di *data retention*: mediante decreto, infatti, poteva essere stabilita una diversa durata di conservazione, non superiore comunque a diciotto mesi, per talune tipologie di dati, nel caso in cui se ne ravvisasse la necessità – senza ulteriori precisazioni o specificazioni volte a definire però come questa "necessità" dovesse intendersi –, mentre nel caso in cui fosse considerato essenziale provvedere ad una conservazione superiore ai ventiquattro mesi, comunque concessa, veniva imposta quale unica condizione la notifica immediata da parte del Governo alla Commissione europea e agli altri Stati membri, accompagnata da una specifica motivazione volta a giustificare l'adozione di tale misura straordinaria. Le finalità perseguite dalla conservazione dei dati e per le quali dunque tali informazioni potevano essere messe a disposizione delle autorità di *law enforcement* erano quelle descritte all'art. 126, co. 2 della legge del 2005, così come modificato dalla legge del 2013: in sostanza si trattava della ricerca, indagine e repressione di reati indicati agli artt. 46-*bis* e 88-*bis* del *Code d'instruction criminelle*, della repressione di chiamate malevole o moleste ai servizi di emergenza; della ricerca dal parte del *Service de médiation pour les télécommunications*[17] dei dati identificativi di coloro che avevano utilizzato in maniera illegale un servizio di telecomunicazione o ancora per scopi di tutela della sicurezza nazionale con riferimento alle attività svolte dalle autorità di intelligence e disciplinate dalla legge organica del 30 novembre 1988.

---

te le utenze aperte da un determinato soggetto e la tipologia di dispositivo sul quale l'utenza era stata attivata.

[17] Riprendendo la definizione che il *Service de médiation* fornisce nel suo sito istituzionale, «Le service de médiation, institué par la loi du 21 mars 1991 auprès de l'IBPT (l'Institut Belge des Services Postaux et des Télécommunications), fonctionne de manière totalement indépendante des opérateurs de télécoms et, dans les limites de ses attributions, ne reçoit d'instruction d'aucune autorité. Tout client mécontent de son opérateur télécoms peut demander l'intervention gratuite du service de médiation. Le médiateur est compétent pour l'ensemble du secteur des télécoms. Le service de médiation est une instance de recours: n'ayant pas pour but de se substituer au service à la clientèle des opérateurs télécoms, il peut agir lorsqu'un client n'a obtenu aucune solution satisfaisante lors de ses contacts avec son fournisseur de télécoms», disponibile all'indirizzo http://www.ombudsmantelecom.be/fr/nos-missions.html?IDC=19.

Sin da questa schematica ricostruzione della disciplina adottata nel 2013 si può ben comprendere come, sotto un profilo prettamente formale, in Belgio non fosse stato adottato un testo unitario, completo ed esaustivo in materia di *data retention* e in trasposizione della DRD, ma anzi si fosse verificata la contemporanea presenza di diversi testi – la normativa e il regio decreto – che peraltro contenevano modifiche alle leggi esistenti, con un continuo rimando ad ulteriori fonti e acuendo così una certa frammentarietà della disciplina, che finiva col complicare il quadro di riferimento di una materia già di per sé difficile [18]. Sotto il profilo sostanziale poi la normativa individuava una grande varietà di autorità legittimate all'accesso, anche diverse da quelle strettamente definibili come autorità di *law enforcement* (si pensi al *Service de médiation pour les télécommunications,* cui era attribuita tale delicata facoltà di accesso), andando così al di là di quanto previsto dalla DRD, che stabiliva quali finalità giustificanti la conservazione e il successivo accesso solo l'indagine, l'accertamento e il perseguimento di reati gravi [19]. Molto similmente a quanto si è detto già con riferimento alle previe discipline normative, anche la legge del 2013 aveva quindi attirato numerose critiche, da ravvisarsi sia nella scelta di lasciare ad un decreto, sebbene in misura più limitata rispetto al passato, la determinazione di aspetti importanti della disciplina, sia nella carenza di regole procedurali precise e puntuali quanto alla delicata fase dell'accesso.

Ancora una volta, però, la disciplina nazionale è stata obbligata a confrontarsi con gli avvenimenti caratterizzanti il livello dell'Unione europea: la normativa belga era stata adottata, infatti, con grande ritardo, in un periodo in cui la legittimità della DRD risultava già fortemente contestata in numerosi Stati membri, così che si era giunti alla promozione del

---

[18] Così E. PEERAER, *Data retention: the Belgian approach*, in *Masaryk University Journal of Law and Technology*, 1, 2012, p. 125.

[19] Una spiegazione che possa giustificare l'ampiezza degli scopi indicati da tale normativa può essere ravvisata nel fatto che la medesima legge rappresentava anche la trasposizione della Direttiva 2002/58 ed in particolare della facoltà concessa dall'art. 15, che permetteva, come si ricorderà, di derogare all'obbligo generale di cancellazione dei metadati al fine di raggiungere scopi estremamente ampi quali sicurezza nazionale, difesa, sicurezza pubblica, prevenzione, ricerca, accertamento e perseguimento dei reati.

noto rinvio alla CGUE che avrebbe poi portato, non molto tempo dopo l'entrata in vigore della legge belga del 2013, alla storica sentenza *DRI* e dunque alla invalidazione della DRD. In questo intricato contesto, proprio sulla base dei motivi che avevano spinto le Corti austriaca e irlandese a promuovere l'intervento dei giudici di Lussemburgo, nonché considerando quanto affermato nelle Conclusioni dell'Avvocato generale Cruz Villalon del 12 dicembre 2013, le ONG *Liga voor Mensenrechten* e *Ligue des droits de l'homme*, nonché l'*Ordre des barreaux francophones et germanophone*, presentavano dinnanzi alla Corte costituzionale belga, nel febbraio 2014, ricorso per annullamento dell'art. 5 della legge in materia di *data retention*. Ad un primo sguardo, potrebbe certamente sembrare curiosa la scelta dei ricorrenti di non attendere la valutazione ultima della CGUE prima di adire la Corte costituzionale; tale decisione in realtà trova logica spiegazione nell'istituto del ricorso diretto previsto dal sistema di giustizia costituzionale belga, che può essere presentato solo entro sei mesi dalla pubblicazione della normativa che si intende impugnare [20]: per

[20] La Corte costituzionale belga, oltre ad un controllo di costituzionalità di tipo concreto, effettua anche un controllo astratto mediante ricorso per annullamento. Quest'ultimo può essere promosso dal Consiglio dei ministri, dagli organi esecutivi delle Regioni e delle Comunità, dal Presidente dell'Assemblea legislativa (nazionale, regionale o comunitaria) nonché, a seguito di riforma intervenuta nel 1988, da persone fisiche e giuridiche. Il termine temporale per la presentazione del ricorso è di sei mesi dalla pubblicazione della normativa da impugnare. Merita solo marginalmente ricordare come la *Cour d'Arbitrage*, istituita nel 1983 con la funzione di dirimere controversie essenzialmente attinenti al riparto di competenze tra Stato ed entità federate, sia stata protagonista, a partire dal 2003, di un percorso graduale di riforme che hanno portato ad un ampliamento delle competenze, sino a toccare anche la garanzia dei diritti costituzionali previsti nel Titolo II (artt. 8-32) e negli artt. 170, 172 e 191 della Costituzione belga. Mediante la *Loi de révision constitutionnelle* del 7 maggio 2007 è poi avvenuto il passaggio da *Cour d'Arbitrage* a *Cour constitutionnelle*. Per maggiori approfondimenti sull'evoluzione di tale organo nonché sulla giustizia costituzionale belga si rimanda, *ex multis*, a N. VIZIOLI, *La giustizia costituzionale in Belgio*, in J. LUTHER, R. ROMBOLI, R. TARCHI (a cura di), *Esperienze di giustizia costituzionale*, Vol. II, Giappichelli, Torino, 2002, p. 411 ss.; P. CARROZZA, *La Cour d'Arbitrage belga*, in G. F. FERRARI, A GAMBARO (a cura di), *Corti nazionali e comparazione giuridica*, ESI, Napoli, 2006, p. 105 ss.; E.A. FERIOLI, *Il Belgio*, in P. CARROZZA, A. DI GIOVINE, G.F. FERRARI (a cura di), *Diritto costituzionale comparato*, Tomo I, Laterza, Roma-Bari, 2014, p. 319 ss.; A. PIN, *La giustizia*

questo motivo, vista la scadenza di tale termine nel febbraio 2014, non era stato possibile aspettare di conoscere le sorti della DRD. Nondimeno, già in quel periodo, oltre alla ritenuta violazione dei diritti fondamentali tutelati dalla stessa Costituzione belga, i ricorrenti avevano potuto far affidamento sulle Conclusioni dell'Avvocato generale, considerate convincenti basi in grado di rafforzare le posizioni sostenute nel ricorso, in attesa della decisione della CGUE, che sarebbe comunque utilmente giunta nelle more del giudizio dinnanzi ai giudici nazionali; con il risultato che, qualora i giudici di Lussemburgo avessero confermato le considerazioni di Cruz Villalon, invalidando la DRD, la Corte costituzionale non avrebbe potuto ignorare l'impatto di tale dirompente decisione, dai riflessi inevitabili – per quanto indiretti – anche nel contesto nazionale.

2. *La* Cour constitutionnelle *annulla la normativa nazionale sulla conservazione dei metadati: l'unicità dell'*Arrêt *11 giugno 2015, n. 84.*

Mentre le ONG sopra citate avevano promosso ricorso di annullamento ritenendo la normativa nazionale in materia di *data retention* incompatibile principalmente [21] con i diritti alla vita privata e alla protezione dei dati, tutelati sia a livello nazionale dall'art. 22 della Costituzione che dalla Carta di Nizza e dalla Convenzione EDU, l'*Ordre des barreaux francophones et germanophone*, ovvero l'associazione rappresentativa degli interessi degli avvocati, aveva invece considerato la legge del 2013 illegittima nella parte in cui non prevedeva eccezioni riguardanti la conservazione e accesso a dati relativi a conversazioni di avvocati e medici, volte a

costituzionale, in T.E. FROSINI (a cura di), *Diritto pubblico comparato*, Il Mulino, Bologna, 2019, p. 267 ss.

[21] Le ONG avevano ritenuto la normativa capace di compromettere anche – e conseguentemente alla ingerenza nei diritti alla vita privata e alla protezione dei dati – i diritti alla confidenzialità delle comunicazioni, il diritto alla libertà personale e alla libertà d'espressione, di riunione e di associazione, alla libertà di stampa, finanche al diritto al giusto processo e ad un ricorso effettivo, nonché i principi di proporzionalità e di presunzione di innocenza.

tutelare il segreto professionale [22]. Tutte le ricorrenti, comunque, avevano provveduto a richiamare le considerazioni svolte dell'Avvocato generale Cruz Villalon con riferimento alla DRD: queste ultime erano state ritenute del tutto applicabili anche alla normativa nazionale belga che adottava, similmente a quanto disposto a livello dell'UE, una forma di conservazione generalizzata ed indiscriminata [23].

Ebbene, affrontando tali delicate questioni, con *Arrêt* 11 giugno 2015, n. 84, la legge del 30 luglio 2013, così faticosamente e lentamente adottata dal legislatore belga, era stata annullata con effetto retroattivo. Con una sentenza da taluni [24] definita una pedissequa riproposizione della pronuncia *DRI*, nel frattempo adottata dalla CGUE, la Corte costituzionale stabiliva chiaramente che, sulla base di una «identité des motifs avec ceux qui ont amené la Cour de Justice de l'Union européenne à juger la

[22] La normativa sulla conservazione infatti permetteva di memorizzare ed eventualmente accedere ai metadati relativi alle comunicazioni svolte da avvocati e medici, permettendo così di conoscere se e quando un avvocato era stato consultato e da chi – risalendo dunque ai clienti –. In questo modo, pur non avendo accesso ai contenuti delle comunicazioni, risultava nondimeno possibile trarre conclusioni chiare e precise sul rapporto sussistente tra avvocato e cliente. Ciò avrebbe finito pertanto col compromettere il segreto professionale, che rappresenta un principio generale prodromico al rispetto e alla garanzia dei diritti fondamentali; venivano così in particolar modo richiamati dai ricorrenti i diritti alla eguaglianza e alla non discriminazione tutelati dagli artt. 10 e 11 della Costituzione belga: la legge del 2013 infatti avrebbe portato al risultato di trattare in maniera identica situazioni differenti, bisognose invece di appropriate e specifiche misure. Una lesione degli artt. 10 e 11 sarebbe inoltre derivata, più genericamente, dalla assenza di distinzione tra individui legalmente indagati per la commissione di un crimine e coloro invece che non lo erano: i metadati di entrambi tali soggetti infatti sarebbero stati sottoposti egualmente al medesimo obbligo di conservazione.

[23] Interessante è anche il richiamo alle sentenze di varie Corti costituzionali quali quella cipriota, romena, bulgara e ceca, nonché in particolare della decisione del Tribunale costituzionale federale tedesco del 2 marzo 2010, avente ad oggetto la legge tedesca di trasposizione della DRD, a conferma di come «la conservation des données créait un sentiment diffus et continu de surveillance qui peut entraver le libre exercice des droits fondamentaux», para. A.2.9.

[24] F. VERBRUGGEN, S. ROYER, H. SEVERIJNS, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, in *European Law Blog,* 1 ottobre 2018, http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/.

directive conservation des données invalide, il y a lieu de constater que par l'adoption de l'article 5 de la loi attaquée, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52.1 de la Charte des droits fondamentaux de l'Union européenne», para. B.10.3. La posizione della Corte, espressa nella sintetica affermazione riportata, si rivelava già sotto tale profilo opposta a quanto sostenuto dal Governo belga, intervenuto nel procedimento, che considerava invece la legge nazionale nettamente più limitata in termini di ingerenza nella sfera privata e maggiormente garantista rispetto a quanto disposto dalla Direttiva europea. La legge del 2013, infatti, riconosceva espressi diritti agli utenti, quali quello ad essere informati della conservazione, ad accedere ai dati, ad ottenere rettifica e a proporre azione dinnanzi alla *Commission de la protection de la vie privée* o al tribunale di prima istanza; il periodo di conservazione risultava inoltre limitato a dodici mesi, mentre l'accesso era concesso solo a determinate categorie di soggetti [25]. Secondo il Governo la disciplina inserita nella legge non doveva pertanto essere considerata sproporzionata rispetto allo scopo perseguito, diversamente da quanto sostenuto dalle ricorrenti che avevano al contrario lamentato la mancanza di una modulazione della durata della conservazione a seconda della tipologia dei dati interessati, nonché l'assenza di qualsiasi limitazione al solo perseguimento dei reati gravi; ciò che le ONG avevano poi sottolineato quale aspetto fortemente problematico era l'impatto sui diritti fondamentali derivante dal regime di *bulk data retention*, capace di modificare significativamente il rapporto tra autorità pubblica e cittadini e di creare una sensazione diffusa di controllo costante, «contraire à la conception générale partagée dans les démocraties occidentales selon laquelle la vie privée est considérée comme un droit de défense du citoyen à l'encontre de l'intrusion injustifiée dans sa vie privée par l'autorité», para. A.9.2.1.1.

Proprio su questo specifico punto la Corte costituzionale aveva mostrato di essere in accordo con la ricostruzione svolta dai ricorrenti, con una decisione che costituisce pressoché un *unicum* nel panorama europeo: «alors que les Cours constitutionnelles qui ont eu à connaitre de la validité des lois nationales transposant la Directive 2006/24 ont principa-

[25] Para. A.5.5., *Arrêt* 11 giugno 2015, n. 84.

lement annulé ces lois pour insuffisance de garantie procédurales, la Cour constitutionnelle belge énonce clairement qu'une obligation de conservation généralisée et indifférenciée des données de communication est contraire au principe de proportionnalité»[26]. I giudici belgi erano giunti quindi alla medesima conclusione espressa dalla CGUE nella sentenza *DRI*, affermando che sul fronte della disciplina della *data retention* «la loi attaquée ne se distingue nullement de la directive sur ce point», para. B.10.1. Le categorie di dati conservati erano infatti identiche a quelle stabilite dalla DRD e soprattutto, «tout comme la Cour de justice l'a constaté à propos de la directive, la loi s'applique également à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, aves les infractions énumérées par la loi attaquée. De même, la loi s'applique sans aucune exception, également à des personnes dont les communications sont soumises au secret professionnel», para. B.10.1[27].

Non sussisteva quindi, diversamente dai criteri stabiliti dalla CGUE, alcuna disposizione volta a promuovere una conservazione di tipo mirato e targettizzato sulla base dei soggetti coinvolti, della zona geografica interessata o del periodo di tempo, e non veniva neppure richiesta la sussistenza di alcuna correlazione tra la conservazione/accesso ai metadati e una minaccia alla sicurezza pubblica. Per tutte queste ragioni dunque la Corte aveva ritenuto che, con riferimento all'art. 5 della legge del 2013 – ovvero la disposizione che specificamente prevedeva la modifica dell'art. 126 della legge del 2005 –, il legislatore avesse ecceduto i limiti imposti dal rispetto del principio di proporzionalità, violando anche gli artt. 10 e 11 della Costituzione belga, volti a riconoscere i diritti alla eguaglianza e alla non discriminazione, letti in combinazione con gli artt. 7, 8 e 52 del-

[26] F. COUDERT, F. VERBRUGGEN, *Conservation des données de communications électronique en Belgique: un juste équilibre?*, in V. FRANSSEN, D. FLORE (a cura di), *Societé numerique et droit penal*, Bruylant, Bruxelles, 2019, p. 248.

[27] Viene inoltre evidenziato come «Il ressort des travaux préparatoires de la loi attaquée que le législateur a entendu adapter la terminologie employée afin de la rendre compatible avec la directive 2006/24/CE, les catégories de fournisseurs visées par la loi correspondant à celles énumérées par ladite directive (Doc. parl., Chambre, 2012-2013, DOC 53-2921/001, p. 12)», para. B.8., Corte cost. belga 11 giugno 2015, n. 84.

la Carta di Nizza. Considerato poi che tutte le disposizioni della legge impugnata risultavano correlate e strettamente dipendenti dall'art. 5, l'intera legge era stata infine annullata.

Questa decisione, accolta con entusiasmo da numerose ONG, era stata in realtà per certi aspetti criticata dalla dottrina, che aveva ritenuto il vaglio della Corte costituzionale troppo "ossequioso" verso la posizione espressa dalla CGUE, avendo invece tenuto troppo poco in considerazione le peculiarità da un lato della disciplina belga e dall'altro delle doglianze mosse dalle ricorrenti. Ritenendo che gli aspetti di similarità con l'invalidata DRD fossero sufficienti a determinare l'annullamento della normativa di trasposizione, i giudici nazionali avevano mancato oltretutto di considerare i criteri stabiliti dall'art. 15 della Direttiva *e-Privacy*, ovvero l'unica normativa europea di riferimento a seguito della pronuncia *DRI* e che sarebbe divenuta pertanto la base e il fondamento di qualsiasi successiva disposizione nazionale in materia di conservazione dei dati. Affrontare tali aspetti specifici, anziché effettuare una sorta di "copia-incolla" della sentenza dei giudici di Lussemburgo, avrebbe permesso alla Corte costituzionale di fornire indicazioni preziose ed utili per il legislatore nazionale, che avrebbe dovuto farsi carico della difficile predisposizione di una nuova disciplina interna [28]. I giudici belgi insomma, pur arrivando al medesimo esito già raggiunto da altre Corti nazionali, si erano fermati, diversamente da queste, alle considerazioni relative alla legittimità della conservazione generalizzata ed indiscriminata, senza addentrarsi in una ulteriore e precisa analisi circa l'eventuale carenza di tutele nella successiva fase di accesso, sulla quale poco o nulla era stato detto, o quanto alla sussistenza di idonee salvaguardie e garanzie di sicurezza dei dati.

---

[28] Come ben sottolineato da Naudts, «the GwH [Corte costituzionale belga] could have taken this opportunity to expand upon the CJEU's reasoning. (…) The GwH saw no further need to examine or clarify the law's impact on the other fundamental rights that had been invoked by the applicants, such as the rights to freedom of expression and fair trial. When a future law is drafted, it is highly likely that the potential infringement of these rights will nonetheless remain a point of contention», L. NAUDTS, *Belgian Constitutional Court nullifies Belgian Data Retention Law*, in *European Data Protection Law Review*, 3, 2015, p. 210. Lo stesso autore sottolinea come anche la dichiarata violazione dei diritti all'eguaglianza e alla non discriminazione non sia stata in realtà accompagnata da una chiara argomentazione.

Quali che siano le considerazioni circa la correttezza e completezza della pronuncia della Corte costituzionale [29], essa aveva comunque indubbiamente determinato la necessità di un ulteriore intervento normativo a livello nazionale. Ecco quindi che, anche sulla base delle sollecitazioni delle autorità di *law enforcement*, il legislatore belga si era mosso con grande rapidità, già all'indomani della sentenza della Corte costituzionale: a seguito dell'annullamento della legge del 2013 tornava infatti in vigore, quale unica disposizione applicabile, la previa versione dell'art. 126 della legge del 13 giugno 2005 – ovvero nel suo dettato precedente alle modifiche apportate dalla legge del 2013 –, nonché l'*Arrêté royal* del 19 settembre 2013. Con riferimento a quest'ultimo infatti è bene precisare come «aprés l'annulation d'une loi par la Cour constitutionnelle, les actes réglementaires pris sur la base de la norme annulée demeurent dans l'ordre juridique, mais ils sont en sursis. En clair, l'annulation n'affecte pas comme telle l'existence de ces actes et décisions, leur validité pouvant toutefois être remise en cause par l'autorité administrative ou juridictionnelle qui les a adoptés» [30]. Si componeva così un quadro piuttosto confu-

[29] Come riportato da Naudts, non tutti hanno accolto con favore la decisione della Corte costituzionale: «on the side of the judiciary, Investigative Judge Philippe Van Linthout referred to the judgement as "a black day for justice". His concern that judicial authorities had lost an important weapon in the battle against crime was shared by Belgium's Attorney Generals and Federal Prosecutor. Indeed, in Belgium, 90% of all judicial investigations rely upon data retained by telecom operators», L. NAUDTS, *Belgian Constitutional Court nullifies Belgian Data Retention Law*, cit., p. 211. Oltretutto, a seguito della sentenza, si poneva il problema di determinare le sorti delle prove raccolte sulla base della legge dichiarata incostituzionale e utilizzate in procedimenti già avviati. Alcune Corti infatti avevano risolto tale criticità ritenendo illegale la conservazione dei metadati ma non la richiesta di accesso ad essi, che quindi risultava legittima, mentre altre avevano ritenuto valide le prove ottenute mediante conservazione dei metadati e accesso agli stessi qualora acquisite sulla base dell'art. 126 nella sua versione antecedente alla modifica apportata dalla legge del 2013. Per una analisi più completa delle decisioni assunte dai giudici nazionali con riferimento alle prove ottenute sulla base della normativa in materia di *data retention* poi dichiarata incostituzionale, si rimanda a C. FIEVET et al., *Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information*, in *Revue du Droit des Technologies de l'Information*, 68-69, 2017, p. 125.

[30] C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, cit., p. 234.

so e frammentato in diverse normative, che abbisognavano in tempi ristretti di un attento chiarimento e di una sistematizzazione coerente.

3. *La* Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques.

3.1. *La necessaria adozione di una nuova normativa sulla conservazione e accesso ai metadati: il complesso dibattito emerso dai* Travaux préparatoires.

Le criticità già riscontrate nel lungo e travagliato percorso che aveva condotto alla approvazione della legge del 2013, unitamente alle complesse posizioni espresse tanto dai giudici europei quanto da quelli nazionali, avevano reso estremamente articolato e vivo il dibattito relativo alla adozione della nuova disciplina in materia di *data retention*. Gli studi e le analisi svolte in sede di elaborazione del testo normativo, come emerge con chiarezza dai *Travaux préparatoires*, avevano messo in luce la difficoltà di coniugare efficienza ed utilità dello strumento della *data retention* con i criteri indicati in primis dalla CGUE. Così, il legislatore belga, dopo attente analisi, giungeva alla conclusione secondo cui una normativa nazionale in grado di soddisfare congiuntamente tutti i requisiti imposti dalla giurisprudenza europea avrebbe finito col vanificare lo stesso strumento della conservazione dei metadati. Nel *Doc. par. Chambre*, 2015-2016, DOC 54-1567/001, nel quale sono riportate le considerazioni svolte dal Governo e il dibattito in sede parlamentare, si leggono infatti profonde perplessità quanto alla possibile predisposizione di una forma di conservazione targettizzata: «après analyse approfondie, (…) il n'est pas possible d'opérer une différenciation a priori de cet élément. (…) Limiter la conservation des données à celles concernant des personnes qui font déjà l'objet d'une enquête pénale ou de renseignement n'a pas de sens car cette possibilité existe déjà par ailleurs», para. 7; in altre parole, le limitazioni temporale, dei soggetti e della area geografica, poste alla base di una conservazione mirata risultavano, a parere del legislatore, inefficaci e concretamente irrealizzabili. Una conservazione circoscritta ad un determinato periodo o circostanza poteva ad esempio essere adottata in caso di si-

tuazioni particolari o minacce temporanee all'ordine pubblico, mentre risultava impossibile con riferimento alla finalità di prevenzione e lotta al terrorismo: rispetto a tale minaccia è infatti pressoché impossibile indicare in anticipo un intervallo di tempo durante il quale la conservazione si possa rivelare utile. L'individuazione poi di soggetti e di aree territoriali delimitate alle quali restringere la conservazione comportava il rischio concreto e grave di giungere a pericolose discriminazioni.

Queste considerazioni parevano inoltre confermate dal fatto che né i giudici di Lussemburgo né tantomeno i giudici costituzionali nazionali avevano statuito il necessario rispetto, cumulativo e contemporaneo, dei criteri e requisiti fissati relativamente alle due fasi di conservazione e accesso ai metadati: proprio su questo specifico aspetto – che, come si vedrà, sarà ribadito con forza dallo stesso Governo belga nelle successive vicende giurisprudenziali che coinvolgeranno la normativa stessa – si fondava l'intero approccio normativo in materia di *data retention*. Anziché individuare nella giurisprudenza europea – e, di riflesso, in quella nazionale – un divieto assoluto all'adozione di sistemi di conservazione generalizzata ed indiscriminata, il legislatore belga aveva piuttosto ritenuto che una forma di *bulk data retention* fosse da considerarsi illegittima solo quando non accompagnata da una regolamentazione dell'accesso rispettosa dei requisiti indicati nella sentenza *DRI*. Una disciplina più restrittiva e rigida della fase di accesso sarebbe dunque stata in grado di compensare [31] un regime più ampio e permissivo di conservazione dei metadati [32].

---

[31] Questo termine viene oltretutto impiegato dalla *Commission pour la protection de la vie privée*, che afferma come «aucun des deux arrets ne conclut qu'un seul des quatre éléments suffit à constituer une violation du principe de proportionnalité. Si un élément déterminé des arrets ne peut pas etre retenu, il faut compenser cet élément par un régime plus strict sur les autres aspects», *Doc. parl.*, *Chambre*, 2015-2016, doc. 54, 1567/001, p. 13.

[32] Di estremo rilievo è la considerazione svolta proprio su questo delicato punto relativo all'interpretazione della giurisprudenza europea e nazionale in materia di *data retention*: «Ni l'arrêt de la Cour constitutionnelle ni celui de la Cour de justice de l'Union européenne ne concluent toutefois qu'un seul des éléments suffit à constituer une violation du principe de proportionnalité. Si tel était le cas, et l'absence de différenciation entre les personnes constituant l'élément essentiel de la législation nationale et européenne annulée, on peut penser que la Cour de justice et la Cour constitutionnelle au-

Perplessità e critiche ad una simile lettura erano però state avanzate da alcune ONG, tra cui *Datapanik*, *Liga voor Mensenrechten* e *Ligue des droits de l'homme*[33]: secondo queste ultime, la nuova normativa pareva caratterizzata dalla pericolosa riproposizione di una conservazione generalizzata, da considerarsi *per se* illegittima e sproporzionata, indipendentemente dalla disciplina dell'accesso. Sotto un profilo più generale poi veniva sottolineato come la stessa utilità del regime di conservazione dei dati, affermata dal Governo, non fosse in realtà fondata o supportata da studi e statistiche; le ONG, invece citavano analisi e ricerche attestanti la mancanza di prove concrete circa l'efficacia di tali sistemi nella lotta alla criminalità[34]. Per questi motivi le ONG chiedevano una rinuncia definitiva a simili strumenti di sorveglianza massiva.

3.2. *Un difficile compromesso tra efficienza ed elevata tutela dei diritti alla riservatezza e protezione dei dati.*

Nonostante le serie critiche rilevate e le difficoltà riscontrate nel predisporre un testo normativo che fosse compatibile con la giurisprudenza europea, il legislatore belga, sulla base delle riflessioni emerse dai lavori preparatori, giungeva infine alla approvazione della legge del 29 maggio 2016[35] in materia di raccolta e conservazione dei metadati. Questa nor-

---

raient uniquement examiné cet aspect et auraient conclu à la violation du droit au respect de la vie privée sans examiner les autres éléments», para. 7, lett. c).

[33] Si legga sul punto il documento *Avis de Datapanik, la Liga voor Mensenrechten, la Ligue des droits de l'Homme et la NURPA concernant le projet de loi relatif à la collecte et à la conservation des données dans le secteur des communications électroniques*, del 2 febbraio 2016.

[34] Venivano ad esempio citati gli studi elaborati dal Massachusetts Institute of Technology, *Reality mining: sensing complex social systems*, 2005; lo studio del 2011 svolto dal Centro Studi del Bundestag (*Die praktischen auswirkungen der vorratsdatenspeichrung auf die entwicklung der aufklarungsquoten in den EU-mitgliedsstaaten*), nonché uno studio del Dipartimento di criminologia del *Max Planck Institute* del 2012 (*Schutzlücken durch Wegfall der Vorratsdatenspeicherung? Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten*).

[35] *Loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques, M.B. 18 juillet 2016.*

mativa interveniva principalmente sull'art. 126 della legge del 13 giugno 2005, modificandolo totalmente, nonché su alcune disposizioni del *Code d'instruction criminelle* e sulle normative attinenti alle attività delle autorità di intelligence e di *law enforcement*. Partendo dunque dall'art. 126 che, come si ricorda, era già stato riformato dalla previa legge del 2013 successivamente annullata, veniva ribadito come i fornitori di servizi di telecomunicazioni pubbliche avessero l'obbligo di conservare i dati generati o trattati nell'ambito di fornitura dei propri servizi, ad esclusione dei contenuti delle comunicazioni. Il comma 2 poi elencava specificamente le autorità che potevano ottenere l'accesso ai dati conservati, limitatamente ed unicamente agli scopi indicati: le autorità giudiziarie per finalità di ricerca, accertamento e perseguimento di reati; i servizi di intelligence e sicurezza per la raccolta di informazioni sulla base della legge del 30 novembre 1988 che ne regola appunto le attività; gli ufficiali di polizia giudiziaria dell'*Institut belge des services postaux et des télécommunications* (IBPT) [36] per la ricerca, accertamento e perseguimento di reati che costituiscono violazione delle norme di sicurezza delle reti di telecomunicazione; i servizi di emergenza nel caso in cui venisse richiesto il loro intervento per una situazione di pericolo e questi non fossero in grado di ottenere dati completi o esatti circa il soggetto che ha effettuato la chiamata o l'ubicazione dello stesso; e ancora l'Ufficiale di polizia giudiziaria appartenente alla *Cellule des personnes disparues de la Police Fédérale* per operazioni di soccorso o ricerca di persone scomparse ed infine il *Service de médiation pour les télécommunications* che poteva però accedere solo ai dati identificativi e unicamente allo scopo di identificare persone che avessero fatto uso illecito di reti Internet o servizi di telecomunicazione. Sotto questo profilo e diversamente dalla disciplina del 2013, il legislatore belga aveva mostrato una particolare attenzione alla determinazione, con un

[36] «L'IBPT est le régulateur fédéral compétent pour le marché des communications électroniques, le marché postal, le spectre électromagnétique des radiofréquences et la radiodiffusion sonore et télévisuelle dans la Région de Bruxelles-Capitale», https://www.ibpt.be/consommateurs/l-ibpt; tale Istituto può imporre sanzioni amministrative laddove venga constatato, nello svolgimento e nei limiti dei propri compiti di vigilanza e controllo, il verificarsi di condotte contrarie alla legge. I suoi poteri e prerogative sono inseriti nel Capitolo II della legge 13 giugno 2005 e successive modifiche.

alto livello di precisione, dei soggetti autorizzati all'accesso e delle finalità per le quali tale ingerenza veniva consentita, nonché, come si vedrà, della procedura da seguire; sebbene quindi fossero state colmate alcune delle lacune caratterizzanti la previa normativa – che peraltro proprio sotto tali profili era stata reputata particolarmente insidiosa dalla dottrina, dalla *Commission de la protection de la vie privée* nonché dalla stessa Corte costituzione nella sua sentenza –, deve comunque essere sottolineato come le autorità autorizzate risultassero piuttosto numerose e gli scopi estremamente ampi, così che i rischi di abusi venivano ampliati, insieme ai dubbi quanto alla rispondenza della disciplina al principio di stretta necessità.

La durata della conservazione era identificata in dodici mesi per tutte le tipologie di dati (dati d'identificazione, dati relativi all'accesso, alla connessione alla rete, all'ubicazione e i dati di comunicazione), lasciando però al Re la puntuale indicazione, sulla base di una delibera del Consiglio dei Ministri [37], della specifica e puntuale categoria di dati da sottoporre a conservazione.

Il comma 4 dell'art. 126 prevedeva invece alcuni importanti obblighi in capo agli operatori di servizi di telecomunicazione, tenuti a garantire standard di sicurezza e tutela dei dati parificabili a quelli assicurati ai dati in rete, nonché a predisporre misure tecniche ed organizzative volte a proteggere i metadati conservati da qualsiasi rischio di accesso illecito o di abuso. La conservazione, inoltre, doveva avvenire unicamente entro i confini dell'Unione europea: su quest'ultimo punto, diversamente da quanto si è visto con riferimento alla normativa tedesca [38], il legislatore belga aveva considerato sufficiente la previsione di una *data retention* nei limiti del territorio dell'UE e non, più restrittivamente, nel solo territorio nazionale. Veniva comunque imposto l'obbligo di distruzione dei dati

[37] Viene anche disposto il previo parere da parte della *Commission de la protection de la vie privée* e dell'*Institut belge des services postaux et des télécommunications* (art. 126, co. 3).

[38] Come si ricorderà, infatti, la Germania ha adottato nel 2015 una specifica normativa in materia di conservazione dei dati, la *Gesetz zur Einfuhrung einer Speicherflicht und einer Hochstspeicherfrist fur Verkehsdaten*, del 26 ottobre 2015, nella quale è stato imposto l'obbligo in capo ai fornitori di servizi di telecomunicazione di conservare i metadati esclusivamente entro i confini nazionali.

conservati una volta scaduto il termine stabilito di dodici mesi, unitamente alla garanzia di tracciabilità dell'utilizzo dei dati, che trovava realizzazione in un apposito registro nel quale dovevano essere indicate tutte le richieste di accesso ai dati avanzate dalle autorità pubbliche sopra elencate [39].

La disciplina della conservazione dei metadati così descritta veniva poi coordinata con ulteriori modifiche al *Code d'instruction criminelle*, in particolare agli artt. 46-*bis* e 88-*bis*, mediante l'inserimento di alcune importanti indicazioni riguardanti le condizioni di accesso ai metadati. L'elemento fondamentale di tali riforme era da individuarsi nell'esistenza di una modulazione della possibilità di accesso a seconda della gravità dei reati perseguiti e della tipologia di dati interessati. L'art. 46-*bis* infatti stabiliva che per scopi di indagine relativa a reati genericamente intesi, dunque senza carattere di gravità, il Procuratore del Re poteva avanzare richiesta ai fornitori di servizi di telecomunicazione al fine di ottenere l'accesso ai dati d'identificazione relativi ad un abbonato o, a contrario, ai dati d'identificazione dei servizi di comunicazione elettronica attivati da un determinato soggetto. Tale accesso tuttavia doveva essere accompagnato da una decisione del Procuratore stesso, scritta, motivata e proporzionata, cioè rispettosa quanto più possibile del diritto alla vita privata e avente carattere di sussidiarietà nello specifico contesto dell'indagine svolta. La richiesta di accesso da parte degli ufficiali di polizia giudiziaria poteva invece essere effettuata solo in casi di estrema urgenza e comunque sempre sulla base di un previo accordo verbale con il Procuratore e di un provvedimento motivato e scritto. Con riferimento alla sopra richiamata tipologia di dati, che potremmo genericamente definire come dati di identificazione, veniva inoltre specificato come per i reati per i quali era

[39] Questo allo scopo di consentire, oltre ad un controllo preciso, anche la predisposizione di studi statistici relativi alla *data retention*, che il Ministro della Giustizia era tenuto a presentare alla Camera dei rappresentanti al fine di permettere una ricostruzione puntuale dei casi in cui le richieste di accesso venivano avanzate nonché, elemento molto importante, del tempo trascorso tra la data di inizio della conservazione del metadato e il momento in cui la domanda di accesso veniva avanzata. Ciò all'evidente scopo di poter valutare se il termine di conservazione di dodici mesi fosse da considerarsi appropriato e proporzionato o se invece esso risultasse troppo esteso rispetto alla reale necessità espressa dalle autorità di intelligence e *law enforcement*.

prevista una detenzione correttiva di un anno o una pena superiore, potessero essere richiesti dal Procuratore (o in casi di urgenza, come si è detto, dalla polizia giudiziaria) solo i dati risalenti ad un massimo di sei mesi precedenti alla richiesta.

Ai sensi del riformato art. 88-*bis*, poi, in caso di sussistenza di indizi gravi di reati per i quali era stabilita una detenzione di un anno o pena superiore e laddove le informazioni derivanti dai metadati fossero necessarie per stabilire la verità dei fatti, l'autorità giudiziaria ovvero, nello specifico, il giudice istruttore, avrebbe potuto richiedere l'accesso ai dati relativi al traffico e i dati sulla localizzazione. Per queste informazioni, considerate maggiormente intrusive nella sfera privata, quindi, la domanda di accesso doveva essere effettuata solamente dal giudice ed essere altresì correlata da una ordinanza motivata, comprensiva delle ragioni per le quali la richiesta stessa era stata avanzata, della attestazione della proporzionalità dell'istanza e dell'efficacia temporale della domanda, che non poteva comunque protrarsi oltre due mesi dalla data dell'ordinanza medesima. Anche in questo caso però la possibilità di andare "indietro nel tempo" veniva differenziata sulla base della severità del reato perseguito: per i reati di cui al libro II, titolo I *ter* del *Code pénal*[40], i dati richiesti potevano riguardare un termine di tempo fino a dodici mesi prima dell'ordinanza, mentre per i reati indicati nell'art. 90-*ter*, co. 2 a 4 o per i reati perpetrati nel contesto di una organizzazione criminale (art. 324-*bis*) o ancora per quei reati per i quali era prevista una detenzione di cinque anni o pena superiore, i dati erano solo quelli risalenti ad un massimo di nove mesi prima dell'ordinanza; infine per tutti gli altri reati rientranti nella categoria indicata dalla disposizione in esame – ovvero quelli per i quali fosse stabilita una detenzione superiore ad un anno – i dati potevano riguardare i soli sei mesi precedenti alla richiesta. Veniva inoltre precisata una limitazione quanto ai mezzi di comunicazione elettronica impiegati da avvocati o medici, sottoposti a segreto professionale: le norme sino ad ora analizzate non valevano per queste categorie di soggetti, i cui dati potevano essere richiesti solo in caso di sussistenza di un sospetto, in capo ai professionisti citati, di commissione di reato punibile con almeno un anno di detenzione o di concorso alla commissione degli stessi reati o

[40] Tale Titolo è specificamente dedicato alle «*Infractions terroristes*».

ancora qualora terzi sospettati della commissione di reati avessero utilizzato i mezzi di comunicazione relativi a questi soggetti [41].

Ciò che infine si vuole sottolineare è la modifica apportata alla legge organica del 30 novembre 1998 sui servizi di intelligence, nella quale venivano altresì inserite alcune specifiche condizioni per l'accesso ai metadati: veniva così richiesta una previa decisione del dirigente del servizio di intelligence volta a stabilire il metodo di accesso ai dati e, laddove possibile, le persone, associazioni, gruppi, luoghi o eventi interessati dall'accesso, nonché la minaccia potenziale da scongiurare e la durata delle operazioni di accesso ai metadati; anche in questo caso veniva riproposta una gradazione temporale che limitava la possibilità di richiesta di accesso a dati risalenti sino a sei mesi prima, in caso di minacce derivanti da attività di criminalità organizzata; sino a dodici mesi per minacce derivanti da attività di terrorismo o estremismo e, in via residuale, sino a nove mesi per tutte le altre tipologie di minacce che rientrano nelle competenze dei servizi di intelligence. Si comprende dunque come anche per le autorità di intelligence fosse previsto l'obbligo di fondare le proprie istanze su una minaccia specifica e ben individuata, e comunque effettuando un vaglio di necessità basato su parametri oggettivi, così da circoscrivere quanto più possibile l'ingerenza allo stretto necessario [42].

Dalla analisi svolta con riferimento alle principali modifiche introdotte con la legge del 2016, si nota con evidenza come accanto alla conferma di una forma di conservazione che manteneva i caratteri propri di *bulk data retention*, fossero tuttavia aumentate le salvaguardie quanto alla fase di accesso: erano individuati elenchi specifici – per quanto piuttosto am-

[41] Anche nei casi in cui l'accesso è consentito sono poi comunque previste apposite e specifiche tutele, quali l'informazione preventiva all'ordine degli avvocati o dell'ordine dei medici da parte del giudice istruttore (art. 88-*bis*, co. 3).

[42] Nei lavori preparatori citati, il legislatore aveva indicato come, con riferimento alla disciplina della conservazione e accesso ai dati da parte di autorità di intelligence, fosse necessario che «les méthodes ordinaires s'avèrent insuffisantes pour récolter les informations nécessaires à une mission de renseignement (subsidiarité), il y a une menace potentielle, elles sont proportionnelles au degré de gravité de la menace, la décision du chef du service est écrite et motivée. *Ces conditions impliquent que les services de renseignement doivent, pour chaque méthode, justifier le lien entre la cible et la menace*», para. 9, enfasi aggiunta.

pi – di soggetti autorizzati e di scopi per i quali l'accesso poteva essere concesso; erano previste tutele preventive e salvaguardie da possibili abusi mediante l'obbligo di predisposizione di richieste scritte e motivate che dovevano contenere indicazioni precise soprattutto quanto alla proporzionalità e necessità dell'ingerenza. Venivano previste condizioni differenti di accesso, tenendo conto delle categorie di dati interessati e dell'ampiezza del periodo di disponibilità degli stessi; non era invece stabilita alcuna deroga alla regola generale della conservazione, che restava identificata in dodici mesi massimi: ciò che variava era solo la possibilità di andare "indietro nel tempo" nella successiva fase di accesso nonché le specifiche condizioni procedurali imposte, mentre indipendentemente da tale modulazione, la conservazione rimaneva comunque fissa ad un anno. Risulta pertanto chiara ed evidente la concretizzazione di quanto già emerso dai lavori preparatori, secondo cui le condizioni stabilite dal giudice dell'UE non dovevano intendersi come tutte obbligatoriamente sussistenti in maniera cumulativa, risultando invece sufficiente che una più ampia ingerenza nella fase di conservazione fosse compensata da maggiori tutele nella fase di accesso.

Nonostante tale sforzo normativo – e quasi quanto avvenuto in passato fosse destinato a ripetersi –, a pochi mesi dall'approvazione della nuova legge in materia di *data retention*, la disciplina belga si era trovata nuovamente costretta a scontrarsi con gli avvenimenti caratterizzanti il livello sovranazionale e, in particolare con la posizione espressa dalla CGUE. Risale infatti al dicembre 2016 la pronuncia *Tele2*, nella quale, come noto, confermata la posizione già enunciata nella sentenza *DRI*, erano stati chiariti taluni criteri e requisiti relativi al dibattuto art. 15 Direttiva *e-Privacy*. Il nuovo intervento dei giudici di Lussemburgo, che era andato nella direzione di confermare l'incompatibilità con il diritto dell'UE e, in particolare, con la Carta di Nizza, di una forma di conservazione generalizzata ed indiscriminata, non era dunque passato inosservato neppure in Belgio ed aveva anzi rianimato i dubbi e le criticità che già nella fase di predisposizione della normativa del 2016 erano stati denunciati da talune ONG e dalla dottrina [43]. La normativa nazionale, poco prima adottata, veniva così

[43] Forget ad esempio rilevava come il periodo di conservazione imposto dalla normativa belga non rispettasse i requisiti di proporzionalità e necessità: le statistiche elaborate dal *Institut belge des services postaux et des télécommunications* nel documento *Informations stati-*

ben presto messa in discussione sotto il profilo della conformità al diritto dell'UE, sulla base dei rilevanti principi affermati nella sopravvenuta sentenza *Tele2*: agli inizi di gennaio 2017 era stato infatti promosso un ricorso per annullamento dinnanzi alla Corte costituzionale, che aveva visto quali ricorrenti, ancora una volta, l'*Ordre des barreaux francophones et germanophone*, nonché l'associazione dei professionisti operanti nell'ambito fiscale (*Academie Fiscale*), insieme ad alcuni cittadini e ONG (non a caso le medesime *Liga voor Mensenrechten* e *Ligue des droits de l'homme* che avevano sollevato così tante obiezioni con riferimento al progetto di legge).

4. *L'ulteriore intervento della* Cour constitutionnelle *e il dialogo con la CGUE: andata e ritorno.*

4.1. *Il ricorso di annullamento avverso la legge del 2016: le contrastanti letture della giurisprudenza della CGUE promosse da Governo e ricorrenti.*

Richiedendo ancora una volta l'intervento della Corte costituzionale, i ricorrenti avevano sottolineato in maniera chiara come il legislatore belga, pur essendo intervenuto con significative modifiche sulla disciplina del-

---

stiques: conservation des données pour 2014 et 2015, del 27 settembre 2016, avevano infatti mostrato come la maggioranza dei metadati richiesti dalle autorità di *law enforcement* fossero risalenti ai tre mesi precedenti. Sulla base di tali studi, pareva quindi piuttosto incongruente e sproporzionato attestare la durata della *data retention* al quadruplo di quanto generalmente necessario; così C. FORGET, *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, cit., p. 239. La stessa autrice poi sottolineava un ulteriore aspetto di interesse: ai sensi degli artt. 122 e 123 della medesima legge del 13 giugno 2015, i fornitori di servizi di telecomunicazione erano autorizzati a conservare i metadati derivanti dalle comunicazioni effettuate dai propri utenti, per mere finalità di marketing o di fatturazione. Tali dati risultavano accessibili dalle autorità giudiziarie mediante richiesta alle condizioni previste dagli artt. 46-*bis* e 88-*bis* del *Code d'instruction criminelle*. Tuttavia «celles-ci n'étant pas répertoirées ou listées par les operateurs, il n'est pas possible de déterminer si les données conservées en vertu des articles 122 et 123 de la loi du 13 juin 2005 diffèrent de celles traitées et conservées en vertu de son article 126. Dans l'hypothèse où ces données ne se recouperaient pas, il eut été intéressant de déterminer l'intérêt des données collectées à des fins de facturation dans le cadre d'enquêtes pénales et en conséquence, la réelle nécessité d'imposer la conservation de données supplémentaires aux opérateurs», p. 239.

l'accesso, non avesse in alcun modo riformato il proprio approccio rispetto alla annullata legge del 2013. Mancava in particolare qualsiasi tentativo di introdurre una forma di *targeted data retention*, così come definita dai giudici di Lussemburgo nelle pronunce *DRI* e *Tele2*. La riconferma di una *bulk data retention* non poteva, a parere dei ricorrenti, essere giustificata neppure da quanto sostenuto dal Governo belga, ovvero che la generalizzazione della conservazione andasse a tutto beneficio non solo delle vittime del reato, che meritavano di essere tutelate, anche indirettamente, mediante la predisposizione di tecniche di indagine in grado di assicurare una lotta più efficace alla criminalità [44], ma anche dello stesso sospettato che, grazie ad una conservazione ampia e dunque ad una maggiore disponibilità di informazioni, avrebbe potuto provare la propria innocenza. Sul punto i ricorrenti avevano infatti affermato come «la justification apportée par le législateur à cet égard ne peut convaincre puisque le droit pénal repose sur le principe de présomption d'innocence avec pour corollaire que la charge de la preuve repose sur le ministère public (...). Il ne serait dès lors pas pertinent d'invoquer le fait que la mesure peut tout aussi bien bénéficier à la victime d'une infraction» [45]. Similmente a quan-

[44] Il Governo aveva sostenuto che «la recherche de la vérité est dans l'intérêt tant de la victime et de l'accusé (qui pourra par exemple démontrer qu'il se trouvait ailleurs au moment des faits) que de toutes les autres personnes concernées», para. B.20.1., evidenziando peraltro come le ulteriori finalità previste a motivazione della conservazione dei metadati – ad esempio nel caso di ricerca di persone scomparse o in caso di chiamate d'emergenza – imponessero un diverso ragionamento ed una differente valutazione circa la proporzionalità dell'ingerenza.

[45] Così si legge al para. A.3.5 della decisione della Corte costituzionale 19 luglio 2018, n. 96, di cui si parlerà a breve. Sotto il profilo degli ulteriori scopi e benefici che potevano derivare, secondo l'interpretazione del Governo belga, da un regime di conservazione generalizzata, veniva sottolineato come nella sentenza *Tele2* i giudici europei avessero affermato che non può considerarsi conforme al diritto UE una normativa nazionale che allo scopo di combattere reati, prevedesse una *bulk data retention*. Ne deriverebbe dunque che una normativa che predispone tale tipo di conservazione per scopi diversi dalla lotta alla criminalità – ad esempio, come previsto nel regime belga, per la ricerca di persone scomparse o l'identificazione di coloro che hanno effettuato chiamate d'emergenza – avrebbe dovuto essere considerata esclusa da un simile divieto. Al contrario, i ricorrenti avevano invece sostenuto che se neppure la lotta al terrorismo o alla criminalità organizzata era risultata obiettivo talmente rilevante da ritenere una ingerenza

to già rilevato nel dibattito dottrinario apertosi a livello europeo, forti critiche erano state espresse dai ricorrenti con riferimento alla mancanza di un concreto vaglio circa la reale utilità ed efficacia di forme di *bulk data retention* e dunque della necessità di sottoporre l'intera popolazione belga ad una forma di sorveglianza ritenuta totalmente sproporzionata rispetto all'obiettivo da raggiungere [46]. Da ciò, i ricorrenti rilevavano pericoli non solo per la garanzia dei diritti alla vita privata e alla protezione dei dati, ma anche del diritto alla libertà di espressione: la combinazione della legge del 2016 e di quella del 1998 regolante le attività dei servizi di intelligence avrebbe potuto comportare rischi di abuso di potere, a detrimento anche della categoria dei giornalisti, con il possibile risultato di «renforcer l'autocensure chez le citoyen qui a le vague sentiment d'être surveillé, ce qui peut avoir un impact sur l'exercice de sa liberté d'opinion et d'information et constituer de la sorte une ingérence par rapport à l'article 11 de Charte des droits fondamentaux de l'Union européenne» [47]. Sotto questo profilo veniva poi evidenziato come non fosse neppure disposto un obbligo di notifica nei confronti dei soggetti i cui dati risultavano sottoposti ad accesso [48].

---

così vasta nella sfera privata proporzionata allo scopo, tantomeno avrebbero potuto esserlo altri scopi di minore rilievo quali quelli previsti dalla normativa belga.

[46] Para. A.3.5, Corte cost. 19 luglio 2018, n. 96. L'*Ordre des barreaux* inoltre si spingeva ad una analisi ancora più approfondita di tale aspetto, accusando il Governo di fingere di non comprendere il riferimento effettuato dai ricorrenti «à d'autres mécanismes moins attentatoires à la vie privée de l'ensemble des citoyens comme les méthodes de repérage existantes en droit belge ou de 'quick freeze' qui visent une décision obligeant les opérateurs a conserver des données à propos de personnes identifiées dans une zone géographique ou une période temporelle délimitée. *Le raisonnement de l'Etat belge reposerait en réalité sur une volonté politique de poursuivre a tout prix dans la voie de la conservation générale des données sous prétexte d'un contexte de risque terroriste et malgré l'inconstitutionnalité du système de surveillance généralisé mis en place*», para. A.3.6., Corte cost. 19 luglio 2018, n. 96, enfasi aggiunta.

[47] Para. A.18.4, Corte cost. 19 luglio 2018, n. 96.

[48] Gli Ordini professionali degli Avvocati e l'*Academie Fiscale*, anche con riferimento alla legge del 2016 e similmente a quanto era già stato oggetto di censura nella legge del 2013, avevano poi considerato le disposizioni sulla conservazione e accesso ai metadati contrarie al rispetto del segreto professionale che caratterizza professioni delicate quali quella legale o contabile: l'accesso ai metadati in tale ambito avrebbe permesso di de-

Il Governo belga, intervenuto dinnanzi alla Corte costituzionale, aveva, al contrario, ribadito la correttezza delle scelte legislative: l'obbligo di conservazione precede logicamente la fase di utilizzo dei dati per scopi investigativi, così che solo la richiesta di accesso permette di determinare la gravità del reato, consentendo dunque unicamente in quel momento di modulare adeguatamente e proporzionalmente l'ingerenza nella sfera privata rispetto all'obiettivo perseguito. Per questi motivi logici, prima ancora che giuridici, risultava impossibile provvedere ad una differenziazione della durata della conservazione *a priori*, poiché non potevano conoscersi in precedenza i reati per i quali i metadati avrebbero potuto essere impiegati. Facendo leva sulle considerazioni già chiaramente espresse nei lavori preparatori all'adozione della normativa nazionale, veniva anche confermata dal Governo la legittimità e compatibilità di un sistema di conservazione generalizzata rispetto al diritto nazionale ed europeo: la sola *data retention*, autonomamente intesa, non può consentire di stabilire chiare conclusioni sulla vita privata degli utenti, che potrebbero invece essere definite solo con il successivo accesso; per tali ragioni, le salvaguardie poste in essere – quali la conservazione sul solo territorio dell'UE nonché il controllo affidato ad IBPT e all'Autorità nazionale per la protezione dei dati – risultavano sufficienti con riferimento alla fase di conservazione, soprattutto alla luce delle ancor più stringenti tutele previste per la fase di accesso [49]. Ribadendo quanto già sottolineato prima dell'ado-

terminare se un professionista era stato consultato, consentendo di conseguenza l'identificazione dei clienti e i dati relativi alle comunicazioni avvenute (luogo, durata, data). Per quanto la normativa all'epoca vigente avesse introdotto alcune disposizioni specifiche su questo profilo, nel complesso la mancata predisposizione di un divieto assoluto di conservazione dei metadati afferenti a mezzi di comunicazione appartenenti a tali soggetti e la previsione di alcune casistiche che consentivano, al contrario, l'accesso a tali metadati, risultava lesiva di un interesse generale, ravvisabile nella garanzia di una reale segretezza del rapporto tra professionista e cliente e capace di incidere sui diritti alla vita privata e al giusto processo. Ad aggravare tale quadro vi era inoltre l'assenza di meccanismi di controllo volti a consentire al professionista di opporsi alla raccolta, conservazione e accesso a dati coperti da segreto professionale.

[49] Del resto, ancora una volta con un ragionamento di tipo logico e fattuale più che giuridico, il Governo stabiliva come «la loi attaquée permet précisément aux enquêteurs, dans un cadre soigneusement déterminé, d'accéder à certaines métadonnées concernant une personne faisant l'objet d'une telle enquête. Cela suppose que ces métadonnées

zione della normativa, il Governo ammetteva nuovamente nelle proprie memorie come «le législateur n'a pas pu répondre à l'ensemble des critiques formulées par la jurisprudence pour considérer que la directive 2006/24/CE était illégale. Il indique toutefois qu'un seul élément ne pourrait suffire à constituer une violation du principe de proportionnalité au sens de la jurisprudence de la Cour de justice et de celle de la Cour» [50]. Il Governo proponeva così una lettura del tutto particolare delle decisioni dei giudici di Lussemburgo: nella pronuncia *DRI*, la Direttiva 2006/24 era stata dichiarata in contrasto con il principio di proporzionalità e necessità sulla base di una combinazione di tre elementi: il fatto che la conservazione fosse generalizzata, l'assenza di differenziazione quanto alle categorie dei dati conservati e alla loro utilità, l'assenza o l'insufficienza di regole riguardanti l'accesso ai metadati [51]. Era la totalità di questi aspetti, letti in maniera combinata e in quanto tutti contemporaneamente sussistenti, ad aver portato alla dichiarazione di mancata conformità al diritto dell'UE. Con riferimento invece alla successiva sentenza *Tele2*, secondo il Governo, «ni la Cour de justice ni la Cour n'ont jugé que l'un de ces éléments pouvait suffire à conclure au caractère disproportionné de la mesure. Le contrôle du principe de proportionnalité suppose en effet une approche globale. Contrairement à ce que soutiennent les parties requérantes, l'arrêt de la Cour de Justice de l'Union européenne du 21 décembre 2016 ne remettrait nullement en cause ce constat» [52].

---

aient été conservées en amont de l'enquête et donc à un moment où il n'était pas possible d'opérer la différenciation visée par le requérant», para. A.5.12, Corte cost. 19 luglio 2018, n. 96.

[50] Para. A.7.3, Corte cost. 19 luglio 2018, n. 96.

[51] «Si chaque citoyen n'est, en effet, pas potentiellement un criminel, chaque citoyen peut potentiellement être confronté à la criminalité, que ce soit en tant que victime, en tant que prévenu ou en tant que témoin et dès lors avoir un intérêt à la recherche de la vérité», para. A.10.3., Corte cost. 19 luglio 2018, n. 96. Ne conseguiva dunque che sarebbe stato sbagliato individuare la carenza di un singolo elemento nella lista dei requisiti fissata dalla CGUE – per esempio la mancanza di una *targetd retention* – e valutare quell'unico criterio non rispettato come in sé idoneo a rendere la disciplina sulla conservazione e accesso ai metadati irrimediabilmente e totalmente incompatibile con la Carta Europea dei Diritti Fondamentali.

[52] Para. A.10.4, Corte cost. 19 luglio 2018, n. 96. Il Governo aggiungeva come fosse

4.2. *L'*Arrêt interlocutoire *19 luglio 2018, n. 96: un necessario chiarimento quanto alla cumulativa sussistenza dei requisiti fissati a livello europeo.*

Proprio prendendo avvio dai diversi approcci e letture della medesima giurisprudenza della CGUE, proposti dai ricorrenti da un lato e dal Governo dall'altro, la Corte costituzionale nella sentenza del 19 luglio 2018, n. 96, prendeva atto di come la decisione *DRI* così come la successiva *Tele2* fossero passibili di due diverse interpretazioni, sinteticamente ma magistralmente descritte: «dans une premiére interprétation, l'illégalité de l'obligation de conservation générale et indifférenciée des données résulterait de l'absence de garanties suffisantes relatives à l'accès aux données conservées et au délai de conservation; dans une deuxième interprétation, l'obligation de conservation serait illégal, précisément en raison de son caractère général et indifférencié» para. A.14.1. Ne conseguiva, dunque, la necessità di predisporre un rinvio pregiudiziale alla CGUE, alla quale

---

da considerarsi impossibile «de lutter contre la criminalité grave telle que la cybercriminalité si l'on ne prévoit pas une obligation générale et indifférenciée de conservation des données de communication électronique. (…) Il répété une fois encore qu'à son estime, il n'existe pas d'autre moyen pour atteindre les objectifs poursuivis par le législateur qu'imposer une obligation générale de conservation», para. A.13.3. Corte cost. 19 luglio 2018, n. 96. Il Governo belga dunque è stato chiaro nel ribadire come qualsiasi considerazione quanto al mancato rispetto del requisito di stretta necessità della *bulk data retention* fosse da respingersi. Sotto questo profilo inoltre venivano riportati alcuni dati, che il Governo ha presentato a supporto proprio della utilità di una conservazione generalizzata e della durata di dodici mesi indicata dalla legge del 2016: «Dans son mémoire en réplique, le Conseil des ministres note une fois encore que le fait qu'une différenciation sur le plan du délai de conservation des données était impossible n'est pas sans justification raisonnable. Aussi bien dans le cadre des enquêtes pénales que dans le cadre des services de renseignement, le délai concerné est apparu nécessaire. Il ressort des chiffres de l'IBPT que, pour l'année 2014, 15 % des demandes qui émanaient des autorités judiciaires et qui étaient fondées sur les articles 46-*bis* et 88-*bis* du Code d'instruction criminelle adressées à Base Company et Proximus avaient rapport à des données qui dataient de plus de neuf mois jusqu'à douze mois avant la demande. Il apparaît également des chiffres de la "Federal Computer Crime Unit" (FCCU) pour la période de 2012 à 2014 que 29 % des demandes avaient rapport aux données qui dataient de plus de neuf mois jusqu'à douze mois avant la demande. Les chiffres présentés par le Service général du renseignement et de la sécurité (SGRS) vont dans le même sens», para. A.36.

sola spettava il compito di sciogliere il complesso nodo interpretativo in maniera definitiva, delineando quali dei due differenti approcci fosse da considerarsi corretto. Svolgendo una puntuale e ampia ricostruzione delle motivazioni e delle considerazioni poste alla base di entrambi gli orientamenti, la Corte costituzionale belga ha cercato di fornire nel rinvio un ampio quadro della difficile questione posta all'attenzione dei giudici di Lussemburgo, richiamando peraltro anche la – all'epoca – più recente giurisprudenza della Corte europea dei Diritti dell'Uomo. In particolare, veniva presentata alla CGUE la sentenza *Centrum For Rattvisa*[53], nella parte in cui era riconosciuto alle autorità nazionali un ampio margine di apprezzamento quanto alla scelta dei mezzi volti alla salvaguardia della sicurezza. In tale pronuncia i giudici di Strasburgo avevano ritenuto la normativa svedese, comportante forme di intercettazione massiva delle comunicazioni elettroniche per finalità securitarie – tra cui la lotta alla minaccia terroristica –, conforme alla Convenzione EDU e al suo art. 8 sulla tutela della vita privata alla luce di una analisi globale di tutte le salvaguardie predisposte dal legislatore, lette nel loro insieme. La scelta della Corte belga di richiamare proprio tale sentenza ben potrebbere essere vista come un suggerimento rivolto ai giudici di Lussemburgo ad osservare anche quanto stava accadendo nella giurisprudenza della Corte EDU, che pareva diretta verso una lettura meno stringente dei requisiti di legittimità di forme di sorveglianza e controllo delle telecomunicazioni[54]. Su questa stessa linea può essere considerato anche il richiamo espresso svolto dalla Corte costituzionale alle grandi difficoltà concretamente riscontrate dalla maggioranza degli Stati membri nella predisposizione di una disci-

[53] *Centrum For Rattvisa c. Svezia*, ricorso n. 35252/08, deciso il 19 giugno 2018 dalla *Third Section* della Corte EDU e poi, su ricorso dell'associazione *Centrum For Rattvisa* impugnato dinnanzi alla *Grand Chamber*. Quest'ultima, come si è avuto modo di richiamare nel Capitolo 3, si è pronunciata con sentenza del 25 maggio 2021, confermando sotto taluni profili il pur discusso approccio adottato dalla *Thrid Section* nella pronuncia del 2018 e rinvenibile anche nella sentenza *Big Brother Watch e altri c. Regno Unito*, ricorsi n. 58170/13, 62322/14 e 24960/15, decisa il 13 settembre 2018, sottoposta anch'essa al successivo vaglio della *Grand Chamber* conclusosi con pronuncia del 25 maggio 2021.

[54] Su questi profili, si rimanda alle riflessioni svolte nel Capitolo 3 e alla bibliografia ivi richiamata.

plina nazionale conforme e rispettosa dei criteri individuati in *DRI* e *Tele2*, quasi a sottolineare che le criticità incontrate dai legislatori belgi risultavano in realtà avere carattere diffuso in tutta l'UE, affondando le proprie radici non nei limiti o nell'approccio di un singolo legislatore nazionale bensì in questioni ben più profonde e condivise a livello europeo.

Su tutte queste complesse considerazioni quindi poggiava la decisione della Corte costituzionale di promuovere un rinvio pregiudiziale alla CGUE [55], chiedendo espressamente se una normativa come quella belga del 2016, che prevedeva sì una conservazione generalizzata ma che era anche accompagnata da garanzie solide quanto alla sicurezza dei metadati e all'accesso agli stessi, fosse da ritenersi in contrasto con quanto disposto dall'art. 15 Direttiva *e-Privacy*, letto congiuntamente alla Carta di Nizza e alla Convenzione EDU. Un quesito questo che, unitamente alle valutazioni proposte, pareva suggerire la possibilità di una lettura "globale" dei requisiti emersi dalla giurisprudenza della CGUE, così da non individuare nella mera *bulk data retention* un elemento di incompatibilità con il diritto dell'UE bensì proponendo una valutazione della normativa in materia di conservazione e accesso nel suo complesso e nell'insieme di tutele e salvaguardie predisposte. Nella stessa direzione era del resto da leggersi anche l'ulteriore rilevante quesito, volto a comprendere le possibili conseguenze di un eventuale annullamento della legge nazionale sulla *data retention*, che si sarebbe resa necessaria qualora i giudici di Lussemburgo avessero confermato una interpretazione avversa alla possibilità di adottare forme di conservazione generalizzata ed indiscriminata [56]. In particolare, i giudici belgi volevano indurre la CGUE a riflettere sulla possibilità di prorogare gli effetti di una normativa nazionale dichiarata incompatibile con il diritto dell'UE, al fine di evitare una situazione di incertezza giuridica e di compromettere così indagini in corso, con gravi ripercussioni sulla garanzia della sicurezza e sull'efficacia delle azioni di contrasto

[55] Domanda di pronuncia pregiudiziale proposta dalla *Cour constitutionnelle* il 2 agosto 2018, Causa C-520/18.

[56] La Corte si è chiesta e ha chiesto alla CGUE se «possano essere mantenuti provvisoriamente gli effetti (*di una tale legge*) al fine di evitare una situazione di incertezza giuridica e di permettere che i dati raccolti e conservati in precedenza possano ancora essere utilizzati per il raggiungimento degli obiettivi previsti dalla legge».

alla criminalità. Una questione così delicata, questa, che anche la Corte Suprema irlandese avrebbe poi successivamente posto alla CGUE, nel rinvio pregiudiziale C-140/20 *G.D. c. Commissioner of the Garda Siochana e altri*, ancora pendente.

4.3. *Di ritorno da Lussemburgo: la decisa risposta dei giudici costituzionali belgi nell'*Arrêt *22 aprile 2021, n. 57.*

L'attesa risposta ai complessi quesiti posti dalla *Cour Constitutionnelle* belga è giunta il 6 ottobre 2020, con la nota pronuncia *La Quadrature du Net*: come ampiamente osservato nel Capitolo 2 di questo lavoro, con questa decisione di estremo rilievo la CGUE ha introdotto, con riferimento alla disciplina della *data retention*, una distinzione tra finalità di sicurezza nazionale da un lato e repressione di reati gravi dall'altro: se per il perseguimento del primo scopo, una forma di *bulk data retention*, pur accompagnata da precise salvaguardie e specifiche condizioni e limitazioni, può essere considerata uno strumento proporzionato, per finalità di sicurezza pubblica è stata invece nuovamente ribadita l'incompatibilità con il diritto dell'UE della conservazione generalizzata ed indiscriminata; la discussa *targeted data retention* rimane dunque, in tale contesto, l'unico strumento che gli Stati membri possono legittimamente adottare.

I giudici costituzionali così, riprendendo il ricorso dinnanzi ad essi promosso nel 2017 e proprio (ri)partendo dall'analisi della posizione espressa dalla CGUE, si sono pronunciati con l'*Arrêt* 22 aprile 2021, n. 57, in quella che si è rivelata sin da subito una sentenza dagli effetti "sconvolgenti" per la disciplina della *data retention* in Belgio. A un solo giorno di distanza dalla sentenza del *Conseil d'État* francese, anche questo similmente chiamato a riprendere le redini del processo interrottosi con il rinvio pregiudiziale, la *Cour Constitutionnelle* ha annullato gli articoli 2, b), da 3 a 11 e 14 della legge del 29 maggio 2016 posta alla sua attenzione: dinnanzi alla chiara posizione espressa nella pronuncia *La Quadrature du Net*, infatti, la Corte non ha potuto che riconoscere la previsione di una conservazione generalizzata ed indiscriminata per scopi di garanzia della sicurezza pubblica, imposta dalla normativa belga, in contrasto con l'art. 15 Direttiva *e-Privacy* letto alla luce della Carta di Nizza e della Costituzione nazionale. La distinzione operata dalla legge del 2016 circa le

procedure di accesso relative ai dati d'identificazione, a quelli riguardanti il servizio/mezzo di comunicazione impiegato dall'utente e ai metadati genericamente intesi, non è stata dunque considerata una forma di limitazione alla conservazione conforme ai criteri indicati dalla CGUE: «cette catégorisation ne correspond par ailleurs pas aux distinctions qui sont opérées par la Cour de justice dans son arrêt du 6 octobre 2020 en ce qui concerne les différentes catégories de données susceptibles de faire l'objet d'une obligation de conservation généralisée et indifférenciée», para. B.17 [57]. Sulla base di queste brevi – ed invero piuttosto sbrigative – valutazioni, la Corte belga è giunta così ad una affermazione di estremo rilievo: «l'arrêt de la Cour de justice (…) impose un changement de perspective par rapport au choix que le législateur a effectué: l'obligation de conservation des données relatives aux communications électroniques doit être l'exception, et non la règle. La réglementation prévoyant une telle obligation doit par ailleurs être soumise à des règles claires et précises concernant la portée et l'application de la mesure en cause et imposant des exigences minimales», para. B.19. Ne deriva come «il appartient au législateur d'élaborer une réglementation qui respecte les principes applicables en matière de protection des données à caractère personnel, à la lumière de la jurisprudence de la Cour de justice, et de tenir compte, le cas échéant, des précisions apportées par celle-ci en ce qui concerne les différents types de mesures législatives jugées compatibles aver l'art. 15, para. 1, de la Charte des droits fondamentaux de l'Unione européenne», para. B. 19. Ciò basta per giungere all'annullamento delle disposizioni della legge del 2016.

Una disamina dunque che, similmente a quanto avvenuto in passato all'indomani della sentenza *DRI*, ha riproposto in maniera sintetica le posizioni espresse dalla CGUE, fermandosi peraltro alla materia della con-

[57] Si ricorda infatti che i giudici di Lussemburgo hanno operato una distinzione quanto alla legittimità dell'intrusione nella sfera privata di una forma di conservazione generalizzata a seconda che si tratti di metadati, indirizzi IP o dati identificativi: solo per queste ultime due tipologie di dati, ritenuti meno lesivi della riservatezza – non essendo in grado, da soli, di rivelare informazioni circa le abitudini o relazioni sociali degli utenti e dunque rappresentando una ingerenza non grave –, è possibile impiegare una forma di *bulk data retention*, pur, anche in questo caso, sottoposta a precisi limiti e garanzie.

servazione, senza cioè giungere ad analizzare la legittimità e proporzionalità delle garanzie poste alla fase di accesso dei metadati, della durata della *data retention* o delle salvaguardie predisposte quanto alla sicurezza dei dati. La sola previsione di una conservazione generalizzata è sufficiente, ancora una volta, per ravvisare l'incompatibilità della normativa nazionale con il diritto dell'UE [58].

Quella dalla Corte costituzionale belga si rivela così certamente una decisione di estremo rilievo non solo nel contesto nazionale ma anche in quello europeo: essa si presenta quale esemplificazione di un approccio giurisprudenziale peculiare e differente da quello adottato in altri Stati membri. Ciò diviene ancor più evidente se si osserva la richiamata sentenza del Consiglio di Stato francese, dalla portata diversa, se non per certi versi addirittura opposta rispetto a quella qui analizzata: mentre nella sua fortemente dibattuta e controversa pronuncia la Corte francese di *Palais-Royal* ha ritenuto in gran parte sussistenti le condizioni e i requisiti indicati dalla CGUE al fine di garantire la proporzionalità di un regime di *bulk data retention* per scopi di sicurezza nazionale, facendo così par-

[58] Con riferimento poi alla delicata questione relativa agli effetti dell'annullamento della normativa in materia di *data retention* rispetto agli elementi di prova impiegati in procedimenti penali e originati proprio da una conservazione generalizzata successivamente ritenuta in contrasto con il diritto dell'UE, la Corte costituzionale belga richiama in maniera ampia le considerazioni svolte dalla CGUE nella sentenza *La Quadrature du Net*: i giudici costituzionali perciò riconoscono di non poter legittimamente conservare e mantenere, neppure provvisoriamente, gli effetti delle disposizioni annullate. Così «il appartient au juge pénal compétent de statuer, le cas échéant, sur l'admissibilité des preuves qui ont été recueillies lors de la mise en œuvre des dispositions annulées conformément à l'art. 32 du titre préliminaire du Code de procédure pénale et à la lumière des précisions apportées par la Cour de justice dans l'arrêt du 6 octobre 2020», para. B.24.3. I timori espressi dal Governo belga e, in parte, anche dai giudici costituzionali stessi, quanto alle potenziali dirompenti conseguenze dell'annullamento della normativa nazionale sulla certezza giuridica, non possono dunque essere risolti con una limitazione nel tempo degli effetti dell'annullamento: è rimessa in capo ai singoli giudici la determinazione, nel caso concreto ad essi sottoposto, della ammissibilità delle prove, anche sulla base di quei criteri forniti dalla CGUE, già analizzati nel Capitolo 2. Se da un lato tale soluzione può certamente facilitare una valutazione *ad hoc* e specifica da parte dei giudici nei singoli procedimenti, risulta tuttavia chiaro come un approccio complessivo, quale quello della conservazione temporanea degli effetti della disciplina annullata, avrebbe comportato maggiore chiarezza e certezza.

zialmente salva la disciplina nazionale nonché mettendo in discussione l'efficacia e la legittimità costituzionale di una forma di conservazione targettizzata, i giudici costituzionali belgi hanno proposto invece una interpretazione ben più letterale della pronuncia dei giudici di Lussemburgo dell'ottobre 2020, ritenendo *in toto* incompatibile con il diritto dell'UE una normativa, quale quella del 2016, che riproponeva una conservazione generalizzata e che non inseriva quelle rigide limitazioni previste dalla giurisprudenza europea quanto al possibile impiego di un simile invasivo strumento per scopi di sicurezza nazionale [59]. Una lettura, quest'ultima, che non mette in discussione la fattibilità tecnica, l'utilità o la proporzionalità di una forma di conservazione targettizzata e che anzi affida unicamente e in maniera invero sintetica e rapida al solo legislatore nazionale il compito di valutare e approvare forme di conservazione in grado di rispettare i puntuali requisiti sanciti dalla giurisprudenza sovranazionale.

L'esito di questo giudizio porta dunque alla luce, in maniera limpida e incontrovertibile, quanto le problematiche e criticità legate alla disciplina della *data retention* siano tutt'altro che risolte e quanto la giurisprudenza della CGUE non possa considerarsi interamente risolutiva di quelle complesse questioni che ancora oggi interessano tanto le Istituzioni europee quanto i legislatori e i giudici nazionali: partendo dalla medesima sentenza *La Quadrature du Net*, è significativo come, a distanza di un giorno l'una dall'altra, due alte Corti in due differenti Stati membri si siano pronunciate in maniera tanto differente, in un caso adottando una lettura definita "*customized*" dei principi stabiliti dai giudici di Lussemburgo [60] e nell'altro invece optando per una attuazione strettamente aderente a quanto disposto dalla CGUE, senza valutare le specifiche e peculiari condizioni e limiti complessivamente stabiliti dal legislatore nazionale del 2016.

---

[59] Questa distanza di approcci e letture è stata del resto evidenziata in alcuni primi commenti alle due pronunce nazionali citate: sul punto si rimanda a M.-C. DE MONTECLER, *Conservation des données: la Cour constitutionnelle belge donne sa lecture*, in *Dalloz. Actualité. Le quotidien du droit*, 28 aprile 2021 ma anche alla ampia dottrina richiamata nel Capitolo 2.

[60] A. VEDASCHI, *"Customizing" La Quadrature du Net: the French Council of State, national security and data retention*, cit.

Se questo complesso quadro apre inevitabilmente a più ampie e approfondite riflessioni sul futuro della *data retention* nell'UE, già in parte anticipate e che vedranno nelle considerazioni conclusive di questo lavoro un ulteriore spazio, la sentenza della *Cour constitutionnelle* belga ripropone nel più specifico contesto nazionale problematiche e criticità di cui il legislatore belga dovrà ora – e come in passato – farsi carico, nel difficile tentativo di determinare un punto di equilibrio tra esigenze securitarie e tutela dei diritti fondamentali.

4.4. *Ancora una difficile prova per il legislatore belga: cenni all'*Avant-project de loi *proposto dal Governo.*

Come facile prevedere e come in una sorta di *deja-vu*, la sentenza della Corte costituzionale ha determinato reazioni molto differenti: accolta vittoriosamente dalle ONG che avevano promosso il ricorso di annullamento nel 2017 [61], la decisione ha però provocato preoccupazione in capo alle autorità di *law enforcement* e di intelligence, che hanno nuovamente invocato un rapido intervento normativo in grado di predisporre tutele adeguate senza inficiare l'efficacia e l'efficienza dello strumento della *data retention* [62]. Sotto questa spinta, i *vice-Premiers Ministres* Van Quickenborne e De Sutter e i Ministri Dedonder e Verlinden hanno prsentato il 7 maggio 2021 un primo *avant-projet de loi* relativo alla conservazione dei metadati e un *project d'arrêté royal* volto a modificare il vigente *arrêté* del 2013. Questo progetto di legge, definito significativamente «une solution pour concilier vie privée et sécurité» [63] e attualmente ancora in fase

[61] La *Ligue des droits humains*, ad esempio, ha visto nella pronuncia della Corte il riconoscimento che «la surveillance généralisée et indiscriminée des personnes est incompatible avec les valeurs démocratiques», come riportato da J. BALBONI, M. SAMAIN, *La conservation des données télécom au coeur d'une guerre de pouvoir*, in *L'Echo*, 25 maggio 2021.

[62] Come evidenziato da Petra De Sutter, *vice-Premier Ministre*, «la police et la justice verront ainsi disparaître un important outil d'enquête. En effet, l'on recourt aux données de télécommunications dans 90% des enquêtes judiciaires», in *Communiqué de presse*, 7 maggio 2021, disponibile all'indirizzo https://desutter.belgium.be/fr/le-conseil des-ministres-approuve-le-nouveau-projet-de-loi-sur-la-conservation-des-donn%C3%A9es.

[63] *Ibidem.*

di valutazione, contiene alcuni profili di grande rilievo: per la prima volta, infatti, viene promossa non solo una forma di conservazione dei metadati targettizzata sulla base di criteri geografici, ma anche una distinzione chiara per quanto attiene alla finalità di garanzia della sicurezza nazionale, per la quale è prevista una durata più prolungata di conservazione in ragione dei livelli di minaccia individuati dall'OCAM, l'*Organe de coordination pour l'analyse de la menace*[64].

Quanto al primo profilo, il progetto proposto mira ad introdurre un obbligo di conservazione di dodici mesi per gli indirizzi IP – come si è visto esclusi dal divieto di conservazione generalizzata secondo quanto disposto dai giudici della CGUE –, mentre con riferimento ai dati di traffico e di ubicazione la *data retention* dovrebbe avere carattere mirato, cioè riguardante solo specifiche aree geografiche; esse in particolare dovrebbero essere individuate mediante criteri ben determinati, come il numero di reati di cui all'art. 90-*ter* del *Code d'instruction criminelle* verificatisi in una zona o in un *arrondissement judiciaire* o le aree per le quali l'OCAM individua un livello di pericolo pari o superiore a 3 – ovvero livello grave, per il quale il rischio del verificarsi di una minaccia alla sicurezza nazionale è verosimile e probabile o, nel caso del livello 4, di un pericolo serio ed imminente –, o ancora luoghi espressamente definiti, quali a titolo esemplificativo aeroporti, porti o sedi di importanti istituzioni, considerati potenzialmente a maggior rischio di divenire teatro della commissione di reati. Anche la durata della conservazione è modulata sulla base del grado di pericolo delle diverse are geografiche individuate, pur sempre nel limite massimo di dodici mesi. Permane comunque un obbligo di conservazione generalizzata di un anno ai soli e ristretti fini di «lutter contre la fraude ou l'utilisation malveillante du réseau de communications électroniques, et pour garantir la sécurité des réseaux».

Proprio questi profili sono stati criticati dalla *Autorité de protection des données*, alla quale è stato richiesto un vaglio preventivo circa la confor-

[64] Questo organo, istituito con la *Loi du 10 juillet 2006 relative à l'analyse de la menace*, sostituisce il *Groupe interforces antiterroriste* e ha il compito di effettuare una periodica valutazione della minaccia terroristica basandosi sulle informazioni fornite da organi quali il *Service Général du Renseignement et de la Sécurité*, la polizia *local* e quella federale, le autorità doganali.

mità del progetto ai requisiti fissati in particolare dal diritto dell'UE. Nel suo lungo e dettagliato *Avis* 28 giugno 2021, n. 108, l'Autorità ha innanzitutto specificato come, nel complesso e pur ravvisando alcuni positivi tentativi di adeguamento della disciplina interna, il progetto non realizzi completamente quel cambio di prospettiva imposto dalla Corte costituzionale nella sua pronuncia, ovvero di considerare l'obbligo di conservazione come l'eccezione e non la regola. La confermata previsione di una *data retention* ampia e priva di restrizioni territoriali, seppur limitatamente a determinati scopi sopra richiamati, quali appunto la lotta alle frodi o all'utilizzo illecito di reti di telecomunicazione, rischia di «aboutir à réintroduire, *de facto*, des obligations de conservation généralisée et indifférenciée des données», para. 47; in altre parole, l'Autorità manifesta significativi dubbi quanto alla proporzionalità e necessità di una conservazione sistematica di metadati per scopi di prevenzione e repressione di reati, quali quelli indicati, certamente limitati e precisamente individuati ma la cui gravità – e dunque capacità di legittimare una forma di conservazione generalizzata – resta dubbia. Inoltre, per quanto attiene all'innovativo criterio geografico, volto a garantire una *targeted data retention* secondo le indicazioni della CGUE, vengono riproposte alcune perplessità e timori che già avevano caratterizzato il dibattito a livello europeo, tra cui il pericolo di discriminazione nei confronti di soggetti che risiedono in aree ad alto tasso di criminalità o considerate maggiormente a rischio. Particolare attenzione dunque deve essere posta ai criteri di determinazione delle zone nelle quali la conservazione è resa obbligatoria, in modo che tale soluzione non risulti nei fatti né discriminatoria né interpretata in maniera talmente estensiva da condurre *de facto* ad un ritorno alla *bulk data retention*.

Insomma, numerose e precise osservazioni sono state formulate dalla Autorità garante belga, che ha in conclusione richiesto una maggiore chiarezza nelle disposizioni da adottare ma anche una valutazione più approfondita e cauta quanto alla proporzionalità e necessità dell'obbligo di conservazione, della sua durata e della possibilità di accesso. Pare rilevante quindi richiamare il monito finale presente nel recente *Avis* predisposto dalla Autorità: «Une nouvelle annulation par la Cour constitutionnelle de la loi serait de nature à entacher la confiance des citoyennes et les citoyens dans les institutions démocratiques. Il est, dans cette perspective,

tout à fait crucial de s'assurer que l'avant-projet de loi ne réintroduise pas, *de jure* ou *de facto*, une obligation de conservation généralisée et indifférenciée des données de trafic ou de localisation de l'ensemble ou d'une proportion trop importante des utilisateurs de moyens de communications électroniques en Belgique», p. 77.

Sarà dunque interessante osservare gli sviluppi futuri di questa proposta per comprendere se il Governo e il Parlamento procederanno nella direzione di integrare le considerazioni dell'*Autorité* nel testo normativo.

5. *Un approfondito dibattito legislativo e una attenta considerazione dei criteri enunciati dalla giurisprudenza della CGUE: ingredienti per un approccio virtuoso o per un fallimento annunciato?*

La ricostruzione dei puntuali interventi della Corte costituzionale belga [65], nonché dei continui sforzi posti in essere dal legislatore al fine di reagire ai significativi e dirompenti effetti della giurisprudenza tanto na-

[65] Per completezza, è bene ricordare che la Corte costituzionale belga ha promosso un ulteriore rinvio alla CGUE relativo alla disciplina in materia di trasferimento, conservazione e trattamento di PNR: i giudici belgi infatti sono stati chiamati nel 2017 a valutare la conformità alla Costituzione della normativa nazionale *Loi du 25 décembre 2016 relative au traitement des données des passagers*, trasposizione della Direttiva UE 2016/681. Dal ricorso di annullamento presentato ancora una volta dalla ONG *Ligue des droits humains* è scaturita una attenta analisi della Corte costituzionale non solo della normativa interna bensì anche della Direttiva di riferimento nonché della rilevante giurisprudenza della CGUE in materia di trasferimento dati e di PNR (*Parere 1/15* in particolare). I dubbi significativi quanto alla conformità al diritto dell'UE della disciplina belga e, indirettamente, della regolamentazione europea, hanno portato i giudici ad indirizzare alcuni importanti quesiti pregiudiziali alla CGUE volti, per quanto qui maggiormente rileva, a determinare se un sistema di raccolta, trasferimento e trattamento generalizzato di PNR, che riguarda cioè tutti i passeggeri aerei, sia da ritenersi compatibile con gli artt. 7, 8 e 52 della Carta di Nizza, anche in assenza di elementi oggettivi che consentano di creare una connessione tra il soggetto cui i PNR si riferiscono e un rischio per la sicurezza pubblica, requisito invece richiesto dalla costante giurisprudenza in materia di conservazione e accesso ai metadati. Anche questo rinvio, ancora pendente dinnanzi alla CGUE, rivela la grande attenzione e l'accurata analisi svolta dai giudici costituzionali belgi con riguardo alla delicata disciplina della conservazione e accesso a dati e metadati per scopi securitari.

zionale quanto sovranazionale, senza ignorarne o limitarne la portata e anzi prestando una lucida e approfondita attenzione ai principi in essa emersi, mostrano con chiarezza le peculiarità dell'approccio belga alla sfida della *data retention*.

Se le prime normative in materia di conservazione dei metadati, risalenti al 2000, risultavano espressione di una tensione pro-securitaria, volta a sfruttare appieno le potenzialità della *data retention*, esse si sono tuttavia ben presto scontrate con una ulteriore consapevolezza: quella dei pericoli concreti che un tale strumento comporta per il godimento e la tutela dei diritti fondamentali. Una consapevolezza che si è del resto manifestate nelle rimostranze, perplessità e contrasti caratterizzanti il difficile e lungo percorso legislativo che aveva condotto, con notevole ritardo, alla adozione della disciplina nazionale di attuazione della DRD.

Il dibattito su tale delicata disciplina è divenuto poi ancor più complesso a seguito degli interventi della Corte costituzionale belga: con le pronunce sopra esaminate, in particolare, i giudici hanno imposto al legislatore una seria riflessione sulle salvaguardie e sui confini da porre in essere sia rispetto alla fase della conservazione dei metadati sia al successivo accesso, in piena conformità e concordanza con i requisiti stabiliti dalla giurisprudenza della CGUE. Ecco dunque che da un punto di partenza fortemente sbilanciato a favore della garanzia della sicurezza, si è gradualmente passati, anche e soprattutto mediante l'intervento delle Corti – sollecitate dall'attivismo di cittadini ed ONG – ad un approccio maggiormente critico verso lo strumento della *data retention* e alla previsione di sempre più stringenti e precise garanzie e limitazioni.

In questo contesto, la rilevanza degli accadimenti avvenuti a livello europeo affiora con grande forza: nelle continue pronunce della Corte costituzionale non può che ravvisarsi l'incidenza delle decisioni dei giudici di Lussemburgo e l'importanza della promozione di un dialogo con questi ultimi volto ad ottenere chiarimenti e, come nel caso del rinvio pregiudiziale del 2018, finanche a promuovere una lettura meno rigida dei criteri individuati nelle sentenze *DRI* e *Tele2*, evidenziando le difficoltà reali incontrate dal legislatore nell'attuazione di tali principi. Se si guarda alle scelte del Governo e del Parlamento, poi, si nota come questi, similmente ai giudici nazionali, abbiano svolto un approfondito studio della portata delle pronunce della CGUE, avviando una critica ma concreta

riflessione sui requisiti da esse fissati. Pur essendo giunto, nella normativa del 2016 così come nel progetto di legge attualmente ancora in discussione, ad una soluzione consapevolmente di compromesso tra l'elevato standard di tutela posto dalla giurisprudenza europea e la necessità di preservare lo strumento della *data retention*, il legislatore belga ha espressamente ammesso i limiti e le problematiche riscontrate nella predisposizione del nuovo dettato normativo, allontanandosi così dall'atteggiamento di chi – anche nel contesto nazionale italiano – ha quasi del tutto ignorato le conseguenze dell'intervento deciso della CGUE o ne ha interpretativamente limitato o riletto la portata, come accaduto nel Regno Unito e, più recentemente, in Francia, con la discussa pronuncia del *Conseil d'État*. Il legislatore belga, infatti, non ha cercato di aggirare i problemi e le criticità emerse, bensì ha provato a fornire una lettura – non troppo forzata e lontana da quanto chiaramente espresso dai giudici di Lussemburgo – in grado di consentire alla autorità di *law enforcement* e di intelligence di disporre di un efficace sistema di lotta alla criminalità. Questo approccio può ben essere rinvenuto nel tentativo di passare da disposizioni generiche e vaghe, quali quelle della legge del 2013, che lasciavano ampio spazio all'intervento del Governo mediante l'adozione di decreti, a norme invece più precise e determinate nonché a salvaguardie specifiche riguardanti l'accesso ai metadati, sino alla previsione, attualmente in fase di valutazione e approvazione, di una conservazione limitata a determinate zone geografiche, benché accompagnata da eccezioni ancora dibattute. Con quest'ultima proposta il Governo ha peraltro dimostrato di saper fare un passo indietro rispetto alle posizioni precedentemente assunte con riferimento alla *targeted data retention*, ritenuta in passato irrealizzabile ed inefficace ma divenuta l'unica possibile strada da percorrere dinnanzi alle più recenti pronunce della CGUE. Così la soluzione prospettata nel maggio 2021 rappresenta certamente un intervento innovativo e sotto taluni profili persino creativo, nella parte in cui viene operato ad esempio un richiamo ai livelli di rischio predisposti dall'OCAM quali possibili elementi di riferimento al fine di addivenire ad una delimitazione dell'obbligo di *data retention* su base geografica nonché temporale, essendo prevista la possibilità di prolungare l'obbligo di conservazione sino al perdurare di un pericolo per la sicurezza di grado 3 o 4. Questo primo tentativo è dunque prova della volontà del Governo di agire sì con rapidità per

rispettare le esigenze sottolineate dalle autorità di *law enforcement* e di intelligence, ma anche con cautela e ponderazione così da adottare una disciplina normativa efficace ma stabile e capace cioè di scongiurare – o quanto meno resistere ad – un ulteriore intervento della Corte costituzionale: come sottolineato nel documento predisposto dalla Autorità garante nazionale, un nuovo annullamento della legge nazionale per incompatibilità con il diritto dell'UE avrebbe infatti il pericoloso effetto di aumentare ulteriormente confusione ed incertezza.

Sebbene il futuro della *data retention* in Belgio sia pertanto ancora tutto da determinare, quanto può sin da ora essere rilevato è come i più recenti sviluppi, dall'intervento della Corte costituzionale al progetto di legge sopra analizzato, confermino la consapevolezza del rilievo del sistema della *data retention* e dell'importanza di predisporre rapidamente una normativa dedicata, senza però limitare il dibattito e l'attenzione che una materia così delicata richiede. Senza dubbio il recente sforzo del Governo belga di integrare una forma targettizzata di conservazione nel proprio ordinamento denota un atteggiamento molto differente da quello ad esempio registratosi in Francia ad opera dell'intervento del *Conseil d'État*: mentre quest'ultimo ha messo fortemente in dubbio, se non *de facto* escluso, la realizzabilità e legittimità di una *targeted data retention*, tale soluzione è stata invece accolta dai Ministri belgi promotori del progetto di legge esaminato, che pure non ha escluso *in toto* una forma generalizzata per taluni limitati scopi e per specifiche categorie di dati. Facendo questo, e lungi dal presupporre un approccio acritico e poco consapevole delle problematicità reali di una corretta attuazione dei criteri stabiliti dalla CGUE, l'approccio del Governo belga rivela tutta la complessità di un bilanciamento che pare ancora difficile da realizzarsi nella concretezza delle scelte normative.

CAPITOLO 6

L'ITALIA. I MOLTEPLICI INTERVENTI NORMATIVI E GIURISPRUDENZIALI IN MATERIA DI *DATA RETENTION*, TRA OCCASIONI PERDUTE E UN DIBATTITO CHE FATICA AD AFFERMARSI

SOMMARIO: 1. La disciplina normativa in materia di *data retention*. – 1.1. Il frenetico susseguirsi di modifiche all'art. 132 Codice Privacy. – 1.2. Dalle deroghe legate ad esigenze emergenziali alla Legge Europea 2017, sino al d.lgs. 10 agosto 2018, n. 101. – 2. Le Corti italiane e la *data retention*: una lettura restrittiva dei principi e criteri definiti dalla CGUE. – 2.1. La sentenza della Corte costituzionale 14 novembre 2006, n. 372: una conferma del corretto bilanciamento tra diritti fondamentali e garanzia della sicurezza. – 2.2. La rilevante e discussa Ordinanza del Tribunale di Padova: una prima presa di posizione dei giudici italiani dinnanzi alle pronunce della CGUE. – 2.3. La costante giurisprudenza della Corte di Cassazione: un approccio "rassicurante". – 3. Dall'impegno di riforma assunto dal Governo al rinvio pregiudiziale promosso dal Tribunale di Rieti: l'Italia verso una reale svolta? – 3.1. Le ripercussioni della sentenza *H.K. c. Prokuratuur* nel contesto italiano. – 3.2. Il mancato dibattito sulla proporzionalità della conservazione generalizzata: necessarie riflessioni.

1. *La disciplina normativa in materia di* data retention.

1.1. *Il frenetico susseguirsi di modifiche all'art. 132 Codice Privacy.*

Volendo proseguire nella ricostruzione dei differenti approcci nazionali adottati dinnanzi alla sfida della *data retention*, particolare attenzione deve essere posta alla disciplina normativa e alle vicende giurisprudenziali

che hanno caratterizzato l'Italia e che presentano senza dubbio notevoli peculiarità. Mentre i due Stati sino ad ora analizzati si sono rivelati protagonisti di un intenso dialogo con i giudici di Lussemburgo, frutto di una ampia discussione precedente o successiva alla adozione di specifiche normative sulla *data retention* e di un attento intervento delle Corti nazionali, spesso grazie all'attivismo di ONG e cittadini, l'Italia ha invece conosciuto da un lato una quasi totale mancanza di dibattito legislativo quanto alla proporzionalità dello strumento della conservazione e accesso ai metadati per scopi securitari e dall'altro una costante adozione, da parte dei giudici nazionali, di letture fortemente «restrittive degli standard garantistici enunciati dalla CGUE», mosse dall'intento «di salvare la disciplina interna (…) ed evitare ipotesi di inutilizzabilità probatoria» [1]. Solo recentemente le Corti e il legislatore nazionale paiono aver intrapreso, con notevole ritardo rispetto a quanto avvenuto negli altri Stati membri, una strada differente, maggiormente sensibile alla complessità e delicatezza – forse prima coscientemente ignorata – della materia, tanto da promuovere per la prima volta un rinvio ai giudici di Lussemburgo.

Per poter comprendere questi rilevanti sviluppi, nonché al fine di riflettere sulle specificità dell'approccio italiano, si rende necessario innanzitutto provvedere ad una ricostruzione critica dell'assetto normativo vigente e della sua evoluzione nel tempo.

Questa disamina non può che prendere abbrivio dalla primigenia e ancora oggi principale disposizione di riferimento in materia di *data retention* [2]: l'art. 132 del d.lgs. n. 196/2003 [3]. Nella sua versione originale,

---

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

[2] Con riferimento invece all'acquisizione e accesso da parte delle autorità di *law enforcement* di dati relativi al contenuto delle telecomunicazioni bisogna fare riferimento alla disciplina sulle intercettazioni telefoniche, di flussi telematici o informatici, che richiedono una previa autorizzazione del giudice. Per maggiori approfondimenti sul punto, si rimanda, *ex multis*, a S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018 e A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, Milano, 2019.

[3] D.lgs. 30 giugno 2003, n. 196, *Codice in materia di protezione dei dati personali*, meglio noto come Codice Privacy.

questa previsione stabiliva in capo ai fornitori di servizi di telefonici [4] un generale obbligo di conservazione dei metadati (anche detti "dati esterni delle comunicazioni") relativi al traffico telefonico per una durata di trenta mesi, per scopi di accertamento e repressione di reati [5]. Tale misura, predisposta ben prima della adozione della DRD, risultava attuativa dell'art. 15 Direttiva *e-Privacy* che, come noto, concedeva agli Stati membri di predisporre, per specifiche ma ampie finalità securitarie, una disciplina derogatoria rispetto all'obbligo generale di cancellazione (o anonimizzazione) dei dati e metadati. Si veniva quindi a creare un regime di *bulk data retention* volto a consentire alle autorità di *law enforcement* la possibilità di disporre dei dati conservati e di accedervi al fine di indagare e reprimere qualsiasi tipologia di reato, senza alcun riferimento al carattere di gravità dei reati stessi; non era pertanto richiesto che lo scopo perseguito fosse di una severità tale da giustificare una significativa ingerenza nella vita privata degli utenti.

Il dettato normativo originario dell'art. 132, così come sopra descritto, non ha però avuto lunga vita: esso, piuttosto singolarmente, era stato modificato mediante d.l. 24 dicembre 2003, n. 354 (convertito con legge 26 febbraio 2004, n. 45), proprio a pochi mesi dalla sua adozione e ancor prima dell'entrata in vigore del Codice Privacy entro cui era inserito. Il testo riformato stabiliva innanzitutto una nuova durata della conservazione, per finalità generiche di repressione e accertamento dei reati, pari a ventiquattro mesi, inserendo inoltre una distinzione (c.d. doppio binario) riguardante la conservazione dei metadati necessari alla lotta ai reati più

---

[4] Venivano all'epoca esclusi dall'obbligo di conservazione i dati telematici.

[5] Tale disciplina rappresentava una deroga alla regola generale fissata all'art. 123 del medesimo Codice, secondo cui il trattamento dei dati da parte dei fornitori di servizi di telecomunicazione doveva essere limitato a quanto strettamente necessario per finalità di fatturazione, pagamento in caso di interconnessione, documentazione in caso di contestazione della fattura o per pretesa di pagamento e per un periodo comunque non superiore a sei mesi. Con riferimento a tale norma, dunque, il principio guida generale era da ricondursi alla «c.d. *data protection* (in contrapposizione alla *data retention*), per cui il soggetto interessato ha diritto a non vedere diffondere all'esterno aspetti della propria vita privata, nella specie i dati relativi alle proprie comunicazioni telefoniche», C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, 2008, p. 399.

gravi, individuati in quelli previsti dall'art. 407, co. 2, lett. a) c.p.p. [6] e nei delitti a danni di sistemi informatici e telematici, per i quali veniva previsto un obbligo di conservazione di ulteriori ventiquattro mesi, oltre ai ventiquattro già previsti, arrivando quindi ad un massimo di quattro anni totali [7]. Tale differenziazione in realtà comportava un aggravio in capo al

[6] Essi sono «i delitti appresso indicati: 1) delitti di cui agli articoli 285 (devastazione, saccheggio e strage), 286 (guerra civile), 416-*bis* (associazioni di tipo mafioso anche straniere) e 422 del codice penale (strage), 291-*ter*, limitatamente alle ipotesi aggravate previste dalle lettere a), d) ed e) del co. 2, e 291-*quater*, co. 4, del testo unico approvato con decreto del Presidente della Repubblica 23 gennaio 1973, n. 43; 2) delitti consumati o tentati di cui agli articoli 575 (omicidio), 628, co. 3 (rapina) 629, co. 2 (estorsione), e 630 dello stesso codice penale (sequestro di persona a scopo di estorsione); 3) delitti commessi avvalendosi delle condizioni previste dall'articolo 416 bis del codice penale ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo; 4) delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui agli articoli 270, co. 3 (associazione sovversiva), [270 *bis* 2], e 306, co. 2, del codice penale (banda armata); 5) delitti di illegale fabbricazione, introduzione nello Stato, messa in vendita, cessione, detenzione e porto in luogo pubblico o aperto al pubblico di armi da guerra o tipo guerra o parti di esse, di esplosivi, di armi clandestine nonché di più armi comuni da sparo, escluse quelle previste dall'articolo 2, co. 3, della legge 18 aprile 1975, n. 110; 6) delitti di cui agli articoli 73, limitatamente alle ipotesi aggravate ai sensi dell'articolo 80, co. 2, e 74 del Testo unico delle leggi in materia di disciplina degli stupefacenti e sostanze psicotrope, prevenzione, cura e riabilitazione dei relativi stati di tossicodipendenza, approvato con decreto del Presidente della Repubblica 9 ottobre 1990, n. 309, e successive modificazioni; 7) delitto di cui all'articolo 416 del codice penale (associazione per delinquere) nei casi in cui è obbligatorio l'arresto in flagranza; 7-*bis*) dei delitti previsti dagli articoli 600 (riduzione o mantenimento in schiavitù o in servitù), 600-*bis*, co. 1, 600 ter, co. 1 e 2, 601, (tratta di persone), 602 (acquisto e alienazione di schivi), 609-*bis* (violenza sessuale) nelle ipotesi aggravate previste dall'articolo 609 *ter*, 609 *quater*, 609-*octies* del codice penale, nonché dei delitti previsti dall'art. 12, co. 3, del testo unico di cui al decreto legislativo 25 luglio 1998, n. 286, e successive modificazioni».

[7] Questa modifica, così rapidamente adottata, è da leggersi quale risposta alle forti critiche che avevano accompagnato la prima versione dell'art. 132 Codice Privacy, considerato potenzialmente dannoso per una efficace garanzia della sicurezza. Secondo tale visione, il rischio era quello di causare la perdita di informazioni e metadati di rilevante importanza per le indagini e i procedimenti penali: «la straordinaria necessità e urgenza del d.l. 24 dicembre 2003, n. 354 è stata motivata sulla base del danno irreparabile che

fornitore di servizi di telecomunicazione: questi infatti non poteva anticipatamente sapere se i metadati prodotti dai propri utenti sarebbero stati utilizzati nell'ambito di indagini riguardanti i reati ritenuti maggiormente gravi previsti dai decreti legge o attinenti invece agli altri reati per i quali i termini di conservazione erano più brevi, così che *de facto* il *service provider* si trovava costretto a conservare tutti i metadati per il termine massimo previsto di quattro anni. Quella che veniva introdotta, quindi, non era affatto una limitazione dello strumento della *data retention*: questa era imposta per la repressione di qualsiasi reato e, solo con riferimento al successivo ed eventuale accesso ai metadati, la possibilità di "andare indietro nel tempo" e dunque di acquisire i metadati risultava ristretta a ventiquattro mesi per tutti i reati, mentre veniva ampliata per i reati considerati gravi. Rileva dunque come la facoltà di accesso, al di là della estensione temporale della conservazione, non fosse preclusa in alcun caso, neppure per i reati privi del carattere di "serietà". Quanto poi alla disciplina regolante le procedure di richiesta di acquisizione dei metadati, veniva individuato come atto necessario un decreto motivato del giudice, ottenibile su istanza del pubblico ministero, del difensore dell'imputato, di persona sottoposta a indagini, persona offesa e altre parti private [8].

---

l'originario articolo 132, una volta entrato in vigore, avrebbe prodotto, ossia l'eliminazione dei dati per i quali il periodo di custodia era scaduto; è lo stesso decreto legge a evidenziare la necessità di prevenirne la perdita nell'ipotesi in cui ne risulti necessaria l'acquisizione, in particolare, ai fini della repressione di reati di particolare gravità», M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Diritto Penale Contemporaneo*, 3, 2016, p. 171. Come lo stesso autore sottolinea, la legge di conversione aveva poi introdotto rilevanti modifiche rispetto al testo originario del Decreto: nella versione finale infatti sparivano i riferimenti ai dati telematici, che erano invece stati inseriti inizialmente tra le categorie di metadati da conservare, nonché la più ampia durata di trenta mesi, aumentata a sessanta per reati gravi; veniva anche prevista, in una ottica maggiormente garantista, l'autorizzazione preventiva del giudice, mentre il Decreto attribuiva tale compito anche al pubblico ministero.

[8] Il comma 3 della disposizione in esame infine stabiliva una distinzione tra dati relativi alle chiamate in arrivo e in uscita: solo per le prime veniva prevista una procedura più rapida e snella che consentiva l'accesso alle informazioni ad opera del difensore dell'imputato mediante richiesta diretta al fornitore del servizio di comunicazione, a condizione che l'ottenimento dei dati fosse finalizzato a prevenire un pregiudizio alle indagini difensive.

A pochi anni di distanza, il c.d. Decreto o Pacchetto Pisanu, contenente misure urgenti per il contrasto del terrorismo internazionale (d.l. 27 luglio 2005, n. 144, convertito con legge 31 luglio 2005, n. 155), introduceva una ulteriore rilevante novità destinata a ripercuotersi in maniera significativa sull'efficacia applicativa dell'art. 132 Codice Privacy; a seguito degli attentati terroristici di Madrid e Londra, che avevano riaffermato con drammaticità e forza l'esigenza di una ampia tutela della sicurezza all'interno del dibattito parlamentare e delle decisioni politiche, veniva infatti prevista una deroga alla regola della durata di conservazione indicata dall'art. 132: al fine di indagine e repressione dei soli reati di terrorismo, tutti i metadati dovevano essere trattenuti dagli operatori sino al 31 dicembre 2007, producendo l'estensione della *data retention* ad una data specifica, con una scelta che verrà riproposta dal legislatore italiano anche in successivi interventi normativi. Venivano poi sostanzialmente modificati anche i termini di conservazione e la procedura di accesso: mentre restavano invariati i ventiquattro mesi previsti per i dati relativi al traffico telefonico, cui si aggiungeva l'obbligo di conservazione dei dati attinenti alle chiamate senza risposta, veniva per la prima volta imposta anche la *retention* dei dati telematici, per un periodo di sei mesi, rimanendo sempre esclusi i contenuti delle comunicazioni stesse. Risultava inoltre mantenuta la distinzione (c.d. doppio binario) tra reati in generale e quelli di cui all'art. 407, co. 1, lett. a) c.p.p. e delitti a danno di sistemi informatici e telematici, riproponendo per questi ultimi un periodo di conservazione più ampio, di ulteriori ventiquattro mesi per i dati di traffico telefonico e sei mesi per i dati di traffico telematico. Per questi specifici reati, considerati più gravi, la richiesta di accesso ai dati continuava a dover essere autorizzata dal giudice, mentre la disciplina dell'accesso subiva, con riferimento a tutti gli altri reati, una significativa riforma motivata da «esigenze di snellimento della procedura»[9]: diveniva infatti sufficiente in quei casi il mero decreto motivato del pubblico ministero.

---

[9] Così le ha definite M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, cit., p. 176. Una scelta, questa, in realtà piuttosto dibattuta e contestata: «la soluzione maggiormente equilibrata, in linea con la disciplina dettata per i mezzi di ricerca della prova tradizionali (ispezioni, perquisizioni, sequestri), era la previsione del decreto motivato dell'autorità giudiziaria. Non ha senso, infatti, negare al giudice la legittima-

Mentre sino a tale momento le modifiche alla disciplina della *data retention*, apportate mediante ravvicinate e piuttosto confuse deroghe, erano comunque tutte attuative della facoltà espressa dall'art. 15 Direttiva *e-Privacy*, con il d.lgs. 30 maggio 2008, n. 109 veniva invece effettuato un intervento volto a dare attuazione alla Direttiva 2006/24/CE, apportando così una modifica profonda all'art. 132 Codice Privacy [10]. Risultava infatti superata la previa distinzione tra reati genericamente intesi, reati indicati dall'art. 407, co. 2, lett. a), c.p.p. e reati di terrorismo, così che per la finalità generica di repressione di qualsiasi reato veniva imposta una durata fissa di conservazione di due anni per il traffico telefonico, un anno per il traffico telematico e trenta giorni per le chiamate senza risposta, eliminando così il sistema del doppio binario. Rimaneva invece immutata la disciplina di accesso, sulla base della quale i metadati potevano essere richiesti con decreto motivato del pubblico ministero, anche su istanza presentata dal difensore dell'imputato, del soggetto sottoposto ad indagini, della vittima o ancora di altre parti private [11]. Il risultato di tutte le innovazioni in-

---

zione all'acquisizione», S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, Milano, 2019, p. 1584.

[10] Con legge 18 marzo 2008, n. 48 si era provveduto a modificare nuovamente l'art. 132, prevedendo un obbligo di conservazione da tre a sei mesi dei dati di traffico, a fini di svolgimento di indagini preventive e per accertamento e repressione di determinati reati. In questa sede si vuole tuttavia concentrare l'attenzione sugli interventi normativi più rilevanti e di maggiore impatto, pur nella consapevolezza che, oltre a quelli elencati, anche altre normative sono intervenute in materia nel corso del tempo. Per una più approfondita analisi della interezza degli interventi normativi intercorsi a partire dal 2003, si rimanda a C. FATTA, *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, cit; P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1, 2016. Per una analisi riguardante la disciplina normativa e la giurisprudenza attinente al periodo precedente alla adozione dell'art. 132 Codice Privacy, che qui non si vuole prendere in esame, si richiamano invece M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, cit.; G.M. BACCARI, *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, Milano, 2019, p. 1599 ss.

[11] Il dibattito circa la definizione dei soggetti abilitati a richiedere l'accesso ai metadati conservati e le procedure da seguire è stato ampio: prima si riteneva che l'ottenimento dei tabulati telefonici (dunque dei metadati delle comunicazioni) dovesse essere

trodotte dal Decreto in esame avevano finito così col produrre un assottigliamento delle tutele e limitazioni precedentemente previste, escludendo definitivamente, «ai fini dell'acquisizione, qualsiasi rilevanza della tipologia delle fattispecie criminose per cui si procede, parallelamente a una *reductio ad unum* delle modalità e degli organi legittimati a disporre dei dati» [12], nonché mancando di imporre specifiche misure di sicurezza in capo ai fornitori di servizi, ai quali veniva lasciata ampia discrezionalità anche nella determinazione delle "procedure interne" da porre in essere per rispondere alle richieste di accesso avanzate dalle autorità di *law enforcement*.

Proprio queste lacune, insieme alle ristrette garanzie previste, erano state oggetto, negli anni successivi, di particolare attenzione da parte della dottrina che, soprattutto all'indomani della sentenza *DRI*, aveva iniziato a riflettere seriamente sulle implicazioni dell'invalidazione della DRD per la disciplina italiana e ad interrogarsi sulla conformità della normativa nazionale rispetto ai requisiti e principi individuati dalla CGUE. Molti autori avevano così affermato, con decisione, come le condizioni disposte dall'art. 132 Codice Privacy non potessero essere considerate compatibili con gli elevati standard di tutela elaborati dai giudici di Lussemburgo: mancava non solo l'individuazione delle categorie di reati per le quali era consentito provvedere alla conservazione e all'accesso – che al contrario erano resi possibili per qualsiasi tipo di reato –, ma anche la determinazione dei criteri oggettivi volti a fissare un nesso tra conservazione/accesso e pericolo o sospetto di un reato; risultava inoltre dubbio il carattere di indipendenza del pubblico ministero e dunque la correttezza della attribuzione a tale organo dell'unica forma di controllo preventivo svolta sulla richiesta di accesso ai metadati [13].

---

sottoposto alle medesime regole processuali valide per le intercettazioni, per passare poi a considerare sufficiente un decreto motivato del Pubblico ministero, successivamente proponendo una autorizzazione del giudice su richiesta avanzata da p.m., optando infine, per il mero decreto del p.m. Questi aspetti, insieme ai rilevanti parallelismi riferiti alla disciplina delle intercettazioni, sono analizzati da P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, cit., nonché da M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, cit.

[12] M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, cit., p. 181.

[13] R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata quaestio(?)*, in *Diritto Penale Contemporaneo*, 3, 2017; similmente, anche Iovene affermava che, alla luce dei pa-

1.2. *Dalle deroghe legate ad esigenze emergenziali alla Legge Europea 2017, sino al d.lgs. 10 agosto 2018, n. 101.*

La problematicità e – per gran parte della dottrina che si era occupata del tema – l'evidente contrasto tra la disciplina italiana e quanto delinea-

---

rametri fissati dalla giurisprudenza europea, l'art. 132 Codice Privacy non rappresentava una restrizione legittima dei diritti tutelati dalla Carta di Nizza: la disciplina italiana «non pone alcun limite, oltre a quello strettamente temporale, alla conservazione dei dati di traffico telefonico e telematico, che risulta quindi indiscriminata; non limita a particolari forme gravi di criminalità l'uso dei dati (…); non prevede specifiche modalità per l'accesso, né richiede il vaglio di un giudice o di altra autorità indipendente (…); non distingue la durata della conservazione in base all'obiettivo perseguito o alla persona interessata ma semplicemente distinguendo tra dati relativi al traffico telefonico, a quello telematico e alle chiamate senza risposta; non prevede misure per la sicurezza dei dati», F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, in *Cassazione Penale*, 12, 2014, p. 808. Anche Caputo si esprimeva in questi termini: «ci troviamo evidentemente di fronte ad una normativa, l'art. 132 Cod. Privacy, che non risponde a quanto richiesto dalla sentenza della CGUE almeno per ciò che concerne il rapporto fra l'obbligo di conservare i dati e una minaccia per la sicurezza pubblica e la mancata previsione che tale obbligo sia correlato alla necessità di prevenire gravi reati», P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, cit., p. 7. Dello stesso avviso Marcolini, che ha ritenuto «difficilmente negabile che, se oggetto di scrutinio da parte della CGUE fosse stata non la Dir. 2006/24/CE, bensì l'art. 132 Cod. Privacy, l'esito sarebbe stato identico. A tacere di ogni altro profilo, una disciplina, quale quella nazionale, che consente la *data retention* per qualsiasi reato, anche in ipotesi di una contravvenzione di minima gravità, non supererebbe nemmeno lontanamente lo stress test comunitario», S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, cit., p. 1592. Talune critiche alla disciplina dell'art. 132 Codice Privacy erano addirittura state mosse a partire dalle sue più risalenti formulazioni: G.E. VIGEVANI, *Articolo 132*, in AA.VV., *Codice della privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Giuffrè, Milano, 2004, p. 1668, aveva espresso sin da subito dubbi quanto ai pericoli che la disciplina in esame presentava per i diritti fondamentali, pur riguardando i soli metadati, non necessariamente ed automaticamente da considerarsi meno invasivi della sfera privata rispetto ai contenuti delle comunicazioni. Non si può non rilevare, tuttavia, per completezza, come alcuni autori avessero al contrario ritenuto la normativa italiana di trasposizione della DRD eccessivamente restrittiva rispetto a quanto disciplinato dalla normativa dell'UE, vedendo nella durata contenuta prevista dal decreto esaminato (un solo anno per i dati telematici) una tutela ulteriore e maggiore rispetto ai limiti più ampi stabiliti dalla Direttiva 2006/24/CE (M. RICCARDI, *Dati esteriori delle comunicazioni e tabulati di traffico*, cit., p. 180).

to dalla CGUE, avevano portato, ancor prima della sentenza *Tele2* avente specificamente ad oggetto normative nazionali attuative dell'art. 15 Direttiva *e-Privacy*, ad invocare l'adozione di una riforma della normativa italiana in materia di *data retention*. Davanti al perdurante "silenzio assordante" del normatore europeo, infatti, spettava al legislatore italiano il difficile compito di adeguare la disciplina nazionale al diritto dell'UE, così come interpretato dai giudici di Lussemburgo: seguendo le orme di quanto in quel periodo stava avvenendo in altri Stati membri (Regno Unito, Lussemburgo e Germania, ad esempio), il Governo e/o il Parlamento avrebbero dovuto innanzitutto promuovere un intervento volto a verificare la conformità della normativa italiana ai criteri fissati dalla giurisprudenza della CGUE e, qualora la disciplina interna fosse stata trovata viziata dalle stesse carenze e violazioni dei diritti fondamentali che avevano caratterizzato la DRD, provvedere alla adozione di un nuovo testo normativo [14]. Similmente a quanto avvenuto a livello sovranazionale, anche in Italia questo percorso non ha però purtroppo avuto inizio.

Non solo: mentre in altri Stati membri, come il Belgio, i giudici nazionali erano stati investiti, dinnanzi all'inerzia del legislatore nazionale, di questioni di legittimità costituzionale della normativa attuativa della DRD, fungendo così da motore propulsivo per un rinnovato intervento legislativo e imponendo una più profonda riflessione sui requisiti che la nuova disciplina interna doveva possedere, in Italia le Corti nazionali non hanno svolto questo ruolo. Seppure l'analisi specifica e puntuale della giurisprudenza italiana in materia verrà elaborata nel successivo paragrafo, pare utile sin da ora sottolineare come non si sia registrata a seguito

[14] Come ben precisato da Iovene, «spetta ai legislatori nazionali verificare se la normativa nazionale di attuazione della direttiva rispetti o meno le indicazioni fornite dalla CGUE. Infatti, poiché la direttiva lasciava margini di discrezionalità agli Stati membri in determinati ambiti, non è escluso che la legge nazionale rispetti i criteri guida contenuti nella sentenza», F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, cit., p. 4278. Del resto, come ricordato da Arena, anche secondo Cruz Villalon, Avvocato generale nel caso *DRI*, alcune discipline nazionali, laddove si fossero discostate dalla DRD, smorzandone o correggendone le criticità, avrebbero potuto risultare conformi al diritto dell'UE (para. 157, Conclusioni), A. ARENA, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014.

delle sentenze *DRI* e *Tele2* né alcuna pronuncia di incostituzionalità della disciplina di cui all'art. 132 Codice Privacy, né tantomeno decisioni di disapplicazione della normativa nazionale, neppure dinnanzi alle forti criticità e carenze rilevate da gran parte della dottrina.

Il percorso italiano però non si è contraddistinto solo per un iniziale immobilismo e mantenimento dello *status quo* dinnanzi alla dirompente e rilevante giurisprudenza della CGUE: al contrario, l'Italia ha deciso di imboccare una strada addirittura opposta rispetto a quella maggiormente garantista e più restrittiva quanto all'impiego dello strumento della *data retention* indicata dai giudici europei e da molte altre Corti e legislatori di altri Stati membri.

L'art. 132 Codice Privacy, infatti, ha subito, a partire dal 2015, svariati interventi che ne hanno profondamente segnato la disciplina, determinando importanti cambiamenti nel verso di un ampliamento dell'obbligo di conservazione dei metadati. Il decreto legge antiterrorismo del 2015 (d.l. 18 febbraio 2015, n. 7, convertito con modificazioni dalla legge 17 aprile 2015, n. 43), adottato poco tempo dopo il terribile attentato alla sede del giornale satirico Charlie Hebdo a Parigi, aveva previsto, all'art. 4-*bis*, co.1, che «al fine di poter agevolare le indagini esclusivamente per i reati di cui agli articoli 51, comma 3-*quater* e 407, comma 2, lett. a) del c.p.p. (…), i dati relativi al traffico telefonico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto sono conservati dal fornitore fino al 31 dicembre 2016 per finalità di accertamento e repressione dei reati. Per le medesime finalità i dati relativi al traffico telematico effettuato a decorrere dalla data di entrata in vigore della legge di conversione del presente decreto, esclusi comunque i contenuti della comunicazione, sono conservati dal fornitore fino al 31 dicembre 2016». La deroga all'art. 132 Codice Privacy, così introdotta[15], avrebbe dovuto cessare a partire dal 1 gennaio 2017.

Con il d.l. 30 dicembre 2015, n. 210 (c.d. Decreto milleproroghe), convertito con modificazioni dalla legge 25 febbraio 2016, n. 21, però, il

[15] «La modifica introdotta dall'art. 4-*bis* legge n. 43 del 2015 non costituisce una modifica al regime di conservazione dei dati di traffico telefonico e telematico previsto dall'art. 132 Cod. Privacy ma una previsione in deroga che riguarda unicamente i reati di cui agli artt. 51, co. 3-*quater* e 407, co. 2, lett. a)», P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, cit., p. 2.

legislatore nazionale interveniva nuovamente in materia, ancora una volta senza agire direttamente sull'art. 132 Codice Privacy, bensì modificando la disposizione prevista dal previo decreto legge antiterrorismo: così facendo, l'art. 4-*bis*, co. 1 veniva riformato estendendo sino al 30 giugno 2017 l'obbligo di conservazione per i medesimi reati già da quelle disposizioni indicati. Tale decisione, che ancora una volta risentiva fortemente degli attentati terroristici del novembre 2015 che avevano colpito con maggiore violenza la città di Parigi, rifletteva quindi la scelta effettuata dal legislatore già ad inizi 2015: quella cioè di porre in essere un intervento normativo motivato da ragioni emergenziali e dalla percepita urgenza di rafforzare l'efficacia dello strumento della *data retention*, ritenuto utile e prezioso per fronteggiare la minaccia terroristica [16]. Anche in questo caso, quindi, tale delicata materia veniva modificata senza la predisposizione di una disciplina complessiva e di un intervento organico e maggiormente chiaro, come invece auspicato dagli operatori dei servizi di telecomunicazione che vedevano di volta in volta – e senza possibilità di previsione – allungarsi i termini di conservazione, con un significativo impatto economico ed un aggravio dei costi in termini di risorse necessarie (server e personale). Le conseguenze sui *service providers* infatti non erano certamente di poco rilievo se si considera il risultato pratico provocato dal duplice intervento normativo esaminato: come già era avvenuto in passato, quando ancora vigeva il c.d. doppio binario, il fornitore di servizi di telecomunicazione non poteva conoscere in anticipo per quali reati i metadati prodotti dai propri utenti sarebbero stati utilizzati, così da risultare costretto ad estendere alla totalità dei metadati la conservazione sino al termine massimo, individuato al 30 giugno 2017, e poter essere nelle condizioni di assolvere correttamente all'obbligo imposto dalla legge antiterrorismo e dal decreto milleproroghe, qualora una richiesta di accesso ai dati gli fosse stata inoltrata dalle autorità di *law enforcement*. Sotto il profilo

[16] Come riportato da Scaffardi, «la ratio dell'estensione temporale rispetto alla normativa previgente si può desumere dalle schede di lettura che accompagnavano l'atto, vale a dire mettere a disposizione dell'autorità investigativa strumenti efficaci contro una minaccia, quella del terrorismo, sempre più grave ed estesa, che i mezzi informatici rendono pervasiva annullando i confini temporali e territoriali», L. SCAFFARDI, *La data retention va in ascensore*, in *Forum di Quaderni costituzionali*, 28 luglio 2017, p. 2.

della conservazione, dunque, l'art. 4-*bis*, co. 1 del d.l. n. 210/2015 finiva, concretamente, col soppiantare l'applicabilità della durata di conservazione più breve imposta dall'art. 132 Codice Privacy. Quest'ultima disposizione restava certamente operativa quanto alla disciplina dell'accesso nei casi di repressione e indagine di reati diversi da quelli indicati dall'art. 4-*bis*, co. 1: anche qualora il fornitore avesse provveduto a conservare i dati per il periodo massimo, l'accesso sarebbe stato infatti legittimo e valido solo nei limiti temporali previsti dal Codice Privacy, e non oltre. In altre parole, nella pratica, la conservazione veniva estesa alla durata stabilita dai decreti legge susseguitisi nel 2015, mentre con riferimento all'accesso per scopi diversi da quelli in tali normative trattati, la possibilità di "andare indietro nel tempo" fornita alle autorità di *law enforcement* restava circoscritta a quanto stabilito dall'art. 132 Codice Privacy. Risulta chiaro quindi come quella che avrebbe dovuto rappresentare una eccezione, volta a fronteggiare una situazione emergenziale, fosse nei fatti divenuta una regola generale sotto il profilo della conservazione dei metadati.

Il contesto normativo, reso particolarmente complesso dall'intersecarsi di diverse normative e dalla concreta conseguenza prodotta che aveva finito con l'invertire regola straordinaria e disciplina ordinaria, è stato poi ancor più problematicamente riconfermato nel 2017: allo scadere della proroga definita con il secondo Decreto del 2015, l'art. 132 Codice Privacy avrebbe dovuto tornare ad operare a pieno regime e la durata della conservazione e del relativo accesso ai metadati avrebbe quindi dovuto riconfermarsi la medesima per qualsiasi tipo di reato, senza alcuna distinzione. Il 20 novembre 2017, tuttavia, con la c.d. Legge Europea 2017, n. 167, ovvero la Legge che reca le "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione europea", veniva introdotta, per mezzo di un emendamento all'originario Disegno di Legge, una disposizione riguardante la conservazione dei metadati: l'art. 24, infatti, ha previsto che «in attuazione dell'art. 20 della Direttiva (UE) 2017/541 del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio, al fine di garantire strumenti di indagine efficace in considerazione delle straordinarie esigenze di contrasto al terrorismo, anche internazionale, per le finalità

dell'accertamento e della repressione dei reati di cui agli artt. 51, co. 3-*quater* e 407, co. 2, lett. a) del c.p.p., il termine di conservazione dei dati di traffico telefonico e telematico nonché dei dati relativi alle chiamate senza risposta, di cui all'art. 4-*bis* del d.l. 18 febbraio 2015, n. 7 (…) è stabilito in settantadue mesi, in deroga a quanto previsto dall'art. 132 del Codice in materia di protezione dei dati personali». Ne emerge dunque come per finalità di lotta al terrorismo o reati di simile gravità – i reati cui viene fatto rimando sono infatti essenzialmente delitti consumati o tentati con finalità di terrorismo e delitti di devastazione, saccheggio, strage, guerra civile, associazione di tipo mafioso – il periodo di conservazione dei metadati sia stato dilatato in maniera significativa ad una durata di ben sei anni. Sebbene ad una prima lettura tale misura possa sembrare di ristretto impatto, riguardando solo la conservazione e l'accesso per finalità limitate e particolarmente gravi, anche in questo caso, come per i previ interventi normativi del 2015, diviene di fondamentale importanza considerare il risultato pratico: il fornitore di servizi di telecomunicazione non può infatti conoscere in anticipo se i metadati relativi alle comunicazioni dei propri utenti verranno utilizzati nell'ambito di indagini riguardanti i reati previsti dall'art. 24 della Legge Europea 2017 – e dovendo dunque operare una conservazione di settantadue mesi – o per tutti gli altri reati, per i quali i termini di conservazione sono invece quelli fissati dall'art. 132 Codice Privacy. Ancora una volta, pertanto, l'operatore sarà chiamato a conservare tutti i metadati raccolti per un periodo di settantadue mesi, in modo da poter fornire alle autorità di *law enforcement* i dati risalenti sino a sei anni prima laddove richiesti per reati di terrorismo o altri indicati dall'art. 407 c.p.p[17]. Si è così creata di nuovo quella complessa situazione sulla base della quale l'art. 132 Codice Privacy resta pienamente operativo solo sotto il profilo dell'accesso ai metadati per reati differenti da quelli disciplinati dall'art. 24 richiamato: concretamente, «nel momento della trasmissione dei dati all'autorità giudiziaria il fornitore è obbligato a verificare che gli stessi siano riconducibili al periodo di

[17] Per una analisi dei pratici effetti per gli operatori economici del settore, si rimanda a G. NAZZARO, *Tabulati di traffico storico per finalità di accertamento e repressione dei reati: caratteristiche e tempi di conservazione*, in *Sicurezza e Giustizia*, 3, 2018, p. 58.

conservazione che, a seconda del tipo di reato perseguito, risulta fissato dall'art. 132 Codice Privacy o della legge europea 2017. Se ad esempio, un dato da conservarsi per ventiquattro mesi (ma di fatto conservato per settantadue mesi per la ricordata ragione che è impossibile conoscere a priori per quale tipo di reato verrà domandato l'accesso), fosse richiesto dopo ventiquattro mesi ed un giorno, sarebbero illegittime tanto la sua trasmissione quanto la sua acquisizione da parte dell'autorità giudiziaria» [18].

L'intervento normativo predisposto dall'art. 24 Legge Europea 2017 presenta pertanto due problematiche fondamentali: ampliando così significativamente la durata della conservazione, sebbene limitatamente a reati quali terrorismo e criminalità organizzata, esso si pone infatti in una posizione di profonda divergenza rispetto alla giurisprudenza della CGUE che neppure per finalità di lotta al terrorismo aveva ritenuto proporzionata una *data retention* dalla durata di gran lunga inferiore (due anni). I giudici di Lussemburgo, sin dalla sentenza *DRI*, hanno sottolineato l'importanza di fondare la scelta della durata della conservazione su criteri obiettivi in grado di garantirne il carattere limitato allo stretto necessario (sentenza *DRI*, par. 64); ebbene, una simile specificazione, volta a comprovare la necessità di una conservazione tanto ampia, non pare essere stata presa in considerazione dal legislatore italiano, che non ha svolto alcun rinvio a studi o analisi finalizzate a determinare l'utilità e l'efficacia di una *data retention* così prolungata. Inoltre, l'estensione generalizzata della durata della conservazione a settantadue mesi ha prodotto l'effetto di rendere la disciplina emergenziale, prevista per la straordinaria lotta al fe-

[18] S. SIGNORATO, *Novità in tema di data retention. La riformulazione dell'art. 12 Codice Privacy da parte del D. Lgs. 10 agosto 2018, n. 101*, in *Diritto penale contemporaneo*, 11, 2018, p. 157. Sul punto, si evidenzia come la Corte di Cassazione avesse già più volte affermato l'inutilizzabilità di metadati risalenti ad un periodo superiore al termine massimo di conservazione previsto dalla legge, come ad esempio stabilito nella pronuncia Cass., Sez. V Penale, 25 gennaio 2016, n. 7265: «Sono patologicamente inutilizzabili i dati relativi al traffico telefonico contenuti nei tabulati acquisiti dall'Autorità giudiziaria dopo i termini previsti dall'art. 132 D.Lgs. 30 giugno 2003, n. 196, atteso il divieto di conservazione degli stessi da parte del gestore al fine di consentire l'accertamento dei reati oltre il periodo normativamente predeterminato»; ma anche Cass., Sez. V Penale, 5 dicembre 2014, n. 15613.

nomeno terroristico, una disciplina *de facto* ordinaria, quanto meno sotto il profilo della conservazione dei metadati [19].

Oltre a questi aspetti critici e per fugare qualsiasi dubbio o errore valutativo, è necessario precisare come la misura analizzata non abbia in realtà introdotto alcuna qualificazione o limitazione relativa alla gravità del reato, come invece richiesto dalla giurisprudenza della CGUE: l'art. 24 Legge Europea 2017 è infatti intervenuto sulla durata della conservazione nonché, indirettamente, sulla possibilità di accesso ai metadati per specifiche categorie di reati ritenuti di una pericolosità e rilevanza tale da giustificare una *data retention* più estesa. Per tutti gli altri reati però la conservazione resta regolata, in maniera del tutto indistinta sotto il profilo del carattere di gravità, dall'art. 132 Codice Privacy, che prevede sì una differenziazione sulla base della tipologia di metadati e mezzi di comunicazione interessati – a seconda cioè che si tratti di dati derivanti da servizi di telefonia, telematici o chiamate senza risposta – ma nulla dice quanto alla finalità della conservazione e dell'accesso, che rimane quella generica di repressione dei reati, senza qualificazione alcuna e senza restrizione ai soli reati gravi [20].

Sulla base di simili considerazioni, anche quest'ultimo intervento normativo è stato da più parti criticato e discusso, sia sotto il profilo della fonte normativa impiegata, sia sotto quello della conformità al diritto dell'UE e alla giurisprudenza della CGUE. Con riferimento al primo aspetto, la modalità con la quale un inasprimento così significativo della disciplina della conservazione è stato attuato è sembrata quan-

---

[19] S. SIGNORATO, *Novità in tema di data retention*, cit., p. 157.

[20] Come ben sintetizzato da Resta, «benché l'acquisibilità dei dati raccolti oltre due anni prima (per i tabulati telefonici, un anno prima per i telematici e un mese per le chiamate senza risposta) sia limitata ai reati particolarmente gravi, proprio la natura retrospettiva di questo strumento investigativo implica la conservazione generalizzata dei dati di traffico per sei anni, salvo poi limitarne l'utilizzabilità processuale ai soli casi considerati. L'incidenza della misura sulla privacy dei cittadini è, dunque, particolarmente forte, a fronte di un'utilizzabilità processuale dei dati così massivamente raccolti, in fondo limitata, con implicazioni probabilmente poco coerenti con il principio di proporzionalità tra esigenze investigative e privacy», F. RESTA, *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna*, in *Giustizia Insieme*, 6 marzo 2021.

to meno «furtiva» [21] e singolare: la disposizione in esame è stata inserita in una legge sugli adempimenti comunitari, preceduta da una disposizione in attuazione della Direttiva 2014/33 in materia di ascensori (!), anziché essere prevista in una normativa *ad hoc* e specifica relativa ad una materia tanto delicata e dal forte impatto sui diritti fondamentali. Ciò ha fatto sorgere il sospetto che il legislatore abbia intenzionalmente voluto, «di soppiatto» [22] e senza attirare troppo l'attenzione, inserire nell'ordinamento una modifica che avrebbe meritato invece – e come è del resto avvenuto in molti altri Stati membri – un ampio dibattito parlamentare, fondato su studi e analisi oggettive capaci di riflettere le reali esigenze investigative e di individuare la soluzione in grado di garantire al meglio un equilibrio tra diritti fondamentali e necessità securitarie. Sul punto, Walter Verini, uno dei Deputati che avevano presentato nell'estate 2017 l'emendamento integrante la modifica alla disciplina della *data retention*, aveva motivato la decisione di tale proposta riferendosi alla esigenza, asserita dalla Procura nazionale antiterrorismo in occasione di alcune audizioni parlamentari, di adottare nuovi strumenti di prevenzione e lotta al terrorismo, tra cui, appunto, una conservazione dei metadati di più lunga durata. Questo richiamo piuttosto generico, privo di chiari riferimenti fattuali e di dati, rivela però la mancanza, all'interno della discussione parlamentare, di considerazioni in grado di dimostrare oggettivamente e sulla base di criteri precisi la proporzionalità delle misure introdotte con la Legge Europea rispetto agli scopi preposti. Proprio basandosi su tali valutazioni, anche il Presidente del Garante per la protezione dei dati italiano, all'epoca Antonello Soro, aveva espresso le proprie perplessità e contrarietà alla scelta operata dal legisla-

[21] L. SCAFFARDI, *La data retention va in ascensore*, cit., p. 1.

[22] Così L. SCUDIERO, *La Camera porta di soppiatto la data retention a sei anni*, in *Lex Digital*, 21 luglio 2016, che afferma anche: «se possibile, più che il merito questa volta inquieta il metodo, secondo cui un emendamento di grandissimo impatto sulle libertà civili dei cittadini italiani viene occultato in un provvedimento di altro tenore (e criticità giuridico-politica), per sottrarlo ad una degna e trasparente discussione parlamentare sul suo contenuto». Dello stesso autore, si legga anche L. SCUDIERO, *Data retention a sei anni. La Corte di Giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR*, in *MediaLaws*, 1, 2017.

tore: «la Corte di giustizia ha costruito l'architrave del rapporto tra prevenzione, tecnologia e dignità proprio sul principio di proporzionalità tra esigenze investigative e protezione dei dati» [23]. Così, aumentando significativamente la durata della conservazione dei metadati, non solo vengono ignorate le sentenze della CGUE in materia ma si sottopongono a rischi ancora maggiori gli utenti dei servizi di telecomunicazione, i cui dati risultano, per un periodo ancor più lungo, esposti a possibili – e invero frequenti – *data breach* e attacchi informatici, oltre che al pericolo di abusi da parte di soggetti pubblici e privati, aumentando peraltro irragionevolmente anche i costi e le responsabilità in capo agli operatori economici in tale campo, che debbono porre in essere misure molto forti e onerose per garantire la sicurezza dei metadati conservati per una durata così estesa. Lo stesso Giovanni Buttarelli, in quegli anni Garante Europeo della Protezione dei Dati, al termine della presentazione dell'*Annual Report* alla Commissione per le libertà civili, giustizia e affari interni del Parlamento europeo, aveva redarguito il legislatore italiano, considerando l'intervento normativo promosso con la Legge Europea un grave errore, anche alla luce della sua in-

[23] È quanto affermato da Soro il 24 ottobre 2016, in occasione del Convegno svoltosi a Firenze dal titolo "Privacy digitale e protezione dei dati personali tra persona e mercato". Lo stesso Soro ha inoltre precisato: «L'emendamento Verini segue la stessa impostazione di precedenti interventi che negli anni scorsi hanno modificato la disciplina della *data retention*. E, come già accaduto nel 2015, la norma introduce modalità di trattamento dei dati di traffico telefonico e telematico in palese contrasto con l'ordinamento e con la giurisprudenza dell'Unione europea. Pur essendo consapevole dell'esigenza di non ritardare l'approvazione della legge europea con una terza lettura, penso che sia comunque indispensabile che il legislatore riconduca questa disciplina al criterio della proporzionalità. In futuro si dovrà meglio definire, con una disciplina organica e meno estemporanea, una materia così ricca di implicazioni sui diritti dei cittadini e sulle esigenze di giustizia», si legge nell'articolo reperibile sul sito web del Garante, *Terrorismo: Soro, troppi 6 anni di conservazione dei dati*, disponibile al link: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/ 6651715. La posizione del Garante della Privacy è stata poi espressa anche in un apposito Parere (n. 8005333 sullo schema di decreto legislativo recante attuazione della Dir. 2016/680 del PE e del Consiglio, del 22 febbraio 2018) nel quale si è ribadito l'invito al legislatore nazionale a rivedere e modificare la normativa in materia di *data retention*, sproporzionata rispetto ai criteri indicati dalla giurisprudenza della CGUE nonché alle reali esigenze investigative.

compatibilità con i principi espressi a livello dell'UE [24].

Nonostante le decise reazioni, le critiche e l'acceso dibattito apertosi in ambito – per lo più – accademico [25], la disposizione prevista dalla Legge Europea 2017 non ha conosciuto modifiche o ripensamenti, neppure quando una perfetta occasione per una più seria ristrutturazione della materia è stata offerta dalla entrata in vigore del GDPR e dunque dalla necessità di adeguare l'ordinamento interno, e in particolare il Codice Privacy, alle significative novità apportate dal Regolamento europeo [26]. Pur essendo direttamente applicabile, infatti, il GDPR ha lasciato su alcune materie – ad esempio su taluni profili relativi alla disciplina del trattamento di categorie particolari di dati – un certo margine di intervento e discrezionalità ai legislatori nazionali. Per rispondere a questa esigenza di riforma, che ha interessato il legislatore ma che ha richiesto anche l'intervento attivo e l'adozione di specifici atti da parte dell'Autorità Garante, è stato approvato il d.lgs. 10 agosto 2018, n. 101 [27], nel quale si inseriscono anche talune modifiche all'art. 132 in materia di *data retention*,

[24] «Da magistrato capisco che la giustizia abbia molte difficoltà e ostacoli oggi, e che organi investigativi debbano essere equipaggiati per fare indagini. (…) La scelta dell'Italia ha molto sorpreso Bruxelles, c'è molta attenzione da parte del Parlamento UE. Teniamo presente che un Paese come la Germania ha previsto un tempo di *data retention* che al massimo arriva a 10 settimane. Oltre al fatto che la Corte europea aveva annullato una Direttiva che prevedeva un massimo di due anni», intervista a Giovanni Buttarelli, pubblicata da Carola Frediani per *La Stampa*, il 13 novembre 2017.

[25] Anche la stampa nazionale si è occupata del tema, dandone risalto in diversi momenti, dalla proposta dell'emendamento alla approvazione finale della Legge Europea 2017. Tra tutti si legga R. BARBERIO, *Parliamo di Russia ma la vera anomalia sul 'data retention' è l'Italia*, in *HuffingtonPost*, 5 luglio 2018.

[26] Merita ricordare come il Decreto PDR 15 gennaio 2018, n. 15 che attua la Direttiva 2016/680, non riguardi la materia della *data retention*. Se è vero infatti che l'art. 10 di tale normativa fissa le condizioni per la conservazione dei dati, ciò non deve fuorviare il lettore: in quel caso il riferimento è alla conservazione di dati trattati nel corso di un procedimento penale o delle previe indagini, non avendo quindi nulla a che vedere con la più generale disciplina attinente all'obbligo di conservazione dei metadati da parte di servizi di telecomunicazione, oggetto di questa disamina.

[27] Per una ampia ed aggiornata ricostruzione della normativa italiana vigente, si rimanda a R. D'ORAZIO, G. FINOCCHIARO, O. POLLICINO, G. RESTA (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021.

in particolare con riferimento ai commi 3 e 5 e alla previsione di un nuovo comma 5-*bis*. Queste riforme tuttavia non hanno apportato novità sostanziali, mettendo in luce la mancata volontà del legislatore nazionale di cogliere una utile opportunità per adeguare la disciplina interna della conservazione dei metadati a quanto indicato dalla giurisprudenza della CGUE e per far tesoro non solo delle critiche e perplessità energicamente manifestate nel corso degli anni dalla dottrina ma anche del vasto dibattito che, su tale complessa materia, si era già ampiamente aperto in molti altri Stati membri. Il cambiamento operato sul comma 3 risulta infatti essenzialmente finalizzato a chiarire il dettato della disposizione, senza stravolgerne o cambiarne il significato: viene semplicemente sostituito il precedente riferimento all'art. 8, co. 2, lett. f) riguardante la conservazione e accesso al traffico entrante, con la più immediata previsione «la richiesta di accesso diretto alle comunicazioni telefoniche in entrata può essere effettuata solo quando possa derivarne un pregiudizio effettivo e concreto per lo svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397». Similmente, anche il comma 5 si limita a sostituire il previo richiamo all'art. 17 Codice Privacy, sul "Trattamento che presenta rischi specifici", abrogato dal d.lgs. n. 101/2018, con il rimando al nuovo art. 2-*quinquiesdecies*, che stabilisce come, con riguardo ai trattamenti svolti per l'esecuzione di un compito di interesse pubblico che possono presentare rischi elevati per i diritti e le libertà delle persone fisiche, il Garante possa prescrivere misure e accorgimenti a garanzia dell'interessato. I due interventi indicati mirano perciò solo ad armonizzare la disciplina esistente con il GDPR e con le conseguenti modifiche apportate al Codice Privacy. Ancor più sorprendentemente e problematicamente, poi, il nuovo comma 5-*bis* ha riconfermato la – discussa, quanto meno in dottrina – modifica apportata dalla Legge Europea del 2017, prevedendo che viene «fatta salva la disciplina di cui all'art. 24 della legge 20 novembre 2017, n.167», riproponendosi così tutte le criticità già in precedenza sottolineate.

In conclusione, dalla ricostruzione dell'evoluzione normativa qui proposta risulta come il legislatore non abbia mostrato un approccio realmente attento né all'evolversi della materia a livello dell'UE né alle azioni intraprese da altri Stati membri che si sono invece rivelati maggiormente sensibili alla giurisprudenza della CGUE, seppur con notevoli differenze.

Ciò che traspare è una normativa che si è evoluta in maniera disordinata, non organica e che ha seguito una direzione per certi versi opposta rispetto a quella tendenza, registratasi in altri ordinamenti nazionali, ad un adeguamento della disciplina interna alle garanzie stabilite a livello europeo, generalmente mediante una diminuzione della durata di conservazione dei dati, un aumento delle salvaguardie ed una più attenta specificazione delle categorie di reati per i quali l'accesso viene garantito. L'Italia, al contrario, ha non solo aumentato il periodo di *data retention* con una estensione notevole e limitatamente motivata in termini di necessità e proporzionalità, ma non ha neppure modificato la disciplina esistente corredandola di salvaguardie e limiti maggiori e meglio determinati. La parabola normativa italiana è stata mossa essenzialmente da emergenziali necessità di innalzamento del livello di tutela della sicurezza e di incremento dell'efficienza dell'intervento delle autorità pubbliche, assicurando loro la possibilità di accedere ad un numero elevato di metadati conservati. Quel che sembra mancare nelle considerazioni del legislatore è, insomma, l'attenzione al bilanciamento da operare con i diritti alla riservatezza e alla protezione dei dati, nonché una riflessione approfondita sui limiti e sulla proporzionalità di tali delicate scelte. Un approccio, che, nonostante le critiche di gran parte della dottrina, ha ottenuto, almeno sino al 2021, l'avvallo delle Corti nazionali.

2. *Le Corti italiane e la* data retention*: una lettura restrittiva dei principi e criteri definiti dalla CGUE.*

2.1. *La sentenza della Corte costituzionale 14 novembre 2006, n. 372: una conferma del corretto bilanciamento tra diritti fondamentali e garanzia della sicurezza.*

La Corte costituzionale italiana, con sentenza 14 novembre 2006, n. 372, si è pronunciata per la prima ed unica volta sulla legittimità dell'art. 132 Codice Privacy. Questa decisione tuttavia risulta assai singolare se si pensa che i giudici costituzionali hanno dovuto valutare la normativa richiamata sotto un profilo opposto rispetto a quanto ha caratterizzato i primi interventi giurisprudenziali tanto di Corti nazionali di altri Stati

membri quanto dei giudici di Lussemburgo. Mentre questi infatti erano stati chiamati a vagliare la proporzionalità dell'invasione nella sfera privata causata dalla disciplina della conservazione generalizzata dei metadati, i rinvii alla Corte costituzionale promossi dai Giudici per le indagini preliminari dei Tribunali di Pavia, Roma e Palmi ponevano invece in discussione la legittimità costituzionale dei limiti temporali imposti dal sistema a doppio binario e delle garanzie procedurali – quali la previa autorizzazione del giudice – previste dall'art. 132 Codice Privacy. La questione posta dai giudici di merito dunque non era basata su dubbi di legittimità attinenti al carattere indiscriminato della conservazione o alla possibilità di accesso ai metadati estesa a qualsiasi reato, anche privo del carattere di gravità richiesto dalla DRD; al contrario, ad essere ritenuta irragionevole era la mancata disponibilità dei metadati, anche per la finalità di repressione dei reati "comuni", per l'intero periodo in cui i fornitori di servizi di telecomunicazione erano comunque obbligati alla conservazione. Questo meccanismo del "doppio binario", a parere dei giudici *a quo*, risultava in «garanzie sostanzialmente vuote: utili forse a massimizzare sulla carta gli standards di protezione della segretezza delle comunicazioni ma in realtà concretamente inidonee a tale scopo e quindi irragionevoli» [28]; ciò alla luce del fatto che, nonostante – e anzi proprio a causa – del doppio binario, i metadati venivano comunque tutti conservati, nella prassi concreta e per esigenze fattuali ineludibili, per la massima durata dei quarantotto mesi [29]. Similmente, anche la previa autorizzazione del giudice, richiesta quale condizione per il legittimo accesso ai metadati, era stata ri-

[28] M. PINNA, *Doppio binario di accesso ai dati sul traffico telefonico: una scelta legislativa ragionevole ratificata (con argomenti non irresistibili) dalla Corte costituzionale*, in *Giurisprudenza Costituzionale*, 2006, p. 3929. A commento di tale pronuncia si legga anche E. BASSOLI, *Acquisizione dei tabulati vs. privacy: la* data retention *al vaglio della Consulta*, in *Diritto di Internet*, 3, 2007, p. 14.

[29] «Secondo il giudice rimettente, l'esistenza fisica dei dati, non ancora distrutti, comporterebbe un tasso di pericolosità, derivante dalla possibile illecita diffusione degli stessi, destinato a rimanere costante per tutto il tempo anteriore la loro distruzione, senza subire variazioni in rapporto alla gravità dei reati. Da ciò discenderebbe l'irragionevolezza della bipartizione – contenuta nella norma censurata – dei termini di accessibilità dei dati da parte dell'autorità giudiziaria», para. 5.2, Corte cost. 14 novembre 2006, n. 372.

tenuta immotivatamente onerosa, tanto da costituire una ingiustificata complicazione della procedura, potenzialmente contrastante con il principio di obbligatorietà dell'esercizio dell'azione penale (art. 112 Cost.) nonché con la più generale aspettativa della garanzia, da parte dello Stato, delle condizioni essenziali della convivenza civile dinnanzi a comportamenti criminosi (artt. 101, 104 e 112 Cost.).

La Consulta, nella sua pronuncia, ha fatto salva la normativa esistente, ritenendo infondate le questioni poste alla sua attenzione. Quanto al profilo della previa autorizzazione all'accesso, i giudici costituzionali hanno sottolineato come la materia, nelle more del giudizio, fosse stata profondamente innovata dal Decreto Pisanu e dalla relativa legge di conversione. Queste riforme, come si è visto, avevano eliminato l'intervento preventivo del giudice, ritenendo sufficiente il mero decreto motivato da parte del pubblico ministero: tale scelta del legislatore aveva fatto venir meno tutti i rilievi di illegittimità indicati dai Giudici rimettenti, così che la Consulta non ha ritenuto di doversi ulteriormente pronunciare sulle delicate questioni della proporzionalità ed imparzialità del previo controllo giudiziario. Un profilo questo, che risulta oggi tutt'altro che pacifico alla luce dei requisiti di indipendenza e terzietà richiesti dalla CGUE nella sua ultima pronuncia *H.K. c. Prokuratuur* e che ha aperto, come si vedrà, un ampio dibattito anche nel contesto italiano.

Rispetto all'illegittimità della disciplina della *data retention* strutturata secondo il meccanismo del doppio binario, i giudici costituzionali hanno poi riconosciuto che «il legislatore ha operato un bilanciamento tra il principio costituzionale della tutela della riservatezza dei dati relativi alle comunicazioni telefoniche, riconducibile all'art. 15 Cost., e l'interesse della collettività, anch'esso costituzionalmente protetto, alla repressione degli illeciti penali», para. 5.1.[30]. Tale bilanciamento è stato ritenuto ra-

[30] Merita sottolineare, per completezza, come nella Costituzione italiana non esista un espresso riconoscimento dei diritti alla riservatezza e alla protezione dei dati. Nondimeno questi diritti risultano protetti nell'ordinamento nazionale, da un lato mediante le fonti di livello internazionale e sovranazionale (quali la Convenzione EDU e Carta di Nizza) al cui rispetto l'Italia si è vincolata, e dall'altro mediante la giurisprudenza della Corte costituzionale, che ha individuato negli artt. 14 e 15 le basi costituzionali del diritto alla privacy, unitamente ai riferimenti più generici ai diritti alla libertà personale e alla dignità. Come affermato da Resta, il riconoscimento dei diritti alla privacy e alla

gionevole in quanto «affinché la norma sfugga alla censura di illegittimità costituzionale non è necessario, come ritiene il giudice *a quo*, che dalla differente disciplina del tempo di accessibilità dei dati, a seconda della gravità dei reati da perseguire, derivi una maggiore o minore tutela del diritto alla riservatezza; è sufficiente che la maggiore o minore limitazione sia posta in rapporto con la maggiore o minore gravità attribuita dal legislatore a reati diversi, individuati secondo scelte di politica criminale non censurabili in questa sede» (par. 5.3).

Ad apparire di notevole interesse in questa pronuncia sono innanzitutto i dubbi espressi dai giudici *a quo*: pur non contestando, diversamente da quanto avvenuto in altri ordinamenti, lo strumento della *data retention* generalizzata, è stata purtuttavia riconosciuta l'esistenza di una lesione dei diritti fondamentali derivante dalla sola conservazione dei metadati, indipendentemente e prima dell'accesso; è sulla base di questa importante valutazione che i giudici del rinvio sono giunti poi – discutibilmente – alla conclusione secondo cui proprio il perdurare della lesione, protratta per quarantotto mesi, rende irragionevole la differenziazione in termini di accesso e disponibilità dei metadati a seconda della gravità del reato [31].

Anche nelle considerazioni espresse dalla Corte costituzionale si deduce una presa di posizione rilevante per comprendere l'approccio della giurisprudenza italiana dinnanzi al tema della conservazione dei metadati e del bilanciamento tra esigenze securitarie e diritti fondamentali: si tratta dell'affermazione secondo cui, trascorso un periodo di tempo durante il quale i dati sono accessibili anche per reati non gravi, è ragionevole pre-

---

data protection è pertanto avvenuto non grazie ad esplicite garanzie costituzionali bensì principalmente – e soprattutto negli ultimi decenni – mediante l'interazione tra livello interno e sovranazionale (G. RESTA, *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il Codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004).

[31] «Lo stesso legislatore ha ritenuto che, per mantenere l'equilibrio, all'aumento del peso di una delle due entità debba corrispondere un proporzionale aumento dell'altra, con la conseguenza che, in corrispondenza di reati di particolare gravità, la limitazione, in termini relativi, della tutela della riservatezza è stata aumentata in ragione del maggior disvalore sociale sotteso ai reati di cui all'art. 407, comma 2, lettera *a*), cod. proc. pen.», para. 5.2., Corte cost. 14 novembre 2006, n. 372.

vedere una ulteriore e più ampia durata di conservazione e di accesso, che dovrà però essere giustificata e proporzionata alla maggiore gravità dell'offesa che la disponibilità dei metadati è volta a contrastare. Un ragionamento, questo, che sembra scontrarsi sia con quanto poi dichiarerà la CGUE, sia con quello che la DRD stessa all'epoca statuiva, disponendo l'obbligo di conservazione dei metadati unicamente per finalità di repressione di reati qualificati dai legislatori nazionali come gravi. Nonostante tali rilievi critici, la posizione espressa dalla Corte costituzionale è stata ampiamente confermata e seguita dal legislatore italiano, che non ha mai inserito nella normativa nazionale il requisito della gravità del reato, consentendo dunque l'accesso ai metadati per finalità generali di lotta a qualsiasi tipo di reato e prevedendo tutt'al più disposizioni eccezionali in deroga alla regola generale, riferite a tipologie particolari di reati quali il terrorismo e volte ad ampliare la durata di conservazione.

2.2. *La rilevante e discussa Ordinanza del Tribunale di Padova: una prima presa di posizione dei giudici italiani dinnanzi alle pronunce della CGUE.*

Dopo svariati anni nei quali i Giudici italiani sono sostanzialmente rimasti silenti, anche dinnanzi alle rilevanti decisioni della CGUE, si sono registrate a partire dal 2017 alcune pronunce in materia di *data retention*, che risultano determinanti al fine di definire il peculiare approccio della giurisprudenza italiana. Tra queste, particolare importanza riveste l'Ordinanza del Tribunale di Padova (Ord. 15 marzo 2017, Pres. Marassi) che viene segnalata come «uno dei rari casi, ad oggi noti, in cui l'avvocato della difesa ha chiesto al giudice di dichiarare l'inutilizzabilità nel processo di tutti i dati esterni del traffico telefonico, a chiunque intestati, acquisiti in fase di indagini dalla pubblica accusa ex art. 132 Codice Privacy, a seguito della nota sentenza della CGUE sulla *data retention*»[32]. Tale richiesta era peraltro correlata, in subordine, dalla domanda di sospendere il procedimento e provvedere ad un rinvio pregiudiziale alla CGUE, sottoponendo il delicato quesito volto a determinare «se gli artt. 7, 8 e 52, par. 1 della CDFUE ostino ad una normativa nazionale, quale

[32] R. FLOR, *Data retention ed art. 132 Cod. privacy: vexata quaestio(?)*, cit., p. 356.

l'art. 132 Codice Privacy, che consente l'acquisizione e la conservazione dei dati esterni del traffico telefonico e telematico per qualsiasi tipo di reato». Tre sono essenzialmente le motivazioni che hanno spinto i giudici a rigettare l'eccezione di inutilizzabilità dei tabulati – dunque dei metadati – promossa dalla difesa: innanzitutto, il Tribunale affermava che l'art. 132 Codice Privacy non poteva essere considerato norma attuativa della DRD, in quanto entrato in vigore nel 2003, ovvero ben prima della adozione della direttiva europea; di conseguenza, la sentenza *DRI*, vertente proprio sulla DRD, non poteva comportare alcun effetto nei confronti della disciplina italiana richiamata [33]. La seconda considerazione svolta dal Tribunale stabiliva che il reato per il quale l'accesso ai metadati veniva richiesto, nel caso in esame l'accertamento di un reato di tentato incendio doloso, risultava possedere quel carattere di gravità – imposto dalla giurisprudenza della CGUE, ma non specificamente previsto nella normativa italiana – idoneo a legittimare l'ingerenza nella sfera privata. Infine, il terzo argomento, di grande rilievo, proposto era quello secondo cui la potenziale ammissibilità, in un caso come quello esaminato, delle ben più invasive intercettazioni telefoniche, attinenti quindi al contenuto delle conversazioni, non poteva che far ritenere giustificata e proporzionata la lesione più limitata del diritto alla riservatezza derivante dall'accesso ai meri metadati.

Poiché molte di queste posizioni verranno successivamente riprese anche dai giudici della Corte di Cassazione, una attenta disamina di questa Ordinanza risulta imprescindibile. Innanzitutto, ciò che risalta con estrema immediatezza – e la dottrina non ha mancato di rimarcarlo – è la rapidità e superficialità con la quale il Tribunale di Padova ha affrontato una questione estremamente delicata e complessa, che già nel 2017 aveva sollevato ampia analisi e dibattito in molti Stati membri oltre che in seno alle Istituzioni stesse dell'UE e alla CGUE. Forse proprio questa analisi poco accurata ha portato i giudici italiani ad esprimere valutazioni sotto certi profili marcatamente erronee: senza dubbio l'art. 132 Codice Priva-

[33] Si legge infatti nella Ordinanza: «Il *dictum* della menzionata sentenza [*DRI*] non ha alcuna rilevanza nell'odierno processo. Infatti l'art. 132 Cod. Privacy non è norma di attuazione della DRD, essendo questo entrato in vigore in tempo antecedente: dunque l'invalidità della direttiva non si trasmette ad esso».

cy nella sua versione originaria non costituiva attuazione della DRD ma lo è divenuto nel 2008, quando il legislatore è intervenuto, con il già analizzato d.lgs. n. 109/2008, proprio sull'art. 132 per dare attuazione alla Direttiva europea 2006/24. È inoltre da rilevare come la sentenza *Tele2* della CGUE, che pure non è stata per nulla presa in considerazione dai giudici del Tribunale, avesse ribadito chiaramente i criteri delineati dalla *DRI* anche con riferimento alle discipline nazionali attuative del noto art. 15 Direttiva *e-Privacy*, tra cui appunto l'art. 132 Codice Privacy. Sebbene poi la sentenza *DRI* non abbia avuto alcuna efficacia diretta avverso le normative nazionali di attuazione della disciplina europea, è altrettanto vero che, indirettamente, qualora i vizi comportanti l'invalidità della DRD fossero stati rinvenuti anche nella disciplina interna attuativa, quest'ultima avrebbe dovuto essere considerata non compatibile con il diritto dell'UE e in violazione dei diritti fondamentali tutelati agli artt. 7 e 8 della Carta di Nizza, per le stesse ragioni e criticità individuate nella Direttiva europea medesima [34]. Trascurando simili valutazioni, il Tribunale di Padova ha finito dunque con l'ignorare – o il non voler prendere in considerazione – tutte quelle problematiche che la dottrina italiana, già a seguito della *DRI*, aveva messo in rilievo.

Quanto poi alla affermata sussistenza del requisito di gravità del reato, deve essere obiettato come la definizione del concetto e delle caratteristiche che determinano la gravità di un crimine non possa essere lasciata alla discrezionalità e libera valutazione del giudice, caso per caso, bensì debba essere stabilita dalla legge stessa, come del resto richiesto dalla giurisprudenza della CGUE e come specificato persino nella DRD, secondo cui la conservazione e l'accesso ai metadati dovevano essere motivati esclusivamente dalla finalità di repressione della criminalità grave, aspetto che sia il legislatore italiano prima che il giudice poi hanno così dimostrato di non considerare [35].

---

[34] Così F. RUGGIERI, *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cassazione Penale*, 6, 2017, p. 2486.

[35] «Evidente allora l'errore commesso dal Tribunale di Padova che, decidendo quale fattispecie integri l'ipotesi del reato grave, tale da prevalere in un giudizio di proporzionalità rispetto alla riservatezza del cittadino sottoposto a processo, ha esercitato (ed usurpato) funzioni legislative. Solo il legislatore, in un paese di *civil law* come l'Italia,

Infine, il ragionamento secondo cui l'accesso ai soli metadati deve ritenersi del tutto accettabile nei casi, come quello in esame, in cui sarebbe stato concesso il ricorso alle ben più invasive intercettazioni, pare del tutto fuorviante: la CGUE, infatti, a partire dalla sentenza *DRI*, ha riscontrato finanche nella sola conservazione dei metadati una grave ingerenza nella vita privata degli utenti, dovuta alla possibilità, mediante lettura aggregata di tali informazioni, di ricostruire abitudini, preferenze e stili di vita, a prescindere dall'esame del contenuto delle conversazioni stesse. Sebbene la CGUE non si sia spinta ad equiparare l'impatto provocato da un accesso massivo al contenuto delle comunicazioni con quello ai metadati, ritenendo solo il primo lesivo del nucleo essenziale del diritto alla riservatezza, essa è comunque giunta a richiedere un livello elevato di protezione e salvaguardie anche con riferimento ai semplici metadati. Oltretutto, non va dimenticato come il dibattito dottrinario, già evidenziato, abbia fortemente criticato la distinzione operata dalla CGUE, che pare ormai superata alla luce delle moderne tecnologie e delle possibilità e potenzialità estremamente invasive che la lettura aggregata dei metadati può comportare. Una affermazione come quella espressa dal Tribunale di Padova pare dunque quanto meno frutto di una eccessiva semplificazione di quelle che invece erano all'epoca e sono tutt'ora profonde e ampiamente discusse questioni.

L'esaminata Ordinanza può quindi ben essere considerata una significativa esemplificazione di tutte le problematiche già evidenziate con riferimento all'evoluzione della normativa italiana in materia di *data retention* e risulta strettamente correlata alle scelte del legislatore stesso ed in particolare al mancato – o, quando presente, maldestro – intervento di

può predeterminare in via generale ed astratta i modi dell'intrusione nella riservatezza dei propri cittadini ai sensi degli artt. 8 CDFUE e 8 CEDU. Se il giudice di ciascun caso singolo fosse autorizzato a svolgere un proprio bilanciamento in tema di *data retention*, da un lato si produrrebbero oscillazioni interpretative difficilmente giustificabili nella demarcazione del confine tra reato grave e reato non grave. Dall'altro si correrebbe il rischio che la giurisprudenza, legittimamente, si appiattisca nel ritenere tutto 'grave', anche al fine di non disperdere attività di accertamento spesso preziosa, complessa e necessaria, sino ad arrivare ad un totale annacquamento del requisito di gravità: risultato che si collocherebbe agli antipodi rispetto agli auspici della sentenza CGUE sulla *data retention*», F. RUGGIERI, *Data retention e giudice di merito penale*, cit., p. 2478.

adeguamento ai requisiti e criteri delineati dalla giurisprudenza della CGUE; è proprio nell'atteggiamento del legislatore italiano che vanno infatti riscontrate le radici di «impropri fenomeni di supplenza giudiziaria, di cui il provvedimento in commento appare emblematica espressione: comprensibile nei fini (perseguire la giustizia del caso concreto) ma censurabile nell'ordito, in spregio ai principi della separazione fra poteri e della certezza del diritto» [36]. Queste criticità, unitamente alla "leggerezza" nella lettura delle complesse e rilevanti sentenze dei giudici di Lussemburgo, vedranno una chiara riproposizione anche nelle decisioni della Corte di Cassazione.

2.3. *La costante giurisprudenza della Corte di Cassazione: un approccio "rassicurante".*

Nelle pronunce emesse dalla Sez. V, 24 aprile 2018, n. 33851 e Sez. III penale, 23 agosto 2019, n. 36380 – che verranno analizzate unitamente, stante le simili doglianze affrontate e le analoghe considerazioni effettuate dai giudici [37] – i ricorrenti avevano ritenuto l'art. 132 Codice Privacy in completo contrasto con gli artt. 7, 8 e 52 della Carta di Nizza, contenendo «tutti i vizi già individuati dalla Corte di giustizia, con conseguente necessità di disapplicare la norma interna e di ritenere la prova acquisita vietata dalla legge e quindi non utilizzabile» [38]. In subordine poi

---

[36] F. RUGGIERI, *Data retention e giudice di merito penale*, cit., p. 2488.

[37] Entrambi i casi originavano dall'impugnazione promossa dai difensori di soggetti la cui condanna – nel primo caso per sequestro di persona e lesioni personali gravi in danno a minore e nel secondo invece per cessione di cocaina – si era fondata anche sull'impiego di indizi ottenuti mediante l'analisi di metadati conservati da compagnie telefoniche. Tali informazioni avevano consentito, ad esempio, nel secondo caso affrontato dalla Corte, di determinare la cellula telefonica agganciata dall'imputato e dunque la sua ubicazione nell'ora precisa in cui il reato era stato commesso.

[38] Para. 3.2, Cass. 23 agosto 2019, n. 36380. In particolare, veniva evidenziata la mancanza di qualsiasi indicazione circa i reati al cui accertamento era finalizzato l'accesso ai metadati, nonché il fatto che non fosse previsto un controllo svolto da un giudice o un'autorità amministrativa indipendente quanto alla necessità dell'accesso, bensì tale delicata decisione di acquisire i metadati conservati dai fornitori di servizi di telecomunicazione fosse affidata ad una parte del procedimento penale, ovvero il pubblico

il difensore dell'imputato aveva richiesto alla Corte di Cassazione di provvedere al rinvio pregiudiziale alla CGUE «affinché accerti se gli artt. 7, 8 e 52 della Carta dei diritti fondamentali dell'UE ostino ad una normativa nazionale, quale quella d.lgs. n. 196/2003, art. 132 che consente l'acquisizione e la conservazione del traffico telematico per qualsiasi tipo di reato e senza un previo controllo della richiesta da parte di un'autorità indipendente» [39].

La Corte di Cassazione è giunta, in entrambi i casi piuttosto rapidamente, a respingere le richieste formulate nell'impugnazione sotto il profilo della disciplina della *data retention*, ritenendo infondate le motivazioni addotte sul punto. I giudici, dopo aver ricostruito la giurisprudenza della CGUE, hanno concluso che essa fosse da riferirsi unicamente agli «Stati privi di una regolamentazione dell'accesso e della conservazione dei dati, mentre lo Stato italiano si è dotato di una specifica disciplina. (…) Nella disciplina italiana peraltro si rinvengono l'enunciazione della finalità di repressione dei reati; la delimitazione temporale dell'attività di memorizzazione; l'intervento preventivo dell'autorità giudiziaria, funzionale all'effettivo controllo della stretta necessità dell'accesso ai dati» [40]. Sulla base dell'analisi svolta dai giudici italiani sono risultati quindi del tutto rispettati i requisiti indicati dalla CGUE, compreso quello del previo controllo di un organo indipendente: la Corte di Cassazione, infatti, già nella sentenza del 2018, aveva sostenuto come la traduzione del testo della decisione *DRI*, nella parte in cui veniva utilizzato il termine *giudice* quale soggetto preposto al controllo preventivo all'accesso ai metadati, fosse da considerarsi erronea. Adottando una interpretazione del tutto letterale del termine impiegato dai giudici di Lussemburgo, i pubblici ministeri, che non possono definirsi "giudici", non avrebbero certamente potuto essere considerati soggetti adatti a svolgere il controllo preliminare, con la conseguenza che la normativa italiana avrebbe dovuto essere di-

ministero. Veniva inoltre rilevata, con riferimento alla durata della conservazione stessa, l'assenza di qualsiasi differenziazione della disciplina sulla base delle categorie di dati interessati così come la mancanza di garanzie contro il rischio di abusi nella fase di accesso.

[39] Para. 3.2, Cass. 23 agosto 2019, n. 36380.

[40] Para 3.5, Cass. 23 agosto 2019, n. 36380.

chiarata sotto tale profilo non rispondente al requisito indicato dalla CGUE. Dal raffronto con la versione francese della pronuncia emergeva, tuttavia, a parere dei giudici italiani, una forte discrepanza rispetto al termine *giudice* impiegato nella traduzione italiana: in francese infatti veniva utilizzato il sostantivo *jurisdiction*, da intendersi pertanto come "magistratura", considerata nella sua totalità e dunque comprensiva sia dei giudici che dei pubblici ministeri (rispettivamente *magistrats du siege* e *magistrats du parquet*). L'utilizzo di un termine più ampio veniva riscontrato anche nella traduzione inglese, nella quale si utilizzava la parola generica *Court*, che potrebbe ricomprendere sia i *judges* che i *prosecutors*. Da tale analisi, la Corte di Cassazione ha fatto derivare come «più che al termine giudice, riportato nella traduzione in maniera non fedele, deve farsi riferimento a quello di autorità giudiziaria, che pacificamente ricomprende anche la figura del pubblico ministero» [41]. Sulla base di tale ragionamento, sono state così respinte le doglianze espresse dai ricorrenti con specifico riferimento al carattere di indipendenza dell'organo preposto al previo controllo sull'accesso ai metadati; su tale punto però sia la CGUE che i giudici italiani stessi sono tornati nuovamente a distanza di tempo a riflettere, con esiti ben diversi da quelli qui riportati, come si avrà modo di evidenziare nell'analisi dei più recenti sviluppi giurisprudenziali.

Nei due casi esaminati, diversamente da quanto affermato dalla dottrina, che già più volte e in più occasioni aveva sottolineato le forti criticità della normativa italiana sul piano della compatibilità con la Carta di Nizza ed il diritto dell'UE, la Corte di Cassazione si è mostrata coerente e costante nel voler mantenere quello che è stato definito un «atteggiamen-

[41] Para 3.6, Cass. 23 agosto 2019, n. 36380. A ciò si aggiungeva come «la soluzione italiana [di affidare il controllo preventivo al pubblico ministero] è coerente con il sistema di tipo accusatorio, nel quale, nel corso delle indagini preliminari, è il pubblico ministero l'autorità giudiziaria che procede, e con il sistema processuale che prevede, mediante le indagini difensive ed i poteri riconosciuti ai difensori anche in tema di acquisizione del dato, l'estensione, anche se parziale, del potere investigativo alla difesa. E ciò in una situazione in cui l'acquisizione del dato genera una compromissione decisamente inferiore rispetto a quella relativa alla captazione delle conversazioni, sia telefoniche che ambientali, la cui tutela è affidata invece al controllo del giudice per le indagini preliminari», para. 3.7 e 3.8.

to "rassicurante"», espressione di un «approccio semplicistico ad un tema (…) colmo di nodi irrisolti» [42]. La posizione espressa dalla Suprema Corte italiana si è rivelata così per certi versi avventata e superficiale, mancando oltretutto di considerare i numerosi rinvii pregiudiziali che già erano stati all'epoca promossi dai giudici di altri Stati membri nei confronti della CGUE, a dimostrazione della complessità che caratterizzava – e caratterizza ancora – i molteplici profili della disciplina della *data retention* e dell'accesso ai metadati. I giudici italiani, al contrario dei colleghi inglesi, belgi, estoni e francesi, avevano invece ritenuto la giurisprudenza europea chiara, non meritevole di ulteriori interventi – anche correttivi, proposti più o meno tra le righe dal IPT inglese e dalla *Cour Constitutionnelle* belga –, risolvendo anzi con grande agilità e semplicità molti dei quesiti che sono invece ancora oggi sottoposti al vaglio della CGUE. Che ciò sia derivato da una certa ritrosia al dialogo con il giudice europeo, da una scarsa conoscenza della materia in esame o ancora dalla ferrea volontà di garantire la giustizia nel caso concreto, evitando di mettere in discussione la legittimità di elementi di prova di grande rilievo, il risultato è stato certamente quello della adozione di una posizione discutibile, se non addirittura erronea. Ne è esemplificazione evidente l'affermazione, peraltro ripresa dalla Ordinanza del Tribunale di Padova, secondo cui la giurisprudenza europea avrebbe riguardato Stati sprovvisti di una regolamentazione sulla conservazione ed accesso ai metadati: nulla di più sbagliato se si considera che sentenze come *Tele2* e *Ministerio Fiscal* avevano al contrario avuto ad oggetto proprio e unicamente discipline nazionali in materia di *data retention*, determinando criteri e requisiti che devono quindi ispirare tutti i legislatori degli Stati membri così come quello europeo. Lo stesso può dirsi rispetto alla riproposizione della già criticata considerazione secondo cui «l'acquisizione del dato genera una compromissione decisamente inferiore rispetto a quella relativa alla captazione delle conversazioni» [43]. La Corte di Cassazione nella sua analisi, inoltre, mostra di concentrarsi fortemente sul requisito del controllo effettuato da un giudice o da un organo indipendente, tralasciando però di considerare gli altri e altrettanto importanti criteri indicati dalla giurisprudenza euro-

[42] L. LUPÁRIA, *Data Retention e processo penale*, cit., p. 761.

[43] Para. 3.7, Cass. 23 agosto 2019, n. 36380.

pea: nulla viene detto, ad esempio, circa la proporzionalità e necessità della natura indiscriminata e generalizzata della conservazione o della durata della *data retention* stessa [44] o quanto alla sussistenza di elementi oggettivi che, seppur indirettamente, colleghino la conservazione alla esigenza di garanzia della sicurezza; non viene neppure preso in considerazione il requisito della gravità del reato e dunque della necessaria presenza di un elenco di reati o di una soglia specifica sulla base della quale l'accesso ai metadati risulti proporzionato alla severità dell'ingerenza nei diritti fondamentali: non bisogna infatti dimenticare come, sebbene ai sensi della Legge Europea 2017 venga fissato un termine temporale di conservazione differenziato e più elevato per talune tipologie di reato, l'accesso ai metadati è comunque garantito per la repressione e indagine relativa a qualsiasi reato, senza alcuna specificazione e differenziazione sulla base della gravità [45]. Al di là della questione, all'epoca ancora aperta e sottopo-

[44] Come affermato dalla giurisprudenza della CGUE, l'ingerenza nella vita privata rappresentata dalla conservazione dei metadati è indipendente dal successivo ed eventuale accesso, e deve quindi, come tale, sottostare ai principi di proporzionalità e necessità. Anche sulla base di tali considerazioni, pare evidente come una *data retention* generalizzata e decisamente prolungata quale quella italiana muova significativi dubbi di compatibilità con il diritto dell'UE. Sul piano della durata, le peculiarità dei singoli ordinamenti nazionali e delle concrete modalità di indagine penale, nonché della tipologia di criminalità che caratterizza un certo Stato – si pensi alla criminalità organizzata di stampo mafioso che rappresenta una realtà forte nel contesto italiano –, potrebbero certamente giustificare una differenziazione nella disciplina della durata della conservazione, ma ciò che dovrebbe ancor prima essere considerato in sede di scelta legislativa sono le concrete e reali esigenze investigative, i dati e le analisi oggettive che possono motivare cioè le decisioni dei legislatori nazionali e risultare in elementi importanti per una fondamentale ed ineludibile valutazione della proporzionalità della durata della *data retention* stessa. Senza dubbio comunque la determinazione di una corretta e proporzionata durata di conservazione dei dati è tema fortemente dibattuto: Signorato ad esempio ritiene che un congruo arco temporale sia da individuarsi in un periodo dai trentasei ai settantadue mesi. «Si è consapevoli che una simile impostazione si scontra con quella prevalente, anche sul piano europeo, volta ad affermare la necessità di tempi di conservazione assai più brevi. Non di rado si tratta però di approcci sbilanciati nella direzione di una aprioristica tutela della privacy», S. SIGNORATO, *Novità in tema di data retention*, cit., p. 160. Una riflessione che non sia sbilanciata né dall'uno né dall'altro lato (pro securitario o garantista dei diritti fondamentali) è quindi necessaria quanto complessa da sviluppare.

[45] «Come affermato dalla stessa Suprema Corte, la disciplina nazionale sull'acquisi-

sta al vaglio della CGUE, circa la necessità della contemporanea garanzia e previsione dei requisiti sulla conservazione e di quelli attinenti invece alla fase di accesso, la Corte di Cassazione non si è assolutamente posta, alla radice, il problema della legittimità della *bulk data retention* e non ha ritenuto fondamentale aprire alcun dibattito su un tema che ha assunto invece in altri Stati membri un grande rilievo e che ha attirato l'attenzione tanto dei legislatori quanto dei giudici in tali Paesi. Nell'esaminare, infine, la figura del pubblico ministero e la possibilità che il controllo ad esso assegnato assolva al criterio di indipendenza delineato dai giudici di Lussemburgo, la Corte di Cassazione ha fondato la propria posizione essenzialmente sull'analisi della terminologia impiegata dalla CGUE nelle diverse traduzioni della sentenza *DRI*. Ebbene, sul punto, come chiaramente rilevato da Lupária, emerge una certa disattenzione da parte dei giudici italiani che hanno mancato di considerare l'impiego della terminologia indicata in altre normative europee: nella decisione quadro 2002/584/GAI, ad esempio, il legislatore europeo ha usato i termini di *autorité judiciare* e di *judicial authority* per riferirsi all'autorità giudiziaria ampiamente intesa e dunque comprensiva anche della pubblica accusa e non solo dei giudici in senso stretto. Sulla base di questa lettura più ampia dei vocabili adottati in altre fonti del diritto dell'UE, le parole *juridiction* e *Court* utilizzate nelle traduzioni francese e inglese delle pronunce in materia di *data retention* non potrebbero dunque essere intese quali sinonimi del termine più generale di "autorità giudiziarie", facendo piuttosto emergere l'intenzione della CGUE di riferirsi, mediante l'impiego di tali vocaboli, più specificamente e restrittivamente ad organi precisi, quali appunto i giudici, confermando così la correttezza della traduzione italiana. Certamente l'obiettivo del requisito stabilito dalla CGUE è da individuarsi nella indipendenza rispetto al potere esecutivo del soggetto pre-

---

zione dei dati esterni alle comunicazioni non è in alcun modo circoscritta in ordine alle tipologie di reato oggetto di indagine o accertamento. Ciononostante, nell'ottica della Corte, il mero riferimento alle "finalità di repressione dei reati" sembra di per sé essere sufficiente a negare ogni ipotesi di contrasto della normativa nazionale con quella eurounitaria, tralasciando di considerare anche la fondamentale applicazione del principio di proporzionalità, così rilevante nella giurisprudenza della CGUE», I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention, in *Sistema Penale*, 5, 2020, p. 186.

posto al controllo, ma è altrettanto vero che l'indipendenza deve essere intesa nel senso di terzietà ed imparzialità, come peraltro specificato dalla ben più risalente giurisprudenza europea [46]: se il pubblico ministero italiano, diversamente da quello di altri Stati membri, risulta senza dubbio indipendente dal Governo e dal Ministero della Giustizia, esso tuttavia assume il ruolo di vera e propria parte nel processo penale eventualmente avviato, così da risultare organo non imparzialità [47]. Focalizzandosi invece su una lettura strettamente letterale dei termini impiegati dal giudice europeo anziché sul significato sostanziale e sulla *ratio* del requisito posto, la Corte di Cassazione nelle pronunce analizzate non si era all'epoca posta alcun quesito circa la portata del criterio dell'indipendenza fissato dalla CGUE, diversamente da quanto invece fatto dalla Corte Suprema estone, che aveva promosso, con rinvio risalente al 2018, l'intervento dei giudici di Lussemburgo al fine di chiarire e precisare correttamente questo delicato profilo. «In un quadro caratterizzato più da dubbi che certezze, la strada maestra che si sarebbe dovuta seguire (…) era quella, sollecitata, del rinvio pregiudiziale. (…) Gli ermellini avrebbero dovuto effettiva-

[46] Si legga, in particolare, la sentenza 19 settembre 2006, *Graham J. Wilson v. Ordre des avocats du barreau du Luxembourg*, C-506/04, nella quale viene specificato che la nozione di "indipendenza" deve essere intesa come comprensiva di due differenti aspetti: «Il primo aspetto, avente carattere esterno, presuppone che l'organo sia tutelato da pressioni o da interventi dall'esterno idonei a mettere a repentaglio l'indipendenza di giudizio dei suoi membri per quanto riguarda le controversie loro sottoposte (…). Tale indispensabile libertà da siffatti elementi esterni richiede talune garanzie idonee a tutelare la persona che svolge la funzione giurisdizionale, come, ad esempio, l'inamovibilità (…). Il secondo aspetto, avente carattere interno, si ricollega alla nozione di imparzialità e riguarda l'equidistanza dalle parti della controversia e dai loro rispettivi interessi concernenti l'oggetto di quest'ultima. Questo aspetto impone il rispetto dell'obiettività (…) e l'assenza di qualsivoglia interesse nella soluzione da dare alla controversia all'infuori della stretta applicazione della norma giuridica», para. 51-52.

[47] «Certamente, le garanzie di indipendenza del magistrato inquirente nei riguardi del potere esecutivo possono dirsi particolarmente forti nel nostro ordinamento – a differenza di quanto accade in numerosi altri Stati membri. D'altro canto, tuttavia, risulta difficile sostenere che la posizione dell'organo di pubblica accusa all'interno del procedimento penale sia una di assoluta indifferenza quanto al risultato finale dell'accertamento di responsabilità», I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention*,* cit., p. 190.

mente domandare se anche un organo formalmente indipendente quale il pubblico ministero italiano, ma non terzo ed imparziale, possa soddisfare lo standard di garanzie richiesto dalla Carta di Nizza»[48]. Del resto, nessun rinvio alla CGUE era stato promosso neppure con riferimento alla sorte delle prove derivanti da metadati conservati sulla base di una normativa non conforme al diritto dell'UE: mentre i giudici italiani hanno risolto tale questione ritenendo che le prove non debbano essere considerate automaticamente inutilizzabili[49], la Corte costituzionale belga e la Corte Suprema irlandese[50] avevano richiesto l'intervento dei giudici di Lussemburgo, al fine di ottenere un chiarimento interpretativo quanto alle possibili conseguenze della dichiarazione di invalidità o incostituzionalità della normativa nazionale in materia di *data retention*.

Per tutte le ragioni sopra indicate e per le incongruenze e superficialità nell'analisi di una disciplina che avrebbe meritato ben altro peso ed attenzione, le decisioni della Corte di Cassazione in materia di *data retention* hanno attirato notevoli critiche da parte della dottrina: così, con riferimento alla pronuncia del 2019 e nello specifico alla assenza di valutazioni complete quanto alla compatibilità della normativa italiana rispetto ai numerosi requisiti fissati dalla giurisprudenza europea, è stato rilevato come «il vuoto motivazionale che affligge in proposito la decisione *de qua* non può che essere apertamente stigmatizzato: pare, invero, inaccettabile che i supremi giudici nomofilattici, vista la sostanziale impossibilità di salvare da siffatto punto di vista la legittimità delle previsioni interne, ab-

---

[48] L. LUPÁRIA, *Data Retention e processo penale*, cit., p. 763.

[49] «È noto che la inutilizzabilità cosiddetta "patologica", rilevabile, a differenza di quelle "fisiologica" e "relativa" anche nell'ambito del giudizio abbreviato, costituisce un'ipotesi estrema e residuale, ravvisabile solo con riguardo a quegli atti probatori assunti *contra legem*, la cui utilizzazione è vietata in modo assoluto. Nella fattispecie in rassegna, anche a voler disapplicare il D.lgs. 196 del 2003, art. 132, ci si troverebbe in presenza di un atto compiuto in assenza di legge ordinaria, conforme, però, ai principi fondamentali dell'ordinamento e in particolare al disposto dell'art. 15 Cost. che prevede limitazioni alla libertà e segretezza di ogni forma di comunicazione mediante atto motivato della autorità giudiziaria. Pertanto l'atto sarebbe utilizzabile, qualunque fosse la conclusione sul tema dei rapporti tra normativa interna e principi sovranazionali», sentenza 24 aprile 2018, n. 33851, para. 1.3.2.

[50] Si richiama sul punto l'analisi svolta nel Capitolo 2 del presente lavoro.

biano del tutto omesso di argomentare questo profilo» [51]. Una posizione, quella dei giudici italiani, che è stata vista come motivata – ma non per questo giustificabile – dalla volontà di preservare l'efficacia dello strumento della *data retention* e dunque la legittimità delle prove da esso derivate, senza addivenire a modifiche o interventi normativi, a scapito però dell'elevato livello di tutela della riservatezza e della protezione dei dati individuato dalla giurisprudenza della CGUE.

Critiche che non sono tuttavia servite, quanto meno in un primo momento, a promuovere un cambiamento di rotta da parte dei giudici italiani: le successive sentenze Sez. III 25 settembre 2019, n. 48737 e Sez II, 10 dicembre 2019, n. 5741, della Corte di Cassazione si sono poste infatti in linea di continuità con le due pronunce sopra esaminate, ribadendo la compatibilità dell'art. 132 Codice Privacy con il diritto dell'UE, nonostante l'assenza di restrizioni alla conservazione e la mancanza di limitazioni all'accesso ai metadati per i soli scopi di repressione dei reati gravi, predeterminati per legge. In particolare, con riferimento a tale ultimo profilo, secondo i giudici italiani la determinazione del carattere di gravità rappresenta una valutazione che non può sottoporsi ad una rigida codificazione da parte del legislatore e che deve pertanto essere correttamente rimessa al vaglio, caso per caso, del giudice. Ciò, a parere della Corte, non si tradurrebbe in un contrasto con la giurisprudenza della CGUE, che affermerebbe anzi solo la sussistenza di un rapporto di proporzionalità tra accesso – e dunque ingerenza – e reato sul quale investigare «in base ad una verifica che il giudice di merito deve compiere in concreto» [52], come ribadito peraltro nella sentenza *Ministerio Fiscal*, ri-

[51] L. LUPÁRIA, *Data Retention e processo penale*, cit., p. 764. Dello stesso avviso anche Rezende che afferma come la Corte di Cassazione si sia «sottratta alla resa dei conti con la tormentata disciplina della *data retention* (…). Dal percorso motivazionale della Corte difficilmente emergono profili di analisi sostanziale della disciplina italiana nella materia esaminata. Al contrario, essa sembra faticare nel dare il giusto peso alle questioni poste», I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention*,* cit., p. 185.

[52] «Alla luce di tali principi, deve dunque affermarsi il principio secondo cui l'articolo 132 c.pr., nella parte in cui non limita l'accesso ai dati di traffico telefonico, a fini di giustizia penale, a categorie di reati ritenuti particolarmente gravi, non si pone in contrasto con la disciplina sovranazionale di matrice Eurounitaria, il cui rispetto impone

chiamata proprio dai giudici della Cassazione. Sebbene questa analisi – maggiormente articolata ed attenta nonché estesa anche alla più recente giurisprudenza della CGUE disponibile all'epoca – sia un segnale positivo che va nella direzione di attribuire una più ampia rilevanza e profondità allo studio e alle considerazioni necessarie per risolvere le questioni complesse attinenti alla materia della *data retention*, l'esito finale di una simile disamina si è rivelato invero piuttosto discutibile. Senza dubbio la CGUE nelle proprie decisioni non parla mai della necessaria adozione, da parte del legislatore nazionale, di un catalogo di reati "gravi", ma è altrettanto vero che nella sentenza *DRI* viene affermata l'invalidità della DRD proprio nella parte in cui «non stabilisce espressamente che tale accesso e l'uso ulteriore dei dati di cui trattasi debbano essere strettamente limitati a fini di prevenzione e di accertamento di reati gravi delimitati con precisione o di indagini penali ad essi relative» (para. 61), senza dimenticare che la DRD stessa imponeva che la conservazione fosse effettuata al fine di «garantire la disponibilità dei suddetti dati a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale» (art. 4). Da tale lettura della previgente normativa europea nonché della giurisprudenza della CGUE, e diversamente da quanto sostenuto dai giudici italiani, deriva come un elemento fondamentale per determinare in maniera preventiva la natura grave del reato, al di là della singola valutazione dei giudici, sia da individuarsi nell'indicazione, all'interno della disciplina normativa che regola conservazione ed accesso, di un elenco di reati gravi o nella determinazione di criteri volti a stabilire il carattere di "gravità" (ad esempio basandosi sugli anni di reclusione). Simili considerazioni sono peraltro confermate anche dalle scelte normative effettuate dalla maggioranza de-

---

invece una valutazione in concreto della proporzione tra gravità dell'ingerenza nel diritto fondamentale alla vita privata che l'accesso ai dati comporta e gravità del reato oggetto d'indagine. Questa valutazione – che, ovviamente, dipende da una serie di variabili connesse alla particolarità dei casi concreti – mal si presta ad una preventiva, rigida, codificazione e non può che essere rimessa alla prudente valutazione dell'autorità giudiziaria, o comunque indipendente, che, per la normativa Eurounitaria così come interpretata dalla giurisprudenza della Corte di Lussemburgo, costituisce indefettibile garanzia rispetto alla tutela dei diritti fondamentali», sentenza 25 settembre 2019, n. 48737, para. 3.6.

gli altri Stati membri (quali Belgio, Spagna e Svezia ad esempio). Ciò peraltro va a tutto favore del rispetto del principio di certezza del diritto e di una applicazione dell'art. 132 Codice Privacy che non sia lasciata alla discrezionalità del potere giudiziario e dunque passibile di diverse interpretazioni, dalle potenziali significative conseguenze nei confronti degli imputati o indagati e dei loro diritti.

3. *Dall'impegno di riforma assunto dal Governo al rinvio pregiudiziale promosso dal Tribunale di Rieti: l'Italia verso una reale svolta?*

3.1. *Le ripercussioni della sentenza* H.K. c. Prokuratuur *nel contesto italiano.*

L'analisi del percorso normativo e giurisprudenziale italiano sin qui svolto ha messo in luce quella che è stata definita una disciplina «disarmonica» [53] rispetto ai principi delineati dalla giurisprudenza della CGUE; le sentenze esaminate e gli interventi legislativi che hanno caratterizzato il panorama nazionale dimostrano come la disciplina della *data retention*, le sue complessità e le rilevanti pronunce adottate a livello sovranazionale, unitamente al serio dibattito apertosi in ambito accademico nonché politico all'interno delle diverse istituzioni dell'UE e di numerosi Stati membri, non abbiano suscitato in Italia «l'interesse che meritavano, né in dottrina né in giurisprudenza e soprattutto non hanno turbato il sonno del legislatore nazionale» [54].

Solo in tempi estremamente recenti si è potuto intravedere un maggiore e ravvivato discussione in materia: piuttosto singolarmente non sono state le dirompenti pronunce dell'ottobre 2020 – che hanno più ampiamente chiarito i limiti della *data retention* e che hanno aperto un così complesso e vivace dibattito in Francia e Belgio, circa i limiti della conservazione generalizzata ed indiscriminata per scopi di garanzia della sicurezza nazionale o pubblica – a scatenare una significativa reazione di Cor-

---

[53] 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*, 2, 2017, p. 356.

[54] S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, cit., p. 1591.

ti e legislatore nel contesto italiano. Con sentenza n. 10022, del 10 novembre 2020, infatti, la Suprema Corte italiana ribadiva nuovamente il proprio previo orientamento, riconfermando ancora una volta la compatibilità della disciplina italiana in materia di *data retention* con il diritto dell'UE poiché «la deroga stabilita dalla norma alla riservatezza delle comunicazioni è prevista per un periodo di tempo limitato, ha come esclusivo obiettivo l'accertamento e la repressione dei reati ed è subordinata alla emissione di un provvedimento da parte di un'autorità giurisdizionale». A seguito delle importanti sentenze *La Quadrature du Net* e *Privacy International*, dunque, non si è registrato alcun mutamento di indirizzo nella giurisprudenza della Corte di Cassazione: rispetto a quest'ultima e anche nei confronti della citata ultima pronuncia del 2020 sono quindi riproponibili le già evidenziate criticità che hanno caratterizzato le precedenti pronunce dei giudici italiani e che sembrano ancor più marcate dopo gli ulteriori chiarimenti disposti dalla CGUE.

A non passare inosservata, invece, è stata – forse anche a causa dei richiami all'ordinamento italiano operati dall'Avvocato generale Pitruzzella nelle sue Conclusioni – la sentenza dei giudici di Lussemburgo nel caso *H.K. c. Prokuratuur* derivante, come si ricorderà, dal rinvio della Corte Suprema estone, avente ad oggetto primariamente la disciplina dell'accesso, i requisiti della gravità del reato e, soprattutto, il carattere indipendente del controllo giudiziario preventivo all'accesso ai metadati. È stata questa decisione ad aver provocato, innanzitutto, una reazione nel Parlamento e nel Governo italiano: si fa riferimento all'accoglimento da parte del Governo dell'ordine del giorno 9/2670-A/10, proposto in occasione dell'esame del disegno di Legge Europea 2019/2020, avvenuto il 1 aprile 2021. Pur rappresentando al momento solo una dimostrazione della volontà e della responsabilità politica espressa dal Governo, quest'ultimo con l'approvazione dell'OdG indicato si è impegnato a rivedere la disciplina della *data retention* e dell'accesso ai metadati tenendo in considerazione i principi e criteri enucleati dalla costante e continua giurisprudenza europea in materia. Questa "presa in carico" di una questione da tempo rimasta fuori dal dibattito politico e parlamentare, è stata considerata un «cambio di passo importante» [55] rispetto al passato: seb-

[55] Così F. RESTA, *Data retention, che cambia con l'impegno del Governo a adeguare la normativa italiana*, in *AgendaDigitale*, 9 aprile 2021.

bene sia difficile prevedere come il Governo interverrà e quali disposizioni deciderà di adottare, l'espressa intenzione di occuparsi della materia volgendo lo sguardo a quanto accaduto – e continua ad accadere – sul piano sovranazionale, non può che essere visto come una importante occasione di cambiamento e riflessione, che si è fatta attendere per anni.

Se dunque solo nei mesi a venire si potranno osservare le possibili evoluzioni sul piano normativo e le discussioni che ne seguiranno, rilevanti novità si sono invece già registrate sul piano giurisprudenziale: se infatti una certa disattenzione e mancanza di approfondita considerazione delle decisioni della CGUE in materia di *data retention* ha caratterizzato il percorso della giurisprudenza italiana sin qui tratteggiato, i requisiti stabiliti dalla pronuncia *H.K c. Prokuratuur* sono stati invece esaminati e considerati da diverse Corti che, confrontandosi con il portato della giurisprudenza europea, sono giunte ad esiti anche molto differenti tra loro. Sebbene non si voglia qui provvedere ad una ricostruzione dettagliata di tutte le decisioni assunte dai Tribunali italiani ed aventi quali riferimento proprio gli effetti della pronuncia dei giudici di Lussemburgo del marzo 2021, pare nondimeno imprescindibile cercare di evidenziare i profili di maggiore interesse di alcuni di questi interventi giurisprudenziali, così da rilevarne difformità e criticità. A breve distanza di tempo l'uno dall'altro, ad esempio, il Tribunale di Milano, VII Sezione Penale con ordinanza n. 585/2021 del 22 aprile 2021 e il Tribunale di Roma, Sezione G.i.p.-G.u.p., con decreto del 25 aprile 2021 sono addivenuti a due opposte conclusioni: il giudice milanese, infatti, ha rigettato l'eccezione promossa dal difensore dell'imputato, volta ad ottenere l'inutilizzabilità dei metadati acquisiti sulla base di una autorizzazione del p.m. Tale conclusione è fondata sulla considerata conformità della normativa italiana rispetto al diritto dell'UE, anche sulla base delle ampiamente richiamate motivazioni – già risultate però piuttosto criticate – impiegate dal Tribunale di Padova e dalla Corte di Cassazione nelle decisioni sopra approfondite. Pronunciandosi sul portato della sentenza della CGUE per l'ordinamento interno, il giudice lombardo ha ritenuto sussistente una netta distinzione tra l'organo di accusa estone, con riferimento al quale il caso europeo originava, e il p.m. italiano: mentre il primo è autorità «soggetta alla sfera di competenza del Ministero della Giustizia che partecipa alla pianificazione delle misure necessarie per la lotta all'accertamento dei reati», il secondo è

«chiamato ad esercitare sotto la vigilanza del Ministero di Grazia e Giustizia le funzioni che la legge gli attribuisce, con garanzia dell'impersonalità del suo ufficio e con la caratteristica ulteriore che esso riveste nel processo penale il ruolo di parte pubblica e non privata», p. 4. Ciò quindi basta, a parere dei giudici milanesi, per considerare non trasponibili rispetto all'ordinamento italiano le censure mosse dai giudici di Lussemburgo, ritenendo peraltro l'orientamento della Corte di Cassazione italiana come in nulla superato dai contenuti della sentenza della CGUE del 2 marzo 2021 [56].

Il giudice romano, al contrario, ha dichiarato l'incompatibilità dell'art. 132 Codice Privacy rispetto al diritto dell'UE, così come interpretato dalla CGUE, nella parte in cui viene attribuito al p.m. il compito di controllare la legittimità dell'accesso ai metadati. Diversamente dal collega milanese, infatti, il G.i.p. romano ha posto attenzione ad uno specifico requisito affermato dalla giurisprudenza europea, ovvero quello della neutralità: il p.m., essendo una parte del processo, non può che considerarsi privo del necessario e imprescindibile carattere di terzietà [57]. Il G.i.p. poi si è spinto oltre, non ritenendo di dover disapplicare la norma interna bensì di poter direttamente applicare la normativa sovranazionale, sulla base di quanto affermato dai giudici di Lussemburgo. Così facendo, il G.i.p. ha proposto una lettura differente da coloro che invece hanno rin-

---

[56] Per approfondimenti, si rimanda a V. TORDI, *La disciplina italiana in materia di data retention a seguito della sentenza della Corte di giustizia Ue: il Tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sistema Penale*, 7 maggio 2021 e 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*, II, 2021, pp. 540-554. Quest'ultimo, così come anche Tordi, fornisce una lettura critica della pronuncia del G.i.p. di Milano, che non solo non attribuisce alla pronuncia *H.K. c. Prokuratuur* alcun profilo innovativo, ma compie addirittura «un tuffo nel passato: vengono riproposti pedissequamente gli approdi giurisprudenziali [della Corte di Cassazione] che oggi, però, risultano essere del tutto inadeguati», p. 552.

[57] «Le argomentazioni sostenute [dalla CGUE] sono inequivoche e non possono circoscriversi agli ordinamenti giuridici nei quali la figura del PM non è indipendente: il Giudice europeo, a ben vedere, ha motivato l'attribuzione del controllo preventivo al Giudice in ragione (non solo dell'indipendenza ma soprattutto) della neutralità nei confronti delle parti del procedimento penale», p. 2.

venuto nella vaghezza del termine di "gravità" del reato impiegato dalla giurisprudenza sovranazionale un elemento tale da impedire la diretta applicabilità della decisione nel contesto italiano [58]. Il G.i.p. romano, al contrario, ha ritenuto che la determinazione della categoria dei reati gravi, non direttamente specificata dalla CGUE e neppure dal legislatore italiano, sia «facilmente individuabile con il rinvio integrale ai reati previsti nel catalogo dettato dagli artt. 266 c.p.p. e 266-*bis* c.p.p.» (p. 5) ovvero nei casi in cui sono ammesse le attività di intercettazione. Sebbene questo assunto possa certamente essere criticato per la sua portata creativa, alcuni primi commentatori hanno sottolineato come «siffatta significativa svolta esegetica presenti il pregio di essere non solo garantista, ma anche pragmatica: suggerendo di applicare in modo sostanzialmente analogico la disciplina delle intercettazioni ai tabulati, il G.i.p. di Roma ha individuato un modo per evitare che l'autorità giudiziaria italiana non possa più avvalersi di uno strumento di importanza chiave nell'accertamento dei reati (…) nelle more di un intervento normativo del legislatore nella materia *de qua*» [59].

---

[58] Di tale avviso il G.i.p. Dott. Fanelli, sempre del Tribunale di Roma, Sezione G.i.p.-G.u.p. che, il 28 aprile 2021 ha ritenuto la pronuncia *H.K. c. Prokuratuur* non direttamente applicativa, considerati troppo generici i riferimenti a fondamentali concetti quali "lotta contro forme gravi di criminalità" o "gravi minacce alla sicurezza pubblica"; essi, proprio sulla base della giurisprudenza europea, debbono essere invece individuati dalle normative interne degli Stati membri. L'art. 132 Codice Privacy deve pertanto continuare ad essere applicato sino a quando un auspicabile intervento del legislatore nazionale specifichi le condizioni e i requisiti dell'accesso. Per l'analisi di questo e di altri simili provvedimenti in materia, come quello del G.i.p. Savio, anch'egli del Tribunale di Roma, si rimanda più ampiamente a L. GRANOZIO, *Corte di Giustizia sui tabulati: soluzioni contrastanti*, in *Penale. Diritto e Procedura*, 18 maggio 2021 e A. MALACARNE, *Ancora sulle ricadute interne della sentenza della Corte di Giustizia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il 'non luogo a procedere' sulla richiesta del p.m.*, in *Sistema Penale*, 5 maggio 2021.

[59] J. DELLA TORRE, *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della CGUE: la svolta garantista in un primo provvedimento del G.i.p. di Roma*, in *Sistema Penale*, 29 aprile 2021. Di avviso opposto invece Torre, che ritiene da recidere il rapporto "ombelicale" tra tabulati e intercettazioni: «la materia dei dati esteriori dovrebbe essere caratterizzata, a livello interno, da quella autonomia e indipendenza rinvenibili a livello europeo. Tale strumento di prova è, infatti, dotato di

Questa interpretazione giurisprudenziale, che propone dunque la diretta applicabilità del diritto dell'UE, non ha tuttavia trovato sino ad ora seguito: mentre la Corte di Assise del Tribunale di Napoli il 16 giugno 2021 si è pronunciata in maniera del tutto simile al Tribunale di Milano [60], il G.i.p del Tribunale di Tivoli, pur riconoscendo con ordinanza del 9 giugno 2021 l'incompatibilità della disciplina italiana rispetto al diritto europeo, così come interpretato dalla CGUE [61], ha infine escluso l'applicazione diretta della sentenza dei giudici di Lussemburgo [62]. Rilevando

"multiformi potenzialità (…) destinate ad accrescersi con il perfezionarsi della tecnologia", non potendosi quindi aprioristicamente stabilire se lo stesso sia meno invasivo dell'apprensione del contenuto di una conversazione», F. TORRE, *Data retention. Una ventata di "ragionevolezza" da Lussemburgo*, cit., p. 552.

[60] La Corte ha infatti respinto l'eccezione avanzata dai difensori degli imputati volta alla declaratoria di nullità dei metadati acquisiti a giudizio, ritenendo che i principi affermati dalla CGUE nella pronuncia del marzo 2021 non possano essere «trasfusi in via automatica nell'ordinamento nazionale», in quanto il p.m. non solo è organo autonomo e indipendente da qualsiasi altro potere ma, diversamente da quanto disposto riguardo all'organo di accusa estone, il p.m. italiano è chiamato anche a motivare adeguatamente con decreto le esigenze che spingono alla richiesta di accesso ai metadati. Del tutto similmente al giudice lombardo poi, anche la Corte campana ha ritenuto legittima una valutazione caso per caso del criterio di gravità del reato, considerando dunque l'assenza di una specifica elencazione o categorizzazione normativa come non determinante una violazione dei requisiti stabiliti dalla giurisprudenza sovranazionale.

[61] Si legga sul punto un primo commento di S. ATERNO, *Data retention: gli effetti nel nostro Paese della sentenza del 2 marzo 2021 della CGUE*, in *e-Lex*, 21 giugno 2021.

[62] «Vi è dunque un evidente contrasto tra la Corte di Cassazione e la CGUE in ordine alla compatibilità dell'art. 132 d.lgs. 196/2003 con la Direttiva 2002/58/CE almeno laddove tale norma nazionale prevede la competenza del PM ad autorizzare l'acquisizione dei tabulati relativi ai dati di traffico telefonico e telematico»; tuttavia, «ipotizzando di dover disapplicare la normativa attualmente vigente nel nostro ordinamento in tema di acquisizione di tabulati (art. 132) per l'asserita incompatibilità con la disciplina comunitaria così come interpretata dalla sentenza della CGUE, non vi è dubbio che verrebbe a crearsi un vuoto normativo che, ad avviso della scrivente, non potrebbe essere colmato da attività ermeneutiche rimesse alla decisione del singolo giudice. (…) Per tutte queste ragioni, deve ritenersi che la sentenza della CGUE sopra menzionata non possa trovare immediata e diretta applicazione nel procedimento in esame, con la conseguenza che, in attesa di un intervento del legislatore nazionale, deve invece ritenersi applicabile l'art. 132 d.lgs. n. 196, dovendosi dare continuità all'orientamento giurisprudenziale di legittimità ormai consolidatosi (…)», p. 2.

quella contrapposizione tra giurisprudenza sovranazionale e costante orientamento espresso dalla Corte di Cassazione oggetto di analisi nel previo paragrafo, il giudice di Tivoli ha evidenziato il bisogno di un intervento del legislatore nazionale in grado di fornire criteri certi e precisi e di risolvere così la complessa situazione attuale.

Un contesto così confuso e contrastante, quello appena descritto, da creare inevitabilmente dubbi ed interrogativi applicativi di non poco rilievo, capaci di incidere notevolmente sul processo penale, sulla legittimità delle prove acquisite e dunque sui diritti di vittime ed imputati e sull'interesse generale ad una giustizia efficace e ad una efficiente repressione dei reati. In questo quadro articolato – nel quale peraltro anche la dottrina è intervenuta auspicando l'intervento chiarificatore di un'alta Corte nazionale [63] o evidenziando l'esigenza, resa ancor più forte dalle discordanti posizioni espresse dai giudici, di una presa di posizione del legislatore mediante approvazione di una nuova normativa in materia di accesso ai metadati, che sappia tenere conto anche della giurisprudenza sovranazionale [64]–, si inserisce l'ordinanza di rinvio pregiudiziale alla CGUE

[63] Tra i tanti, si legga E.N. LA ROCCA, *A margine di una recente sentenza della Corte di Giustizia UE (C-748/18): riflessi sinistri sulla disciplina delle intercettazioni in Italia*, in *Diritti Comparati*, 8 aprile 2021. Torre ritiene inoltre «del tutto probabile che in tempi brevi si perverrà al giudizio della Corte costituzionale, chiamata a fare chiarezza a seguito delle molteplici soluzioni interpretative che verranno offerte dalla giurisprudenza di merito», F. TORRE, *Data retention. Una ventata di "ragionevolezza" da Lussemburgo*, cit., p. 552.

[64] F. RINALDINI, *Data retention e procedimento penale. Gli effetti della sentenza della Corte di giustizia nel caso H.K. sul regime di acquisizione dei tabulati telefonici e telematici: urge l'intervento del legislatore*, in *Giurisprudenza Penale Web*, 5, 2021. Anche il Garante per la Protezione dei Dati Personali, Pasquale Stanzione, nella Relazione per l'anno 2020, tenutasi il 2 luglio 2021, ha posto particolare rilievo non solo alla lettura garantista promossa dalla CGUE in materia di *data retention* e all'importanza del dialogo con tale Corte avviato dal rinvio pregiudiziale promosso dal Tribunale di Rieti, ma anche all'intervento del legislatore: «Tali esigenze di garanzia dovrebbero essere valorizzate anche dal legislatore nazionale, chiamato in questo ambito a una riforma che il Garante ha più volte sollecitato e che, dopo l'accoglimento del relativo Ordine del Giorno al disegno di legge europea, appare finalmente ben avviata», GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Tecnica, protezione dei dati e nuove vulnerabilità. Relazione del Presidente Pasquale Stanzione 2020*, 2021, p. 16. Più ampie e dettagliate considerazioni, del

disposta dal Tribunale di Rieti, Sezione Penale. Il 4 maggio 2021, il giudice laziale ha infatti promosso tre quesiti, incentrati tutti sul requisito di indipendenza del vaglio giurisprudenziale stabilito dalla giurisprudenza sovranazionale, chiedendo in particolare se l'art. 15 Direttiva *e-Privacy* debba essere letto nel senso che esso osta «ad una normativa nazionale [quale quella dell'art. 132 Codice Privacy] la quale renda il p.m., organo di dotato di piene totali garanzie di indipendenza e autonomia (…), competente a disporre mediante decreto motivato l'acquisizione dei dati relativi al traffico e all'ubicazione ai fini di un'istruttoria penale» (para. 4.3.1) [65]. È questo il primo rinvio promosso da una Corte italiana avente ad oggetto la materia della *data retention* e accesso ai metadati [66]: una reazione invero già da tempo invocata ed attesa, nella direzione della instaurazione di un dialogo con i giudici di Lussemburgo, quale frutto di una maggiore comprensione della complessità della disciplina in oggetto e della necessità di ottenere chiarimenti ai tanti interrogativi aperti dalla

tutto coerenti comunque con quanto già rilevato, sono state promosse dal Garante anche nella *Segnalazione sulla disciplina della conservazione, a fini di giustizia, dei dati di traffico telefonico e telematico*, inviata il 2 agosto 2021 al Ministro della Giustizia, Prof.ssa Marta Cartabia.

[65] Il giudice del rinvio peraltro propone numerose valutazioni, finalizzate a porre in evidenza le differenze tra il p.m. italiano e l'organo di accusa estone, rilevando quelle che definisce "differenze strutturali" tra le due autorità, nonché sottolineando come nell'ordinamento italiano il giudice, a norma dell'art. 495 c.p.p. sia tenuto ad ammettere le prove solo dopo aver sentito le parti, così fornendo anche un'ulteriore tutela oltre al vaglio del p.m. A tale quesito si aggiunge quello relativo alla possibilità di modulare in chiave irretroattiva gli effetti della eventuale sentenza determinante l'incompatibilità con il diritto dell'UE della disciplina italiana in materia di *data retention* e accesso ai metadati, «al fine di non pregiudicare fondamentali esigenze di certezza del diritto e certezza investigativa, limitatamente ai giudizi tuttora pendenti, in chiave di prevenzione e repressione di gravi rati, nell'ottica anche di consentire un possibile a auspicabile intervento del legislatore nazionale in materia, senza che si realizzino ingiustificate disparità di trattamento con altri istituti della legislazione nazionale, ad esempio in tema di intercettazioni telefoniche», para. 5. Per approfondimenti, si legga G. STAMPANONI BASSI, *Acquisizioni dei tabulati telefonici e telematici: il Tribunale di Rieti propone questione pregiudiziale alla CGUE*, in *Giurisprudenza Penale*, 13 maggio 2021 e L. GRANOZIO, *Corte di Giustizia sui tabulati: soluzioni contrastanti*, cit.

[66] Domanda di pronuncia pregiudiziale proposta dal Tribunale di Rieti nel procedimento penale a carico di G.B. e R.H., causa C-334/21.

scarna normativa europea e dalla ampia ma discussa giurisprudenza sovranazionale. Senza dubbio, è importante sottolineare come il rinvio non abbia ad oggetto la *data retention* in quanto tale, così che nessun quesito è stato, neppure in questa occasione, sollevato quanto alla legittimità della disciplina della conservazione generalizzata ed estremamente ampia nella durata prevista in Italia, nemmeno dinnanzi alle forti e precise considerazioni della CGUE nelle pronunce *La Quadrature du Net* e *Privacy International*. Questo aspetto non può che essere ritenuto problematico, soprattutto se osservato in comparazione alle significative reazioni registratesi in altri ordinamenti, come il Belgio: mentre, come si è visto, la Corte costituzionale belga ha recentemente dichiarato l'illegittimità costituzionale della normativa interna che prevedeva una forma di conservazione generalizzata ed indiscriminata ritenuta in contrasto con il diritto dell'UE, in Italia questo delicatissimo e determinante profilo è stato ignorato o è stato addirittura rapidamente risolto, come emerso dalla sentenza della Corte di Cassazione 10 novembre 2020, n. 10022. Se questa mancata attenzione verso uno degli elementi più problematici e discussi dello strumento della *data retention* deve far riflettere sulla correttezza e completezza dell'analisi dei giudici nazionali, il riconoscimento dell'esistenza di criticità ed incertezze quanto alla conformità della disciplina nazionale rispetto a taluni criteri indicati dal diritto dell'UE, unitamente alla promozione dell'intervento della CGUE in materia, dimostrati dal Tribunale di Rieti, vanno nondimeno indicati come sviluppi positivi e di rilievo nel panorama italiano. A ciò sono da sommarsi l'inedito impegno assunto dal Governo mediante l'approvazione dell'OdG citato, nonché gli svariati interventi delle Corti, che non hanno mancato di considerare più attentamente rispetto al passato – pur con esiti non sempre chiari – l'impatto della giurisprudenza sovranazionale sull'ordinamento interno. Così, per quanto sia presto per considerare questi recenti progressi come rappresentativi di una vera e propria svolta rispetto a quanto ha caratterizzato la giurisprudenza e gli interventi normativi degli ultimi due decenni, essi nondimeno costituiscono un passo importante verso l'apertura di una discussione approfondita sulla *data retention*. Ed è questo ciò che forse con più chiarezza emerge dai recenti provvedimenti delle Corti italiane: la necessità di una riflessione e di un intervento da parte del legislatore nazionale, il solo capace di scongiurare

insidiosi contrasti giurisprudenziali e di effettuare scelte precise quanto ai requisiti procedurali, alle garanzie e ai limiti nonché alla determinazione di concetti chiave quali quello di "reato grave". Sarà da questo intervento normativo, insieme ai chiarimenti che il rinvio pregiudiziale apporterà e al contributo che la giurisprudenza nazionale saprà fornire, che dipenderà il futuro, ancora incerto, della disciplina della *data retention* in Italia.

3.2. *Il mancato dibattito sulla proporzionalità della conservazione generalizzata: necessarie riflessioni.*

Se, dunque, a partire dalla prima metà del 2021 e sotto la spinta della sentenza *H.K. c. Prokuratuur* si è assistito ad un primo timido ma rilevante risveglio del dibattito in tema di *data retention* e accesso ai metadati, che ben potrebbe costituire la base per un futuro intervento normativo più puntuale e per una più approfondita valutazione degli effetti della giurisprudenza della CGUE da parte delle Corti nazionali, non possono comunque non essere avanzate in questa sede alcune considerazioni conclusive sull'approccio italiano ricostruito nei previ paragrafi. Al di là infatti degli ultimi sviluppi, le cui conseguenze restano tutte da determinare, è innegabile come, sotto il profilo normativo, gli interventi di modifica e riforma succedutisi sino ad ora siano andati nella direzione di ampliare, anziché restringere, la portata della conservazione e dell'accesso ai metadati – dal mancato inserimento di limitazioni e restrizioni quanto ai reati per i quali la *data retention* e l'accesso sono consentiti, alla aumentata durata della conservazione[67]–. L'avvicendarsi di continue riforme legi-

[67] «Insomma nel sistema plasmato dal legislatore nazionale vi è un circuito di criminalità grave per il quale l'obbligo di conservazione è di sei anni, termine certamente contrario al principio di proporzionalità; ed un circuito di criminalità comune per il quale l'obbligo di conservazione riguarda tutti i reati, del pari contrario a detto principio. Con l'aggravante che, nella prassi, il gestore, non potendo ovviamente distinguere ex ante chi, fra i propri clienti, sarà autore di reati gravi, anche terroristici, e chi di 'semplici' reati comuni, dovrà conservare in modo generalizzato i dati di tutti, tenendoli a disposizione delle agenzie di *law enforcement* per sei anni», S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, cit., p. 1593.

slative, spesso non anticipate da una appropriata discussione parlamentare capace di cogliere la reale portata e la delicatezza della materia in esame, hanno finito col creare quello che è stato ritenuto un «pasticcio normativo» [68]. Il susseguirsi di deroghe, proroghe e discipline eccezionali, finite poi col divenire la regola nella realtà applicativa, non ha che acuito la confusione di una regolamentazione frammentaria e in continuo cambiamento. Così facendo, il legislatore nazionale ha evitato quanto invece sarebbe stato di estrema importanza, ovvero addivenire ad una seria riflessione sulla materia, promuovendo un intervento normativo ordinato, capace di andare oltre la singola e temporanea urgenza o esigenza emergenziale e di coprire così la disciplina della *data retention* in modo complessivo, anziché inserirla in maniera sparsa in diverse fonti, oltretutto non sempre appropriate per regolare una materia che presenta un impatto così rilevante sui diritti fondamentali. Senza dubbio gli attacchi terroristici che hanno scosso il Continente europeo hanno spinto il legislatore italiano ad introdurre con rapidità e "a caldo" eccezioni alla disciplina generale in materia di riservatezza e protezione dei dati, ma è altrettanto vero che la discussa "normalizzazione" dell'emergenza non può giustificare la mancanza di una successiva riflessione, "a mente fredda", su una materia tanto articolata e che dovrebbe essere oggetto di considerazioni di ben più ampio respiro. Del resto, la «vicenda dell'art. 24, legge n. 167/2017 dimostra ancora una volta che interventi "tampone" od eccezionali non possono che complicare il quadro, quando a mancare o comunque a non raggiungere gli standard richiesti è la stessa normativa base. Ed appare davvero grave che il legislatore nazionale si sottragga alla responsabilità di dettare una disciplina organica della questione» [69]. Nonostante le critiche e le riflessioni promosse da parte della dottrina, nemmeno la giurisprudenza italiana, similmente al legislatore e diversamente dagli omologhi di altri Stati membri, ha mostrato di saper cogliere la problematicità della

[68] P. CAPUTO, *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1, 2016, p. 36. Andolina parla di «tormentata stratificazione della normativa», E. ANDOLINA, *L'acquisizione nel processo penale dei dati 'esteriori' delle comunicazioni telefoniche e telematiche*, Padova, Cedam, 2018.

[69] S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, cit., p. 1593.

disciplina e di considerare appieno i difficili requisiti previsti dalle pronunce della CGUE. È solo a distanza di quasi un decennio dalla sentenza *DRI* che talune Corti hanno valutato, come si è visto, l'esistenza di profili di incompatibilità della normativa interna rispetto al diritto dell'UE tali da portare alla disapplicazione della legislazione nazionale o, ancora, al rinvio pregiudiziale ai giudici di Lussemburgo. Così, nel perdurante silenzio del legislatore – o meglio nel rumore scomposto e confuso provocato dai vari interventi e disposizioni eccezionali succedutesi negli ultimi anni – e in attesa di registrare evoluzioni future sia sul fronte normativo che su quello giurisprudenziale, la normativa italiana sulla *data retention* continua ad essere attuata, e proprio la proporzionalità della conservazione generalizzata ed indiscriminata di tutti i metadati pare essere un profilo ancora troppo poco discusso e posto in dubbio.

La mera disapplicazione[70] della disciplina della conservazione e accesso ai metadati, pur da taluni auspicata, non rappresenta uno sviluppo del

[70] Come si è visto nei casi sopra analizzati, infatti, i difensori degli imputati o indagati avevano richiesto ai giudici la disapplicazione della normativa in materia di *data retention* in quanto contrastante con il diritto dell'UE. Anche la dottrina aveva del resto ritenuto percorribile tale via: «Se l'art. 132 Cod. Privacy è contrario agli artt. 7, 8 e 52 CDFUE, esso deve essere disapplicato, come ogni norma che contrasti con il diritto comunitario, secondo gli elementari insegnamenti che governano da decenni i rapporti tra diritto dell'Unione e diritto interno. (…) L'unica risposta possibile, pertanto, è che, finché il legislatore nazionale non interviene ad emendare i profili di contrasto dell'art. 132 Cod. Privacy con il diritto dell'UE, l'attività di *data retention* non dovrebbe essere possibile: altrimenti il vuoto di disciplina – addebitabile allo Stato – gioverebbe allo Stato stesso nelle sue indagini e, viceversa, un diritto fondamentale come quello alla riservatezza dei dati risulterebbe nei fatti tutt'altro che inviolabile», S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, cit., p. 1592. Per Flor «se le norme interne dei singoli Stati, come nel caso italiano, non rispettano gli standard ricavabili dalla sentenza della Corte, esse dovrebbero essere disapplicate dal giudice interno per contrasto con il diritto europeo», R. FLOR, *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, in *Diritto dell'Informazione e dell'Informatica*, 2014, p. 793 e dello stesso avviso anche S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di diritto pubblico comunitario*, 3-4, 2015, p. 819 ss. In questo contesto, alcuni autori si sono anche interrogati su una ulteriore possibile soluzione, sebbene anch'essa non soddisfacente e non totalmente risolutiva delle problematiche evidenziate: potrebbe cioè il singolo operatore delle telecomunicazioni,

tutto soddisfacente [71], costituendo solo una soluzione ai singoli casi concreti sottoposti ai giudici, che lascia sicuramente perplessi e preoccupati per gli effetti che potrebbe provocare sulle indagini in corso e sui procedimenti penali in atto fondati sulla raccolta e analisi dei dati di traffico e telematici; per questo la corretta soluzione alla complessa situazione italiana è dunque certamente da individuarsi in un intervento normativo complessivo [72], che agisca sia sulla disciplina della conservazione quanto su quella dell'accesso e che sia in grado di valutare, con quella discussione ampia e partecipata che ha caratterizzato altri ordinamenti, la possibile inclusione dei criteri individuati dalla giurisprudenza della CGUE. Prendendo utilmente atto delle pronunce delle Corti di altri Stati membri, quali quella francese e belga, il legislatore nostrano dovrebbe così interrogarsi sull'impatto delle pronunce dell'ottobre 2020 e della distinzione in esse promossa tra strumenti di conservazione e accesso impiegati per finalità di sicurezza nazionale e quelli invece adoperati per scopi di repressione di reati gravi, nonché sulla necessità di ripensare la disciplina naziona-

---

nell'inerzia del legislatore, non ritenersi vincolato all'obbligo di conservazione dei metadati? «Posto che il perdurante onere di conservazione dei dati affligge non solo il diritto alla riservatezza, ma ostacola anche la libera circolazione dei servizi (ponendo costi di servizio aggiuntivi agli operatori, gravati della conservazione e delle relative spese) ci si può chiedere se anche il gestore stesso – non remunerato dall'ordinamento per un onere gestionale illegittimo – possa essere interessato a dismettere la conservazione o proseguirla con richiesta di un risarcimento per il danno economico patito», F. GUELLA, *Data retention e circolazione dei livelli di tutela dei diritti in Europa*, cit., p. 356.

[71] «La soluzione della disapplicazione presenta evidentemente i limiti dell'essere un rimedio legato al caso concreto, destinato ad operare *ex post*, quando ormai la violazione dei diritti fondamentali si è verificata», F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?*, cit., p. 4282.

[72] Nel 2019, Marcolini auspicava ed individuava quale possibile soluzione un rinvio alla CGUE da parte della Cassazione, azione da intendersi «nella più ampia prospettiva di "provocare" il legislatore nazionale – l'unico realmente legittimato a riordinare una disciplina dalle ormai troppe incongruenze e slabbrature – il cui intervento non pare più in alcun modo differibile: e il più generale aggiornamento della disciplina nazionale sul trattamento dei dati personali ai contenuti del Reg. 2016/679 potrebbe rappresentare il momento propizio», S. MARCOLINI, *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, cit., p. 1596. Purtroppo tale previsione, come si è visto, non si è realizzata.

le alla luce di quella ormai affermata incompatibilità con la Carta di Nizza di una forma di conservazione generalizzata ed indiscriminata, che sino ad ora non pare essere stata posta adeguatamente in discussione nel contesto italiano.

CONCLUSIONI

Il percorso tratteggiato nelle pagine di questo lavoro induce ad elaborare talune considerazioni che intendono non solo ricondurre a sintesi tutte le tappe del cammino svolto, ma fornire ulteriormente una prospettiva sui successivi passi da intraprendere. Tendere lo sguardo verso il futuro si rende quanto mai necessario dinnanzi alla complessa sfida della *data retention* che, lontana dall'essere giunta ad un punto di arrivo, si presenta tuttora in continuo divenire. Diversi, infatti, sono gli sviluppi attesi tanto sul fronte giurisprudenziale quanto su quello legislativo, sia a livello nazionale sia sovranazionale. Così, partendo da tale consapevole premessa, non può che riconoscersi come la "*great difficulty*" del tema, e cioè la ricerca di quel difficile equilibro tra esigenze securitarie e diritti fondamentali alla riservatezza e alla protezione dei dati che ha sin dalle sue origini caratterizzato la disciplina normativa della conservazione e accesso ai metadati [1], risulti ancora lontana dall'aver trovato una sua stabile risolu-

[1] La sfida è stata ben descritta dall'Avvocato generale Saugmandsgaard Øe nelle sue Conclusioni al caso *Tele2*: egli inizia le sue considerazioni richiamando la nota frase del 1788 di James Madison, uno dei principali autori della Costituzione statunitense: «If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself». La "grande difficoltà" descritta da Madison, nella quale peraltro riecheggia il quesito di Giovenale "*quis custodiet ipsos custodes?",* viene così trasposta dall'Avvocato generale nel contesto specifico della *data retention*: da una parte, i sistemi di conservazione dei metadati consentono al governo di controllare i governati, mentre dall'altra risulta altrettanto fondamentale obbligare il governo a controllare – e limitare – sé stesso. Dinnanzi a tale "*great difficulty*", è compito della Corte e dei giudici del rinvio nonché dei legislatori definire un «punto di equilibrio tra l'obbligo incombente agli Stati membri di garantire la sicurezza delle persone che si trovano sul loro ter-

zione. Ed è per questo che il dibattito nel contesto europeo continua a presentarsi vivace e in evoluzione, nonostante i molteplici interventi chiarificatori della CGUE abbiano fornito importanti principi e requisiti sull'interpretazione dell'art. 15 Direttiva *e-Privacy* alla luce della Carta di Nizza.

Volendo trarre alcune valutazioni conclusive all'oggi dalla lunga ed articolata *data retention saga*, emerge da quest'ultima come i giudici di Lussemburgo, pur dimostrando di non sottovalutare il rilievo della tutela della sicurezza nazionale e pubblica e riconoscendone anzi la «capitale importanza» [2], abbiano al contempo affermato l'importanza dei diritti fondamentali anche dinnanzi a quella tensione pro-securitaria spesso sfociata in una garanzia della sicurezza "a tutti i costi" [3]. Il monito chiaro che

---

ritorio e il rispetto dei diritti fondamentali alla vita privata e alla protezione dei dati di carattere personale sanciti dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE», para. 5.

[2] *Digital Rights Ireland*, para. 42. Nell'esaminato *Parere 1/15* la CGUE riconosce che la «protezione della sicurezza pubblica contribuisce altresì alla tutela dei diritti e delle libertà altrui», para. 149.

[3] Questa posizione è chiaramente espressa dalle efficaci parole dell'Avvocato generale Campos Sanchez-Bordona nelle Conclusioni al rinvio *La Quadrature du Net*: «la lotta al terrorismo è, letteralmente, vitale per lo Stato e il suo successo costituisce un obiettivo di interesse generale irrinunciabile per uno Stato di diritto (…). Di fronte a tale valutazione mi sembra pertinente rilevare che la lotta contro il terrorismo 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. (…) Certamente, la soluzione più pratica ed efficace sarebbe la conservazione generale e indifferenziata di tutti i dati che possono essere raccolti dai fornitori di servizi di comunicazione elettronica, ma ho già rilevato che la questione non può essere risolta in termini di efficacia pratica, bensì di *efficacia giuridica*, e nel contesto di uno Stato di diritto», para. 129-135, enfasi aggiunta.

ne è derivato è quello di una dichiarazione del carattere non recessivo dei diritti e delle libertà neppure di fronte alle esigenze securitarie e alle ampie potenzialità delle nuove tecnologie, che trova evidente esternazione nella rigida attuazione dei principi di proporzionalità e necessità effettuata con grande rigore dalla CGUE. È proprio da questo vaglio che l'orientamento dei giudici europei ha assunto contorni sempre più chiari: da un lato non è stata negata *in toto* la legittimità dell'adozione di sistemi di conservazione generalizzata ed indiscriminata di metadati, ritenuti proporzionati e giustificati laddove finalizzati a contrastare una reale minaccia per la sicurezza nazionale; dall'altro lato, per scopi di garanzia della sicurezza pubblica e dunque di repressione dei reati gravi l'unica forma di conservazione limitata a quanto strettamente necessario è stata invece identificata nella discussa conservazione mirata. Questa lettura, determinatasi con maggior decisione nelle più recenti pronunce *La Quadrature du Net* e *Privacy International*, ha certamente confermato la capacità dei giudici di Lussemburgo «di essere rigorosi nella tutela dei diritti su uno dei terreni più spinosi, dato che la gravità della situazione internazionale tende ad attutire la sensibilità verso i diritti dei sospetti terroristi e genera una maggiore propensione verso le esigenze della sicurezza piuttosto che verso quelle della giustizia e della libertà» [4].

La riassuntiva ricostruzione della giurisprudenza della CGUE proposta in queste pagine deve, tuttavia, tenere in debito conto di come l'operato dei giudici europei si sia dovuto inserire entro la peculiare architettura dell'UE, caratterizzata da quel complesso riparto di competenze tra livello sovranazionale e Stati membri che diviene ancor più delicato in ambiti di azione, quale quello della garanzia della sicurezza, che i Governi nazionali sono da sempre restii a cedere alle Istituzioni europee [5]. In que-

---

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

[5] Le posizioni degli Stati membri intervenuti nei procedimenti dinnanzi alla CGUE, il chiaro riferimento dell'*Invstigatory Powers Tribunal* nel rinvio *Privacy International* a quanto disposto dall'art. 4, co. 2, TUE, nonché talune delle disposizioni inserite nella bozza del nuovo Regolamento *e-Privacy*, fanno emergere con estrema chiarezza il tentativo di escludere dall'ambito di applicazione del diritto dell'UE – e dunque dalla rigida applicazione dei principi di proporzionalità e necessità emersa dalla giurisprudenza della

sto contesto i giudici di Lussemburgo hanno determinato, nella materia di cui trattasi, un'interpretazione estensiva dell'ambito di applicazione del diritto dell'UE, riconducendo a quest'ultimo tutte le attività che implichino un trattamento dei dati da parte di soggetti privati – in questo caso fornitori di servizi di telecomunicazione –. In tal modo è risultata contestualmente estesa la garanzia fornita dalla Carta di Nizza [6], così da scongiurare il rischio che il semplice richiamo a finalità di tutela della sicurezza, anche nazionale, divenga grimaldello per scardinare le porte di quella "*fortress of digital privacy*" [7] faticosamente e meticolosamente eretta dal legislatore europeo, ma soprattutto dalla giurisprudenza della CGUE [8].

Ponendosi quali «*ultimate protector of constitutional rights in Europe*» [9], i giudici di Lussemburgo hanno quindi indubbiamente incentivato un innalzamento del livello di tutela dei diritti alla riservatezza e alla prote-

---

CGUE – tutte le discipline e gli strumenti finalizzati alla garanzia della sicurezza nazionale.

[6] La CGUE si è così posta quale «guardiano delle libertà» (G. DE MINICO, *La risposta europea al terrorismo del tempo ordinario: il lawmaker e il giudice*, in *Osservatorio sulle fonti*, 2, 2017, p. 17) e dei diritti della Carta di Nizza, «[providing] the grounds to confirm and steadily expand the scope of application of EU fundamental rights to the Member States and thereby the jurisdiction of the CJEU itself for the interpretation of those rights», A. TORREZ PEREZ, *The federalizing force of the EU Charter of Fundamental Rights*, in *International journal of constitutional law*, 4, 2017, p. 1081.

[7] L.P. VANONI, *Balancing privacy and national security in the global digital era: a comparative perspective of the EU and US constitutional systems*¸ in L. VIOLINI, A. BARAGGIA (a cura di), *The fragmented landscape of fundamental rights protection in Europe: the role of judicial and non-judicial actors*, Elgar Publishing, Cheltenham, 2018, p. 114 ss.

[8] Le tappe fondamentali del percorso che ha portato ad un solido riconoscimento dei diritti alla riservatezza e alla protezione dei dati sono certamente da ravvedersi nella previsione degli artt. 7 e 8 della Carta di Nizza e nell'art. 16 TFUE, poi rafforzati dalla vasta e rilevante giurisprudenza della CGUE in materia; questa, oltre che dalle storiche pronunce della *data retention saga*, risulta composta da ulteriori pronunce tra le quali non può che citarsi la sentenza 13 maggio 2014, C-131/12, *Google Spain SL e Google Inc. v. Agencia Espanola de Proteccion de Dator (AEPD) e al.*, nella quale ha trovato riconoscimento il c.d. *diritto all'oblio* (sul punto, *ex multis*, si legga G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, Roma, 2015).

[9] D. FENNELLY, *Data retention: the life, death and afterlife of a directive,* in *ERA Paper*, 2018, p. 19.

zione dei dati, come peraltro chiaramente emerso dall'analisi comparata svolta in questo lavoro: Belgio e Regno Unito, pur seguendo percorsi differenti, sono stati testimoni dell'inserimento lento ma costante di rigide garanzie e salvaguardie, tanto nella fase di conservazione quanto in quella successiva dell'accesso ai metadati. La predisposizione di un obbligo di conservazione legato esclusivamente all'adozione di una *retention notice* da parte del *Secretary of State* e il relativo sistema di *double lock* per vagliarne il carattere necessario alla finalità perseguita, la creazione di organi *ad hoc* deputati al controllo di legittimità dell'accesso ai metadati da parte delle autorità pubbliche nonché l'introduzione di un elenco di reati gravi per i quali l'accesso stesso è consentito, sono tutti segnali dello sforzo compiuto da legislatore e Corti inglesi allo scopo di limitare l'ingerenza nella sfera privata provocata dallo strumento della *data retention,* accompagnandolo con disposizioni sempre più chiare e precise, volte a delimitarne i confini applicativi. Stesso risultato finale, sebbene mediante differenti soluzioni regolatorie, è ravvisabile anche in Belgio, dove la normativa del 2016, recentemente invalidata, già introduceva una differenziazione dei tempi di conservazione a seconda della tipologia di dati considerati, dei soggetti coinvolti – ad esempio particolari tutele erano previste per i soggetti sottoposti a segreto professionale – e delle finalità perseguite, prestando poi attenzione a definire una soglia di gravità dei reati per i quali l'accesso veniva consentito. In Italia la giurisprudenza della CGUE ha invece iniziato solo in tempi recentissimi ad essere presa in seria considerazione: le sentenze dei giudici di Lussemburgo, in particolare *H.K. c. Prokuratuur*, si sono rivelate base fondante non solo del primo rinvio pregiudiziale in materia di *data retention*, promosso nel maggio 2021 [10], ma anche del formale impegno assunto dal Governo a promuovere un ripensamento della disciplina vigente; questi sviluppi, pur non essendosi ancora concretizzati in alcuna riforma normativa – diversamente da quanto osservato appunto in Belgio e Regno Unito –, rappresentano sicuramente i primi – per quanto incerti – segnali di un tardivo risveglio da parte dei giudici e del Governo italiani, preludendo quantomeno ad

[10] Ci si riferisce alla domanda di pronuncia pregiudiziale promossa con ordinanza del 4 maggio 2021 dal Tribunale di Rieti nel procedimento penale a carico di G.B. e R.H. (causa C-334/21 dinnanzi alla CGUE), ampiamente esaminata nel Capitolo 6, para. 3.1.

una valutazione più attenta e consapevole dei principi e requisiti stabiliti dalla giurisprudenza sovranazionale.

Dinnanzi all'inerzia del legislatore europeo, la CGUE ha saputo dunque provocare negli ordinamenti nazionali, seppur in misura e con esiti differenti, una significativa attenuazione di quella deriva pro-securitaria che vedeva nell'adozione di sistemi di conservazione generalizzata di metadati un insostituibile strumento di contrasto alle minacce alla sicurezza.

Nonostante questo indubbio effetto positivo, l'approccio garantista tenuto dai giudici di Lussemburgo non ha però mancato di rivelare i propri limiti e criticità: legislatori e Corti nazionali hanno dovuto affrontare profonde criticità applicative e persistenti dubbi interpretativi relativi ai principi affermati dalla giurisprudenza sovranazionale, di cui peraltro i continui rinvii pregiudiziali alla CGUE sono chiara esternazione. Gli interrogativi quanto ai requisiti indicati nelle sentenze dell'ottobre 2020[11], insieme alla perdurante difficoltà di porre in essere forme di conservazione mirata, che ha sollevato quesiti quanto alla sua concreta realizzabilità ed utilità nonché alla sua conformità al principio di non discriminazione, si accompagnano alla vaghezza di taluni criteri indicati dalla CGUE, quali il concetto di "gravità" del reato. In questi profili problematici non possono che ravvisarsi le difficoltà dell'«attività costruttiva» dei giudici di

[11] La distinzione tra sicurezza nazionale e pubblica non è stata certo esente da critiche. Accanto alla difficoltà di determinare con precisione il significato dei criteri e requisiti indicati dai giudici di Lussemburgo nella sentenza *La Quadrature du Net* con riferimento alla possibile adozione di forme di *bulk data retention* – cosa debba intendersi, ad esempio, per minaccia grave, reale, attuale o prevedibile per la sicurezza nazionale –, un ulteriore pericolo è stato rilevato, sin da prima delle sentenze dell'ottobre 2020, da Verbruggen, Royer e Severijns: questi hanno sottolineato come «an EU-law taboo on a general data retention will also increase the dependence of intelligence agencies, especially those of small countries like Belgium, on information of foreign services that might not (or no longer) be bound by EU law or choose not to abide by it, for instance US, post-Brexit-UK or Israeli services which are important partners in the fight against terrorism and the so-called foreign fighters. Again, even if the human rights and accountability concerns behind the outright banning of blanket data retention are sincere, the remedy might be worse than the illness», F. VERBRUGGEN, S. ROYER, H. SEVERIJNS, *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, in *European Law Blog,* 1 ottobre 2018, http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-dataretention-taboo-for-human-rights-sake/.

Lussemburgo che, pur con dirompenti ed inedite pronunce, scontano il limite di doversi attenere al *petitum* e ai confini comunque dettati dal riparto di competenze tra Stati membri e UE [12]. Proprio l'analisi comparata svolta nelle pagine di questo lavoro contribuisce a fornire una fotografia nitida di tali criticità, capaci di ripercuotersi in maniera evidente nel contesto nazionale: accanto infatti al già rilevato impatto positivo della giurisprudenza della CGUE, riscontrato nelle convergenti reazioni di Regno Unito e nel Belgio, lo studio degli ordinamenti selezionati ha posto in evidenza anche significative divergenze, che hanno condotto a disomogenee soluzioni normative e giurisprudenziali, risultanti così in punti di equilibrio tra esigenze securitarie e salvaguardie dei diritti alla riservatezza e alla protezione dei dati differentemente individuati.

Utile è divenuta a tal fine la ricostruzione del percorso che ha caratte-

[12] Nelle sentenze della CGUE, tanto in quelle sulla *data retention saga* quanto in quelle attinenti al trasferimento dati verso Stati terzi, è impossibile non ravvisare uno spiccato approccio para-legislativo del giudice di Lussemburgo, «che esalta la dimensione costruttiva dell'attività del giudice, laddove non si limita ad invalidare (o censurare) le norme che è chiamato a vagliare, ma nell'intento di concretizzare principi espressi dalla pregressa giurisprudenza tenda a riscriverne di nuove, anche con il piglio tipico del comitato di tecnica legislativa», A. VEDASCHI, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione Europea*, in *Giurisprudenza Costituzionale*, 4, 2017, p. 1925. E del resto questa funzione si è resa necessaria proprio a causa del perdurante mancato intervento del legislatore sovranazionale che, a seguito della invalidazione della DRD, non è più intervenuto in materia di *data retention* con una normativa *ad hoc*, così spingendo la CGUE a «compiere sforzi ulteriori, valorizzando il patrimonio della Carta», M. BASSINI, *La Corte di giustizia e la conservazione dei dati. Spunti di una rilettura 'postuma'*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, Napoli, 2021, p. 131. Nonostante queste corrette riflessioni, anche le pronunce dell'ottobre 2020 hanno chiaramente posto in luce i limiti di questo approccio: le condizioni e salvaguardie che devono essere predisposte al fine di imporre una conservazione generalizzata che sia realmente proporzionata e limitata a quanto necessario, così come le circostanze che sono tali da giustificare l'adozione di una più invasiva forma di *data retention*, sono indicate – necessariamente – in termini estremamente vaghi e ampi e lasciate alla determinazione dei legislatori nazionali. Questo apre inevitabilmente ad incertezze e possibili disomogeneità attuative, peraltro già confermate dalle diversità di reazioni espresse dal *Conseil d'État* francese e della *Cour Constitutionnelle* belga a seguito della pronuncia *La Quadrature du Net.*

rizzato lo sviluppo e l'evoluzione della disciplina della *data retention* nei tre Stati considerati per ravvisare le diversità e le peculiarità di ciascun ordinamento. Con riferimento al Regno Unito, ad esempio, l'approvazione di una nuova normativa in materia di conservazione dei metadati proprio nelle more della decisione *Tele2* – peraltro derivante da un rinvio pregiudiziale promosso dagli stessi giudici d'Oltremanica – ha mostrato senza dubbio un iniziale atteggiamento del legislatore inglese di "autonomia", se non di voluta "lontananza", rispetto a quelle che sarebbero state le posizioni finali espresse dai giudici europei. Le modifiche normative in tale delicato ambito si sono del resto susseguite nel Regno Unito ad un ritmo estremamente rapido, in maniera a tratti confusa e caratterizzata sovente da problematiche sovrapposizioni tra interventi legislativi e giurisprudenziali, non sempre coordinati e coerenti tra loro. Il legislatore così è stato più volte chiamato ad apportare modifiche sostanziali alla normativa vigente, talvolta anche solo poco tempo dopo la sua adozione: tali interventi si rendevano necessari alla luce delle pronunce dei giudici nazionali che ravvisavano la non conformità della disciplina interna rispetto ai principi stabiliti nella giurisprudenza della CGUE. Nonostante quindi, come prima sottolineato, le ultime riforme, soprattutto quelle introdotte nel 2018 con il *Data Retention and Acquisition Regulation,* abbiano manifestato una maggiore attenzione del legislatore inglese verso la previsione di più robuste salvaguardie e garanzie dei diritti fondamentali, è da rilevarsi come il percorso articolato e non privo di ostacoli sopra descritto sia comunque risultato in una conferma della possibilità di addivenire a *retention notice* di carattere generalizzato o dalla ampia estensione, nonché nella predisposizione di forme di acquisizione generalizzata di metadati da parte di autorità di intelligence – pure ad oggi al vaglio dell'*Investigatory Powers Tribunal* –. Ciò a dimostrazione di come una certa distanza rispetto ai requisiti sanciti dalla CGUE sia ancora ravvisabile nella disciplina inglese.

Il Belgio, diversamente dal Regno Unito, ha invece seguito un percorso lineare e maggiormente garantista, introducendo ben prima del legislatore d'Oltremanica solide condizioni e limitazioni al sistema di conservazione dei metadati, pur mantenendo, almeno sino ai più recenti sviluppi, una *data retention* generalizzata ed indiscriminata anche laddove finalizzata alla tutela della sicurezza pubblica. La linearità del percorso evolutivo

della normativa belga in materia di conservazione dei metadati è da ravvisarsi nel ripetersi di uno schema ordinato e consequenziale: la Corte costituzionale nazionale, quale effetto delle pronunce della CGUE, veniva chiamata a pronunciarsi sulla conformità al diritto dell'UE della disciplina all'epoca vigente e solo a seguito della posizione espressa dai giudici costituzionali si sviluppava il dibattito legislativo finalizzato all'adozione di una nuova regolamentazione della materia. Sul fronte giurisprudenziale, poi, i rinvii pregiudiziali promossi dalla *Cour constitutionnelle* con riferimento sia alla disciplina della *data retention* – rinvio sfociato nella pronuncia *La Quadrature du Net* –, sia a quella in materia di raccolta e trattamento di PNR per scopi securitari, evidenziano una grande attenzione ed un approfondito studio da parte dei giudici belgi della *case law* della CGUE nonché dei dubbi interpretativi da essa derivanti; in tal modo la Corte costituzionale ha dimostrato di sapersi smarcare dall'iniziale approccio più ossequioso verso la giurisprudenza europea, promuovendo così un dialogo con i giudici di Lussemburgo volto mettere in luce anche i profili problematici e le criticità applicative emerse.

Fortemente differente rispetto al percorso seguito dai due Stati sin qui analizzati, è infine l'evoluzione normativa e giurisprudenziale in Italia. Le Corti nazionali, innanzitutto, hanno sempre – piuttosto rapidamente e talvolta superficialmente – ritenuto la normativa nazionale conforme al diritto dell'UE, considerando peraltro inutile – se non solo in tempi recentissimi – provvedere ad un rinvio pregiudiziale innanzi alla CGUE. Certamente è importante evidenziare come nel nostro ordinamento non esistano forme di ricorso diretto di annullamento alla Corte costituzionale, come in Belgio, o specifiche Corti *ad hoc* deputate a dirimere controversie aventi ad oggetto sistemi di sorveglianza, come avviene nel Regno Unito, che rappresentano indubbiamente istituti e istituzioni in grado entrambi di facilitare ONG e cittadini a richiedere ed ottenere l'intervento dei giudici; è altrettanto vero però che anche nel contesto italiano si sono presentate, nel corso degli anni, molteplici occasioni nelle quali i giudici avrebbero ben avuto modo di valutare approfonditamente la conformità della disciplina in materia di *data retention* rispetto al diritto dell'UE e ai diritti riconosciuti anche nella Costituzione italiana [13]. La Corte

[13] Si fa riferimento ai procedimenti penali, giunti talvolta anche dinnanzi alla Corte

di Cassazione, dinnanzi a tali possibilità, si è invece sempre sottratta ad un'analisi attenta e problematizzata della disciplina della conservazione e accesso ai metadati, «fatica[ndo] nel dare il giusto peso alle questioni poste» [14]. Ciò appare del tutto singolare se si pensa ai molteplici rinvii pregiudiziali promossi nei medesimi anni dai giudici di molti altri Stati europei, che hanno dimostrato dunque di saper cogliere la complessità della materia e del portato della giurisprudenza della CGUE. Neppure il legislatore italiano, poi, ha dimostrato di sapersi – o volersi – interrogare quanto all'incidenza della giurisprudenza europea rispetto all'assetto normativo interno, intervenendo con singole e spesso confuse disposizioni di natura emergenziale e temporanea nonché con continue proroghe e discipline derogatorie che hanno infine portato alla determinazione di una conservazione della durata di settantadue mesi per talune tipologie di reati quali il terrorismo, mentre per tutti i restanti reati la *data retention* resta regolata dall'art. 132 Codice Privacy. Non potendo previamente conoscere per quali reati verrà richiesto l'accesso, però, i fornitori di servizi di telecomunicazioni sui quali incombe l'obbligo di conservazione si trovano necessariamente a dover memorizzare i metadati per l'intera durata massima di sei anni, con l'effetto che la conservazione risulta *de facto* estremamente lunga, con una scelta che non trova eguali nel panorama europeo e neppure presenta una giustificazione specifica o chiaramente motivata da parte del legislatore stesso. Diversamente da quanto si è visto nella normativa inglese e belga, inoltre, nella disciplina italiana risulta totalmente assente la previsione di una limitazione della possibilità di accesso per il solo perseguimento di reati di carattere grave [15].

---

di Cassazione e analizzati nel Capitolo 6, para. 2, nei quali i difensori degli imputati hanno più volte sollevato quesiti attinenti alla compatibilità della normativa italiana in materia di *data retention* con la Carta di Nizza, talvolta richiedendo in subordine la proposizione di un rinvio pregiudiziale alla CGUE.

[14] I. REZENDE, *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention*,* in *Sistema Penale*, 5, 2020, p. 185.

[15] L'analisi comparata delle diverse soluzioni e reazioni registratesi in differenti Stati rivela in maniera ancor più evidente la sua importanza ed utilità con riferimento all'Italia, nella quale, come si è visto, l'affermarsi di un dibattito serio e consapevole sulla portata delle pronunce della CGUE ha conosciuto significative difficoltà e resistenze. Se infatti «il diritto comparato può essere usato strumentalmente per illuminare la conoscenza di un di-

Dinnanzi ad una tale ricostruzione e alle osservazioni promosse, che mettono in luce divergenze di reazioni e approcci, emerge quindi con evidenza il perdurare, nel territorio europeo, di un panorama frammentario ed instabile, in continua evoluzione: in Belgio, infatti, le prossime mosse del legislatore nazionale si riveleranno determinanti per comprendere se, a seguito del deciso intervento della Corte costituzionale, si registrerà un definitivo abbandono della *bulk data retention* per scopi di sicurezza pubblica a favore di un'inedita forma di conservazione mirata; questa dovrà individuare criteri soggettivi e geografici in grado di non risultare in forme discriminatorie, mentre altrettanto sfidante sarà la delimitazione delle condizioni per le quali una conservazione generalizzata potrà essere adottata in caso di minacce alla sicurezza nazionale.

Il Regno Unito, ormai Stato terzo rispetto all'UE, risulta oggi vincolato – nel contesto europeo – al solo rispetto della Convenzione EDU e dei più flessibili e meno stringenti requisiti e parametri di proporzionalità fissati dai giudici di Strasburgo nelle pronunce in materia di sistemi di sorveglianza e controllo dei dati per scopi securitari. Pur avendo interesse a mantenere un livello di garanzia dei diritti fondamentali sostanzialmente equivalente a quello sancito entro i confini europei, da ciò dipendendo la continuità e stabilità del flusso di dati provenienti dall'UE, la direzione che i futuri interventi normativi del legislatore inglese intenderanno intraprendere è ancora difficile da prevedere. Particolare attenzione dovrà allora essere dedicata agli attesi effetti della sentenza *Privacy International*, rispetto alla quale l'*Investigatory Powers Tribunal* deve ancora compiutamente pronunciarsi: sarà questa un'occasione importante per iniziare a riflettere sugli sviluppi della *data retention* nell'era *post-Brexit* e sulla convergenza o meno delle decisioni giurisprudenziali e degli interventi nor-

---

ritto nazionale», contribuendo così a fornire una maggiore «comprensione di sé stessi» (L. PEGORARO, A. RINELLA, *Sistemi costituzionali comparati*, Giappichelli, Torino, 2017, p. 33), lo studio delle scelte e delle considerazioni svolte da legislatori e Corti di altri ordinamenti rappresenta senza dubbio un efficace spunto di riflessione nel contesto italiano e in special modo per i diversi attori nazionali chiamati a confrontarsi con la disciplina della *data retention*, con l'auspicio che anche l'appello del Presidente dell'Autorità garante per la protezione dei dati personali del 3 agosto 2021, richiamato nel Capitolo 6 (v. para. 3.2.), possa condurre ad una discussione approfondita sul futuro della conservazione dei metadati in Italia.

mativi Oltremanica rispetto ai principi e criteri affermati dalla CGUE.

Maggiormente incerta, infine, si presenta la situazione italiana, rispetto alla quale dovranno attendersi tanto la risposta della CGUE al rinvio pregiudiziale promosso, quanto l'intervento del Governo e/o del legislatore.

Sul fronte degli ordinamenti nazionali, pertanto, la situazione appare tuttora estremamente articolata, mostrando difformità di soluzioni che difficilmente si potranno tradurre in tempi rapidi in un percorso convergente e di sintesi.

Le persistenti incertezze e difficoltà applicative dei requisiti e principi stabiliti dalla giurisprudenza della CGUE, nonché la sfida di individuare un corretto contemperamento tra esigenze securitarie e diritti fondamentali non sono però emerse solo nella dimensione interna all'UE, bensì hanno caratterizzato anche la dimensione esterna ai confini europei e, in particolare, la disciplina del trasferimento dati verso Stati terzi. In tale ambito, infatti, l'efficacia dello strumento dell'adeguatezza e la correttezza delle valutazioni svolte dalla Commissione sono state più volte contrastate dalla CGUE sia nella *Schrems saga*, sia nel *Parere 1/15*: in queste decisioni il livello di garanzia dei diritti alla riservatezza e alla protezione dei dati stabilito a seguito delle negoziazioni e degli accordi con USA e Canada è stato ritenuto dai giudici di Lussemburgo non sostanzialmente equivalente a quello assicurato nell'UE. Così facendo sono stati posti in particolare evidenza i limiti e la debolezza del concetto stesso di adeguatezza e degli ulteriori strumenti di *data transfer* disposti dalla normativa europea: il rischio concreto è che le condizioni di trasferimento dati contrattate con Stati terzi possano tradursi in un "compromesso al ribasso" a scapito di una solida tutela dei diritti e a favore invece di una salvaguardia degli interessi economici e politici legati alla garanzia di un continuo e sicuro flusso di dati [16].

[16] «Such agreements, far from strengthening privacy protection, would almost certainly weaken it. Even among Western democracies, the search for transnational common ground and the institutional priorities of the negotiators would be inimical to a privacy-protective accord», S.J. SCHULHOFER, *An international right to privacy? Be careful what you wish for*, in *International Journal of Constitutional Law*, 1, 2016, p. 238. Ciò induce l'autore a chiedersi, in ultima analisi, se quella di una negoziazione tra UE e Stati terzi per il raggiungimento di accordi in materia di protezione dei dati e di tutela della privacy sia una soluzione, alla luce delle vicende giudiziarie europee, ancora per-

Di fronte a tali criticità e pericoli, tuttavia, non può non rilevarsi come attraverso le discusse negoziazioni con Stati terzi le Istituzioni dell'UE abbiano prodotto innegabili ripercussioni positive: è stato proprio sfruttando l'ormai imprescindibile ed irrinunciabile *data flow* che l'UE è riuscita a farsi promotrice di un più elevato standard di tutela dei diritti fondamentali alla riservatezza e alla protezione dei dati, dimostrando peraltro di comprendere come in un mondo globalizzato e "datizzato", che impone di trascendere i classici concetti di territorialità e sovranità territoriale, una concreta salvaguardia dei dati prodotti e riguardanti i cittadini europei non possa che realizzarsi in una forma di garanzia capace di andare oltre i confini dell'UE stessa[17]. Rispondendo quindi a quel "principio missionario" (art. 3, co. 5, TUE) di espansione ed esportazione dei propri valori e principi, l'Unione ha incoraggiato il raggiungimento di una convergenza regolatoria che, per quanto discussa[18] e lontana dall'essere pienamente raggiunta, ha certamente il pregio di favorire l'affermarsi di maggiori tutele e di una più marcata attenzione alla *data protection* e alla riservatezza negli Stati terzi destinatari del flusso di dati, anche qualo-

---

corribile ed idonea alla realizzazione del reale obiettivo ultimo della adeguatezza delle garanzie offerte dallo Stato terzo.

[17] Per Cole e Fabbrini, la sentenza *Schrems* ha avuto il merito di rendere «the case for a comprehensive transatlantic privacy compact all the more compelling», D. COLE, F. FABBRINI, *Bridging the transatlantic divide? The United States, The European Union and the protection of privacy across borders*, in *International Journal of Constitutional Law,* 1, 2016, p. 236. Similmente, anche G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA-UE,* in V. ZENO-ZENCOVICH-, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, p. 3 ss. Nello stesso volume, si rimanda a V. ZENO-ZENCOVICH, *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di comunicazione*, p. 7 ss. per interessanti riflessioni sul concetto di "sovranità digitale" e a-territorialità delle telecomunicazioni.

[18] Si rinvia a quelle considerazioni critiche, già evidenziate nel Capitolo 3, che scorgono nello strumento della decisione di adeguatezza una forma moderna di "imperialismo normativo" (M. LEFFI, *I trasferimenti di dati terzi nel nuovo Regolamento UE*, in *Rivista di Diritti Comparati*, 2, 2017, p. 203), nell'"esaltante illusione" dell'UE di poter imporre con effettiva efficacia anche nella dimensione esterna gli standard di tutela sanciti entro i propri confini (C. KUNER, *Reality and illusion in EU data transfer regulation post Schrems*, in *German Law Journal*, 4, 2017, p. 898).

ra le operazioni di raccolta e trattamento siano svolte da autorità pubbliche per finalità securitarie [19].

L'azione dell'UE nella dimensione esterna, pur risultando dunque caratterizzata da criticità e deviazioni negative, si presenta al contempo portatrice di effetti positivi; tale rilevata complessità, che rende difficile trarre un bilancio netto e definitivo sulla efficacia dello strumento dell'adeguatezza e sulla sua interpretazione da parte della CGUE, viene accresciuta dal forte intreccio con le vicende interne ai confini europei: nelle negoziazioni in corso, così come in quelle future, le Istituzioni europee debbono necessariamente considerare i principi fissati dalla giurisprudenza della CGUE anche in materia di *data retention* per scongiurare un atteggiamento ipocrita [20] che potrebbe concretizzarsi nella determinazione di standard di tutela stringenti per il flusso di dati verso Stati terzi che non risultano poi però essere efficacemente e concretamente garantiti nel contesto interno europeo. Indicativi di un simile rischio sono del resto i numerosi rinvii pendenti attinenti alla conformità della Direttiva UE 2016/681 in materia di PNR alla Carta di Nizza: tali quesiti pregiudiziali sono stati promossi proprio a seguito del *Parere 1/15* che, pur riguardan-

---

[19] In risposta alla visione di Schulhofer, sopra richiamata nella nota 16, Cole e Fabbrini hanno chiaramente ritenuto come «transatlantic negotiations are necessary to protect transatlantic rights. The concerns Schulhofer raises, while sound, are not a reason to reject such negotiations. Some of the concerns he has at the transatlantic level are equally present at the domestic level, and Schulhofer has not shown that the dynamics he predicts (a race to the bottom, or the watering down of domestic standards to meet transnational standards) are inevitable. Most importantly, because current domestic law in both the EU and the US provides no meaningful protection to foreign nationals from crossborder surveillance, and safeguards are unlikely to expand unilaterally on this front in the future, there is little or no downside, and considerable upside, to a transatlantic effort to address this concern», D. COLE, F. FABBRINI, *Transatlantic Negotiations for Transatlantic Rights: Why an EU-US Agreement is the Best Option for Protecting Privacy Against Crossborder Surveillance*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, Londra, 2017, p. 212.

[20] In questi termini, come ampiamente visto nelle pagine di questo lavoro, si è pronunciato C. KUNER, *Reality and illusion in EU data transfer regulation post Schrems*, cit., p. 898, ma anche I. BROWN, D. KORFF, *Exchanges of personal data after the Schrems II judgement*, PE 694.678, luglio 2021, p. 32.

do la dimensione esterna, ha finito col fissare requisiti e principi quanto alla raccolta e trattamento di PNR tali da far sorgere dubbi sulla proporzionalità della disciplina interna all'UE stessa. Nei casi pendenti, nonché in quelli futuri che potrà essere chiamata a decidere [21], anche la CGUE, che con le sue pronunce in materia di *data transfer* si è posta quale «main defender of the fundamental right to data privacy in EU and transatlantic relations» [22], dovrà quindi necessariamente fronteggiare il pericolo di una deriva "ipocrita", oltre a dover prestare attenzione all'altrettanto insidioso rischio di proporre una lettura talmente rigida del criterio di adeguatezza da impedire *de facto* il concreto raggiungimento di accordi con Stati terzi, provocando dannose situazioni di stallo [23]. Non può che ravvisarsi, in

[21] Oltre ai rinvii pendenti aventi ad oggetto la disciplina europea in materia di raccolta e trattamento dei PNR, la CGUE potrebbe, come da molti pronosticato, essere ben presto chiamata a pronunciarsi sulla validità e conformità alla Carta di Nizza della decisione di adeguatezza riguardante il trasferimento dati verso il Regno Unito, adottata dalla Commissione il 28 giugno 2021 (sul punto, E. CELESTE, *Cross-border data protection after Brexit*, in *Brexit Institute Working Paper Series*, 4, 2021, in particolare p. 13).

[22] M. ZALNIERIUTE, *Developing a European standard for international data transfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *Modern Law Review*, 6, 2018, p. 1056. La delicata questione della "extra-territorialità" delle tutele offerte dalla CGUE con riferimento ai diritti alla riservatezza e protezione dei dati è peraltro emersa – seppure con diverse sfumature – in ulteriori pronunce riguardanti ambiti differenti da quello attinente alla decisione di adeguatezza oggetto di approfondimento nelle pagine di questo lavoro: ci si riferisce alle pronunce 24 settembre 2019, C-507/17, *Google LLC c. CNIL* e 3 ottobre 2019, C-18/18, *Glawischnig-Piesczek c. Facebook* (per una ricostruzione di tali rilevanti decisioni, si rimanda rispettivamente a J. QUINN, *Google v. CNIL: circumscribing the extraterritorial effect*, in F. FABBRINI, E. CELESTE, J. QUINN (a cura di), *Data protection beyond borders: transatlantic perspectives on extraterritoriality and sovereignity*, Hart, Oxford, 2021, p. 47 ss. e nello stesso volume O. POLLICINO, *Data protection and freedom of expression beyond EU borders: EU judicial perspectives*, p. 81 ss).

[23] Si pensi al fatto che, in assenza di un accordo in materia di trasferimento di PNR, i vettori aerei diretti verso il Canada sono comunque tenuti ad inviare alle autorità pubbliche canadesi i dati riguardanti i passeggeri europei; il trattamento di tali dati è regolato da un *Committment* elaborato dalla *Border Service Agency* canadese ed allegato al primo accordo in materia di trasferimento di PNR con l'UE (Decisione 2006/253/CE) che prevede un livello di tutela dei dati e della riservatezza di gran lunga inferiore a quello stabilito dalla bozza di accordo UE-Canada "respinta" dalla CGUE. Non stupisce dunque come dinnanzi a tali criticità e proprio per ovviare a simili situazioni, alcuni au-

questi profili problematici, una forte similitudine con quanto già rilevato in materia di conservazione dei metadati, rispetto alla quale i principi stabiliti dalla CGUE si scontrano con le difficoltà attuative ed i dubbi interpretativi rilevati dal legislatore, tanto europeo quanto nazionale.

Ecco allora che, riconducendo ad unità tutte le considerazioni conclusive sin qui avanzate, è possibile comprendere come il punto di equilibrio tra esigenze securitarie e tutela dei diritti fondamentali nel complesso caso della *data retention* si presenti ancora oggi in continuo movimento, suscettibile di oscillare in direzioni differenti sotto il peso delle spinte degli eventi storico-politici nonché del progresso tecnico-scientifico. Osservare con attenzione i futuri sviluppi diviene pertanto un esercizio essenziale quanto sfidante: i fronti ancora aperti sono infatti molteplici e tutti strettamente interrelati, andando dai rinvii tuttora pendenti dinnanzi ai giudici di Lussemburgo, alle negoziazioni in corso con Stati terzi volte a stabilire modalità legittime di trasferimento dei dati oltre i confini dell'UE, dall'atteso intervento del legislatore europeo sino alle reazioni e soluzioni – normative e giurisprudenziali – che ciascuno Stato membro vorrà elaborare nei prossimi anni. Le prime disomogenee risposte di Francia e Belgio alle determinanti sentenze della CGUE *Privacy International* e la *Quadrature du Net* hanno già rivelato però «a persisting tension between the practices of national law enforcement authorities, the reluctance of

---

tori abbiano sottolineato l'esigenza di promuovere una soluzione a livello globale, nella forma cioè di un trattato internazionale multilaterale che fissi standard di protezione non solo tra due singole parti – come avviene mediante lo strumento della decisione di adeguatezza europeo – ma in grado di coinvolgere gran parte della comunità internazionale. Di questo avviso S. MITSILEGAS, *Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime*, in *Columbia Human Rights Law Review*, 3, 2016, p. 1 ss. e K. LACHMAYER, *Rethinking Privacy Across Borders: Developing Transnational Rights on Data Privacy*, in *Tilburg Law Review*, 20, 2015, p. 7 ss. Da tale prospettiva, allora, la disciplina europea in materia di *data transfer* e le decisioni di adeguatezza in particolare potrebbero essere viste come uno strumento per «rafforzare la leadership dell'Unione nell'intento di definire le future linee globali in materia di protezione dei dati, piuttosto che una reale garanzia di un più elevato ed efficace livello di protezione dei dati trasferiti verso Paesi terzi», A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, RomaTrE-Press, Roma, 2016, p. 268.

national legislators to deprive their police bodies of useful and effective tools to tackle crimes, and the principled approach of the CJUE that has so far pushed towards a more proportionate balancing between national security and data protection. The frequency with which cases in this area are emerging witnesses that the data retention question in Europe is far from settled and that much still needs to be done in order to put national law enforcement practices in line with EU fundamental rights» [24].

Dinnanzi a tali tensioni e costanti difficoltà, il delicato compito di porre un freno alla dilagante e critica frammentarietà di approcci nel contesto europeo non può più ormai essere affidato unicamente alla CGUE: il ruolo suppletivo assunto sin dalla sentenza *Digital Rights Ireland* dalla giurisprudenza dei giudici di Lussemburgo necessita ora di essere seguito da un intervento coordinato e quanto più coerente possibile da parte di Commissione [25], Consiglio e Parlamento dell'UE, chiamati a determinare una sintesi che sia in grado di ottenere il consenso degli Stati membri, riuscendo al contempo ad integrare i principi e requisiti sanciti nella ormai consolidata *case law* della CGUE. Pur nella consapevolezza della difficoltà di giungere a tale soluzione, affrontare questa sfida assume ormai carattere improrogabile e non più rinviabile ad un intervento che non sia legislativo [26]. Una simile normativa non dovrebbe, a parere di chi scrive,

[24] E. CELESTE, *Commission v. Spain and H.K. v. Prokuratuur*, in *Bridge Blog*, 15 marzo 2021.

[25] Questa, come si è messo in evidenza nel Capitolo 2, ha ora l'importante compito di valutare tanto la possibilità di un intervento normativo *ad hoc* in materia di *data retention* quanto l'opportunità di attivare procedure di infrazione avverso quegli Stati membri che non abbiano correttamente trasposto nell'ordinamento interno la facoltà sancita dall'art. 15 Direttiva *e-Privacy*, nei limiti dell'interpretazione fornita dalla giurisprudenza della CGUE.

[26] Un intervento normativo a livello europeo era del resto stato da taluni auspicato già all'indomani della sentenza *DRI*: «an EU instrument that harmonizes *data retention* regimes and thus indirectly ensures comparable data protection standards within the region would be the most appropriate solution to balance potentially conflicting interest: enhancing security and safeguarding data privacy rights», F. GALLI, *Digital Rights Ireland as on opportunity to foster a desirable approximation of data retention provisions,* in *Maastricht Journal of European and Comparative Law*, 3, 2016, p. 475. Più recentemente anche Lupária ha ribadito: «la giurisprudenza della CGUE e delle Corti nazionali dimostrano come la *data retention* rappresenti un istituto davvero magmatico e in perenne

prescindere da studi basati su statistiche, indagini e dati fattuali capaci di fornire una corretta comprensione dell'efficacia dello strumento della *data retention*: ciò consentirebbe infatti di svolgere non solo valutazioni maggiormente fondate e consapevoli sulla proporzionalità e necessità dell'ingerenza nei diritti fondamentali prodotta dagli obblighi di conservazione e dalle operazioni di accesso ai metadati, ma anche di rifuggire da quell'insidioso «blind belief in the effectiveness of data-driven solutions» che rischia di tradursi in «a worrying trend towards technological solutionism» [27]. Una risposta legislativa in materia di *data retention* dovrebbe inoltre tenere in debita considerazione l'essenziale contributo derivante sia dalle diverse ma interessanti soluzioni normative adottate a livello nazionale, portatrici di rilevanti e profondi spunti di riflessione che l'analisi comparata ha ben messo in luce, sia dalle vicende giurisprudenziali che hanno visto quali protagonisti i giudici di Lussemburgo così come molte Corti nazionali.

Con riferimento a quest'ultimo profilo, ciò che in definitiva non può essere ignorato nel futuro necessario dibattito sulla regolamentazione dei sistemi di conservazione e accesso ai metadati è quella attenzione ai diritti alla riservatezza e alla protezione dei dati che si è sempre più affermata negli ultimi decenni nel contesto europeo, anche davanti a forti derive

---

evoluzione, il quale abbisogna di un urgente intervento normativo da parte del legislatore UE», L. LUPÁRIA, *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019, p. 761.

[27] EDRI, *Data retention revisited*, Bruxelles, 2020, p. 4, disponibile all'indirizzo https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pd f. Porre attenzione ai dati reali e allo studio delle casistiche concrete di impiego degli strumenti di *data retention* consentirebbe anche di trovare un punto di sintesi tra chi, come Drewry, ritiene che la conservazione di tipo generalizzato rappresenti uno strumento assolutamente vincente che consente, diversamente dalle possibili alternative quali la *data preservation*, di tornare indietro nel tempo, in un'epoca in cui ormai il passato è rinvenibile principalmente nei dati digitali (L. DREWRY, *Crimes without culprits: why the EU needs data retention and how it can be balanced with the right to privacy*, in *Wisconsin international law journal*, 4, 2015, p. 728 ss.), e chi invece rinviene proprio nell'eccesso di informazioni e dati uno strumento che rallenta e pregiudica l'efficacia delle attività svolte da autorità di *law enforcement* e intelligence (M. SCHEININ, *Towards evidence-based discussion on surveillance: a rejoinder to Richard A. Epstein*, in *European Constitutional Law Review*, 12, 2016, p. 347).

securitarie. Ciò che anche la CGUE – seguita poi, come si è visto, da talune Corti nazionali – ha ben fatto emergere dalla propria giurisprudenza, è infatti l'importanza di non sacrificare aprioristicamente le libertà dinnanzi alle minacce alla sicurezza [28], bensì di predisporre condizioni e garanzie tali da rendere la compressione della sfera privata proporzionata al fine da raggiungere [29]. Così facendo si prendono le distanze da quella concezione che ravvedendo nella garanzia della sicurezza una finalità eccezionale in grado di giustificare qualsiasi misura, rischia di scardinare il vitale sistema di riconoscimento e difesa dei diritti fondamentali, vero baluardo di una società democratica e di uno Stato di diritto. Allontanarsi da quest'ultima insidiosa visione significa innanzitutto emancipare i diritti alla riservatezza e alla protezione dei dati da una loro concezione unicamente soggettiva, relegata cioè alla sola tutela della sfera privata: quella che viene promossa è piuttosto una lettura capace di cogliere l'intrinseca connessione e legame di questi due diritti con il godimento e la garanzia di altri diritti e libertà fondamentali quali la libertà di espressione, di associazione, di formazione e manifestazione del pensiero e dei propri convincimenti, realmente "liberi" solo quando non condizionati dal timore di un controllo del potere pubblico sulle proprie comunicazioni, sui legami con altri soggetti, sulle abitudini o sui luoghi frequentati. In questo senso vanno lette le parole di Rodotà che già nel 2004 affermava, con lucida incisività, come «la privacy è uno strumento necessario per difendere la società della libertà e per opporsi alle spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale» [30]. Questa rappresentazione dei diritti alla riservatezza e alla protezione dei dati, che Solove denomina, non a caso, «pluralistic conception of privacy» [31], consente

---

[28] In questi termini A. VEDASCHI, *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'UE*, in *Giurisprudenza costituzionale*, 4, 2017, p. 1921.

[29] Così G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e della 'emergenza normalizzata'*, in *Rivista AIC*, 4, 2019, p. 85.

[30] S. RODOTÀ, *Privacy, libertà, dignità*, 2004, disponibile all'indirizzo https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293.

[31] Similmente, molti hanno sottolineato il legame tra diritti alla privacy e alla protezione dei dati ed altri diritti e libertà fondamentali: oltre agli autori già richiamati in

di comprendere come «freedom from surveillance, whether public or private, is foundational to the practice of informed and reflective citizenship. Privacy therefore is and indispensable structural feature of liberal democratic political systems» [32].

È allora partendo dalla consapevolezza del valore anche sociale della tutela dei diritti alla privacy e alla protezione dei dati che deve essere letta la sfida della *data retention* e della determinazione di un punto di equilibrio tra sicurezza e diritti fondamentali, resa ancor più delicata e complessa nell'attuale contesto caratterizzato dall'inarrestabile incedere del progresso tecnico-scientifico e dell'affermarsi di sistemi di sorveglianza sempre più invasivi e sofisticati [33]. Non stupisce, dunque, che persino Catherine DeBolle, all'epoca *Executive Director* di Europol, abbia riconosciuto che «we do not have to choose either freedom or security. There is no need to compromise on individual privacy for the sake of public security», come affermato nel Report del Convegno organizzato il 23 novembre 2018 e significativamente titolato «*Freedom AND security. Killing the zero sum process*». Se da un lato pare del tutto utopistico credere di poter contrastare forme di criminalità grave senza ricorrere all'impiego delle nuove tecnologie e dei *Big Data*, concependo così diritti e libertà come assoluti e non suscettibili di compressioni e limitazioni, nondimeno risul-

---

questo lavoro, in particolare nel Capitolo 1, Bignami ha messo in luce come «one of the most important lessons of the past five years has been that privacy breaches, whenever they occur, make democracies vulnerable, whenever they are» (F. BIGNAMI, *Schrems II: the right to privacy and the new illiberism*, in *Media Laws*, 3, 2020, p. 309), così che l'adozione di normative volte ad instaurare forme di controllo esteso sui dati e metadata finiscono col rappresentare un insidioso «pattern of democratic backsliding» (M. ROTENBERG, E. KYRIAKIDES, *Preserving Article 8 in times of crisis*, in F. BIGNAMI (a cura di), *EU law in populist times. Crises and prospects*, Cambridge University Press, Cambridge, 2020, p. 342).

[32] J.E. COHEN, *What privacy is for?*, in *Harvard Law Review*, 126, 2012, p. 1905.

[33] Come chiaramente rilevato da Vedaschi, «nella *digital age*, l'elemento tecnologico si inserisce dunque nel già complesso rapporto tra sicurezza e diritti, facendo sì che esso perda la sua "biunivocità" e si trasformi in una relazione a tre fattori», A. VEDASCHI, *Sicurezza e diritti nella* digital age. *La tecnologia: un'arma a doppio taglio nella lotta al terrorismo internazionale*, in L. LLOREDO ALIX, A. SOMMA (a cura di), *Scritti in onore di Mario G. Losano. Dalla filosofia del diritto alla comparazione giuridica*, Accademia University Press, Torino, 2021, p. 521.

ta erroneo leggere sicurezza e diritti fondamentali come elementi in irriducibile contrasto [34]. In questo senso, pertanto, «the relation between privacy and security is not a trade-off between two incompatible values. Strong privacy and data protection – which implies, for instance, data security and data minimisation – can benefit law enforcement. The challenge is to include synergies in the decision-making» [35].

L'analisi della disciplina della *data retention* ha posto in luce la consapevolezza e la volontà tanto delle Istituzioni a livello sovranazionale quanto di quelle nazionali di scongiurare il rischio di cedere sia alla tentazione di una garanzia della sicurezza a tutti i costi, sia ad una anacronistica ed irrealizzabile tutela assoluta dei diritti fondamentali incapace di fare i conti con le ineludibili esigenze securitarie. Se è vero che «there are few words more dangerously confusing in their meaning than "liberty" and "security"» [36], nelle vicende che hanno caratterizzato la regolamentazione dei sistemi di conservazione dei metadati è possibile rinvenire un momento importantissimo e forse ineguagliato di riflessione profonda e tutt'altro che priva di difficoltà sulla necessità di stabilire criteri e requisiti regolanti sistemi di controllo e sorveglianza. Tali specifiche salvaguardie e limitazioni debbono garantire l'efficacia dello strumento della conservazione e, allo stesso tempo, un forte rispetto dei diritti fondamentali, così dimostrando che la determinazione di un punto di equilibrio tra garanzia della sicurezza e tutela dei diritti e delle libertà è, e deve essere, l'obiettivo cui tendere [37]. Evitare di cadere nella logica del *trade-off*, più semplicistica

---

[34] Di "completamento reciproco", anziché di antagonismo, parla anche P. RIDOLA, *Libertà e diritti nello sviluppo storico del costituzionalismo*, in P. RIDOLA, R. NANIA (a cura di), *I diritti costituzionali*, Giappichelli, Torino, 2006, p. 3 ss.

[35] H. HIJIMANS, *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 16 TFEU*, Springer, 2016. Dello stesso avviso anche Ojanen: «one of the major lessons from *DRI* and *Schrems* is that the trade-off between privacy and security *in abstracto* should be rejected», T. OJANEN, *Rights-based review of electronic surveillance after Digital Rights Ireland and Schrems in the European Union*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, 2017, p. 18.

[36] C. GEARTY, *Escaping Hobbes: liberty and security for our democratic (not anti-terrorist) age*, in *LSE Working Papers*, 3, 2010.

[37] Interessante è la provocazione pronunciata da Vermeulen in occasione della sopra

ma dalle conseguenze imprevedibili, ed alimentare al contempo un serio dibattito in tal senso tra UE e Stati membri, tra legislatori e Governi, tra Parlamenti e Corti, tra Autorità garanti e autorità di *law enforcement*, tra sviluppatori di nuove tecnologie e giuristi, tra Corti nazionali e CGUE, diviene senza dubbio uno degli sforzi maggiori che il mondo del diritto deve e dovrà sostenere. Le pagine che precedono hanno inteso fornire un contributo a questo ampio dibattito, destinato a divenire sempre più centrale e delicato: ciò nella convinzione che solo un armonico dialogo tra i diversi attori sopra individuati potrà generare frutti condivisi e utili allo sviluppo globale di un ecosistema giuridico e sociale adeguato alle sfide del futuro.

---

richiamata Conferenza di Europol: «With a bit of creativity, it is possible to come to a good set of selectors which make your life easy for the future. Not as easy as receiving everything without having to do anything, but my invitation is: why don't you give it a try?», EUROPOL, *Freedom AND security. Killing the zero sum process*, Conference Report, 2018, p. 18, disponibile all'indirizzo https://www.europol.europa.eu/publications-documents/freedom-and-security-killing-zero-sum-process.

BIBLIOGRAFIA

AA.VV., *Convegno AIC, Libertà e sicurezza nelle democrazie contemporanee. Atti del Convegno annuale, Bari, 17-18 ottobre 2003: annuario 2003*, Cedam, Padova, 2008.

AGAMBEN G., *Stato di eccezione,* Bollato-Boringhieri, Torino, 2003.

ALPA G., MARKESINIS B., *Il diritto alla privacy nell'esperienza di common law e nell'esperienza italiana*, in *Rivista trimestrale di diritto civile e procedura civile*, 51, 1974, p. 417 ss.

ALPA G. (a cura di), *Diritto e intelligenza artificiale*, Pacini Giuridica, Pisa, 2020.

ANDOLINA E., *L'acquisizione nel processo penale dei dati 'esteriori' delle comunicazioni telefoniche e telematiche*, Padova, Cedam, 2018.

ANDREJEVIC M., *Surveillance in the big data era. Emerging pervasive information and communications technologies*, in *Law, Governance and Technology Series*, 11, 2014, p. 55 ss.

ARENA A., *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quaderni costituzionali*, 3, 2014, p. 722 ss.

ARTEMIOU E., *The way out of Digital Rights Ireland*, in *CiTiP Law Blog*, 19 giugno 2018.

ASSANTE E., *Cosa ci può insegnare il caso Cambridge Analytica*, in *Federalismi.it*, 9, 2018, p. 1 ss.

ATERNO S., *Data retention: gli effetti nel nostro Paese della sentenza del 2 marzo 2021 della CGUE*, in *e-Lex*, 21 giugno 2021.

AUDIBERT M., *Conservation des données de connexion. Comment le Conseil d'État a sauvé la majorité des enquête judiciaires*, in *Vielle Juridique*, 96, 2021, p. 16 ss.

AZOULAI L., RITLENG D., BONINI M., *L'État, c'est moi: il Consiglio di Stato francese, fra salvaguardia della sicurezza nazionale e protezione dei dati*, in *CERIDAP*, 26 luglio 2021.

AZOULAI L., RITLENG D., *L'État c'est moi. Le conseil d'État, la sécurité et la conservation des données*, in *Revue Trimestrielle de Droit Européen*, 2, 2021, p. 349 ss.

BACCARI G.M., *Il trattamento (anche elettronico) dei dati personali per finalità di accertamento dei reati*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, Milano, 2019, p. 1599 ss.

BALBONI J., SAMAIN M., *La conservation des données télécom au coeur d'une guerre de pouvoir*, in *L'Echo*, 25 maggio 2021.

BALDASSARRE A., *Privacy e Costituzione. L'esperienza statunitense*, Bulzoni, Roma, 1974.

BALDINI V., *Sicurezza e libertà nello Stato di diritto in trasformazione*, Giappichelli, Torino, 2004.

BALDUCCI ROMANO F., *La protezione dei dati personali nell'UE tra libertà di circolazione e diritti fondamentali dell'uomo*, in *Rivista italiana di diritto pubblico comunitario,* 6, 2015, p. 1619 ss.

BARBERIS M., *Liberté, égalité, sécurité. Gli equivoci della guerra al terrore*, in *Il Mulino*, 4, 2016.

BASSINI M., *La Corte di giustizia e la conservazione dei dati. Spunti di una rilettura 'postuma'*, in L. E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, Napoli, 2021, p. 111 ss.

BASSU C., *Terrorismo e costituzionalismo. Percorsi comparati*, Giappichelli, Torino, 2010.

BAUMAN Z., LYON D., *Liquid surveillance. A conversation*, Polity Press, Cambridge, 2013.

BENDER D., *The Judicial Redress Act: A Path to Nowhere,* in *Privacy Advisor Blog*, Issue 17, 2015.

BENEDIZIONE L., PARIS E., *Preliminary reference and dialogue between Courts as tools of reflection on the EU system of multilevel protection of rights: the case of the Data Retention Directive*, in *German Law Journal*, 6, 2015, p. 1727 ss.

BENTHAM J., *Panopticon or the inspection-house*, T. Payne, Londra, 1791.

BIFULCO R., *Il trasferimento dei dati personali nella sentenza Schrems II: dal contenuto essenziale al principio di proporzionalità e ritorno*, in *Diritto Pubblico Europeo Rassegna Online*, 2, 2020, p. 1 ss.

BIGNAMI F., *Protecting privacy against the Police in the European Union: the Data Retention Directive,* in AA. VV., *Melanges en l'honneur de Philippe Léger*, Editions Pedone, Parigi, 2006, p. 109 ss.

BIGNAMI F., *Privacy and law enforcement in the European Union: the Data Retention Directive*, in *Chicago Journal of International Law*, 1, 2007, p. 233 ss.

BIGNAMI F., RESTA G., *Transatlantic privacy regulation: conflict and cooperation*, in *Law and Contemporary Problems*, 4, 2015, p. 231 ss.

BIGNAMI F., *Schrems II: the right to privacy and the new illiberism*, in *MediaLaws*, 3, 2020, p. 308 ss.

BLOUNSTEIN E., *Privacy as an aspect of human dignity*, in *New York University Law Review*, 39, 1964, p. 962 ss.

BOEHM F., COLE M., *Data retention after the judgement of the Court of Justice of the EU*, The Greens in the EP Working Paper, 2014, p. 1 ss.

BOGNETTI G., *Introduzione al diritto costituzionale comparato (Il metodo)*, Giappichelli, Torino, 1994.

BONETTI P., *Terrorismo, emergenza e costituzioni democratiche,* Il Mulino, Bologna, 2006.

BONFIGLIO S., *Diritto alla privacy e lotta al terrorismo nello spazio pubblico europeo*, in *Diritto e Sicurezza*, 3, 2014, p. 1 ss.

BORGIA F., *Profili critici in materia di trasferimento dei dati personali verso i Paesi extra-europei*, in *Il mercato unico digitale*, in *Diritto Mercato e Tecnologia, Numero Speciale*, 2017, p. 140 ss.

BOTTA M., VIOLA DE AZEVEDO CUNHA M., *La protezione dei dati personali nelle relazioni tra UE e USA, le negoziazioni sul trasferimento dei PNR*, in *Il Diritto dell'Informazione e dell'Informatica*, 2, 2010, p. 315 ss.

BOWDEN C., *The US Surveillance programmes and their impact on EU citizens' fundamental rights. Note to the European Parliament*, 2013, p. 1 ss.

BRADFORD A., *The Brussels effect*, in *Northwestern University Law Review*, 1, 2012, p. 1 ss.

BRIN D., *The transparent society. Will technology force us to choose between privacy and freedom?*, Perseus Books, New York, 1998.

BRKAN M., *The unstoppable expansion of the EU fundamental right to data protection. little shop of horrors?*, in *Maastricht Journal of European and Comparative Law*, 5, 2016, p. 812 ss.

BRKAN M., *The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning,* in *German Law Journal,* 20, 2019, p. 876 ss.

BROUWER E., *Ignoring Dissent and Legality. The EU's Proposal to Share the Personal Information of All Passengers*, in *CEPS Paper in Liberty and Security in Europe*, 2011, p. 1 ss.

BROWN I., KORFF D., *Exchanges of personal data after the Schrems II Judgement*, PE 694.678, luglio 2021, p. 1 ss.

BRUGIOTTI E., *La privacy attraverso le generazioni dei diritti. Dalla tutela della riservatezza alla protezione dei dati personali*, in *Dirittifondamentali.it*, 2, 2013, p. 1 ss.

BUQUICCHIO Q., *Aspetti internazionali della protezione dei dati: il ruolo svolto*

dal Consiglio d'Europa, in N. MATTEUCCI (a cura di), *Privacy e banche dati*, Il Mulino, Bologna, 1981.

BURNS H., *What the Schrems II ruling means for Brexit*, in *AfterBrexit Blog*, 16 luglio 2020.

BUTLER A., HIDVEGI F., *From Snowden to Schrems: how the surveillance debate has impacted US-EU relations and the future of international data protection*, in *Seton Hall Journal of Diplomacy and International Relations*, Special Issue 2015/2016, p. 1 ss.

CADOPPI A., CANESTRARI S., MANNA A., PAPA M. (a cura di), *Cybercrime*, Utet, Milano, 2019.

CAGGIANO G., *Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione*, in *MediaLaws*, 2, 2018, p. 64 ss.

CALIFANO L., *Privacy e sicurezza*, in *Diritto e Sicurezza*, 3, 2013, p. 1 ss.

CALIFANO L., COLAPIETRO C. (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, Editoriale Scientifica, Napoli, 2017.

CALIFANO L., *Introduzione*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, Editoriale Scientifica, Napoli, 2017, p. I ss.

CALIFANO L., *Principi e contenuti del Regolamento UE 2016/679 in materia di protezione dei dati personali*, in L. SCAFFARDI (a cura di), *I 'profili' del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, Torino, 2018, p. 1 ss.

CALVINO M., LOSANO M.G., TRIPODINA C. (a cura di), *Lotta al terrorismo e tutela dei diritti fondamentali*, Giappichelli, Torino, 2009.

CAMERON I., *Balancing data protection and law enforcement needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, 54, 2017, p. 1467 ss.

CAMERON I., *European Union Law restraints on intelligence activities*, in *International Journal of Intelligence and Counter-Intelligence*, 3, 2020, p. 452 ss.

CANNETTI G.A., *Passenger Name Records tra istanze di sicurezza globale e tutela dei dati personali*, in *I quaderni europei. Il diritto alla privacy e trattamento automatizzato dei dati fra diritto civile, diritto penale e diritto internazionale ed europeo*, 63, 2014, p. 86 ss.

CAPUTO P., *La conservazione dei dati di traffico telefonico e telematico nella normativa antiterrorismo*, in *Archivio Penale*, 1, 2016, p. 1 ss.

CARDONE A., *La "normalizzazione" dell'emergenza*, Giappichelli, Torino, 2011.

CARPANELLI E., LAZZERINI N., *PNR: problems not resolved? The EU PNR conundrum, after Opinion 1/15 of the CJEU*, in *Air and Space Law*, 42, 2017, p. 377 ss.

CARRERA S., GUILD E., *Safe Harbour or into the Storm? EU-US Data transfer after Schrems Judgement*, CEPD Liberty and Security in Europe Papers, novembre 2015, p. 1 ss.

CARRERA S., GUILD E., *The end of Safe Harbour: what future for EU-US data transfers?,* in *Maastricht Journal of European and Comparative law*, 3, 2015, p. 651 ss.

CARROZZA P., DI GIOVINE A., FERRARI G.F. (a cura di), *Diritto costituzionale comparato*, V Ed., Laterza, Roma-Bari, 2014.

CARROZZA P., *La Cour d'Arbitrage belga*, in G.F. FERRARI, A GAMBARO (a cura di), *Corti nazionali e comparazione giuridica*, ESI, Napoli, 2006, p. 105 ss.

CARTABIA M., *L'ora dei diritti fondamentali nell'Unione Europea*, in M. CARTABIA (a cura di), *I diritti in azione*, Il Mulino, Bologna, 2007, p. 1 ss.

CAS J., BELLANOVA R., BURGESS J.P., FRIEDWALD M., PEISSL W., *Introduction: Surveillance, privacy and security*, in J. CAS, R. BELLANOVA, J.P. BURGESS, M. FRIEDWALD, W. PEISSL (a cura di), *Surveillance, privacy and security: Citizens' perspectives*, Routledge, Londra, 2017, p. 1 ss.

CASSART A., HENROTTE J-F., *L'invalidation de la directive 2006/24 sur la conservation des données de communication électronique ou la chronique d'une mort annoncée*, in *Jurisprudence de Liege*, 20, 2014, p. 954 ss.

CELESTE E., *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019, p. 134 ss.

CELESTE E., *Commission v. Spain and H.K. v. Prokuratuur: taking the plank out of EU's own eye*, in *Bridge Blog*, 15 marzo 2021.

CELESTE E., *Cross-border data protection after Brexit*, in *Brexit Institute Working Paper Series*, 4, 2021, p. 1 ss.

CELESTE E., *From the UK adequacy decision to Big Brother Watch: increasingly divergent approaches to mass surveillance in Europe*, in *DCU Brexit Insititute news*, 28 maggio 2021.

CEPEDA ESPINOSA M.J., *Privacy*, in M. ROSENFELD, A. SAJO (a cura di), *The Oxford handbook of comparative constitutional law*, Oxford University Press, Oxford, 2013, p. 966 ss.

CERRINA FERONI G., MORBIDELLI G., *La sicurezza: un valore super primario*, in *Percorsi Costituzionali*, 1, 2008, p. 31 ss.

CHRISTAKIS T., *'Schrems III'? First thoughts on the EDPB post-Schrems II Recommendations on International Data Transfers*, in *European Law Blog*, 13 novembre 2020.

CHRISTAKIS T., PROPP K., *How EU's intelligence services aim to avoid the EU's highest Court and what it means for the US*, in *LawFare*, 8 marzo 2021.

CHRISTAKIS T., *Squaring the circle? International surveillance, underwater cables and EU-US adequacy negotiations*, in *European Law Blog*, 12 aprile 2021.

CHRISTAKIS T., BOUSLIMANI K., *National security, surveillance and human rights*, in R. GEISS, N. MELZER (a cura di), *Oxford handbook on the International Law of global security*, Oxford University Press, Oxford, in corso di pubblicazione.

CLEMENTI F., TIBERI G., *Sicurezza interna, diritti e cooperazioni internazionale nella lotta al terrorismo*, in *Astrid-online.it*, 1, 2013.

COBBE J., *Casting the dragnet: communications data retention under the Investigatory Powers Act*, in *Public Law*, 2018, p. 1 ss.

COHEN J.E., *What privacy is for?*, in *Harvard Law Review*, 126, 2012, p. 1904 ss.

COLE M., BOEHM F., *EU Data Retention – Finally abolished? Eight years in light of Article 8*, in *Critical Quarterly for Legislation and Law*, 1, 2014, p. 58 ss.

COLE D., FABBRINI F., *Bridging the transatlantic divide? The United States, The European Union and the protection of privacy across borders*, in *International Journal of Constitutional Law,* 1, 2016, p. 220 ss.

COLE D., FABBRINI F., *Transatlantic Negotiations for Transatlantic Rights: Why an EU-US Agreement is the Best Option for Protecting Privacy Against Cross-border Surveillance*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, Londra, 2017, p. 197 ss.

COUDERT F., *Schrems vs. Data Protection Commissioner: a slap on the wrist for the Commission and new powers for Data Protection Authorities,* in *European Law Blog*, 15 ottobre 2015.

COUDERT F., *The legitimacy of bulk transfers of PNR data to law enforcement authorities under the strict scrutiny of AG Mengozzi*, in *Europan Data Protection Law Review*, 4, 2016, p. 596 ss.

COUDERT F., VERBRUGGEN F., *Conservation des données de communications électronique en Belgique: un juste équilibre?*, in V. FRANSSEN, D. FLORE (a cura di), *Societé numerique et droit penal*, Bruylant, Bruxelles, 2019, p. 248 ss.

CRESPI S., *Diritti fondamentali, Corte di giustizia e riforma del sistema UE di protezione dei dati*, in *Rivista italiana di diritto pubblico comunitario*, 3-4, 2015, p. 819 ss.

CRESPI S., *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, 3, 2016, p. 687 ss.

CRESPI S., *The applicability of Schrems principles to the Member States: national security and data protection within the EU context*, in *European Law Review*, 43, 2018, p. 669 ss.

CRESPI S., *Applicazione di tracciamento Immuni tra normative nazionale e diritto UE in materia di protezione dei dati personali*, in *Freedom, Security & Justice*, 2, 2020, p. 20 ss.

CURICCIATI L., *Diritto alla riservatezza e sicurezza nella giurisprudenza delle Corti costituzionali e sovrastatali europee. Il caso della Data Retention Directive*, in *Democrazia e Sicurezza*, 2, 2017, p. 89 ss.

D'ALOIA A. (a cura di), *Intelligenza artificiale (Contributi del Convegno su 'Intelligenza artificiale e diritto. Come regolare un mondo nuovo', Parma, 12 ottobre 2018),* in *BioLaw Journal*, 1, 2019.

D'ORAZIO R., *La tutela multilivello del diritto alla protezione dei dati personali e la dimensione globale*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Giappichelli, Torino, 2019, p. 61 ss.

D'ORAZIO R., FINOCCHIARO G., POLLICINO O., RESTA G. (a cura di), *Codice della privacy e data protection*, Giuffrè, Milano, 2021.

DASKAL J., *The un-territoriality of data*, in *Yale Law Journal*, 2, 2015, p. 326 ss.

DASKAL J., *What comes next: the aftermath of European Court's blow to transatlantic data transfers*, in *Just Security*, 17 luglio 2020.

DE GREGORIO G., TORINO R., *Privacy, tutela dei dati personali e Big Data*, in E. TOSI (a cura di), *Privacy digitale*, Giuffrè, Milano, 2019, p. 450 ss.

DE HERT P., GUTWIRTH S., *Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action*, in S. GUTWIRTH, Y. POULLET, P. DE HERT. C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing data protection?*, Springer, Berlino, 2009, p. 3 ss.

DE HERT P., PAPAKONSTANTINOU V., *The UK contribution to the field of EU data protection: let's not go for 'third country' status after Brexit*, in *Computer Law and Security Review*, 33, 2017, p. 354 ss.

DE MINICO G., *Costituzione. Emergenza e terrorismo*, Jovene, Napoli, 2016.

DE MINICO G., *La risposta europea al terrorismo del tempo ordinario: il lawmaker e il giudice*, in *Osservatorio sulle fonti*, 2, 2017, p. 1 ss.

DE MINICO G., *Big Data e la debole resistenza delle categorie giuridiche. Privacy e lex mercatoria*, in *Diritto pubblico*, 1, 2019, p. 89 ss.

DE MINICO G., *Libertà in rete. Libertà dalla rete*, Giappichelli, Torino, 2020.

DE MINICO G., *Virus e algoritmi. Impariamo da un'esperienza dolorosa*, in *LaCostituzione.info*, 1 aprile 2020.

DE MONTECLER M.-C., *Conservation des données: la Cour constitutionnelle belge donne sa lecture*, in *Dalloz. Actualité. Le quotidien du droit*, 28 aprile 2021.

DE SIMONE C., *Pitting Karlsruhe against Luxembourg? German data protection*

and the contested implementation of the EU Data Retention Directive, in *German Law Journal*, 11, 2010, p. 291 ss.

DE SIMONE R., *Corte di giustizia dell'UE, Grande Sezione, sentenza 6 ottobre 2015, in causa C-362/14, Maximillian Schrems c. Data Protection Commissioner,* in *Rivista italiana di diritto pubblico comunitario*, 4, 2015, p. 1793 ss.

DE TERWANGNE C., DEGRAVE E. (a cura di), *La protection des données à caractère personnel en Belgique: manuel de base*, Politeia, Bruxelles, 2019.

DE VERGOTTINI G., *Diritto costituzionale comparato*, Cedam, Padova, 2004.

DE VERGOTTINI G., *Guerra e Costituzione. Nuovi conflitti e sfide alla democrazia*, Il Mulino, Bologna, 2004.

DE VERGOTTINI G., *Una rilettura del concetto di sicurezza nell'era digitale e della 'emergenza normalizzata'*, in *Rivista AIC*, 4, 2019, p. 66 ss.

DE VILLENFAGNE F., DUSSOLIER S., *La Belgique sort enfin ses armes contre la cybercriminalité: à propos de la loi du 28 novembre 2000 sur la criminalité informatique*, in *A&M*, 1, 2001, p. 71 ss.

DE VRIES K., BELLANOVA R., DE HERT P., GUTWIRTH S., *The German Constitutional Court judgement on data retention: proportionality overrides unlimited surveillance (doesn't it?)*, in S. GUTWIRTH, Y. POULLET, P. DE HERT, R. LEENS (a cura di), *Computers, privacy and data protection: an element of choice*, Springer, Berlino, 2011, p. 3 ss.

DEGRAVE E., POULLET Y., *Le droit au respect de la vie privée face aux nouvelles technologies*, in M. VERDUSSEN, N. BONBLED (a cura di), *Les droits constitutionnels en Belgique*, Bruylant, Bruxelles, 2011, p. 1001 ss.

DEGRAVE E., *La Commission de la protection de la vie privée: l'Autorité de régulation du secteur des traitements de données à caractère personnel*, in *Revue du Centre d'étude et de recherches en administration publique*, 26, 2016, p. 37 ss.

DEL VESCOVO D., *L'accesso delle autorità pubbliche a dati personali di natura meramente identificativa non costituisce ingerenza grave nei diritti fondamentali degli interessati*, in *Amministrativamente – Rivista di diritto amministrativo*, 11-12, 2018, p. 12 ss.

DELLA MORTE G., *La tempesta perfetta. Covid-19, deroghe alla protezione dei dati personali ed esigenze di sorveglianza di massa*, in *SIDI Blog*, 30 marzo 2020.

DELLA TORRE J., *L'acquisizione dei tabulati telefonici nel processo penale dopo la sentenza della Grande Camera della CGUE: la svolta garantista in un primo provvedimento del g.i.p. di Roma*, in *Sistema Penale*, 29 aprile 2021.

DETERMANN L., *California Privacy Law. Practical guide and commentary*, IAPP, Portsmouth, 2020.

DHONT J.X., *Schrems II. The EU adequacy regime in existential crisis?*, in *Maastricht Journal of European and Comparative Law*, 5, 2019, p. 597 ss.

DI MARTINO A., *La protezione dei dati personali*, in S. PANUNZIO (a cura di), I *diritti fondamentali e le Corti in Europa*, Jovene, Napoli, 2005, p. 365 ss.

DI MARTINO A., *Bundesverfassungsgericht dichiara l'incostituzionalità della data retention e torna sul rapporto tra libertà e sicurezza*, in *Giurisprudenza costituzionale*, 5, 2010, p. 4059 ss.

DI MARTINO A., *Profili costituzionali della privacy in Europa e negli Stati Uniti*, Jovene, Napoli, 2017.

DI MATTEO F., *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella Direttiva PNR?*, in *Diritti Umani e Diritto Internazionale*, 1, 2017, p. 213 ss.

DICOSOLA M., *La data retention directive e il dialogo tra Corti costituzionali e Corte di giustizia nel sistema multilivello europeo*, in *Diritti Comparati*, 20 febbraio 2014, p. 1 ss.

DIEBOLD F.X., *On the origin(s) and development of Big Data phenomenon, the term and the discipline*, PIER Working Paper, 13, 2012, p. 1 ss.

DIMITROVA A., BRKAN M., *Balancing national security and data protection: the role of the EU and US policy-makers and Courts before and after NSA affair*, in *Journal of Common Market Studies*, 4, 2018, p. 751 ss.

DOCKSEY C., *Opinion 1/15: privacy and security, finding the balance*, in *Maastricht Journal of European and Comparative Law*, 6, 2017, p. 768 ss.

DOCQUIR B., *Droit du numérique*, Larcier, Bruxelles, 2018.

DREWRY L., *Crimes without culprits: why the EU needs data retention and how it can be balanced with the right to privacy*, in *Wisconsin International Law Journal*, 4, 2015, p. 728 ss.

DUCATO R., *Il riconoscimento facciale tra rischi di 'mitridatizzazione sociale' e prospettive di regolamentazione*, in L.E. RIOS VEGA, L. SCAFFARDI, I. SPIGNO (a cura di), *I diritti fondamentali nell'era della digital mass surveillance*, Editoriale Scientifica, Napoli, 2021, p. 187 ss.

DURICA J., *Directive on the retention of data on electronic communication in the rulings of the Constitutional Courts of EU Member States and efforts for its renewed implementation*, in *The Lawyer Quarterly*, 2, 2013, p. 143 ss.

ELLIOTT M., WILLIAMS J., YOUNG A.L. (a cura di), *The UK Constitution after Miller. Brexit and beyond*, Hart, Londra, 2020.

EPSTEIN R., *The ECJ's Fatal Imbalance: Its cavalier treatment of national security issues poses serious risk to public safety and sound commercial practices*, in *European Constitutional Law Review*, 12, 2016, p. 330 ss.

EUROJUST, *Data retention regimes in Europe in light of the CJEU ruling of 21*

December in Joined Cases C-203/15 and C-698/15, 10098/17 Eurojust 91, 6 novembre 2017.

EUROPOL, *Freedom AND security. Killing the zero sum process*, Conference Report, 2018.

FABBRINI F., *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quaderni costituzionali*, 2, 2009, p. 419 ss.

FABBRINI F., *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*, 28, 2015, p. 65 ss.

FABBRINI F., *The EU Charter of Fundamental Rights and the rights to data privacy: the EU Court of Justice as a Human Rights Court*, in S. DE VRIES et al. (a cura di), *The EU Charter of Fundamental Rights as a binding instrument: five years old and growing*, Bloomsbury, Londra, 2015, p. 261 ss.

FABBRINI F., *Brexit. Tra diritto e politica*, Il Mulino, Bologna, 2021.

FALLETTA P., *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande Sezione), 6 ottobre 2015, Schrems c. DPC, C-362/14)*, in *Federalismi.it*, 24, 2015, p. 1 ss.

FAMIGLIETTI G., *Il diritto alla riservatezza o la riservatezza come diritto*, in A. D'ALOIA (a cura di), *Bio-tecnologie e valori costituzionali. Il contributo della giustizia costituzionale*, Giappichelli, Torino, 2004, p. 299 ss.

FANTIN S., *The impact of Schrems II: a list of homeworks*, in *CiTiP Law Blog*, 23 luglio 2020.

FARINA M., *La data protection ai tempi del coronavirus tra prevenzione dei reati e repressione del contagio*, in *BioLaw Journal*, 20 marzo 2020.

FATTA C., *La tutela della privacy alla prova dell'obbligo di data retention e delle misure antiterrorismo*, in *Diritto dell'Informazione e dell'Informatica*, 2008, p. 395 ss.

FEILER L., *The legality of the Data Retention Directive in light of the fundamental rights to privacy and data protection*, in *European Journal of Law and Technology*, 3, 2010, p. 1 ss.

FENNELLY D., *Data retention: the life, death and afterlife of a directive*, in *ERA Paper*, 2018, p. 1 ss.

FERIOLI E.A., *Il Belgio*, in P. CARROZZA, A. DI GIOVINE, G.F. FERRARI (a cura di), *Diritto costituzionale comparato*, Tomo I, V Ed., Laterza, Roma-Bari, 2014, p. 319 ss.

FIEVET C. et al., *Droit au respect de la vie privée et à la protection des données en lien avec les technologies de l'information*, in *Revue du Droit des Technologies de l'Information*, 68-69, 2017, p. 94 ss.

FINOCCHIARO G., *Riflessioni sul poliedrico Regolamento europeo sulla privacy*, in *Quaderni costituzionali*, 4, 2018, p. 895 ss.

FLICK G.M., *Dei diritti e delle paure*, in S. MOCCIA (a cura di), *I diritti fondamentali della persona alla prova dell'emergenza*, ESI, Napoli, 2009.

FLICK G.M., *Elogio della dignità (se non ora, quando?)*, in *Rivista AIC*, 4, 2014, p. 1 ss.

FLOR R., *Data retention e limiti al potere coercitivo dello Stato in materia penale: le sentenze del Bundesverfassungsgericht e della Curtea Constitutionala*, in *Cassazione Penale*, 5, 2011, p. 1952 ss.

FLOR R., *Dalla data retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo?*, in *Diritto dell'Informazione e dell'Informatica*, 2014, p. 775 ss.

FLOR R., *Dalla 'data retention' al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive 'de jure condendo'*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, Roma, 2015, p. 223 ss.

FLOR R., *Data retention ed art. 132 Cod. privacy: vexata quaestio(?)*, in *Diritto Penale Contemporaneo*, 3, 2017, p. 356 ss.

FLORA M., *The unlawfulness of data retention confirmed by the Court of Justice of the European Union and the Austrian Constitutional Court*, in *Journal of European Consumer and Market Law*, 3, 2015, p. 102 ss.

FORGET C., *L'obligation de conservation des 'métadonnées': la fin d'une longue saga juridique?*, in *Journal des Tribunaux*, 13, 2017, p. 233 ss.

FORMICI G., *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, in *Osservatorio AIC*, 3, 2018, p. 433 ss.

FORMICI G., *La* digital mass surveillance *al vaglio della Corte Europea dei Diritti dell'Uomo: da* Zakharov *a* Big Brother Watch, in *Federalismi.it – Focus Human Rights*, 23, 2020, p. 44 ss.

FORMICI G., *The external dimension of the European rule of law in the digital age: an analysis through the lens of the ECJ case-law on data transfer*, in *Cahiers Jean Monnet n. 6/2020, Actes des ateliers doctoraux 2019 "L'État de droit" de l'Université degli Studi di Milano et de la European School of Law Toulouse, Centre d'excellence Europe Capitole*, Lextenso, Toulouse, 2020, p. 215 ss.

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

FORNI L., VETTOR T. (a cura di), *Sicurezza e libertà in tempi di terrorismo globale*, Giappichelli, Torino, 2018.

FOUCAULT M., PIERROT M. (a cura di), *Jeremy Bentham. Panopticon ovvero la casa d'ispezione*, Marsilio, Venezia, 1997.

FRIEDMAN L., *The Republic of choice, law, authority and culture*, Harvard University Press, Cambridge, Massachusetts, 1990.

FROSINI T.E., *Il diritto costituzionale alla sicurezza,* in *Forum di Quaderni costituzionali*, 2006, p. 1 ss.

FROSINI T.E., *La tutela dei dati e il diritto all'oblio*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, Torino, 2018, p. 89 ss.

FROSINI T.E. (a cura di), *Diritto pubblico comparato*, Il Mulino, Bologna, 2019.

FROSINI T.E., *Il metodo del e nel diritto pubblico comparato*, in L. LLOREDO ALIX, A. SOMMA (a cura di), *Scritti in onore di Mario G. Losano. Dalla filosofia del diritto alla comparazione giuridica*, Accademia University Press, Torino, 2021, p. 99 ss.

FROSINI V., *La protezione della riservatezza nella società informatica*, in N. MATTEUCCI, *Privacy e banche dei dati*, Il Mulino, Bologna, 1981, p. 41 ss.

FROSINI V., *Diritto alla riservatezza e calcolatori elettronici*, in AA. VV., *Il riserbo e la notizia*, Jovene, Napoli, 1983, p. 19 ss.

GALLI F., *Digital Rights Ireland as an opportunity to foster a desirable approximation of data retention provisions*, in *Maastricht Journal of European and Comparative Law*, 3, 2016, p. 460 ss.

GAMBARO A., MONATERI P.G., SACCO R., *Comparazione giuridica*, in *Digesto italiano*, Utet, Milano, 1989.

GAMBINI M., *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *EJJL*, 1, 2013, p. 1 ss.

GAMBINO S., *Diritto costituzionale italiano e comparato. Lezioni*, Periferia, Assago, 2002.

GAVISON R., *Privacy and the limits of law*, in *The Yale Law Journal*, 3, 1980, p. 421 ss.

GEARTY C., *Escaping Hobbes: liberty and security for our democratic (not anti-terrorist) age*, in *LSE Working Papers*, 3, 2010, p. 1 ss.

GILMARTIN C., *Privacy Rights: how should a Court remedy legislative incompatibility with EU law?*, in *UK Human Rights Blog*, 8 maggio 2018.

GIUPPONI T.F., *La sicurezza e le sue dimensioni costituzionali*, in S. VIDA (a cura di), *Diritti umani. Teorie, analisi, applicazioni*, Bononia University Press, Bologna, 2008, p. 1 ss.

GONZALES FUSTER G., *The emergence of personal data protection as a fundamental right of the EU*, Spinger, Berlino, 2014.

GRANGER M., IRION K., *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection*, in *European Law Review,* 6, 2014, p. 835 ss.

GRANOZIO L., *Corte di Giustizia sui tabulati: soluzioni contrastanti*, in *Penale. Diritto e Procedura*, 18 maggio 2021.

GRAZIANI C., *PNR EU-Canada, la Corte di giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali,* in *DPCE Online*, 4, 2017, p. 959 ss.

GREENWALD G., *No place to hide: Edward Snowden, the NSA and the US surveillance state*, Hamish Hamilton, Londra, 2014.

GROPPI T., *Democrazia e terrorismo,* ESI, Napoli, 2009.

GUELLA F., *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*, 2, 2017, p. 349 ss.

GUILD E., CARRERA S., *The political and judicial life of metadata: Digital Rights Ireland and the trial of the Data Retention Directive*, CEPS Paper in Liberty and Security in Europe, 65, 2014, p. 1 ss.

HERLIN-KARNELL E., *Annotation of Ireland v. Parliament and Council*, in *Common Market Law Review*, 46, 2009, p. 1667 ss.

HEITZER S., KULHING J., *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in *European Law Review*, 2, 2015, p. 263 ss.

HIJMANS H., *The EU as a constitutional guardian of internet privacy and data protection. The story of Art. 116 TFEU*, PHD Thesis, 2016, https://pure.uva.nl/ws/files/2676807/169421_DEFINTIEF_ZELF_AANGEPAS_full_text_.pdf.

HIJMANS H., *PNR Agreement EU-Canada scrutinised: CJEU gives very precise guidance to negotiators*, in *European Data Protection Law Review*, 3, 2017, p. 406 ss.

HIRSCHL R., *Comparative matters: the renaissance of comparative constitutional law*, Oxford University Press, Oxford, 2014.

HUGHES K., *The social value of privacy, the value of privacy to society and human rights discourse*, in B. ROESSLER, D. MOKROSINKA (a cura di), *Social dimensions of privacy. Interdisciplinary perspectives*, Cambridge University Press, Cambridge, 2015, p. 225 ss.

IOVENE F., *Data retention tra passato e futuro. Ma quale presente?*, in *Cassazione Penale*, 12, 2014, p. 4274 ss.

JACOBS F., *The EU after Brexit. Institutional and policy implications*, Palgrave, Londra, 2018.

JONES C., HAYES B., *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*, in *Securing Europe through Counter-Terrorism – Impact, Legitimacy & Effectiveness – Paper*, 2013, p. 1 ss.

KAPLAN J., *Intelligenza artificiale. Guida al futuro prossimo*, Luiss University Press, Roma, 2017.

KONSTADINIDES T., *Wavering between centres of gravity: comment on Ireland v. Parliament and Council*¸ in *European Law Review*, 35, 2010, p. 88 ss.

KONSTADINIDES T., *Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem*, in *European Current Law Issue*, 1, 2012, p. I ss.

KORFF D., BROWN I., *The inadequacy of the EU Commission's draft GDPR adequacy decision on the UK*, in *Data protection and digital competition Blog*, 3 marzo 2021.

KOSTA E., VALCKE P., *Retaining the data retention directive*, in *Computer Law & Security Report*, 22, 2006, p. 370 ss.

KOSTA E., *The way to Luxemburg: national Court decisions on the compatibility of the Data Retention Directive with the rights to privacy and data protection*, in *SCRIPTed*, 3, 2013, p. 339 ss.

KOSTA E., *SSHD v. Watson and Others: a thin nail on the coffin of UK data retention legislation*, in *European Data Protection Law Review*, 4, 2018, p. 520.

KRACK N., *The myth of Pegasus: journalists safety and press freedom as modern chimaera? Story of the abusive use of a military spyware*, in *CiTiP Law Blog*, 27 luglio 2021.

KUHLING J., HEITZER S., *Returning through the national back door? The future of data retention after the ECJ judgement on Directive 2006/24 in the UK and elsewhere*, in *European Law Review*, 2, 2015, p. 263 ss.

KUNER C., *Transborder data flows and data privacy law*, Oxford University Press, Oxford, 2013.

KUNER C., *A super right to data protection? The Irish Facebok case and the future of EU data transfer regulation*, in *LSE Blog*, 24 giugno 2014.

KUNER C., *Reality and illusion in EU data transfer regulation post Schrems*, in *German Law Journal*, 4, 2017, p. 881 ss.

KUNER C., *The Schrems II judgement of the Court of Justice and the future of data transfer regulation*, in *European Law Blog*, 17 luglio 2020.

LA ROCCA E.N., *A margine di una recente sentenza della Corte di Giustizia UE (C-748/18): riflessi sinistri sulla disciplina delle intercettazioni in Italia*, in *Diritti Comparati*, 8 aprile 2021.

LACHMAYER K., *Rethinking Privacy Across Borders: Developing Transnational Rights on Data Privacy*, in *Tilburg Law Review*, 20, 2015, p. 7 ss.

LEFFI M., *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, in *Rivista di Diritti Comparati*, 2, 2017, p. 187 ss.

LEHNER E., *Democrazia e tutela dei dati personali nell'UE: l'evoluzione nella negoziazione sul PNR dopo il Trattato di Lisbona*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli Editore, Santarcangelo di Romagna, 2013, p. 941 ss.

LEMMENS K., *Respect de la vie privée et de la personnalité*, in M. VERDUSSEN, N. BONBLED (a cura di), *Les droits constitutionnels en Belgique*, Bruylant, Bruxelles, 2011, p. 901 ss.

LENAERTS K., *Limits on limitations: the essence of fundamental rights in the EU*, in *German Law Journal*, 20, 2019, p. 781 ss.

LLOYD I., *Data retention*, in *Computer Law & Security Review*, 34, 2018, p. 407 ss.

LOMBARDI G., *Premesse al corso di diritto pubblico comparato. Problemi di metodo*, Giuffrè, Milano, 1986.

LORELLO L., *Il dilemma sicurezza vs. libertà al tempo del terrorismo*, in *Democrazia e Sicurezza*, 2017, p. 1 ss.

LOWE D., *The European Union's passenger name record data Directive 2016/681: is it fit for the purpose?*, in *International Criminal Law Review*, 16, 2016, p. 856 ss.

LUPÁRIA L., *Data Retention e processo penale. Un'occasione mancata per prendere i diritti davvero sul serio*, in *Giurisprudenza penale*, 4, 2019, p. 753 ss.

LYNSKEY O., *The DRD is incompatible with the rights to privacy*, in *Common Market Law Review*, 2014, p. 1789 ss.

LYNSKEY O., *The extraterritorial impact of data protection law through an EU law lens*, in F. FABBRINI, E. CELESTE, J. QUINN (a cura di), *Data protection beyond borders: transatlantic perspectives on extraterritoriality and sovereignity*, Hart, Oxford, 2021, p. 191 ss.

MACASKILL K., *Brexit: potential trade and data implications for digital and fintech industries*, in *International Data Privacy Law*, 1, 2017, p. 3 ss.

MALACARNE A., *Ancora sulle ricadute interne della sentenza della Corte di Giusti-*

zia in materia di acquisizione di tabulati telefonici: il G.i.p. di Roma dichiara il 'non luogo a procedere' sulla richiesta del p.m., in *Sistema Penale*, 5 maggio 2021.

MANTELERO A., *Il costo della privacy tra valore della persona e ragione dell'impresa*, Giuffrè, Milano, 2007.

MANTELERO A., *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, p. 239 ss.

MARCOLINI S., *L'istituto della data retention dopo la sentenza della Corte di giustizia del 2014*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Utet, Milano, 2019, p. 1579 ss.

MARKOU C., *The Cyprus and other EU Courts rulings on data retention: the Directive as a privacy bomb*, in *Computer Law & Security Review*, 28, 2012, p. 468 ss.

MAYER-SCHONBERGER V., CUKIER K., *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà*, Garzanti, Milano, 2013.

MBIOH W.R., *Post-Och Telestyrelsen and Watson and the Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017, p. 273 ss.

MENDEZ M., *Passenger Name Record Agreement*, in *European Constitutional Law Review*, 3, 2007, p. 127 ss.

MENDEZ M., *Opinion 1/15: the Court of Justice meets PNR data (again!),* in *European Papers*, 3, 2017, p. 803 ss.

MESSINA D., *Il Regolamento (EU) 2016/679 in materia di protezione dei dati personali alla luce della vicenda "Cambridge Anlaytica"*, in *Federalismi.it*, 20, 2018, p. 1 ss.

MIADZVETSKAYA J., *Schrems II: on appropriate safeguards and risks of divergent application of EU law*, in *CiTiP Law Blog*, 29 settembre 2020.

MIDIRI F., *La giuridificazione della protezione dei dati in Italia*, in *Giustamm*, 5, 2016.

MIGLIETTI L., *Profilo storico-comparativi del diritto alla privacy*, in *Diritti Comparati*, 4 dicembre 2014.

MILANOVIC M., *The Grand normalization of mass surveillance: ECtHR Grand Chamber judgments in Big Brother Watch and Centrum for Rattvisa*, in *EJIL:Talk!*, 26 maggio 2021.

MILFORD P., *The retention of communications data: a view from industry*, in *Practical Law IP & IT*, 19 novembre 2008, p. 1 ss.

MILLER R.A., *Privacy and power: a transatlantic dialogue in the shadow of the NSA-affair*, Cambridge University Press, Cambridge, 2017.

MITSILEGAS S., *Surveillance and digital privacy in the transatlantic "war on terror": the case for a global privacy regime*, in *Columbia Human Rights Law Review*, 3, 2016, p. 1 ss.

MOBILIO G., *Tecnologie per il riconoscimento facciale. Rischi per i diritti fondamentali e sfide regolative*, Editoriale Scientifica, Napoli, 2021.

MONTUORI L., SIANO M., *Evoluzione del concetto di consenso informato nel mondo digitale e transizione del marketing tradizionale alle attuali sfide della profilazione*, in G. BUSIA, L. LIGUORI, O. POLLICINO (a cura di), *Le nuove frontiere della privacy nelle tecnologie digitali: bilanci e prospettive*, Aracne, Roma, 2017, p. 101 ss.

MORBIDELLI G., PEGORARO L., REPOSO A., VOLPI M., *Diritto pubblico comparato*, Giappichelli, Torino, 2014.

MUNIR A., YASIN S., BAKAR S., *Data retention rules: a dead end*, in *European Data Protection Law Review*, 3, 2017, p. 71 ss.

MURPHY C.C., *Fundamental rights and security: the difficult position of the European judiciary*, in *European Public Law*, 16, 2010, p. 289 ss.

MURPHY C.C., *Romanian Constitutional Court decision n. 1258 of 8th October 2009*, in *Common Market Law Review*, 3, 2010, p. 933 ss.

MURRAY D., FUSSEY P., *Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data*, in *Israel Law Review*, 1, 2019, p. 31 ss.

NAUDTS L., *Belgian Constitutional Court nullifies Belgian Data Retention Law*, in *European Data Protection Law Review*, 3, 2015, p. 208 ss.

NAZZARO G., *Tabulati di traffico storico per finalità di accertamento e repressione dei reati: caratteristiche e tempi di conservazione*, in *Sicurezza e Giustizia*, 3, 2018, p. 56 ss.

NI LOIDEAIN N., *EU data privacy law and serious crime. Data retention and policymaking*, Oxford University Press, Oxford, in corso di pubblicazione.

NIGER S., *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006.

NINO M., *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di data retention*, in *Diritto dell'Unione europea*, 4, 2014, p. 803 ss.

NINO M., *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'informazione e dell'informatica*, 4, 2015, p. 755 ss.

O'LEARY S., *Balancing rights in a digital age*, in *Irish Jurist*, 59, 2018, p. 82 ss.
OJANEN T., *Making the essence of fundamental rights real: the Court of Justice of the EU clarifies the structure of fundamental rights under the Charter*, in *European Constitutional Law Review*, 12, 2016, p. 318 ss.
OJANEN T., *Rights-based review of electronic surveillance after DRI and Schrems in the European Union*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and transatlantic relations*, Hart Publishing, Londra, 2017, p. 13 ss.
ORGANIZZAZIONE PER LA COOPERAZIONE E LO SVILUPPO ECONOMICO (OECD), *Tracking and tracing COVID: protecting privacy and data while using apps and biometrics*, 2020.
OROFINO M., *Diritto alla protezione dei dati personali e sicurezza: osservazioni critiche su una presunta contrapposizione*, in *MediaLaws*, 2, 2018, p. 82 ss.
ORWELL G., *1984*, Secker&Warburg, Londra, 1949.

PAGALLO U., *La tutela della privacy negli Stati Uniti d'America e in Europa*, Giuffrè, Milano, 2008.
PALLARO P., *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffrè, Milano, 2002.
PAOLUCCI F., *Riconoscimento facciale e diritti fondamentali: è la sorveglianza un giusto prezzo da pagare?*, in *MediaLaws*, 1, 2021, p. 204 ss.
PASCUZZI G., *Il diritto alla riservatezza nell'era di Internet*, in AA.VV., *Studi in onore di Piero Schlesinger*, Giuffré, Milano, 2004, p. 337 ss.
PASCUZZI G., *Conoscere comparando: tra tassonomie ed errori cognitivi*, in *Diritto pubblico comparato ed europeo*, 4, 2017, p. 1779 ss.
PASCUZZI G., *Il diritto dell'era digitale*, V Edizione, Il Mulino, Bologna, 2020.
PAVARANI E., *Diritto al rispetto della vita privata e familiare*, in C. DEFILIIPPI, D. BOSI, R. HARVEY (a cura di), *La Convenzione europea dei diritti dell'uomo e delle libertà fondamentali*, ESI, Napoli, 2006, p. 291 ss.
PEARCE H., *Brexit-update: UK-EU data transfers in anticipation of an adequacy decision*, in *University of Portsmouth Blog*, 9 marzo 2021.
PEDILARCO E., *Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione europea-Stati Uniti sul trasferimento dei dati dei passeggeri aerei*, in *Diritto pubblico comparato ed europeo*, 2006, p. 1225 ss.
PEERAER E., *Data retention: the Belgian approach*, in *Masaryk University Journal of Law and Technology*, 1, 2012, p. 121 ss.
PEGORARO L., RINELLA A., *Sistemi costituzionali comparati*, Giappichelli, Torino, 2017.
PERLO N., *La decisione del Consiglio di Stato francese sulla data retention: co-*

me conciliare l'inconciliabile, in *Rivista di Diritti Comparati*, 2, 2021, p. 163 ss.

PETRUCCO F., *The right to privacy and new technologies: between evolution and decay*, in *MediaLaws*, 1, 2019, p. 148 ss.

PEYROU S., *La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques*, in *Journal de Droit Européen*, 2, 2015, p. 395 ss.

PFISTERER V., *The right to privacy. A fundamental right in search of its identity: uncovering the CJEU's flawed concept of the right to privacy*, in *German Law Journal*, 20, 2019, p. 722 ss.

PIN A., *La giustizia costituzionale*, in T.E. FROSINI (a cura di), *Diritto pubblico comparato*, Il Mulino, Bologna, 2019, p. 267 ss.

PINNA M., *Doppio binario di accesso ai dati sul traffico telefonico: una scelta legislativa ragionevole ratificata (con argomenti non irresistibili) dalla Corte costituzionale*, in *Giurisprudenza Costituzionale*, 2006, p. 3929 ss.

PIRODDI P., *Art. 16 TFUE*, in F. POCAR, M.C. BARUFFI (a cura di), *Commentario breve ai Trattati dell'Unione europea*, Cedam, Padova, II Ed., 2014, p. 189 ss.

PIRODDI P., *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo Regolamento generale sulla protezione dei dati,* in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015, p. 827 ss.

PIZZETTI F., *La privacy come diritto fondamentale alla protezione dei dati personali nel Trattato di Lisbona*, in P. BILANCIA, M. D'AMICO (a cura di), *La nuova Europa dopo il Trattato di Lisbona*, Giuffrè, Milano, 2009, p. 83 ss.

PIZZETTI F., *Datagate, Prism, caso Snowden: il mondo tra una nuova grande guerra cibernetica e controllo globale*, in *Federalismi.it*, 13, 2013, p. 1 ss.

PIZZETTI F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino, 2016.

PIZZETTI F. (a cura di), *Intelligenza artificiale, protezione dei dati personali e regolazione*, Giappichelli, Torino, 2018.

PIZZETTI F., *Il nuovo approccio cinese e l'importanza di un mercato unico digitale globale*, in *Agenda Digitale*, 27 agosto 2021.

POLI S., *The legal basis of Internal market measures with a security dimension: comment on case C-301/06, Ireland vs. Parliament/Council*, in *European Constitutional Law Review*, 6, 2010, p. 135 ss.

POLLICINO O., *Internet nella giurisprudenza delle Corti europee: prove di dialogo?*, in www.forumcostituzionale.it, 31 dicembre 2013.

POLLICINO O., *Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo? il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain*, in G. RESTA, V. ZENO-ZENCOVICH (a cura di), *Il diritto al-*

l'oblio su Internet dopo la sentenza Google Spain, Roma TrE-Press, Roma, 2015, p. 7 ss.

POLLICINO O., BASSINI M., *La Corte di Giustizia e una trama ormai nota: la sentenza Tele2 Sverige sulla conservazione dei dati di traffico per finalità di sicurezza e ordine pubblico*, in *Diritto Penale Contemporaneo*, 9 gennaio 2017, p. 1 ss.

POLLICINO O., BASSINI M., *Social network e tutela dei dati personali*, in L. SCAFFARDI (a cura di), *I "profili" del diritto. Regole, rischi e opportunità nell'era digitale*, Giappichelli, Torino, 2018, p. 65 ss.

POLLICINO O., *Diabolical persistence. Thoughts on the Schrems II decision*, in *MediaLaws*, 3, 2020, p. 315 ss.

POLLICINO O., *Data protection and freedom of expression beyond EU borders: EU judicial perspectives*, in F. FABBRINI, E. CELESTE, J. QUINN (a cura di), *Data protection beyond borders: transatlantic perspectives on extraterritoriality and sovereignity*, Hart, Oxford, 2021, p. 81 ss.

POLLICINO O., PAOLUCCI F., *Big Brother (cannot) watch: the Grand Chambeer ruled against surveillance in the Snowden revelation's aftermath*, in *EU-LawLive*, 31 maggio 2021.

PONTIN B., *The environmental case for Brexit. A socio-legal perspective*, Hart, Londra, 2021.

PORCEDDA M.G., *The recrudescence of 'Security v. Privacy' after the 2015 terrorist attacks and the value of privacy rights in the European Union*, in E. ORRÙ, M.G. PORCEDDA, S. WEYDNER-VOLKMANN (a cura di), *Rethinking surveillance and control: beyond the 'security versus privacy' debate*, Nomos, Baden-Baden, 2017, p. 137 ss.

POSNER E., VERMEULEN A., *Terror in balance: security, liberty and the Courts*, Oxford University Press, Cambridge, Massachusetts, 2007.

POULLET Y., *The fight against crime and/or the protection of privacy: a thorny debate!*, in *International Review of Law, Computers and Technology*, 2, 2004, p. 251 ss.

PRIEST D., TIMBERG C., MEKHENNET S., *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, in *The Washington Post*, 1 luglio 2021.

QUEK M.P., *Personal data privacy protection in an age of globalization: the UE-USA Safe Harbour compromise*, in *Journal of European Public Policy*, 3, 2002, p. 325 ss.

QUINN J., *Google v. CNIL: circumscribing the extraterritorial effect*, in F. FABBRINI, E. CELESTE, J. QUINN (a cura di), *Data protection beyond borders:*

transatlantic perspectives on extraterritoriality and sovereignity, Hart, Oxford, 2021, p. 47 ss.

QUINTEL T., *Investigatory Powers Tribunal: Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Ors Part II*, in *European Data Protection Law Review*, 3, 2017, p. 393 ss.

RAGHENO N., *Data protection: la future nouvelle Autorité dee protection des données*, in *Cahier du Juriste*, 2, 2017, p. 29 ss.

RANCHORDAS S., *Constitutional sunsets and experimental legislation*, Elgar, Cheltenham, 2014.

RAUHOFER J., MAC SITHIGH D., *The data retention directive never existed*, in *Scripted* n. 118, 2014, p. 1 ss.

REGAN P.M., *Legislating privacy, technology, social values and public policy*, University of North Carolina Press, Chapel Hill, 1995.

REIDENBERG J., *The transparent citizen,* in *Loyola University Chicago Law Journal*, 47, 2015, p. 437 ss.

RESTA F., *Conservazione dei dati e diritto alla riservatezza. La Corte di giustizia interviene sulla data retention. I riflessi sulla disciplina interna*, in *Giustizia Insieme*, 6 marzo 2021.

RESTA F., *Data retention, che cambia con l'impegno del Governo a adeguare la normativa italiana*, in *AgendaDigitale*, 9 aprile 2021.

RESTA G., *Il diritto alla protezione dei dati personali*, in F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH (a cura di), *Il Codice dei dati personali. Temi e problemi*, Giuffrè, Milano, 2004, p. 23 ss.

RESTA G., ZENO-ZENCOVICH V. (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press, Roma, 2015.

RESTA G., *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE,* in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, p. 23 ss.

RESTA G., SOMMA A., ZENO-ZENCOVICH V. (a cura di), *Comparare. Una riflessione tra le discipline*, Mimesis, Sesto San Giovanni, 2020.

REZENDE I., *Dati esterni alle comunicazioni e processo penale: questioni ancora aperte in tema di* data retention*,* in *Sistema Penale*, 5, 2020, p. 183 ss.

RICCARDI M., *Dati esteriori delle comunicazioni e tabulati di traffico. Il bilanciamento tra privacy e repressione del fenomeno criminale nel dialogo tra giurisprudenza e legislatore*, in *Diritto Penale Contemporaneo*, 3, 2016, p. 156 ss.

RICHARDS N., *The dangers of surveillance*, in *Harvard Law Review*, 126, 2013, p. 1934 ss.

RIDOLA P., *Libertà e diritti nello sviluppo storico del costituzionalismo*, in P. RIDOLA, R. NANIA (a cura di), *I diritti costituzionali*, Giappichelli, Torino, 2006, p. 3 ss.

RIDOLA P., *Diritto comparato e diritto costituzionale europeo*, Giappichelli, Torino, 2010.

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

RODA S., *Shortcomings of the PNR Directive in light of Opinion 1/15 of the Court of Justice of the European Union*, in *European Data Protection Law Review*, 6, 2020, p. 66 ss.

RODOTÀ S., *Tecnologia e diritti*, Il Mulino, Bologna, 1995.

RODOTÀ S., *Privacy, libertà, dignità, discorso conclusivo della Conferenza internazionale sulla protezione dei dati,* www.privacy.it/archivio/rodo20040916.html, 2004.

RODOTÀ S., *Il diritto di avere diritti*, Laterza, Roma-Bari, 2012.

RODOTÀ S., *Il mondo nella rete. Quali i diritti, quali i vincoli,* Laterza, Roma-Bari, 2013.

ROJSZCZAK M., *The uncertain future of data retention laws in EU: is a legislative reset possible?*, in *Computer Law and Security Review*, 41, 2021, p. 1 ss.

ROSENFELD M., *Judicial balancing in times of stress: comparing diverse approaches to the war of terror*, Benjamin N. Cardozo School of Law Working Paper, 5, 2005, p. 2079 ss.

ROSSI DAL POZZO F., *Servizi di trasporto aereo e diritti dei singoli nella disciplina comunitaria*, Giuffrè, Milano, 2008.

ROTENBERG M., KYRIAKIDES E., *Preserving Article 8 in times of crisis*, in F. BIGNAMI (a cura di), *EU law in populist times. Crises and prospects*, Cambridge University Press, Cambridge, 2020, p. 342 ss.

ROUSEAU D., *L'identité constitutionnelle, bouclier de l'identité nationale ou branche de l'etoile europeenne?*, in L. BURGORGUE-LARSEN (a cura di), *L'identité constitutionnelle saisie par les Juge en Europe*, Edition Pedone, Parigi, 2011, p. 89 ss.

ROUVROY A., POULLET Y., *The right to informational self-determination and the value of self-development: reassessing the importance of privacy for democracy*, in S. GUTWIRTH, Y. POULLET, P. DE HERT. C. DE TERWANGNE, S. NOUWT (a cura di), *Reinventing data protection?*, Springer, Berlino, 2009, p. 45 ss.

ROVELLI S., *Case Prokuratuur: proportionality and the independence of authorities in data retention*, in *European Papers*, 6, 2021, p. 199 ss.

ROYER S., CAREEL S., *Access denied. The CJEU raffirms la Quadrature du Net and clarifies requirements for access to retained data*, in *CiTiP Law Blog*, 23 marzo 2021.

RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi),* in *Federalismi.it*, 23, 2016, p. 1 ss.

RUBINSTEIN I., MARGULIES P., *Risk and rights in transatlantic data transfers: EU privacy law, US surveillance and the search for common ground*, in *Roger Williams University Legal Studies Paper*, 18 febbraio 2021, p. 1 ss.

RUFFOLO U. (a cura di), *XXVI lezioni di diritto dell'intelligenza artificiale*, Giappichelli, Torino, 2021.

RUGGERI A., *Dignità dell'uomo, diritto alla riservatezza, strumenti di tutela (prime notazioni)*, in *Consulta Online*, III, 2016, p. 1 ss.

RUGGIERI F., *Data retention e giudice di merito penale. Una discutibile pronuncia*, in *Cassazione Penale*, 6, 2017, p. 2486 ss.

RUHRMANN H., *Facing the future: protecting human rights in policy strategies for facial recognition technology in law enforcement,* University of California Berkeley, Berkeley, 2019.

RUOTOLO M., *La sicurezza nel gioco del bilanciamento*, in *Astrid Rassegna*, 2009.

RUSINOVA V., *A European perspective on privacy and mass surveillance at the crossroad*, Working Papers HSE, 2019, p. 1 ss.

SAJFERT J., *Bulk data interception/retention judgements of the CJEU. A victory and a defeat for privacy*, in *European Law Blog*, 26 ottobre 2020.

SAJFERT J., *Big Brother Watch and Centrum for Rattvisa judgements of the Grand Chamber of the European Court of Human Rights: the altamount of privacy?*, in *European Law Blog*, 8 giugno 2021.

SALVATORE V., *Il diritto al rispetto della vita privata: le sfide digitali, una prospettiva di diritto comparato*, Studio Servizio di Ricerca del Parlamento europeo, PE 628.243, 2018, p. 1 ss. GAMBINI M., *La protezione dei dati personali come diritto fondamentale della persona: meccanismi di tutela*, in *Espaço Juridico*, 1, 2013, p. 149 ss.

SARTORETTI C., *Il regolamento europeo sulla privacy: confini, sovranità e sicurezza al tempo del web,* in *federalismi.it*, 13, 2019, p. 1 ss.

SAULNIER-CASSIA E., *La Directive (UE) 2016/681: miscellanies sur l'utilisation des données des dossier passagers dans l'Union Européenne*, in C. CHEVALLIER GOVERS (a cura di), *L'èchange des données dans l'Espace de liberté, de sécurité et de Justice de l'Union Européenne*, Mare & Martin, 2017, p. 21 ss.

SAVASTANO F., *Uscire dall'UE. Brexit e il diritto di recedere dai Trattati*, Giappichelli, Torino, 2019.

SAXBY S., *European Parliament says 'No!' to Member States'data retention proposal*, in *Computer Law & Security Report*, 21, 2005, p. 279 ss.

SCAFFARDI L., *Nuove tecnologie, prevenzione del crimine e privacy, alla ricerca di un difficile bilanciamento*, in A. TORRE (a cura di), *Costituzioni e sicurezza dello Stato*, Maggioli, Santarcangelo di Romagna, 2013, p. 245 ss.

SCAFFARDI L., *La Data Retention nel Regno Unito e l'Investigatory Powers Act 2016: una legge per il futuro troppo legata al passato*, in *Quaderni costituzionali*, 2, 2017, p. 412 ss.

SCAFFARDI L., *La data retention va in ascensore*, in *Forum di Quaderni costituzionali*, 28 luglio 2017, p. 1 ss.

SCAFFARDI L., *Giustizia genetica e tutela della persona. Uno studio comparato sull'uso (e abuso) delle Banche dati del DNA a fini giudiziari*, Cedam, Padova, 2017.

SCARCIGLIA R., *Metodi e comparazione giuridica*, Cedam, Padova, 2021.

SCHEININ M., *Towards evidence-based discussion on surveillance*, in *European Constitutional Law Review*, 12, 2016, p. 347 ss.

SCHULHOFER S.J., *An international right to privacy? Be careful what you wish for*, in *International Journal of Constitutional Law*, 1, 2016, p. 238 ss.

SCHWARTZ P.M., SOLOVE D., *Reconciling personal information in the United States and European Union*, in *California Law Review*, 102, 2014, p. 1 ss.

SCHWEDA S., *Germany: Parliament adopts new data retention law*, in *European Data Protection Law Review*, 1, 2015, p. 223 ss.

SCUDIERO L., *La Camera porta di soppiatto la data retention a sei anni*, in *Lex Digital*, 21 luglio 2016.

SCUDIERO L., *Data retention a sei anni. La Corte di Giustizia dell'UE la boccerebbe come ha fatto con l'accordo Europa Canada sui PNR*, in *MediaLaws*, 1, 2017, p. 178 ss.

SENOR M., *Un altro 'tango down' in tema di data retention*, in *MediaLaws*, 22 luglio 2015.

SERENA A., *The leviathan, the chains, the lock: dynamics of power in the digital surveillance state*, in *MediaLaws. Law and Media Working Papers Series*, 8, 2017, p. 1 ss.

SESSO SARTI O., *Profilazione e trattamento dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona. Il diritto alla protezione dei dati personali nel Reg. UE 2016/679*, Editoriale Scientifica, Napoli, 2017, p. 574 ss.

SHAFFER G., *Globalization and social protection: the impact of EU and International Rules in the ratcheting up of US data privacy standards*, in *Yale Journal of International Law,* 25, 2000, p. 1 ss.

SICA S., D'ANTONIO V., *I Safe Harbour privacy principles: genesi, contenuti, criticità,* in *Diritto dell'Informazione e dell'Informatica*, 4-5, 2015, p. 801 ss.

SICA S., D'ANTONIO V., *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, RomaTrE-Press, Roma, 2016, p. 137 ss.

SIGNORATO S., *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Giappichelli, Torino, 2018.

SIZAIRE V., FOEGLE J-P., *Les fausses notes du souverainisme juridique. À propos de l'arrêt de l'assemblée du Conseil d'État du 21 avril 2021*, in *Revue des Droits de l'Homme*, giugno 2021, p. 1 ss.

SMITS M., *Comparative law and its influence on national legal systems*, in M. REIMANN, M. ZIMMERMANN (a cura di), *The Oxford handbook of comparative law*, Oxford University Press, Oxford, 2006, p. 513 ss.

SMITH S.W., *Clouds on the horizon: cross-border surveillance under the US CLOUD Act*, in F. FABBRINI, E. CELESTE, J. QUINN (a cura di), *Data protection beyond borders: transatlantic perspectives on extraterritoriality and sovereignity*, Hart, Oxford, 2021, p. 119 ss.

SOLOVE D., *Conceptualizing privacy*, in *California Law Review*, 90, 2002, p. 1088 ss.

SOLOVE D., *Understanding privacy*, Harvard University Press, Cambridge, Massachusetts, 2008.

SOLOVE D., *Nothing to hide. The false trade-off between privacy and security*, Yale University Press, New Haven, 2011.

SORO A., *Democrazia e potere dei dati. libertà, algoritmi e umanesimo digitale*, Baldini+Castoldi, Milano, 2019.

SPATTI M., *Il trasferimento dei dati relativi ai PNR: gli accordi UE con Australia e USA*, in *Diritto del commercio internazionale*, 3, 2013, p. 683 ss.

SPILLER E., *La sentenza Tele2 Sverige: verso una* digital rule of law *europea?*, in *IANUS*, 15, 2017, p. 279 ss.

STAMPANONI BASSI G., *Acquisizioni dei tabulati telefonici e telematici: il Tribunale di Rieti propone questione pregiudiziale alla CGUE*, in *Giurisprudenza Penale*, 13 maggio 2021.

TAYLOR M., *The EU Data Retention Directive*, in *Computer Law & Security Report*, 22, 2006, p. 309 ss.

TERPAN F., *EU-US data transfer from Safe Harbour to Privacy Shield: back to square one?*, in *European Papers*, 3, 2018, p. 1058 ss.

TIBERI G., *L'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura*

elettronica dei passeggeri aerei al vaglio della Corte di giustizia, in *Quaderni costituzionali*, 2006, p. 824 ss.

TIBERI G., *Il diritto alla protezione dei dati personali nelle Carte e nelle Corti sovranazionali (in attesa del Trattato di Lisbona)*, in *Cassazione Penale*, 11, 2009, p. 4467 ss.

TORDI V., *La disciplina italiana in materia di data retention a seguito della sentenza della Corte di giustizia Ue: il Tribunale di Milano nega il contrasto con il diritto sovranazionale*, in *Sistema Penale*, 7 maggio 2021.

TORRE F., *Data retention. Una ventata di "ragionevolezza" da Lussemburgo (a margine della sentenza della Corte di giustizia 2 marzo 2021, C-746/18)*, in *ConsultaOnline*, II, 2021, p. 540 ss.

TORRETTA P., *Diritto alla sicurezza e (altri) diritti e libertà della persona: un complesso bilanciamento costituzionale*, in A. D'ALOIA (a cura di), *Diritti e Costituzione. Profili evolutivi e dimensioni inedite*, Giuffrè, Milano, 2003, p. 451 ss.

TORREZ PEREZ A., *The federalizing force of the EU Charter of Fundamental Rights*, in *International journal of constitutional law*, 4, 2017, p. 1080.

TRACOL X., *Legislative genesis and judicial death of a directive: the European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it*, in *Computer Law & Security Review*, 30, 2014, p. 736 ss.

TRACOL X., *"Invalidator" strikes back: the harbour has never been* safe, in *Computer Law and Security Review*, 3, 2016, p. 1 ss.

TRACOL X., *EU–U.S. Privacy Shield: The saga continues*, in *Computer Law and Security Review*, 32, 2016, p. 775 ss.

TRACOL X., *The judgement of the Grand Chamber dated 21 December 2016 in the two joint Tele2Sverige and Watson cases: the need for a harmonised legal framework on the retention of data at EU level*, in *Comupter Law & Security Review*, 33, 2017, p. 541 ss.

TRACOL X., *Ministerio Fiscal: access of public authorities to personal data retained by providers of electronic communications services*, in *European Data Protection Law Review*, 1, 2019, p. 127 ss.

TROPEA G., *Il contact tracing digitale e l'epidemia: sindrome cinese?*, in *LaCostituzione.info*, 9 aprile 2020.

TRUMMER I., *Liberty v. SSHD & SSFCA: you have the right to remain silent; anything you say will be gathered and retained by the Government*, in *Tulane Journal of International and Comparative Law*, 28, 2020, p. 388 ss.

TZANOU M., *EU regulation of transatlantic data transfers and online surveillance*, in *Human Rights Law Review*, 17, 2015, p. 545 ss.

UBERTAZZI T.M., *Diritto alla privacy, natura e funzioni giuridiche*, Cedam, Padova, 2004.

UNCTAD, *Data protection regulations and international data flows: implications for trade and development*, 2016.

VAINIO N., *Fundamental rights compliance and the politics of interpretation: explaining Member State and Court reactions to Digital Rights Ireland*, in T. BRAUTIGAM, S. MIETTINEN (a cura di), *Data protection, privacy and European regulation in the digital age*, Unigrafia, Helsinki, 2016, p. 229 ss.

VAINIO N., MIETTINEN S., *Telecommunications data retention after DR: legislative and judicial reactions in the Member States*, in *International Journal of Law and Information Technology*, 23, 2015, p. 290 ss.

VAN BELLINGHEN M., ZGAJEWSKI T., *Les enjeux de la transposition en Belgique des nouvelles directives européennes sur les communications électroniques*, Academia Press, Gent, 2012.

VANBERG A.D., MAUNICK M., *Data protection in the UK post-Brexit: the only certainty is uncertainty*, in *International Review of Law, Computers and Technology*, 1, 2018, p. 190 ss.

VANONI L.P., *Il IV emendamento della Costituzione americana tra terrorismo internazionale e datagate: security v. privacy*, in *Federalismi.it*, 1, 2015, p. 1 ss.

VANONI L.P., *Balancing privacy and national security in the global digital era: a comparative perspective of the Eu and US constitutional systems*¸ in L. VIOLINI, A. BARAGGIA (a cura di), *The Fragmented Landscape of Fundamental Rights Protection in Europe: the Role of Judicial and non-Judicial Actors*, Elgar Publish, Cheltenham, 2018, p. 114 ss.

VECCHIO F., *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*, 12 giugno 2014.

VEDASCHI A., *A' la guerre comme à la guerre? La guerra nel diritto pubblico comparato*, Giappichelli, Torino, 2007.

VEDASCHI A., *I programmi di sorveglianza di massa nello Stato di diritto. La data retention al test di legittimità*, in *Diritto pubblico comparato ed europeo*, 3, 2014, p. 1224 ss.

VEDASCHI A., LUBELLO V., *Data Retention and its implications for the fundamental right to privacy*, in *Tilburg Law Review*, 20, 2015, p. 14 ss.

VEDASCHI A., NOBERASCO G.M., *From DRD to PRN: looking for a new balance between privacy and security*, in D. COLE, F. FABBRINI, S. SCHULHOFER (a cura di), *Surveillance, privacy and trans-Atlantic relations*, Hart Publishing, Oxford, 2015, p. 67 ss.

VEDASCHI A., *L'accordo internazionale sui dati dei passeggeri aviotrasportati (PNR) alla luce delle indicazioni della Corte di giustizia dell'Unione Europea*, in *Giurisprudenza Costituzionale*, 4, 2017, p. 1913 ss.

VEDASCHI A., *Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement*, in *International Data Privacy Law*, 2, 2018, p. 124 ss.

VEDASCHI A., *"Customizing" La Quadrature du Net: the French Council of State, national security and data retention*, in *Bridge Blog*, 5 maggio 2021.

VEDASCHI A., *Sicurezza e diritti nella* digital age. *La tecnologia: un'arma a doppio taglio nella lotta al terrorismo internazionale*, in L. LLOREDO ALIX, A. SOMMA (a cura di), *Scritti in onore di Mario G. Losano. Dalla filosofia del diritto alla comparazione giuridica*, Accademia University Press, Torino, 2021, p. 518 ss.

VERBRUGGEN F., ROYER S., SEVERIJNS H., *Reconsidering the blanket-data-retention-taboo, for human rights' sake?*, in *European Law Blog,* 1 ottobre 2018.

VERMEULEN G., *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities*, in G. VERMEULEN, E. LIEVENS (a cura di), *Data protection and privacy under pressure. Transatlantic tensions, EU serveillance and Big Data*, Maklu, Anversa, 2017, p. 49 ss.

VIGEVANI G.E., *Articolo 132*, in AA.VV., *Codice della privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Giuffrè, Milano, 2004, p. 1666 ss.

VIOLANTE T., *Data retention in Portugal*, in M. ZUBIK, J. PODKOWIK, R. RYBSKI (a cura di), *European Constitutional Courts towards data retention laws*, Springer, Berlino, 2020, p. 175 ss.

VIVARELLI A., *The crisis of the rights to informational self-determination*, in *The Italian Law Journal*, 1, 2020, p. 301 ss.

VIZIOLI N., *La giustizia costituzionale in Belgio*, in J. LUTHER, R. ROMBOLI, R. TARCHI (a cura di), *Esperienze di giustizia costituzionale*, Vol. II, Giappichelli, Torino, 2002, p. 411 ss.

VOGIATZOGLOU P., *Data retention tales: the Council of the EU strickes back?*, in *CiTiP Law Blog*, luglio 2019.

VOGIATZOGLOU P., FANTIN S., *National and public security within and beyond the Police Directive*, in A. VEDDER, J. SCHROERS, C. DUCUING, P. VALCKE (a cura di), *Security and Law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*, Intersentia, Bruxelles, 2019, p. 27 ss.

VOGIATZOGLOU P., *Mass surveillance, predictive policing and the implementation*

of the CJEU and ECtHR requirement of objectivity, in *European Journal of Law and Technology*, 1, 2019, p. 1 ss.

VOGIATZOGLOU P., BERGHOLM J., *Privacy International and La Quadrature du Net: the latest on data retention in the name of national and public security*, in *CiTiP Law Blog*, 27 ottobre 2020.

WALKER D., *Data retention in the UK: pragmatic and proportionate or a step too far?*, in *Computer Law and Security Review*, 25, 2009, p. 325 ss.

WALTER C. (a cura di), *Terrorism as challenge for national and international law: security versus liberty?*, Springer, Berlino, 2004.

WARREN S.D., BRANDEIS L.D., *The right to privacy,* in *Harvard Law Review*, 4, 1890, p. 193 ss.

WESTIN A., *Privacy and freedom*, in *Washington and Lee Law Review*, 20, 1968, p. 1 ss.

WESTPHAL D., *German federal constitutional Court delivers roadmap for national data retention laws – without transferral to ECJ*, in *Vienna Journal on International Constitutional Law*, 5, 2011, p. 222 ss.

WHITE M., *Protection by judicial oversight or an oversight in protection?*, in *Journal of Information Rights, Policy and Practice*, 2, 2017, p. 1 ss.

WHITE M., *The Privacy International case in the IPT: respecting the right to privacy?*, in *EU Law Analysis*, 14 settembre 2017.

WHITE M., *Data Retention incompatible with EU law: Victory? Victory you say?*, in *EU Law Analysis*, 24 maggio 2018.

WHITE M., *Is the incompatibility of UK data retention law with EU law really a victory?*, in *Legal Studies*, 41, 2021, p. 130 ss.

WHITMAN J., *The two Western culture of privacy: dignity versus liberty*, in *Yale Law Journal*, 113, 2004, p. 1151 ss.

WIMMER K., JONES J., *Brexit and implications for privacy*, in *Fordham International Law Journal*, 5, 2017, p. 1554 ss.

WOODHAMS S., *Spyware: an unregulated and escalating threat to independent media*, *Center for International Media Assistence*, agosto 2021.

WOODS L., *High Court strikes down data retention laws in ruling on DRIPA*, in *European Data Protection Law Review*, 3, 2015, p. 236 ss.

WOODS L., *Investigatory Powers Tribunal (IPT): Privacy International v. Secretary of State for Foreign and Commonwealth Affairs and Others*, in *European Data Protection Law Review*, 3, 2017, p. 247 ss.

WOODS L., *The Investigatory Powers Act 2016*, in *European Data Protection Law Review*, 3, 2017, p. 103 ss.

WOODS L., *Trasnferring personal data outside the EU: clarification from the ECJ?*, in *EU Law Analysis*, 4 agosto 2017.

WOODS L., *UK: heading towards Brexit but with Data Protection Bill implementing GDPR*, in *European Data Protection Law Review*, 3, 2017, p. 500 ss.
WOODS L., *Mobile phone theft and EU e-privacy law: the CJEU clarifies police powers*, in *EU Law Analysis*, 4 ottobre 2018.
WOODS L., *Data protection, the UK and the EU: the draft adequacy decisions*, in *EU Law Analysis*, 24 febbraio 2021.
WRAY W.B., *A European approach to the United States Constitutional privacy*, in *Craighton International and Comparative Law Review*, 51, 2015, p. 51 ss.

ZAGATO L., *Il trasferimento di dati personali verso Stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*, in *Diritto del commercio internazionale*, 2, 2008, p. 297 ss.
ZALNIERIUTE M., *Developing a European standard for international data trasnfers after Snowden: Opinion 1/15 on the EU-Canada PNR Agreement*, in *Modern Law Review*, 6, 2018, p. 1046 ss.
ZALNIERIUTE M., *The future of data retention regimes and national security in the EU after the Quadrature du Net and Privacy International judgments*, in *Insights*, 28, 2020, p. 1 ss.
ZALNIERIUTE M., *A struggle for competence: national security, surveillance and the scope of EU law at the Court of Justice of the EU*, in *Modern Law Review*, 85, 2021, p. 1 ss.
ZEDNER L., *Why blanket surveillance is no security blanket. Data retention in the United Kingdom after the European Data Retention Directive*, in R.A. MILLER (a cura di), *Privacy and Power. A transatlantic dialogue in the shadow of the NSA-Affair*, Cambridge University Press, Cambridge, 2017, p. 564 ss.
ZENO-ZENCOVICH V., *Intorno alla decisione nel caso Schrems: la sovranità digitale e il governo internazionale delle reti di comunicazione*, in V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma TrE-Press, Roma, 2016, p. 7 ss.
ZENO-ZENCOVICH V., *Dati, grandi dati, dati granulari e la nuova epistemiologia del giurista*, in *MediaLaws*, 2, 2018, p. 32 ss.
ZICCARDI G., *Internet, controllo e libertà. Trasparenza, sorveglianza e segreto nell'era tecnologica*, Raffaello Cortina, Milano, 2015.
ZICCARDI G., *Tecnologie per il potere. Come usare i social network in politica*, Raffaello Cortina, Milano, 2019.
ZILLER J., *Il Conseil d'Etat si rifiuta di seguire il pifferaio magico di Karlsruhe*, in *CERIDAP*, 2, 2021.

Finito di stampare nel mese di settembre 2021
nella Stampatre s.r.l. di Torino
Via Bologna, 220

UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI GIURISPRUDENZA
PUBBLICAZIONI DEL DIPARTIMENTO DI DIRITTO PUBBLICO ITALIANO E SOVRANAZIONALE

Studi di diritto pubblico

Per i tipi di Giuffrè

1. VITTORIO ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni*, 1963, pp. XXII-348.
2. ROBERTO GIANOLIO, *Le occupazioni d'urgenza*, 1963, pp. VII-226.
3. VITTORIO ITALIA, *La denominazione nel diritto pubblico*, 1966, pp. XVII-209.
4. VALERIO ONIDA, *Le leggi di spesa nella Costituzione*, 1969, pp. IV-892.
5. VITTORIO ITALIA, *Gli statuti nel diritto pubblico*. vol. I, *Potestà e norma statutaria*, 1974, pp. XXVI-430.
6. CARLO EMILIO TRAVERSO, *Il partito politico nella Costituzione italiana*, 1969.
7. PIETRO GIUSEPPE GRASSO, *Il principio* nullum crimen sine lege *nella Costituzione italiana*, 1972, pp. XII-372.
8. RICCARDO VILLATA, *L'esecuzione delle decisioni del Consiglio di Stato*, 1971, pp. VIII-636.
9. VITTORIO ITALIA, *Le disposizioni di principio stabilite dal legislatore*, 1970, pp. XVI-366.
10. GIANFRANCO MOR, *Le sanzioni disciplinari ed il principio* nullum crimen sine lege, 1970, ristampa 1974, pp. VIII-224.
11. VITTORIO ITALIA, *La deroga nel diritto pubblico*, 1977, pp. XII-257.
12. RICCARDO VILLATA, *Autorizzazioni amministrative e iniziativa economica privata*, 1974, pp. VIII-212.
13. GIANFRANCO MOR, *Profili dell'amministrazione regionale*, 1974, pp. VIII-244.
14. ALDO BARDUSCO, *La struttura dei contratti delle pubbliche amministrazioni*, 1974, pp. VIII-404.
15. GUIDO GRECO, *Provvedimenti amministrativi costitutivi di rapporti giuridici tra privati*, 1977, pp. IV-406.
16. CARLO EMILIO TRAVERSO, *La tutela costituzionale della persona umana prima della nascita*, 1977, pp. IV-252.
17. ALDO BARDUSCO, *Lo stato regionale italiano*, 1980, pp. IV-252.
18. RICCARDO VILLATA, *«Disapplicazione» dei provvedimenti amministrativi e processo penale*, 1980, pp. IV-176.
19. GUIDO GRECO, *L'accertamento autonomo del rapporto nel giudizio amministrativo*, 1980, pp. IV-256.
20. MARIA LUISA MAZZONI HONORATI, *Il* referendum *nella procedura di revisione costituzionale*, 1982, pp. VIII-168.

21. Carlo Emilio Traverso, *Partito politico e ordinamento costituzionale*, 1983, pp. IV-280.
22. Erminio Ferrari, *I servizi sociali*, vol. I, 1986, pp. XVI-276.
23. Enzo Balboni-Fabrizio D'Addabbo-Antonio D'Andrea-Giovanni Guiglia, *La difficile alternanza. Il sistema parlamentare italiano alla prova (1985-1987)*, 1988, pp. XVI-236.
24. Carlo Enrico Paliero-Aldo Travi, *La sanzione amministrativa*, 1988, pp. XVI-356.
25. Marco Sica, *Effettività della tutela giurisdizionale e provvedimenti d'urgenza*, 1991, pp. XII-352.
26. Giovanni Bognetti, *La cultura giuridica e le facoltà di giurisprudenza a Milano nel secolo ventesimo*, 1991, pp. X-198.
27. Serena Manzin Maestrelli, *Il partito politico nella giurisprudenza del tribunale costituzionale federale tedesco*, 1991, pp. VIII-156.
28. Marta Cartabia, *La tutela dei diritti nel procedimento amministrativo*, 1991, pp. VI-138.
29. Giovanni Bognetti, *Europa in crisi*, 1991, pp. VIII-184.
30. Marilisa D'Amico, *Giudizio sulle leggi ed efficacia temporale delle decisioni di incostituzionalità*, 1993, pp. XIV-182.
31. Giovanni Bognetti, *La costituzione economica italiana. Interpretazione e proposta di riforma*, 1993, pp. X-206.
32. Marilisa D'Amico, *Donna e aborto nella Germania riunificata*, 1994, pp. VIII-286.
33. Gabriella Mangione, *La revisione del* Grundgesetz *in materia di asilo*, 1994, pp. X-106.
34. Giovanni Bognetti, *Costituzione, televisione e legge antitrust*, 1996, pp. VI-136.
35. Luca Antonini, *Dovere tributario, interesse fiscale e diritti costituzionali*, 1996, pp. XII-446.
36. Eugenio Bruti Liberati, *Consenso e funzione nei contratti di diritto pubblico tra amministrazioni e privati*, 1996, pp. X-352.
37. Maurizio Cafagno, *La tutela risarcitoria degli interessi legittimi. Fini pubblici e reazioni di mercato*, 1996, pp. VIII-360.
38. Marco Bignami, *Costituzione flessibile, costituzione rigida e controllo di costituzionalità in Italia (1848-1956)*, 1997, pp. VIII-242.
39. Giovanni Bognetti, *Lo stato e i gruppi di interesse negli ordinamenti borghesi*, 1998, pp. XII-182.
40. Margherita Ramajoli, *Attività amministrativa e disciplina antitrust*, 1998, pp. XII-524.
41. *Norme di correttezza costituzionale, convenzioni ed indirizzo politico*. Atti del Convegno organizzato in ricordo del Prof. Paolo Biscaretti di Ruffia, a cura di Gianfranco Mor, Stefania Ninatti, Quirino Camerlengo e Giulio Enea Vigevani, 1999, pp. VIII-194.
42. Gabriella Mangione, *Il diritto di asilo nell'ordinamento costituzionale tedesco*, 1999, pp. X-262.
43. Alessandra Concaro, *Il sindacato di costituzionalità sul decreto-legge*, 2000, pp. X-198.
44. Maria Elena Gennusa, *La posizione costituzionale dell'opposizione*, 2000, pp. X-316.
45. Luca Antonini, *Il regionalismo differenziato*, 2000, pp. XII-418.

46. *Percorsi e vicende attuali della rappresentanza e della responsabilità politica*. Atti del Convegno - Milano, 16-17 marzo 2000, a cura di Nicolò Zanon e Francesca Biondi, introduzione di Gustavo Zagrebelsky, 2001, pp. XVI-302.
47. MIRYAM IACOMETTI, *I Presidenti di Assemblea parlamentare*, 2001, pp. X-518.
48. *Studi in onore di Umberto Pototschnig*, voll. I e II, 2002, pp. X-1602.
49. *Le trasformazioni dello stato regionale italiano. In ricordo di Gianfranco Mor*, a cura di Vittorio Angiolini, Lorenza Violini, Nicolò Zanon, 2002, pp. X-488.
50. QUIRINO CAMERLENGO, *I fatti normativi e la certezza del diritto costituzionale*, 2002, pp. XIV-444.
51. GIUSEPPE MONACO, *Pubblico ministero ed obbligatorietà dell'azione penale*, 2003, pp. XIV-412.
52. WLADIMIRO TROISE MANGONI, *L'opposizione ordinaria del terzo nel processo amministrativo*, 2004, pp. X-350.
53. FRANCESCO GOISIS, *Contributo allo studio delle società in mano pubblica come persone giuridiche*, 2004, pp. X-396.
54. STEFANIA NINATTI, *Giudicare la democrazia? Processo politico e ideale democratico nella giurisprudenza della Corte di Giustizia Europea*, 2004, pp. XIV-324.
55. *L'incerto federalismo. Le competenze statali e regionali nella giurisprudenza costituzionale*, a cura di Nicolò Zanon e Alessandra Concaro, 2005, pp. VI-424.
56. *Itinerari di sviluppo del regionalismo italiano*. Primo Incontro di Studio "Gianfranco Mor" sul diritto regionale, a cura di Lorenza Violini, con la collaborazione di Quirino Camerlengo, 2005, pp. X-590.
57. *La giustizia costituzionale ed i suoi utenti*. Atti del Convegno internazionale in onore del prof. Valerio Onida - Milano, 15 aprile 2005, a cura di Pasquale Pasquino e Barbara Randazzo, 2006, pp. X-192.
58. QUIRINO CAMERLENGO, *Contributo ad una teoria del diritto costituzionale cosmopolitico*, 2007, pp. X-358.
59. MARCO CUNIBERTI, *Autorità indipendenti e libertà costituzionali*, 2007, pp. XVI-590.
60. MONICA DELSIGNORE, *La compromettibilità in arbitrato nel diritto amministrativo*, 2007, pp. XIV-306.
61. PAOLO PIZZA, *Le società per azioni di diritto singolare tra partecipazioni pubbliche e nuovi modelli organizzativi*, 2007, pp. XVI-698.
62. SARA VALAGUZZA, *La frammentazione della fattispecie nel diritto amministrativo a conformazione europea*, 2008, pp. XXXII-422.
63. LUCA BERTONAZZI, *Il ricorso straordinario al Presidente della Repubblica: persistente attualità e problemi irrisolti del principale istituto di amministrazione giustiziale*, 2008, pp. X-324.
64. BARBARA RANDAZZO, *Diversi ed uguali. Le confessioni religiose davanti alla legge*, 2008, pp. XX-456.
65. *Come decidono le Corti Costituzionali (e altre Corti)* - How Constitutional Cours make decisions. Atti del Convegno internazionale svoltosi a Milano, il 25-26 maggio 2007, a cura di Pasquale Pasquino e Barbara Randazzo, 2009, pp. VIII-232.
66. GIUSEPPE PERICU, *Scritti scelti*, 2009, pp. VI-956.

67. STEFANO CATALANO, *La "presunzione di consonanza". Esecutivo e Consiglio nelle Regioni a statuto ordinario*, 2010, pp. VIII-392.
68. IRENE PELLIZZONE, *Contributo allo studio sul rinvio presidenziale delle leggi*, 2011, pp. XVIII-318.
69. *Verso il decentramento delle politiche di* welfare. Incontro di studio "Gianfranco Mor" sul diritto regionale, a cura di Lorenza Violini, 2011, pp. VIII-504.
70. MONICA DELSIGNORE, *Il contingentamento dell'iniziativa economica privata. Il caso non unico delle farmacie aperte al pubblico*, 2011, pp. VIII-208.
71. SARA VALAGUZZA, *Società miste a partecipazione comunale. Ammissibilità e ambiti*, 2012, pp. X-214.
72. WLADIMIRO TROISE MANGONI, *Il potere sanzionatorio della CONSOB. Profili procedimentali e strumentalità rispetto alla funzione regolatoria*, 2012, pp. VIII-248.
73. FRANCESCA BIONDI, *Il finanziamento pubblico dei partiti politici. Profili costituzionali*, 2012, pp. XIV-232.
74. BARBARA RANDAZZO, *Giustizia costituzionale sovranazionale. La Corte europea dei diritti dell'uomo*, 2012, pp. X-270.
75. GIUSEPPE ARCONZO, *Contributo allo studio sulla funzione legislativa provvedimentale*, 2013, pp. XIV-376.
76. LUCA PIETRO VANONI, *Laicità e libertà di educazione. Il crocifisso nelle aule scolastiche in Italia e in Europa*, 2013, pp. VIII-318.
77. BENEDETTA VIMERCATI, *Consenso informato e incapacità. Gli strumenti di attuazione del diritto costituzionale all'autodeterminazione terapeutica*, 2014, pp. X-346.
78. ELISA FAGNANI, *Tutela dei diritti fondamentali e crisi economica: il caso dell'istruzione. Stato di attuazione, funzioni amministrative e finanziamento del sistema*, 2014, pp. XII-412.
79. *Scritti scelti di Giovanni Bognetti*, a cura di Miryam Iacometti, 2015, pp. XXXVI-530.
80. PAOLO PROVENZANO, *I vizi nella forma e nel procedimento amministrativo. Fra diritto interno e diritto dell'Unione europea*, con prefazione di Diana-Urania Galetta, 2015, pp. XX-332.
81. *Il controllo preventivo dei trattati dell'Unione europea*. Atti del Convegno tenutosi a Milano il 28 maggio 2014, a cura di Nicolò Zanon, 2015, pp. XII-202.
82. STEFANIA LEONE, *Contributo allo studio dello scioglimento anticipato nel sistema costituzionale*, 2016, pp. X-394.
83. ALESSANDRA OSTI, *Teoria e prassi dell'*access to Justice. *Un raffronto tra ordinamento nazionale e ordinamenti esteri*, 2016, pp. X-238.
84. ANNALISA NEGRELLI, *Accesso al mercato e autorizzazioni amministrative nazionali*, 2016, pp. XLII-450.
85. ANTONIA BARAGGIA, *L'autonomia universitaria nel quadro costituzionale italiano ed europeo. Già e non ancora ...*, 2016, pp. XII-268.
86. SARA VALAGUZZA, *Il giudicato amministrativo nella teoria del processo*, 2016, pp. XIII-348.
87. BENEDETTA LIBERALI, *Problematiche costituzionali nelle scelte procreative. Riflessioni intorno alla fecondazione medicalmente assistita e all'interruzione volontaria di gravidanza*, 2017, pp. XVI-772.

88. FILIPPO ROSSI, *La costruzione giuridica del licenziamento. Legislazione, dottrina e prassi fra XIX e XX secolo*, 2017, pp. X-322.
89. *Il diritto all'acqua*, a cura di Lorenza Violini e Barbara Randazzo, 2017, pp. VI-282.
90. FEDERICO GAFFURI, *Il principio di non contestazione nel processo amministrativo*, 2018, pp. XVI-304.

Per i tipi di Giappichelli

91. GIADA RAGONE, Eine empirische Wende? *La Corte costituzionale e le sfide della complessità tecnico-scientifica*, 2020, pp. X-246.
92. LORENZA VIOLINI, *Una forma di Stato a regionalismo differenziato? Percorsi e argomenti per l'attuazione dell'art. 116, III comma, Cost.*, 2021, pp. XVIII-286.
93. *La Costituzione non odia. Conoscere, prevenire e contrastare l'*hate speech on line, a cura di Marilisa D'Amico e Cecilia Siccardi, 2021, pp. XXII-234.
94. GIULIA FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, 2021, pp. XIV-434.

UNIVERSITÀ DEGLI STUDI DI MILANO

FACOLTÀ DI GIURISPRUDENZA
PUBBLICAZIONI DEL DIPARTIMENTO DI DIRITTO PUBBLICO ITALIANO E SOVRANAZIONALE

Studi di diritto pubblico

Per i tipi di Giuffrè

1. VITTORIO ITALIA, *Libertà e segretezza della corrispondenza e delle comunicazioni*, 1963, pp. XXII-348.
2. ROBERTO GIANOLIO, *Le occupazioni d'urgenza*, 1963, pp. VII-226.
3. VITTORIO ITALIA, *La denominazione nel diritto pubblico*, 1966, pp. XVII-209.
4. VALERIO ONIDA, *Le leggi di spesa nella Costituzione*, 1969, pp. IV-892.
5. VITTORIO ITALIA, *Gli statuti nel diritto pubblico*. vol. I, *Potestà e norma statutaria*, 1974, pp. XXVI-430.
6. CARLO EMILIO TRAVERSO, *Il partito politico nella Costituzione italiana*, 1969.
7. PIETRO GIUSEPPE GRASSO, *Il principio* nullum crimen sine lege *nella Costituzione italiana*, 1972, pp. XII-372.
8. RICCARDO VILLATA, *L'esecuzione delle decisioni del Consiglio di Stato*, 1971, pp. VIII-636.
9. VITTORIO ITALIA, *Le disposizioni di principio stabilite dal legislatore*, 1970, pp. XVI-366.
10. GIANFRANCO MOR, *Le sanzioni disciplinari ed il principio* nullum crimen sine lege, 1970, ristampa 1974, pp. VIII-224.
11. VITTORIO ITALIA, *La deroga nel diritto pubblico*, 1977, pp. XII-257.
12. RICCARDO VILLATA, *Autorizzazioni amministrative e iniziativa economica privata*, 1974, pp. VIII-212.
13. GIANFRANCO MOR, *Profili dell'amministrazione regionale*, 1974, pp. VIII-244.
14. ALDO BARDUSCO, *La struttura dei contratti delle pubbliche amministrazioni*, 1974, pp. VIII-404.
15. GUIDO GRECO, *Provvedimenti amministrativi costitutivi di rapporti giuridici tra privati*, 1977, pp. IV-406.
16. CARLO EMILIO TRAVERSO, *La tutela costituzionale della persona umana prima della nascita*, 1977, pp. IV-252.
17. ALDO BARDUSCO, *Lo stato regionale italiano*, 1980, pp. IV-252.
18. RICCARDO VILLATA, *«Disapplicazione» dei provvedimenti amministrativi e processo penale*, 1980, pp. IV-176.
19. GUIDO GRECO, *L'accertamento autonomo del rapporto nel giudizio amministrativo*, 1980, pp. IV-256.
20. MARIA LUISA MAZZONI HONORATI, *Il* referendum *nella procedura di revisione costituzionale*, 1982, pp. VIII-168.

21. Carlo Emilio Traverso, *Partito politico e ordinamento costituzionale*, 1983, pp. IV-280.
22. Erminio Ferrari, *I servizi sociali*, vol. I, 1986, pp. XVI-276.
23. Enzo Balboni-Fabrizio D'Addabbo-Antonio D'Andrea-Giovanni Guiglia, *La difficile alternanza. Il sistema parlamentare italiano alla prova (1985-1987)*, 1988, pp. XVI-236.
24. Carlo Enrico Paliero-Aldo Travi, *La sanzione amministrativa*, 1988, pp. XVI-356.
25. Marco Sica, *Effettività della tutela giurisdizionale e provvedimenti d'urgenza*, 1991, pp. XII-352.
26. Giovanni Bognetti, *La cultura giuridica e le facoltà di giurisprudenza a Milano nel secolo ventesimo*, 1991, pp. X-198.
27. Serena Manzin Maestrelli, *Il partito politico nella giurisprudenza del tribunale costituzionale federale tedesco*, 1991, pp. VIII-156.
28. Marta Cartabia, *La tutela dei diritti nel procedimento amministrativo*, 1991, pp. VI-138.
29. Giovanni Bognetti, *Europa in crisi*, 1991, pp. VIII-184.
30. Marilisa D'Amico, *Giudizio sulle leggi ed efficacia temporale delle decisioni di incostituzionalità*, 1993, pp. XIV-182.
31. Giovanni Bognetti, *La costituzione economica italiana. Interpretazione e proposta di riforma*, 1993, pp. X-206.
32. Marilisa D'Amico, *Donna e aborto nella Germania riunificata*, 1994, pp. VIII-286.
33. Gabriella Mangione, *La revisione del* Grundgesetz *in materia di asilo*, 1994, pp. X-106.
34. Giovanni Bognetti, *Costituzione, televisione e legge antitrust*, 1996, pp. VI-136.
35. Luca Antonini, *Dovere tributario, interesse fiscale e diritti costituzionali*, 1996, pp. XII-446.
36. Eugenio Bruti Liberati, *Consenso e funzione nei contratti di diritto pubblico tra amministrazioni e privati*, 1996, pp. X-352.
37. Maurizio Cafagno, *La tutela risarcitoria degli interessi legittimi. Fini pubblici e reazioni di mercato*, 1996, pp. VIII-360.
38. Marco Bignami, *Costituzione flessibile, costituzione rigida e controllo di costituzionalità in Italia (1848-1956)*, 1997, pp. VIII-242.
39. Giovanni Bognetti, *Lo stato e i gruppi di interesse negli ordinamenti borghesi*, 1998, pp. XII-182.
40. Margherita Ramajoli, *Attività amministrativa e disciplina antitrust*, 1998, pp. XII-524.
41. *Norme di correttezza costituzionale, convenzioni ed indirizzo politico*. Atti del Convegno organizzato in ricordo del Prof. Paolo Biscaretti di Ruffia, a cura di Gianfranco Mor, Stefania Ninatti, Quirino Camerlengo e Giulio Enea Vigevani, 1999, pp. VIII-194.
42. Gabriella Mangione, *Il diritto di asilo nell'ordinamento costituzionale tedesco*, 1999, pp. X-262.
43. Alessandra Concaro, *Il sindacato di costituzionalità sul decreto-legge*, 2000, pp. X-198.
44. Maria Elena Gennusa, *La posizione costituzionale dell'opposizione*, 2000, pp. X-316.
45. Luca Antonini, *Il regionalismo differenziato*, 2000, pp. XII-418.

46. *Percorsi e vicende attuali della rappresentanza e della responsabilità politica*. Atti del Convegno - Milano, 16-17 marzo 2000, a cura di Nicolò Zanon e Francesca Biondi, introduzione di Gustavo Zagrebelsky, 2001, pp. XVI-302.
47. MIRYAM IACOMETTI, *I Presidenti di Assemblea parlamentare*, 2001, pp. X-518.
48. *Studi in onore di Umberto Pototschnig*, voll. I e II, 2002, pp. X-1602.
49. *Le trasformazioni dello stato regionale italiano. In ricordo di Gianfranco Mor*, a cura di Vittorio Angiolini, Lorenza Violini, Nicolò Zanon, 2002, pp. X-488.
50. QUIRINO CAMERLENGO, *I fatti normativi e la certezza del diritto costituzionale*, 2002, pp. XIV-444.
51. GIUSEPPE MONACO, *Pubblico ministero ed obbligatorietà dell'azione penale*, 2003, pp. XIV-412.
52. WLADIMIRO TROISE MANGONI, *L'opposizione ordinaria del terzo nel processo amministrativo*, 2004, pp. X-350.
53. FRANCESCO GOISIS, *Contributo allo studio delle società in mano pubblica come persone giuridiche*, 2004, pp. X-396.
54. STEFANIA NINATTI, *Giudicare la democrazia? Processo politico e ideale democratico nella giurisprudenza della Corte di Giustizia Europea*, 2004, pp. XIV-324.
55. *L'incerto federalismo. Le competenze statali e regionali nella giurisprudenza costituzionale*, a cura di Nicolò Zanon e Alessandra Concaro, 2005, pp. VI-424.
56. *Itinerari di sviluppo del regionalismo italiano*. Primo Incontro di Studio "Gianfranco Mor" sul diritto regionale, a cura di Lorenza Violini, con la collaborazione di Quirino Camerlengo, 2005, pp. X-590.
57. *La giustizia costituzionale ed i suoi utenti*. Atti del Convegno internazionale in onore del prof. Valerio Onida - Milano, 15 aprile 2005, a cura di Pasquale Pasquino e Barbara Randazzo, 2006, pp. X-192.
58. QUIRINO CAMERLENGO, *Contributo ad una teoria del diritto costituzionale cosmopolitico*, 2007, pp. X-358.
59. MARCO CUNIBERTI, *Autorità indipendenti e libertà costituzionali*, 2007, pp. XVI-590.
60. MONICA DELSIGNORE, *La compromettibilità in arbitrato nel diritto amministrativo*, 2007, pp. XIV-306.
61. PAOLO PIZZA, *Le società per azioni di diritto singolare tra partecipazioni pubbliche e nuovi modelli organizzativi*, 2007, pp. XVI-698.
62. SARA VALAGUZZA, *La frammentazione della fattispecie nel diritto amministrativo a conformazione europea*, 2008, pp. XXXII-422.
63. LUCA BERTONAZZI, *Il ricorso straordinario al Presidente della Repubblica: persistente attualità e problemi irrisolti del principale istituto di amministrazione giustiziale*, 2008, pp. X-324.
64. BARBARA RANDAZZO, *Diversi ed uguali. Le confessioni religiose davanti alla legge*, 2008, pp. XX-456.
65. *Come decidono le Corti Costituzionali (e altre Corti)* - How Constitutional Cours make decisions. Atti del Convegno internazionale svoltosi a Milano, il 25-26 maggio 2007, a cura di Pasquale Pasquino e Barbara Randazzo, 2009, pp. VIII-232.
66. GIUSEPPE PERICU, *Scritti scelti*, 2009, pp. VI-956.

67. STEFANO CATALANO, *La "presunzione di consonanza". Esecutivo e Consiglio nelle Regioni a statuto ordinario*, 2010, pp. VIII-392.
68. IRENE PELLIZZONE, *Contributo allo studio sul rinvio presidenziale delle leggi*, 2011, pp. XVIII-318.
69. *Verso il decentramento delle politiche di* welfare. Incontro di studio "Gianfranco Mor" sul diritto regionale, a cura di Lorenza Violini, 2011, pp. VIII-504.
70. MONICA DELSIGNORE, *Il contingentamento dell'iniziativa economica privata. Il caso non unico delle farmacie aperte al pubblico*, 2011, pp. VIII-208.
71. SARA VALAGUZZA, *Società miste a partecipazione comunale. Ammissibilità e ambiti*, 2012, pp. X-214.
72. WLADIMIRO TROISE MANGONI, *Il potere sanzionatorio della CONSOB. Profili procedimentali e strumentalità rispetto alla funzione regolatoria*, 2012, pp. VIII-248.
73. FRANCESCA BIONDI, *Il finanziamento pubblico dei partiti politici. Profili costituzionali*, 2012, pp. XIV-232.
74. BARBARA RANDAZZO, *Giustizia costituzionale sovranazionale. La Corte europea dei diritti dell'uomo*, 2012, pp. X-270.
75. GIUSEPPE ARCONZO, *Contributo allo studio sulla funzione legislativa provvedimentale*, 2013, pp. XIV-376.
76. LUCA PIETRO VANONI, *Laicità e libertà di educazione. Il crocifisso nelle aule scolastiche in Italia e in Europa*, 2013, pp. VIII-318.
77. BENEDETTA VIMERCATI, *Consenso informato e incapacità. Gli strumenti di attuazione del diritto costituzionale all'autodeterminazione terapeutica*, 2014, pp. X-346.
78. ELISA FAGNANI, *Tutela dei diritti fondamentali e crisi economica: il caso dell'istruzione. Stato di attuazione, funzioni amministrative e finanziamento del sistema*, 2014, pp. XII-412.
79. *Scritti scelti di Giovanni Bognetti*, a cura di Miryam Iacometti, 2015, pp. XXXVI-530.
80. PAOLO PROVENZANO, *I vizi nella forma e nel procedimento amministrativo. Fra diritto interno e diritto dell'Unione europea*, con prefazione di Diana-Urania Galetta, 2015, pp. XX-332.
81. *Il controllo preventivo dei trattati dell'Unione europea*. Atti del Convegno tenutosi a Milano il 28 maggio 2014, a cura di Nicolò Zanon, 2015, pp. XII-202.
82. STEFANIA LEONE, *Contributo allo studio dello scioglimento anticipato nel sistema costituzionale*, 2016, pp. X-394.
83. ALESSANDRA OSTI, *Teoria e prassi dell'*access to Justice. *Un raffronto tra ordinamento nazionale e ordinamenti esteri*, 2016, pp. X-238.
84. ANNALISA NEGRELLI, *Accesso al mercato e autorizzazioni amministrative nazionali*, 2016, pp. XLII-450.
85. ANTONIA BARAGGIA, *L'autonomia universitaria nel quadro costituzionale italiano ed europeo. Già e non ancora ...*, 2016, pp. XII-268.
86. SARA VALAGUZZA, *Il giudicato amministrativo nella teoria del processo*, 2016, pp. XIII-348.
87. BENEDETTA LIBERALI, *Problematiche costituzionali nelle scelte procreative. Riflessioni intorno alla fecondazione medicalmente assistita e all'interruzione volontaria di gravidanza*, 2017, pp. XVI-772.

88. FILIPPO ROSSI, *La costruzione giuridica del licenziamento. Legislazione, dottrina e prassi fra XIX e XX secolo*, 2017, pp. X-322.
89. *Il diritto all'acqua*, a cura di Lorenza Violini e Barbara Randazzo, 2017, pp. VI-282.
90. FEDERICO GAFFURI, *Il principio di non contestazione nel processo amministrativo*, 2018, pp. XVI-304.

Per i tipi di Giappichelli

91. GIADA RAGONE, Eine empirische Wende? *La Corte costituzionale e le sfide della complessità tecnico-scientifica*, 2020, pp. X-246.
92. LORENZA VIOLINI, *Una forma di Stato a regionalismo differenziato? Percorsi e argomenti per l'attuazione dell'art. 116, III comma, Cost.*, 2021, pp. XVIII-286.
93. *La Costituzione non odia. Conoscere, prevenire e contrastare l'*hate speech on line, a cura di Marilisa D'Amico e Cecilia Siccardi, 2021, pp. XXII-234.
94. GIULIA FORMICI, *La disciplina della* data retention *tra esigenze securitarie e tutela dei diritti fondamentali. Un'analisi comparata*, 2021, pp. XIV-434.