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

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.