medialaws
Rivista di diritto dei media
2/2018

Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione

Giandonato Caggiano
Professore ordinario di diritto dell'Unione europea, Università degli Studi di Roma Tre

Il bilanciamento tra diritti fondamentali e finalità di sicurezza in materia di conservazione dei dati personali da parte dei fornitori di servizi di comunicazione

Abstract

La conservazione e l'accesso ai dati di traffico delle comunicazioni da parte delle autorità pubbliche è un ambito di complesso bilanciamento tra diritti fondamentali: esigenze di sicurezza da un lato si contemperano con quelle di riservatezza e correttezza del trattamento dei dati, in un contesto di flussi informativi che travalica molto spesso i confini della sovranità nazionale. Il contributo della giurisprudenza, anche sovranazionale, alla definizione del corretto bilanciamento si dimostra come essenziale alla individuazione del corretto bilanciamento, specie di fronte alle esitazioni del legislatore europeo ad armonizzare la materia della *data retention* e alle difficoltà ad applicarla negli scambi con paesi terzi.

Data retention requires balancing a variety of fundamental rights that public authorities seek to on the other one, public authorities must respect privacy and ensure fairness of data processing, often across national jurisdictions. Courts, especially at the EU level, have a prominent role in balancing the different perspectives and rights at stake, given the reluctance to harmonize the matter of data retention by EU legislation and to apply it to third countries.

Sommario

1. Introduzione. - 2. La conservazione dei dati delle comunicazioni elettroniche e i rischi di sorveglianza di massa. - 3. Le sentenze *Digital Rights* e *Google* sul bilanciamento tra diritti fondamentali e sicurezza. - 4. La sentenza *Scherms* e l'invalidità della dichiarazione di adeguatezza della Commissione. - 5. L'interpretazione conforme alla Carta delle legislazioni nazionali nella sentenza *Tele2/Watson*. - 6. La proposta della Commissione di direttiva *e-privacy* che rinuncia all'armonizzazione legislativa in materia e rinvia ai principi generali del Regolamento generale sulla protezione dei dati. - 7. La legge comunitaria 2017 prolunga il termine di conservazione dei dati.

Keyword

Data retention, Conservazione dati, Privacy, Dati personali, Sorveglianza

1. Introduzione

La conservazione e l'accesso delle autorità pubbliche per finalità di sicurezza ai dati di traffico delle comunicazioni (d'ora in poi: *data retention*) si segnalano tra gli aspetti più controversi della tutela multilivello dei diritti fondamentali, sottoposta a crescenti esigenze di bilanciamento con le finalità di sicurezza nel settore della prevenzione e contrasto del terrorismo.

La materia della *data retention* appare particolarmente emblematica della complessità di interazione tra giudici e legislatore sia nell'Unione che negli Stati-membri. Proprio in questo ambito, la Corte di giustizia dimostra di voler consolidare la propria funzione

costituzionale nell'ordinamento dell'Unione[1] e le corti costituzionali di vari Stati membri intervengono sulle legislazioni nazionali[2] mentre il legislatore europeo esita ancora ad adottare una nuova normativa europea di armonizzazione dopo la dichiarazione di invalidità della precedente[3] e il legislatore italiano ha adottato una norma incompatibile con la Carta dei diritti fondamentali, così come interpretata dalla Corte di giustizia[4].
Un quadro ricco di spunti generali sull'evoluzione dell'ordinamento dell'Unione che cercheremo di svolgere nel presente lavoro.

2. La conservazione dei dati delle comunicazioni elettroniche e i rischi di sorveglianza di massa

Sino all'avvento delle comunicazioni digitali, un controllo generalizzato di massa era stato concepito solo da qualche governo dittatoriale[5]. L'ascolto e la visione degli individui in qualsiasi momento della vita sono invece una potenzialità attuale per effetto delle informazioni raccolte nei "centri informatici" dei *service provider* e delle piattaforme di servizi su internet OTT (dai social network ai motori di ricerca)[6]; nonché per il possibile uso di "virus infettanti" di computer e smartphone che li trasformano in strumenti di intercettazione ambientale[7].
Gli operatori privati, spesso localizzati fuori dall'Unione, entrano in contatto con un'enorme quantità di dati personali, che possono riguardare il contenuto oppure l'"invo-

[1] V. *infra*, paragrafi 3, 4 e 5.

[2] Non è possibile in questa sede occuparsi della prospettiva di diritto pubblico comparato, ma appare utile accennare all'entità della tutela costituzionale multilivello in materia. Particolarmente interessante la sentenza del Tribunale costituzionale tedesco (sentenza del 2 marzo 2010, n. 11 (1 BvR 256/08, 1 BvR 586/08, 1 BvR 263/08) che ha dichiarato l'illegittimità delle norme nazionali che prevedevano l'obbligo di conservazione dei dati per un periodo di sei mesi, in assenza di una richiesta originata da indagini preliminari. Secondo molti commentatori, l'argomentazione del Tribunale avrebbe ispirato la sentenza *Digital Rights Ireland* della Corte di giustizia. Già prima della sentenza della Corte di giustizia varie corti costituzionali avevano dichiarato incostituzionali le legislazioni nazionali di attuazione della direttiva *data retention* (Bulgaria, Romania, Repubblica ceca, Cipro), v. T. Konstadinides, *Destroying Democracy on the Ground of Defending It? The Data Retention Directive*, *the Surveillance State and Our Constitutional Ecosystem*, in *European law review*, 2011, 722 ss.

Dopo la sentenza della Corte di giustizia, altre corti costituzionali di vari Stati membri sono intervenute sulle leggi nazionali di conservazione dei dati (Austria, Slovenia, Romania, Slovacchia, Irlanda, Paesi Bassi e Bulgaria, Polonia) o sulle nuove leggi in materia (Belgio). Il quadro della situazione nei vari ordinamenti è descritta da N. Vainio, *Fundamental rights compliance and the politics of interpretation: Explaining Member State and court reactions to* Digital Rights Ireland, in T. Bräutigam - S. Miettinen (eds.), *Data Protection, Privacy and European Regulation in the Digital Age*, Helsinki, December 2016, 229 ss.

[3] V. *infra*, par. 6.

[4] V. *infra*, par. 7.

[5] Sul controllo di massa nella DDR realizzato con varie modalità, ivi comprese le tracce dei vestiti dei fuggitivi da lasciare al fiuto dei cani molecolari, basti richiamare il film *Le vite degli altri*, Regista Henckel von Donnersmarck, Germania, 2006. Tra gli autori di fantascienza, l'Oscar delle citazioni va a G. Orwell, *1984*, 1949 reperibile *on line* in inglese e nella traduzione italiana.

[6] *Over-the-top* è la categoria di servizi di comunicazione di audio, video e altri media su Internet senza il coinvolgimento dell'operatore di rete nel controllo o distribuzione del contenuto (chat, come WhatsApp, Facebook Messenger, WeChat; chiamate in video o in audio, come Skype, Gmail, Viber; servizi di video-streaming, come Netflix, Amazon Prime, YouTube). I servizi sono forniti sotto forma di applicazioni che eseguono il servizio di accesso a Internet. Tali servizi sostituiscono sempre di più la tradizionale telefonia vocale, SMS e posta elettronica con servizi *online* funzionalmente equivalenti

[7] EP STUDY, *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*, PE 583.137, disponibile *online*.

lucro" (d'ora in poi: metadati) delle comunicazioni elettroniche[8].
La conoscenza/consapevolezza dell'esistenza di pratiche legali e illegali, in base alle quali possono essere registrati per anni i dati di persone che non sono sospettati di gravi reati, ha determinato una crescente richiesta di stringenti criteri di (ri)equilibrio tra diritti fondamentali e finalità di sicurezza.
Il fenomeno della registrazione dei dati digitali era però già regolamentato, come vedremo in seguito, sia a livello europeo che nazionale. In linea di principio, la registrazione del contenuto delle comunicazioni deve essere determinata *ex ante* su autorizzazione delle autorità giudiziarie. La registrazione e conservazione di metadati appaiono utili solo *ex-post*, quando subentrino ragioni investigative su una determinata persona, a determinate condizioni fissate dalla legge. In entrambe le fattispecie, la questione giuridica consiste nel bilanciamento degli interessi in gioco da parte del giudice e del legislatore a livello dell'Unione e degli Stati membri. Le due tipologie di dati sono sottoposte dal Trattato di Lisbona alla medesima base giuridica (art. 16 TFUE)[9], ma continuano ad essere oggetto di strumenti diversi di diritto derivato.
Nel settore delle comunicazioni, il riconoscimento della Carta dei diritti quale fonte di diritto primario[10] ha prodotto importanti sviluppi giurisprudenziali che suggeriscono riflessioni generali sul consolidamento del ruolo costituzionale della Corte di giustizia. Oltre che il rispetto del "nucleo essenziale" del diritto alla *privacy* e alla tutela dei dati personali, la Carta impone i principi di necessità e proporzionalità. Il principio del primato e l'idoneità di disposizioni della Carta a produrre un effetto diretto determinano l'obbligo di disapplicare la normativa interna incompatibile.
In premessa, vale la pena di ricordare che le disposizioni contenute nella Carta si applicano a istituzioni, organi e organismi dell'Unione «nel rispetto del principio di sussidia-

[8] Nell'uso degli apparati telefonici fissi o mobili e/o su internet si generano tecnicamente i metadati delle comunicazioni, quali l'origine, la destinazione, la data, l'ora, la durata, la tipologia, gli apparati utilizzati, ecc. Per le comunicazione mobili, si registra l'ubicazione dell'utente tramite la scia delle cellule agganciate lungo il percorso. Così, la nostra "scia o impronta digitale" contiene una grande quantità di informazioni personali, gestibile tramite l'analisi e la profilazione automatizzata delle comunicazioni. Alla definizione di servizio di comunicazioni elettroniche, si aggiungono quelle di "servizi di comunicazione interpersonali", basate sul numero o indipendente dal numero, v. COM(2016) 590 final, 12 ottobre 2016, proposta di direttiva per l'istituzione di un Codice Europeo delle Comunicazioni Elettroniche del 12 ottobre 2016, art. 2.

[9] Per un'analisi, v. B. Cortese, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona*, in *Il Diritto dell'Unione europea*, 2013, 313 ss.

[10] Sul valore e sugli effetti della Carta, dopo l'entrata in vigore del Trattato di Lisbona, la bibliografia è molto ampia. Tra i tanti, G. Di Federico (ed.), *The EU Charter of Fundamental Rights, From Declaration to Binding Instrument*, Dordrecht, 2011; S.I. Sánchez, *The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights*, in *Common Market Law Review*, 2012, 1564 ss.; K. Lenaerts, *The Court's Outer and Inner Selves: Exploring the External and Internal Legitimacy of the European Court of Justice*, in M. Adams–H. De Waele–J. Meeusen–G. Straetmans, *Judging Europe's Judges. The Legitimacy of the Case Law of the European Court of Justice*, Oxford-Portland, 2013, 13 ss.; D. Sarmiento, *Who's Afraid of the Charter? The Court of Justice, National courts, and the new framework of fundamental rights protection in Europe*, in *Common Market Law Review*, 2013, 1267 ss.; K. Ł. Bojarski, D. Schindlauer, K. Wladasch, *The European Charter of Fundamental Rights as a Living Instrument*, Rome-Warsaw-Vienna, 2014; G. Palmisano (a cura di), *Making the Charter of Fundamental Rights a Living Instrument*, Leiden, 2014; Lenaerts–J.A. Gutiérrez-Fons, *The place of the Charter in the EU constitutional edifice*, in S. Peers–T. Hervey–J. Kenner–A. Ward (a cura di), *The EU Charter of fundamental Rights*, Oxford e Portland (OR) 2014, 1559 ss. ; S. de Vries, U. Bernitz, S. Weatherill (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old*, Oxford, 2015; P. Mori, *Autonomia e primato della Carta dei diritti fondamentali dell'Unione europea, in* G. Nesi, P. Gargiulo (a cura di), *Luigi Ferrari Bravo il diritto internazionale come professione*, Trento, 2015, 169 ss.; L.S. Rossi, *"Stesso valore giuridico dei Trattati"? Rango, primato ed effetti diretti della Carta dei diritti fondamentali dell'Unione europea*, in E. Falletti, V. Piccone (a cura di), *Il filo delle tutele nel dedalo d'Europa*, Napoli, 2016, 73 ss.; A. Spadaro, M. Condinanzi, O. Pollicino (a cura di), *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, Torino, 2016.

rietà», come pure agli Stati membri «esclusivamente nell'attuazione del diritto dell'Unione» (art. 51, par. 1) «secondo le rispettive competenze e nel rispetto dei limiti delle competenze conferite all'Unione nei trattati»[11]. Tale criterio definisce l'ambito applicativo della Carta e delimita conseguentemente la competenza interpretativa della Corte. Anche nell'ordinamento dell'Unione, lo "stato di diritto" richiede una corretta dinamica tra giudice e legislatore. In questa sede ci interessa approfondire l'incidenza della Carta rispetto alle due varianti dell'interpretazione pregiudiziale di validità delle disposizioni del diritto derivato[12] e dell'interpretazione pregiudiziale delle fonti derivate e nazionali. Nell'interpretazione pregiudiziale di validità, il monopolio interpretativo spetta alla Corte di giustizia che può dichiarare anche la totale invalidità dell'atto sottoposto al suo giudizio, quando l'incompatibilità con il Trattato, e in particolare con la Carta, ne vizia la legittimità nel suo insieme. Nell'interpretazione pregiudiziale il dialogo tra giudice nazionale e Corte di giustizia si indirizza al giudizio *a quo* ma resta al legislatore nazionale eliminare la norma eventualmente giudicata incompatibile con il diritto dell'Unione.

Il presente lavoro ha per oggetto gli sviluppi più recenti della giurisprudenza della Corte, che hanno rilanciato, tramite decisioni coraggiose e radicali, il processo costituzionale dell'Unione in una materia così sensibile per i diritti fondamentali. Nella nostra analisi ci limiteremo a richiamare gli aspetti istituzionali rilevanti delle sentenze *Digital Rights Ireland* e *Google Spain*, già adeguatamente approfondite in dottrina, per concentrarci invece sulle più recenti sentenze e sulla (in)attività del legislatore dell'Unione in materia[13].

Il presente contributo si concentra sulla tutela dei dati personali nelle comunicazioni elettroniche, escludendo la normativa del settore penale[14] e, pertanto, la direttiva

[11] La Corte ha chiarito che «i diritti fondamentali garantiti nell'ordinamento giuridico dell'Unione si applicano in tutte le situazioni disciplinate dal diritto dell'Unione, ma non al di fuori di esse»: v. sentenza del 26 febbraio 2013, causa C-617/10, *Åklagaren/Hans Åkerberg Fransson*. Sull'obbligo di interpretazione del diritto interno in conformità alla Carta e ai principi generali da parte del giudice nazionale, v. P. Mori, *La "qualità" della legge e la clausola generale di limitazione dell'art. 52, par. 1, della Carta dei diritti fondamentali dell'UE*, in *Il diritto dell'Unione europea*, 2014, 243 ss.; R. Baratta, *Il telos dell'interpretazione conforme all'*acquis *dell'Unione*, in *Rivista di diritto internazionale*, 2015, p. 28 ss., a p. 41 ss.

[12] In materia, v. lo studio di A. Adinolfi, *L'accertamento in via pregiudiziale della validità di atti comunitari*, Milano, 1997. I principi della giurisprudenza in materia sono riportati nella *Nota informativa della Corte di giustizia*, GUUE C 160/2 28 maggio 2011, paragrafi 15, 16 e 17.

[13] Una riflessione specifica sulle due sentenze in parola, come esempi di interpretazione di validità e interpretazione conforme, corredata di opportuni riferimenti ai precedenti giurisprudenziali, è svolta da F. Bestagno, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali*, in *Diritto dell'Unione europea*, 2015, 21 ss. In un successivo articolo, lo stesso Autore (*I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia*, in *Diritti umani e diritto internazionale*, 2015) riflessioni ricostruttive che abbiamo tenuto in considerazione nel corso di questo scritto.

[14] A livello dell'ex-terzo pilastro, v. direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio**,** *GUUE* L 119, 4.5.2016, 89 ss. La conservazione dei dati su ordine giudiziario è uno strumento investigativo previsto e utilizzato dagli Stati firmatari della convenzione del Consiglio d'Europa sulla criminalità informatica, v. art. 16 della Convenzione sulla criminalità informatica - "Convention on Cybercrime" Budapest, 23 November 2001, ETS No.185.

2017/541 sulla lotta contro il terrorismo. Vedremo però in seguito come il legislatore italiano abbia già richiamato tale direttiva per giustificare, in contrasto con le decisioni della Corte di giustizia, la conservazione generalizzata dei metadati delle comunicazioni per un periodo di sei anni[15].

Peraltro, non è possibile in questa sede occuparci di altre categorie di dati personali, quali il PRR dei viaggiatori aerei, i dati finanziari e fiscali e quelli delle agenzie dell'Unione. Così, esula dall'ambito di questo lavoro, l'approfondimento della giurisprudenza della Corte di Strasburgo[16]. Pur non sottovalutando l'importanza del suo contributo, occorre ricordare che, per la Corte di giustizia, «l'esame sulla validità delle disposizioni legislative devono essere effettuate alla sola luce della Carta»[17].

3. Le sentenze *Digital Rights* e *Google* sul bilanciamento tra diritti fondamentali e sicurezza

Nel 1990 Internet non esisteva ancora quando la Commissione propose il primo testo sulla tutela dei dati personali[18], adottato come direttiva 95/46 (in vigore sino al maggio 2018)[19]. La specificità delle comunicazioni elettroniche, rispetto a tale normativa generale, venne disciplinata per la prima volta dalla direttiva 97/66/CE per la salvaguardia della pubblica sicurezza, della difesa o dell'ordine pubblico (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato), e per l'applicazione del diritto penale, che consentiva la conservazione e l'uso di dati a

[15] Direttiva (UE) 2017/541 del Parlamento europeo e del Consiglio, del 15 marzo 2017, sulla lotta contro il terrorismo e che sostituisce la decisione quadro 2002/475/GAI del Consiglio e che modifica la decisione 2005/671/GAI del Consiglio, *GUUE* L 88, 31 marzo 2017, 6 ss., considerando 21.

[16] Per un'analisi della giurisprudenza della Corte di Strasburgo, v. *Opinion 1/2014 of the Article 29 Working Party on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 27 febbraio 2014. Successivamente, *Zakharov v. Russia*, GC, ric. 47143/06, 4 December 2015; *Szabo and Vissy v. Hungary*, ric. 37138/14, 12 January 2016. Per un commento, v. L. Woods, *Zakharov v Russia: Mass Surveillance and the European Court of Human Rights*, in *EU Law Analysis*, 16 December 2015.

I limiti posti dagli articoli 8, par. 2 CEDU e 52, par. 1 Carta sono equivalenti: l'art. 8, par. 2 CEDU esplicita rispetto alla Carta che la limitazione deve essere «necessaria in una società democratica». La condizione dalla CEDU per giustificare la misura e la legittimità delle limitazioni sembra ulteriormente qualificabile con l'esistenza un «bisogno sociale imperioso», idoneo a mettere in crisi il funzionamento stesso della società. Sul dialogo tra le corti sovranazionali europee, v. M. D. Cole, A. Vandendriessche, *From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabb/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance*, in *Eur. Data Prot. L. Rev.*, 2, 2016, 127 ss.; A. Terrasi, *Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo*, in M. Distefano (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, 127 ss.

[17] C 199/11, *Otis and Others*, par. 47, case C 398/13 P, *Inuit Tapiriit Kanatami*, par. 46 and case C-601/15 PPU, par. 46.

[18] Per la originaria proposta, v. COM/90/314 def, 24.9.90, Proposta di direttiva del Consiglio sulla protezione dei dati personali e della vita privata nell'ambito delle reti digitali pubbliche di telecomunicazione, con particolare riferimento all'ISDN (rete digitale integrata nei servizi) e alle reti digitali per servizi pubblici di radiotelefonia mobile.

[19] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, *GUUE* n. L 281 del 23.11.1995, 31 ss.

fini di contrasto[20]. La questione della necessità di bilanciamento tra diritti fondamentali ed esigenze di sicurezza era ben presente al momento dell'adozione della prima disciplina generale delle comunicazioni elettroniche dell'Unione (pacchetto di direttive del 2002), dopo la distruzione delle Torri gemelle[21].

L'adozione della direttiva c.d. *data retention* del 2006[22] apparve necessaria al legislatore europeo dopo gli attacchi terroristici di Madrid e Londra. Essa legittimava la raccolta di metadati da parte dei *service provider* senza alcun collegamento con indagini in corso ma solo nell'eventualità (in nessun modo pronosticabile al momento della raccolta) di "sopravvenienti indagini" collegate alla commissione di gravi reati[23].

Nella storica sentenza *Digital Rights Ireland*[24], la Corte di giustizia sottolinea l'estrema sensibilità dei metadati: «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»[25].

La Corte ha dichiarato invalida l'intera direttiva 2006/24 per violazione dei diritti al

[20] V. direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, *GUUE* L 24 del 30.1.1998, p. 1 ss. (art. 14, par. 1).

[21] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva *e-privacy*), *GUUE* L 201 del 31.07.2002. La direttiva *e-privacy* è stata rivista dalla direttiva 2009/136/CE del Parlamento europeo e del Consiglio del 25 novembre 2009 recante modifica (…) della direttiva 2002/58/CE (…), *GUUE* L 337, 18.12.2009, 11 ss. Per alcuni aspetti della riforma del pacchetto sulle comunicazioni elettroniche del 2019, v. G. Caggiano, *La riforma del regime delle radiofrequenze nel quadro delle comunicazioni elettroniche*, in *Studi sull'integrazione europea*, 2010, 79 ss.; Id, *La regolazione delle reti delle comunicazioni e dell'energia nel diritto dell'Unione europea*, in *Studi sull'integrazione europea*, 2011, 41 ss.

[22] La 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, del 15 marzo 2006, *GUUE* L 105/54 del 13.4.2006, ha previsto l'obbligo degli Stati membri di provvedere affinché determinate categorie di dati (elencati nell'art. 5), siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione. L'attacco terroristico di Londra è esplicitamente richiamato nel decimo considerando della direttiva 2006/24/CE.

[23] La direttiva *data retention*, ancorchè "di fatto" complementare all'indagine e alla prevenzione del crimine, venne giudicata nel 2009 dalla Corte di Giustizia come correttamente adottata sulla base giuridica della realizzazione del mercato (art. 95 TCE, divenuto oggi art. 114 TFUE) perché riferita alle attività dei provider (e non al terzo pilastro), v. sentenza 10 febbraio 2009, C-301/06, *Irlanda c. Parlamento e Consiglio*, sulla scelta della base giuridica della direttiva 2006/24. Per un commento, v. F. Fabbrini, *Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consiglio*, in *Quad. cost.*, 2009, 419 ss.

[24] S. Peers, *Data Retention: A Landmark Court of Justice's Ruling (4) Will this saga continue and how?*, 8 Aprile 2014, in *Eulawanalysis*, 2014: «*The CJEU has seized the chance to give an iconic judgment on the protection of human rights in the EU legal order. Time will deal whether the Digital Rights judgment is seen as the EU's equivalent of classic civil rights judgments of the US Supreme Court, on the desegregation of schools (Brown) or criminal suspects' rights (Miranda). If the Charter ultimately contributes to the development of a 'constitutional patriotism' in the European Union, this judgment will be one of its foundations*».

[25] Corte di giustizia, sentenza *Digital Rights Ireland*, punto 27.

rispetto della vita privata e alla protezione dei dati personali[26]. La sentenza presuppone il rango di diritto primario della Carta senza un esplicito richiamo all'art. 6, par. 1 TUE. La Corte applica il test di necessità in senso stretto a tutte le misure che prevedano limitazioni all'esercizio del diritto alla protezione dei dati personali e al rispetto della vita privata: «derogazioni e limitazioni in relazione alla protezione di dati personali devono essere applicate solamente qualora ciò si riveli strettamente necessario»[27]. La Corte ha sottolineato che «non importa che le informazioni in questione, relative alla vita privata siano dati sensibili o se le persone interessate siano state colpite direttamente»[28].

Secondo la sentenza in parola, «l'obbligo di conservare per un certo periodo dati relativi alla vita privata di una persona e alle sue comunicazioni" e l'accesso delle autorità nazionali competenti ai dati costituiscono di per sé un'ingerenza nei diritti garantiti dalla Carta[29]. Dal punto di vista del *test di necessità in senso stretto*, i criteri di accesso ai dati da parte delle autorità pubbliche (persone autorizzate, uso strettamente necessario, ecc.) devono essere oggetto di scrutinio e analisi approfondita. Inoltre, il *test di proporzionalità* richiede che la misura limitativa sia, da un lato, essenziale al raggiungimento della finalità d'interesse generale; e, dall'altro, il più possibile "meno intrusiva" di altre alternative, quali, ad esempio, controllo sui dati solo di una parte della popolazione o di una zona geografica.

La Corte osserva che la direttiva *data retention* prevede ingerenze nei diritti fondamentali «di vasta portata e di particolare gravità nell'ordinamento giuridico dell'Unione» e non appresta adeguate garanzie[30]. La Corte pondera le finalità di interesse generale cui risponde la disciplina sottoposta al suo esame (principalmente la lotta al terrorismo e alla criminalità), ma all'esito del giudizio di bilanciamento con i diritti fondamentali giudica che tali ingerenze non rispondano al principio di proporzionalità (art. 52. par. 1 della Carta).

La decisione accerta le ingerenze nei diritti protetti dalla Carta, la loro prevalenza rispetto ad altri interessi in gioco e il superamento dei limiti imposti dal rispetto del principio di proporzionalità per l'assenza delle necessarie garanzie (art. 52, par. 1)[31].

---

[26] Sulla sentenza della Corte, v. M. P. 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 *Eur. L. Rev.*, 2014, 835 ss.; O. Lynskey, *The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland*, in *Comm. Mark. L. Rev.*, 2014, 1789 ss.; 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*, 2014, 803 ss.; E. Rossi, *Il diritto alla "privacy" nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa*, in *Dir. com. scambi internaz.*, 2014, 331 ss.; M. Messina, *La Corte di giustizia Ue si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità*, in *Rivista OIDU*, 2014, 396 ss.

[27] *Digital Rights Ireland*, punto 47.

[28] *Digital Rights Ireland*, punto 33.

[29] *Digital Rights Ireland*, punti 34 e 35.

[30] Sentenza *Digital Rights*, cit., punto 37. Per l'affermazione secondo la quale la direttiva 2006/24 «non prevede garanzie sufficienti, come richieste dall'articolo 8 della Carta», v. *ibidem*, punto 66; v. anche il punto 68, ai sensi del quale «non si può ritenere pienamente garantito il controllo da parte di un'autorità indipendente, esplicitamente richiesto dall'articolo 8, paragrafo 3 della Carta, del rispetto dei requisiti di protezione e sicurezza» dei dati medesimi.

[31] L. Woods, *Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber)*, in *EU Law Analysis*, 21 December 2016

Considerata l'ampiezza e pervasività dei profili di contrasto con i diritti in discussione[32], la Corte dichiara l'invalidità totale della direttiva con effetti *ex tunc*[33]. Anche l'Avvocato Generale Cruz Villalón era giunto al medesimo risultato ma sulla base delle carenze del requisito della "previsione legislativa" che difettava, a suo avviso, di sufficiente precisione sulle condizioni di accesso e impiego dei dati conservati[34]. La sentenza, anticipando i temi della giurisprudenza successiva, evoca la necessità di analoghi strumenti di salvaguardia nell'ipotesi in cui la raccolta e la conservazione dei dati siano disposti per motivi di sicurezza da parte di autorità straniere[35].

Nella quasi parallela sentenza *Google*, meno rilevante per la prospettiva del presente lavoro, il riferimento alla Carta nello specifico del diritto all'identità personale (o diritto all'oblio), si riferisce al ruolo dei motori di ricerca nei confronti degli utenti europei, conferendo loro una funzione di cancellazione di alcuni dati personali non più attuali ma conservando un giudizio di seconda istanza alle autorità nazionali indipendenti. La scelta di non richiamare i principi generali dell'ordinamento dell'Unione, né la CEDU, sottolinea il ruolo costituzionale che la Corte di giustizia riconosce alla Carta. La sentenza in parola ribadisce più volte che dei diritti "derivanti" o "risultanti" dalla Carta si deve tener conto nella «ponderazione dei contrapposti diritti e interessi in gioco»[36].

Tuttavia, nella sentenza in parola vale la pena di sottolineare l'ampliamento dell'ambito di applicazione territoriale della direttiva 95/46 sulla tutela dei dati personali. L'interpretazione estensiva è finalizzata ad assicurare garanzie equivalenti ai dati trattati/trasferiti fuori dai confini dell'Unione[37]. Secondo la disciplina in vigore[38], il trasferimento di dati personali da Stati membri dell'Unione verso Paesi-terzi è vietato, a meno che non sia garantito un livello di protezione "adeguato", accertato e validato dalla Com-

[32] La Corte non si è neppure posta la questione di una dichiarazione di invalidità parziale (o di annullamento parziale) per parti "separabili" dell'atto che potrebbe costituire una questione di ricevibilità della domanda pregiudiziale, v. conclusioni dell'AG Juliane Kokott presentate il 23 dicembre 2015, causa C-477/14, *Pillbox* 38 (UK) Limited, paragrafi 13-16 e giurisprudenza ivi citata.

[33] Si noti che la Corte non ha limitato gli effetti nel tempo della dichiarazione di invalidità, come invece aveva chiesto l'avvocato generale.

[34] V. le conclusioni dell'avvocato generale P. Cruz Villalón, presentate il 12 dicembre 2013 in causa *Digital Rights*, spec. al punto 153.

[35] V. *Digital Rights*, punto. 68 che ricorda che «tale direttiva non impone che i dati di cui trattasi siano conservati sul territorio dell'Unione».

[36] Sentenza *Google*, cit., punti 74, 81 e 97 della motivazione e punto 4) del dispositivo.

[37] A tal fine, la Corte ritiene rilevante non tanto il luogo in cui il trattamento dei dati viene fisicamente effettuato, quanto il luogo in cui il motore di ricerca esercita la propria attività, ove apra in uno Stato membro una succursale o una filiale destinata alla promozione e alla vendita degli spazi pubblicitari proposti da tale motore di ricerca e l'attività della quale si dirige agli abitanti di detto Stato membro. L'interpretazione della Corte anticipa così il Regolamento generale sulla protezione dei dati del 2016 che valorizza il criterio di applicabilità della normativa europea al destinatario del servizio e non del criterio della localizzazione del prestatore del servizio, v. art. 3, Campo di applicazione territoriale: «Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento o di un incaricato del trattamento nell'Unione. Il presente regolamento si applica al trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento che non è stabilito nell'Unione […]».

[38] Nel nuovo Regolamento generale del 2016, *cfr.* gli articoli 45 (trasferimento sulla base di una decisione di adeguatezza); 46 (altre garanzie adeguate, comprese le norme vincolanti d'impresa); art. 49 (deroghe in specifiche situazioni).

missione attraverso una specifica decisione[39]. In deroga a tale divieto, il trasferimento verso Paesi-terzi è consentito anche nel caso di consenso della persona interessata, interesse pubblico preminente, ecc., nonché sulla base di adeguati strumenti contrattuali.

4. La sentenza *Scherms* e l'invalidità della dichiarazione di adeguatezza della Commissione

Proprio rispetto al trasferimento dei dati personali dall'Unione europea alle piattaforme di servizi su internet (*social network*), localizzate negli Stati Uniti, il "cammino costituzionale" della Corte di giustizia si perfeziona ulteriormente[40].
Secondo la sentenza *Schrems*[41], i dati personali devono essere improntati all'effettiva osservanza della Carta negli atti dell'Unione, che devono tener conto dell'adeguatezza della tutela di altri ordinamenti giuridici coinvolti nella conservazione dei dati. Secondo la disciplina in vigore (confermata sostanzialmente dal Regolamento generale del 2016), il trasferimento di dati personali da Stati membri dell'Unione verso Paesi-terzi è vietato, a meno che non sia garantito un livello di protezione "adeguato", accertato e validato dalla Commissione attraverso una specifica decisione[42]. In deroga a tale divieto, il trasferimento verso Paesi-terzi è consentito anche nel caso di consenso della persona interessata, interesse pubblico preminente, ecc., nonché sulla base di adeguati

[39] L'Accordo sull'approdo sicuro è un accordo concluso nel 2000 tra Unione europea e Stati Uniti per garantire la protezione dei dati dei cittadini europei, anche quando i dati sono in possesso di imprese americane, fuori dal territorio europeo. Il funzionamento dell'accordo si basava sulla richiesta di autocertificazione alle aziende americane circa il rispetto delle regole sulla protezione dei dati. La Commissione aveva in precedenza valutato che tutte le autorità americane competenti avevano accesso libero ai dati conservati e trattati negli Stati Uniti, v. COM(2013) 847 final sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite.

[40] In argomento v. M. Nino, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012, 147 ss.; D. Bigo et al., *Open Season for Data Fishing in the Web: The Challenges of the US PRISM Programme for the EU*, *Policy Brief*, CEPS, Brussels, June 2013; v. anche Id., *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law*, *Paper in Liberty and Security in Europe*, CEPS, Brussels, November 2013. Per un'ampia disamina delle differenze tra UE e USA in materia di trattamento dei dati per finalità di contrasto della criminalità, si veda F. Bohem, *A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes, Study for the LIBE Committee*, PE 2015; P. M. Schwartz, D. J. Solove, *Reconciling Personal Information in the United States and European Union*, in *California L. Rev.*, 2014, 877; F. Bignami, G. Resta, *Transatlantic Privacy Regulation: Conflict and Cooperation*, in LCP, 2015, 101 ss. Sul sistema statunitense si veda anche F. Bignami, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Study for the LIBE Committee, PE 519.215, May 2015.

[41] Sentenza 6 ottobre 2015, causa C-362/14, *Schrems*. Per un'analisi, v. S. Carrera, E. Guild, *Safe Harbour or into the Storm? EU-US Data Transfers after the Schrems Judgment*, in *CEPS Liberty and Security in Europe Papers*, November 2015. Sulla sentenza e i suoi seguiti, v. V. Zeno-Zencovich, G. Resta (a cura di), *La protezione transnazionale dei dati personali Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, in particolare i contributi di V. Zeno-Zencovich, G. Resta, C. Comella, O. Pollicino-M. Bassini, G. Finocchiaro, P. Piroddi.

[42] L'Accordo sull'approdo sicuro è un accordo concluso nel 2000 tra Unione europea e Stati Uniti per garantire la protezione dei dati dei cittadini europei, anche quando i dati sono in possesso di imprese americane, fuori dal territorio europeo. Il funzionamento dell'accordo si basava sulla richiesta di autocertificazione alle aziende americane circa il rispetto delle regole sulla protezione dei dati. La Commissione ha valutato che le autorità americane avevano accesso libero ai dati conservati e trattati negli Stati Uniti, v. COM(2013) 847 final sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite.

strumenti contrattuali.

Con la sentenza *Scherms*, la Corte di giustizia statuisce l'invalidità della decisione della Commissione classificabile come atto esecutivo di terzo livello dell'ordinamento dell'Unione[43]. I motivi di invalidità si ritrovano, al di là delle assicurazioni offerte a suo tempo dalle autorità statunitensi, nelle modalità effettive di interpretazione e gestione dei dati. In tale ordinamento di destinazione dei dati personali, non erano previste regole idonee a limitare le ingerenze allo "stretto necessario" per conseguire l'obiettivo della protezione della sicurezza nazionale, né specifici rimedi di natura giurisdizionale o amministrativa a tutela dei soggetti interessati. Le deroghe ammissibili avrebbero dovuto essere munite di un meccanismo di controllo indipendente e di mezzi di ricorso adeguati[44]. Pertanto, le ingerenze riscontrate superano di gran lunga quanto strettamente necessario e, nel caso specifico, intaccano il contenuto essenziale del diritto al rispetto della vita privata in un quadro giuridico "affievolito" di tutela. In conclusione, la sorveglianza di massa dei cittadini dell'Unione non è conforme alla Carta[45].

La Corte riafferma solennemente il proprio cammino costituzionale: «[…] secondo la quale l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali[46][…]. La Corte è competente in via esclusiva a dichiarare l'invalidità di un atto dell'Unione […] e la natura esclusiva di tale competenza ha lo scopo di garantire la certezza del diritto assicurando l'applicazione uniforme del diritto dell'Unione[47] […]. Per quanto i giudici nazionali siano effettivamente legittimati ad esaminare la validità di un atto dell'Unione […], essi non sono tuttavia competenti a constatare essi stessi l'invalidità di un siffatto atto[48]. *A fortiori*, in sede di esame di una domanda, […] le autorità nazionali di controllo non sono competenti a constatare esse stesse l'invalidità di una siffatta decisione»[49].

Si tratta della riconferma della giurisprudenza *Foto-Frost*, il cui obbligo di rinvio è parte

[43] Tale decisione veniva impropriamente chiamata "Accordo UE-Usa Safe Harbor" mentre, in realtà, si trattava in sostanza di un atto unilaterale della Commissione a seguito di documentazione presentata dall'Amministrazione Usa.

[44] Le difficoltà derivano dall'impiego che le autorità americane fanno delle deroghe previste dalla disposizione dell'Allegato I, quarto comma.

[45] Sentenza 6 ottobre 2015, cit., par. 93, 94 e 95. In particolare, viene giudicata incompatibile con la Carta (articoli 7 e 8) «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».

[46] Nel testo della sentenza *Scherms*, la Corte cita le sue precedenti sentenze *Commissione e a./Kadi*, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; *Inuit Tapiriit Kanatami e a./Parlamento e Consiglio*, C-583/11 P, EU:C:2013:625, punto 91, nonché *Telefónica/Commissione*, C-274/12 P, EU:C:2013:852, punto 56.

[47] Tra le più recenti vengono citate le sentenze *Melki e Abdeli*, C-188/10 e C-189/10, punto 54, nonché *CIVAD*, C-533/10, punto 40.

[48] La Corte cita in tal senso le sentenze *Foto-Frost*, 314/85, EU:C:1987:452, punti da 15 a 20, nonché *IATA e ELFAA*, C-344/04, EU:C:2006:10, punto 27. Su quest'ultima v. G. Gattinara, *La questione pregiudiziale di validità rispetto al diritto internazionale pattizio secondo la sentenza IATA*, in *SIE*, 2006, 343 ss.

[49] V. paragrafi 60-62.

integrante dell'*acquis* comunitario, nonostante il mancato inserimento nelle varie modifiche dei Trattati istitutivi. In tale giurisprudenza in materia, la Corte aveva più ampiamente motivato che i giudici nazionali non sono competenti a dichiarare l'invalidità degli atti delle istituzioni dell'Unione perché il rinvio pregiudiziale di validità deve garantire l'uniforme applicazione del diritto comunitario da parte dei giudici nazionali, soprattutto quando viene messa in dubbio la validità del diritto dell'Unione. Infatti, le divergenze fra i giudici nazionali su tale validità potrebbero compromettere la stessa unità dell'ordinamento giuridico comunitario e ledere il principio fondamentale della certezza del diritto.

E' importante sottolineare che nella sentenza *Scherms*, la Corte di giustizia dichiara l'invalidità dell'atto in parola, in sede di interpretazione pregiudiziale, senza esserne richiesta esplicitamente dal ricorrente nel procedimento principale né dal giudice di rinvio. Quando una persona si rivolge a un'autorità nazionale di controllo, essa esamina la compatibilità della decisione alla base del trasferimento dei dati con la protezione della vita privata e delle libertà e dei diritti fondamentali della persona: «[…]tali giudici devono sospendere la decisione e investire la Corte di un procedimento pregiudiziale per accertamento di validità, allorché essi ritengono che uno o più motivi di invalidità formulati dalle parti o, eventualmente, sollevati d'ufficio siano fondati »[50]. Come richiamato dall'Avvocato generale[51], «nell'ambito del ricorso per annullamento, la legittimità di un atto deve essere valutata in base alla situazione di fatto e di diritto esistente al momento in cui l'atto è stato adottato, e la valutazione della Commissione può essere criticata solo se essa risulta manifestamente erronea alla luce degli elementi di cui la stessa disponeva al momento dell'adozione dell'atto in questione»[52].

La Corte ha altresì rilevato che garantire l'accesso a rimedi efficaci e un controllo giurisdizionale indipendente costituiscono condizioni essenziali per garantire lo Stato di diritto[53]: «l'esigenza di un controllo giurisdizionale effettivo, destinato ad assicurare il rispetto delle disposizioni del diritto dell'Unione, è inerente all'esistenza di uno Stato di diritto»[54]. Al riguardo, condizione essenziale è il diritto ad ottenere una tutela giurisdizionale (art. 19 TUE ai sensi del quale gli Stati membri hanno l'obbligo di assicurare la tutela giurisdizionale effettiva «nei settori disciplinati dal diritto dell'Unione») e dell'art. 47 della Carta (che influisce sulla interpretazione di molte regole nazionali processuali, ad esempio in materia di diritto alla difesa e al patrocinio legale a spese dello Stato, purché strumentali alla tutela di diritti conferiti da norme dell'Unione).

Decisiva è anche la giurisprudenza sul giusto processo che è applicabile nei procedi-

---

[50] Al riguardo la Corte cita la sentenza *T & L Sugars e Sidul Açúcares/Commissione*, C-456/13 P, EU:C:2015:284, punto 48 e la giurisprudenza ivi citata.

[51] *Ivi*, paragrafi 131 e 132.

[52] V., segnatamente, sentenza *BVGD/Commissione* (T-104/07 e T-339/08, EU:T:2013:366, punto 291), che richiama la sentenza *IECC/Commissione* (C-449/98 P, EU:C:2001:275, punto 87). Sentenza 1° ottobre 2009, C-247/08, *Gaz de France – Berliner Investissement*, EU:C:2009:600, punto 49 e la giurisprudenza ivi citata.

[53] *Schrems*, par. 95.

[54] V, in tal senso, la Corte richiama la propria giurisprudenza al riguardo: sentenze *Les Verts/Parlamento*, 294/83, EU:C:1986:166, punto 23; *Johnston*, 222/84, EU:C:1986:206, punti 18 e 19; *Heylens e a.*, 222/86, EU:C:1987:442, punto 14, nonché *UGTRioja e a.*, da C428/06 a C434/06, EU:C:2008:488, punto 80.

menti dinanzi ai giudici dell'Unione e nei procedimenti che si svolgono davanti ai giudici nazionali quando gli Stati attuano le norme dell'Unione. Secondo la giurisprudenza *Kadi*, [55], tale controllo di legittimità alla luce dei diritti fondamentali assume il valore di "garanzia costituzionale"[56] e riguarda qualsiasi atto dell'Unione. Il sistema di tutela giurisdizionale dei trattati si regge infatti sui due pilastri dei giudici dell'Unione e di quelli nazionali[57]. Quest'ultimi «stabiliscono i rimedi giurisdizionali necessari per assicurare una tutela giurisdizionale effettiva nei settori disciplinati dal diritto dell'Unione, secondo e l'art 47 della Carta»[58].

Una nuova decisione di adeguatezza del trattamento dei dati trasferiti negli Stati è stata adottata da parte della Commissione dopo l'invalidità della precedente decisione, perché era urgente ripristinare le comunicazioni a livello transatlantico[59].

5. L'interpretazione conforme alla Carta delle legislazioni nazionali nella sentenza *Tele2/Watson*

Rispetto all'interpretazione delle disposizioni in materia di *data retention*, la Corte di giustizia è ritornata in argomento nella sentenza *Tele2/Watson* del 21 dicembre 2016[60]. Le controversie *a quo* vertevano sull'obbligo generale imposto in Svezia e nel Regno Unito ai fornitori di servizi di comunicazioni elettroniche sulla base della direttiva *e-privacy* 2002/58 (art.15, par.1), una normativa antecedente alla direttiva *data retention* ma non "travolta" dal giudizio di invalidità di quest'ultima.

Nella sentenza, la Corte di giustizia ha dichiarato che tale disposizione alla luce della Carta (articoli 7, 8, 11 e art. 52, n. 1) osta ad una normativa nazionale che, ai fini della lotta contro la criminalità, prevede la conservazione generale e indiscriminata di tutti i dati di traffico e di localizzazione di tutti gli abbonati e degli utenti registrati relativi a tutti i mezzi di comunicazione elettronica. Sono giudicati incompatibili con gli obblighi di attuazione della Carta, le legislazioni nazionali che prevedano l'obbligo degli operatori di conservazione generalizzata e indifferenziata dei dati personali e consentano,

[55] In tal senso, sentenze *Commissione e a./Kadi*, C-584/10 P, C-593/10 P e C-595/10 P, EU:C:2013:518, punto 66; *Inuit Tapiriit Kanatami e a./Parlamento e Consiglio*, C-583/11 P, EU:C:2013:625, punto 91, nonché *Telefónica/Commissione*, C-274/12 P, EU:C:2013:852, punto 56.

[56] V. sentenze del 29 giugno 2010, *E e F*, C-550/09, Racc. pag. I-6213, punto 44, nonché d26 giugno 2012, *Polonia/Commissione*, C-335/09 P, punto 48.

[57] *Cfr.* sentenza del 3 ottobre 2013, in causa C-583/11 P, *Inuit Tapiriit Kanatami*, cit., punto 90.

[58] *Ivi*, punto 101.

[59] Per il nuovo atto della Commissione, v. Decisione di esecuzione (Ue) 2016/1250 della Commissione del 12 luglio 2016 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy [notificata con il numero C(2016) 4176] C(2016) 4176 final, Allegati da 1 to 7, in *GURI* 29-9-2016 2a Serie speciale - n. 74, 1-112. Sulla decisione, v. WP 238, Opinion 1/2016 on the EU – U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016. Per un commento, v. S. Crespi, *La nuova proposta di decisione di adeguatezza della commissione europea riguardo agli Usa: lo scudo Ue/Usa per la privacy*, in *Eurojus.it*, 2016. Nei confronti della nuova decisione è stato già proposto ricorso dal medesimo ricorrente, v. causa T-670/16, ricorso proposto il 16 settembre 2016, *Digital Rights Ireland/Commissione*.

[60] Sentenza del 21 dicembre 2016 nelle cause riunite C-203/15 e C-698/15, *Tele2 Sverige AB e Tom Watson*. Per un commento, v. I. Cameron, *'A. Court of Justice Balancing data protection and law enforcement needs: Tele2 Sverige and Watson',* in *Common Market Law Review,* 2017, 1467 ss.

senza specifici meccanismi di trasparenza, l'accesso da parte delle autorità nazionali. La conservazione di tali dati deve essere comunque rispettosa del principio di proporzionalità e l'accesso deve essere sottoposto ad un preventivo controllo da parte dei giudici e/o dell'autorità indipendente competente. Si tratta di un'indicazione significativa dell'obbligo di interpretazione conforme alla Carta da parte delle disposizioni nazionali nell'attuazione del diritto dell'Unione.

La direttiva e-*privacy* consente la memorizzazione dei dati soltanto nella misura e per la durata necessaria per la fatturazione dei servizi, per la loro commercializzazione e per la fornitura di servizi a valore aggiunto. Al contrario ne fa divieto senza il consenso dell'utilizzatore interessato, salvo che si verifichino determinate condizioni previste dalla legge (art. 15, n. 1)[61]. La Corte afferma che l'interpretazione di tale deroga relativa a un diritto fondamentale non può che essere restrittiva. L'elencazione degli obiettivi ha carattere esaustivo e non può essere travisata dagli Stati membri: «(…) una disposizione siffatta non può giustificare che la deroga al suddetto obbligo di principio e, in particolare, al divieto di memorizzare tali dati (…), divenga la regola, a pena di privare quest'ultima norma di gran parte della sua portata»[62].

Più in particolare, la sentenza *Tele2/Watson* afferma che è necessario un bilanciamento con i livelli di tutela e l'adozione di modalità operative proporzionate. Il livello di proporzionalità viene applicato al margine di discrezionalità degli Stati membri per la conservazione dei dati e l'accesso da parte delle autorità nazionali competenti. E' incompatibile con il diritto dell'Unione la legislazione nazionale che: non limiti l'accesso ai dati alle sole finalità di lotta contro la criminalità grave, non sottoponga l'accesso ad un controllo preventivo da parte di un giudice o di un'autorità amministrativa indipendente[63]; non esiga che i dati siano conservati nel territorio dell'Unione; non imponga di comunicare appena possibile all'interessato l'avvenuto accesso; non fondi su elementi oggettivi le circostanze in presenza delle quali l'accesso è ammesso[64].

L'Avvocato generale esplicita nuovamente l'ulteriore condizione di ricerca di una misura meno intrusiva che possa offrire la medesima efficacia nella lotta contro i reati gravi[65].

---

[61] L'art. 15, par. 1, prima frase, della direttiva 2002/58 stabilisce che le misure legislative restrittive devono avere come obiettivo «la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica». La medesima disposizione deve essere integrata e interpretata alla luce del rinvio alla direttiva 95/46: «Deroghe e restrizioni: […] una misura necessaria alla salvaguardia: a) della sicurezza dello Stato; b) della difesa; c) della pubblica sicurezza; d) della prevenzione, della ricerca, dell'accertamento e del perseguimento di infrazioni penali o di violazioni della deontologia delle professioni regolamentate; e) di un rilevante interesse economico o finanziario di uno Stato membro o dell'Unione europea, anche in materia monetaria, di bilancio e tributaria; f) di un compito di controllo, ispezione o disciplina connesso, anche occasionalmente, con l'esercizio dei pubblici poteri nei casi di cui alle lettere c), d) ed e); g) della protezione della persona interessata o dei diritti e delle libertà altrui (art. 13, par. 1)».

[62] Par. 89.

[63] *Cfr.* Corte EDU, 12 gennaio 2016, *Szabó e Vissy c. Ungheria*, CE:ECHR:2016:0112JUD003713814, paragrafi 77 e 80.

[64] *Cfr.* Corte EDU, 4 dicembre 2015, *Zakharov c. Russia*, CE:ECHR:2015:1204JUD004714306, par. 260.

[65] Conclusioni dell'Avvocato generale nella causa *Tele2 Sverige AB* (C-203/15 e C-698/15), punti 209 e 211.

La disposizione dichiarata invalida invece non richiede alcuna correlazione tra la conservazione dei dati e l'esistenza di una minaccia per la sicurezza pubblica. La limitazione della conservazione non è prevista «per un periodo di tempo e/o a una zona geografica e/o una cerchia di persone suscettibili di essere implicate in una maniera o in un'altra in una violazione grave, oppure persone che potrebbero, per altri motivi, contribuire, mediante la conservazione dei loro dati, alla lotta contro la criminalità»[66]. Secondo la Corte, l'obiettivo di interesse generale non vale di per sé solo a giustificare una normativa nazionale[67].

6. La proposta della Commissione di direttiva *e-privacy* che rinuncia all'armonizzazione legislativa in materia e rinvia ai principi generali del Regolamento generale sulla protezione dei dati

Le implicazioni della giurisprudenza della Corte di giustizia si prevedono particolarmente interessanti in sede di attuazione delle decisioni a livello dell'Unione e degli ordinamenti nazionali nazionale.

Al riguardo, occorre premettere che la direttiva *data retention*, dichiarata invalida dalla Corte di giustizia nel 2014, non è stata a oggi ancora sostituita.

A seguito delle decisioni della Corte di giustizia, il legislatore dell'Unione e i legislatori nazionali dovranno correggere gli elementi di incompatibilità con la Carta[68]. Le sentenze *Scherms* e *Tele2/Watson* consentono di riconoscere effetti diretti alla regola generale di divieto di conservazione indiscriminata dei dati, salvo che per esigenze specifiche di contrasto ai reati gravi e con il supporto di specifiche garanzie processuali. Ne consegue l'obbligo per i giudici nazionali e la pubblica amministrazione di procedere alla disapplicazione delle norme nazionali contrastanti.

Al riguardo, le eventuali incertezze applicative della dichiarazione di invalidità della direttiva *data retention* sulle norme nazionali (che pure, ex art. 51 della Carta, poteva considerarsi "strettamente collegate" anche se non di trasposizione in senso tecnico) sono da ritenersi superate dalla successiva interpretazione restrittiva svolta direttamente dalla Corte sulle deroghe previste dalla direttiva *e-privacy* tuttora vigente.

Da parte degli Stati-membri, si manifesta una forte "resistenza" a seguire le indicazioni della Corte nel senso di ridimensionare, tramite un'armonizzazione normativa più

[66] *Scherms*, punto 106. Nello stesso senso la sentenza *Digital Rights*, punto 59.

[67] *Scherms*, punto 103. Nello stesso senso sentenza *Digital Rights*, punto 51. Ne consegue il giudizio su tale disposizione: «Una normativa nazionale come quella in discussione nei procedimenti principali travalica dunque i limiti dello stretto necessario e non può essere considerata giustificata, in una società democratica, così come richiede l'articolo 15, paragrafo 1, della direttiva 2002/58, letto alla luce degli articoli 7, 8 e 11 nonché dell'articolo 52, paragrafo 1, della Carta» (*Scherms*, punto 108).

[68] Il Regolamento generale sulla protezione dei dati (GDPR), regolamento UE n. 2016/679) del 24 maggio 2016, mira a rendere maggiormente efficace il livello di tutela dei dati personali trattati nelle comunicazioni elettroniche in accordo con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. In primo luogo, i nuovi servizi offerti mediante Internet e utilizzati da un numero crescente di consumatori, come ad esempio le chiamate VoIP (*Voice over IP*), o la sempre più diffusa messaggistica istantanea non rientrerebbero nel campo di applicazione della direttiva *ePrivacy* né del regolamento 679/2016.

stringente, uno strumento di contrasto. ritenuto strategico per la sicurezza nazional[69]. E' indiscutibile che la conservazione dei metadati è ritenuta da molti Stati membri un "paracadute" importante per la propria sicurezza, consentendo accertamenti *ex-post* sui comportamenti di individui sospettati per reati gravi (comprensivi di quelli di pericolo)[70]. Dal punto di vista dell'interesse pubblico alla sicurezza dello Stato, qualsiasi modalità di conservazione per ordine giudiziario non potrebbe sostituire, in modo altrettanto efficace, la conservazione generalizzata dei "dati storici" in discussione. La conservazione per ordine giudiziario, infatti, non garantisce la possibilità di individuare "tracce precedenti" del reato e ovviamente non fornisce aiuto alle indagini prima che vi sia un soggetto sospettato.

Nella riforma in atto delle comunicazioni elettroniche si manifesta la rinuncia a sostituire la direttiva *data retention* con un altro atto di armonizzazione delle legislazioni nazionali[71]. In discussione, come abbiamo già detto nel corso di questo lavoro, non è però la legittimità dell'obiettivo ma la durata del periodo di conservazione, la necessità e stretta proporzionalità della raccolta, la trasparenza dell'accesso da parte delle Autorità pubbliche, l'esistenza di ricorsi giurisdizionali e amministrativi da parte delle persone coinvolte.

La proposta di aggiornamento della direttiva *e-privacy*, attualmente in discussione al Consiglio e al Parlamento europeo, è incentrata principalmente sull'attività dei *service provider* e non sulla sorveglianza e accesso ai metadati da parte delle Autorità pubbliche. La proposta dovrebbe contenere soltanto un generico rinvio alle limitazioni ammissibili al principio di riservatezza, secondo il Regolamento generale sulla protezione dei dati del 2016 (art. 23). La decisione di non procedere all'armonizzazione aumenta il margine di discrezionalità degli Stati membri e rende più difficile la verifica giurisdizionale dei principi affermati dalla Corte di giustizia.

Secondo le norme proposte, sia il contenuto delle comunicazioni sia i metadati dovranno essere anonimizzati o eliminati in caso di mancato consenso degli utenti, purché non siano necessari per specifiche finalità (*cfr.* art. 6 della proposta di Regolamento). Competente per la violazione delle norme sulle comunicazioni elettroniche

---

[69] Sull'evoluzione del quadro legislativo negli Stati membri, v. FRA, *Data retention across the EU*, disponibile *online*: «*Member States made only limited progress in adopting new legal frameworks for data retention to incorporate the requirements and safeguards set out in the CJEU's case law. Most seem reluctant to amend their national laws to conform to the Digital Rights Ireland and Tele2 judgments. In the meantime, challenges against domestic data retention laws in Member States generally abated, though three characteristic cases challenging data retention were brought in Germany, the Netherlands and the United Kingdom in 2016*».

[70] COM(2011) 225 definitivo, 18.4.2011, Valutazione dell'applicazione della direttiva sulla conservazione dei dati (direttiva 2006/24/CE).

[71] Le implicazioni della sentenza Tele2/Watson sono state analizzate dal servizio giuridico del Consiglio, Doc. Council 5884/11, 1 February 2017 (document partially accessible to the public 29.03.2017), Legal Service to Permanent Representatives Committee, Judgment of the Court of 21 December 2016 in joined Cases C-203/15 and C-698/15 (*Tele2 and Watson*) (Parte III. *Consequences of the judgement for the Council (deleted*). Sulle difficoltà degli Stati-membri a seguire le indicazioni della Corte di giustizia, v. doc. Council 6713/17, 1 March 2017, *Retention of electronic communication data, next steps*, par. 3: «*Many delegations expressed their concerns on the implications of the judgement, which might hinder the effectiveness of the investigations and prosecutions of crimes*». Sul dibattito in seno al Consiglio, Doc. 8798/17, 4 May 2017, Access criteria for competent authorities to retained communication data, Exchange of views; doc. 11107/17, 12 July 2017, Processing and storage of data in the context of the draft ePrivacy Regulation, Introduction and preliminary exchange of views; doc 11110/17, 12 July 2017, Requirements of the Tele 2 judgement regarding data retention, Continuation of discussion;

saranno le Autorità nazionali per la protezione dei dati personali. Per quanto riguarda l'ambito territoriale, la proposta si applica ai servizi forniti agli utenti finali nell'Unione, indipendentemente dal fatto che il fornitore sia stabilito nell'Unione.

Quanto al rispetto dei limiti per la conservazione dei dati nelle legislazioni nazionali non contiene disposizioni di armonizzazione ma contiene una clausola generale che rinvia agli Stati membri di legiferare sulle restrizioni della portata dei diritti e degli obblighi previsti purchè «siffatta limitazione rispetta l'essenza dei diritti e delle libertà fondamentali e costituisce una misura necessaria, appropriata e proporzionata in una società democratica intesa a salvaguardare uno o più interessi pubblici» in conformità al Regolamento generale del 2016[72].

Infatti, anche se la direttiva *data retention* è stata dichiarata invalida dalla Corte di giustizia, molti Stati membri continuano ad applicare le normative nazionali adottate in attuazione di tale direttiva o comunque ispirate da principi e meccanismi dichiarati illegittimi. Gli Stati membri sono pertanto liberi di mantenere o creare quadri di riferimento nazionali in materia di conservazione dei dati che prevedano fra l'altro misure di conservazione mirate, purché essi siano conformi al diritto dell'Unione e tengano conto della giurisprudenza della Corte di giustizia sull'interpretazione della direttiva sulla vita privata elettronica e della carta dei diritti fondamentali[73]. Non ci appare che questa formula di salvaguardia sia efficace quanto potrebbe essere l'adozione di un atto di armonizzazione delle legislazioni nazionali che fissi il periodo massimo ammissibile di conservazione dei dati, le procedure di accesso delle autorità pubbliche, le garanzie di controllo, ecc.

E' evidente che se il legislatore europeo si limitasse alla semplice indicazione dei criteri in parola segnerebbe un regresso nella tutela sostanziale dei diritti fondamentali. Soprattutto ci sembra che la scelta del legislatore dell'Unione di non sostituire la direttiva *data retention* manifesti la volontà degli Stati membri di ridurre il preteso "attivismo giudiziario" della Corte di giustizia.

Quest'ultima potrà certo continuare a reiterare le proprie indicazioni nel contesto del rinvio pregiudiziale sulla compatibilità con il diritto dell'Unione delle singole legislazioni nazionali, come ha fatto nella sentenza *Tele2* nei confronti di Svezia e Regno Unito, chiedendo al giudice nazionale di verificarne i presupposti nel procedimento principale a livello nazionale.

La materia della *data retention* continuerà infatti a far parte del «campo di applicazione del diritto dell'Unione», anche in assenza di un'articolata armonizzazione legislativa.

In ogni caso, i giudici nazionali saranno tenuti a disapplicare quegli aspetti delle legislazioni nazionali che appaiono loro incompatibili con i criteri previsti dal Regolamento del 2016 e ribaditi nella proposta di nuova direttiva *e-privacy* .Tuttavia, a nostro avviso, i giudici nazionali saranno piuttosto propensi a rivolgersi alla propria Corte costituzionale, creando occasioni di divergenza interpretativa delle disposizioni in materia di *data*

[72] Proposta di art. 11, che rinvia alle definizioni dell'art. 23, par. 1, lett. da a) a e), del regolamento (UE) 2016/679, in relazione al monitoraggio, ispezione o funzione regolamentare. In base a procedure che saranno stabilite dalla legislazione degli Stati membri, i fornitori di servizi di comunicazione elettronica forniranno alla competente autorità di controllo informazioni sulle procedure di accesso, sul numero di richieste ricevute, sui motivi legali addotti e sulla loro risposta.

[73] V. considerando 26.

retention.

7. La legge comunitaria 2017 prolunga il termine di conservazione dei dati

Da ultimo merita un accenno il caso dell'ordinamento italiano in cui è in vigore un obbligo generale di conservazione all'art. 132 del Codice della privacy, rivisto nel 2008 a seguito dell'adozione della direttiva *data retention*[74]. Tale disposizione resta in vigore in quanto non è stata rimossa dal legislatore italiano e i giudici italiani in questo periodo sono rimasti "sordi" alle indicazioni della Corte di giustizia[75]. In senso contrario, i termini di conservazione vengono progressivamente prolungati dal legislatore italiano. In deroga alla disposizione in parola, la legge comunitaria del 2017 prevede che i gestori del traffico telefonico e telematico conservino per settantadue mesi, senza meccanismi di consenso o regole di accesso delle Autorità pubbliche, i dati di traffico telefonico e telematico, nonché i dati relativi alle chiamate senza risposta (art. 24)[76]. La finalità dichiarata è quella di garantire strumenti di indagine efficaci in considerazione delle straordinarie esigenze di contrasto del terrorismo e degli altri gravi reati indicati, specificando che in tal modo si darebbe attuazione alla direttiva 2017/541/UE sulla lotta contro il terrorismo[77], in particolare all'obbligo di adottare misure necessarie affinché le autorità competenti dispongano di "strumenti di indagine efficaci" (art. 20)[78]. Più che di un anticipo sui termini di attuazione della direttiva 2017/541 si tratta del prolungamento della normativa italiana antiterrorismo che imponeva l'obbligo di conservazione dei dati relativi al traffico telefonico o telematico conservati dagli operatori dei servizi di telecomunicazione[79].
La nuova previsione sembra in evidente contrasto con le sentenze della Corte di giu-

[74] Sui possibili effetti delle sentenze della Corte di giustizia nell'ordinamento italiano, v. F. Iovene, *"Data retention" tra passato e futuro. Ma quale presente?,* in *Cass. penale*, 2014, 4274 ss.; A. Arena, *La Corte di giustizia sulla conservazione dei dati: quali conseguenze per le misure nazionali di recepimento?*, in *Quad. cost.*, 2014, 722 ss.; 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 *Dir. informaz. informatica*, 2014, 775 ss.; S. Crespi, *Diritti fondamentali, Corte di Giustizia e riforma del sistema UE di protezione dei dati*, in *Riv. it. dir. pubbl. com.*, 2015, 819 ss., spec. par. 6.

[75] R. Flor, *Data retention ed art. 132 cod. privacy: vexata quaestio (?)*, in *Dir. pen. cont.* (www.penalecontemporaneo.it), 9 marzo 2017 (Nota a Trib. Padova, ord. 15 marzo 2017). Secondo l'Autore, che critica fortemente tale sentenza, si tratta di uno dei rari casi conosciuti nella giurisprudenza italiana.

[76] V. Legislatura 17ª, Aula, Resoconto stenografico della seduta n. 894 del 10.10.2017, discussione e approvazione del disegno di legge n. 2886.

[77] La direttiva prevede una normativa complessa e articolata il cui termine di recepimento scade l'8 settembre 2018. Nessun'altra disposizione della direttiva è fatta oggetto di attuazione.

[78] L'A.S. 2886 è stato esaminato dalla 14a Commissione permanente del Senato della Repubblica tra il 14 edil 27 settembre 2017 e approvato senza modifiche rispetto al testo trasmesso dalla Camera dei deputati (A.S. 2886-A).

[79] L'articolo 4-*bis* della legge 17 aprile 2015, n. 43, che disciplina la conservazione dei dati di traffico telefonico o telematico. Tale norma è stata modificato dal decreto-legge 30 dicembre 2015, n. 210, conv. con modif. dalla l. 25 febbraio 2016, n. 21, che ha prorogato al 30 giugno 2017 il termine di conservazione dei dati relativi al traffico telefonico o telematico per le finalità di accertamento e di repressione di alcuni reati. Solo una norma si riferisce al terrorismo (art. 51, comma 3-quater, c.p.p), mentre le altre fattispecie richiamate riguardano altri reati gravi (art. 407, comma 2, lett. a), c.p.p).

stizia, indicate nel presente lavoro, che restringono i margini di conservazione di questi dati, ancorandoli al principio di necessarietà e proporzionalità in senso stretto, e che certamente non consentono un periodo così lungo di conservazione dei metadati.

Come citare il contributo: 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 – Rivista dir. media*, 2018, n. 2, in corso di pubblicazione