https://doi.org/10.6092/issn.1825-1927/17110 ISSN 1825-1927

Conservazione e Circolazione delle Informazioni per fini Investigativi

Condizioni e Garanzie in materia di Protezione dei Dati Personali

Lucia Di Crescenzo*

Abstract. È noto come il *cyber-spazio* sia diventato luogo di elaborazione e veicolazione di attività illecite. Pertanto, il 12 maggio 2022 è stato aperto alla firma il Secondo Protocollo aggiuntivo alla Convenzione di Budapest sulla cooperazione rafforzata e la divulgazione delle prove elettroniche considerato il timore che queste ultime – così come si legge nel Preambolo – potrebbero essere archiviate in giurisdizioni estere, diverse, mutevoli o sconosciute. Inevitabilmente, ad essere minato è anche il superiore diritto alla riservatezza. Tra i punti di contatto comuni al Protocollo e al GDPR figura, non a caso, l'*accountability*. Interessante sarà chiarire come tale obbligo di "rendicontazione" potrà bilanciarsi con l'esigenza, altrettanto avvertita, di perseguimento e repressione dei reati.

Parole chiave: riservatezza, accountability, proporzionalità, prova, circolazione, bilanciamento.

1 La finalità legittimamente perseguita: applicazione del principio di proporzionalità

Al fine di comprendere il tema che ci occupa occorre acquisire maggiore consapevolezza rispetto all'insorgenza di un nuovo ambito di riservatezza che si collega al forte impatto delle tecnologie informatiche[1] sulla società contemporanea e sul diritto.

Si assiste sempre più all'affermazione di un diritto all'autodeterminazione informativa dove all'originaria sequenza "persona-informazione-segretezza" si sostituisce quella più appropriata: "persona-informazione-circolazione-controllo".

Il riferimento è alla riservatezza dell'individuo che svolge la propria personalità in un altro luogo, rappresentato dal sistema informatico, a prescindere dalla natura strettamente personale e confidenziale delle informazioni che si potrebbero raccogliere.

Al fine di rinvenire un fondamento costituzionale del diritto alla riservatezza, per gli ordinamenti interni potrebbe essere insufficiente il riferimento alle sole norme costituzionali – per l'Italia, si pensi all'art. 2 Cost. inteso come fattispecie aperta, fonte di nuovi diritti della personalità, che sconta il limite dell'omessa individuazione delle illegittime ingerenze pubbliche, a differenza di altre previsioni contenute negli artt. 13, 14, 15 della Carta costituzionale – pertanto, appare doveroso, integrare tali disposizioni

* Cultrice della materia in Diritto Processuale Penale Comparato presso il Dipartimento di Scienze Giuridiche – Scuola di Giurisprudenza, Università degli Studi di Salerno. Cultrice della materia in Informatica Giuridica presso l'Università telematica Giustino Fortunato; ✉ luciadicrescenzo2020@gmail.com

1. Per informatica si intende la scienza che si occupa dell'elaborazione, della conservazione e della trasmissione di dati attraverso elaboratori elettronici mentre, con il termine computer forensics si fa riferimento alla disciplina che si occupa delle tecniche e degli strumenti usati per recuperare gli elementi di prova digitali all'interno di un elaboratore elettronico. Per le distinzioni create, a livello dottrinale, in base all'oggetto di analisi della computer forensics, cfr. S. Aterno, 2008, *Acquisizione e analisi della prova informatica*, in *Dir. pen. proc*., Dossier, p. 60; F. Cajani, S. Aterno, 2011, *Aspetti giuridici comuni delle indagini informatiche*, in S. Aterno, F. Cajani, G. Costabile, M. Attiucci, G. Mazzaraco, *Computer forensics e indagini digitali*, Experta, Milano; G. Braghò, 2005, *Le indagini informatiche tra esigenze di accertamento e garanzie di difesa*, in *Dir. inf. e informatica*, p. 524 ss.; F. Corona, 2021, *Il cybercrime: soggetto, oggetto e condotta, in Reati informatici e investigazioni digitali*, F. Corona (a cura di), Pacini Giuridica, Pisa, p. 19; G. Dalia, *I reati informatici*, 2016, in AA.VV. *Manuale di diritto dell'informatica*, Edizioni Scientifiche Italiane, p. 657-689; K. La Regina, 2020, *Le indagini su dispositivi digitali*, in *Investigazioni digitali* (a cura di Michele Iaselli), p. 28-72.

con l'art. 8 CEDU[2], così come interpretato dalla Corte di Strasburgo, che individua i parametri di legittimità dell'ingerenza pubblica nel diritto alla vita privata[3].

Ai sensi del paragrafo 2 le ingerenze dell'autorità sono legittime in presenza di tre requisiti: una previsione legislativa; il perseguimento di una delle finalità legittime previste tassativamente dalla norma; la necessità della misura, in una società democratica, per il conseguimento degli obiettivi prefissati.

In quest'ultima prospettiva della "necessità" si inserisce il criterio della proporzionalità tra ingerenza e finalità legittima perseguita: come vedremo, la Corte di giustizia dell'UE, in diverse occasioni, ha confermato che il diritto dell'Unione osta a regolamentazioni nazionali che impongano a un fornitore di servizi di comunicazione elettronica, al fine di combattere le violazioni in generale o salvaguardare la sicurezza nazionale, la trasmissione o archiviazione generalizzata e indifferenziata dei dati relativi al traffico e all'ubicazione, precisando, altresì, che per quanto riguarda la lotta contro i reati gravi[4], uno Stato membro può anche prevedere la conservazione mirata di tali dati nonché la loro rapida trasmissione ove tale interferenza con i diritti fondamentali sia accompagnata da adeguato controllo giurisdizionale[5].

È evidente, quindi, che per l'enorme capacità di archiviazione dei supporti informatici su cui sono memorizzati e per l'assenza di barriere fisiche alla trasmissione degli stessi sui circuiti telematici, i dati digitali pongono evidenti problemi di tutela della riservatezza individuale.

Ciò ha determinato la nascita di un nuovo concetto di privacy che ha ad oggetto le informazioni personali trattate con i mezzi informatici e riguarda la possibilità di accesso, controllo e trattamento dei dati in tale contesto.

Simile diritto soggettivo, tuttavia, deve essere bilanciato con l'esigenza di dotare gli organi inquirenti di efficaci strumenti investigativi per la repressione dei reati[6].

Il diritto alla riservatezza nell'ambito delle indagini digitali sempre più spesso subisce una compressione in occasione del cd. *tracing* (o "tracciamento"), espressione con cui si indica il "percorso a ritroso" finalizzato a trovare l'origine della condotta di reato posta in essere con strumenti informatici, individuando e conservando alcune informazioni "esterne" legate alla comunicazione effettuata dall'utenza, similmente a quanto si verifica con i tabulati telefonici[7].

---

2. Che insieme alla Convenzione 108+ sono stati definiti come il *global standard* di riferimento sulla protezione dei dati personali. Si ricorda, infatti, che il 18 maggio 2018 il Comitato dei Ministri del Consiglio d'Europa ha adottato un Protocollo che ha modificato la Convenzione sulla protezione delle persone rispetto al trattamento di dati a carattere personale del 1981 (la Convenzione 108), che, dopo le modifiche, è detta 108+. In dottrina, A. Mantelero, 2021, *The future of data protection: Gold standards vs. global standard*, in *Comp. Law & Sec. Review*. Vol. 40, 105500; E.A. Rossi, 2019, *"Data Protection" nei rapporti transnazionali tra imprese. Aspetti problematici della Convenzione n. 108 del Consiglio d'Europa e del regolamento (UE) 679/2016*, in *Studi sull'integrazione europea*, p. 209 ss.

3. M. Bohlander, 2018, *"The Global Panopticon": Mass Surveillance and Data Privacy Intrusion as a Crime Against Humanity?*, in M. Bohlander, M. bose, O. Lagodny, A. Klip (eds.), *Justice Without Borders: Essays in Honour of Wolfgang Schomburg*, Leiden Boston, pp. 73-102.

4. Di pari passo allo sviluppo della tecnologia si è sviluppata una criminalità che ha sfruttato nuove conoscenze per commettere reati già puniti dal codice penale o per tenere nuove condotte offensive non ancora sanzionate penalmente, determinando così l'introduzione da parte del legislatore di nuove fattispecie incriminatrici (cd. computer crimes). In dottrina, cfr. L. Luparia, 2007, *La disciplina processuale e le garanzie difensive*, in L. Luparia, G. Ziccardi, *Investigazione penale e tecnologia informatica,* Giuffré, Milano, p. 130; R. Orlandi, 2009, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc*., p. 128 e ss.; L. Picotti, 2004, *Il diritto penale dell'informatica nell'epoca di internet*, Cedam, Padova, p. 86 e ss.

5. I mezzi informatici rivestono un ruolo fondamentale nello svolgimento delle indagini preliminari e il loro utilizzo è dovuto alle caratteristiche intrinseche dei dati elettronici che, in quanto immateriali, sono volatili ed altamente modificabili anche per effetto di un semplice accesso. O. Dominioni, 2005, *La prova penale scientifica*, Giuffrè, Milano, p. 37; L. Marafioti, 2011, *Digital evidence e processo penale*, in *Cass. pen*., p. 4510.

6. L'assenza di norme specifiche, volte a disciplinare l'assunzione e l'utilizzo delle prove digitali nel processo, ha consentito per lungo tempo agli inquirenti di scegliere i metodi tecnici per l'acquisizione delle fonti di prova, che, a volte, minavano la genuinità degli elementi raccolti o consentivano condotte contrastanti con la privacy individuale, come nel caso di sequestri di componenti informatiche superflue all'accertamento dei fatti di reato. G. Costabile, D. Rasetti, 2003, *Scena criminis, documento informatico e formazione della prova penale*, in *Ciberspazio e diritto*, p. 273. In tema di sequestro di dati informatici, vedasi la sentenza delle Sezioni Unite della Suprema Corte n. 40963/2017, che affronta molte questioni di diritto di grande complessità, tra cui il portato della Convenzione di Budapest sul *cybercrime* e la sua capacità di incidere trasversalmente sul diritto delle prove penali e sulle attività di indagine ben al di là del circoscritto settore inerente all'accertamento dei reati informatici; la distinzione tra le componenti hardware e software di un sistema informatico, funzionale alla definizione del concetto di dato o documento informatico quale *res* in sé, altra e distinta dal supporto in cui è incorporata; principi in materia di sequestro, tra cui la netta affermazione del rilievo da attribuirsi al principio di proporzionalità in una materia in cui non sempre se ne è fatto un buon governo; i principi ricavabili dalla CEDU in materia di diritto al rispetto della vita privata e familiare e di libertà di espressione come interpretati dalla Corte di Strasburgo; regole sulla impugnazione in ordine alla esatta conformazione dell'interesse ad impugnare. La sentenza, inoltre, pare incidere sulla nozione stessa di sequestro, ponendosi quale discrimine tra i casi in cui la restituzione della cosa risolve il provvedimento ablativo e i casi nei quali la restituzione in sé, accompagnata dalla clonazione della memoria elettronica, non scioglie il vincolo di indisponibilità, che si perpetua, appunto, con e nella effettuazione della copia.

7. Ciascun dispositivo (router, computer, server di rete, stampanti, alcuni tipi di telefoni, etc..) ha, quindi, il proprio indirizzo IP, che, in via di semplificazione,

In tale contesto, le frizioni con il diritto alla privacy sono dovute al fatto che per accertare il traffico telematico si conservano i *files* di *log* (o files di registro), che indicano le operazioni compiute dall'utente durante la navigazione e consentono, attraverso gli indirizzi IP (Internet Protocol), l'identificazione dello stesso, del destinatario e, a volte, la ricostruzione del contenuto della comunicazione[8].

Il principio di proporzione – che ricorre continuamente nel tema che ci occupa – è da intendersi come principio di "minima interferenza" nel diritto fondamentale inciso (quella minima interferenza necessaria al raggiungimento dello scopo generale, in questo caso la lotta al crimine).

Tale principio può e deve dirsi contenutistico nel senso che, per assicurarne il rispetto, non è sufficiente ottemperare alla riserva di legge formale ma occorre sindacare il modo con cui il legislatore esercita tale riserva[9].

Allo stesso tempo, tale potere di sindacabilità è sofferto sovente come limite alla collaborazione tra gli Stati e come espediente per affermare le prerogative statutali tramutandosi, spesso, in un'eccessiva azione di controllo o d'ingerenza.

Pertanto, non resta che far salvo, nella materia che ci occupa, l'auspicabile cambio di passo da parte della cultura giuridica sempre nel rispetto di diritti fondamentali ma di derivazione tecnologica.

Per trovare un punto di equilibrio tra il trattamento dei dati in questione, garanzie individuali e necessità investigative[10] appare, quindi, necessario determinare quali possano essere le informazioni concretamente archiviate, quali siano i soggetti gravati da tale obbligo e quale possa essere il tempo massimo di conservazione delle stesse[11].

2 La *Data Retention* alla luce dell'interpretazione della CGUE

Il 29 novembre 2022, la Commissione europea, il Parlamento europeo e il Consiglio hanno raggiunto un accordo politico provvisorio sulla legislazione diretta ad accelerare l'accesso da parte delle autorità ai dati digitali necessari – indipendentemente dal luogo in cui sono situati – per indagare e perseguire illeciti penali. Tale accordo, facendo seguito alla proposta della Commissione, porterà all'emanazione di un Regolamento sugli ordini europei di produzione e di conservazione di prove elettroniche in materia penale[12] e di una Direttiva sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali[13]. L'iniziativa legislativa è il risultato di un percorso durato quasi due anni di valutazioni su come adattare al meglio la giustizia penale alle sfide poste dall'era digitale.

Tali strumenti[14] consentiranno alle autorità giudiziarie di un paese UE di chiedere direttamente l'accesso alle prove elettroniche conservate da qualsiasi prestatore di servizi[15] offerti nell'Unione europea e stabilito o rappresentato in un altro Stato membro.

può essere visto come l'equivalente di un numero telefonico attribuito ai dispositivi collegati su internet. Infatti, come un numero telefonico identifica una data linea telefonica, così un indirizzo IP identifica univocamente uno specifico computer o un qualsiasi altro dispositivo di rete o una rete. Sul tema, F. Cajani, 2008, *Internet protocol. Questioni operative in tema di investigazioni penali e riservatezza*, in *Dir. Internet*., p. 545; T. Rafaraci, 2006, *Intercettazioni e acquisizione di tabulati telefonici*, in R. E. Kostoris, R. Orlandi (a cura di), *Contrasto al terrorismo interno e internazionale*, Giappichelli, Torino, p. 265 e ss.

8. F. Cajani, 2006, *Alla ricerca del log (perduto)*, in *Dir. Internet*, p. 572 e ss. In altri termini, si tratta di *files* che contengono informazioni relative alle attività compiute dagli utilizzatori dei sistemi informatici e telematici, generate dagli stessi sistemi per esigenze prevalentemente di carattere tecnico (per individuare guasti o anomalie funzionali) oppure di sicurezza (con l'intento di prevenire o rilevare intrusioni o violazioni all'interno della propria rete).

9. S. Marcolini, *La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention*, cit., p. 10.

10. Sul conflitto tra *data retention* e diritto alla riservatezza cfr. E. Bassoli, 2007, *Acquisizione dei tabulati Vs. Privacy*: *la data retention al vaglio della Consulta*, in *Riv. dell'internet*, p. 237; A. Camon, 2005, *L'acquisizione dei dati sul traffico delle comunicazioni*, in *Riv. it. dir. e proc. pen*., p. 594.

11. L. Luparia, G. Ziccardi, 2007, *Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali*, Milano, Giuffrè, p. 178; A. Ghirardini, G. Faggioli, 2009, *Computer forensic*, Milano, Apogeo, p. 347 e ss.

12. Regolamento del Parlamento europeo e del Consiglio relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale COM (2018) 225 final 2018/0108 (COD).

13. Direttiva del Parlamento e del Consiglio recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali COM (2018) 226 final 2018/0107 (COD).

14. In dottrina si vedano O. Calavita, 2021, *La proposta di regolamento sugli ordini di produzione e conservazione europei: commissione, consiglio e parlamento a confronto*, in *La legislazione penale*; D. Curtotti, 2021, *Indagini hi-tech, spazio cyber, scambi probatori tra Stati e Internet provider service e"Vecchia Europa": una normativa che non c'è (ancora),* in *Diritto penale e processo*, 6/2021, p. 745 ss.

15. L'acquisizione dei dati del traffico telematico è un tema che ha delle importanti implicazioni a proposito dell'obbligo del *provider* di conservazione di

In particolare, il Regolamento affronta il problema specifico dalla natura volatile delle prove elettroniche e della loro dimensione internazionale, mirando ad adattare i meccanismi di cooperazione all'era digitale e alle moderne forme di criminalità.

Essi si affiancheranno agli attuali strumenti di cooperazione giudiziaria, i quali rimangono pertinenti e possono essere usati dalle autorità competenti in caso di necessità.

Inoltre, al fine di agevolare la raccolta di prove elettroniche, il nuovo Regolamento si basa sui princìpi del reciproco riconoscimento pertanto, ai fini della notifica e dell'esecuzione dell'ordine non occorrerà coinvolgere direttamente l'autorità del Paese in cui si trova il destinatario dello stesso, tranne se non vi ottempera spontaneamente, nel qual caso l'ordine sarà fatto eseguire e sarà necessario l'intervento dell'autorità competente del Paese in cui si trova il rappresentante.

Lo strumento richiede, pertanto, una serie di solide garanzie, come la convalida da parte di un'autorità giudiziaria in ogni singolo caso[16].

I dati personali rientranti nell'ambito di applicazione del Regolamento sono protetti e possono essere trattati solo in conformità con il GDPR e la Direttiva sulla protezione dei dati nelle attività di polizia e giustizia[17].

Sul tema, è interessante evidenziare che poco prima della proposta di Regolamento sulla trasmissione transnazionale delle prove elettroniche, la Corte di Giustizia dell'UE interveniva con alcune pronunce[18] volte a mettere in evidenza la necessità di trovare un equilibrio tra i diritti fondamentali e la lotta alla criminalità.

Nel caso *Tele2 Sverige* del 21 dicembre 2016[19], la Corte di Giustizia dell'UE riteneva che gli Stati membri non potessero imporre ai fornitori di servizi di comunicazione elettronica un obbligo generale e indiscriminato di conservazione dei dati sul traffico e sull'ubicazione.

In particolare la pronuncia si occupa della questione, rimasta aperta[20], dei rapporti intercorrenti tra le discipline nazionali sulla

tali dati. Possono avere un ruolo rilevante per le indagini l'acquisizione di dati di traffico relativi sia alla navigazione in Internet che all'utilizzo della posta elettronica, ma allo stesso tempo possono contenere una serie di informazioni che rientrano nella nozione di riservatezza personale. Sul tema, cfr. O. Signorile, 2009, *Computer Forensic Guidelines: un approccio metodico-procedurale per l'acquisizione e analisi delle digital evidence*, in *Ciberspazio e Diritto*, Mucchi editore, Modena; A. Pietrucci, 2003, *La responsabilità del provider per i contenuti illeciti della rete*, in *Riv. Crit. Dir. Priv*., Napoli; F. Ruggiero, 2001, *Individuazione nel cyberspazio del soggetto penalmente responsabile e ruolo dell'internet provider*, in *Giur. Merito*, Milano. Il legislatore con l'espressione traffico telematico intende riferirsi ai movimenti effettuati nella rete internet dal singolo utente, sebbene la telematica possa avere applicazioni diverse. Sul tema, cfr. altresì, L. A. D'Angelo, 2006, *La conservazione dei dati del traffico telefonico e telematico tra esigenze investigative e tutela della privacy*, in A. A. Dalia (a cura di), *Le nuove norme di contrasto al terrorismo*, Giuffré, Milano, p. 121 e ss.

16. Così come più volte segnalato in dottrina A. Rusinova, 2019, *European Perspective on Privacy and Mass Surveillance at the Crossroads*, disponibile suppers.ssrn.com/sol3/papers.cfm?abstract_id=3347711, pp. 1-22, p. 6; G. Formici, 2020, *La digital mass surveillance al vaglio della Corte europea dei diritti dell'uomo: da Zakharov a Big Brother Watch*, in Federalismi.it, n. 23, disponibile su www.federalismi.it/nv14/articolo-documento.cfm?Artid=43890, pp. 43-71, p. 54.

17. Direttiva (UE) 2016/680, c.d. LED, 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.

18. Sul punto, appare opportuno segnalare che "quando la Corte giust. UE si pronuncia sulla data retention, ha già un non trascurabile retroterra di riflessioni interne agli Stati membri". In questi termini, S. Marcolini, 2022, *La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa*, in R. Flor, S. Marcolini (a cura di) *Dalla data retention alle indagini ad alto contenuto tecnologico*, Giappichelli, Torino, p. 5; R. Flor, 2011, *Data retention e limiti al potere coercitivo dello stato in materia penale: le sentenze del Bundesverfasungsgericht e della Curtea Constitutionala*, in *Cass. pen.,* 2011, p. 1952.

19. Per un accurato commento alla pronuncia cfr., S. Marcolini, *La giurisprudenza della Corte di giustizia dell'Unione europea sulla data retention*, cit., p. 12 ss.; C. Bovino, 2017, Dat*a retention: no all'obbligo generale di conservazione dei dati*, in *Il Quotidiano giuridico*. V. altresì, I. Cameron, 2017, *Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, n. 54, pp. 1467-1495; S. Peyrou, 2017, *Arrêt «Tele2 Sverige»: l'interdiction du stockage de masse de données à caractère personnel réaffirmée par la Cour de justice de l'Union européenne*, in *Journal de droit européen*, n. 237 pp. 107-109, X. Tracol, 2017, *The Judgment of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige and Watson Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level*, in *Computer Law & Security Review*, pp. 541-552.

20. Con una precedente pronuncia, la Grande Sezione, 8 aprile 2014, Digital Rights, C-293/12 e C-594/12 annullava la direttiva 2006/24/CE iniziando a delineare un vero e proprio statuto della *Data retention* segnalando tutta una serie di manchevolezze della disciplina comunitaria (la specificazione dei gravi reati, i casi e i modi di accesso al dato da parte dell'autorità, il periodo di conservazione, la sicurezza dei dati conservati) che la legislazione sul tema, comunitaria o nazionale che sia, è chiamata ad affrontare e risolvere in positivo nel rispetto del principio di proporzionalità.

La direttiva, legittimando una conservazione indifferenziata delle telecomunicazioni con l'obiettivo di contrastare il terrorismo e la criminalità organizzata, risultava contraria ai principi europei di proporzionalità, necessità e finalità limitata dei dati ed era in grado di pregiudicare seriamente le garanzie sottese ai diritti alla vita privata ed alla protezione delle informazioni personali, contemplati dagli articoli 7 e 8 della Carta di sulla sentenza. Sul punto v. T. Ojanen, 2014, *Privacy Is More Than Just a Seven-Letter Word. The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance -*

data retention ed il diritto comunitario.

A seguito di tale sentenza, alcuni Stati hanno espresso il timore di essere ormai privati di uno strumento necessario per salvaguardare la sicurezza nazionale e combattere la criminalità[21].

Così, nei casi *Privacy International* e *La Quadrature du Net* e.a. del 6 ottobre 2020[22] la Corte si pronunciava nuovamente sul tema esaminando l'applicabilità della direttiva e-*Privacy* – 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 – ai casi di specie.

Invero, le autorità nazionali dei vari Stati membri pretendevano che essa non fosse applicabile qualora venisse in rilievo l'esigenza di salvaguardare la sicurezza dello Stato.

A questo riguardo, la Corte precisava che «sebbene spetti agli Stati membri definire i loro interessi essenziali in materia di sicurezza e decidere le misure idonee a garantire la loro sicurezza interna ed esterna, la mera circostanza che una misura nazionale sia stata adottata ai fini della tutela della sicurezza nazionale non può comportare l'inapplicabilità del diritto dell'Unione e dispensare gli Stati membri dal necessario rispetto di tale diritto».

Inoltre, se sia il regolamento sulla protezione dei dati (GDPR) che la direttiva e-*Privacy* non si applicano al trattamento dei dati effettuati dalle autorità competenti nella lotta contro la criminalità o alla salvaguardia della sicurezza nazionale, i trattamenti di dati personali effettuati a questi stessi fini da enti privati rientrano nell'ambito di applicazione di quest'ultimo. Pertanto, i trattamenti di dati personali da parte degli operatori delle telecomunicazioni che derivano da obblighi imposti dalle autorità pubbliche a fini di sicurezza nazionale o di lotta alla criminalità devono rispettare le norme europee sulla tutela dei dati personali.

La Corte precisava, altresì, che nella situazione in cui uno Stato membro debba affrontare una grave minaccia per la sicurezza nazionale che si rivela reale, attuale e prevedibile, la direttiva e-*Privacy* letta alla luce della Carta non preclude di richiedere ai fornitori di servizi di comunicazione elettronica di conservare i dati relativi al traffico e all'ubicazione in modo generalizzato e indiscriminato, ma impone che tale decisione, adottata per un periodo limitato a quanto strettamente necessario, debba essere soggetta a un controllo effettivo al fine di verificare la sussistenza del rispetto delle condizioni e delle garanzie innanzi citate ad opera di un tribunale o di un organo amministrativo indipendente, la cui decisione ha effetto vincolante.

Ritornando alla proposta di Regolamento europeo sulla trasmissione transnazionale delle prove elettroniche, una delle critiche che ha suscitato il testo della proposta della Commissione riguardava la distinzione artificiale che veniva fatta tra dati non relativi al contenuto (dati degli abbonati, dati relativi agli accessi e dati relativi alle operazioni) e dati relativi al contenuto.

Tale distinzione era basata, secondo la Commissione, sulla natura più o meno sensibile dei dati in questione.

L'*European Data Protection Board* (EDPB) esprimeva però dubbi e preoccupazioni in merito alla differenziazione tra "dati non di contenuto" e dati di contenuto, nonché alle quattro nuove categorie di dati personali stabilite dalla proposta di regolamento[23].

Questa considerazione dell'EDPB era inoltre basata sulla precedente giurisprudenza della Corte di giustizia che precisava che «presi nel loro insieme, tali dati sono idonei a consentire di trarre conclusioni molto precise riguardo alla vita privata delle persone i cui dati sono stati conservati, come le abitudini della vita quotidiana, i luoghi di soggiorno permanenti o temporanei, gli spostamenti giornalieri o di altro tipo, le attività esercitate, le relazioni sociali di tali persone e gli ambienti sociali da esse

Court of Justice of the European Union, Decision of 8 April 2014 in *Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, in European Constitutional Law Review*, pp. 528-541.

21. CGUE (grande sezione), 21 dicembre 2016, Tele2 Sverige AB c. Post- och telestyrelsen, C-203/15 e C-698/15, pt. 12. In dottrina, F. Dubuisson, 2016, *La Cour européenne des droits de l'homme et la surveillance de masse*, in *Revue trimestrielle des droits de l'homme*, n. 108, pp. 855-886, p. 856.

22. Il primo caso traeva origine da un ricorso promosso innanzi all'Investigatory Powers Tribunal dalla organizzazione non governativa Privacy International contro il governo britannico, che riguardava la tematica della legittimità, in virtù della pertinente normativa europea, della conservazione ed utilizzo di massa delle informazioni personali ad opera delle agenzie di sicurezza e di intelligence del Regno Unito. Il secondo caso derivava da una serie di ricorsi presentati da alcune organizzazioni di categoria, francesi e belghe, contro i rispettivi governi nazionali innanzi alle autorità giurisdizionali dei loro Paesi, concernenti la compatibilità con il diritto UE delle legislazioni francesi e belghe, intese a disciplinare la raccolta, il trattamento e l'uso delle comunicazioni elettroniche e ad ammettere in definitiva una conservazione in blocco dei dati personali degli utenti dei servizi di comunicazione. Per approfondimenti si rinvia a M. Nino, 2021, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione Europea*, n. 1, pp. 93-124, p. 94 ss.

23. EDPB, "Opinion 23/2018 on Commission proposals on European Production and Preservation Orders for electronic evidence in criminal matters (Art. 70.1.b)", p. 12.

frequentati. In particolare, tali dati forniscono gli strumenti per stabilire il profilo delle persone interessate, informazione tanto sensibile, in rapporto al diritto al rispetto della vita privata, quanto il contenuto stesso delle comunicazioni[24]».

Così, un'ulteriore bozza di relazione del Parlamento europeo conteneva un rifiuto delle nuove categorie di dati introdotte dalla Commissione ed un ritorno a categorie di dati chiare basate sulla legislazione UE e nazionale esistente e in linea con Giurisprudenza della CGUE.

Un'altra critica sollevata verso la bozza di regolamento era l'assenza di una notifica da parte dell'autorità di emissione ad una autorità giudiziaria dello Stato di esecuzione.

Tale notifica veniva successivamente inserita con l'orientamento generale del Consiglio[25] ma in modo molto limitato e senza effetto sospensivo dell'ordine, rendendo possibile una sua esecuzione prima che detta autorità giudiziaria potesse esprimersi.

Secondo la relazione dell'eurodeputata Birgit Sippel, l'autorità di esecuzione dovrebbe poter rifiutare il riconoscimento o l'esecuzione di un ordine di produzione o di conservazione qualora tale rifiuto si basi su motivi specifici e limitati elencati in un nuovo articolo del progetto di relazione, in linea con i motivi adottati nella direttiva 2014/41 / UE sull'ordine europeo di indagine, in modo da garantire la coerenza tra questi due strumenti di cooperazione giudiziaria in materia penale.

Un meccanismo di notifica così significativo dovrebbe inoltre impedire ai prestatori di servizi, vale a dire soggetti privati, di diventare valutatori legali dei diritti fondamentali sollevandoli da ogni tipo di responsabilità in caso di conflitto di leggi. Di conseguenza, l'ordine europeo di produzione o l'ordine europeo di conservazione dovranno essere inviati simultaneamente al fornitore di servizi e all'autorità di esecuzione. In assenza di una reazione dell'autorità di esecuzione per un periodo di tempo determinato, il prestatore di servizi sarà obbligato a conservare o fornire i dati richiesti all'autorità di emissione[26].

È chiaro, quindi, che la valutazione del rispetto dei diritti fondamentali di un ordine di preservazione o di produzione di prove elettroniche non possa essere lasciata ai *service provider*, ma debba anch'essa essere accompagnata da un adeguato controllo giurisdizionale nello stato di esecuzione.

Di recente, la sentenza della Corte di Giustizia UE, emessa il 5 aprile 2022 all'esito del procedimento C-140/20, ha riacceso il dibattito sulla conservazione e l'utilizzo dei dati di traffico e dei dati di localizzazione a fini di prevenzione dei reati.

La questione ebbe inizio nel 2015 quando un tribunale irlandese, a conclusione di un procedimento per omicidio, aveva condannato all'ergastolo l'imputato utilizzando a fini probatori dati di traffico e dati di ubicazione afferenti a chiamate telefoniche.

Gli investigatori della polizia nazionale avevano avuto accesso a questi dati in base al Communications (Retention of Data) Act del 2011. L'imputato aveva contestato l'utilizzo di queste prove, adducendo che questa legge, che disciplina la conservazione di dati di traffico e/o di ubicazione, avrebbe violato i diritti conferitigli dal diritto dell'Unione e nello specifico dalla Direttiva UE 2002/58/CE.

Mediante rinvio pregiudiziale veniva quindi interpellata la Corte di Giustizia dell'Unione Europea, chiamata a pronunciarsi sulla compatibilità tra la predetta Direttiva e la previsione, all'interno degli ordinamenti degli Stati membri, di disposizioni che consentissero, e a quali condizioni, l'utilizzo dei dati relativi al traffico o all'ubicazione, per ragioni di prevenzione di illeciti e tutela della sicurezza pubblica.

Parametro dell'indagine è, nello specifico, l'articolo 15 della Direttiva 58/2002, paragrafo 1, che dispone come gli Stati membri possano adottare disposizioni legislative di conservazione dei dati per un periodo di tempo limitato se necessario per la salvaguardia della sicurezza dello Stato, della difesa, della sicurezza pubblica o per la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.

All'esito del procedimento di rinvio pregiudiziale, nelle disposizioni finali della sentenza, la Corte ha chiarito che questa norma si qualifica come un limite all'introduzione – da parte del legislatore nazionale – di misure preventive che contemplino, per finalità di lotta alla criminalità o di tutela alla pubblica sicurezza, la conservazione generalizzata e indifferenziata dei dati relativi al traffico e dei dati relativi all'ubicazione.

Sono invece conformi al Diritto Europeo tutte quelle disposizioni volte ad introdurre, per le medesime finalità di prevenzione di illeciti e tutela della sicurezza pubblica, misure che prevedano:

24. C.G.U.E., Digital Rights Ireland Ltd, 8 aprile 2014, C-293/12 e C-594/12; C.G.U.E., Tele2 Sverige AB, 21 dicembre 2016, C-203/15 e C-698/15.

25. Orientamento generale del Consiglio UE sulla proposta di Regolamento adottato dai Ministri della Giustizia degli Stati membri il 7 dicembre 2018.

26. Birgit Sippel, "Draft report on the proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, COM (2018)0225 – C8-0155/2018 – 2018/0108(COD), LIBE Committee, 24 October 2019, p. 146.

- la conservazione mirata dei dati relativi al traffico e dei dati relativi all'ubicazione che sia delimitata, sulla base di elementi oggettivi e non discriminatori, in funzione delle categorie di persone interessate o mediante un criterio geografico, per un periodo temporalmente limitato allo stretto necessario, ma rinnovabile;
- la conservazione generalizzata e indifferenziata degli indirizzi IP attribuiti all'origine di una connessione, per un periodo temporalmente limitato allo stretto necessario;
- la conservazione generalizzata e indifferenziata dei dati relativi all'identità civile degli utenti di mezzi di comunicazione elettronica;
- il ricorso a un'ingiunzione rivolta ai fornitori di servizi di comunicazione elettronica, mediante una decisione dell'autorità competente soggetta a un controllo giurisdizionale effettivo, di procedere, per un periodo determinato, alla conservazione rapida dei dati relativi al traffico e dei dati relativi all'ubicazione di cui dispongono tali fornitori di servizi.

Al di là del supporto interpretativo offertoci dalla Corte di giustizia, non può sottacersi come il susseguirsi di tali pronunce, tuttavia, destabilizza uno dei principi cardini degli ordinamenti giuridici ossia la certezza del diritto.

Un esempio, per l'ordinamento italiano, è rappresentato proprio dall'art. 132 del D.lgs. 196 del 2003.

Com'è noto, tale disposizione – oggetto di diversi rimaneggiamenti – fissa una timeline di conservazione specifica dei dati.

In una recente pronuncia della Suprema Corte di Cassazione[27] è stato chiarito che, soprattutto a seguito delle modifiche intervenute con il decreto legge n. 132 del 2021, siamo di fronte ad una "giurisdizionalizzazione" della procedura di acquisizione dei dati.

Tale condizione potrebbe alimentare le difficoltà riscontrate dalle autorità investigative ed incidere negativamente sul piano della cooperazione e dello scambio di informazioni. Sarebbe opportuno porre un rimedio attraverso la predisposizione di regole uniformi sulla conservazione dei dati che siano rispettose dei diritti fondamentali, del principio di proporzionalità evitando, inoltre, acquisizioni di massa[28].

3 Il Secondo Protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica. Prime osservazioni

A fare il paio con tali considerazioni è, indubbiamente, il Secondo Protocollo sulla cooperazione rafforzata e la divulgazione delle prove elettroniche aggiuntivo alla Convenzione di Budapest[29] – aperto alla firma il 12 maggio 2022 – considerato il timore che tali prove, così come si legge nel Preambolo, potrebbero essere archiviate in giurisdizioni estere, diverse, mutevoli o sconosciute.

Preliminarmente, in seguito alla pubblicazione del progetto di disposizioni, l'EDPB con la Dichiarazione 2/2021, adottata il 2 febbraio 2021, ha ritenuto di rinnovare il proprio contributo esperto e costruttivo al fine di garantire che le riflessioni relative alla protezione dei dati fossero tenute in debito conto nel processo generale di elaborazione del protocollo addizionale, considerando

27. Cass. pen., VI sez., n. 15836/2023. Avverso una sentenza della Corte di Appello di Brescia – che aveva confermato la condanna in primo grado per reati quali: abuso d'ufficio, peculato, turbata libertà degli incanti, falso materiale in atto pubblico, falso ideologico, truffa ai danni dello stato ecc. – gli imputati proponevano ricorso per Cassazione ma uno, in particolare, articolava un unico motivo attinente proprio la violazione di legge e difetto di motivazione in merito all'utilizzabilità dei tabulati dell'utenza (e la relativa localizzazione) intestata alla figlia ma in uso allo stesso imputato, al fine di provare la sua responsabilità per aver attestato falsamente l'adozione di atti presso il luogo di lavoro pur essendo in quel momento altrove.

    I tabulati sarebbero stati acquisiti dalla polizia giudiziaria senza alcun intervento del pubblico ministero determinando un'inutilizzabilità patologica, atteso che l'atto sarebbe stato assunto in violazione dell'art. 15 Cost.; tanto da determinare l'accoglimento del motivo e l'annullamento con rinvio della sentenza impugnata. Giudizio ancora in corso di definizione.

28. In questi termini, F. Spiezia, 2022, *Cooperazione internazionale e tutela delle vittime nel cyberspazio*, in *Diritto penale e processo. Speciale cybercrime*, 9/2022, p. 1142. Rispetto alle nuove emergenti tecnologie, l'A. aggiunge che "la professionalizzazione di tale settore rimane nell'UE una questione aperta, decisamente da realizzare per la nascita di un sistema penale che veda nella tecnologia una preziosa alleata e non solo l'arma del nemico da neutralizzare". Sul punto, vedi inoltre M.A. Biasiotti, M. Epifani, F. Turchi, 2015, *Opportunità e sfide per la prova elettronica*, in *Informatica e diritto*, XXIV,1-2, p. 19.

29. È il 23 novembre 2001 quando la Convenzione del Consiglio d'Europa sulla criminalità informatica viene aperta alla firma degli Stati membri e non membri dell'UE. Entrerà in vigore il 1° luglio 2004 e ratificata dall'Italia solo nel 2008 con la legge n. 48.

che le riunioni dedicate alla preparazione di tale protocollo si sarebbero svolte in sessioni chiuse e che nel mandato del T-CY[30] non sia stato previsto il coinvolgimento diretto delle autorità preposte alla protezione dei dati nel processo di elaborazione.

Invero, l'accesso transfrontaliero ai dati personali è già stato affrontato in passato dalle autorità preposte alla protezione dei dati dell'UE in varie posizioni e pareri[31].

Ciò che emerge è che l'EDPB rimane pienamente consapevole del fatto che le circostanze per cui le autorità giudiziarie e di polizia si trovano di fronte a una "situazione transfrontaliera" rispetto all'accesso a dati personali nel contesto delle rispettive indagini possano risultare impegnative e riconosce l'obiettivo legittimo di rafforzare la cooperazione internazionale sulla criminalità informatica e l'accesso alle informazioni.

Parallelamente, l'EDPB ribadisce che devono essere garantite la protezione dei dati personali e la certezza del diritto, contribuendo così all'obiettivo di stipulare accordi sostenibili per la condivisione di dati personali con paesi terzi per finalità di polizia e giudiziarie che siano pienamente compatibili con i trattati dell'UE e la Carta dei diritti fondamentali dell'Unione europea.

In particolare, per quanto riguarda "l'accesso transfrontaliero diretto a dati informatici memorizzati" di cui all'articolo 32, lettera b), della Convenzione di Budapest, l'EDPB ribadisce in particolare che, di norma, il titolare del trattamento può comunicare i dati solo sulla base di un'autorizzazione dell'autorità giudiziaria o altro documento che giustifichi la necessità di accedere ai dati e indichi la base giuridica pertinente per tale accesso, presentati da un'autorità nazionale competente (giudiziaria o di polizia) conformemente al diritto interno, in cui sia anche specificato lo scopo per il quale i dati sono richiesti.

Poiché la Convenzione di Budapest e i suoi protocolli addizionali sono strumenti internazionali vincolanti, l'EDPB sottolinea che, in linea con la giurisprudenza della Corte di giustizia dell'Unione europea, "gli obblighi imposti da un accordo internazionale non possono avere l'effetto di compromettere i principi costituzionali del Trattato CE, tra i quali vi è il principio secondo cui tutti gli atti comunitari devono rispettare i diritti fondamentali, atteso che tale rispetto costituisce il presupposto della loro legittimità"[32]. È quindi essenziale che le parti negoziali dell'UE assicurino che le disposizioni stabilite nel protocollo addizionale siano conformi all'*acquis* dell'UE nel campo della protezione dei dati, al fine di garantirne la compatibilità con il diritto primario e derivato dell'UE.

Eccettuati i casi di urgenza validamente accertati, e alla luce della giurisprudenza della Corte, le autorità richiedenti dovrebbero limitarsi al pubblico ministero, a un'autorità giudiziaria o un'altra autorità indipendente.

L'EDPB ritiene inoltre che il coinvolgimento sistematico delle autorità giudiziarie nelle parti richieste sia essenziale per garantire un esame efficace della conformità delle richieste alla Convenzione nonché l'applicazione del principio della doppia punibilità nel campo della cooperazione giudiziaria.

Oltre ad assicurare il rispetto dei diritti dei singoli e il giusto processo nel meccanismo previsto di cooperazione giudiziaria, tale salvaguardia prevede anche una garanzia essenziale relativa alle condizioni procedurali di accesso ai dati personali.

Come già menzionato nel suo precedente contributo, in relazione alla sicurezza del trattamento dei dati, l'EDPB invita il T-CY a prendere in considerazione, come garanzia specifica per la protezione dei dati, un meccanismo finalizzato a notificare senza indugio le violazioni dei dati che potrebbero configurare gravi ingerenze nei diritti e nelle libertà degli interessati.

L'EDPB sottolinea infine il requisito dell'articolo 52, paragrafo 1, della Carta dei diritti fondamentali dell'UE[33], secondo cui eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla Carta sono soggette al principio di proporzionalità e possono essere apportate solo laddove siano necessarie. Per essere legittimo ai sensi del diritto dell'UE, quindi, il progetto

30. Mandato per l'elaborazione di un progetto di secondo protocollo aggiuntivo alla convenzione di Budapest sulla criminalità informatica, approvato dalla 17a sessione plenaria del Comitato della Convenzione sulla criminalità informatica (T-CY) l'8 giugno 2017, T-CY (2017).

31. Si vedano le osservazioni del Gruppo di lavoro Articolo 29 sulla questione dell'accesso diretto delle autorità di contrasto di paesi terzi ai dati conservati in un'altra giurisdizione, come proposto nel progetto di elementi per un protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, 5.12.2013; nonché la Dichiarazione del Gruppo sugli aspetti relativi a protezione dei dati e privacy dell'accesso transfrontaliero alle prove elettroniche, 29 novembre 2017; parere 3/2019 del GEPD concernente la partecipazione ai negoziati in vista di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica; parere 7/2019 del GEPD sulle proposte relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale; parere 23/2018 dell'EDPB, adottato il 26 settembre 2018, sulle proposte della Commissione relative agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale.

32. Cfr. sentenza della Corte di giustizia dell'Unione europea del 3 settembre 2008, Kadi/Consiglio, cause riunite C-402/05 P e C-415/05 P, ECLI:EU:C:2008:461, punto 285.

33. Cfr. anche l'articolo 8, paragrafo 2, della Convenzione europea dei diritti dell'uomo.

di disposizioni del protocollo previsto deve soddisfare tale requisito. Ciò riguarda pertanto sia i dati personali contenuti nella richiesta sia quelli contenuti nella risposta a tale richiesta.

Per tali ragioni, l'EDPB riteneva essenziale che il testo provvisorio fosse integrato da disposizioni specifiche sulle garanzie per la protezione dei dati, da valutare poi insieme ad altre disposizioni, al fine di garantire che il progetto di protocollo addizionale si traduca in un accordo sostenibile per la condivisione di dati personali con paesi terzi a fini di polizia e giudiziari, pienamente compatibile con i trattati dell'UE e con la Carta e rispettoso dei principi chiave e in particolare quelli di liceità, correttezza e trasparenza, limitazione delle finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza.

Analogamente, l'EDPB sottolinea l'importanza di garantire i diritti individuali fondamentali (accesso, rettifica, cancellazione) limitando qualsiasi restrizione nel rispetto del principio di proporzionalità e un efficace ricorso giudiziario per gli interessati in caso di violazione delle garanzie per la protezione dei dati. L' esercizio di tali diritti richiede anche la notifica all'interessato, almeno una volta che tale notifica non metta più a rischio l'indagine.

Nel paragrafo che segue si cercherà di analizzare se le indicazioni dell'EDPB siano state recepite anche, e soprattutto, alla luce della Decisione (UE) 2023/436 del Consiglio del 14 febbraio 2023, che autorizza gli Stati membri a ratificare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione di Budapest.

4 Conclusioni

Com'è noto, al momento della registrazione del nome di dominio presso il prestatore di servizi designato, ciascun titolare è obbligato a fornire un numero di informazioni che includono anche dati personali. Tali informazioni sono conservate in un archivio digitale mantenuto dal prestatore di servizi.

Prima dell'entrata in vigore del GDPR tali informazioni erano rese disponibili a chiunque ne facesse richiesta attraverso un servizio gratuito denominato WHOIS e, trattandosi di informazioni disponibili su fonti aperte, la Convenzione di Budapest ne consentiva l'utilizzo come prova elettronica, indipendentemente dal luogo in cui i dati si trovavano[34]. A ciò va aggiunta la possibilità riconosciuta alle forze dell'ordine di mantenere l'anonimato nel corso delle investigazioni su fonti aperte.

Chiaramente, tale sistema – che si è cercato di arginare con il regime sanzionatorio introdotto dal GDPR[35] – è stato considerato in molti Paesi in potenziale conflitto con i principi dettati in materia di protezione dei dati personali.

Per tali ragioni, il Secondo Protocollo fornisce, indubbiamente: una base giuridica per la divulgazione di informazioni relative alla registrazione dei nomi di dominio e per la cooperazione diretta con i fornitori di servizi per le informazioni sugli abbonati; modi efficaci per ottenere informazioni sugli abbonati e dati relativi al traffico; cooperazione immediata in caso di emergenza; strumenti di assistenza reciproca e garanzie in materia di protezione dei dati personali.

Cercare di garantire lo svolgimento delle attività di indagine e la persecuzione dei reati anche in un ambiente senza confini garantendo, al contempo, il rispetto dei diritti e delle libertà fondamentali dell'individuo è da sempre uno dei principali obiettivi della Convenzione di Budapest.

Il Secondo Protocollo addizionale nasce proprio dall'esigenza di bilanciare i poteri investigativi con i diritti e le libertà fondamentali.

In particolare, il Capo III è dedicato, principalmente, alle "condizioni e garanzie" (art. 13) e alla protezione dei dati personali[36] (art. 14). Come già chiarito dall'*European Data Protection Board*, la Garanzie Essenziali Europee devono rappresentare la base per suggerire una possibile regolamentazione della materia rispettando diversi punti: i trattamenti di dati personali devono essere

34. Nel 2018 si stimava che il numero di richieste WHOIS effettuate mediamente da una unità di contrasto alla criminalità informatica in Europa potesse superare il migliaio alla settimana, fatto dovuto non solo alla semplicità e immediatezza di accesso a informazioni di forte utilità, ma anche alla possibilità per le forze dell'ordine di mantenere l'anonimato nel corso delle investigazioni su fonti aperte. Per un accurato approfondimento in merito all'art. 6 del Secondo Protocollo, si rinvia a M. Lucchetti, 2022, *L'acquisizione di informazioni sulla registrazione di nomi di dominio nelle investigazioni in materia di cybercrime (art. 6)*, in *Diritto penale e processo. Speciale cybercrime*, 8/2022, p. 1041-1044.

35. Sul rapporto tra Cybersecurity e GDPR v. G. Auricchio, *Il Cyberterrorismo*, in Iaselli M. (a cura di), Investigazioni digitali, Milano, p. 718 – 728.

36. Il tema della protezione dei dati personali è senza dubbio, insieme alla sicurezza dei dati, quello destinato ad avere maggiore rilevanza nel panorama delle indagini digitali transfrontaliere, in quanto gli strumenti informatici sono ormai i contenitori della personalità dell'individuo e dei terzi che hanno rapporti con quest'ultimo. Cfr. P. Perri, 2022, *Le condizioni di salvaguardia e la protezione dei dati personali*, in *Diritto penale e processo*, 9/2022, p. 1150-1154.

basati su regole chiare, precise e accessibili; bisogna dimostrare la necessità e la proporzionalità riguardo ai legittimi obiettivi perseguiti; deve essere predisposto un meccanismo di supervisione indipendente; l'individuo deve disporre di rimedi effettivi.

Un ruolo fondamentale è svolto dal principio di pertinenza e non eccedenza nel trattamento dei dati personali: ciò comporta che i dati raccolti dovranno essere adeguati a quanto necessario per le finalità investigative e non dovranno essere sovrabbondanti rispetto agli scopi prefissati, specie se trattasi di dati personali "sensibili[37]".

Inoltre, il comma 3 dell'art. 14 richiama il fondamentale principio della qualità del dato già presente nella Dir. 2016/680 in base al quale tutte le parti sono tenute ad adottare delle misure ragionevoli per garantire l'esattezza dei dati raccolti[38]. Dirimente potrà essere l'adesione a una best practices in ambito di investigazioni digitali.

Tra i punti di contatto comuni al Protocollo e al GDPR figura anche l'*accountability*, che riveniamo al comma 8 dell'articolo 14.

Ciò fa sorgere in capo alle Parti l'obbligo di "dimostrare" come e per quale scopo sono stati trattati i dati personali di una persona fisica.

Interessante sarà osservare come tale obbligo di "rendicontazione" potrà bilanciarsi con l'esigenza, altrettanto avvertita, di perseguimento e repressione dei reati.

Invero, attraverso l'applicazione di tale principio il soggetto che dispone il trattamento gode di una certa autonomia nella scelta degli strumenti e delle modalità con le quali tratterà i dati personali, pur sapendo però che il relativo operato (*rectius* trattamento) potrà essere oggetto di specifica analisi da parte delle Autorità di vigilanza a ciò preposte.

Su tale obbligo di rendicontazione inciderà sicuramente il comma 7 dell'art. 14 che si occupa, nello specifico, del tema della sicurezza dei dati e degli incidenti di sicurezza. Invero, ciascuna parte dovrà garantire (e dimostrare) adeguate misure di sicurezza di natura tecnologica, materiale ed organizzativa per la protezione dei dati personali proprio al fine di scongiurare incidenti di sicurezza quali: perdita, accessi, divulgazione, alterazione o distruzione accidentali e non autorizzati dei dati. L'assolvimento dell'obbligo di rendicontazione potrà essere riscontrato con una puntuale tenuta dei relativi registri di trattamento.

Una differenza rispetto al GDPR, invece, la rinveniamo in tema di notifica di violazioni di dati personali. Infatti, il comma 7, lett. b) dell'art. 14 prevede la possibilità che la notifica all'Autorità deputata a riceverla possa essere ritardata od omessa qualora metta a repentaglio la sicurezza nazionale o comprometta misure di sicurezza pubblica, introducendo un'eccezione che invece per il titolare del trattamento nel GDPR non è contemplata. L'articolo prevede, altresì, l'eventuale notifica della violazione anche agli interessati, così come richiesto dall'EDPB, pur permanendo le eccezioni che potrebbero giustificarne il ritardo o l'omissione.

Il mancato rispetto delle prescrizioni dell'art. 14 consente ad una Parte di sospendere, previo ragionevole preavviso, il trasferimento dei dati personali ad altra Parte.

La sospensione dei trasferimenti può essere intesa come vera e propria contromisura utile a prevenire o interrompere una possibile violazione che riguardi anche la sicurezza dei dati oggetto di trattamento[39].

In dottrina[40] è stato affermato che dalla lettura dell'art. 14 emerga come il legislatore oltre al noto principio della *double criminality* abbia voluto sottolineare l'importanza della *double privacy* nelle indagini digitali.

In tale contesto, anche al fine di non paralizzare le esigenze di cooperazione a fini investigativi, si cercherà di correre ai ripari anche con l'art. 6 del Protocollo addizionale che definisce le basi legali e le procedure da adottare per la cooperazione diretta tra le autorità competenti di una Parte e un prestatore di servizi di registrazione di nomi di dominio nel territorio di un'altra parte proprio al fine di adeguarsi con le *policy* e le buone pratiche in corso di definizione nel contesto del governo di Internet.

Molta attenzione, dunque, dovrà essere riservata all'adozione di adeguate misure di sicurezza e alla notifica degli incidenti a specifiche Autorità che devono essere dichiarate al momento della firma del Protocollo, secondo metodologie analoghe a quelle indicate nel GDPR, ossia basate su una preventiva analisi del rischio.

37. Come meglio definiti all'art. 9 del GDPR rubricato "categoria particolari di dati personali".

38. Sul tema, cfr. V.S.M. Guariniello, 2020, *Le best practices in materia di computer forensics*, in M. Iaselli (a cura di), Investigazioni digitali, Milano, p. 77 ss.

39. P. Annicchino, 2022, *(In)sicurezza dei dati, contromisure e attività di contrasto alla criminalità informatica*, in *Diritto penale e processo. Speciale cybercrime*, 9/2022, p. 1158.

40. Cfr. P. Perri, *Le condizioni di salvaguardia e la protezione dei dati personali*, cit., p. 1154.

Il fine è quello di evitare non solo violazioni in materia di protezione dei dati personali, bensì – e soprattutto – scongiurare che errori investigativi possano depotenziare l'effettività degli strumenti di cooperazione internazionale[41].

Bibliografia

Annicchino P., (In)sicurezza dei dati, contromisure e attività di contra-sto alla criminalità informatica, in Diritto penale e processo. Speciale cyber-crime, 9/2022,1158.

Aterno S., Acquisizione e analisi della prova informatica, in Diritto penale e processo, 2008, 60.

Aterno S., cisterna A., Il legislatore interviene ancora sulla data retention, ma non è finita, in Diritto penale e processo, 2009, 279.

Auricchio G., Il Cyberterrorismo, in Iaselli M. (a cura di), Investigazioni digitali, 718-728.

Bassoli E., Acquisizione dei tabulati vs. privacy: la data retention al vaglio della Consulta, in Rivista dell' internet, 2007, 237.

Biasiotti M. A., Epifani M., Turchi F., Opportunità e sfide per la prova elettronica, in Informatica e diritto, 2015, 1-2, 19.

Bohlander M., *"The Global Panopticon": Mass Surveillance and Data Privacy Intrusion as a Crime Against Humanity?*, in M. Bohlander, M. bose, O. Lagodny, A. Klip (eds.), *Justice Without Borders: Essays in Honour of Wolfgang Schomburg*, Leiden Boston, 2018, pp. 73-102.

Bovino C., Data retention: no all'obbligo generale di conservazione dei dati, in il quotidiano giuridico, 2017.

Braghò G., Le indagini informatiche tra esigenze di accertamento e garanzie di difesa, in dir. inf. e informatica, 2005, 524 ss.

Cajani F., Alla ricerca del log (perduto), in dir. internet, 2006, 572 ss.

Cajani F., Aterno S., Aspetti giuridici comuni delle indagini informatiche, in Aterno S., Cajani F., Costabile G., Attiucci M., Mazzaraco G., Computer forensics e indagini digitali, 2011.

Cajani F., Internet protocol. questioni operative in tema di investigazioni penali e riservatezza, in dir. internet. 2008, 545.

Calavita O., La proposta di regolamento sugli ordini di produzione e conservazione europei: commissione, consiglio e parlamento a cofronto, in La legislazione penale, 2021.

Cameron I., *Balancing Data Protection and Law Enforcement Needs: Tele2 Sverige and Watson*, in *Common Market Law Review*, n. 54, 2017, pp. 1467-1495.

Camon A., L'acquisizione dei dati sul traffico delle comunicazioni, in Rivista italiana diritto e procedura penale, 2005, 594.

Corona F., Il cybercrime: soggetto, oggetto e condotta, in Reati informatici e investigazioni digitali, Corona F. (a cura di), 2021, 19.

Costabile G., Rasetti D., Scena criminis, documento informatico e formazione della prova penale, in ciberspazio e diritto, 2003, 273.

Curtotti D., Indagini hi-tech, spazio cyber, scambi probatori tra Stati e internet provider service e "vecchia europa": una normativa che non c'è (ancora), in Diritto penale e processo, 6/2021, 745 ss.

D'Angelo L. A., La conservazione dei dati del traffico telefonico e telematico tra esigenze investigative e tutela della privacy, Dalia A.A. (a cura di), Le nuove norme di contrasto al terrorismo, 2006, 121 ss.

Dalia G., I reati informatici, in AA.VV. Manuale di diritto dell'informatica, 2016, 657-689.

Dominioni O, La prova penale scientifica, 2005, 37.

Dubuisson F., *La Cour européenne des droits de l'homme et la surveillance de masse*, in *Revue trimestrielle des droits de l'homme*, n. 108, pp. 855-886, 2016, p. 856.

41. Autorevole dottrina, sotto questo profilo, osserva che la disciplina della data retention pare oggi far prevalere le necessità legate alla tutela della riservatezza più che al progredire delle indagini penali S. Aterno, A. Cisterna, 2009, *Il legislatore interviene ancora sulla data retention, ma non è finita*, in *Dir. pen e proc*., p. 279.

Flor R., Data retention e limiti al potere coercitivo dello stato in materia penale: le sentenze del bundesverfasungsgericht e della curtea constitutionala, in Cass. pen., 2011, 1952.

Formici G., *La digital mass surveillance al vaglio della Corte europea dei diritti dell'uomo: da Zakharov a Big Brother Watch*, in Federalismi.it, n. 23, disponibile su www.federalismi.it/nv14/articolo-documento.cfm?Artid=43890, 2020, pp. 43-71, p. 54.

Ghirardini A., Faggioli G., Computer forensic, 2009, 347 ss.

Guariniello V.S.M., Le best practices in materia di computer forensics, in Iaselli M. (a cura di), Investigazioni digitali, 2020, 77 ss.

La Regina K., Le indagini su dispositivi digitali, in Investigazioni digitali, Iaselli M. (a cura di), 2020, 28-72.

Lucchetti M., L'acquisizione di informazioni sulla registrazione di nomi di dominio nelle investigazioni in materia di cybercrime (art. 6), in Diritto penale e processo. speciale cybercrime, 8/2022,1041-1044.

Luparia L., La disciplina processuale e le garanzie difensive, in Luparia L., Ziccardi G., Investigazione penale e tecnologia informatica, 2007, 130.

Luparia L., Ziccardi G., Investigazione penale e tecnologia informatica. L'accertamento del reato tra progresso scientifico e garanzie fondamentali, 2007, 178.

Mantelero A., The future of data protection: gold standards vs. global standard, in comp. law & sec. review. vol. 40, 2021, 105500.

Marafioti L., Digital evidence e processo penale, in Cass. pen., 2011, 4510.

Marcolini S., La giurisprudenza della corte di giustizia dell'unione europea sulla data retention: il baluardo dei diritti fondamentali in Europa, in Flor R., Marcolini S. (a cura di) Dalla data retention alle indagini ad alto contenuto tecnologico, 2022, 5.

Nino M., 2021, *La disciplina internazionale ed europea della data retention dopo le sentenze Privacy International e La Quadrature du Net della Corte di giustizia UE*, in *Il Diritto dell'Unione Europea*, n. 1, pp. 93-124, p. 94 ss.

Ojanen T., *Privacy Is More Than Just a Seven-Letter Word. The Court of Justice of the European Union Sets Constitutional Limits on Mass Surveillance - Court of Justice of the European Union, Decision of 8 April 2014* in *Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and Others, in European Constitutional Law Review*, 2014, pp. 528-541.

Orlandi R., Questioni attuali in tema di processo penale e informatica, in riv. dir. proc., 2009, 128 ss.

Peyrou S., *Arrêt «Tele2 Sverige»: l'interdiction du stockage de masse de données à caractère personnel réaffirmée par la Cour de justice de l'Union européenne*, in *Journal de droit européen*, n. 237, 2017, pp. 107-109.

Perri P., Le condizioni di salvaguardia e la protezione dei dati personali, in Diritto penale e processo, 9/2022,1150-1154.

Picotti L., Il diritto penale dell'informatica nell'epoca di internet, 2004, p. 86.

Pietrucci A., La responsabilità del provider per i contenuti illeciti della rete, in riv. crit. dir. priv., 2003.

Rafaraci T., Intercettazioni e acquisizione di tabulati telefonici, in Kostoris, R.E., Orlandi R. (a cura di), Contrasto al terrorismo interno e internazionale, 2006, 265 ss.

Rossi E. A., "Data protection" nei rapporti transnazionali tra imprese. Aspetti problematici della convenzione n. 108 del Consiglio d'Europa e del Regolamento (UE) 679/2016, in Studi sull'integrazione europea, 2019, 209 ss.

Ruggiero F., individuazione nel cyberspazio del soggetto penalmente responsabile e ruolo dell'internet provider, in Giur. merito, 2001.

Rusinova A., *European Perspective on Privacy and Mass Surveillance at the Crossroads*, disponibile suppers.ssrn.com/sol3/papers.cfm?abstr
2019, pp. 1-22, p. 6.

Signorile O., Computer forensic guidelines: un approccio metodico-procedurale per l'acquisizione e analisi delle digital evidence, in Ciberspazio e diritto, 2009.

Spiezia F., Cooperazione internazionale e tutela delle vittime nel cyberspazio, in Diritto penale e processo. Speciale cybercrime, 9/2022, 1142.

Tracol X., *The Judgment of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige and Watson Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level*, in *Computer Law & Security Review*, 2017, pp. 541-552.