Freedom, Security & Justice: European Legal Studies

Rivista giuridica di classe A

2023, n. 2

EDITORIALE SCIENTIFICA

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

Indice-Sommario
2023, n. 2

Editoriale

Saggi e Articoli

FOCUS

Convenzione europea dei diritti dell'uomo e delle libertà fondamentali e ordinamento italiano: nuovi sviluppi sostanziali e procedurali

Il Focus contiene i testi rivisti di alcune delle relazioni tenute in occasione del Convegno internazionale organizzato presso l'Università degli Studi di Salerno (17 aprile 2023)

Commenti e Note

DIGITALIZZAZIONE DELLA COOPERAZIONE GIUDIZIARIA INTERNAZIONALE IN MATERIA PENALE E TUTELA DEI DATI PERSONALI NEL DIRITTO UE: ALLA RICERCA DI UNA COMPATIBILITÀ (IM)POSSIBILE

Marco Buccarella*

SOMMARIO: 1. Il secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione giudiziaria internazionale. – 2. Il contrasto alla criminalità informatica nel contesto giuridico internazionale: il ruolo del Consiglio d'Europa e l'importanza della Convenzione di Budapest. – 2.1 *Segue*: l'impegno delle Nazioni Unite oltre la Convenzione di Budapest: verso un trattato globale sui crimini informatici. 3. La tutela dei dati personali nell'ambito delle indagini digitali transfrontaliere: le regole del Consiglio d'Europa. – 4. La firma e la ratifica del Secondo Protocollo da parte dei Paesi membri dell'Unione europea. – 5. Potenziali profili di incompatibilità con la normativa UE in materia di trattamento dei dati personali. – 6. Il Secondo Protocollo tra luci, ombre e proposte risolutive.

1. Il secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione giudiziaria internazionale

La tecnologia, oltre ad offrire nuove opportunità di sviluppo sul piano sociale, culturale ed economico, costituisce il terreno fertile per la proliferazione di sempre più resilienti forme di criminalità, che sfruttano l'elemento tecnologico sia per compiere reati sia al fine di eluderne l'azione di contrasto da parte delle autorità[1]. Simili manifestazioni

Articolo sottoposto a doppio referaggio anonimo.

* Dottorando di Ricerca in Scienze Giuridiche, Università di Foggia – Università di Siena. Indirizzo e-mail: marco.buccarella@unifg.it.

Il presente contributo rielabora e sviluppa, anche alla luce delle iniziative intraprese dalla Comunità internazionale nell'attività di contrasto al *cybercrime*, il contenuto della relazione pubblicata dall'Autore nell'ambito della Raccolta degli Atti del IV Convegno annuale dell'Associazione Italiana Studiosi del Diritto dell'Unione europea "*Ambiente, digitale, economia: l'Unione europea verso il 2030*", tenutosi presso l'Università degli Studi di Bari il 3 e 4 novembre 2022.

[1] Sul fenomeno della criminalità informatica e sull'emersione di nuove forme di reati, anche in rapporto all'evoluzione delle tradizionali categorie giuridiche, si veda R. FLOR, *Lotta alla "criminalità informatica" e tutela di "tradizionali" e "nuovi" diritti fondamentali nell'era di Internet*, in *DirittoPenaleContemporaneo.it*, 20 settembre 2012. Per un approfondimento sulla criminalità informatica nel quadro del diritto dell'Unione europea, cfr. L. PICOTTI, L*a nozione di "criminalità informatica" e la sua rilevanza per le competenze penali europee*, in *Rivista trimestrale di diritto penale dell'economia,*

criminose si sono tradotte, sul piano internazionale, in nuove sfide per gli Stati, chiamati ad implementare le modalità di cooperazione giudiziaria e di coordinamento delle autorità nazionali, in un quadro di profondi cambiamenti e di rinnovate esigenze. La rilevanza della problematica del *cybercrime*, nel contesto internazionale, è dimostrata dall'impegno assunto in proposito dalle Nazioni Unite, che nel 2019 hanno istituito un Comitato speciale (*Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes*), incaricato di condurre i negoziati per l'elaborazione di uno strumento giuridico pattizio volto a contrastare l'impiego degli strumenti tecnologici per scopi criminosi[2]. Ad oggi il Comitato ha articolato la propria attività nell'ambito di cinque sessioni di lavoro, tenutesi tra Vienna e New York; si è in attesa del sesto incontro, programmato a New York dal 21 agosto al 1° settembre 2023, e della sessione conclusiva, prevista nell'arco temporale 29 gennaio – 9 febbraio 2024[3].

Il quadro normativo internazionale in materia di cooperazione giudiziaria penale è stato di recente interessato da un nuovo strumento pattizio approvato dal Consiglio d'Europa, ovvero il *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and disclosure of electronic evidence* (d'ora in avanti il "Secondo Protocollo")[4]. Tale trattato, aperto alla firma degli Stati il 12 maggio 2022 ed ad oggi sottoscritto da quarantuno Paesi, contempla disposizioni volte a rafforzare la cooperazione tra gli Stati nelle attività di ricerca, reperimento e divulgazione delle c.d. prove digitali o elettroniche[5]. Le due materie principalmente interessate dal Secondo Protocollo, cioè la cooperazione giudiziaria in materia penale e il correlato trattamento dei dati personali, sono state oggetto di una pluralità di atti di diritto derivato in ambito UE[6] e trovano la loro base giuridica, rispettivamente, nell'art. 16 TFUE e nell'art. 82, par.

2011, n. 4, pp. 827 ss. Per una ricognizione delle fonti sovranazionali e delle competenze penali dell'UE nel contrasto alla criminalità informatica, cfr. U. SIEBER, *Computerkriminalität*, in U. SIEBER, F. H. BRÜNER, H. SATZGER, B. VON HEINTSCHEL-HEINEGG (hrsg.), *Europäisches Strafrecht*, Baden-Baden, 2011, pp. 393 ss.

[2] Risoluzione dell'Assemblea Generale ONU del 20 gennaio 2019, A/RES/74/247. Per un approfondimento in proposito, si veda A. MATTARELLA, *La futura convenzione ONU sul cybercrime e il contrasto alle nuove forme di criminalità informativa*, in *Sistema Penale*, 2022, n. 3, pp. 41-75.

[3] Per un resoconto sulle attività e sullo stato di avanzamento dei lavori, è possibile consultare la Sezione del sito delle Nazioni Unite dedicata al Comitato, liberamente consultabile al seguente link: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

[4] Consiglio d'Europa, Secondo Protocollo aggiuntivo alla Convenzione sulla criminalità informatica sulla cooperazione rafforzata e la divulgazione delle prove elettroniche, STCE n. 224.

[5] Sulla portata, sul significato e sul contenuto del nuovo accordo addizionale alla Convenzione di Budapest, si vedano i contributi che compongono lo Speciale dedicato al Secondo Protocollo, suddiviso in due parti e pubblicato in *Diritto Penale e Processo*, 2022, n. 8, pp. 1017-1060, e n. 9, pp. 1137-1174. In merito alla relazione intercorrente, in generale, tra le misure previste dal Secondo Protocollo e la disciplina contenuta nel Regolamento del Consiglio (UE) 2017/1939 del 12 ottobre 2017 che istituisce la Procura europea (EPPO) si veda A. PROCACCINO, *Il Secondo Protocollo e le indagini della Procura europea*, in *Diritto Penale e Processo*, 2022, n. 9, pp. 1168 ss.

[6] Per un approfondimento sugli atti di diritto derivato in materia e, più in generale, sul Secondo Protocollo nel quadro del diritto internazionale e del diritto dell'Unione europea, cfr. G.M. RUOTOLO, *Il Secondo Protocollo alla Convenzione cybercrime sulle prove elettroniche tra diritto internazionale e relazioni esterne dell'Unione europea*, in *Diritto Penale e Processo*, 2022, n. 8, pp. 1022 ss.

1, TFUE. Giova poi precisare, rispetto al quadro normativo dell'Unione e alle libertà sancite dai Trattati, che il diritto alla protezione dei dati personali rappresenta un diritto autonomo[7] e fondamentale[8], tutelato da norme di rango primario e peraltro oggetto di uniformazione[9] e di armonizzazione[10]. Un simile contesto di norme comuni postula la riconducibilità del nuovo accordo addizionale alla Convenzione di Budapest all'art. 3, par. 2, TFUE e, quindi, all'ambito di competenza *esclusiva* dell'Unione a concludere accordi internazionali[11]. Gli Stati membri sono perciò stati autorizzati prima a firmare[12] e poi a ratificare[13], nell'interesse dell'Unione[14], il Secondo Protocollo, atteso che le sue disposizioni "rientrano in un settore disciplinato in larga misura da norme comuni ai sensi dell'articolo 3, paragrafo 2, del trattato sul funzionamento dell'Unione europea (TFUE), compresi gli strumenti che agevolano la cooperazione giudiziaria in materia penale, garantendo norme minime in materia di diritti processuali e garanzie in merito alla protezione dei dati e alla riservatezza"[15]. Del resto, l'autorizzazione in favore dei Paesi membri si è resa necessaria, sia per la firma che per la ratifica del Secondo Protocollo, giacché "solo gli Stati possono esserne parti"[16].

---

[7] A seguito dell'entrata in vigore del Trattato di Lisbona, che ha conferito forza vincolante alla Carta dei diritti fondamentali dell'Unione europea (c.d. Carta di Nizza) e dunque anche all'art. 8 che contempla il diritto alla protezione dei dati personali, quest'ultimo è da considerarsi quale situazione giuridica soggettiva autonoma rispetto al diritto alla privacy. In proposito, cfr. F. ROSSI DAL POZZO, *La tutela dei dati personali nella giurisprudenza della Corte di Giustizia*, in *rivista.eurojus.it*, 2018, pp. 1-24 e in part. pp. 9-12; W. VAN BALLEGOOIJ, *Data protection and general principles of EU law*, in K.S. ZIEGLER, P.J. NEUVONEN, V. MORENO-LAX (eds.), *Research Handbook on General Principles in EU Law. Constructing Legal Orders in Europe*, Cheltenham, 2022, 545-562. Sulla distinzione tra diritto alla privacy e diritto alla protezione dei dati personali nell'ambito delle attività di accertamento e perseguimento dei reati, si veda S. RICCI, *Il trattamento dei dati personali a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *I dati personali nel diritto europeo*, Torino, 2019, pp. 1130 ss.

[8] Cfr. G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018, n. 1, pp. 9 ss.; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016.

[9] Cfr. GDPR.

[10] Cfr. Direttiva 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002, relativa al "trattamento dei dati personali e la tutela della vita privata nel settore delle comunicazioni elettroniche"; Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa 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".

[11] S. LORENZMEIER, R. PETROV, C. VEDDER (a cura di), *EU External Relations Law. Shared Competences and Shared Values in Agreements Between the EU and Its Eastern Neighbourhood*, Cham, 2021; L. AZOULAI (a cura di), *The Question of Competence in the European Union*, Oxford, 2014.

[12] Decisione 2022/722 del Consiglio del 4 aprile 2022 che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche.

[13] Decisione 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 sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche.

[14] Sulla base degli artt. 16, 82, par. 1, e 218, par. 6, TFUE.

[15] Considerando 3 della Decisione 2022/722 del Consiglio del 4 aprile 2022 e della Decisione 2023/436 del Consiglio del 14 febbraio 2023.

[16] Considerando 13 della Decisione 2022/722 e della Decisione 2023/436, cit.

Nell'ambito del presente lavoro ci si interrogherà sul rapporto tra le previsioni del Secondo Protocollo e la disciplina dell'Unione europea in materia di protezione dei dati personali, onde verificare la sussistenza di eventuali profili di incompatibilità. Dopo un preliminare inquadramento del contesto giuridico internazionale in cui si innesta il secondo accordo aggiuntivo alla Convenzione di Budapest (§ 2 e § 2.1), ci soffermeremo sulle previsioni del Secondo Protocollo in materia di protezione dei dati personali (§ 3) e sulle indicazioni fornite dall'Unione ai fini della firma e della ratifica del nuovo trattato da parte degli Stati membri (§ 4). Il successivo raffronto tra la disciplina del Secondo Protocollo in materia di *data protection* e la rilevante normativa e giurisprudenza UE (§ 5), consentirà di svolgere alcune riflessioni conclusive sul grado di *privacy compliance* del nuovo trattato e sulle possibili implicazioni sui diritti delle persone fisiche sottoposte ad attività di indagine e accertamento a carattere transfrontaliero (§ 6).

2. Il contrasto alla criminalità informatica nel contesto giuridico internazionale: il ruolo del Consiglio d'Europa e l'importanza della Convenzione di Budapest

Prima di approfondire gli aspetti rilevanti del rapporto tra il Secondo Protocollo e la normativa UE in materia di *data protection*, conviene soffermarsi brevemente sul trattato internazionale cui accede l'accordo addizionale in commento, cioè la Convenzione del Consiglio d'Europa di Budapest del 2001 (c.d. Convenzione di Budapest)[17]. Si tratta del primo strumento giuridico internazionale pattizio che, nell'introdurre nozioni di tipo tecnico in materia digitale[18], ha predisposto un sistema di cooperazione volto a contrastare gli illeciti commessi con e sulla rete, tendenzialmente caratterizzati da atemporalità e aterritorialità[19]. In questa categoria rientra un'ampia gamma di infrazioni, che vanno dalle violazioni di *copyright* ai reati in materia di pornografia minorile. Con la Convenzione di Budapest, si è dato avvio ad un nuovo corso di politica comune in materia di criminalità informatica, ispirato ai due obiettivi che guidano l'attività del Consiglio d'Europa: armonizzazione normativa e cooperazione internazionale[20]. Giova precisare che tale accordo si è innestato nel quadro internazionale di tutele in precedenza delineato, in materia di privacy e trattamento dei dati personali, dall'art. 8 della Convenzione europea

[17] Consiglio d'Europa, *Convenzione sulla criminalità informatica*, STE n. 185, aperta alla firma il 23 novembre 2001 ed entrata in vigore il 1° luglio 2004. Per un approfondimento sul contenuto della Convenzione nella prospettiva dell'ordinamento italiano, v. L. PICOTTI, *Ratifica della convenzione cybercrime e nuovi strumenti di contrasto contro la criminalità informatica e non solo*, in *Diritto dell'internet*, 2008, n. 5, 437-448.

[18] Tra cui, ad esempio, le definizioni di *computer data* o *service provider*.

[19] Per un approfondimento sulle disposizioni contemplate dalla Convenzione di Budapest, cfr. J. CLOUGH, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization*, in *Monash University Law Review*, vol. 40, 2014, n. 3; M. KEYSER, *The Council of Europe Convention on Cybercrime*, in *Journal of Transnational Law & Policy*, vol. 12.2, 2003.

[20] Lo strumento principale d'azione del Consiglio d'Europa consiste nel predisporre e favorire la stipulazione di accordi o convenzioni internazionali tra gli Stati membri e, spesso, anche tra Paesi terzi, tali da costituire la base per l'armonizzazione delle legislazioni nazionali e la cooperazione internazionale.

per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU)[21] e dalla Convenzione n. 108 del Consiglio d'Europa, il primo strumento giuridico internazionale applicabile anche ai trattamenti di dati effettuati dalle autorità per finalità di prevenzione, accertamento e repressione dei crimini[22].

Le iniziali incertezze che hanno accompagnato l'*iter* di approvazione della Convenzione di Budapest hanno lasciato posto alla sempre più diffusa consapevolezza, da parte degli Stati, dell'effettiva utilità di un trattato vincolante volto a delineare un quadro giuridico di cooperazione condiviso, indispensabile per l'attività di contrasto ai crimini informatici. Questa consapevolezza ha trovato una prima conferma nel 2006, quando il Consiglio d'Europa, dopo appena due anni dall'entrata in vigore della Convenzione di Budapest, ha approvato un primo Protocollo addizionale, incentrato sull'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici[23]. Il 17 novembre 2021, a distanza di vent'anni dall'apertura alla firma della Convenzione sul *cybercrime*, il Comitato dei Ministri del Consiglio d'Europa è nuovamente intervenuto in materia, approvando il Protocollo *de quo*. Come si è detto, il fine di tale trattato è rafforzare, anche oltre i confini territoriali, i poteri spettanti agli organismi preposti all'applicazione della legge nell'ambito delle attività di reperimento, archiviazione e impiego delle prove digitali[24]. Lo stesso Consiglio d'Europa, in un proprio comunicato ufficiale risalente alla fine del 2021, ha definito il Secondo Protocollo come uno strumento finalizzato a potenziare "*its legal arsenal*"[25], in materia di contrasto alla criminalità informatica.

Come si evince dalla breve disamina condotta sin qui, l'accordo di recente sottoscritto si pone nel solco tracciato dalla Convenzione di Budapest, fornendo la base giuridica per la cooperazione tra gli Stati nello specifico ambito delle indagini digitali e delle attività di raccolta e utilizzo delle prove elettroniche. Nella prospettiva del Consiglio d'Europa, la proliferazione di crimini informatici può essere contrastata riducendo gli effetti negativi dovuti alla disconnessione tra la giurisdizione territoriale degli Stati e alle farraginose modalità di trasmissione di dati e informazioni oltre i confini nazionali. In tal senso il Secondo Protocollo contempla, oltre a previsioni di carattere più generale, specifiche disposizioni a carattere tecnico, volte ad agevolare, *rectius* accelerare, le procedure di comunicazione tra autorità statali e fornitori di servizi e, quindi, la divulgazione di dettagliate informazioni sugli abbonati, sui dati di traffico e sulla

[21] L'articolo 8 della CEDU è stato storicamente interpretato dalla Corte Europea dei Diritti dell'Uomo (Corte EDU) come norma, a carattere generale, finalizzato principalmente alla fondamentale tutela dalle ingerenze arbitrarie, da parte di un'autorità pubblica, nella vita privata e familiare, nel domicilio e nella corrispondenza delle persone fisiche. Cfr. *ex multis* Corte EDU, sentenza del 27 ottobre 1994, 18535/91, *Kroon and Others v. the Netherlands*.

[22] Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale*, Strasburgo, 28 gennaio 1981.

[23] Consiglio d'Europa, *Protocollo addizionale alla Convenzione sulla criminalità informatica, relativo all'incriminazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici*, STE n. 189.

[24] Cfr. D. CURTOTTI, *Speciale sul Secondo Protocollo addizionale alla Convenzione di Budapest. Premessa*, in *Diritto Penale e Processo*, 2022, n. 8, pp. 1017 ss.

[25] Consiglio d'Europa, Comunicato del 17 novembre 2021, Ref. DC 207(2021).

registrazione dei nomi di dominio. Ciò spiega il motivo per cui le nuove previsioni in materia di indagini digitali interessano non soltanto le competenti autorità dei Paesi, bensì anche prestatori di servizio privati, come i gestori dei *provider* o le società fornitrici dei servizi di telecomunicazione[26]. L'applicabilità di alcune previsioni del Secondo Protocollo anche nei confronti di tali soggetti si spiega in ragione della tipologia dei servizi erogati dai privati, consistenti per lo più in piattaforme digitali ove possono transitare (ed essere conservate) tracce o elementi determinanti ai fini della ricostruzione dei fatti di reato.

2.1. *Segue*: l'impegno delle Nazioni Unite oltre la Convenzione di Budapest: verso un trattato globale sui crimini informatici

Il quadro di cooperazione definito dalla Convenzione di Budapest, quale principale strumento vincolante ad oggi vigente in materia di *cybercrime*, sembrerebbe destinato ad evolversi[27], atteso il progressivo avanzamento dei lavori del già citato Comitato ONU, preposto all'elaborazione di un trattato internazionale sui crimini informatici. Le attività del Comitato, cui stanno partecipando anche due rappresentanti del Consiglio d'Europa, dovrebbero concludersi, stando al calendario dei lavori, nella sessione finale prevista per febbraio 2024. Il Comitato *ad hoc*, in vista della sesta e penultima sessione di lavori in programma a New York dal 21 agosto al 1° settembre 2023, ha diffuso la bozza del testo del trattato «on countering the Use of Information and Communications Technologies for Criminal Purposes»[28]. La versione del trattato ad oggi divulgata – e che dovrebbe essere definitivamente adottata nei primi mesi del 2024 – si compone di sessantasette articoli, suddivisi in nove capitoli. Tale bozza, oltre a contemplare norme generali di carattere introduttivo (Capitolo I "General Provisions"– artt. 1-5) e conclusivo (Capitolo IX "Final Provisions"– artt. 59-67), reca disposizioni volte a disciplinare: i fenomeni criminosi transazionali rilevanti ai fini del trattato (Capitolo II "Criminalization" – artt. 6-21); i conseguenti criteri di giurisdizione (Capitolo III "Jurisdiction" – art. 22); specifiche questioni procedurali (Capitolo IV "Procedural measures and law enforcement" – artt. 23-34); i meccanismi di cooperazione internazionale (Capitolo V "International Cooperation" – artt. 35-52); iniziative e misure volte ad impedire la commissione di crimini informatici (Capitolo VI "Preventive measures" – artt. 53-58). L'approvazione del nuovo trattato delle Nazioni Unite dovrebbe essere funzionale, almeno nelle aspettative, all'implementazione degli strumenti internazionali vigenti in materia di *cybercrime*; l'idea sottesa all'istituzione del Comitato *ad hoc* è infatti quella di potenziare

[26] Cfr. P. PERRI, *Le condizioni di salvaguardia e la protezione dei dati personali*, in *Diritto Penale e Processo*, 2022, n. 9, pp. 1150 ss.
[27] Sul tema della cooperazione giudiziaria in materia penale, si veda, per un approfondimento ulteriore e aggiornato rispetto al quadro giuridico internazionale, M. CHIAVARIO, A. PERDUCA, *Cooperazione giudiziaria internazionale in materia penale*, Torino, 2022.
[28] La bozza del trattato è stata pubblicata sul sito ufficiale ONU ed è liberamente consultabile al seguente link: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session.

il quadro di cooperazione *illo tempore* delineato dalla Convenzione di Budapest, soprattutto ampliandone la base in termini di consenso e partecipazione da parte degli Stati[29]. Tuttavia, proprio il coinvolgimento di un maggior numero di soggetti nella fase di negoziazione[30] e, quindi, il fronteggiarsi di differenti prospettive si stanno frapponendo al raggiungimento dell'obiettivo delle Nazioni Unite di approvare una disciplina più completa in materia, anche tramite l'individuazione di definizioni normative condivise in ambito internazionale. Detta difficoltà trova conferma nell'omesso inserimento, nella bozza del trattato, del fondamentale concetto di "cybercrime" e nella circostanza che ancora sussiste una discussione, in seno al Comitato, con riferimento al significato da attribuire alle nozioni di "Computer system", "Information and communications technology device", "Computer data" e "Digital information"[31].

Ci è impossibile approfondire in questa sede il contenuto di quella che ancora costituisce solo una bozza del futuro accordo[32], ma per quanto rileva con riferimento al presente lavoro e al tema della protezione dei dati personali nell'UE, ci limitiamo ad osservare come la versione ad oggi diffusa sia sostanzialmente priva di disposizioni dedicate alla *data protection*. In particolare, nell'ambito della bozza dell'accordo si rinviene un generico riferimento alla privacy solo nel Preambolo, nella parte in cui gli Stati riconoscono "the right to protection against unlawful interference with privacy, including the protection of personal data"[33]. Clausole di carattere ancor più generale sono poi contemplate dagli artt. 5 "Respect for human rights" e 24 "Conditions and safeguards", che impongono agli Stati il rispetto dei diritti umani. L'omessa previsione di una disciplina *ad hoc* in materia di *data protection* non sembra collimare con il quadro normativo internazionale[34], atteso che eventuali restrizioni al diritto alla privacy, come riconosciuto dalla Dichiarazione Universale dei diritti umani[35] e dal Patto sui diritti civili

[29] Cfr. Risoluzione dell'Assemblea Generale ONU del 20 gennaio 2019, cit.
[30] Alle attività del Comitato hanno peraltro preso parte un discreto numero di *stakeholders* e soggetti privati. L'elenco degli *stakeholders* è consultabile, per ciascuna delle sessioni di lavoro, nella già citata Sezione del sito ONU dedicata al Comitato *ad hoc*, liberamente consultabile al seguente link: https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.
[31] Cfr. art. 1 del *Draft text of the Convention*, 29 maggio 2023, liberamente consultabile al seguente link: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session.
[32] Per un commento alla bozza del trattato ad oggi diffusa, si vedano J. BANDLER, *The Proposed UN Cybercrime Treaty and a Path Forward*, in *New York Law Journal*, 25 maggio 2023 e il *policy brief* di S. WALFER, *Still poles apart. UN cybercrime treaty negotiations*, Ginevra, giugno 2023, pubblicato per conto di *Global Initiative Against Transnational Organized Crime*.
[33] Cfr. Preambolo, punto 12, del *Draft text of the Convention*, 29 maggio 2023, liberamente consultabile al seguente link: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session.
[34] Per completezza espositiva, giova precisare che il quadro normativo internazionale si compone di strumenti giuridici incentrati quasi esclusivamente sul trattamento dei soli dati personali, relativi cioè a soggetti identificati o quanto meno identificabili; pertanto, nel prosieguo si farà riferimento solo alla tutela dei *personal data* e non anche dei c.d. big data non personali, ancorché utilizzati dagli Stati nell'ambito di specifici programmi informatici per la prevenzione dei crimini. Per un approfondimento sul tema dei *big data* non personali e della loro progressiva emersione nel diritto internazionale e dell'Unione europea, si veda G.M. RUOTOLO, *The God that failed. La tutela dei co-patterners nell'ordinamento internazionale ed europeo, in Rivista di diritto dei media,* 2018, n. 3, p. 191 ss.; G.M. RUOTOLO, *I dati non personali: l'emersione dei big data nel diritto dell'Unione europea,* in *Studi sull'integrazione europea,* 2018, p. 97 ss.
[35] Cfr. Assemblea Generale delle Nazioni Unite, *Dichiarazione Universale dei diritti umani*, 10 dicembre 1984, art. 12.

e politici[36], devono essere adottate nel rispetto dei criteri di legittimità e di non arbitrarietà. Infatti, la prassi del Comitato per i diritti umani delle Nazioni Unite comprova che ogni misura implicante una limitazione alla privacy delle persone fisiche, finanche attuata per ragioni di sicurezza[37], deve fondarsi su norme di legge chiare e dimostrarsi necessaria e proporzionata al fine da perseguire[38].

Rispetto al contesto giuridico dell'Unione europea, la totale assenza, nell'ambito della bozza del trattato ONU, di previsioni in materia di *data protection* si pone in contrasto con le indicazioni precedentemente fornite dall'*European Data Protection Supervisor* (EPDS), competente a vigilare sul rispetto del diritto alla protezione dei dati personali da parte di organismi e istituzioni UE[39]. L'EPDS, nell'esprimere un parere sulla decisione del Consiglio UE che ha autorizzato la partecipazione della Commissione ai lavori del Comitato ONU[40], aveva rimarcato le responsabilità dell'Unione rispetto ad ogni forma di trasferimento dei dati personali verso Paesi terzi[41]. Sul piano generale, l'EPDS aveva quindi auspicato, da un lato, l'elaborazione di norme specifiche a presidio del diritto alla protezione dei dati personali e, dall'altro, la prevalenza, in luogo del futuro accordo ONU, dei maggiori standard di tutela previsti dagli altri trattati – anche bilaterali – vigenti in materia. Sotto il profilo tecnico-operativo, l'EPDS aveva poi formalizzato raccomandazioni in merito alla necessità di: a) prevedere regimi di tutela differenziati sulla base della tipologia dei dati oggetto di trattamento; b) escludere ogni forma di cooperazione diretta, implicante un trasferimento transfrontaliero di dati personali, tra Paesi e fornitori di servizi privati; 3) allegare al trattato un elenco delle autorità competenti, per ciascuno Stato, a ricevere dati personali in applicazione delle misure di cooperazione[42]. Il raffronto tra la bozza ad oggi diffusa dal Comitato *ad hoc* e le raccomandazioni del'EPDS dimostra come, nell'ipotesi in cui tale versione dovesse essere condivisa e proposta per la sottoscrizione da parte degli Stati, potrebbero emergere

[36] Cfr. Assemblea Generale delle Nazioni Unite, *Patto Internazionale sui diritti civili e politici*, 16 dicembre 1966, art. 17.
[37] Sul concetto di sicurezza nell'era digitale e sul tema dell'equilibrio tra riservatezza ed esigenze securitarie cfr. G. DE VERGOTTINI, *Una rilettura del concetto di sicurezza nell'era digitale e delle emergenza normalizzata*, in *Rivista AIC*, 2019, n. 9, p. 66 ss.
[38] Cfr. *CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 8 aprile 1988, in part. par. 7.
[39] Cfr. artt. 52, parr. 2 e 3, del Regolamento (UE) 2018/1725 «sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE».
[40] EPDS, *Opinion 9/2022 on the Recommendation for a Council Decision authorising the negotiations for a comprehensive international convention on countering the use of information and communications technologies for criminal purposes*, 18 maggio 2022.
[41] In proposito si veda, in una prospettiva più generale, F. BORGIA, *Profili critici in materia di trasferimento dei dati personali verso Paesi extra-europei*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *op. cit.*, pp. 129 ss.
[42] Cfr. EPDS, *Opinion 9/2022*, pp. 14-15.

numerosi problemi di compatibilità del futuro trattato ONU con il quadro giuridico dell'Unione europea[43].

3. La tutela dei dati personali nell'ambito delle indagini digitali transfrontaliere: le regole del Consiglio d'Europa

Dal momento che il Secondo Protocollo incentiva la cooperazione nell'ambiente digitale, uno dei temi che assume maggiore rilevanza è quello della protezione dei dati personali degli interessati[44]. Gli strumenti informatici, infatti, sono notoriamente contenitori di informazioni riguardanti la personalità dell'individuo e dei terzi che hanno rapporti con quest'ultimo[45]; ne consegue che un trattamento non corretto dei dati potrebbe tradursi in violazioni del diritto fondamentale alla riservatezza e, per altro verso, determinare errori investigativi[46].

La particolare sensibilità europea nei confronti del fondamentale diritto alla protezione dei dati personali, quale caposaldo dell'impianto normativo di cui l'Unione si è dotata in ambito *privacy*[47], spiega l'opportunità di interrogarsi sul rapporto che intercorre tra il quadro giuridico UE in materia e le nuove norme previste dal Secondo Protocollo. Nell'ambito di tale accordo, una risposta giuridica ai timori in materia di *data protection* si rinviene negli artt. 13 e 14, rispettivamente rubricati "Condizioni e garanzie" e "Protezione dei dati personali". Le due disposizioni sono tra loro strettamente connesse, nella misura in cui l'art. 13 richiama il contenuto all'art. 15 della Convenzione di Budapest e quindi il rispetto, oltre che dei diritti umani e delle libertà fondamentali, anche del principio di proporzionalità[48]. Si tratta di un principio espressamente riconosciuto

[43] Tale preoccupazione è stata del resto formalizzata anche durante i lavori della quinta sessione, nell'ambito della quale la delegazione dell'Italia, nel condividere gli emendamenti proposti dall'UE all'art. 57 della bozza di trattato, ha rimarcato l'importanza di "include in this article conditions and specific data protection safeguards, recognising the requirements we have to protect privacy and personal data in order to meet our constitutional and international obligations". Cfr. *Statement by ITALY at the Fifth Negotiating Session of the Ad-hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes 11 April 2023*, liberamente consultabile sul sito delle Nazioni Unite al seguente link: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents.

[44] Nel quadro regolatorio dell'Unione, si utilizza la nozione di "interessato" per identificare, in generale, la persona fisica cui si riferiscono i dati oggetto di trattamento. Cfr. art. 4, par. 1, n. 1), del Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla "protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" (c.d. GDPR).

[45] In proposito, cfr. sentenza della Corte EDU del 4 dicembre 2015, *Roman Zakharov v. Russia*, 47143/06.

[46] P. PERRI, *op. cit.*, in *Diritto Penale e Processo*, 2022, n. 9, p. 1152.

[47] Per una ricostruzione sistematica della normativa UE in materia cfr. L. CALIFANO, *Il Regolamento UE 2016/679 e la costruzione di un modello uniforme di diritto europeo alla riservatezza e alla protezione dei dati personali*, in L. CALIFANO, C. COLAPIETRO (a cura di), *Innovazione tecnologica e valore della persona Il diritto alla protezione dei dati personali nel Regolamento UE 2016/679*, Napoli, 2017, pp. 3 ss.

[48] Si veda V. FIORILLO, *Il principio di proporzionalità da parametro di validità a fondamento del diritto alla protezione dei dati personali nella recente giurisprudenza della Corte di Giustizi*a, in *Federalismi.it*, 2017, n. 15, pp. 22 ss.

dalla Carta di Nizza, all'art. 52, par. 1, notoriamente adoperato dalla Corte di Giustizia UE[49] e dalla Corte europea dei diritti dell'uomo[50] come parametro di giudizio, per valutare la compatibilità di misure statali – di controllo, sorveglianza o sicurezza – con le norme fondanti la disciplina in materia di *data protection*[51]. È evidente, dunque, il legame tra l'art. 13 (che rinvia all'art. 15 della Convenzione di Budapest) e il successivo art. 14 del Secondo Protocollo, recante specifiche disposizioni in materia di trattamento e protezione dei dati personali.

Da una prima lettura dell'art. 14 – che consta di ben quindici commi – si può evincere una certa identità dei principi ivi espressi rispetto quelli contemplati dalla Convenzione 108 del Consiglio d'Europa[52], ma anche e soprattutto dal Regolamento (UE) 2016/679, noto come GDPR. Nel testo dell'art. 14 del Secondo Protocollo si rinvengono infatti riferimenti ai principi della finalità del trattamento (par. 2), al principio della qualità del dato (par. 3), alla natura "sensibile" dei dati (par. 4), ai periodi di conservazione (par. 5) e al divieto di assumere decisioni sulla base unicamente di un trattamento automatizzato (par. 6)[53]. Quest'ultimo paragrafo assume particolare rilevanza, specie per quei Paesi che – per tradizione normativa – sono, da un lato, meno sensibili al tema della protezione dei dati personali e, dall'altro, risultano maggiormente inclini all'utilizzo di applicazioni di giustizia predittiva e di *analytics* nell'ambito delle attività di indagine[54]. Il principale elemento che dimostra l'influenza della normativa dell'Unione[55] sul nuovo accordo

[49] Cfr. *ex multis* Corte di Giustizia, Grande Sezione, sentenza del 6 ottobre 2020, *Privacy International contro il Ministro degli Affari Esteri e del Commonwealth ed il Ministro dell'Interno*, C-511/18, C-512/18 e C-520/18; Corte di Giustizia, Grande Sezione, sentenza del 6 ottobre 2020, *La Quadrature du Net e a. contro Premier Ministre e a.*, C-623/17; Corte di Giustizia, Grande Sezione, sentenza del 16 luglio 2020, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, C-311/18; Corte di Giustizia, Grande Sezione, sentenza del 2 ottobre 2018, *Ministerio Fiscal*, C-207/16; Corte di Giustizia, Grande Sezione, sentenza del 21 dicembre 2016, *Tele 2 Sverige contro Watson*, C-203/15 e C-698/15; Corte di Giustizia, Grande Sezione, sentenza del 6 ottobre 2015, *Maximillian Schrems contro Data Protection Commissioner*, C-362/14; Corte di Giustizia UE, sentenza dell'8 aprile 2014, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources et al. and Kärntner Landesregierung et al*.;

[50] Cfr. *ex multis* Corte europea dei diritti dell'uomo, sentenza del 25 maggio 2021, *Big Brother Watch and Others v. the United Kingdom*; Corte europea dei diritti dell'uomo, sentenza del 12 gennaio 2016, *Szabò e Vissy v. Hungary*; Corte europea dei diritti dell'uomo, sentenza del 4 dicembre 2015, *Roman Zakharov v. Russia*.

[51] Tra cui rientrano gli artt. 1 e 8 della CEDU.

[52] Si tratta del primo strumento giuridico internazionale vincolante in materia di protezione dei dati personali. Consiglio d'Europa, *Convenzione sulla protezione delle persone rispetto al trattamento automatizzato dei dati a carattere personale*, c.d. Convenzione n. 108, del 28 gennaio 1981; Consiglio d'Europa, *Protocollo di emendamento alla Convenzione n. 108*, 10 ottobre 2018.

[53] Per un approfondimento sui principi contemplati dal GDPR, M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, in *I dati personali nel diritto europeo*, in V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *op. cit.*, p. 179 ss.; L. BOLOGNINI, *Principi del trattamento,* in L. BOLOGNINI, E. PELINO, C. BISTOLFI (a cura di), *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla , protezione dei dati personali*, Milano, 2016, pp. 94 ss.

[54] Si pensi, ad esempio, alle tecniche di riconoscimento facciale impiegate per l'individuazione di persone ricercate. Simili sistemi si sono spesso rivelati inefficaci e pericolosi in molti casi in cui il ricercato apparteneva a un determinato gruppo etnico. In proposito, cfr. F. BACALU, *Biometric Facial Recognition Technology, Law Enforcement Algorithmic Automation, and Data-driven Predictive Policing Systems in Human Rights Protections and Abuses*, vol. 21, 2022, pp. 38 ss.

[55] In un'ottica più generale, la riconducibilità di alcune delle norme del Secondo Protocollo al GDPR confermerebbe la tesi secondo cui la regolamentazione UE in materia di tecnologia e *data protection* ha

addizionale alla Convenzione di Budapest si rinviene nell'*accountability*, principio cardine del GDPR e simbolo dell'approccio adottato dal legislatore dell'Unione in materia[56]. Evocando la funzione propria di tale principio, il paragrafo 8 dell'art. 14 del Secondo Protocollo impone agli Stati parti di rendere conto delle attività di trattamento dei dati personali, documentandone le modalità di raccolta, utilizzo e divulgazione. Il significato dell'*accountability*, infatti, risiede proprio nel termine "dimostrare", che fa sorgere in capo alle Parti l'obbligo di strutturare un sistema di procedure e modelli mediante i quali illustrare come e per quale scopo sono stati trattati i dati di una persona fisica, finanche nell'ambito di attività di indagini digitali e per il perseguimento di reati informatici. Una simile previsione postula l'obbligo in capo agli Stati di dimostrare la correttezza delle scelte compiute, rispetto al quadro giuridico vigente, nell'individuazione delle misure giuridiche, organizzative e tecniche adottate in concreto.

Un altro punto di contatto, specificamente riguardante il rapporto tra la disciplina UE in materia di trattamento dei dati personali e le previsioni del Secondo Protocollo, si può individuare nell'obbligo di comunicare eventuali incidenti di sicurezza alle competenti Autorità nazionali (eventualmente indicate dai singoli Paesi) e agli interessati (par. 7). Si tratta di una procedura che ricalca in larga misura le metodologie del GDPR, fondate su approccio preventivo di analisi del rischio tale da consentire di individuare *ex ante* misure proporzionate alla probabilità e all'impatto di eventuali incidenti informatici[57]. Rispetto all'approccio utilizzato in ambito UE e suggerito in fase di consultazione dall'*European Data Protection Board* (EDPB)[58], si può tuttavia riscontrare una differenza di non poco conto. L'accordo aggiuntivo alla Convenzione di Budapest, infatti, contempla un'eccezione all'obbligo di comunicare eventuali incidenti di sicurezza all'Autorità competente o agli interessati, prevedendo che tale notifica possa essere ritardata o persino omessa "qualora metta a repentaglio la sicurezza nazionale" o, comunque, ritardata nell'ipotesi in cui rischi di "compromettere misure di protezione della sicurezza pubblica". Si tratta di un'eccezione non disciplinata in ambito UE, che solleva non pochi interrogativi dovuti alla nota difficoltà di definire, in materia di trattamento dei dati personali, il concetto di "sicurezza nazionale" o di "sicurezza pubblica"[59].

influenzato (e sta influenzando) il contenuto di accordi internazionali, con conseguenti implicazioni anche sulle normative di Paesi terzi. In proposito, cfr. E. FAHEY, *The EU as a Global Digital Actor Institutionalising Global Data Protection, Trade, and Cybersecurity*, 2022. In proposito si veda inoltre, anche per ulteriori riferimenti bibliografici, G.M. RUOTOLO, *op. cit.*, pp. 1022-1023.

[56] G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati personali*, in *Nuove Leggi civili commentate*, 2017, n. 1, pp. 2 ss. Per una definizione completa di *accountability*, v. anche la Relazione illustrativa al decreto legislativo recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR.

[57] Per un approfondimento in materia, si veda R. GELLERT, *The Risk-based Approach to Data Protection*, Oxford, 2020.

[58] Cfr. *Statement* dell'EDPB del 13 novembre 2019; *Statement* dell'EDPB n. 2/201; *Contribution* dell'EDPB del 4 maggio 2021.

[59] Sulla difficoltà di distinguere, ai fini della qualificazione del trattamento, la nozione di "sicurezza nazionale" dai concetti limitrofi di "pubblica sicurezza", "sicurezza dello Stato" e "difesa", si veda l'*Opinion* dell'*European Data Protection Supervisor* (EDPS) del 7 marzo 2012.

Il Secondo Protocollo ha poi anche recepito il principio della trasparenza[60], prevedendo l'obbligo di fornire informazioni al soggetto interessato in ordine alle finalità, alle modalità e al soggetto titolare del trattamento. Si tratta di una disposizione particolarmente importante nella prospettiva degli Stati membri dell'Unione, atteso che le informazioni sul trattamento assumono rilevanza anche rispetto ad un eventuale ricorso alle vie giudiziali ed extragiudiziali[61], spesso indispensabili per tutelare i cittadini da illegittimi trattamenti transfrontalieri dei dati. A completamento di questa sintetica disamina dell'art. 14, giova poi evidenziare come la violazione delle disposizioni in esso contenute abilita uno Stato Parte a sospendere – previo ragionevole preavviso – il trasferimento dei dati personali verso un altro Stato Parte. Una siffatta previsione, contemplata dal par. 15 dell'art. 14, dimostra come anche gli interessi sottesi alle nuove misure di cooperazione internazionale digitale possono concretamente recedere, nella prospettiva del Consiglio d'Europa e degli Stati firmatari del Secondo Protocollo, a fronte di attività di indagine che non rispettino le norme in materia di *data protection*.

4. La firma e la ratifica del Secondo Protocollo da parte dei Paesi membri dell'Unione europea

Per completare l'analisi sin qui condotta, occorre sinteticamente soffermarsi anche sulle indicazioni fornite dall'Unione agli Stati membri, anche in tema di riserve, dichiarazioni, notifiche e comunicazioni[62], con le decisioni del 5 aprile 2022[63], e del 14 febbraio 2023[64], recanti le autorizzazioni, rispettivamente, alla sottoscrizione e alla ratifica del Secondo Protocollo.

Per quanto qui interessa rispetto alla normativa UE in materia di *data protection*, il Consiglio dell'Unione ha in primo luogo invitato i Paesi membri ad astenersi dall'apporre

[60] La portata del principio della trasparenza è ben espresso, anche in relazione al tema della semplificazione espressiva, dal considerando 39 del GDPR, secondo cui "Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati. Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano".

[61] Per un approfondimento sui rimedi giudiziali a fronte di un trattamento illegittimo dei dati personali, anche alla luce dei principi fondamentali UE, si veda S. PEERS, T. HERVEY, J. KENNER, *The EU Charter of Fundamental Rights. A Commentary*, 2022, pp. 296 ss.

[62] Per un approfondimento sul Secondo Protocollo nel contesto di quanto previsto, in generale, dal diritto internazionale dei trattati in materia di riserve, dichiarazioni, notifiche e comunicazioni, ci permettiamo di rinviare a M. BUCCARELLA, *Il Secondo Protocollo addizionale alla Convenzione di Budapest alla luce del diritto internazionale dei trattati*, in *Diritto Penale e Processo*, 2022, n. 9, pp. 1160 ss.

[63] Decisione del Consiglio (UE) 2022/722, cit., e il relativo Allegato.

[64] Decisione del Consiglio (UE) 2023/436, cit., e il relativo Allegato.

riserve a carattere "generale" con riferimento all'applicazione degli artt. 7 e 8 del Secondo Protocollo, rispettivamente disciplinanti l'ordine di esibizione delle informazioni e dei dati relativi agli abbonati (da parte dei fornitori di servizi) e la procedura accelerata per la divulgazione dei dati sul traffico[65]. Alla luce di siffatto invito, l'UE ha poi accordato ai Paesi membri il permesso di apporre una riserva parziale in relazione al già richiamato art. 7, consentendo quindi di negare la trasmissione di tutte quelle informazioni sugli accessi degli abbonati che non si rivelino strettamente necessarie a identificare l'utente[66].

Per quanto concerne eventuali dichiarazioni, il Consiglio ha previsto che ogni Paese membro comunichi al Segretario Generale del Consiglio d'Europa le autorità cui dovranno essere notificati gli incidenti di sicurezza e quelle competenti a ricevere ordini di esibizione di dati *ex* art. 7 del Secondo Protocollo, finanche indirizzati a fornitori di servizi ovvero a soggetti privati[67].

In merito al delicato tema del trasferimento transfrontaliero dei dati personali, l'UE ha invitato gli Stati membri a fornire puntuali indicazioni ai Paesi terzi sulla necessità di informare l'interessato in ordine al trattamento dei suoi dati personali, conformemente a quanto previsto dal diritto dell'Unione[68].

Dal momento che il Secondo Protocollo consente poi agli Stati di attuare un accordo bilaterale in luogo delle garanzie in materia di protezione dei dati personali[69], l'Unione ha precisato che tale possibilità resta subordinata all'adozione di una decisione di adeguatezza da parte della Commissione europea[70].

Da ultimo il Consiglio, con le decisioni che autorizzano alla firma e alla ratifica, ha poi fornito agli Stati indicazioni sulle comunicazioni che dovranno rendere in merito ai trasferimenti transfrontalieri dei dati personali verso gli Stati Uniti[71]. In proposito l'UE

---

[65] In merito al contenuto dell'art. 7 si veda l'approfondimento di C. PIROZZOLI, *Acquisizione dei subscriber data: dalla Convezione di Budapest al Protocollo addizionale (art. 7)*, in *Diritto Penale e Processo*, n. 8, 2022, pp. 1050 ss. Con riferimento all'art. 8, si veda invece W. NOCERINO, *La cooperazione internazionale rinforzata per lo scambio di dati degli abbonati e di traffico (art. 8)*, in *Diritto Penale e Processo*, n. 8, 2022, pp. 1050 ss.

[66] Par. 1 dell'Allegato alla Decisione del Consiglio (UE) 2022/722, cit., e dell'Allegato alla Decisione del Consiglio (UE) 2023/436, cit.

[67] Par. 3 dell'Allegato alla Decisione del Consiglio (UE) 2022/722, cit., e dell'Allegato alla Decisione del Consiglio (UE) 2023/436, cit.

[68] Par. 4 dell'Allegato alla Decisione del Consiglio (UE) 2022/722, cit. e dell'Allegato alla Decisione del Consiglio (UE) 2023/436, cit.

[69] L'art. 14, co. 1, lett. c), del Secondo Protocollo stabilisce che "Se la Parte trasmittente e la Parte ricevente non sono vincolate reciprocamente da un accordo di cui al paragrafo l, lettera b), esse possono stabilire di comune accordo che il trasferimento di dati personali a norma del presente protocollo può avvenire sulla base di altri accordi o intese tra le Parti interessate in luogo dei paragrafi da 2 a 15".

[70] Ultimo capoverso del par. 4 dell'Allegato alla Decisione del Consiglio (UE) 2022/722 e dell'Allegato alla Decisione del Consiglio (UE) 2023/436, cit. Per un approfondimento sulla decisione di adeguatezza, cfr. R.T. NIMMER, H.K. TOWLE, *Data Privacy, Protection, and Security Law*, 2021; V. BRECEVICH, *I trasferimenti di dati fuori dallo Spazio Economico Europeo*, in M. MARTONANA (a cura di), *La privacy al passo con il regolamento UE 2016/*679, 2021, pp. 95 ss.

[71] Per un inquadramento sul tema del trasferimento transfrontaliero dai dati personali con riferimento ai rapporti tra Unione europea e USA, si vedano F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona. (Dal Safe Harbour al Privacy Shield)*, in *Rivista di diritto internazionale*, 2016, n. 3, pp. 721 ss.; A. MANTELERO, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe Horbour e Privacy Shield*, in G. RESTA, V. ZENO

ha, da un lato, riconosciuto l'applicabilità ai rapporti tra le autorità procedenti dell'*Umbrella Agreement*[72] in luogo dell'art. 14 del Secondo Protocollo e, dall'altro, ha evidenziato la non applicabilità dello stesso con riferimento ai rapporti con fornitori privati di servizi. Per questi ultimi, infatti, troveranno attuazione le norme del Secondo Protocollo, salvo che non intervenga un accordo integrativo *ad hoc* dell'*Umbrella Agreement*, volto a disciplinare le relazioni con i privati[73].

Giova precisare che Irlanda e Danimarca sono gli unici Paesi membri nei confronti dei quali le indicazioni fornite dall'Unione, in materia di ratifica del Secondo Protocollo, non producono effetti[74]. Tali Stati, ad oggi, non hanno peraltro nemmeno sottoscritto il nuovo accordo aggiuntivo alla Convenzione di Budapest.

5. Potenziali profili di incompatibilità con la normativa UE in materia di trattamento dei dati personali

La riscontrata correlazione tra le norme del nuovo Protocollo e il quadro regolamentare dell'Unione in materia di protezione dei dati personali dimostra, per alcuni versi, un certo grado di *privacy compliance* del nuovo accordo aggiuntivo alla Convenzione di Budapest. In questa prospettiva, il Secondo Protocollo è stato anche definito come uno strumento giuridico che, oltre a promuovere il noto principio della *double criminality*[75], avrebbe posto l'accento sull'importanza della *double privacy* nelle indagini digitali[76].

Tuttavia, se, da una parte, va accolto in maniera positiva l'ennesimo riconoscimento in ambito internazionale dell'importanza del modello UE in materia, dall'altra la versione definitiva del secondo Protocollo, in cui non sono stati recepiti tutti i suggerimenti dell'EDPS[77], porta con sé potenziali rischi per il diritto alla protezione dei dati personali e quindi per le libertà degli interessati. Oltre alla discutibile eccezione all'obbligo di comunicare eventuali incidenti di sicurezza di cui si è detto innanzi, sussistono perplessità in ordine a determinati profili che si affronteranno di seguito.

ZENCOVICH (a cura di), *La protezione transnazionale dei dati, dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma, 2016, pp. 265 ss.; V. BRECEVICH, *op cit.*, pp. 107-112.

[72] Si tratta dell'Accordo quadro sulla protezione delle informazioni personali a fini di prevenzione, indagine, accertamento e perseguimento di reati del 2 giugno 2016 stipulato tra UE e USA, doc. 22016A1210(01), consultabile sul sito ufficiale dell'Unione europea al link https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:22016A1210(01).

[73] Capoversi terzultimo e penultimo del par. 4 dell'Allegato alla Decisione del Consiglio (UE) 2022/722, cit., e dell'Allegato alla Decisione del Consiglio (UE) 2023/436, cit.

[74] Considerando nn. 17 e 18 della Decisione del Consiglio (UE) 2023/436.

[75] Per un approfondimento sul concetto di *double criminality* nella cooperazione internazionale in materia penale e anche in relazione al quadro normativo dell'Unione, si veda W. DE BONDT, *Double criminality in international cooperation in criminal matters*, in G. VERMEULEN, W. DE BONDT, C. RYCKMAN (eds.), *Rethinking International Cooperation in Criminal Matters in the EU: Moving beyond Actors, Bringing Logic Back, Footed in Reality*, Maklu, 2012, pp. 10 ss.

[76] P. PERRI, *Le condizioni di salvaguardia e la protezione dei dati personali*, in *Diritto Penale e Processo*, 2022, n. 9, p. 1158.

[77] Cfr. *Opinion* dell'EPDS n. 3/2019 del 2 aprile 2019.

In primo luogo, una delle criticità riguarda gli effetti derivanti dalle richieste e/o dagli ordini di Paesi terzi rivolti direttamente ai fornitori di servizi operanti nell'Unione, ai sensi degli artt. 6 e 7 del Secondo Protocollo[78]. Sebbene l'Unione abbia invitato gli Stati membri a richiedere la notifica di simili atti anche agli enti di controllo in materia[79], la circostanza che tale notifica non sia idonea, *di per sé*, a sospendere l'efficacia della richiesta e/o dell'ordine potrebbe avere ripercussioni sulle libertà e sui diritti degli interessati. In altri termini, nell'attesa che un'Autorità competente si pronunci, comunque la richiesta e/o l'ordine resterebbero efficaci, il che significa che in tale lasso temporale ogni valutazione e responsabilità in materia di trattamento dei dati sarà di fatto demandata ai prestatori di servizio privati. Si tratta di un aspetto non irrilevante, se consideriamo che i dati degli abbonati e dei traffici in questione, in quanto specificamente riguardanti persone sottoposte ad indagini o procedimenti penali, contengono informazioni tali da incidere seriamente sui diritti fondamentali e sulle altre garanzie previste dal diritto processuale penale degli Stati membri[80]. Sempre sotto il profilo di potenziali ripercussioni sui diritti degli interessati, giova evidenziare che il secondo Protocollo rimette alla normativa degli ordinamenti nazionali la regolamentazione delle ipotesi di limitazione di tali diritti[81]. Si tratta di un aspetto su cui si è soffermato in modo evidentemente critico anche l'EDPS con il parere n. 1/2022, evidenziando il rischio di pratiche arbitrarie da parte degli Stati[82].

Un'altra questione che desta perplessità attiene alle richieste di informazioni sulla registrazione dei nomi di dominio *ex* art. 6 del Secondo Protocollo, specificamente rivolte ai fornitori privati di servizi informatici. Infatti, differentemente da quanto generalmente previsto per gli artt. 7 e 8, con riferimento a siffatte richieste non è stata contemplata la possibilità, per gli Stati sottoscrittori, di rendere dichiarazioni, eventualmente volte a coinvolgere autorità pubbliche nazionali nei correlati processi di valutazione[83].

Una delle maggiori criticità attiene poi alla compatibilità delle norme previste dal Secondo Protocollo, in materia di trasferimenti transfrontalieri, con quanto affermato in

[78] Sul contenuto e la portata dell'art. 6, si veda M. LUCCHETTI, *L'acquisizione di informazioni sulla registrazione di nomi di dominio nelle investigazioni in materia di cybercrime*, in *Diritto Penale e Processo*, 2022, n. 8, pp. 1041 ss. Con riferimento all'art. 7 si rinvia a C. PIROZZOLI, *op. cit.*

[79] A dette autorità spetta, in sostanza, il compito di verificare l'incidenza della richiesta sui dati personali degli interessati ed eventualmente opporre un rifiuto.

[80] Si pensi, ad esempio, ai privilegi, alle immunità e alle tutele speciali concesse a determinate persone come avvocati, giornalisti e informatori.

[81] Per un inquadramento generale sulla limitazione dei diritti degli interessati nell'ambito delle attività di indagine e alla luce della normativa dell'Unione europea, si veda M. MARTORANA, *Il trattamento dei dati personali nell'attività investigativa*, pp. 59 ss. Occorre precisare che nell'ambito dei diritti degli interessati rientra il diritto di accesso ai propri dati personali e il corrispondente diritto di disporre di mezzi giurisdizionali per contrastare una decisione di diniego di accesso. Con riferimento a quest'ultimo diritto, la Corte di Giustizia UE ha espressamente riconosciuto l'illegittimità, per contrarietà a diritti fondamentali, di qualsivoglia normativa che non disciplini la possibilità per le persone fisiche di adire le vie legali al fine di avere accesso ai propri dati personali. Cfr. Corte di Giustizia, Grande Sezione, sentenza del 6 ottobre 2015, *Maximillian Schrems contro Data Protection Commissioner*, C-362/14, par. 95.

[82] EDPS, *opinion* n. 1/2022, cit., par. 107.

[83] Per un approfondimento sulle disposizioni del Secondo Protocollo in materia di riserve e dichiarazioni, sia consentito il rinvio a M. BUCCARELLA, *op. cit.*, pp. 1163-1165.

passato dalla Corte di Giustizia UE[84]. Alla luce di quanto si è osservato nel paragrafo precedente, il nuovo accordo addizionale alla Convenzione di Budapest costituisce, in sostanza, la base giuridica per il trattamento dei dati anche rispetto ai rapporti con Stati terzi. Infatti, ferma restando la possibilità di concludere un accordo bilaterale in materia con l'UE[85], nel caso dei trasferimenti transfrontalieri di dati effettuati sulla base del Secondo Protocollo troveranno applicazione le disposizioni di cui all'art. 14. Tuttavia, per quanto tali previsioni e la Relazione Esplicativa del Secondo Protocollo[86] possano essere ritenute in linea di principio compatibili con la normativa UE, sussiste comunque un certo grado di vaghezza che potrebbe essere ritenuto inidoneo alla luce degli insegnamenti della Corte di Giustizia dell'Unione. È qui sufficiente richiamare il parere 1/15, ove la Corte, con riferimento all'accordo tra Canada e UE sul trasferimento e sul trattamento dei dati del codice di prenotazione[87] e alla possibilità per "il Canada di trattare i dati PNR" di cittadini dell'Unione, aveva ritenuto che la formulazione delle norme fosse "troppo vaga e generica per soddisfare i requisiti di chiarezza e di precisione imposti"[88].

La domanda sorge dunque spontanea: le previsioni del secondo Protocollo sono sufficienti a fondare giuridicamente, *a priori* e in ogni caso, il trattamento transfrontaliero di dati con qualsiasi Paese terzo? Ciò vale anche con riferimento a Stati non membri del Consiglio d'Europa[89], eventualmente non parti della Convenzione 108 e presumibilmente non dotati di una idonea normativa in materia di protezione dei dati personali? Ai posteri – e forse ai giudici UE e degli Stati membri – l'ardua sentenza.

Ancora, rispetto al tema del trasferimento transfrontaliero dei dati personali, sussistono alcune perplessità circa l'accordo che l'Unione ha ritenuto applicabile *ex* art. 14, par. 1, lett. c), del Secondo Protocollo, cioè l'*Umbrella Agreement*. Come si è già avuto modo di osservare in precedenza, tale accordo troverà applicazione in luogo delle norme del Secondo protocollo in materia di protezione dati personali. Tuttavia, stando a quanto pure affermato dall'EDPS nel già menzionato parere n. 1/2022[90], si tratta di un accordo che non può essere applicato *sic et simpliciter*, sia perché non costituisce una

[84] Cfr., in particolare, il parere della Corte di Giustizia, Grande Sezione, 1/2015 del 26 luglio 2017, relativo al "Progetto di accordo tra il Canada e l'Unione europea – Trasferimento dei dati del codice di prenotazione dei passeggeri aerei dall'Unione al Canada"; Corte di Giustizia, Grande Sezione, sentenza del 6 ottobre 2015, *Maximillian Schrems contro Data Protection Commissioner*, C-362/14; Corte di Giustizia, Grande Sezione, sentenza del 16 luglio 2020, *Data Protection Commissioner contro Facebook Ireland Limited e Maximillian Schrems*, C-311/18. Per un approfondimento sul contenuto di tali pronunce, le c.d. sentenze *Schrems I* e *Schrems II*, si veda C. GENTILE, *La saga Schrems e la tutela dei diritti fondamentali*, in *Federalismi.it*, 2021, n. 1, pp. 35 ss.

[85] Previa decisione di adeguatezza, come si evince dall'ultimo capoverso del par. 3 dell'Allegato alla Decisione del Consiglio (UE) 2022/722, cit.

[86] Relazione esplicativa del *Cybercrime Convention Committee* del Consiglio d'Europa del 17 novembre 2021, CM(2021)57-addfinal.

[87] Proposta di accordo tra Canada e UE sul trasferimento e sul trattamento dei dati del codice di prenotazione (*Passenger Name Record* – PNR), presentata il 30 gennaio 2015 alla Corte di Giustizia UE dal Parlamento europeo *ex* art. 218, par. 11, TFUE.

[88] Par. 181 del parere della Corte di Giustizia UE, Grande Sezione, 1/2015, cit.

[89] Il nuovo accordo aggiuntivo alla Convenzione di Budapest può infatti essere sottoscritto anche da Paesi non membri del Consiglio d'Europa. Cfr. l'art. 2 del Secondo Protocollo.

[90] EDPS, *opinion* n. 1/2022, cit., par. 121.

base giuridica per il trasferimento dei dati[91], sia in considerazione di tutte le obiezioni già sollevate da EDPS ed EDPB in merito ad una normativa interna statunitense che incide negativamente sul contenuto dell'*Umbrella Agreement*, cioè il *CLOUD Act*[92]. Per effetto di tale atto, approvato nel 2018, le Autorità giudiziarie ed amministrative degli Stati Uniti hanno il potere di obbligare i fornitori di servizi *cloud* soggetti alla giurisdizione statunitense a produrre dati ed informazioni contenuti in documenti elettronici, finanche conservati in Paesi terzi – tra cui la stessa Unione europea[93]. Già in occasione dell'approvazione del *CLOUD Act* da parte del Congresso, EDPS e EDPB avevano evidenziato l'incompatibilità di tale normativa con il quadro giuridico dell'Unione in materia di *data protection*, auspicando la stipula di un accordo che offrisse idonee garanzie agli interessati, nello specifico ambito dei trasferimenti transfrontalieri di dati e prove digitali per fini investigativi e giudiziari[94]. Sebbene nel 2019 USA e UE si siano impegnati a negoziare siffatto tipo di accordo[95], ad oggi non si è ancora pervenuti ad una proposta risolutiva che riscontrasse l'invito rivolto dalle due Autorità Garanti dell'Unione. Ciononostante il Consiglio dell'Unione, nelle decisioni che autorizzano la firma e la ratifica del Secondo Protocollo, ha ritenuto di riconoscere l'applicabilità dell'*Umbrella Agreement* nei rapporti USA-UE, in luogo delle garanzie fornite dal nuovo accordo aggiuntivo alla Convenzione di Budapest. L'espresso riferimento a tale accordo, cui il *CLOUD Act* è strettamente correlato, postula tuttavia non pochi dubbi in ordine alla compatibilità del Secondo Protocollo con il quadro giuridico UE in materia di dati personali.

6. Il Secondo Protocollo tra luci, ombre e proposte risolutive

All'esito di questa disamina è possibile svolgere alcune riflessioni in ordine all'impatto del Secondo Protocollo nel quadro giuridico internazionale e alla sua compatibilità con la disciplina dell'Unione europea in materia di trattamento dei dati personali.

È indubbio che il Secondo Protocollo costituisce uno strumento giuridico utile, se non addirittura necessario, per adeguare, *rectius* rafforzare, la disciplina sulla cooperazione internazionale in materia penale, nell'ottica di agevolare le indagini digitali

[91] Come precisato proprio dall'art. 1, co. 3, dell'*Umbrella Agreement* del 2 giugno 2016, cit.
[92] *Clarifying Lawful Overseas Use of Data (CLOUD) Act Clarifying Lawful Overseas Use of Data*, adottato dal Congresso USA il 21 marzo 2018 in parziale modifica dello *Stored Communications Act del 1986*. Il testo integrale di tale atto è consultabile sul sito istituzionale del Governo USA al link https://www.justice.gov/dag/page/file/1152896/download.
[93] Per un approfondimento sul contenuto dell'US Cloud Act nella prospettiva del diritto dell'Unione, si veda M. ROJSZCZAK, *CLOUD act agreements from an EU perspective*, in *Computer Law & Security Review*, vol. 38, 2020, pp. 1 ss.
[94] EDPB-EDPS, *Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection* del 12 luglio 2019.
[95] Cfr. *Joint US-EU Statement on Electronic Evidence Sharing Negotiations* del 26 settembre 2019, consultabile sul sito istituzionale del Governo USA al link https://www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing-negotiations.

a carattere transfrontaliero e il perseguimento di crimini informatici. Il *favor* con cui è stato generalmente accolto il secondo Protocollo ha peraltro avuto un impatto positivo sui negoziati in corso dal 2018 in seno all'Unione europea, per il raggiungimento di nuove intese volte ad agevolare l'accesso delle autorità alle prove elettroniche, indipendentemente dalla loro ubicazione e dei dati ivi contenuti. Infatti, con il comunicato stampa del 25 gennaio 2023[96], il Consiglio ha dichiarato di aver finalmente raggiunto, dopo cinque anni di trattative, un accordo con il Parlamento europeo sui progetti di regolamento[97] e direttiva in materia di accesso transfrontaliero alle prove digitali[98]. Il nuovo accordo aggiuntivo alla Convenzione di Budapest potrebbe inoltre avere un impatto positivo anche su altri negoziati di cui si sta discutendo negli ultimi mesi, che vedono l'Unione europea impegnata, sul piano internazionale, nell'elaborazione di un accordo transatlantico in materia di dati personali[99] e del trattato ONU sul *cybercrime*. L'auspicio è che l'Unione, alla luce dei rilievi espressi dall'EPDB sia sull'applicabilità

[96] Pubblicato sul sito del Consiglio UE e liberamente consultabile al seguente link: https://www.consilium.europa.eu/it/press/press-releases/2023/01/25/electronic-evidence.

[97] Consiglio UE, *Analysis of the compromise text – Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings*, 5448/2023, 20 gennaio 2023. Il testo oggetto del compromesso finale è liberamente consultabile, sul sito del Consiglio UE, al seguente link: https://data.consilium.europa.eu/doc/document/ST-5448-2023-INIT/en/pdf.

[98] Consiglio UE, *Analysis of the compromise text – Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings*, 5449/23, 20 gennaio 2023. Il testo oggetto del compromesso finale è liberamente consultabile, sul sito del Consiglio UE, al seguente link: https://data.consilium.europa.eu/doc/document/ST-5449-2023-INIT/en/pdf.

[99] Il 25 marzo 2022 la Presidente von der Leyen e il Presidente Biden hanno annunciato l'adozione di un futuro accordo volto a disciplinare il *Data Privacy Framework*, i cui i principi fondanti, dichiaratamente ispirati dalla sentenza *Schrems II*, sono stati sintetizzati nel comunicato stampa dell'UE "European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework" del 25 marzo 2022. A seguito di tale decisione, il 7 ottobre 2022 il Presidente Biden ha firmato un ordine esecutivo intitolato "Enhancing Safeguards for United States Signals Intelligence Activities", su cui la Commissione ha reso la propria decisione di adeguatezza il 10 luglio 2023, dopo aver acquisito il parere consultivo dell'EDPB e il parere positivo di un Comitato rappresentativo degli Stati membri. Il testo della decisione «on the adequate level of protection of personal data under the EU-US Data Privacy Framework», C(2023) 4745 *final*, è consultabile sul sito istituzionale della Commissione UE, al seguente link: https://commission.europa.eu/system/files/2023-07/Adequacy%20decision%20EU-US%.pdf. Giova precisare che il contenuto della bozza della decisione non era stato tuttavia interamente condiviso dall'EDPB, che aveva evidenziato una serie di criticità nell'ambito del parere consultivo n. 5, adottato il 28 febbraio 2023. Anche il Parlamento UE, con risoluzione dell'11 maggio 2023, 2023/2501(RSP) adottata con 306 voti favorevoli, 27 contrari e 231 astensioni, aveva sollevato perplessità in merito alla bozza proposta dalla Commissione, evidenziando come "Data Privacy Framework principles issued by the US Department of Commerce have not been sufficiently amended, in comparison to those under the Privacy Shield, to provide essentially equivalent protection to that provided under the GDPR". Il testo della risoluzione del Parlamento UE è liberamente consultabile, sul sito istituzionale, al link: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0204_EN.html. La Commissione, a pp. 62-63 della decisione di adeguatezza del 10 luglio 2023, ha richiamato sia la risoluzione del Parlamento Europeo, sia il parere dell'EDPB, «which has been taken into consideration in the preparation of this Decision».

dell'*Umbrella Agreement* sia sul nuovo accordo con gli USA[100], insista per avere maggiori garanzie anche in merito all'attuazione delle misure di "cooperazione rinforzata" previste dal Secondo Protocollo, segnatamente sotto il profilo dei trasferimenti transfrontalieri dei dati personali. Ad alimentare tuttavia i dubbi sulla compatibilità della normativa statunitense rispetto agli standard dell'Unione si aggiunge, in una prospettiva futura, la diversa sensibilità USA al tema privacy, come confermato dalle dichiarazioni formalizzate nel corso dei negoziati ONU per l'approvazione del trattato sul *cybercrime*. In tale sede, la delegazione statunitense ha ribadito la propria contrarietà all'introduzione di specifiche disposizioni in materia di *data protection*, evidenziando l'assenza di "universal set of practices or agreement" cui potersi ispirare nella regolamentazione del trattamento dei dati personali in ambito internazionale[101]. A prescindere dalla fondatezza o meno, sul piano giuridico, di una simile affermazione, le dichiarazioni rese dagli USA offrono un'ulteriore conferma della distanza che separa Washington da Bruxelles sul tema del trasferimento transfrontaliero dei dati personali. Infatti, al disinteresse degli Stati Uniti si contrappone il rigido quadro regolatorio UE, che subordina eventuali trasferimenti transfrontalieri di dati personali all'osservanza degli elevati standard di tutela previsti nell'Unione.

D'altro canto, le perplessità di cui si è detto innanzi postulano interrogativi rilevanti rispetto alla conformità del secondo Protocollo con la normativa UE, tali da poter incidere sul diritto fondamentale alla protezione dei dati personali. Lo stesso EDPS, pur riconoscendo che "is not possible to replicate entirely the terminology and definitions of EU law in a multilateral international agreement", ha sottolineato che "appropriate safeguards for individuals must be ensured in order to fully comply with EU law"[102]. Si tratta di un monito evidentemente volto a richiamare l'attenzione sulla necessità di implementare, in ogni caso, le garanzie a presidio del fondamentale diritto alla protezione dei dati personali.

A fronte di possibili rischi derivanti dai trattamenti di dati personali da parte dei Paesi terzi, i tribunali nazionali e i giudici della Corte di Giustizia dell'Unione europea[103] si confermano oggi il principale baluardo a tutela dei diritti dei cittadini UE. Del resto, i presidi giurisdizionali garantiscono strumenti utili a mitigare i potenziali pregiudizi connessi a qualsiasi trattamento illecito dei dati personali. In un'ottica proattiva, volta ad evitare successive condanne del Secondo Protocollo da parte dei tribunali nazionali o finanche dalla stessa Corte di Giustizia UE, il Parlamento o un altro dei soggetti di cui

[100] EPDB, *Opinion 5/2023 on the European Commission Draft Implementing Decision on the adequate protection of personal data under the EU-US Data Privacy Framework*, 28 febbraio 2023.
[101] Cfr. il punto n. 7 della dichiarazione resa dalla delegazione USA nel corso della terza sessione dei negoziati. Cfr. *U.S. statement in response to Chair's Leading Questions*, liberamente consultabile sul sito ONU al seguente link: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/USA.pdf.
[102] *Executive Summary* dell'*opinion* n. 1/2022 dell'EDPS, cit., p. 1.
[103] Per un approfondimento sul ruolo e sulla giurisprudenza della Corte di Giustizia nella tutela dei dati personali, si veda F. ROSSI DAL POZZO, *La tutela dei dati personali nella giurisprudenza della Corte di Giustizia*, cit.

all'art. 218, par. 11, TFUE[104] potrebbero poi interpellare in via preventiva i giudici di Lussemburgo circa la compatibilità del Secondo Protocollo con il diritto alla protezione dei dati personali, come tutelato nell'Unione da norme di rango primario. Una valutazione *ex ante* da parte della Corte UE consentirebbe di sciogliere ogni dubbio sull'impatto delle nuove misure di cooperazione "rafforzata" – in parte riferite anche a soggetti privati – sul diritto alla protezione dei dati personali. Ciò consentirebbe di escludere in radice eventuali *coup de théâtre* nella fase di attuazione del nuovo accordo. Già il *Safe Harbor* e il *Privacy Shield*[105] sono stati inficiati da una "bocciatura giurisdizionale" *ex post*; d'altronde, anche il *Data Privacy Framework*, benché convalidato dalla Commissione UE con la decisione di adeguatezza del 10 luglio 2023[106], potrebbe subire la medesima sorte, stanti le preoccupazioni espresse dall'EPDB e dal Parlamento europeo[107]. È tuttavia vero che una simile richiesta di parere *ex ante* pone un problema di ricevibilità della richiesta, atteso che l'Unione europea ha già autorizzato i Paesi membri alla firma e alla ratifica del Secondo Protocollo, sebbene ad oggi risulta che nessuno Stato lo abbia ancora ratificato. Persino sul piano internazionale, nonostante le trentasei sottoscrizioni sino ad ora formalizzate, soltanto la Siria ha provveduto alla ratifica del nuovo accordo aggiuntivo alla Convenzione di Budapest. In questo quadro, poiché il trattato non è ancora entrato in vigore e nessuno dei Paesi firmatari – ad eccezione della Siria – ha ad oggi provveduto a ratificarlo, potrebbe comunque valere la pena correre il rischio di una dichiarazione di irricevibilità da parte della Corte di Giustizia dell'Unione europea. La rigidità del quadro regolatorio UE e le vicende che, nella prospettiva dei trasferimenti transfrontalieri dei dati personali, hanno direttamente interessato l'Unione suggeriscono infatti cautela nel rapporto con tutti quei Paesi terzi che, per tradizione giuridica, sono meno sensibili alla tutela della privacy e della protezione dei dati personali. *Rebus sic stantibus*, anche "tentare" di prevenire sarebbe meglio che curare.

[104] Ai sensi dell'art. 218, par. 11, TFUE un eventuale parere negativo della Corte implica che "l'accordo previsto non può entrare in vigore, salvo modifiche dello stesso o revisione dei trattati".
[105] Lo "Scudo USA-UE per la Privacy" è l'accordo che Stati Uniti e Unione europea hanno sottoscritto per introdurre un meccanismo di autocertificazione finalizzato al trasferimento dei dati tra i due Paesi. In merito a tale accordo, l'Unione si era espressa positivamente con Decisione di esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016, relativa all'"adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy". La Corte di Giustizia UE, con la già richiamata sentenza *Schrems II* del 16 luglio 2020, ha tuttavia invalidato la decisione di adeguatezza relativa al *Privacy Shield*. Stessa sorte che ha interessato anche il precedente accordo USA-UE *Safe Harbor*, dichiarato invalido con la sentenza *Schrems I* della Corte di Giustizia UE del 6 ottobre 2015. Per un approfondimento in materia, anche in una prospettiva di comparazione USA e UE, cfr. A.S. OBENDIEK, *Data Governance: Value Orders and Jurisdictional Conflicts*, Oxford, 2022, pp. 77-103.
[106] Decisione del 10 luglio 2023, C(2023) 4745 *final*, cit.
[107] EPDB, *Opinion 5/2023 on the European Commission*, 28 febbraio 2023, cit.; Parlamento europeo, *Resolution of 11 May 2023 on the adequacy of the protection afforded by the EU US Data Privacy Framework*, 2023/2501(RSP), punti 19 e 20.

ABSTRACT: Il 12 maggio 2022 è stato aperto alla firma degli Stati il Secondo Protocollo addizionale alla Convenzione di Budapest del 2001. Si tratta di uno strumento pattizio che mira a favorire la cooperazione tra Paesi nell'ambito delle indagini digitali transfrontaliere, nell'ottica di unire il fronte internazionale contro i reati informatici. In un rinnovato quadro giuridico di cooperazione che coinvolge anche gli Stati membri dell'Unione europea, le norme UE in materia di *data protection* si pongono come contraltare alle attività di raccolta delle prove digitali, che postulano il trattamento di dati personali da parte non soltanto delle autorità degli Stati bensì di una pluralità di soggetti, anche di natura privata. Il presente lavoro mira ad approfondire il rapporto tra le previsioni del Secondo Protocollo e la disciplina UE in materia di protezione dei dati personali, onde verificare la sussistenza di eventuali profili di incompatibilità che potrebbero incidere, in concreto, sull'utilizzabilità degli strumenti previsti dal nuovo accordo aggiuntivo alla Convenzione di Budapest.

KEYWORDS: protezione dei dati personali – Convenzione di Budapest – cooperazione giudiziaria internazionale – criminalità informatica – prove digitali.

THE DIGITALISATION OF CROSS-BORDER JUDICIAL COOPERATION IN CRIMINAL MATTERS: WHAT IS THE IMPACT ON EU DATA PROTECTION LEGAL FRAMEWORK?

ABSTRACT: On 12 May 2022, the Second Additional Protocol to the Budapest Convention was opened for signature by States. It is a treaty agreement which aims to enhance cooperation between countries in the field of cross-border digital investigations, with a view to uniting the international front against cybercrimes. In a renewed legal framework of cooperation that also involves the European Union, the EU data protection rules act as a limit to the activities of collecting digital evidences, which involve the processing of personal data not only by the public authorities but also by private legal entities. This paper aims to deepen the relationship between the provisions of the Second Protocol and the EU legal framework for data protection, in order to verify the existence of any incompatibility profiles that could concretely affect the use of Second Additional Protocol tools.

KEYWORDS: data protection – Budapest Convention – cross-border judicial cooperation – cybercrime – electronic evidences.