I *Post* di AISDUE, V (2023), *aisdue.eu*
Sezione "Atti convegni AISDUE", n. 8, 28 gennaio 2023
Quaderni AISDUE

Il Secondo Protocollo addizionale alla Convenzione di Budapest e le nuove frontiere della cooperazione internazionale in ambito digitale. Quali rischi per la protezione dei dati personali nell'Unione europea?

Marco Buccarella[*]

SOMMARIO: 1. Introduzione. – 2. Cenni sulla Convenzione di Budapest sul *cybercrime*. – 3. Le condizioni di salvaguardia e la protezione dei dati personali nel Secondo Protocollo. – 4. Le indicazioni fornite dall'UE in sede di autorizzazione alla firma da parte dei Paesi membri. – 5. Dubbi sulla *data privacy (non)compliance*: quali rischi per il diritto fondamentale alla protezione dei dati personali? – 6. Riflessioni conclusive.

1. Il quadro normativo cui ricondurre il tema della cooperazione giudiziaria internazionale in materia penale è stato di recente interessato da un nuovo strumento pattizio approvato dal Consiglio d'Europa, ovvero il Secondo Protocollo addizionale alla Convenzione di Budapest

[*] Dottorando di ricerca in Scienze Giuridiche presso l'Università di Foggia – Dipartimento di Giurisprudenza.

sulla criminalità informatica (d'ora in avanti il "Secondo Protocollo")[1]. Tale trattato, aperto alla firma degli Stati il 12 maggio 2022, contempla disposizioni volte a rafforzare la cooperazione internazionale (e non solo) nel contrasto alla criminalità informatica e, in particolare, nell'ambito delle attività di ricerca, reperimento e divulgazione delle c.d. prove digitali o elettroniche[2]. Giova fin da subito precisare che le materie oggetto del Secondo Protocollo, cioè la cooperazione giudiziaria in materia penale e la protezione dei dati personali, sono state oggetto di una pluralità di atti di diritto derivato UE[3] e trovano la loro base giuridica, rispettivamente, nell'art. 16 TFUE e nell'art. 82, par. 1, TFUE. Gli Stati membri sono perciò stati autorizzati a firmare il nuovo accordo addizionale alla Convenzione di Budapest nell'interesse dell'Unione[4], stante la riconducibilità del Secondo Protocollo all'art. 3, par. 2, TFUE e, quindi, all'ambito di competenza esclusiva dell'Unione a concludere accordi internazionali[5]. Del resto, l'autorizzazione in

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

[2] 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*, n. 8, 2022, pp. 1017-1060; n. 9, 2022, pp. 1137-1174. In merito alla relazione intercorrente, in generale, tra le misure previste dal Secondo Protocollo e la disciplina contenuta nel regolamento (UE) 2017/1939 del Consiglio, 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*, n. 9, 2022, p. 1168 ss.

[3] 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*, n. 8, 2022, p. 1022 ss.

[4] Sulla base degli artt. 16, 82, par. 1, e 218, par. 6, TFUE. Cfr. decisione (UE) 2022/722 del Consiglio, del 4 aprile 2022, recante l'autorizzazione agli 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.

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

favore dei Paesi membri si è resa necessaria giacché "l'Unione non può firmare il protocollo, in quanto solo gli Stati possono esserne parti"[6].

2. Prima di approfondire gli aspetti rilevanti del rapporto tra il Secondo Protocollo e la disciplina UE in materia dati personali, conviene soffermarsi brevemente sullo strumento giuridico cui accede l'accordo addizionale in commento, cioè la Convenzione del Consiglio d'Europa di Budapest del 2001[7]. Si tratta del primo strumento giuridico internazionale pattizio che, nell'introdurre nozioni di tipo tecnico in materia digitale[8], ha predisposto un sistema di cooperazione volto a contrastare gli illeciti commessi con e sulla rete, tendenzialmente caratterizzati da atemporalità e aterritorialità[9]. 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[10]. Le iniziali incertezze che hanno accompagnato l'*iter* di approvazione della Convenzione hanno lasciato posto alla sempre più diffusa consapevolezza, da parte degli Stati, dell'effettiva utilità di uno strumento giuridico di portata internazionale volto a delineare un quadro giuridico condiviso, indispensabile per l'attività di contrasto alla criminalità informatica. 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

[6] Considerando n. 13 della decisione (UE) 2022/722, cit.
[7] 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.
[8] Tra cui, ad esempio, le definizioni di *computer data* o *service provider*.
[9] Per un approfondimento sulle disposizioni contemplate dalla Convenzione di Budapest, si vedano J. CLOUGH, *A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonization*, in *Monash University Law Review*, vol. 40, n. 3, 2014; M. KEYSER, *The Council of Europe Convention on Cybercrime*, in *Journal of Transnational Law & Policy*, vol. 12, n. 2, 2003.
[10] 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 e la cooperazione internazionale.

Protocollo addizionale, relativo alla criminalizzazione di atti di natura razzista e xenofobica commessi a mezzo di sistemi informatici[11]. 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 intervenuto nuovamente in materia, approvando il Protocollo di cui qui si discute. Come si è detto, il fine del recente accordo aggiuntivo 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[12]. Lo stesso Consiglio d'Europa, in un comunicato ufficiale risalente alla fine del 2021, ha definito il Secondo Protocollo come uno strumento finalizzato a potenziare "its legal arsenal"[13], in materia di contrasto alla criminalità informatica.

Come dimostra la breve disamina condotta sin qui, l'accordo di recente sottoscritto si pone quindi nel solco tracciato dalla Convenzione di Budapest, fornendo la base giuridica per la cooperazione tra gli Stati nell'ambito delle indagini digitali e, in particolare, con riferimento alle attività di raccolta e utilizzo delle prove elettroniche. Nella prospettiva del Consiglio d'Europa, la proliferazione di crimini informatici può essere combattuta riducendo gli effetti negativi dovuti alla disconnessione tra la giurisdizione territoriale degli Stati e il modo in cui le informazioni si spostano e sono conservate nell'ambito dei 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 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

[11] 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.
[12] Cfr. D. CURTOTTI, *Speciale sul Secondo Protocollo addizionale alla Convenzione di Budapest. Premessa*, in *Diritto Penale e Processo*, n. 8, 2022, p. 1017 ss.
[13] Consiglio d'Europa, comunicato del 17 novembre 2021, Ref. DC 207 (2021).

servizi di telecomunicazione[14]. 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.

3. Dal momento che il Secondo Protocollo incentiva la cooperazione nell'ambiente digitale, uno dei temi che assume maggiore rilevanza è la protezione dei dati personali. Gli strumenti informatici, infatti, sono notoriamente contenitori di informazioni riguardanti la personalità dell'individuo e dei terzi che hanno rapporti con quest'ultimo[15]; ne consegue che un trattamento non corretto dei dati potrebbe tradursi in violazioni del diritto fondamentale alla riservatezza e, per altro verso, in lacune o errori investigativi[16]. In ambito UE il diritto alla protezione dei dati personali, quale corollario della privacy[17], rappresenta un diritto fondamentale[18], tutelato da norme di rango primario e peraltro oggetto di uniformazione[19] e di armonizzazione[20].

---

[14] Cfr. P. PERRI, *Le condizioni di salvaguardia e la protezione dei dati personali*, in *Diritto Penale e Processo*, n. 9, 2022, p. 1150 ss.
[15] In proposito, cfr. sentenza della Corte EDU del 4 dicembre 2015, ric. n. 47143/06, *Roman Zakharov v. Russia*.
[16] P. PERRI, *op. cit.*, p. 1152 ss.
[17] 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, p. 1130 ss.
[18] Cfr. G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, n. 1, 2018, p. 9 ss.; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, 2016.
[19] 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).
[20] 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.

Considerata la rilevanza attribuita dal legislatore dell'Unione al tema privacy[21], è opportuno interrogarsi in questa sede sul rapporto che intercorre tra il quadro giuridico UE in materia di protezione dei dati personali e le nuove norme previste dal Secondo Protocollo. Nell'ambito di tale accordo, la "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 ripropone 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[22]. Si tratta di un principio espressamente riconosciuto dalla Carta dei diritti fondamentali dell'UE all'art. 52, par. 1, notoriamente adoperato dalla Corte di giustizia[23] e dalla Corte europea dei diritti dell'uomo[24] come metro di giudizio, per valutare la compatibilità di misure statali (di sorveglianza o di sicurezza) con le norme fondanti la disciplina in materia di *data protection*[25]. Il principio di proporzionalità, in quanto richiamato dall'art. 13, rappresenta dunque il parametro di riferimento per la disciplina contenuta nel successivo art. 14, che affronta nel dettaglio gli aspetti relativi alla protezione dei dati personali.

Da una prima lettura dell'art. 14 – che consta di ben quindici paragrafi – si può evincere una certa identità dei principi ivi espressi rispetto quelli contemplati dalla Convenzione 108+ del Consiglio

[21] 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, p. 3 ss.

[22] 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*, n. 15, 2017, p. 22 ss.

[23] Cfr. *ex multis* sentenza della Corte dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et al. and Kärntner Landesregierung et al*.

[24] Cfr. *ex multis* sentenza della Corte EDU del 12 gennaio 2016, ric. n. 37138/14, *Szabò e Vissy c. Ungheria*.

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

d'Europa[26], 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)[27]. Quest'ultimo paragrafo integra una previsione di notevole rilievo, specie per quei Paesi che – per tradizione normativa – sono, da un alto, meno "sensibili" al tema della protezione dei dati personali e, dall'altro, risultano più inclini all'utilizzo di applicazioni di giustizia predittiva e di *analytics* nell'ambito delle indagini[28]. Il principale elemento che dimostra l'influenza della normativa dell'Unione[29] sul nuovo accordo addizionale alla Convenzione di Budapest si rinviene nell'*accountability*, principio cardine del GDPR e simbolo dell'approccio seguito dal legislatore UE in materia[30].

[26] 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 (Convenzione n. 108) del 28 gennaio 1981; Consiglio d'Europa, Protocollo di emendamento alla Convenzione n. 108 del 10 ottobre 2018.

[27] Per un approfondimento sui principi contemplati dal GDPR, si vedano M. DELL'UTRI, *Principi generali e condizioni di liceità del trattamento dei dati personali*, 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, p. 94 ss.

[28] 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*, in *Review of Contemporary Philosophy*, vol. 21, 2022, p. 38 ss.

[29] In un'ottica più generale, la riconducibilità di alcune delle norme del Secondo Protocollo al GDPR confermerebbe la tesi per cui la regolamentazione UE in materia di tecnologia e *data protection* ha 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*, London, 2022. In proposito si veda inoltre, anche per ulteriori riferimenti bibliografici, G. M. RUOTOLO, *op. cit.*, pp. 1022 e 1023.

[30] G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati personali*, in *Nuove Leggi civili commentate*, 2017, p. 2 ss. Per una definizione completa di *accountability*, v. anche la relazione illustrativa al decreto legislativo

Evocando la funzione propria di tale principio, il paragrafo 8 dell'art. 14 del Secondo Protocollo impone agli Stati parti di tenere dei registri o di disporre di altri mezzi adeguati rendere conto di come e i dati personali sono consultati, utilizzati e divulgati. Il senso dell'*accountability*, infatti, risiede proprio nel termine "dimostrare", che fa sorgere in capo alle parti l'obbligo di strutturare delle procedure e dei modelli mediante i quali dare evidenza di come e per quale scopo sono stati trattati i dati di una persona fisica. Tale previsione, da un lato, consolida in capo agli Stati una certa libertà nell'individuazione degli strumenti e delle modalità di trattamento dei dati personali e, dall'altro, si traduce nell'obbligo di dare atto e dimostrare – in caso di verifica da parte della competente Autorità di vigilanza – la correttezza delle scelte compiute rispetto alle misure giuridiche, organizzative e tecniche concretamente adottate.

Un altro punto di contatto 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[31]. Rispetto all'approccio utilizzato in ambito UE e suggerito in fase di consultazione dall'*European Data Protection Board* (EDPB)[32], si può tuttavia riscontrare una differenza di non poco conto. L'accordo aggiuntivo alla Convenzione di Budapest, infatti, contempla un'eccezione alla regola 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 trascina con

recante disposizioni per l'adeguamento della normativa nazionale alle disposizioni del GDPR.

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

[32] *Statement* dell'EDPB del 13 novembre 2019; *statement* dell'EDPB n. 2/201; *contribution* dell'EDPB del 4 maggio 2021.

sé 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"[33].

Il Secondo Protocollo ha poi anche recepito il principio della trasparenza[34], 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 UE, atteso che le informazioni sul trattamento assumono rilevanza anche rispetto ad un eventuale ricorso alle vie giudiziali ed extragiudiziali[35], spesso indispensabili per tutelare i cittadini a fronte di 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. Siffatto principio, fissato dal paragrafo 15 dell'art. 14, dimostra come anche gli interessi sottesi alle nuove misure in materia 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*.

[33] 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.

[34] La portata del principio della trasparenza è ben espressa, anche in relazione al tema della semplificazione espressiva, dal considerando n. 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".

[35] 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 (eds.), *The EU Charter of Fundamental Rights. A Commentary*, London, 2022, p. 296 ss.

4. Per completare l'analisi sin qui condotta, occorre sinteticamente soffermarsi anche sulle indicazioni fornite dall'Unione agli Stati membri, con la decisione del 5 aprile 2022 che ha autorizzato la sottoscrizione del Secondo Protocollo[36], in tema di riserve, dichiarazioni, notifiche e comunicazioni[37]. Per quanto qui interessa, il Consiglio dell'Unione ha in primo luogo invitato i Paesi membri ad astenersi dall'apporre riserve a carattere "generale" con riferimento all'applicazione dell'art. 7 e dell'art. 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[38]. A fronte di siffatto invito, l'UE ha poi accordato ai Paesi membri il permesso di apporre una riserva a carattere delimitato rispetto 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[39].

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[40].

---

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

[37] 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*, n. 9, 2022, p. 1160 ss.

[38] 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, p. 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, p. 1050 ss.

[39] Par. 1 dell'Allegato alla decisione (UE) 2022/722, cit.

[40] Par. 3 dell'Allegato alla decisione (UE) 2022/722, cit.

In merito al delicato tema del trasferimento transfrontaliero dei dati personali[41], 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[42].

Dal momento che il Secondo Protocollo consente poi agli Stati di applicare un accordo bilaterale in luogo delle garanzie in materia di protezione dei dati personali[43], l'UE ha specificato che tale possibilità resta subordinata all'adozione di una specifica decisione di adeguatezza da parte della Commissione europea[44].

Da ultimo, con la decisione (UE) 2022/722 il Consiglio ha fornito agli Stati indicazioni sulle comunicazioni che dovranno rendere in merito ai trasferimenti transfrontalieri dei dati personali verso gli Stati Uniti[45]. In proposito, l'UE ha, da un lato, riconosciuto l'applicabilità ai rapporti tra le autorità procedenti dell'*Umbrella Agreement*[46] 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

[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.*, p. 129 ss.

[42] Par. 4 dell'Allegato alla decisione (UE) 2022/722, cit.

[43] L'art. 14, par. 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".

[44] Ultimo capoverso del par. 3 dell'Allegato alla decisione (UE) 2022/722, cit. Per un approfondimento sulla decisione di adeguatezza, cfr. 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, Milano, 2021, p. 95 ss.

[45] 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*, n. 3, 2016, p. 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 ZENCOVICH (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma, 2016, p. 265 ss.; V. BRECEVICH, *op cit.*, pp. 107-112.

[46] 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 www.eur-lex.europa.eu/legal-content/en/TXT/?uri.

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[47].

5. La riscontrata correlazione tra le norme del nuovo Protocollo e il quadro regolamentare dell'Unione in materia dimostra sicuramente un certo grado di *privacy compliance* del nuovo accordo aggiuntivo alla Convenzione di Budapest. Il Secondo Protocollo è stato anche definito come uno strumento giuridico che, oltre a promuovere il noto principio della *double criminality*[48], avrebbe posto l'accento anche sull'importanza della *double privacy* nelle indagini digitali[49]. L'esame dell'art. 14 induce infatti a ritenere che, nell'ambito delle nuove misure di cooperazione, il trattamento dei dati personali dovrà avvenire nel rispetto della normativa prevista in materia da ciascuno Stato coinvolto nell'attività di indagine, ovvero in ossequio alla disciplina sia della "Parte ricevente" sia della "Parte trasmittente"[50]. In questa prospettiva, affinché la cooperazione possa avere luogo sarà necessario che i Paesi interessati assicurino un livello analogo di protezione dei dati personali, stante il potere, riconosciuto ad ogni Stato, di sospenderne il trasferimento laddove si riscontrino carenze in termini di garanzie per le libertà individuali[51].

---

[47] Capoversi terzultimo e penultimo del par. 3 dell'Allegato alla decisione (UE) 2022/722, cit.

[48] 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, p. 10 ss.

[49] P. PERRI, *op. cit.*, p. 1158 ss.

[50] "Parte trasmittente" e "Parte ricevente" sono le due espressioni impiegate dall'art. 14, rispettivamente, per individuare lo Stato che fornisce dati personali, in attuazione del Secondo Protocollo, e il Paese che li riceve. Il nuovo accordo aggiuntivo alla Convenzione di Budapest contempla solo la definizione della "Parte trasmittente", identificata dall'art. 3, lett. e), nello Stato "che trasmette i dati in risposta a una richiesta o in quanto parte di una squadra investigativa comune o, ai fini del capo II, sezione 2, una Parte nel cui territorio si trova un prestatore di servizi di trasmissione o un soggetto che fornisce servizi di registrazione di nomi di dominio".

[51] Art. 14, par. 15, Secondo Protocollo.

Tuttavia, se, da una parte, va accolto con positività 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'*European Data Protection Supervisor* (EDPS)[52], porta con sé potenziali rischi per il diritto alla protezione dei dati personali e quindi per le libertà degli individui. Oltre alla discutibile eccezione all'obbligo di comunicare eventuali incidenti di sicurezza di cui si è detto innanzi, sussistono perplessità in ordine ad alcuni profili che si sintetizzano di seguito.

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[53]. Sebbene l'Unione abbia invitato gli Stati membri a prescrivere la notifica di tali ordini e/o richieste anche agli enti di controllo in materia[54], la circostanza che tale notifica non sia idonea, *di per sé*, a sospendere l'efficacia delle misure di cui agli artt. 6 e 7 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[55]. Sempre sotto il profilo di potenziali ripercussioni sui diritti degli interessati, giova evidenziare che il Secondo Protocollo rimette alle discipline interne la regolamentazione

[52] Cfr. *Opinion* dell'EDPS, n. 3, del 2 aprile 2019.

[53] Sul contenuto e sulla 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*, n. 8, 2022, p. 1041 ss. Con riferimento all'art. 7 si rinvia a C. PIROZZOLI, *op. cit.*

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

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

dei casi di limitazione di tali diritti[56]. Si tratta di un aspetto su cui si è soffermato in modo evidentemente critico anche l'EDPS con il parere 1/2022[57].

Un'altra questione che desta perplessità riguarda le richieste di informazioni sulla registrazione dei nomi di dominio *ex* art. 6 del Secondo Protocollo, sostanzialmente interessanti i fornitori privati di servizi informatici. Infatti, differentemente da quanto generalmente previsto per gli artt. 7 e 8, con riferimento a tali richieste non è stata contemplata la possibilità, per gli Stati sottoscrittori, di rendere dichiarazioni, eventualmente volte a coinvolgere nella decisione autorità pubbliche interne[58].

Una delle maggiori criticità attiene poi alla compatibilità delle norme previste dal Secondo Protocollo, in materia di trasferimenti transfrontalieri, con quanto affermato in passato dalla Corte di giustizia UE[59]. 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

[56] Per un inquadramento generale sulla limitazione dei diritti degli interessati nell'ambito delle attività di indagine e alla luce della normativa UE, si veda M. MARTORANA, *Il trattamento dei dati personali nell'attività investigativa*, p. 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 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. sentenza della Corte del 6 ottobre 2015, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, punto 95, (nota come *Schrems I*).

[57] *Opinion* dell'EDPS, n. 1, 2022, punto 107.

[58] Per un approfondimento sulle disposizioni del Secondo Protocollo in materia di riserve e dichiarazioni, cfr. M. BUCCARELLA, *op. cit.*, pp. 1163-1165.

[59] Cfr., in particolare, il parere della Corte del 26 luglio 2017, 1/15, 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; sentenza *Schrems I*, cit.; sentenza della Corte del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Limited e Maximillian Schrems* (nota come *Schrems II*). Per un approfondimento sul contenuto di tali pronunce, si veda C. GENTILE, *La saga Schrems e la tutela dei diritti fondamentali*, in *federalismi.it*, n. 1, 2021, p. 35 ss.

concludere un accordo bilaterale in materia con l'UE[60], 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 l'*Explanatory Report* del Secondo Protocollo[61] risultino 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. È qui sufficiente richiamare il parere 1/15[62], ove la Corte, con riferimento all'accordo tra Canada e UE sul trasferimento e sul trattamento dei dati del codice di prenotazione[63], aveva ritenuto che la formulazione delle ipotesi in cui il Canada avrebbe potuto trattare i dati PNR fosse "troppo vaga e generica per soddisfare i requisiti di chiarezza e di precisione imposti"[64]. La Corte non si è soffermata soltanto sulla vaghezza di alcuni dei concetti contemplati dall'accordo PNR tra Canada e UE, ma ha altresì stigmatizzato l'inclusione dei dati cd. sensibili o particolari[65] nelle categorie di dati trasferibili, per i quali è invece richiesta una giustificazione rafforzata[66]. Anche il Secondo

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

[61] Comitato della convenzione sulla criminalità informatica (*Cybercrime Convention Committee* o T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence – Explanatory Report*, 17 November 2021, adottato dal Comitato dei Ministri del Consiglio d'Europa, doc. CM (2021) 57-addfinal.

[62] Per un commento a tale parere, si veda C. GRAZIANI, *PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali*, in *DPCE online*, n. 4, 2017, pp. 959-966.

[63] 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 dal Parlamento europeo *ex* art. 218, par. 11, TFUE.

[64] Parere della Corte 1/15, cit, punto 181. Sull'importanza di garantire norme chiare e precise che regolino il trattamento dei dati personali, anche nell'ambito dell'attività di indagine preventiva per l'accertamento e il perseguimento dei reati, cfr. sentenza della Corte del 5 aprile 2022, causa C-140/20, *G.D. c. The Commissioner of the Gardda Siochana e a.*; sentenza della Corte del 2 marzo 2021, causa C-746/18, *H.K.*

[65] L'art. 9 del GDPR impiega la nozione di "dati particolari" per indicare quei dati che "rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale" nonché i "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona". Cfr. anche art. 14, parr. 13-15, e i considerando nn. 51-56 del GDPR.

[66] Parere della Corte 1/15, cit, punti 164-167. Si veda anche l'art. 10 della direttiva (UE) 2016/680, cit., secondo cui il trattamento dei dati particolari è ammesso,

Protocollo contiene disposizioni dal contenuto indeterminato, tra cui, ad esempio, l'art. 14, par. 2, lett. a), che vieta agli Stati di trattare i dati "per una finalità incompatibile". Una definizione di tale concetto non si rinviene nemmeno nel già richiamato *Explanatory Report*[67], atteso che il par. 229, relativo all'art. 14, par. 2, si limita a fornire un elenco generico – ed evidentemente non esaustivo – delle sole finalità ritenute "compatibili". Il nuovo accordo aggiuntivo alla Convenzione di Budapest ammette poi il trattamento dei "dati sensibili", a condizione che siano previste "garanzie adeguate per evitare il rischio di conseguenze pregiudizievoli ingiustificate". Anche in questo caso, tuttavia, né il Secondo Protocollo né l'*Explanatory Report* specificano quali siano gli standard minimi per definire l'adeguatezza delle garanzie. A quanto evidenziato sin qui si aggiungono le criticità connesse alla disciplina sulla conservazione dei dati (o *data retention*), dettata dal par. 5 dell'art. 14 del Secondo Protocollo. Tale norma non specifica precisi limiti di durata, limitandosi a prescrivere che la conservazione avvenga per "il periodo di tempo necessario e opportuno per le finalità del trattamento dei dati" ottenuti attraverso qualsivoglia tipo di indagine, a prescindere dalla natura e dalla gravità del crimine per cui si procede[68].

In questo quadro, la domanda sorge dunque spontanea: le previsioni del Secondo Protocollo sono sufficienti a fondare giuridicamente, *a priori*, il trattamento transfrontaliero di dati con Paesi terzi? Ciò vale

---

finanche nel caso di trattamenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, per ragioni strettamente necessarie e "soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato".

[67] *Explanatory Report*, CM (2021) 57-addfinal, cit.

[68] Sotto quest'ultimo profilo, il Secondo Protocollo si pone in contrasto con quanto affermato dalla recente giurisprudenza UE, ancorché con riferimento alla direttiva 2002/58/CE cit., applicabile al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti di comunicazione pubbliche (art. 3). Secondo la Corte di giustizia, infatti, "solo la lotta alle forme gravi di criminalità e la prevenzione di minacce gravi alla sicurezza pubblica sono idonee a giustificare ingerenze gravi nei diritti fondamentali sanciti agli articoli 7 e 8 della Carta, come quelle che comporta la conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione". Cfr. sentenza *G.D.*, cit., punto 59, che richiama la sentenza della Corte del 6 ottobre 2020, cause riunite C-511/18, C-512/18 e C-520/18, *La Quadrature du Net*, punto 140 e la giurisprudenza ivi citata.

anche con riferimento a Stati non membri del Consiglio d'Europa[69], 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.

Sempre in relazione al tema del trasferimento transfrontaliero dei dati personali, sussistono alcune perplessità in ordine all'accordo che l'UE 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 1/2022[70], si tratta di un accordo che non può trovare applicazione, sia perché non costituisce una base giuridica per il trasferimento dei dati[71], 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*[72]. Per effetto di tale provvedimento, 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[73]. 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 protecion*, auspicando la stipula di un accordo che offrisse idonee garanzie agli interessati, nello specifico

[69] Il Secondo Protocollo può essere sottoscritto anche da Paesi non membri del Consiglio d'Europa. In proposito si veda l'art. 2.
[70] *Opinion* dell'EDPS, n. 1, 2022, cit., punto 121.
[71] Come precisato proprio dall'art. 1, par. 3, dell'*Umbrella Agreement*, cit., June 2016.
[72] *Clarifying Lawful Overseas Use of Data (CLOUD) Act Clarifying Lawful Overseas Use of Data*, 21 March 2018, adottato dal Congresso USA 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 www.justice.gov/dag/page/file/1152896/download.
[73] 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, p. 1 ss.

ambito dei trasferimenti transfrontalieri di dati e prove digitali per fini investigativi e giudiziari[74]. Sebbene nel 2019 USA e UE si siano impegnati per negoziare siffatto tipo di accordo[75], ad oggi non si è ancora pervenuti ad una proposta risolutiva che riscontrasse l'invito *illo tempore* rivolto dalle due Autorità Garanti dell'Unione. Ciononostante, il Consiglio dell'Unione, nella decisione che autorizza la firma 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 la normativa UE in materia di dati personali.

6. All'esito di questa disamina è possibile trarre alcune conclusioni.

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, in considerazione delle innovazioni tecnologiche e nell'ottica di favorire anche le indagini transfrontaliere digitali. Il *favor* con cui è stato generalmente accolto il Secondo Protocollo potrebbe avere un impatto positivo sui negoziati attualmente in corso per l'elaborazione nuovo accordo transatlantico in materia di dati personali, di cui si sta discutendo negli ultimi mesi[76]. L'auspicio è che l'Unione, alla luce dei

[74] 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*, 12 July 2019.

[75] Cfr. *Joint US-EU Statement on Electronic Evidence Sharing Negotiations*, 26 September 2019, consultabile sul sito istituzionale del Governo USA al link www.justice.gov/opa/pr/joint-us-eu-statement-electronic-evidence-sharing.

[76] 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*, di cui i principi fondanti sono stati sintetizzati nel comunicato stampa dell'UE "European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework", 25 March 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 dovrà esprimere un'eventuale decisione di adeguatezza, dopo aver ottenuto un parere consultivo dell'EDPB e il parere positivo di un Comitato rappresentativo degli Stati membri. Proprio di recente, il 13 dicembre 2022, la Commissione ha diffuso una bozza di tale decisione, che sarà prossimamente sottoposta alla valutazione

rilievi dell'EPDB sull'applicabilità dell'*Umbrella Agreement*, richieda maggiori garanzie anche in merito all'attuazione delle nuove misure previste dal Secondo Protocollo, segnatamente sotto il profilo dei trasferimenti transfrontalieri dei dati personali.

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"[77]. Si tratta di un monito evidentemente volto a richiamare l'attenzione sull'importanza di prevedere, in ogni caso, idonee garanzie a presidio del fondamentale diritto alla protezione dei dati personali.

A fronte di eventuali rischi per i diritti delle persone fisiche e nell'attesa che sopravvenga un'eventuale decisione che autorizzi gli Stati membri alla ratifica[78], i giudici nazionali e della Corte di Giustizia dell'Unione europea[79] rappresentano oggi un baluardo contro l'illecito trattamento dei dati personali da parte di Paesi terzi.

---

dell'EDPB. La bozza del testo "on the adequate level of protection of personal data under the EU-US Data Privacy Framework" è consultabile sul sito istituzionale della Commissione UE, al link www.commission.europa.eu/system/files/202212/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf. Per un approfondimento in proposito, si veda G. RUGANI, *Gli ultimi sviluppi della saga sui trasferimenti di dati personali UE-USA: l'Executive Order firmato dal Presidente USA Biden il 7 ottobre 2022 e la proposta di decisione di adeguatezza presentata dalla Commissione UE il 13 dicembre 2022*, in *BlogDUE*, 19 gennaio 2023.

[77] *Opinion* dell'EDPS, n. 1, 2022, cit., punto 1.

[78] Ad oggi, a fronte dell'avvenuta approvazione della decisione (UE) 2022/722, cit., che autorizza gli Stati a firmare il Secondo Protocollo, risulta adottata solo la "proposta" di decisione che ne autorizza anche la ratifica. Si veda la proposta di decisione del Consiglio, del 2 dicembre 2021, 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, COM (2021) 719final.

[79] 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*, in *rivista.eurojus.it*, 2018, pp. 1-24.

D'altro canto, il Parlamento o un altro dei soggetti di cui all'art. 218, par. 11, TFUE[80] potrebbero interpellare direttamente la Corte di giustizia circa la compatibilità del Secondo Protocollo con il diritto alla protezione dei dati personali, tutelato 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 – in parte riferite anche a soggetti privati – sul diritto alla protezione dei dati personali, escludendo in radice un eventuale *coup de théâtre* nella fase di attuazione del nuovo accordo, come invece accaduto prima con il *Safe Harbor* e poi con il *Privacy Shield*[81]. Del resto, si potrebbe profilare un problema di ricevibilità della richiesta di un simile parere, atteso che l'Unione europea ha già autorizzato i Paesi membri alla firma. Dal momento, però, che il trattato non è ancora entrato in vigore e nessuno dei Paesi firmatari ha ad oggi provveduto a ratificarlo, potrebbe comunque valere la pena correre il rischio di una dichiarazione di irricevibilità da parte della Corte. 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 che sono tradizionalmente meno votati alla tutela della privacy e della protezione dei dati personali. In questo quadro, anche "tentare" di prevenire sarebbe meglio che curare.

[80] 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".

[81] 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*, cit. 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.