COMMISSIONE
EUROPEA

Bruxelles, 25.11.2021
COM(2021) 718 final

2021/0382 (NLE)

Proposta di

DECISIONE DEL CONSIGLIO

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

RELAZIONE

1. OGGETTO DELLA PROPOSTA

La presente proposta riguarda la decisione che autorizza gli Stati membri a firmare, nell'interesse dell'Unione europea, il secondo protocollo addizionale alla Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche ("il protocollo").[1] L'obiettivo del protocollo è stabilire norme comuni a livello internazionale per rafforzare la cooperazione in materia di criminalità informatica e la raccolta di prove in formato elettronico a fini di indagini o procedimenti penali.

La Commissione presenterà anche una proposta di decisione del Consiglio dell'Unione europea ("il Consiglio") che autorizza gli Stati membri a ratificare il protocollo nell'interesse dell'Unione europea.

La criminalità informatica continua a rappresentare una sfida considerevole per la nostra società. Nonostante gli sforzi compiuti dalle autorità di contrasto e dalle autorità giudiziarie, gli attacchi informatici, compresi gli attacchi con ransomware, sono in aumento e stanno diventando più complessi.[2] In particolare, poiché Internet è senza frontiere, le indagini sulla criminalità informatica sono quasi sempre di tipo transfrontaliero ed esigono pertanto una stretta cooperazione tra le autorità di paesi diversi.

Le prove elettroniche sono sempre più importanti nelle indagini penali. La Commissione ritiene che attualmente le autorità di contrasto e le autorità giudiziarie abbiano bisogno di accedere alle prove elettroniche nell'85 % delle indagini penali, comprese quelle in materia di criminalità informatica.[3] Le prove di reato sono sempre più spesso detenute in forma elettronica dai prestatori di servizi in giurisdizioni straniere e una risposta efficace della giustizia penale richiede misure adeguate per ottenere tali prove al fine di rispettare lo Stato di diritto.

A livello nazionale, dell'Unione europea[4] e internazionale si cerca di migliorare l'accesso transfrontaliero alle prove elettroniche per le indagini penali in tutto il mondo, anche attraverso il protocollo. È importante garantire l'esistenza di norme compatibili a livello internazionale per evitare conflitti di legge laddove sia richiesto l'accesso transfrontaliero alle prove elettroniche.

2. CONTESTO DELLA PROPOSTA

2.1. Contesto

La Convenzione di Budapest del Consiglio d'Europa sulla criminalità informatica (STCE n. 185) ("la Convenzione") è volta ad agevolare la lotta contro i reati compiuti avvalendosi di reti informatiche. La Convenzione (1) contiene disposizioni che armonizzano gli elementi del diritto penale sostanziale interno e le disposizioni collegate nel settore della criminalità informatica, (2) fornisce le competenze di diritto procedurale penale a livello

[1] Il testo del protocollo sarà allegato alla proposta di decisione del Consiglio che autorizza gli Stati membri a ratificare il protocollo nell'interesse dell'Unione.

[2] Valutazione da parte dell'Unione europea della minaccia rappresentata dalla criminalità organizzata e dalle forme gravi di criminalità del 2021 (SOCTA dell'UE 2021).

[3] SWD(2018) 118 final.

[4] COM (2018) 225 e 226 final.

interno necessarie per le indagini e l'esercizio dell'azione penale in relazione a tali reati, così come in relazione ad altri reati commessi per mezzo di un sistema informatico o laddove le prove siano in formato elettronico e (3) è volta a istituire un rapido ed efficiente regime di cooperazione internazionale.

La Convenzione è aperta agli Stati membri del Consiglio d'Europa e, su invito, ai paesi che non ne sono membri. Ne fanno attualmente parte 66 paesi, tra cui 26 Stati membri dell'Unione europea.[5] La Convenzione non prevede l'adesione dell'Unione europea, che è tuttavia riconosciuta come organizzazione con lo status di osservatore presso il Comitato della Convenzione sulla criminalità informatica (T-CY).[6]

Nonostante gli sforzi profusi per negoziare una nuova Convenzione sulla criminalità informatica a livello delle Nazioni Unite[7], la Convenzione di Budapest rimane la principale convenzione multilaterale in materia di lotta contro la criminalità informatica. L'Unione offre un sostegno costante alla Convenzione[8], anche nel quadro del finanziamento di programmi di sviluppo delle capacità.[9]

A seguito delle proposte del Cloud Evidence Group[10], il Comitato della Convenzione sulla criminalità informatica ha adottato numerose raccomandazioni per affrontare, anche negoziando un secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione internazionale rafforzata, la sfida posta dal fatto che le prove elettroniche relative alla criminalità informatica e ad altri reati sono sempre più conservate da prestatori di servizi ubicati in giurisdizioni straniere, mentre i poteri delle autorità di contrasto rimangono limitati dai confini territoriali. Nel giugno 2017 il Comitato della Convenzione sulla criminalità informatica ha approvato il mandato per la preparazione del secondo protocollo addizionale nel periodo compreso tra settembre 2017 e dicembre 2019.[11] Dato che occorreva più tempo per ultimare le discussioni, e date le limitazioni poste dalla pandemia di COVID-19 nel 2020 e nel 2021, il Comitato della Convenzione sulla criminalità informatica ha successivamente prorogato il mandato due volte, fino a dicembre 2020 e poi fino a maggio 2021.

A seguito dell'invito formulato dal Consiglio europeo nelle sue conclusioni del 18 ottobre 2018[12], il 5 febbraio 2019 la Commissione ha adottato una raccomandazione di decisione del Consiglio che autorizza la Commissione a partecipare, a nome dell'Unione europea, ai negoziati su un secondo protocollo addizionale alla Convenzione del Consiglio

---

5 Tutti tranne l'Irlanda, che ha firmato ma non ratificato la Convenzione e si è comunque impegnata a proseguire nel percorso per l'adesione.

6 Regolamento interno del Comitato della Convenzione sulla criminalità informatica (T-CY (2013)25 rev), disponibile all'indirizzo www.coe.int/cybercrime.

7 Risoluzione 74/247 dell'Assemblea generale delle Nazioni Unite, del dicembre 2019, sul contrasto all'uso di tecnologie dell'informazione e della comunicazione a scopi criminali.

8 JOIN(2020) 81 final.

9 Cfr., ad esempio, l'azione globale estesa contro la criminalità informatica (GLACY+) all'indirizzo https://www.coe.int/en/web/cybercrime/glacyplus.

10 Relazione finale del Cloud Evidence Group del Comitato della Convenzione sulla criminalità informatica: "Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY" (Accesso della giustizia penale alle prove elettroniche nel cloud: raccomandazioni per l'esame da parte del T-CY) del 16 settembre 2016.

11 https://rm.coe.int/t-cy-terms-of-reference-protocol/1680a03690.

12 https://www.consilium.europa.eu/it/press/press-releases/2018/10/18/20181018-european-council-conslusions/

d'Europa sulla criminalità informatica.[13] Il Garante europeo della protezione dei dati ha adottato un parere sulla raccomandazione il 2 aprile 2019.[14] Con decisione del 6 giugno 2019, il Consiglio dell'Unione europea ha autorizzato la Commissione a partecipare, a nome dell'Unione europea, ai negoziati su un secondo protocollo addizionale.[15]

Come indicato nella strategia dell'UE del 2020 per l'Unione della sicurezza[16], nella strategia dell'UE del 2020 in materia di cibersicurezza per il decennio digitale[17] e nella strategia dell'UE del 2021 per la lotta alla criminalità organizzata[18], la Commissione si è impegnata a concludere in modo rapido ed efficace i negoziati sul protocollo. Il Parlamento europeo ha inoltre riconosciuto la necessità di concludere i lavori sul protocollo nella sua risoluzione del 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale.[19]

La Commissione ha partecipato, a nome dell'Unione europea, ai negoziati sul protocollo in linea con la decisione del Consiglio dell'Unione europea. La Commissione si è consultata costantemente con la Commissione speciale del Consiglio per i negoziati in merito alla posizione dell'Unione.

In linea con l'accordo quadro sulle relazioni tra il Parlamento europeo e la Commissione europea[20], la Commissione ha inoltre tenuto informato il Parlamento europeo sull'andamento dei negoziati mediante relazioni scritte e presentazioni orali.

Nella riunione plenaria del 28 maggio 2021, il Comitato della Convenzione sulla criminalità informatica ha approvato il progetto di protocollo al suo livello e lo ha trasmesso per adozione al Comitato dei Ministri del Consiglio d'Europa.[21] Il 17 novembre 2021 il Comitato dei Ministri del Consiglio d'Europa ha adottato il protocollo.

2.2. Il secondo protocollo addizionale

L'obiettivo del protocollo è rafforzare la cooperazione in materia di criminalità informatica e la raccolta di prove di reato in formato elettronico a fini di indagini o procedimenti penali specifici. Il protocollo riconosce la necessità di una cooperazione rafforzata e più efficace tra gli Stati e con il settore privato, nonché di una maggiore chiarezza e certezza del diritto per i prestatori di servizi e altri soggetti per quanto riguarda le circostanze in cui possono rispondere alle richieste di divulgazione di prove elettroniche presentate dalle autorità giudiziarie penali di altre Parti.

Il protocollo riconosce inoltre che un'efficace cooperazione transfrontaliera ai fini della giustizia penale, anche tra autorità del settore pubblico e soggetti del settore privato, richiede condizioni efficaci e solide garanzie per la tutela dei diritti fondamentali. A tal fine, il protocollo segue un approccio basato sui diritti e prevede condizioni e garanzie in linea con

---

13 COM(2019) 71 final.
14 Parere 3/2019 del GEPD concernente la partecipazione ai negoziati in vista di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, del 2 aprile 2019.
15 Decisione del Consiglio 9116/19.
16 COM(2020) 605 final.
17 JOIN(2020) 81 final.
18 COM(2021) 170 final.
19 Risoluzione del Parlamento europeo del 10 giugno 2021 sulla strategia dell'UE in materia di cibersicurezza per il decennio digitale.
20 GU L 304 del 20.11.2010, pag. 47.
21 https://rm.coe.int/0900001680a2aa42

gli strumenti internazionali in materia di diritti umani, compresa la Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (1950). Poiché le prove elettroniche riguardano spesso dati personali, il protocollo prevede altresì solide garanzie per la protezione della vita privata e dei dati personali.

Le disposizioni descritte qui di seguito rivestono particolare importanza per il protocollo. Il protocollo è corredato da una relazione esplicativa dettagliata. Pur non costituendo uno strumento che fornisce un'interpretazione autentica del protocollo, la relazione esplicativa è intesa a "guidare e assistere le Parti" nell'applicazione del protocollo stesso.[22]

2.2.1. Disposizioni comuni

Il capo I del protocollo contiene le disposizioni comuni. L'articolo 2 definisce il campo di applicazione del protocollo, in linea con quello della Convenzione: il protocollo si applica a indagini o procedimenti penali specifici relativi a reati connessi a sistemi e dati informatici, e all'acquisizione di prove di reato in formato elettronico.

L'articolo 3 contiene le definizioni di "autorità centrale", "autorità competente", "emergenza", "dati personali" e "Parte trasmittente". Tali definizioni si applicano al protocollo assieme alle definizioni contenute nella Convenzione.

L'articolo 4 stabilisce le lingue in cui le Parti devono trasmettere ordini, richieste o notifiche a norma del protocollo.

2.2.2. Misure di cooperazione

Il capo II del protocollo contiene misure volte a rafforzare la cooperazione. In primo luogo l'articolo 5, paragrafo 1, stabilisce che le Parti cooperano nella misura più ampia possibile sulla base del protocollo. L'articolo 5, paragrafi da 2 a 5, definisce l'applicazione delle misure del protocollo in relazione ai trattati o alle intese di assistenza giudiziaria esistenti. L'articolo 5, paragrafo 7, stabilisce che le misure di cui al capo II non limitano la cooperazione tra le Parti, o tra le Parti e i prestatori di servizi o altri soggetti, mediante altri accordi, intese, pratiche o leggi nazionali applicabili.

L'articolo 6 fornisce una base per la cooperazione diretta tra le autorità competenti di una Parte e i soggetti che forniscono servizi di registrazione di nomi di dominio di un'altra Parte ai fini della divulgazione dei dati relativi alle registrazioni di nomi di dominio.

L'articolo 7 fornisce una base per la cooperazione diretta tra le autorità competenti di una Parte e i prestatori di servizi di un'altra Parte ai fini della divulgazione delle informazioni relative agli abbonati.

L'articolo 8 fornisce una base per la cooperazione rafforzata tra le autorità ai fini della divulgazione di dati informatici.

L'articolo 9 fornisce una base per la cooperazione tra le autorità ai fini della divulgazione di dati informatici in situazioni di emergenza.

L'articolo 10 fornisce una base per l'assistenza giudiziaria in situazioni di emergenza.

---

[22] Cfr. paragrafo 2 della relazione esplicativa del protocollo.

L'articolo 11 fornisce una base per la cooperazione tramite videoconferenze.

L'articolo 12 fornisce una base per le indagini congiunte e le squadre investigative comuni.

2.2.3. Garanzie

Il protocollo segue un approccio basato sui diritti, con condizioni e garanzie specifiche, alcune delle quali sono inserite nell'ambito delle specifiche misure di cooperazione, nonché nel capo III del protocollo. L'articolo 13 del protocollo impone alle Parti di assicurare che i poteri e le procedure siano soggetti a un adeguato livello di tutela dei diritti fondamentali che garantisca, in linea con l'articolo 15 della Convenzione, l'applicazione del principio di proporzionalità.

L'articolo 14 del protocollo prevede la protezione dei dati personali, quali definiti all'articolo 3 in linea con il protocollo che modifica la Convenzione sulla protezione delle persone rispetto al trattamento di dati a carattere personale (STE n. 223) (Convenzione n. 108+) e con il diritto dell'Unione.

Su tale base, l'articolo 14, paragrafi da 2 a 15, stabilisce i principi fondamentali in materia di protezione dei dati, che includono la limitazione delle finalità, la base giuridica, la qualità dei dati e le norme applicabili al trattamento di categorie particolari di dati, gli obblighi applicabili ai titolari del trattamento, anche in merito alla conservazione, la tenuta di registri, la sicurezza e i trasferimenti successivi, i diritti individuali applicabili, in particolare in materia di notifica, accesso, rettifica e processo decisionale automatizzato, il controllo indipendente ed efficace da parte di una o più autorità nonché il ricorso amministrativo e giudiziario. Le garanzie riguardano tutte le forme di cooperazione previste dal protocollo, con gli adeguamenti necessari per tenere conto delle caratteristiche specifiche della cooperazione diretta (ad esempio nel contesto della notifica di violazioni). L'esercizio di determinati diritti individuali può essere ritardato, limitato o rifiutato ove necessario e proporzionato per perseguire importanti obiettivi di interesse pubblico, in particolare per prevenire rischi per indagini di polizia in corso, il che è anche in linea con il diritto dell'Unione.

L'articolo 14 del protocollo va inoltre letto in combinato disposto con l'articolo 23. L'articolo 23 rafforza l'efficacia delle garanzie previste dal protocollo stabilendo che il Comitato della Convenzione sulla criminalità informatica deve valutare l'attuazione e l'applicazione delle misure adottate nella legislazione nazionale per dare attuazione alle disposizioni del protocollo. In particolare l'articolo 23, paragrafo 3, riconosce esplicitamente che l'attuazione dell'articolo 14 da parte delle Parti sarà valutata quando dieci Parti della Convenzione avranno espresso il loro consenso a essere vincolate dal protocollo.

A titolo di ulteriore garanzia, a norma dell'articolo 14, paragrafo 15, qualora una Parte disponga di prove sostanziali del fatto che un'altra Parte viola in modo sistematico o rilevante le garanzie previste dal protocollo, essa può sospendere il trasferimento di dati personali a tale Parte previa consultazione (non necessaria in caso di urgenza). I dati personali trasferiti prima della sospensione devono continuare ad essere trattati conformemente al protocollo.

Infine, tenuto conto del carattere multilaterale del protocollo, l'articolo 14, paragrafo 1, lettere b) e c), consente alle Parti nelle loro relazioni bilaterali di concordare, a determinate condizioni, modalità alternative per garantire la protezione dei dati personali trasferiti in virtù del protocollo. Se le garanzie di cui all'articolo 14, paragrafi da 2 a 15, si applicano automaticamente alle Parti che ricevono dati personali, in base all'articolo 14, paragrafo 1, lettera b), possono attenersi a tale quadro anche le Parti vincolate reciprocamente da un accordo internazionale che istituisce un quadro globale per la protezione dei dati personali, in

linea con i requisiti applicabili della legislazione delle Parti interessate. Ciò riguarda, ad esempio, la Convenzione n. 108+ (per le Parti che consentono il trasferimento di dati ad altre Parti in virtù di tale Convenzione) o l'accordo quadro UE-USA (nel suo ambito di applicazione, vale a dire per il trasferimento di dati personali tra autorità e, in combinazione con un accordo specifico di trasferimento tra gli Stati Uniti e l'UE, per la cooperazione diretta tra autorità e prestatori di servizi). Inoltre, a norma dell'articolo 14, paragrafo 1, lettera c), le Parti possono anche stabilire di comune accordo che il trasferimento di dati personali avvenga sulla base di altri accordi o intese tra le Parti interessate. Per quanto riguarda gli Stati membri dell'UE, essi possono attenersi a tali accordi o intese alternative per i trasferimenti di dati a norma del protocollo solo se tali trasferimenti sono conformi ai requisiti del diritto dell'Unione in materia di protezione dei dati, segnatamente il capo V della direttiva (UE) 2016/680 (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie) e, per la cooperazione diretta tra autorità e prestatori di servizi ai sensi degli articoli 6 e 7 del protocollo, il capo V del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati).

2.2.4. Disposizioni finali

Il capo IV del protocollo contiene le disposizioni finali. Tra l'altro l'articolo 15, paragrafo 1, lettera a), garantisce che le Parti possano stabilire le loro relazioni in merito alle questioni previste dal protocollo in altri modi, in linea con l'articolo 39, paragrafo 2, della Convenzione. L'articolo 15, paragrafo 1, lettera b), garantisce che gli Stati membri dell'UE che sono Parti del protocollo possano continuare ad applicare il diritto dell'Unione nelle loro relazioni reciproche. L'articolo 15, paragrafo 2, stabilisce inoltre l'applicazione al protocollo dell'articolo 39, paragrafo 3, della Convenzione.

L'articolo 16, paragrafo 3, stabilisce che il protocollo entrerà in vigore una volta che cinque Parti della Convenzione avranno espresso il loro consenso ad essere vincolate dal protocollo.

L'articolo 19, paragrafo 1, prevede che le Parti possano avvalersi di riserve in relazione all'articolo 7, paragrafo 9, lettere a) e b), all'articolo 8, paragrafo 13, e all'articolo 17. L'articolo 19, paragrafo 2, prevede che le Parti possano rilasciare dichiarazioni in relazione all'articolo 7, paragrafo 2, lettera b), e paragrafo 8, all'articolo 8, paragrafo 11, all'articolo 9, paragrafo 1, lettera b), e paragrafo 5, all'articolo 10, paragrafo 9, all'articolo 12, paragrafo 3, e all'articolo 18, paragrafo 2. L'articolo 19, paragrafo 3, stabilisce che una Parte formula le dichiarazioni, notifiche o comunicazioni di cui all'articolo 7, paragrafo 5, lettere a) ed e), all'articolo 8, paragrafo 4 e paragrafo 10, lettere a) e b), all'articolo 14, paragrafo 7, lettera c), e paragrafo 10, lettera b), e all'articolo 17, paragrafo 2.

L'articolo 23, paragrafo 1, fornisce una base per le consultazioni fra le Parti, anche attraverso il Comitato della Convenzione sulla criminalità informatica, in linea con l'articolo 46 della Convenzione. L'articolo 23, paragrafo 2, fornisce inoltre una base per la valutazione dell'uso e dell'attuazione delle disposizioni del protocollo. L'articolo 23, paragrafo 3, garantisce che la valutazione dell'uso e dell'attuazione dell'articolo 14 sulla protezione dei dati abbia inizio una volta che dieci Parti avranno espresso il loro consenso ad essere vincolate dal protocollo.

2.3. Diritto e politiche dell'Unione in materia

La materia oggetto dal protocollo è in gran parte disciplinata da norme comuni basate sull'articolo 82, paragrafo 1, e sull'articolo 16 TFUE. L'attuale quadro giuridico dell'Unione europea comprende in particolare strumenti relativi alla cooperazione delle autorità di contrasto e giudiziarie in materia penale, quali la direttiva 2014/41/UE relativa all'ordine

europeo di indagine penale, la Convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea e la decisione quadro 2002/465/GAI del Consiglio relativa alle squadre investigative comuni. A livello esterno, l'Unione europea ha concluso una serie di accordi bilaterali con paesi terzi, quali gli accordi sulla mutua assistenza giudiziaria tra l'Unione europea e gli Stati Uniti d'America, tra l'Unione europea e il Giappone e tra l'Unione europea e la Norvegia e l'Islanda. L'attuale quadro giuridico dell'Unione europea include anche il regolamento (UE) 2017/1939 relativo all'attuazione di una cooperazione rafforzata sull'istituzione della Procura europea ("EPPO"). Gli Stati membri che partecipano alla cooperazione rafforzata dovrebbero garantire che l'EPPO, nell'esercizio delle sue competenze ai sensi degli articoli 22, 23 e 25 del regolamento (UE) 2017/1939, possa chiedere la cooperazione a norma del protocollo allo stesso modo dei procuratori nazionali di tali Stati membri. Tali strumenti e accordi riguardano, in particolare, gli articoli 8, 9, 10, 11 e 12 del protocollo.

Inoltre, l'Unione ha adottato diverse direttive che rafforzano i diritti procedurali di indagati e imputati.[23] Tali strumenti riguardano, in particolare, gli articoli 6, 7, 8, 9, 10, 11, 12 e 13 del protocollo. Un particolare gruppo di garanzie riguarda la protezione dei dati personali, che è un diritto fondamentale sancito dai trattati dell'UE e dalla Carta dei diritti fondamentali dell'Unione europea. I dati personali possono essere trattati solo in conformità del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) e della direttiva (UE) 2016/680 (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie). Il rispetto della riservatezza delle comunicazioni è un elemento essenziale del diritto fondamentale di ogni persona al rispetto della vita privata e familiare, del domicilio e delle comunicazioni. I dati delle comunicazioni elettroniche possono essere trattati solo in conformità della direttiva 2002/58/CE (direttiva e-privacy). Tali strumenti riguardano, in particolare, l'articolo 14 del protocollo.

L'articolo 14, paragrafi da 2 a 15, del protocollo prevede garanzie adeguate in materia di protezione dei dati in virtù delle norme dell'Unione in materia di protezione dei dati, in particolare l'articolo 46 del regolamento generale sulla protezione dei dati e l'articolo 37 della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie, nonché della pertinente giurisprudenza della Corte di giustizia dell'Unione europea. In linea con gli obblighi previsti dal diritto dell'Unione[24] e al fine di garantire l'efficacia delle garanzie di cui all'articolo 14 del

[23] Direttiva 2010/64/UE del Parlamento europeo e del Consiglio, del 20 ottobre 2010, sul diritto all'interpretazione e alla traduzione nei procedimenti penali (GU L 280 del 26.10.2010, pag. 1); direttiva 2012/13/UE del Parlamento europeo e del Consiglio, del 22 maggio 2012, sul diritto all'informazione nei procedimenti penali (GU L 142 dell'1.6.2012, pag. 1); direttiva 2013/48/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa al diritto di avvalersi di un difensore nel procedimento penale e nel procedimento di esecuzione del mandato d'arresto europeo, al diritto di informare un terzo al momento della privazione della libertà personale e al diritto delle persone private della libertà personale di comunicare con terzi e con le autorità consolari (GU L 294 del 6.11.2013, pag. 1); direttiva (UE) 2016/1919 del Parlamento europeo e del Consiglio, del 26 ottobre 2016, sull'ammissione al patrocinio a spese dello Stato per indagati e imputati nell'ambito di procedimenti penali e per le persone ricercate nell'ambito di procedimenti di esecuzione del mandato d'arresto europeo (GU L 297 del 4.11.2016, pag. 1); direttiva (UE) 2016/800 del Parlamento europeo e del Consiglio, dell'11 maggio 2016, sulle garanzie procedurali per i minori indagati o imputati nei procedimenti penali (GU L 132 del 21.5.2016, pag. 1); direttiva (UE) 2016/343 del Parlamento europeo e del Consiglio, del 9 marzo 2016, sul rafforzamento di alcuni aspetti della presunzione di innocenza e del diritto di presenziare al processo nei procedimenti penali (GU L 65 dell'11.3.2016, pag. 1); direttiva 2012/13/UE del Parlamento europeo e del Consiglio, del 22 maggio 2012, sul diritto all'informazione nei procedimenti penali.

[24] Cfr. il parere 1/15 della Corte di giustizia (Grande Sezione), ECLI:EU:C:2017:592, punto 220. Cfr. anche il contributo del comitato europeo per la protezione dei dati alla consultazione su un progetto di secondo

protocollo, gli Stati membri dovrebbero provvedere a informare le persone i cui dati sono stati trasferiti, fatte salve talune restrizioni volte, ad esempio, a evitare di compromettere le indagini in corso. L'articolo 14, paragrafo 11, lettera c), del protocollo fornisce agli Stati membri una base per soddisfare tale requisito.

La compatibilità dell'articolo 14, paragrafo 1, del protocollo con le norme dell'Unione in materia di protezione dei dati richiede inoltre che gli Stati membri valutino quanto segue riguardo alle possibili modalità alternative per garantire un'adeguata protezione dei dati personali trasferiti a norma del protocollo. In merito ad altri accordi internazionali che istituiscono un quadro globale per la protezione dei dati personali in linea con gli obblighi applicabili della normativa delle Parti interessate, conformemente all'articolo 14, paragrafo 1, lettera b), gli Stati membri dovrebbero tenere conto del fatto che, ai fini della cooperazione diretta, l'accordo quadro UE-USA deve essere integrato da garanzie supplementari - da stabilire in uno specifico accordo di trasferimento tra gli Stati Uniti e l'UE o i suoi Stati membri - che tengano conto delle esigenze specifiche del trasferimento di prove elettroniche direttamente dai prestatori di servizi piuttosto che tra autorità.[25]

Inoltre, a norma dell'articolo 14, paragrafo 1, lettera b), del protocollo, gli Stati membri dovrebbero considerare che, per gli Stati membri dell'UE che sono Parti della Convenzione n. 108+, questa non costituisce di per sé una base adeguata per i trasferimenti transfrontalieri di dati a norma del protocollo verso altre Parti della Convenzione. A tale riguardo, dovrebbero tenere conto dell'ultima frase dell'articolo 14, paragrafo 1, della Convenzione n. 108+[26].

Infine, per quanto riguarda altri accordi o intese ai sensi dell'articolo 14, paragrafo 1, lettera c), gli Stati membri dovrebbero considerare che possono fare riferimento a tali altri accordi o intese solo se la Commissione europea ha adottato una decisione di adeguatezza a norma dell'articolo 45 del regolamento (UE) 2016/679 (regolamento generale sulla protezione dei dati) o dell'articolo 36 della direttiva (UE) 2016/680 (direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie) per il paese terzo interessato che abbia ad oggetto i rispettivi trasferimenti di dati, o se tale altro accordo o intesa garantisce adeguate garanzie in materia di protezione dei dati ai sensi dell'articolo 46 del regolamento generale sulla protezione dei dati o dell'articolo 37, paragrafo 1, lettera a), della direttiva sulla protezione dei dati nelle attività di polizia e giudiziarie.

---

protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest), del 13 novembre 2019, pag. 6 ("Le autorità nazionali competenti alle quali è stato concesso l'accesso ai dati devono informare le persone interessate, secondo le procedure nazionali applicabili, non appena tale notifica non sia più in grado di compromettere le indagini svolte da tali autorità. (...) La notifica è necessaria per consentire alle persone interessate di esercitare, tra l'altro, il loro diritto a un ricorso giurisdizionale e i loro diritti in materia di protezione dei dati in relazione al trattamento dei loro dati").

[25] Per questo motivo la decisione del Consiglio del 21 maggio 2019 che autorizza l'avvio di negoziati in vista di un accordo tra l'Unione europea e gli Stati Uniti d'America sull'accesso transfrontaliero alle prove elettroniche per la cooperazione giudiziaria in materia penale (9114/19) nelle sue direttive di negoziato contiene una serie di garanzie supplementari in materia di protezione dei dati. In particolare, le direttive di negoziato stabiliscono che "[l]'accordo dovrebbe integrare l'accordo quadro con garanzie supplementari che tengano conto del livello di sensibilità delle categorie di dati in questione e delle esigenze specifiche del trasferimento di prove elettroniche direttamente dai prestatori di servizi piuttosto che tra autorità e dei trasferimenti dalle autorità competenti direttamente ai prestatori di servizi".

[26] Cfr. anche la relazione esplicativa del protocollo che modifica la convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, 10 ottobre 2018, punti 106 e 107.

Occorre tenere conto non solo del diritto dell'Unione nella sua forma attuale nella materia in questione, ma anche del suo futuro sviluppo, nella misura in cui ciò sia prevedibile al momento dell'analisi. La materia disciplinata dal protocollo è direttamente rilevante per gli sviluppi futuri prevedibili del diritto dell'Unione. A tale riguardo, occorre prendere atto delle proposte della Commissione in materia di accesso transfrontaliero alle prove elettroniche dell'aprile 2018.[27] Tali strumenti riguardano, in particolare, gli articoli 6 e 7 del protocollo.

La Commissione, partecipando ai negoziati a nome dell'Unione, si è accertata che il protocollo fosse pienamente compatibile con il diritto dell'Unione e con gli obblighi che ne derivano per gli Stati membri. In particolare, la Commissione si è assicurata che le disposizioni del protocollo consentano agli Stati membri di rispettare i diritti fondamentali, le libertà e i principi generali del diritto dell'Unione sanciti dai trattati dell'UE e dalla Carta dei diritti fondamentali dell'Unione europea, compresi la proporzionalità, i diritti processuali, la presunzione di innocenza e il diritto alla difesa delle persone oggetto di procedimenti penali, nonché il diritto alla riservatezza e alla protezione dei dati personali e delle comunicazioni elettroniche quando tali dati sono trattati, compresi i trasferimenti alle autorità di contrasto di paesi al di fuori dell'Unione europea, e ogni obbligo che incombe alle autorità di contrasto e giudiziarie al riguardo. La Commissione ha inoltre tenuto conto del parere del Garante europeo della protezione dei dati[28] e del comitato europeo per la protezione dei dati.[29]

Inoltre, la Commissione ha verificato che le disposizioni del protocollo e le proposte della Commissione in materia di prove elettroniche fossero compatibili, anche man mano che il progetto legislativo si è evoluto nelle discussioni con i colegislatori, e che il protocollo non desse luogo a conflitti di legge. In particolare, si è assicurata che il protocollo includa adeguate garanzie in materia di protezione dei dati e riservatezza, che consentano ai prestatori di servizi dell'UE di rispettare i loro obblighi derivanti dalla normativa dell'UE in materia di protezione dei dati e vita privata, nella misura in cui il protocollo fornisce una base giuridica per il trasferimento di dati in risposta a ordini o richieste emessi da un'autorità di una Parte del protocollo non appartenente all'UE, che impongono a un titolare o responsabile del trattamento dell'UE di divulgare dati personali o dati di comunicazioni elettroniche.

2.4. Riserve, dichiarazioni, notifiche e comunicazioni e altre considerazioni

Il protocollo fornisce alle Parti la base per avvalersi di talune riserve e per formulare dichiarazioni, notifiche o comunicazioni in relazione a determinati articoli. Gli Stati membri dovrebbero adottare un approccio uniforme a talune riserve e dichiarazioni, notifiche e comunicazioni, quale stabilito dall'allegato della presente decisione. Al fine di garantire la compatibilità dell'attuazione del protocollo con il diritto dell'Unione, gli Stati membri dell'UE dovrebbero adottare la posizione riportata di seguito in merito a tali riserve e dichiarazioni. Qualora il protocollo fornisca una base per altre riserve, dichiarazioni, notifiche o

[27] COM (2018) 225 e 226 final.

[28] Parere 3/2019 del GEPD concernente la partecipazione ai negoziati in vista di un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica, del 2 aprile 2019.

[29] Compreso il contributo del comitato europeo per la protezione dei dati alla consultazione su un progetto di secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest), del 13 novembre 2019; la dichiarazione 02/201 sul nuovo progetto di disposizioni del secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest), del 2 febbraio 2021; il contributo del comitato europeo per la protezione dei dati al 6º ciclo di consultazioni su un progetto di secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica, del 4 maggio 2021.

comunicazioni, la presente proposta autorizza gli Stati membri a prevedere e formulare le proprie riserve, dichiarazioni, notifiche o comunicazioni.

Al fine di garantire la compatibilità tra le disposizioni del protocollo e il diritto e le politiche pertinenti dell'Unione, gli Stati membri non dovrebbero avvalersi delle riserve di cui all'articolo 7, paragrafo 9, lettere a)[30] e b)[31]. Inoltre, gli Stati membri dovrebbero formulare la dichiarazione di cui all'articolo 7, paragrafo 2, lettera b)[32], e la notifica di cui all'articolo 7, paragrafo 5, lettera a)[33]. L'assenza di tali riserve, nonché la presentazione della dichiarazione e della notifica, sono importanti per garantire la compatibilità del protocollo con le proposte legislative della Commissione in materia di prove elettroniche, anche man mano che il progetto legislativo evolve nelle discussioni con i colegislatori.

Inoltre, al fine di garantire un'applicazione uniforme del protocollo da parte degli Stati membri dell'UE nella loro cooperazione con Parti che non sono Stati membri dell'UE, gli Stati membri sono incoraggiati a non avvalersi della riserva di cui all'articolo 8, paragrafo 13[34], anche perché tale riserva avrebbe effetti reciproci[35]. Gli Stati membri dovrebbero formulare la dichiarazione di cui all'articolo 8, paragrafo 4, per garantire che possa essere data attuazione agli ordini qualora siano necessarie ulteriori informazioni di supporto, ad esempio sulle circostanze del caso in questione, al fine di valutarne la proporzionalità e la necessità.[36]

Gli Stati membri sono inoltre invitati ad astenersi dal formulare la dichiarazione di cui all'articolo 9, paragrafo 1, lettera b),[37] al fine di garantire un'efficace applicazione del protocollo.

Gli Stati membri dovrebbero formulare le comunicazioni di cui all'articolo 7, paragrafo 5, lettera e)[38], all'articolo 8, paragrafo 10, lettere a) e b)[39], all'articolo 14, paragrafo 7, lettera c), e paragrafo 10, lettera b), per garantire un'applicazione generale efficace del protocollo.[40]

---

30 Che consente alle Parti di riservarsi il diritto di non applicare l'articolo 7 (divulgazione delle informazioni relative agli abbonati).

31 Che consente alle Parti di riservarsi il diritto di non applicare l'articolo 7 (divulgazione delle informazioni relative agli abbonati) a determinati tipi di numeri di accesso qualora ciò sia incompatibile con i principi fondamentali del loro ordinamento giuridico interno.

32 Che consente alle Parti di dichiarare che l'ordine di cui all'articolo 7, paragrafo 1 (divulgazione delle informazioni relative agli abbonati) deve essere emesso da un procuratore o da un'altra autorità giudiziaria, o sotto la sua supervisione, oppure sotto la sorveglianza di un altro organismo indipendente.

33 Che consente alle Parti di notificare al Segretario generale del Consiglio d'Europa che, in caso di emissione di un ordine a norma dell'articolo 7, paragrafo 1 (divulgazione delle informazioni relative agli abbonati), ad un prestatore di servizi sul suo territorio, la Parte richiede, in ogni caso o in determinate circostanze, la notifica contestuale dell'ordine, delle informazioni supplementari e di una sintesi dei fatti relativi all'indagine o al procedimento.

34 Che consente alle Parti di riservarsi il diritto di non applicare l'articolo 8 (esecuzione degli ordini emessi da un'altra Parte) ai dati relativi al traffico.

35 A norma del paragrafo 147 della relazione esplicativa del protocollo, "[l]a Parte che formula una riserva al presente articolo non è autorizzata a trasmettere ordini relativi ai dati sul traffico ad altre Parti a norma [dell'articolo 8,] paragrafo 1".

36 Che consente alle Parti di dichiarare che sono necessarie ulteriori informazioni di supporto per poter dare esecuzione agli ordini di cui all'articolo 8, paragrafo 1 (esecuzione degli ordini emessi da un'altra Parte).

37 Che consente alle Parti di dichiarare che non daranno esecuzione alle richieste di cui all'articolo 9, paragrafo 1, lettera a) (divulgazione accelerata di dati informatici in caso di emergenza) volte unicamente alla divulgazione delle informazioni relative agli abbonati.

38 Che consente alle Parti di comunicare i dati di contatto dell'autorità da esse designata per ricevere notifiche a norma dell'articolo 7, paragrafo 5, lettera a), e per eseguire le azioni di cui all'articolo 7, paragrafo 5, lettere b), c) e d) (divulgazione delle informazioni relative agli abbonati).

39 Che consente alle Parti di comunicare i dati di contatto delle autorità designate per impartire e ricevere ordini a norma dell'articolo 8 (esecuzione degli ordini emessi da un'altra Parte). In linea con i requisiti di cui al

Infine, gli Stati membri dovrebbero adottare le misure necessarie a norma dell'articolo 14, paragrafo 11, lettera c), per garantire che la Parte ricevente sia informata al momento del trasferimento dell'obbligo, previsto dal diritto dell'Unione, di inviare una notifica alla persona a cui si riferiscono i dati[41], nonché degli opportuni dati di contatto per consentire alla Parte ricevente di informare l'autorità competente dello Stato membro dell'UE quando sono cessate le restrizioni di riservatezza e la notifica può essere inviata.

2.5. Motivazione della proposta

Il protocollo entrerà in vigore una volta che cinque Parti avranno espresso il loro consenso ad essere vincolate dal protocollo, conformemente alle disposizioni dell'articolo 16, paragrafi 1 e 2. La cerimonia di firma del protocollo è prevista per marzo 2022.

Gli Stati membri dell'UE dovrebbero adottare le misure necessarie per garantire la rapida entrata in vigore del protocollo, aspetto importante alla luce di diversi fattori.

In primo luogo, grazie al protocollo le autorità di contrasto e le autorità giudiziarie avranno mezzi migliori per ottenere le prove elettroniche necessarie per svolgere indagini penali. Data la crescente importanza delle prove elettroniche per le indagini penali, è urgente dotare le autorità di contrasto e le autorità giudiziarie di strumenti adeguati per ottenere l'accesso alle prove elettroniche in modo efficiente, al fine di garantire che possano combattere efficacemente la criminalità online.

In secondo luogo, il protocollo garantirà che tali misure volte a ottenere l'accesso alle prove elettroniche siano impiegate in modo da consentire agli Stati membri di rispettare i diritti fondamentali, compresi i diritti processuali in materia penale, il diritto alla riservatezza e il diritto alla protezione dei dati personali. In assenza di norme chiare a livello internazionale, le pratiche esistenti possono porre sfide in termini di certezza del diritto, trasparenza, responsabilità e rispetto dei diritti fondamentali e delle garanzie processuali degli indagati nelle indagini penali.

In terzo luogo, il protocollo potrà risolvere e prevenire i conflitti di legge, che interessano sia le autorità sia i prestatori di servizi del settore privato e altri soggetti, prevedendo norme compatibili a livello internazionale per l'accesso transfrontaliero alle prove elettroniche.

In quarto luogo, il protocollo dimostrerà che la Convenzione rimane importante quale principale quadro multilaterale nella lotta contro la criminalità informatica. Ciò sarà cruciale nel processo successivo alla risoluzione 74/247 dell'Assemblea generale delle Nazioni Unite, del dicembre 2019, sul contrasto all'uso delle tecnologie dell'informazione e della comunicazione a fini criminali, che ha istituito un comitato intergovernativo aperto di esperti ad hoc incaricato di elaborare una convenzione internazionale globale sulla lotta contro l'uso delle tecnologie dell'informazione e della comunicazione a fini criminali.

---

regolamento (UE) 2017/1939, gli Stati membri che partecipano alla cooperazione rafforzata sull'istituzione della Procura europea ("EPPO") includono l'EPPO nella comunicazione.

[40] Che consente alle Parti di comunicare l'autorità o le autorità che dovrebbero, rispettivamente, essere informate in caso di incidente di sicurezza o contattate per chiedere l'autorizzazione preventiva in caso di trasferimenti successivi verso un altro Stato o un'altra organizzazione internazionale.

[41] Cfr. la nota 24.

3. BASE GIURIDICA, SUSSIDIARIETÀ E PROPORZIONALITÀ

- *Base giuridica*

La competenza dell'Unione a legiferare in materia di facilitazione della cooperazione tra autorità giudiziarie o autorità omologhe in relazione all'azione penale e all'esecuzione di decisioni si basa sull'articolo 82, paragrafo 1, TFUE. La competenza dell'Unione in materia di protezione dei dati di carattere personale si basa sull'articolo 16 TFUE.

A norma dell'articolo 3, paragrafo 2, TFUE, l'Unione ha competenza esclusiva per la conclusione di accordi internazionali allorché tale conclusione può incidere su norme comuni dell'UE o modificarne la portata. Le disposizioni del protocollo rientrano in un settore disciplinato in larga misura da norme comuni, come illustrato nella sezione 2.3.

Il protocollo rientra pertanto nella competenza esterna esclusiva dell'Unione. Gli Stati membri possono quindi firmare il protocollo, nell'interesse dell'Unione, sulla base dell'articolo 16, dell'articolo 82, paragrafo 1, e dell'articolo 218, paragrafo 5, TFUE.

- *Sussidiarietà (per la competenza non esclusiva)*

Non pertinente.

- *Proporzionalità*

Gli obiettivi dell'Unione in relazione alla presente proposta, quali delineati alla sezione 2.5, possono essere conseguiti solo mediante la stipulazione di un accordo internazionale vincolante che preveda le necessarie misure di cooperazione e garantisca nel contempo un'adeguata tutela dei diritti fondamentali. Il protocollo realizza tale obiettivo. Le disposizioni del protocollo si limitano a quanto necessario per conseguire i suoi obiettivi principali. L'azione unilaterale non costituisce un'alternativa in quanto non fornirebbe una base sufficiente per la cooperazione con i paesi terzi e non potrebbe garantire la necessaria tutela dei diritti fondamentali. Inoltre, l'adesione a un accordo multilaterale come il protocollo, che l'Unione ha potuto negoziare, è più efficiente che l'avvio di negoziati con singoli paesi terzi a livello bilaterale. Nell'ipotesi che tutte le 66 Parti della Convenzione e le future nuove Parti ratifichino il protocollo, questo fornirà un quadro giuridico comune per la cooperazione degli Stati membri dell'UE con i loro principali partner internazionali nella lotta contro la criminalità.

- ***Scelta dello strumento***

Non pertinente.

4. RISULTATI DELLE VALUTAZIONI EX POST, DELLE CONSULTAZIONI DEI PORTATORI DI INTERESSI E DELLE VALUTAZIONI D'IMPATTO

- *Valutazioni ex post/Vaglio di adeguatezza della legislazione vigente*

Non pertinente.

- *Consultazioni dei portatori di interessi*

Il Consiglio d'Europa ha organizzato sei cicli di consultazioni pubbliche in relazione ai negoziati sul protocollo, nei mesi di luglio e novembre 2018, febbraio e novembre 2019,

dicembre 2020 e maggio 2021.[42] Le Parti hanno preso in esame i contributi ricevuti nell'ambito di tali consultazioni.

La Commissione, nel suo ruolo di negoziatore a nome dell'Unione, ha inoltre proceduto a uno scambio di opinioni con le autorità preposte alla protezione dei dati e ha organizzato, nel corso del 2019 e del 2021, riunioni di consultazione mirate con le organizzazioni della società civile, i prestatori di servizi e le associazioni di categoria. La Commissione ha tenuto conto dei contributi ricevuti grazie a tali scambi.

- *Assunzione e uso di perizie*

Nel corso dei negoziati la Commissione ha consultato costantemente il comitato speciale del Consiglio per i negoziati, in linea con la decisione del Consiglio dell'Unione europea, del 6 giugno 2019, che autorizza la Commissione a partecipare, a nome dell'Unione europea, ai negoziati sul protocollo, il che ha offerto agli esperti degli Stati membri l'opportunità di contribuire al processo di formulazione della posizione dell'Unione. Vari esperti degli Stati membri hanno inoltre continuato a partecipare ai negoziati accanto alla Commissione, che vi ha partecipato a nome dell'Unione. Sono stati inoltre consultati i portatori di interessi (cfr. sopra).

- *Valutazione d'impatto*

Durante il periodo 2017-2018 è stata effettuata una valutazione d'impatto a corredo delle proposte della Commissione in materia di prove elettroniche.[43] In tale contesto, la negoziazione di un accordo su un secondo protocollo addizionale alla Convenzione di Budapest sulla criminalità informatica faceva parte dell'opzione favorita. I relativi impatti sono inoltre illustrati nella presente relazione.

- *Efficienza normativa e semplificazione*

Il protocollo può avere implicazioni per talune categorie di prestatori di servizi, tra cui le piccole e medie imprese (PMI), che possono essere oggetto di richieste e ordini di prove elettroniche in virtù del protocollo. Tali prestatori di servizi, tuttavia, sono spesso già adesso oggetto di simili richieste attraverso altri canali esistenti, talvolta tramite autorità diverse, anche sulla base della Convenzione[44], di altri trattati di mutua assistenza giudiziaria o di altri quadri legislativi, tra cui le politiche sulla governance multipartecipativa di Internet.[45] Inoltre i prestatori di servizi, comprese le PMI, beneficeranno di un quadro giuridico chiaro a livello internazionale e di un approccio comune a tutte le Parti del protocollo.

- *Diritti fondamentali*

Gli strumenti di cooperazione previsti dal protocollo rischiano di incidere negativamente sui diritti fondamentali, tra cui, ad esempio, il diritto a un processo equo, alla riservatezza e alla protezione dei dati personali, laddove i dati di una persona possono essere ottenuti nell'ambito di un procedimento penale. Il protocollo segue un approccio basato sui diritti e prevede

---

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations

[43] SWD(2018) 118 final.

[44] Cfr. ad esempio la nota di orientamento n. 10 del Comitato della Convenzione sulla criminalità informatica, sugli ordini di produzione di informazioni relative agli abbonati (articolo 18 della Convenzione di Budapest), del 1º marzo 2017.

[45] Cfr. ad esempio la risoluzione del comitato direttivo dell'ICANN (Internet Corporation for Assigned Names and Numbers), del 15 maggio 2019, relativa alle raccomandazioni sulla specifica temporanea per i dati di registrazione gTLD (domini di primo livello generici), disponibile all'indirizzo www.icann.org.

condizioni e garanzie in linea con gli strumenti internazionali in materia di diritti umani, compresa la Convenzione del Consiglio d'Europa per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (1950). In particolare, il protocollo prevede garanzie specifiche in materia di protezione dei dati. Ove necessario, il protocollo fornisce inoltre alle Parti una base per formulare talune riserve, dichiarazioni o notifiche e prevede motivi validi per rifiutare la cooperazione in risposta a una richiesta in situazioni specifiche. Ciò garantisce la compatibilità del protocollo con la Carta dei diritti fondamentali dell'Unione europea.

5. INCIDENZA SUL BILANCIO

La presente proposta non ha alcuna incidenza sul bilancio dell'Unione. Gli Stati membri possono sostenere costi una tantum per l'attuazione del protocollo e potrebbero esservi costi più elevati per le autorità degli Stati membri a causa dell'aumento previsto del numero di casi.

6. ALTRI ELEMENTI

- *Piani di attuazione e modalità di monitoraggio, valutazione e rendicontazione*

Non esiste alcun piano di attuazione in quanto, dopo la firma e la ratifica del protocollo, gli Stati membri saranno tenuti ad attuarlo.

Per quanto riguarda il monitoraggio, la Commissione parteciperà alle riunioni del Comitato della Convenzione sulla criminalità informatica, in cui l'Unione europea è riconosciuta come organizzazione con funzione di osservatore.

2021/0382 (NLE)

Proposta di

DECISIONE DEL CONSIGLIO

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

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 16, l'articolo 82, paragrafo 1, e l'articolo 218, paragrafo 5,

vista la proposta della Commissione europea,

considerando quanto segue:

(1) Il 9 giugno 2019 il Consiglio ha autorizzato la Commissione a partecipare, a nome dell'Unione, ai negoziati sul secondo protocollo addizionale alla Convenzione del Consiglio d'Europa sulla criminalità informatica (Convenzione di Budapest).

(2) Il testo del secondo protocollo addizionale alla Convenzione sulla criminalità informatica riguardante la cooperazione rafforzata e la divulgazione di prove elettroniche ("il protocollo") è stato adottato dal Comitato dei Ministri del Consiglio d'Europa il 17 novembre 2021 e dovrebbe essere aperto alla firma nel marzo 2022.

(3) Le disposizioni del protocollo rientrano in un settore disciplinato in larga misura da norme comuni ai sensi dell'articolo 3, paragrafo 2, TFUE, compresi gli strumenti che facilitano la cooperazione giudiziaria in materia penale, introducendo norme minime in materia di diritti processuali e garanzie in merito alla protezione dei dati e alla riservatezza.

(4) La Commissione ha inoltre presentato proposte legislative su un regolamento relativo agli ordini europei di produzione e di conservazione di prove elettroniche in materia penale (COM(2018) 225 final) e su una direttiva recante norme armonizzate sulla nomina di rappresentanti legali ai fini dell'acquisizione di prove nei procedimenti penali (COM(2018) 226 final), che introducono ordini europei di produzione e di conservazione vincolanti da rivolgere direttamente a un rappresentante di un prestatore di servizi in un altro Stato membro.

(5) Partecipando ai negoziati a nome dell'Unione, la Commissione ha garantito la compatibilità del secondo protocollo addizionale con le pertinenti norme comuni dell'Unione europea.

(6) Una serie di riserve, dichiarazioni, notifiche e comunicazioni è pertinente al fine di garantire la compatibilità del protocollo con il diritto e le politiche dell'Unione, nonché l'applicazione uniforme del protocollo tra gli Stati membri dell'UE nei loro rapporti con le Parti non appartenenti all'UE e l'effettiva applicazione del protocollo.

(7) Poiché il protocollo prevede procedure rapide che migliorano l'accesso transfrontaliero alle prove elettroniche e un elevato livello di garanzie, la sua entrata in vigore contribuirà alla lotta contro la criminalità informatica e altre forme di criminalità a

livello mondiale, facilitando la cooperazione tra le Parti che sono Stati membri dell'UE e i paesi terzi che sono Parti del protocollo, garantirà un elevato livello di protezione delle persone e risolverà i conflitti di legge.

(8) Poiché il protocollo prevede garanzie adeguate in linea con i requisiti per i trasferimenti internazionali di dati personali in conformità del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680, la sua entrata in vigore contribuirà a promuovere le norme dell'Unione in materia di protezione dei dati a livello globale, agevolerà i flussi di dati tra le Parti che sono Stati membri dell'UE e i paesi terzi che sono Parti del protocollo e garantirà che gli Stati membri dell'UE adempiano ai loro obblighi sanciti dalle norme dell'Unione in materia di protezione dei dati.

(9) La rapida entrata in vigore confermerà inoltre la posizione della Convenzione di Budapest del Consiglio d'Europa quale principale quadro multilaterale nella lotta contro la criminalità informatica.

(10) L'Unione europea non può diventare Parte del protocollo, in quanto sia il protocollo che la Convenzione del Consiglio d'Europa sulla criminalità informatica sono aperti esclusivamente agli Stati.

(11) Pertanto gli Stati membri dovrebbero essere autorizzati a firmare il protocollo, agendo congiuntamente nell'interesse dell'Unione europea.

(12) Gli Stati membri sono incoraggiati a firmare il protocollo durante la cerimonia di firma o il più presto possibile dopo tale data.

(13) Il Garante europeo della protezione dei dati è stato consultato a norma dell'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio e ha espresso un parere in data ...

(14) [A norma degli articoli 1 e 2 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda non partecipa all'adozione della presente decisione, non è da essa vincolata né è soggetta alla sua applicazione.]

[OPPURE:]

[A norma degli articoli 1 e 2 del protocollo n. 21 sulla posizione del Regno Unito e dell'Irlanda rispetto allo spazio di libertà, sicurezza e giustizia, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, e fatto salvo l'articolo 4 di tale protocollo, l'Irlanda ha notificato [, con lettera del...,] che desidera partecipare all'adozione e all'applicazione della presente decisione.]

(15) A norma degli articoli 1 e 2 del protocollo n. 22 sulla posizione della Danimarca, allegato al trattato sull'Unione europea e al trattato sul funzionamento dell'Unione europea, la Danimarca non partecipa all'adozione della presente decisione, non è da essa vincolata né è soggetta alla sua applicazione,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

Gli Stati membri sono autorizzati 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 ("il protocollo").

Articolo 2

All'atto della firma del protocollo, gli Stati membri formulano le riserve, dichiarazioni, notifiche o comunicazioni che figurano nell'allegato.

Articolo 3

La presente decisione entra in vigore il giorno dell'adozione.

Articolo 4

La presente decisione è pubblicata nella Gazzetta ufficiale dell'Unione europea.

Articolo 5

Gli Stati membri sono destinatari della presente decisione.

Fatto a Bruxelles, il

Per il Consiglio
Il presidente