Consiliul
Uniunii Europene

Bruxelles, 2 decembrie 2021
(OR. en)

14614/21

Dosar interinstituțional:
2021/0383(NLE)

JAI 1333
COPEN 433
CYBER 321
ENFOPOL 483
TELECOM 453
EJUSTICE 106
MI 913
DATAPROTECT 277

PROPUNERE

Sursă:	Secretara Generală a Comisiei Europene, sub semnătura dnei Martine DEPREZ, Directoare
Data primirii:	25 noiembrie 2021
Destinatar:	Dl Jeppe TRANHOLM-MIKKELSEN, Secretarul General al Consiliului Uniunii Europene
Nr. doc. Csie:	COM(2021) 719 final
Subiect:	Propunere de DECIZIE A CONSILIULUI de autorizare a statelor membre să ratifice, în interesul Uniunii Europene, cel de Al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și la divulgarea probelor electronice

În anexă, se pune la dispoziția delegațiilor documentul COM(2021) 719 final.

Anexă: COM(2021) 719 final

COMISIA
EUROPEANĂ

Bruxelles, 25.11.2021
COM(2021) 719 final

2021/0383 (NLE)

Propunere de

DECIZIE A CONSILIULUI

de autorizare a statelor membre să ratifice, în interesul Uniunii Europene, cel de Al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și la divulgarea probelor electronice

EXPUNERE DE MOTIVE

1. OBIECTUL PROPUNERII

Prezenta propunere se referă la decizia de autorizare a statelor membre să ratifice, în interesul Uniunii Europene, cel de Al doilea protocol adițional referitor la cooperarea consolidată și la divulgarea probelor electronice la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică („protocolul”)[1]. Scopul protocolului este de a oferi norme comune la nivel internațional în scopul de a consolida cooperarea în materie de criminalitate informatică și colectarea de probe în format electronic pentru anchetele sau procedurile penale.

Prezenta propunere completează o propunere separată a Comisiei de decizie a Consiliului Uniunii Europene („Consiliul”) de autorizare a statelor membre să semneze protocolul în interesul Uniunii Europene.

Criminalitatea informatică reprezintă în continuare o provocare considerabilă pentru societatea noastră. În pofida eforturilor autorităților de aplicare a legii și ale autorităților judiciare, atacurile cibernetice, inclusiv atacurile de tip ransomware, sunt în creștere și devin din ce în ce mai complexe[2]. În special, având în vedere faptul că internetul nu cunoaște frontiere, anchetele privind criminalitatea informatică au aproape întotdeauna un caracter transfrontalier, necesitând astfel o cooperare strânsă între autoritățile din diferite țări.

Probele electronice sunt din ce în ce mai importante în cadrul anchetelor penale. Comisia estimează că, în prezent, autoritățile de aplicare a legii și autoritățile judiciare au nevoie de acces la probe electronice în 85 % din anchetele penale, inclusiv în cele legate de criminalitatea informatică[3]. Probele privind orice infracțiune sunt deținute din ce în ce mai mult în format electronic de către prestatori de servicii din jurisdicții străine, iar un răspuns eficace în materie de justiție penală necesită măsuri adecvate pentru a obține astfel de probe în vederea respectării statului de drept.

Se depun eforturi de îmbunătățire a accesului transfrontalier la probele electronice pentru anchetele penale în întreaga lume, la nivel național, la nivelul Uniunii Europene[4] și la nivel internațional, inclusiv prin intermediul protocolului. Este important să se asigure norme compatibile la nivel internațional pentru a se evita conflictele de legi atunci când se solicită accesul transfrontalier la probele electronice.

2. CONTEXTUL PROPUNERII

2.1. Context

Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică (CETS nr. 185) („convenția”) urmărește facilitarea combaterii infracțiunilor săvârșite prin utilizarea rețelelor informatice. Aceasta (1) conține dispoziții de armonizare a elementelor de drept penal material național ale infracțiunilor și dispozițiilor conexe în domeniul criminalității informatice, (2) prevede competențe procedurale penale naționale necesare pentru

[1] Textul protocolului este inclus ca anexă la prezenta propunere.

[2] Evaluarea amenințării pe care o reprezintă formele grave de criminalitate și criminalitatea organizată în Uniunea Europeană în 2021 (SOCTA UE 2021).

[3] SWD(2018) 118 final.

[4] COM(2018) 225 și 226 final.

investigarea și urmărirea penală a unor astfel de infracțiuni, precum și a altor infracțiuni comise prin intermediul unui sistem informatic sau în cazul cărora probele sunt în format electronic și (3) vizează instituirea unui regim rapid și eficace de cooperare internațională.

Convenția este deschisă statelor membre ale Consiliului Europei și statelor care nu sunt membre ale acestuia, la invitația Consiliului. În prezent, 66 de țări sunt părți la convenție, inclusiv 26 de state membre ale Uniunii Europene[5]. Convenția nu prevede posibilitatea Uniunii Europene de a adera la aceasta. Totuși, Uniunea Europeană este recunoscută ca organizație cu statut de observator în cadrul Comitetului Convenției privind criminalitatea informatică (T-CY)[6].

În pofida eforturilor de negociere a unei noi convenții privind criminalitatea informatică la nivelul Organizației Națiunilor Unite[7], Convenția de la Budapesta rămâne principala convenție multilaterală pentru combaterea criminalității informatice. Uniunea sprijină în mod constant convenția[8], inclusiv în cadrul finanțării programelor de consolidare a capacităților[9].

În urma propunerilor Grupului privind probele stocate în cloud (*Cloud Evidence Group*)[10], Comitetul Convenției privind criminalitatea informatică a adoptat o serie de recomandări pentru a aborda, inclusiv prin negocierea unui al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea internațională consolidată, provocarea reprezentată de faptul că probele electronice referitoare la criminalitatea informatică și la alte infracțiuni sunt deținute din ce în ce mai mult de prestatori de servicii din jurisdicții străine, în timp ce competențele în materie de aplicare a legii rămân limitate de frontierele teritoriale. În iunie 2017, Comitetul Convenției privind criminalitatea informatică a aprobat mandatul pentru elaborarea celui de Al doilea protocol adițional în perioada septembrie 2017-decembrie 2019[11]. Având în vedere nevoia de a avea mai mult timp la dispoziție pentru finalizarea discuțiilor, precum și limitările impuse de pandemia de COVID-19 în 2020 și 2021, Comitetul Convenției privind criminalitatea informatică a prelungit ulterior mandatul de două ori, până în decembrie 2020 și, respectiv, până în mai 2021.

În urma apelului lansat de Consiliul European în concluziile sale din 18 octombrie 2018[12], Comisia a adoptat, la 5 februarie 2019, o recomandare de decizie a Consiliului de autorizare a Comisiei să participe, în numele Uniunii Europene, la negocierile privind un al doilea protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică[13]. La 2

---

5 Toate statele membre, cu excepția Irlandei, care a semnat convenția, dar nu a ratificat-o, angajându-se totuși să continue procesul de aderare.

6 Regulamentul de procedură al Comitetului Convenției privind criminalitatea informatică [T-CY (2013) 25 rev], disponibil la adresa: www.coe.int/cybercrime.

7 Rezoluția 74/247 a Adunării Generale a Organizației Națiunilor Unite (Adunarea Generală a ONU) din decembrie 2019, intitulată „Combaterea utilizării tehnologiilor informației și comunicațiilor în scopuri infracționale”.

8 JOIN(2020) 81 final.

9 A se vedea, de exemplu, Acțiunea mondială extinsă împotriva criminalității informaționale (GLACY +), la adresa: https://www.coe.int/en/web/cybercrime/glacyplus.

10 Raportul final al Grupului privind probele stocate în cloud din cadrul Comitetului Convenției privind criminalitatea informatică intitulat „Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY” (Accesul în cadrul procedurilor de justiție penală la probele electronice stocate în cloud: recomandări de avut în vedere de către T-CY) din 16 septembrie 2016.

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

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

13 COM(2019) 71 final.

aprilie 2019, Autoritatea Europeană pentru Protecția Datelor a adoptat un aviz cu privire la recomandare[14]. Prin decizia din 6 iunie 2019, Consiliul Uniunii Europene a autorizat Comisia să participe, în numele Uniunii Europene, la negocierile privind cel de Al doilea protocol adițional[15].

Astfel cum se menționează în Strategia UE din 2020 privind o uniune a securității[16], în Strategia de securitate cibernetică a UE din 2020 pentru deceniul digital[17] și în Strategia UE din 2021 privind criminalitatea organizată[18], Comisia s-a angajat să încheie rapid și cu succes negocierile privind protocolul. În Rezoluția sa din 2021 referitoare la Strategia de securitate cibernetică a UE pentru deceniul digital[19], Parlamentul European a recunoscut, de asemenea, necesitatea de a încheia lucrările privind protocolul.

Comisia a participat, în numele Uniunii Europene, la negocierile privind protocolul în conformitate cu decizia Consiliului Uniunii Europene. Comisia a consultat în mod constant comitetul special al Consiliului pentru negocierile privind poziția Uniunii.

În conformitate cu Acordul-cadru privind relațiile dintre Parlamentul European și Comisia Europeană[20], Comisia a informat, de asemenea, Parlamentul European cu privire la negocieri prin intermediul unor rapoarte scrise și prezentări orale.

În cadrul reuniunii sale plenare din 28 mai 2021, Comitetul Convenției privind criminalitatea informatică a aprobat proiectul de protocol la nivelul său și l-a transmis spre adoptare Comitetului de Miniștri al Consiliului Europei[21]. La 17 noiembrie 2021, Comitetul de Miniștri al Consiliului Europei a adoptat protocolul.

2.2. Al doilea protocol adițional

Obiectivul protocolului este de a consolida cooperarea în materie de criminalitate informatică și colectarea de probe în format electronic privind infracțiuni în scopul unor anchete sau proceduri penale specifice. Protocolul recunoaște necesitatea unei cooperări sporite și mai eficiente între state și cu sectorul privat, precum și a unei mai mari clarități și securități juridice pentru prestatorii de servicii și alte entități în ceea ce privește circumstanțele în care pot răspunde cererilor din partea autorităților judiciare penale ale altor părți privind divulgarea de probe electronice.

Protocolul recunoaște, de asemenea, că o cooperare transfrontalieră eficace în scopul justiției penale, inclusiv între autoritățile din sectorul public și entitățile din sectorul privat, necesită condiții eficace și garanții solide pentru protecția drepturilor fundamentale. În acest scop, protocolul adoptă o abordare bazată pe drepturi și prevede condiții și garanții în conformitate cu instrumentele internaționale privind drepturile omului, inclusiv Convenția Consiliului Europei din 1950 pentru apărarea drepturilor omului și a libertăților fundamentale. Întrucât

[14] Avizul AEPD nr. 3/2019 din 2 aprilie 2019 privind participarea la negocieri în vederea adoptării unui al doilea protocol adițional la Convenția de la Budapesta privind criminalitatea informatică.
[15] Decizia Consiliului cu numărul de referință 9116/19.
[16] COM(2020) 605 final.
[17] JOIN(2020) 81 final.
[18] COM(2021) 170 final.
[19] Rezoluția Parlamentului European din 10 iunie 2021 referitoare la Strategia de securitate cibernetică a UE pentru deceniul digital.
[20] JO L 304, 20.11.2010, p. 47.
[21] https://rm.coe.int/0900001680a2aa42

probele electronice se referă adesea la date cu caracter personal, protocolul include, de asemenea, garanții solide pentru protecția vieții private și a datelor cu caracter personal.

Dispozițiile menționate în paragrafele următoare prezintă o importanță deosebită pentru protocol. Protocolul este însoțit de un raport explicativ detaliat. Deși raportul explicativ nu constituie un instrument care să ofere o interpretare cu valoare de autoritate a protocolului, acesta este menit „să ghideze și să asiste părțile” în aplicarea protocolului[22].

2.2.1. Dispoziții comune

Capitolul I din protocol prevede dispozițiile comune. Articolul 2 stabilește domeniul de aplicare al protocolului, în conformitate cu domeniul de aplicare al convenției: acesta se aplică în cazul anchetelor sau al procedurilor penale specifice referitoare la infracțiunile legate de sisteme informatice și de date, precum și în cazul colectării de probe în format electronic privind infracțiuni.

Articolul 3 include definiții ale „autorităților centrale”, „autorităților competente”, „situațiilor de urgență”, „datelor cu caracter personal” și „părții care efectuează transferul”. Aceste definiții se aplică protocolului, împreună cu definițiile incluse în convenție.

Articolul 4 stabilește limbile în care părțile ar trebui să transmită ordine, cereri sau notificări în temeiul protocolului.

2.2.2. Măsuri de cooperare

Capitolul II din protocol prevede măsuri de consolidare a cooperării. În primul rând, articolul 5 alineatul (1) stabilește că părțile cooperează pe baza protocolului în cea mai mare măsură posibilă. La articolul 5 alineatele (2)-(5) se stabilește aplicarea măsurilor prevăzute în protocol în raport cu tratatele sau înțelegerile existente în materie de asistență reciprocă. Articolul 5 alineatul (7) prevede că măsurile de la capitolul II nu restricționează cooperarea dintre părți sau cu prestatorii de servicii sau entitățile, prin intermediul altor acorduri, înțelegeri și practici aplicabile sau al dreptului intern aplicabil.

Articolul 6 oferă o bază pentru cooperarea directă dintre autoritățile competente ale unei părți și entitățile unei alte părți care prestează servicii de înregistrare a numelor de domenii, pentru divulgarea datelor de înregistrare a numelor de domenii.

Articolul 7 oferă o bază pentru cooperarea directă dintre autoritățile competente ale unei părți și prestatorii de servicii ai unei alte părți pentru divulgarea datelor privind abonații.

Articolul 8 oferă o bază pentru o cooperare consolidată între autorități în ceea ce privește divulgarea datelor informatice.

Articolul 9 oferă o bază pentru cooperarea dintre autorități în ceea ce privește divulgarea datelor informatice în situații de urgență.

Articolul 10 oferă o bază pentru asistența judiciară reciprocă în situații de urgență.

Articolul 11 oferă o bază pentru cooperarea prin videoconferință.

[22] A se vedea punctul 2 din raportul explicativ privind protocolul.

Articolul 12 oferă o bază pentru anchetele comune și pentru echipele comune de anchetă.

2.2.3. Garanții

Protocolul adoptă o abordare bazată pe drepturi, cu condiții și garanții specifice, dintre care unele sunt încorporate în măsurile specifice de cooperare, precum și în capitolul III din protocol. Articolul 13 din protocol impune părților să se asigure că respectivele competențe și proceduri fac obiectul unui nivel adecvat de protecție a drepturilor fundamentale, astfel încât, în conformitate cu articolul 15 din convenție, să se garanteze aplicarea principiului proporționalității.

Articolul 14 din protocol prevede protecția datelor cu caracter personal, astfel cum sunt definite la articolul 3 din protocol, în conformitate cu Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal (CETS 223) (Convenția 108+) și cu dreptul Uniunii.

Pe această bază, la articolul 14 alineatele (2)-(15) se stabilesc principiile fundamentale în materie de protecție a datelor, inclusiv limitarea scopului, temeiul juridic, calitatea datelor și normele aplicabile prelucrării categoriilor speciale de date, obligațiile aplicabile operatorilor, inclusiv în ceea ce privește păstrarea datelor, păstrarea evidențelor, securitatea și transferurile ulterioare, drepturile individuale exercitabile, inclusiv în ceea ce privește notificarea, accesul, rectificarea și procesul decizional automatizat, supravegherea independentă și eficace de către una sau mai multe autorități, precum și căile de atac administrative și judiciare. Garanțiile acoperă toate formele de cooperare prevăzute în protocol, cu adaptările necesare pentru a aborda caracteristicile specifice ale cooperării directe (de exemplu, în contextul notificării privind încălcarea). Exercitarea anumitor drepturi individuale poate fi întârziată, limitată sau refuzată în cazul în care acest lucru este necesar și proporțional pentru a urmări obiective importante de interes public, în special în scopul prevenirii riscului la adresa unor anchete în curs efectuate de autoritățile de aplicare a legii, ceea ce este, de asemenea, în conformitate cu dreptul Uniunii.

Articolul 14 din protocol ar trebui, de asemenea, citit în coroborare cu articolul 23 din protocol. Articolul 23 consolidează eficacitatea garanțiilor incluse în protocol, datorită prevederii conform căreia Comitetul Convenției privind criminalitatea informatică va evalua implementarea și transpunerea în practică a măsurilor luate în legislația națională în vederea punerii în aplicare a dispozițiilor protocolului. În special, la articolul 23 alineatul (3) se prevede în mod explicit faptul că punerea în aplicare de către părți a articolului 14 se evaluează de îndată ce zece părți la convenție și-au exprimat consimțământul de a-și asuma obligații în temeiul protocolului.

Ca o garanție suplimentară, în temeiul articolului 14 alineatul (15), în cazul în care o parte are dovezi substanțiale că o altă parte încalcă în mod sistematic sau semnificativ garanțiile prevăzute în protocol, aceasta poate suspenda transferul de date cu caracter personal către partea respectivă în urma consultării (ceea ce nu este necesar în caz de urgență). Toate datele cu caracter personal transferate înainte de suspendare continuă să fie tratate în conformitate cu protocolul.

În cele din urmă, având în vedere caracterul multilateral al protocolului, articolul 14 alineatul (1) literele (b) și (c) din protocol oferă părților posibilitatea ca, în cadrul relațiilor lor bilaterale, să convină, în anumite condiții, asupra unor modalități alternative de asigurare a protecției datelor cu caracter personal transferate în temeiul protocolului. În timp ce garanțiile prevăzute la articolul 14 alineatele (2)-(15) se aplică în mod implicit părților care primesc date

cu caracter personal, în temeiul articolului 14 alineatul (1) litera (b), părțile care au obligații reciproce în baza unui acord internațional de instituire a unui cadru cuprinzător pentru protecția datelor cu caracter personal în conformitate cu cerințele aplicabile ale legislației părților în cauză se pot baza, de asemenea, pe cadrul respectiv. Această dispoziție se referă, de exemplu, la Convenția 108+ (pentru părțile care permit transferurile de date către alte părți în temeiul convenției menționate) sau la Acordul-cadru UE-SUA (în cadrul domeniului său de aplicare, și anume pentru transferul de date cu caracter personal între autorități și, în combinație cu o înțelegere specifică în materie de transfer între SUA și UE, pentru cooperarea directă dintre autorități și prestatorii de servicii). În plus, în temeiul articolului 14 alineatul (1) litera (c), părțile pot, de asemenea, să stabilească de comun acord că transferul de date cu caracter personal are loc pe baza altor acorduri sau înțelegeri încheiate între părțile în cauză. Pentru statele membre ale UE, astfel de acorduri sau de înțelegeri alternative pot fi invocate pentru transferurile de date în temeiul protocolului numai dacă aceste transferuri respectă cerințele legislației Uniunii în materie de protecție a datelor, și anume capitolul V din Directiva (UE) 2016/680 (Directiva privind protecția datelor în materie de asigurare a respectării legii) și (în ceea ce privește cooperarea directă dintre autorități și prestatorii de servicii în temeiul articolelor 6 și 7 din protocol) capitolul V din Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor).

2.2.4. Dispoziții finale

Capitolul I din protocol prevede dispozițiile finale. Printre altele, articolul 15 alineatul (1) litera (a) garantează că părțile pot stabili în alt mod relațiile dintre ele cu privire la aspectele prevăzute în protocol, în conformitate cu articolul 39 alineatul (2) din convenție. Articolul 15 alineatul (1) litera (b) garantează că statele membre ale UE care sunt părți la protocol pot continua să aplice dreptul Uniunii în relațiile lor reciproce. Articolul 15 alineatul (2) stabilește, de asemenea, că articolul 39 alineatul (3) din convenție se aplică protocolului.

Articolul 16 alineatul (3) indică faptul că protocolul va intra în vigoare de îndată ce cinci părți la convenție și-au exprimat consimțământul de a-și asuma obligații în temeiul protocolului.

Articolul 19 alineatul (1) prevede că părțile pot recurge la rezerve în ceea ce privește articolul 7 alineatul (9) literele (a) și (b), articolul 8 alineatul (13) și articolul 17. Articolul 19 alineatul (2) prevede că părțile pot face declarațiile menționate la articolul 7 alineatul (2) litera (b) și alineatul (8), articolul 8 alineatul (11), articolul 9 alineatul (1) litera (b), articolul 9 alineatul (5), articolul 10 alineatul (9), articolul 12 alineatul (3) și articolul 18 alineatul (2). Articolul 19 alineatul (3) stabilește că o parte face declarațiile, notificările sau comunicările identificate la articolul 7 alineatul (5) literele (a) și (e), articolul 8 alineatul (4), articolul (8) alineatul (10) literele (a) și (b), articolul 14 alineatul (7) litera (c), articolul 14 alineatul (10) litera (b) și articolul 17 alineatul (2).

Articolul 23 alineatul (1) oferă o bază pentru consultări între părți, inclusiv prin intermediul Comitetului Convenției privind criminalitatea informatică, în conformitate cu articolul 46 din convenție. Articolul 23 alineatul (2) oferă, de asemenea, o bază pentru evaluarea utilizării și punerii în aplicare a dispozițiilor protocolului. Articolul 23 alineatul (3) garantează că evaluarea utilizării și a punerii în aplicare a articolului 14 privind protecția datelor începe de îndată ce zece părți și-au exprimat consimțământul de a-și asuma obligații în temeiul protocolului.

2.3. Dreptul și politica Uniunii în domeniu

Domeniul vizat de protocol este reglementat în mare parte de norme comune întemeiate pe articolul 82 alineatul (1) și pe articolul 16 din TFUE. Cadrul juridic actual al Uniunii Europene include în special instrumente privind aplicarea legii și cooperarea judiciară în materie penală, cum ar fi Directiva 2014/41/UE privind ordinul european de anchetă în materie penală, Convenția cu privire la asistența judiciară reciprocă în materie penală între statele membre ale Uniunii Europene și Decizia-cadru 2002/465/JAI a Consiliului privind echipele comune de anchetă. Pe plan extern, Uniunea Europeană a încheiat o serie de acorduri bilaterale între Uniune și țări terțe, cum ar fi acordurile privind asistența judiciară reciprocă între Uniunea Europeană și Statele Unite ale Americii, între Uniunea Europeană și Japonia și între Uniunea Europeană și Norvegia și Islanda. Cadrul juridic actual al Uniunii Europene include, de asemenea, Regulamentul (UE) 2017/1939 al Consiliului de punere în aplicare a unei forme de cooperare consolidată în ceea ce privește instituirea Parchetului European (EPPO). Statele membre care participă la cooperarea consolidată ar trebui să se asigure că EPPO poate, în exercitarea competențelor sale, astfel cum se prevede la articolele 22, 23 și 25 din Regulamentul (UE) 2017/1939, să solicite cooperarea în temeiul protocolului în același mod ca și procurorii naționali ai statelor membre respective. Aceste instrumente și acorduri se referă în special la articolele 8, 9, 10, 11 și 12 din protocol.

În plus, Uniunea a adoptat mai multe directive care consolidează drepturile procedurale ale persoanelor suspectate și ale celor acuzate[23]. Aceste instrumente se referă în special la articolele 6, 7, 8, 9, 10, 11, 12 și 13 din protocol. Un set special de garanții se referă la protecția datelor cu caracter personal, care este un drept fundamental consacrat în tratatele UE și în Carta drepturilor fundamentale a Uniunii Europene. Datele cu caracter personal pot fi prelucrate numai în conformitate cu Regulamentul (UE) 2016/679 (Regulamentul general privind protecția datelor) și cu Directiva (UE) 2016/680 (Directiva privind protecția datelor în materie de asigurare a respectării legii). Dreptul fundamental al oricărei persoane la respectarea vieții private și de familie, a domiciliului și a secretului comunicațiilor include respectarea caracterului privat al comunicațiilor ca element esențial. Datele transmise în cadrul comunicațiilor electronice pot fi prelucrate numai în conformitate cu Directiva 2002/58/CE (Directiva asupra confidențialității și comunicațiilor electronice). Aceste instrumente se referă în special la articolul 14 din protocol.

[23] Directiva 2010/64/UE a Parlamentului European și a Consiliului din 20 octombrie 2010 privind dreptul la interpretare și traducere în cadrul procedurilor penale, JO L 280, 26.10.2010, p. 1; Directiva 2012/13/UE a Parlamentului European și a Consiliului din 22 mai 2012 privind dreptul la informare în cadrul procedurilor penale, JO L 142, 1.6.2012, p. 1; Directiva 2013/48/UE a Parlamentului European și a Consiliului din 22 octombrie 2013 privind dreptul de a avea acces la un avocat în cadrul procedurilor penale și al procedurilor privind mandatul european de arestare, precum și dreptul ca o persoană terță să fie informată în urma privării de libertate și dreptul de a comunica cu persoane terțe și cu autorități consulare în timpul privării de libertate, JO L 294, 6.11.2013, p. 1; Directiva (UE) 2016/1919 a Parlamentului European și a Consiliului din 26 octombrie 2016 privind asistența juridică gratuită pentru persoanele suspectate și persoanele acuzate în cadrul procedurilor penale și pentru persoanele căutate în cadrul procedurilor privind mandatul european de arestare, JO L 297, 4.11.2016, p. 1; Directiva (UE) 2016/800 a Parlamentului European și a Consiliului din 11 mai 2016 privind garanțiile procedurale pentru copiii care sunt persoane suspectate sau acuzate în cadrul procedurilor penale, JO L 132, 21.5.2016, p. 1; Directiva (UE) 2016/343 a Parlamentului European și a Consiliului din 9 martie 2016 privind consolidarea anumitor aspecte ale prezumției de nevinovăție și a dreptului de a fi prezent la proces în cadrul procedurilor penale, JO L 65, 11.3.2016, p. 1; Directiva 2012/13/UE a Parlamentului European și a Consiliului din 22 mai 2012 privind dreptul la informare în cadrul procedurilor penale.

La articolul 14 alineatele (2)-(15) din protocol sunt prevăzute garanții adecvate privind protecția datelor în sensul normelor Uniunii privind protecția datelor, în special al articolului 46 din Regulamentul general privind protecția datelor și al articolului 37 din Directiva privind protecția datelor în materie de asigurare a respectării legii, precum și al jurisprudenței relevante a Curții Europene de Justiție. În conformitate cu cerințele dreptului Uniunii[24] și pentru a garanta eficacitatea garanțiilor prevăzute la articolul 14 din protocol, statele membre ar trebui să asigure notificarea persoanelor fizice ale căror date au fost transferate, sub rezerva anumitor restricții, de exemplu pentru a se evita punerea în pericol a anchetelor în curs. Articolul 14 alineatul (11) litera (c) din protocol oferă statelor membre o bază pentru îndeplinirea acestei cerințe.

Compatibilitatea articolului 14 alineatul (1) din protocol cu normele Uniunii în materie de protecție a datelor impune, de asemenea, statelor membre să ia în considerare următoarele aspecte în ceea ce privește posibilele modalități alternative de a asigura protecția adecvată a datelor cu caracter personal transferate în temeiul protocolului. În ceea ce privește alte acorduri internaționale de stabilire a unui cadru cuprinzător pentru protecția datelor cu caracter personal în conformitate cu cerințele aplicabile ale legislației părților în cauză, în temeiul articolului 14 alineatul (1) litera (b), statele membre ar trebui să țină seama de faptul că, în scopul cooperării directe, Acordul-cadru UE-SUA trebuie să fie completat cu garanții suplimentare – care urmează să fie prevăzute într-o înțelegere specifică în materie de transfer între SUA și UE/statele sale membre – care să țină seama de cerințele unice ale transferului de probe electronice direct de către prestatorii de servicii, mai degrabă decât între autorități[25].

De asemenea, în temeiul articolului 14 alineatul (1) litera (b) din protocol, statele membre ar trebui să aibă în vedere faptul că, pentru statele membre ale UE care sunt părți la Convenția 108+, convenția în sine nu oferă o bază adecvată pentru transferurile transfrontaliere de date în temeiul protocolului către alte părți la convenția menționată. În acest sens, respectivele state membre ar trebui să ia în considerare ultima teză de la articolul 14 alineatul (1) din Convenția 108+[26].

În cele din urmă, în ceea ce privește alte acorduri sau înțelegeri prevăzute la articolul 14 alineatul (1) litera (c), statele membre ar trebui să aibă în vedere faptul că se pot baza pe astfel de alte acorduri sau înțelegeri numai în cazul în care fie Comisia Europeană a adoptat, în

---

[24] A se vedea Curtea de Justiție (Marea Cameră), Avizul 1/15, ECLI:EU:C:2017:592, punctul 220. A se vedea, de asemenea, contribuția CEPD la consultarea referitoare la proiectul celui de Al doilea protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta), 13 noiembrie 2019, p. 6 („Autoritățile naționale competente cărora li s-a acordat accesul la date trebuie să informeze persoanele afectate, în temeiul procedurilor naționale aplicabile, de îndată ce notificarea în cauză nu mai este susceptibilă să pună în pericol anchetele desfășurate de autoritățile respective. [...] Notificarea este necesară pentru a le permite persoanelor afectate să își exercite, printre altele, dreptul la o cale de atac și drepturile în materie de protecție a datelor în ceea ce privește prelucrarea datelor care le vizează").

[25] Acesta este motivul pentru care Decizia Consiliului din 21 mai 2019 de autorizare a deschiderii negocierilor în vederea unui acord între Uniunea Europeană și Statele Unite ale Americii privind accesul transfrontalier la probele electronice în scopul cooperării judiciare în materie penală (9114/19) conține în directivele sale de negociere o serie de garanții suplimentare privind protecția datelor. În special, directivele de negociere stipulează că „Acordul ar trebui să completeze acordul-cadru cu garanții suplimentare care iau în considerare nivelul de sensibilitate al categoriilor de date în cauză și cerințele unice ale transferului de probe electronice efectuat direct de către prestatorii de servicii, mai degrabă decât la nivel de autorități, precum și ale transferurilor efectuate de autoritățile competente direct către prestatorii de servicii."

[26] A se vedea, de asemenea, Raportul explicativ privind Protocolul de modificare a Convenției pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, 10 octombrie 2018, punctele 106-107.

temeiul articolului 45 din Regulamentul general privind protecția datelor (UE) 2016/679 sau al articolului 36 din Directiva (UE) 2016/680 privind protecția datelor în materie de asigurare a respectării legii, o decizie privind caracterul adecvat al nivelului de protecție asigurat de țara terță în cauză care acoperă respectivele transferuri de date, fie în cazul în care un astfel de alt acord sau altă înțelegere asigură în sine garanții adecvate privind protecția datelor, în temeiul articolului 46 din Regulamentul general privind protecția datelor sau al articolului 37 alineatul (1) litera (a) din Directiva privind protecția datelor în materie de asigurare a respectării legii.

Trebuie să se țină seama nu numai de dreptul Uniunii în forma sa actuală din domeniul în cauză, ci și de evoluția sa viitoare, în măsura în care acest lucru este previzibil la momentul analizei. Domeniul reglementat de protocol are o relevanță directă pentru evoluțiile viitoare previzibile ale dreptului Uniunii. În acest sens, ar trebui menționate propunerile Comisiei[27] din aprilie 2018 privind accesul transfrontalier la probele electronice. Aceste instrumente se referă în special la articolele 6 și 7 din protocol.

Cu ocazia participării la negocieri în numele Uniunii, Comisia s-a asigurat că protocolul este pe deplin compatibil cu dreptul Uniunii și cu obligațiile statelor membre în temeiul acestuia. În special, Comisia s-a asigurat că dispozițiile protocolului permit statelor membre să respecte drepturile fundamentale, libertățile și principiile generale ale dreptului Uniunii, astfel cum sunt consacrate în tratatele UE și în Carta drepturilor fundamentale a UE, inclusiv proporționalitatea, drepturile procedurale, prezumția de nevinovăție și dreptul la apărare al persoanelor care fac obiectul unor proceduri penale, precum și viața privată și protecția datelor cu caracter personal și a datelor transmise în cadrul comunicațiilor electronice atunci când sunt prelucrate astfel de date, inclusiv transferurile către autoritățile de aplicare a legii din țările din afara Uniunii Europene, precum și orice obligații care le revin în acest sens autorităților de aplicare a legii și autorităților judiciare. De asemenea, Comisia a luat în considerare avizul Autorității Europene pentru Protecția Datelor[28] și avizul Comitetului european pentru protecția datelor[29].

În plus, Comisia s-a asigurat că dispozițiile protocolului și propunerile Comisiei privind probele electronice sunt compatibile, inclusiv pe măsură ce proiectul de act legislativ a evoluat în discuțiile cu colegiuitorii, și că protocolul nu generează conflicte de legi. În special, Comisia s-a asigurat că protocolul include garanții adecvate privind protecția datelor și a vieții private, care permit prestatorilor de servicii din UE să își respecte obligațiile care le revin în temeiul legislației UE privind protecția datelor și a vieții private, în măsura în care protocolul oferă un temei juridic pentru transferurile de date ca răspuns la ordinele sau cererile transmise de o autoritate a unei țări terțe care este parte la protocol prin care se solicită unui operator sau

[27] COM(2018) 225 și 226 final.

[28] Avizul AEPD nr. 3/2019 din 2 aprilie 2019 privind participarea la negocieri în vederea adoptării unui al doilea protocol adițional la Convenția de la Budapesta privind criminalitatea informatică.

[29] Inclusiv „Contribuția CEPD la consultările privind proiectul celui de al doilea protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta) din 13 noiembrie 2019”; „Declarația 02/201 privind noul proiect de dispoziții ale celui de Al doilea protocol adițional la Convenția Consiliului Europei privind criminalitatea informatică (Convenția de la Budapesta), astfel cum a fost adoptată la 2 februarie 2021”; „Contribuția CEPD la cea de a 6-a rundă de consultări privind proiectul celui de Al doilea protocol adițional la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică din 4 mai 2021”.

unei persoane împuternicite de către operator să divulge date cu caracter personal sau date transmise în cadrul comunicațiilor electronice.

2.4. Rezerve, declarații, notificări și comunicări, precum și alte considerații

Protocolul oferă o bază pentru ca părțile să recurgă la anumite rezerve și să facă declarații, notificări sau comunicări cu privire la anumite articole. Statele membre ar trebui să adopte o abordare uniformă cu privire la anumite rezerve și declarații, notificări și comunicări, astfel cum se prevede în anexa la prezenta decizie. Pentru a asigura compatibilitatea punerii în aplicare a protocolului cu dreptul Uniunii, statele membre ale UE ar trebui să adopte poziția prezentată mai jos cu privire la rezervele și declarațiile respective. În cazul în care protocolul oferă o bază pentru alte rezerve, declarații, notificări sau comunicări, prezenta propunere autorizează statele membre să ia în considerare și să își formuleze propriile rezerve, declarații, notificări sau comunicări.

Pentru a asigura compatibilitatea dintre dispozițiile protocolului și legislația și politicile relevante ale Uniunii, statele membre nu ar trebui să recurgă la rezervele prevăzute la articolul 7 alineatul (9) literele (a)[30] și (b)[31]. În plus, statele membre ar trebui să facă declarația prevăzută la articolul 7 alineatul (2) litera (b)[32] și notificarea prevăzută la articolul 7 alineatul (5) litera (a)[33]. Lipsa acestor rezerve, precum și prezentarea declarației și a notificării sunt importante pentru a asigura compatibilitatea protocolului cu propunerile legislative ale Comisiei privind probele electronice, inclusiv pe măsură ce proiectele legislative evoluează în discuțiile cu colegiuitorii.

În plus, pentru a se asigura o aplicare uniformă a protocolului de către statele membre ale UE în cadrul cooperării lor cu părțile care nu sunt state membre ale UE, statele membre sunt încurajate să nu recurgă la rezerva prevăzută la articolul 8 alineatul (13)[34], inclusiv pentru că o astfel de rezervă ar avea un efect reciproc[35]. Statele membre ar trebui să facă declarația prevăzută la articolul 8 alineatul (4) pentru a se asigura că ordinele pot fi puse în aplicare în cazul în care sunt necesare informații justificative suplimentare, de exemplu cu privire la circumstanțele cazului în cauză, pentru a evalua proporționalitatea și necesitatea[36].

---

[30] Care oferă părților posibilitatea de a-și rezerva dreptul de a nu aplica articolul 7 (divulgarea datelor privind abonații).

[31] Care oferă părților posibilitatea de a-și rezerva dreptul de a nu aplica articolul 7 (divulgarea datelor privind abonații) în cazul anumitor tipuri de numere de acces dacă acest lucru ar fi incompatibil cu principiile fundamentale ale sistemului lor juridic național.

[32] Care oferă părților posibilitatea de a declara că ordinul prevăzut la articolul 7 alineatul (1) (divulgarea datelor privind abonații) trebuie emis de un procuror sau de o altă autoritate judiciară sau sub supravegherea acestora sau, în caz contrar, trebuie să fie emis sub supraveghere independentă.

[33] Care oferă părților posibilitatea de a notifica Secretarului General al Consiliului Europei faptul că, atunci când se emite, în temeiul articolului 7 alineatul (1) (divulgarea datelor privind abonații), un ordin adresat unui prestator de servicii care își desfășoară activitatea pe teritoriul lor, părțile solicită, în fiecare caz sau în circumstanțe identificate, notificarea simultană a ordinului, a informațiilor suplimentare și a unui rezumat al faptelor legate de anchetă sau de procedură.

[34] Care oferă părților posibilitatea de a-și rezerva dreptul de a nu aplica articolul 8 (punerea în aplicare a ordinelor emise de o altă parte) în cazul datelor privind traficul.

[35] A se vedea punctul 147 din raportul explicativ privind protocolul, care stabilește că „[o] parte care își rezervă dreptul de a nu aplica prezentul articol nu este autorizată să transmită altor părți ordine legate de datele privind traficul prevăzute la [articolul 8] alineatul (1)”.

[36] Care oferă părților posibilitatea de a declara că sunt necesare informații justificative suplimentare pentru punerea în aplicare a ordinelor prevăzute la articolul 8 alineatul (1) (punerea în aplicare a ordinelor emise de o altă parte).

De asemenea, statele membre sunt încurajate să nu facă declarația prevăzută la articolul 9 alineatul (1) litera (b)[37], pentru a asigura o aplicare eficientă a protocolului.

Statele membre ar trebui să efectueze comunicările prevăzute la articolul 7 alineatul (5) litera (e)[38], articolul 8 alineatul (10) literele (a) și (b)[39], articolul 14 alineatul (7) litera (c) și articolul 14 alineatul (10) litera (b), pentru a asigura o aplicare generală eficace a protocolului[40].

În cele din urmă, statele membre ar trebui, de asemenea, să ia măsurile prevăzute la articolul 14 alineatul (11) litera (c) pentru a se asigura că partea destinatară este informată în momentul transferului cu privire la obligația prevăzută de dreptul Uniunii de a furniza o notificare persoanei la care se referă datele[41], precum și datele de contact corespunzătoare pentru a-i permite părții destinatare să informeze autoritatea competentă din statul membru al UE de îndată ce nu se mai aplică restricții privind confidențialitatea și se poate furniza notificarea.

2.5. Motivele propunerii

Protocolul va intra în vigoare de îndată ce cinci părți și-au exprimat consimțământul de a-și asuma obligații în temeiul protocolului în conformitate cu dispozițiile de la articolul 16 alineatele (1) și (2). Ceremonia de semnare a protocolului este prevăzută să aibă loc în martie 2022.

Statele membre ale UE ar trebui să ia măsurile necesare pentru a asigura intrarea rapidă în vigoare a protocolului și ratificarea sa, ceea ce este important având în vedere o serie de factori.

În primul rând, protocolul va asigura faptul că autoritățile de aplicare a legii și autoritățile judiciare sunt mai bine echipate în vederea obținerii de probe electronice necesare pentru anchetele penale. Având în vedere importanța tot mai mare a probelor electronice pentru anchetele penale, este nevoie urgent ca autoritățile de aplicare a legii și autoritățile judiciare să dispună de instrumentele adecvate pentru a obține accesul la probele electronice într-un mod eficace pentru a se asigura că pot combate criminalitatea online în mod corespunzător.

În al doilea rând, protocolul va garanta că astfel de măsuri de obținere a accesului la probele electronice vor fi utilizate într-un mod care să permită statelor membre să respecte drepturile fundamentale, inclusiv drepturile procedurale penale, dreptul la viață privată și dreptul la protecția datelor cu caracter personal. În absența unor norme clare la nivel internațional,

---

[37] Care oferă părților posibilitatea de a declara că nu vor executa cererile prevăzute la articolul 9 alineatul (1) litera (a) (divulgarea accelerată în situații de urgență a datelor informatice) care vizează numai divulgarea datelor privind abonații.

[38] Care oferă părților posibilitatea de a comunica datele de contact ale autorității pe care o desemnează să primească notificările prevăzute la articolul 7 alineatul (5) litera (a) și să efectueze acțiunile descrise la articolul 7 alineatul (5) literele (b), (c) și (d) (divulgarea datelor privind abonații).

[39] Care oferă părților posibilitatea de a comunica datele de contact ale autorităților desemnate să transmită și să primească ordine în temeiul articolului 8 (punerea în aplicare a ordinelor emise de o altă parte). În conformitate cu cerințele prevăzute în Regulamentul (UE) 2017/1939, statele membre care participă la cooperarea consolidată în ceea ce privește instituirea Parchetului European (EPPO) includ EPPO în comunicare.

[40] Care oferă părților posibilitatea de a comunica autorității sau autorităților care ar trebui să fie notificate în cazul unui incident de securitate sau să fie contactate pentru a solicita autorizarea prealabilă în cazul transferurilor ulterioare către un alt stat sau o altă organizație internațională.

[41] A se vedea nota de subsol 24 de mai sus.

practicile existente pot pune probleme cu privire la securitatea juridică, transparență, responsabilitate și respectarea drepturilor fundamentale și a garanțiilor procedurale ale persoanelor suspectate în cadrul anchetelor penale.

În al treilea rând, protocolul va soluționa și va preveni conflictele de legi care afectează atât autoritățile, cât și prestatorii de servicii din sectorul privat și alte entități, oferind norme compatibile la nivel internațional pentru accesul transfrontalier la probele electronice.

În al patrulea rând, protocolul va demonstra importanța pe care o are în continuare convenția ca principal cadru multilateral pentru combaterea criminalității informatice. Acest aspect va avea o importanță majoră în cadrul procesului care se desfășoară în urma adoptării, în decembrie 2019, a Rezoluției 74/247 a Adunării Generale a Organizației Națiunilor Unite, intitulate „Combaterea utilizării tehnologiilor informației și comunicațiilor în scopuri infracționale", care a instituit un comitet deschis interguvernamental ad-hoc format din experți, însărcinat cu elaborarea unei convenții internaționale cuprinzătoare privind combaterea utilizării tehnologiilor informației și comunicațiilor în scopuri infracționale.

3. TEMEI JURIDIC, SUBSIDIARITATE ȘI PROPORȚIONALITATE

- *Temeiul juridic*

Competența Uniunii de a legifera în chestiuni privind facilitarea cooperării dintre autoritățile judiciare sau echivalente în ceea ce privește procedurile în materie penală și executarea deciziilor se întemeiază pe articolul 82 alineatul (1) din TFUE. Competența Uniunii în materie de protecție a datelor cu caracter personal se întemeiază pe articolul 16 din TFUE.

În conformitate cu articolul 3 alineatul (2) din TFUE, Uniunea are competență exclusivă în ceea ce privește încheierea acordurilor internaționale, atunci când acestea pot aduce atingere normelor comune ale UE sau pot modifica domeniul lor de aplicare. Dispozițiile protocolului se încadrează într-un domeniu reglementat în mare măsură de norme comune, astfel cum se arată în secțiunea 2.3 de mai sus.

Prin urmare, protocolul intră în sfera competenței externe exclusive a Uniunii. Prin urmare, ratificarea protocolului de către statele membre, în interesul Uniunii, poate avea loc în temeiul articolului 16, al articolului 82 alineatul (1) și al articolului 218 alineatul (6) din TFUE.

- *Subsidiaritatea (în cazul competențelor neexclusive)*

Nu se aplică.

- *Proporționalitatea*

Obiectivele Uniunii în ceea ce privește prezenta propunere, astfel cum sunt prezentate în secțiunea 2.5 de mai sus, pot fi îndeplinite numai prin încheierea unui acord internațional cu caracter obligatoriu care să prevadă măsurile de cooperare necesare, asigurând, în același timp, protecția adecvată a drepturilor fundamentale. Protocolul îndeplinește acest obiectiv. Dispozițiile protocolului se limitează la ceea ce este necesar pentru atingerea obiectivelor sale principale. Acțiunea unilaterală nu constituie o alternativă, deoarece nu ar oferi o bază suficientă pentru cooperarea cu țările terțe și nu ar putea asigura protecția necesară a drepturilor fundamentale. De asemenea, aderarea la un acord multilateral precum protocolul, pe care Uniunea a fost în măsură să îl negocieze, este mai eficientă decât inițierea de negocieri la nivel bilateral cu țări terțe individuale. Presupunând că toate cele 66 de părți, precum și viitoarele noi părți la convenție vor ratifica protocolul, acesta va oferi un cadru juridic comun

pentru cooperarea statelor membre ale UE cu partenerii lor internaționali cei mai importanți în lupta împotriva criminalității.

- ***Alegerea instrumentului***

Nu se aplică.

4. REZULTATELE EVALUĂRILOR *EX POST*, ALE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRILOR IMPACTULUI

- *Evaluările ex post/verificarea adecvării legislației existente*

Nu se aplică.

- *Consultările cu părțile interesate*

Consiliul Europei a organizat șase runde de consultări publice în legătură cu negocierile privind protocolul, în iulie și noiembrie 2018, februarie și noiembrie 2019, decembrie 2020 și mai 2021[42]. Părțile au analizat contribuțiile primite în cadrul acestor consultări.

De asemenea, Comisia, în calitatea sa de negociator în numele Uniunii, a făcut schimb de opinii cu autoritățile de protecție a datelor și a organizat, în cursul anilor 2019 și 2021, reuniuni de consultare specifice cu organizații ale societății civile, prestatori de servicii și asociații profesionale. Comisia a luat în considerare contribuțiile primite în urma acestor schimburi.

- *Obținerea și utilizarea cunoștințelor de specialitate*

În cadrul negocierilor, Comisia a consultat în mod sistematic comitetul special al Consiliului pentru negocieri, în conformitate cu Decizia Consiliului Uniunii Europene din 6 iunie 2019 de autorizare a Comisiei să participe la negocieri în numele Uniunii, ceea ce a oferit experților statelor membre posibilitatea de a contribui la procesul de formulare a poziției Uniunii. O serie de experți din statele membre au continuat, de asemenea, să participe la negocieri, în paralel cu participarea Comisiei în numele Uniunii. De asemenea, au avut loc consultări cu părțile interesate (a se vedea mai sus).

- *Evaluarea impactului*

În perioada 2017-2018 a fost efectuată o evaluare a impactului care să însoțească propunerile Comisiei privind probele electronice[43]. În acest context, din opțiunea preferată a făcut parte negocierea unui acord referitor la un al doilea protocol adițional la Convenția de la Budapesta privind criminalitatea informatică. Impacturile relevante sunt prezentate, de asemenea, în expunerea de motive din prezenta propunere.

- *Adecvarea reglementărilor și simplificarea*

Protocolul poate avea implicații pentru anumite categorii de prestatori de servicii, inclusiv pentru întreprinderile mici și mijlocii (IMM-uri), deoarece aceștia pot face obiectul unor cereri și ordine privind probele electronice în temeiul protocolului. Cu toate acestea, în prezent, acești prestatori fac deja adesea obiectul unor astfel de cereri prin intermediul altor canale existente, transmise uneori prin intermediul unor autorități diferite, inclusiv pe baza

[42] https://www.coe.int/en/web/cybercrime/protocol-consultations
[43] SWD(2018) 118 final.

convenției[44], a altor tratate de asistență judiciară reciprocă sau a altor cadre, inclusiv a politicilor multipartite privind guvernanța internetului[45]. De asemenea, prestatorii de servicii, inclusiv IMM-urile, vor beneficia de un cadru juridic clar la nivel internațional și de o abordare comună a tuturor părților la protocol.

- *Drepturile fundamentale*

Instrumentele de cooperare prevăzute în protocol pot afecta drepturile fundamentale în cazul în care datele unei persoane pot fi obținute în contextul unei proceduri penale, inclusiv, de exemplu, dreptul la un proces echitabil, dreptul la viață privată și dreptul la protecția datelor cu caracter personal. Protocolul adoptă o abordare bazată pe drepturi și prevede condiții și garanții în conformitate cu instrumentele internaționale privind drepturile omului, inclusiv Convenția Consiliului Europei din 1950 pentru apărarea drepturilor omului și a libertăților fundamentale. În special, protocolul prevede garanții specifice privind protecția datelor. Dacă este necesar, protocolul oferă, de asemenea, o bază pentru formularea de către părți a anumitor rezerve, declarații sau notificări și include motive de refuz al cooperării ca răspuns la o cerere în situații specifice. Acest lucru asigură compatibilitatea protocolului cu Carta drepturilor fundamentale a UE.

5. IMPLICAȚII BUGETARE

Propunerea nu are implicații asupra bugetului Uniunii. Este posibil ca statele membre să suporte costuri punctuale pentru punerea în aplicare a protocolului și ar putea exista costuri mai mari pentru autoritățile statelor membre din cauza creșterii preconizate a numărului de cazuri.

6. ALTE ELEMENTE

- *Planurile de punere în aplicare și măsurile de monitorizare, evaluare și raportare*

Nu există un plan de punere în aplicare deoarece, în urma semnării și ratificării acestuia, statele membre vor trebui să pună în aplicare protocolul.

În ceea ce privește monitorizarea, Comisia va participa la reuniunile Comitetului Convenției privind criminalitatea informatică, în cadrul cărora Uniunea Europeană este recunoscută ca organizație cu statut de observator.

[44] A se vedea, de exemplu, Nota orientativă nr. 10 a Comitetului Convenției privind criminalitatea informatică din 1 martie 2017 privind ordinele de divulgare pentru informațiile referitoare la abonați (articolul 18 din Convenția de la Budapesta).

[45] A se vedea, de exemplu, Rezoluția Consiliului de cooperare pe internet pentru alocarea de nume și numere de domenii internet (ICANN) din 15 mai 2019 referitoare la recomandările privind specificația temporară pentru datele de înregistrare gTLD, disponibilă la adresa www.icann.org.

2021/0383 (NLE)

Propunere de

DECIZIE A CONSILIULUI

de autorizare a statelor membre să ratifice, în interesul Uniunii Europene, cel de Al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și la divulgarea probelor electronice

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 16, articolul 82 alineatul (1) și articolul 218 alineatul (6),

având în vedere propunerea Comisiei Europene,

având în vedere aprobarea Parlamentului European,

întrucât:

(1) La 9 iunie 2019, Consiliul a autorizat Comisia să participe, în numele Uniunii, la negocierile privind cel de Al doilea protocol adițional la Convenția de la Budapesta a Consiliului Europei privind criminalitatea informatică.

(2) Textul celui de Al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și la divulgarea probelor electronice („protocolul”) a fost adoptat de Comitetul de Miniștri al Consiliului Europei la 17 noiembrie 2021 și se preconizează că protocolul va fi deschis spre semnare în martie 2022.

(3) Dispozițiile protocolului se încadrează într-un domeniu reglementat în mare măsură de norme comune în sensul articolului 3 alineatul (2) din TFUE, inclusiv instrumente care facilitează cooperarea judiciară în materie penală și care asigură standarde minime privind drepturile procedurale, precum și protecția datelor și a vieții private.

(4) De asemenea, Comisia a prezentat propuneri legislative referitoare la un regulament privind ordinele europene de divulgare și de păstrare a probelor electronice în materie penală [COM(2018) 225 final] și la o directivă de stabilire a unor norme armonizate privind desemnarea reprezentanților legali în scopul obținerii de probe în cadrul procedurilor penale [COM(2018) 226 final], prin care se introduc ordinele europene obligatorii transfrontaliere de divulgare și de păstrare a probelor electronice care trebuie adresate direct unui reprezentant al unui prestator de servicii dintr-un alt stat membru.

(5) Prin participarea sa la negocieri, în numele Uniunii, Comisia a asigurat compatibilitatea celui de Al doilea protocol adițional cu normele comune relevante ale Uniunii Europene.

(6) O serie de rezerve, declarații, notificări și comunicări sunt relevante pentru a asigura compatibilitatea protocolului cu legislația și politicile Uniunii, precum și aplicarea uniformă a protocolului de către statele membre ale UE în relația acestora cu părțile din afara UE și aplicarea eficace a protocolului.

(7) Având în vedere că protocolul prevede proceduri rapide care îmbunătățesc accesul transfrontalier la probele electronice și un nivel ridicat de garanții, intrarea în vigoare va contribui la combaterea criminalității informatice și a altor forme de criminalitate la nivel mondial prin facilitarea cooperării dintre statele membre ale UE și țările terțe care sunt părți la protocol, va asigura un nivel ridicat de protecție a persoanelor și va soluționa conflictele de legi.

(8) Având în vedere că protocolul prevede garanții adecvate în conformitate cu cerințele privind transferurile internaționale de date cu caracter personal în temeiul Regulamentului (UE) 2016/679 și al Directivei (UE) 2016/680, intrarea sa în vigoare va contribui la promovarea standardelor Uniunii în materie de protecție a datelor la nivel mondial, va facilita fluxurile de date între statele membre ale UE și țările terțe care sunt părți la protocol și va asigura respectarea de către statele membre ale UE a obligațiilor care le revin în temeiul normelor Uniunii privind protecția datelor.

(9) Intrarea rapidă în vigoare va confirma, de asemenea, rolul Convenției de la Budapesta a Consiliului Europei ca principal cadru multilateral pentru combaterea criminalității informatice.

(10) Uniunea Europeană nu poate deveni parte la protocol, deoarece atât protocolul, cât și Convenția Consiliului Europei privind criminalitatea informatică sunt deschise numai statelor.

(11) Prin urmare, statele membre ar trebui să fie autorizate să ratifice protocolul, acționând împreună în interesul Uniunii Europene.

(12) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului și a emis un aviz la …

(13) [În conformitate cu articolele 1 și 2 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și fără a aduce atingere articolului 4 din protocolul menționat, Irlanda nu participă la adoptarea prezentei decizii, nu are obligații în temeiul acestuia și nu face obiectul aplicării sale.]

[SAU]

[În conformitate cu articolele 1 și 2 din Protocolul nr. 21 privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, și fără a aduce atingere articolului 4 din protocolul menționat, Irlanda și-a notificat [, prin scrisoarea din...,] intenția de a participa la adoptarea și la aplicarea prezentei decizii.]

(14) În conformitate cu articolele 1 și 2 din Protocolul nr. 22 privind poziția Danemarcei, anexat la Tratatul privind Uniunea Europeană și la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentei decizii, nu are obligații în temeiul acesteia și nu face obiectul aplicării sale,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Statele membre sunt autorizate să ratifice, în interesul Uniunii Europene, cel de Al doilea protocol adițional la Convenția privind criminalitatea informatică referitor la cooperarea consolidată și la divulgarea probelor electronice („protocolul”).

Articolul 2

Atunci când ratifică protocolul, statele membre formulează rezervele, declarațiile, notificările sau comunicările care sunt prevăzute în anexă.

Articolul 3

Prezenta decizie intră în vigoare la data adoptării.

Articolul 4

Prezenta decizie se publică în *Jurnalul Oficial al Uniunii Europene*.

Articolul 5

Prezenta decizie se adresează statelor membre.

Adoptată la Bruxelles,

Pentru Consiliu,
Președintele