EIROPAS
KOMISIJA

Briselē, 25.11.2021.
COM(2021) 719 final

2021/0383 (NLE)

Priekšlikums

PADOMES LĒMUMS,

ar kuru dalībvalstīm atļauj Eiropas Savienības interesēs ratificēt Konvencijas par kibernoziegumiem otro papildu protokolu par pastiprinātu sadarbību un elektronisko pierādījumu izpaušanu

PASKAIDROJUMA RAKSTS

1. PRIEKŠLIKUMA PRIEKŠMETS

Šis priekšlikums attiecas uz lēmumu, ar kuru dalībvalstīm atļauj Eiropas Savienības interesēs ratificēt otro papildu protokolu par pastiprinātu sadarbību un elektronisko pierādījumu izpaušanu[1] ("Protokols") Eiropas Padomes Budapeštas Konvencijai par kibernoziegumiem. Protokola mērķis ir starptautiskā līmenī nodrošināt kopīgus noteikumus, lai pastiprinātu sadarbību kibernoziedzības jomā un pierādījumu vākšanu elektroniskā veidā krimināllizmeklēšanai vai tiesvedībai.

Šis priekšlikums papildina atsevišķu Komisijas priekšlikumu Eiropas Savienības Padomes ("Padome") lēmumam, ar ko dalībvalstīm atļauj parakstīt Protokolu Eiropas Savienības interesēs.

Kibernoziedzība joprojām ir liels izaicinājums mūsu sabiedrībai. Neraugoties uz tiesībaizsardzības un tiesu iestāžu centieniem, kiberuzbrukumi, t. sk. uzbrukumi, izmantojot izspiedējprogrammatūru, kļūst arvien biežāki un kompleksāki[2]. It īpaši tādēļ, ka internetam nav robežu, kibernoziegumu izmeklēšana gandrīz vienmēr ir pārrobežu rakstura, tādēļ ir nepieciešama cieša sadarbība starp dažādu valstu iestādēm.

Elektroniskajiem pierādījumiem krimināllizmeklēšanās ir arvien lielāka nozīme. Komisija lēš, ka mūsdienās tiesībaizsardzības un tiesu iestādēm 85 % krimināllizmeklēšanu, t. sk. saistībā ar kibernoziegumiem, ir vajadzīga piekļuve elektroniskajiem pierādījumiem.[3] Ārvalstu jurisdikcijās pakalpojumu sniedzēji pierādījumus par jebkādiem noziedzīgiem nodarījumiem arvien biežāk glabā elektroniskā formā, un efektīvai krimināltiesiskai reakcijai ir vajadzīgi atbilstīgi pasākumi, lai iegūtu šādus pierādījumus tiesiskuma ievērošanai.

Visā pasaulē, valstu, Eiropas Savienības[4] un starptautiskā līmenī tiek īstenoti centieni uzlabot pārrobežu piekļuvi elektroniskiem pierādījumiem krimināllizmeklēšanā, t. sk. izmantojot Protokolu. Ir svarīgi nodrošināt saderīgus noteikumus starptautiskā līmenī, lai izvairītos no tiesību normu kolīzijām gadījumos, kad tiek prasīta pārrobežu piekļuve elektroniskiem pierādījumiem.

2. PRIEKŠLIKUMA KONTEKSTS

2.1. Pamatinformācija

Eiropas Padomes Budapeštas Konvencijas par kibernoziegumiem (Eiropas Padomes līgumu sērija Nr. 185) ("Konvencija") mērķis ir atvieglot cīņu pret noziedzīgiem nodarījumiem, kas tiek veikti, izmantojot datortīklus. Tajā 1) ir ietverti noteikumi, ar ko saskaņo nodarījumu iekšzemes materiālo krimināltiesību normu elementus un saistītus noteikumus kibernoziedzības jomā, 2) nodrošina iekšzemes kriminālprocesuālās pilnvaras, kas nepieciešamas, lai izmeklētu šādus nodarījumus un sāktu kriminālvajāšanu par tiem, kā arī par citiem nodarījumiem, kuri izdarīti, izmantojot datorsistēmu, vai par kuriem pierādījumi ir elektroniskā formā, un tās 3) mērķis ir izveidot ātru un efektīvu starptautiskās sadarbības režīmu.

---

1 Protokola teksts ir iekļauts šā priekšlikuma pielikumā.
2 2021. gada Eiropas Savienības smagās un organizētās noziedzības draudu novērtējums (ES *SOCTA* 2021).
3 SWD(2018) 118 final.
4 COM(2018) 225 un 226 final.

Konvencija pēc uzaicinājuma ir pieejama parakstīšanai gan Eiropas Padomes dalībvalstīm, gan valstīm, kas nav dalībvalstis. Konvencijas Puses patlaban ir 66 valstis, t. sk. 26 Eiropas Savienības dalībvalstis.[5] Konvencijā nav paredzēta iespēja, ka Eiropas Savienība varētu pievienoties Konvencijai. Tomēr Eiropas Savienība ir atzīta par novērotājorganizāciju Konvencijas par kibernoziegumiem komitejā (*T-CY*).[6]

Neraugoties uz centieniem Apvienoto Nāciju Organizācijas līmenī[7] risināt sarunas par jaunu konvenciju par kibernoziegumiem, Budapeštas konvencija joprojām ir galvenā daudzpusējā konvencija cīņai pret kibernoziedzību. Savienība konsekventi atbalsta Konvenciju[8], arī finansējot spēju veidošanas programmas.[9]

Pēc Mākoņdatu pierādījumu grupas priekšlikumiem[10] Konvencijas par krimināLnoziegumiem komiteja pieņēma vairākus ieteikumus, lai, t. sk. sarunās par Konvencijas par kibernoziegumiem otro papildu protokolu par pastiprinātu starptautisko sadarbību, risinātu problēmu, ko rada apstāklis, ka pakalpojumu sniedzēji elektroniskos pierādījumus saistībā ar kibernoziegumiem un citiem nodarījumiem arvien vairāk glabā ārvalstu jurisdikcijās, savukārt tiesībaizsardzības pilnvaras joprojām ierobežo teritoriālās robežas. 2017. gada jūnijā Konvencijas par kibernoziegumiem komiteja apstiprināja darba uzdevumus otrā papildu protokola sagatavošanai laikposmā no 2017. gada septembra līdz 2019. gada decembrim.[11] Ņemot vērā to, ka ir vajadzīgs ilgāks laiks diskusiju pabeigšanai, kā arī Covid-19 pandēmijas radītos ierobežojumus 2020. un 2021. gadā, Konvencijas par kibernoziegumiem komiteja darba uzdevumus pagarināja divas reizes, proti, līdz 2020. gada decembrim un pēc tam līdz 2021. gada maijam.

Pēc Eiropadomes 2018. gada 18. oktobra secinājumos[12] izteiktā aicinājuma Komisija 2019. gada 5. februārī pieņēma ieteikumu Padomes Lēmumam, ar ko Komisiju pilnvaro Eiropas Savienības vārdā piedalīties sarunās par Eiropas Padomes Konvencijas par kibernoziegumiem otro papildu protokolu.[13] Eiropas Datu aizsardzības uzraudzītājs 2019. gada 2. aprīlī pieņēma atzinumu par ieteikumu.[14] Ar 2019. gada 6. jūnija lēmumu Eiropas Savienības Padome pilnvaroja Komisiju Eiropas Savienības vārdā piedalīties sarunās par otro papildu protokolu.[15]

---

5 Visas valstis, izņemot Īriju, kura Konvenciju ir parakstījusi, bet nav ratificējusi, tomēr ir apņēmusies turpināt pievienošanās procesu.

6 Konvencijas par kibernoziegumiem komitejas reglaments (*T-CY* (2013)25 rev), pieejams vietnē www.coe.int/cybercrime.

7 Apvienoto Nāciju Organizācijas Ģenerālās asamblejas (ANO ĢA) 2019. gada decembra Rezolūcija 74/247 par vēršanos pret informācijas un komunikācijas tehnoloģiju izmantošanu noziedzīgiem nolūkiem.

8 JOIN(2020) 81 final.

9 Skatīt, piemēram, *Global Action on Cybercrime Extended* (*GLACY*)+, https://www.coe.int/en/web/cybercrime/glacyplus.

10 Konvencijas par kibernoziegumiem komiteja Mākoņdatu pierādījumu grupas 2016. gada 16. septembra galīgais ziņojums "Krimināltiesību iestāžu piekļuve elektroniskiem pierādījumiem mākonī: *T-CY* ieteikumi apsvēršanai".

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

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

13 COM(2019) 71 final.

14 EDAU 2019. gada 2. aprīļa atzinums par dalību sarunās saistībā ar Budapeštas Konvencijas par kibernoziegumiem otro papildprotokolu, Atzinums 3/2019.

15 Padomes lēmums, atsauce 9116/19.

Kā norādīts 2020. gada ES Drošības savienības stratēģijā[16], 2020. gada ES kiberdrošības stratēģijā digitālajai desmitgadei[17] un 2021. gada ES organizētās noziedzības apkarošanas stratēģijā[18], Komisija ir apņēmusies ātri un sekmīgi pabeigt sarunas par Protokolu. Eiropas Parlaments savā 2021. gada rezolūcijā par ES kiberdrošības stratēģiju digitālajai desmitgadei[19] arī atzina nepieciešamību pabeigt darbu attiecībā uz Protokolu.

Komisija Eiropas Savienības vārdā piedalījās sarunās par Protokolu saskaņā ar Eiropas Savienības Padomes lēmumu. Sarunās par Savienības nostāju Komisija pastāvīgi apspriedās ar Padomes īpašo komiteju.

Saskaņā ar Pamatnolīgumu par Eiropas Parlamenta un Eiropas Komisijas attiecībām[20] Komisija arī informēja Eiropas Parlamentu par sarunām, gan iesniedzot rakstiskus ziņojumus, gan sniedzot mutiskas prezentācijas.

Konvencijas par kibernoziegumiem komitejas plenārsēdē 2021. gada 28. maijā Konvencijas par kibernoziegumiem komiteja apstiprināja Protokola projektu savā līmenī un nosūtīja projektu pieņemšanai Eiropas Padomes Ministru komitejā.[21] Eiropas Padomes Ministru padome Protokolu pieņēma 2021. gada 17. novembrī.

2.2. Otrais papildu protokols

Protokola mērķis ir pastiprināt sadarbību kibernoziedzības jomā un pierādījumu par noziedzīgu nodarījumu vākšanu elektroniskā formā konkrētas krimināllizmeklēšanas vai tiesvedības vajadzībām. Protokolā atzīst vajadzību pēc pastiprinātas un efektīvākas sadarbības starp valstīm un privāto sektoru un lielākas skaidrības un juridiskās noteiktības pakalpojumu sniedzējiem un citām struktūrām attiecībā uz apstākļiem, kādos tās var atbildēt uz citu Pušu tiesībaizsardzības iestāžu pieprasījumiem izpaust elektroniskos pierādījumus.

Protokolā arī atzīst to, ka efektīvai pārrobežu sadarbībai krimināltiesību jomā, t. sk starp publiskā sektora iestādēm un privātā sektora struktūrām, ir nepieciešami efektīvi noteikumi un stingras garantijas pamattiesību aizsardzībai. Šajā nolūkā Protokolā ievēro tiesībām balstītu pieeju un paredz noteikumus un garantijas saskaņā ar starptautiskajiem cilvēktiesību instrumentiem, t. sk. Eiropas Padomes 1950. gada Cilvēktiesību un pamatbrīvību aizsardzības konvenciju. Tā kā elektroniskie pierādījumi bieži attiecas uz personas datiem, Protokolā ir iekļauti arī stingras garantijas privātuma un personas datu aizsardzībai.

Nākamajās daļās minētie noteikumi Protokolam ir īpaši svarīgi. Protokolam ir pievienots sīki izstrādāts paskaidrojuma ziņojums. Lai gan paskaidrojuma ziņojums nav instruments, kas nodrošinātu Protokola autoritatīvu interpretāciju, tā mērķis ir "sniegt norādes Pusēm un tām palīdzēt" Protokola piemērošanā.[22]

---

16 COM(2020) 605 final.
17 JOIN(2020) 81 final.
18 COM(2021) 170 final.
19 Eiropas Parlamenta 2021. gada 10. jūnija rezolūcija par ES kiberdrošības stratēģiju digitālajai desmitgadei.
20 Atsauce L 304/47.
21 https://rm.coe.int/0900001680a2aa42
22 Sk. Protokola paskaidrojuma ziņojuma 2. punktu.

2.2.1. Kopīgi noteikumi

Protokola I nodaļā paredz kopīgus noteikumus. Tā 2. pants nosaka Protokola piemērošanas jomu saskaņā ar Konvencijas piemērošanas jomu: to piemēro attiecībā uz konkrētām krimināllizmeklēšanām vai tiesvedībām, kas saistītas ar datorsistēmām un datiem, un attiecībā uz pierādījumu par noziedzīgu nodarījumu vākšanu elektroniskā formā.

Tā 3. pantā ir ietvertas definīcijas attiecībā uz "centrālajām iestādēm", "kompetentajām iestādēm", "ārkārtas situācijām", "personas datiem" un "nosūtošo Pusi". Šīs definīcijas piemēro Protokolam kopā ar Konvencijā iekļautajām definīcijām.

Tā 4. pants nosaka valodas, kurās Pusēm būtu jāiesniedz rīkojumi, pieprasījumi vai paziņojumi saskaņā ar Protokolu.

2.2.2. Sadarbības pasākumi

Protokola II nodaļā paredz pasākumus pastiprinātai sadarbībai. Pirmkārt, 5. panta 1. punkts nosaka, ka Puses, pamatojoties uz Protokolu, sadarbojas pēc iespējas plašākā mērogā. Tā 5. panta 2.–5. punkts nosaka Protokola pasākumu piemērošanu saistībā ar spēkā esošajiem savstarpējās palīdzības līgumiem vai režīmiem. Tā 5. panta 7. punkts nosaka, ka II nodaļas pasākumi neierobežo sadarbību starp Pusēm vai ar pakalpojumu sniedzējiem vai struktūrām, šajā nolūkā izmantojot citus piemērojamus nolīgumus, režīmus, praksi vai iekšzemes tiesību aktus.

Tā 6. pants nodrošina pamatu tiešai sadarbībai starp kompetentajām iestādēm vienas Puses teritorijā un struktūrām, kas sniedz domēna nosaukuma reģistrācijas pakalpojumus citas Puses teritorijā, domēna vārda reģistrācijas datu izpaušanas nolūkā.

Tā 7. pants nodrošina pamatu tiešai sadarbībai starp kompetentajām iestādēm vienas Puses teritorijā un pakalpojumu sniedzējiem citas Puses teritorijā abonenta datu izpaušanas nolūkā.

Tā 8. pants nodrošina pamatu iestāžu pastiprinātai sadarbībai datorizētu datu izpaušanas nolūkā.

Tā 9. pants nodrošina pamatu iestāžu sadarbībai datorizētu datu izpaušanas nolūkā ārkārtas situācijās.

Tā 10. pants nodrošina pamatu savstarpējas tiesiskās palīdzības sniegšanai ārkārtas situācijās.

Tā 11. pants nodrošina pamatu sadarbībai, izmantojot videokonferences.

Tā 12. pants nodrošina pamatu kopīgām izmeklēšanām un kopējām izmeklēšanas grupām.

2.2.3. Garantijas

Protokolā ir ievērota tiesībās balstīta pieeja ar īpašiem noteikumiem un garantijām, daži no kuriem ir iekļauti īpašajos sadarbības pasākumos, kā arī Protokola III nodaļā. Protokola 13. pants prasa, lai Puses nodrošinātu, ka uz pilnvarām un kārtību attiecina pienācīgu pamattiesību aizsardzības līmeni, kas saskaņā ar Konvencijas 15. pantu nodrošina proporcionalitātes principa piemērošanu.

Protokola 14. pants paredz personas datu aizsardzību, kā noteikts Protokola 3. pantā, saskaņā ar grozījumu protokolu Konvencijai par personu aizsardzību attiecībā uz personas datu

apstrādi (Eiropas Padomes līgumu sērija 223) (Konvencija 108+) un Savienības tiesību aktiem.

Uz šā pamata 14. panta 2.–15. punkts nosaka datu aizsardzības pamatprincipus, t. sk. mērķa ierobežojumu, juridisko pamatu, datu kvalitāti un noteikumus, kas piemērojami attiecībā uz īpašu kategoriju datu apstrādi, pienākumus, kas piemērojami pārziņiem, arī attiecībā uz datu glabāšanu, reģistru uzturēšanu, drošību un attiecībā uz tālāku nosūtīšanu, īstenojamas individuālās tiesības, t. sk. attiecībā uz paziņošanu, piekļuvi, labošanu un automatizētu lēmumu pieņemšanu, vienas vai vairāku iestāžu veiktu neatkarīgu un efektīvu uzraudzību, kā arī tiesiskās aizsardzības līdzekļiem administratīvā kārtā un tiesā. Garantijas attiecas uz visiem Protokolā noteiktajiem sadarbības veidiem, vajadzības gadījumā veicot pielāgojumus, lai ņemtu vērā tiešās sadarbības īpašās iezīmes (piemēram, saistībā ar pārkāpumu paziņošanu). Konkrētu individuālo tiesību īstenošanu var atlikt, ierobežot vai atteikt, ja tas ir nepieciešams un ir samērīgi, lai sasniegtu svarīgus sabiedrisko interešu mērķus, it īpaši, lai novērstu risku notiekošām tiesībaizsardzības iestāžu izmeklēšanām, kas atbilst arī Savienības tiesību aktiem.

Protokola 14. pants arī jālasa saistībā ar Protokola 23. pantu. Tā 23. pants pastiprina Protokola garantiju efektivitāti, paredzot, ka Konvencijas par kibernoziegumiem komiteja novērtēs to pasākumu īstenošanu un piemērošanu, kas veikti valstu tiesību aktos, lai īstenotu Protokola noteikumus. It īpaši 23. panta 3. punktā skaidri atzīst, ka Pušu veikto 14. panta īstenošanu novērtēs pēc tam, kad desmit Konvencijas Puses būs paudušas piekrišanu uzņemties Protokola saistības.

Kā papildu garantiju saskaņā ar 14. panta 15. punktu gadījumā, ja Pusei ir būtiski pierādījumi, ka cita Puse sistemātiski vai būtiski pārkāpj Protokolā noteiktās garantijas, tā pēc apspriešanās (kas nav nepieciešama steidzamības gadījumā) var apturēt personas datu sūtīšanu minētajai Pusei. Personas datus, kas nosūtīti pirms apturēšanas, turpina apstrādāt saskaņā ar Protokolu.

Visbeidzot, ņemot vērā Protokola daudzpusējo raksturu, Protokola 14. 1. punkta b. un c. apakšpunkts ļauj Pusēm to divpusējās attiecībās, ievērojot konkrētus nosacījumus, vienoties par alternatīviem veidiem, kā nodrošināt saskaņā ar Protokolu nosūtīto personas datu aizsardzību. Lai gan 14. panta 2.–15. punktā paredzētās garantijas pēc noklusējuma piemēro Pusēm, kas saņem personas datus, pamatojoties uz 14. panta 1. punkta b. apakšpunktu, Puses, kurām ir savstarpēji saistošs starptautisks nolīgums, ar ko izveido visaptverošu personas datu aizsardzības regulējumu saskaņā ar piemērojamajām attiecīgo Pušu tiesību aktu prasībām, var arī balstīties uz minēto regulējumu. Tas attiecas, piemēram, uz Konvenciju 108+ (attiecībā uz tām Pusēm, kas saskaņā ar minēto Konvenciju atļauj nosūtīt datus citām Pusēm) vai ES un ASV jumta nolīgumu (ciktāl tas ietilpst tā piemērošanas jomā, t. i., personas datu nosūtīšanai starp iestādēm un kopā ar īpašu nosūtīšanas kārtību starp ASV un ES – attiecībā uz tiešu sadarbību starp iestādēm un pakalpojumu sniedzējiem). Turklāt, pamatojoties uz 14. panta 1. punkta c. apakšpunktu, Puses var arī savstarpēji noteikt, ka personas datu nosūtīšana notiek, pamatojoties uz citiem nolīgumiem vai režīmiem starp attiecīgajām Pusēm. ES dalībvalstis uz šādu alternatīvu nolīgumu vai režīmu datu nosūtīšanai saskaņā ar Protokolu var balstīties tikai tad, ja šāda nosūtīšana atbilst Savienības datu aizsardzības tiesību aktu prasībām, proti, Direktīvas (ES) 2016/680 (Tiesībaizsardzības direktīva) V nodaļas un (attiecībā uz tiešu sadarbību starp iestādēm un pakalpojumu sniedzējiem saskaņā ar Protokola 6. un 7. pantu) Regulas (ES) 2016/679 (Vispārīgā datu aizsardzības regula) V nodaļas prasībām.

2.2.4. Nobeiguma noteikumi

Protokola IV nodaļā paredz nobeiguma noteikumus. Cita starpā 15. panta 1. punkta a. apakšpunkts nodrošina, ka Puses var izveidot savas attiecības jautājumos, kas Protokolā noteikti citādi, atbilstīgi Konvencijas 39. panta 2. punktam. Tā 15. panta 1. punkta b. apakšpunkts nodrošina, ka ES dalībvalstis, kas ir Protokola Puses, savās savstarpējās attiecībās var turpināt piemērot Savienības tiesību aktus. Tā 15. panta 2. punkts arī nosaka, ka Protokolam piemēro Konvencijas 39. panta 3. punktu.

Tā 16. panta 3. punktā norādīts, ka Protokols stāsies spēkā, tiklīdz piecas Konvencijas puses būs izteikušas piekrišanu uzņemties Protokola saistības.

Tā 19. panta 1. punkts paredz, ka Puses var izdarīt atrunas attiecībā uz 7. panta 9. punkta a. apakšpunktu un 9. punkta b. apakšpunktu, 8. panta 13. punktu un 17. pantu. Tā 19. panta 2. punkts paredz, ka Puses var sniegt deklarācijas saistībā ar 7. panta 2. punkta b. apakšpunktu un 8. punktu, 8. panta 11. punktu, 9. panta 1. punkta b. apakšpunktu un 5. punktu, 10. panta 9. punktu, 12. panta 3. punktu un 18. panta 2. punktu. Tā 19. panta 3. punkts nosaka, ka Puse sniedz deklarācijas, paziņojumus vai paziņojumus, kas noteikti 7. panta 5. punkta a. un e. apakšpunktā, 8. panta 4. punktā un 10. punkta a. un b. apakšpunktā, 14. panta 7. punkta c. apakšpunktā un 10. punkta b. apakšpunktā un 17. panta 2. punktā.

Tā 23. panta 1. punkts nodrošina pamatu, lai Puses varētu savstarpēji apspriesties, t. sk. ar Konvencijas par kibernoziegumiem komitejas starpniecību, atbilstīgi Konvencijas 46. pantam. Tā 23. panta 2. punkts arī nodrošina pamatu Protokola noteikumu izmantošanas un īstenošanas novērtējumam. Tā 23. panta 3. punkts nodrošina to, ka 14. panta par datu aizsardzību izmantošanas un īstenošanas novērtēšana sākas tad, kad desmit Puses ir paudušas piekrišanu uzņemties Protokola saistības.

2.3. Savienības tiesību akti un politika šajā jomā

Uz jomu, ko reglamentē Protokols, lielā mērā attiecas kopīgi noteikumi, kuru pamatā ir LESD 82. panta 1. punkts un 16. pants. Pašreizējais Eiropas Savienības tiesiskais regulējums it īpaši ietver instrumentus par tiesībaizsardzības iestāžu un tiesu iestāžu sadarbību krimināllietās, piemēram, Direktīvu 2014/41/ES par Eiropas izmeklēšanas rīkojumu krimināllietās, Konvenciju par Eiropas Savienības dalībvalstu savstarpēju palīdzību krimināllietās un Padomes Pamatlēmumu 2002/465/TI par kopējām izmeklēšanas grupām. Ārējās attiecībās Eiropas Savienība ir noslēgusi vairākus divpusējus nolīgumus starp Savienību un trešām valstīm, piemēram, nolīgumus par savstarpējo juridisko palīdzību starp Eiropas Savienību un Amerikas Savienotajām Valstīm, starp Eiropas Savienību un Japānu un starp Eiropas Savienību un Norvēģiju un Islandi. Pašreizējais Eiropas Savienības tiesiskais regulējums arī ietver Regulu (ES) 2017/1939, ar ko īsteno ciešāku sadarbību Eiropas Prokuratūras ("*EPPO*") izveidei. Dalībvalstīm, kas piedalās ciešākā sadarbībā, būtu jānodrošina, ka *EPPO*, īstenojot savas kompetences, kā to nosaka 22., 23. un 25. pants Regulā (ES) 2017/1939, var censties panākt sadarbību saskaņā ar Protokolu tādā pašā veidā kā minēto dalībvalstu prokurori. Šie instrumenti un nolīgumi it īpaši attiecas uz Protokola 8., 9., 10., 11. un 12. pantu.

Turklāt Savienība ir pieņēmusi vairākas direktīvas, kas stiprina aizdomās turēto un apsūdzēto procesuālās tiesības.[23] Šie instrumenti it īpaši attiecas uz Protokola 6., 7., 8., 9., 10., 11., 12.

[23] Eiropas Parlamenta un Padomes Direktīva 2010/64/ES (2010. gada 20. oktobris) par tiesībām uz mutisko un rakstisko tulkojumu kriminālprocesā (OV L 280, 26.10.2010., 1. lpp.); Eiropas Parlamenta un Padomes Direktīva 2012/13/ES (2012. gada 22. maijs) par tiesībām uz informāciju kriminālprocesā (OV L 142, 1.6.2012., 1. lpp.); Eiropas Parlamenta un Padomes Direktīva 2013/48/ES (2013. gada 22. oktobris) par

un 13. pantu. Viens konkrēts garantiju kopums attiecas uz personas datu aizsardzību, kas ir pamattiesības, kuras nostiprinātas ES Līgumos un Eiropas Savienības Pamattiesību hartā. Personas datus var apstrādāt tikai saskaņā ar Regulu (ES) 2016/679 (Vispārīgā datu aizsardzības regula) un Direktīvu (ES) 2016/680 (Tiesībaizsardzības direktīva). Ikvienas personas pamattiesības uz savas privātās un ģimenes dzīves, dzīvokļa un saziņas neaizskaramību ietver saziņas privātās dzīves ievērošanu kā būtisku elementu. Elektroniskās komunikācijas datus var apstrādāt tikai saskaņā ar Direktīvu 2002/58/EK (E-privātuma direktīva). Šie instrumenti it īpaši attiecas uz Protokola 14. pantu.

Protokola 14. panta 2.–15. punkts paredz atbilstošas datu aizsardzības garantijas Savienības datu aizsardzības noteikumu, it īpaši Vispārīgās datu aizsardzības regulas 46. panta un Tiesībaizsardzības direktīvas 37. panta, un Eiropas Savienības Tiesas attiecīgās judikatūras nozīmē. Saskaņā ar Savienības tiesību aktu prasībām[24] un lai garantētu Protokola 14. pantā noteikto garantiju efektivitāti, dalībvalstīm būtu jānodrošina to personu informēšana, kuru dati ir nosūtīti, šajā nolūkā ievērojot konkrētus ierobežojumus, piemēram, lai neapdraudētu notiekošās izmeklēšanas. Protokola 14. panta 11. punkta c. apakšpunkts nodrošina pamatu dalībvalstīm, lai tās varētu izpildīt šo prasību.

Protokola 14. panta 1. punkta saderība ar Savienības datu aizsardzības noteikumiem arī nosaka, ka dalībvalstis apsver iespējamos alternatīvos veidus, kā nodrošināt saskaņā ar Protokolu nosūtīto personas datu pienācīgu aizsardzību. Attiecībā uz citiem starptautiskiem nolīgumiem, ar ko izveido visaptverošu personas datu aizsardzības regulējumu atbilstīgi piemērojamajām attiecīgo Pušu tiesību aktu prasībām, dalībvalstīm saskaņā ar 14. panta 1. punkta b. apakšpunktu būtu jāņem vērā, ka attiecībā uz tiešu sadarbību ES un ASV jumta nolīgums ir jāpapildina ar papildu garantijām, kuras jāparedz īpašā datu nosūtīšanas nolīgumā starp ASV un ES/tās dalībvalstīm un kurās ņem vērā unikālās prasības par elektronisko pierādījumu nosūtīšanu, ko tieši veic pakalpojumu sniedzēji, nevis iestādes savā starpā.[25]

---

tiesībām uz advokāta palīdzību kriminālprocesā un Eiropas apcietināšanas ordera procesā, par tiesībām uz to, ka pēc brīvības atņemšanas informē trešo personu, un par tiesībām, kamēr atņemta brīvība, sazināties ar trešām personām un konsulārajām iestādēm (OV L 294, 6.11.2013., 1. lpp.); Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1919 (2016. gada 26. oktobris) par juridisko palīdzību aizdomās turētajiem un apsūdzētajiem kriminālprocesā un pieprasītajām personām Eiropas apcietināšanas ordera procesā (OV L 297, 4.11.2016., 1. lpp.); Eiropas Parlamenta un Padomes Direktīva (ES) 2016/800 (2016. gada 11. maijs) par procesuālajām garantijām bērniem, kuri ir aizdomās turētie vai apsūdzētie kriminālprocesā (OV L 132, 21.5.2016., 1. lpp.); Eiropas Parlamenta un Padomes Direktīva (ES) 2016/343 (2016. gada 9. marts) par to, lai nostiprinātu konkrētus nevainīguma prezumpcijas aspektus un tiesības piedalīties klātienē lietas izskatīšanā tiesā kriminālprocesā (OV L 65, 11.3.2016., 1. lpp.); Eiropas Parlamenta un Padomes Direktīva 2012/13/ES (2012. gada 22. maijs) par tiesībām uz informāciju kriminālprocesā.

[24] Sk. Tiesas atzinumu 1/15 (virspalāta), ECLI:EU:C:2017:592, 220. punkts. Sk. arī EDAK ieguldījumu Eiropas Padomes Konvencijas par kibernoziegumiem (Budapeštas konvencijas) otrā papildu protokola projekta apspriešanā, 2019. gada 13. novembris, 6. lpp. ("Kompetentās valsts iestādes, kurām ir piešķirta piekļuve datiem, par to informē attiecīgās personas atbilstoši piemērojamajām valsts procesuālajām normām no brīža, kad šī saziņa vairs nevar traucēt šo iestāžu veiktajai izmeklēšanai. [..] [I]nformēšana ir nepieciešama, lai ļautu šīm personām to tiesību pārkāpuma gadījumā tostarp īstenot tiesības uz tiesisko aizsardzību un tiesības uz datu aizsardzību saistībā ar to datu apstrādi").

[25] Tāpēc Padomes 2019. gada 21. maija Lēmumā, ar ko pilnvaro sākt sarunas, lai noslēgtu Eiropas Savienības un Amerikas Savienoto Valstu nolīgumu par pārrobežu piekļuvi elektroniskajiem pierādījumiem tiesu iestāžu sadarbībai krimināllietās (9114/19), tā sarunu norādēs ir ietverti vairāki papildu datu aizsardzības pasākumi. It īpaši sarunu norādēs ir noteikts, ka "[n]olīgumam būtu jāpapildina "jumta nolīgums" ar papildu aizsardzības pasākumiem, kuros ņem vērā attiecīgo datu kategoriju sensitivitātes līmeni un unikālās prasības attiecībā uz to, ka elektroniskos pierādījumus nosūta tieši pakalpojumu sniedzēji, nevis iestādes savā starpā, un uz to, ka kompetentās iestādes nosūtīšanu veic tieši pakalpojumu sniedzējiem."

Turklāt saskaņā ar Protokola 14. panta 1. punkta b. apakšpunktu dalībvalstīm būtu jāņem vērā tas, ka attiecībā uz ES dalībvalstīm, kas ir Konvencijas 108+ līgumslēdzējas puses, minētā konvencija pati par sevi nenodrošina pienācīgu pamatu datu pārrobežu nosūtīšanai saskaņā ar Protokolu citām minētās konvencijas pusēm. Šajā sakarībā tām būtu jāņem vērā 14. panta 1. punkta pēdējais teikums Konvencijā 108+[26].

Visbeidzot, attiecībā uz citiem nolīgumiem vai režīmiem saskaņā ar 14. panta 1. punkta c. apakšpunktu dalībvalstīm būtu jāņem vērā, ka tās var balstīties uz šādiem citiem nolīgumiem vai režīmiem tikai tad, ja Eiropas Komisija saskaņā ar Vispārīgās datu aizsardzības regulas (ES) 2016/679 45. pantu vai Tiesībaizsardzības direktīvas (ES) 2016/680 36. pantu par attiecīgo trešo valsti ir pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību, kas attiecas uz attiecīgo datu nosūtīšanu, vai ja šāds cits nolīgums vai režīms pats par sevi nodrošina atbilstošas datu aizsardzības garantijas saskaņā ar Vispārīgās datu aizsardzības regulas 46. pantu vai Tiesībaizsardzības direktīvas 37. panta 1. punkta a. apakšpunktu.

Jāņem vērā ne tikai Savienības tiesību aktu pašreizējā situācija attiecīgajā jomā, bet arī to turpmākās izmaiņas, ciktāl tās ir paredzamas analīzes gaitā. Joma, uz kuru attiecas Protokols, ir tieši saistīta ar paredzamajām Savienības tiesību aktu izmaiņām nākotnē. Šajā sakarībā būtu jāņem vērā Komisijas 2018. gada aprīļa priekšlikumi par pārrobežu piekļuvi elektroniskiem pierādījumiem.[27] Šie instrumenti it īpaši attiecas uz Protokola 6. un 7. pantu.

Komisija, piedaloties sarunās Savienības vārdā, nodrošināja, ka Protokols ir pilnībā saderīgs ar Savienības tiesību aktiem un dalībvalstu pienākumiem saskaņā ar tiem. It īpaši Komisija nodrošināja, ka Protokola noteikumi ļauj dalībvalstīm ievērot ES Līgumos un Pamattiesību hartā nostiprinātās pamattiesības, brīvības un ES tiesību aktu vispārējos principus, tostarp proporcionalitāti, procesuālās tiesības, nevainīguma prezumpciju un personu, pret kurām notiek kriminālprocess, tiesības uz aizstāvību, kā arī privātuma un personas datu un elektroniskās komunikācijas datu aizsardzību, šādiem datiem tiekot apstrādātiem, tostarp kad tos pārsūta tiesībaizsardzības iestādēm valstīs ārpus Eiropas Savienības, un jebkādus pienākumus, kas šajā ziņā ir saistoši tiesībaizsardzības un tiesu iestādēm. Komisija ņēma vērā arī Eiropas Datu aizsardzības uzraudzītāja atzinumu[28] un Eiropas Datu aizsardzības kolēģijas atzinumu[29].

Turklāt Komisija nodrošināja to, ka Protokola noteikumi un Komisijas priekšlikumi par e-pierādījumiem ir saderīgi, arī tāpēc, ka tiesību akta projekts tika izstrādāts diskusijās ar abiem likumdevējiem, un Protokols nerada tiesību normu kolīzijas. It īpaši Komisija nodrošināja, ka Protokols ietver atbilstošas datu aizsardzības un privātuma garantijas, kas ļauj ES pakalpojumu sniedzējiem pildīt savus pienākumus saskaņā ar ES datu aizsardzības un privātuma tiesību aktiem, ciktāl Protokols nodrošina juridisku pamatu datu nosūtīšanai, reaģējot uz iestādes, kura nav Protokola ES līgumslēdzēja puse, izdotiem rīkojumiem vai

---

[26] Sk. arī skaidrojošo ziņojumu Protokolam, ar ko groza Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi, 2018. gada 10. oktobris, 106.–107. punkts.

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

[28] EDAU 2019. gada 2. aprīļa atzinums par dalību sarunās saistībā ar Budapeštas Konvencijas par kibernoziegumiem otro papildprotokolu, Atzinums 3/2019.

[29] Arī "EDAK ieguldījums Eiropas Padomes Konvencijas par kibernoziegumiem (Budapeštas konvencijas) otrā papildu protokola projekta apspriešanā, 13.11.2019."; "Paziņojums 02/201 par jaunu noteikumu projektu Eiropas Padomes Konvencijas par kibernoziegumiem (Budapeštas Konvencija) otrajam papildprotokolam, kas pieņemts 2021. gada 2. februārī"; "EDPB ieguldījums sestajā konsultāciju kārtā par Eiropas Padomes Budapeštas Konvencijas par kibernoziegumiem otrā papildu protokola 2021. gada 4. maija projektu".

pieprasījumiem, kas prasa ES pārzinim vai apstrādātājam izpaust personas datus vai elektroniskās komunikācijas datus.

2.4. Atrunas, deklarācijas, paziņojumi un ziņojumi, un citi apsvērumi

Protokols nodrošina pamatu, lai Puses varētu izmantot konkrētas atrunas un sniegt deklarācijas, paziņojumus vai ziņojumus saistībā ar konkrētiem pantiem. Dalībvalstīm būtu jāizmanto vienota pieeja attiecībā uz konkrētām atrunām un deklarācijām, paziņojumiem un ziņojumiem, kā izklāstīts šā lēmuma pielikumā. Lai nodrošinātu Protokola īstenošanas saderību ar Savienības tiesību aktiem, ES dalībvalstīm attiecībā uz minētajām atrunām un deklarācijām būtu jāieņem turpmāk izklāstītā nostāja. Ja Protokols nodrošina pamatu citām atrunām, deklarācijām, paziņojumiem vai ziņojumiem, šis priekšlikums pilnvaro dalībvalstis apsvērt un izdarīt savas atrunas, sniegt deklarācijas, paziņojumus vai ziņojumus.

Lai nodrošinātu Protokola noteikumu un attiecīgo Savienības tiesību aktu un politikas saderību, dalībvalstīm nevajadzētu izmantot atrunas saskaņā ar 7. panta 9. punkta a.[30] un b.[31] apakšpunktu. Turklāt dalībvalstīm būtu jāsniedz deklarācija saskaņā ar 7. panta 2. punkta b. apakšpunktu[32] un paziņojums saskaņā ar 7. panta 5. punkta a. apakšpunktu[33]. Šo atrunu neesība un deklarācijas iesniegšana, un ziņošana ir svarīga, lai nodrošinātu Protokola saderību ar Komisijas priekšlikumiem par e-pierādījumiem, kā arī pilnveido tiesību aktu priekšlikumus diskusijās ar abiem likumdevējiem.

Turklāt, lai nodrošinātu to, ka ES dalībvalstis, sadarbojoties ar Pusēm, kas nav ES dalībvalstis, Protokolu piemēro vienādi, dalībvalstis tiek mudinātas neizmantot atrunu saskaņā ar 8. panta 13. punktu[34] arī tāpēc, ka šādai atrunai būtu savstarpēja ietekme[35]. Dalībvalstīm būtu jāsniedz deklarācija 8. panta 4. punktā noteiktā deklarācija, lai nodrošinātu, ka rīkojumi var tikt īstenoti, ja ir vajadzīga papildu pamatojoša informācija, piemēram, par konkrētas lietas apstākļiem, lai novērtētu proporcionalitāti un nepieciešamību.[36]

Dalībvalstis tiek arī mudinātas atturēties no deklarācijas sniegšanas saskaņā ar 9. panta 1. punkta b. apakšpunktu[37], lai nodrošinātu Protokola efektīvu piemērošanu.

Lai nodrošinātu Protokola vispārēju efektīvu piemērošanu[38], dalībvalstīm būtu jāsniedz paziņojumi saskaņā ar 7. panta 5. punkta e. apakšpunktu[39], 8. panta10. punkta a. un b. apakšpunktu[40], 14. panta 7. punkta c. apakšpunktu un 10. punkta b. apakšpunktu.

---

[30] Ļaujot Pusēm paturēt tiesības nepiemērot 7. pantu (abonenta datu izpaušana).

[31] Ļaujot Pusēm paturēt tiesības nepiemērot 7. pantu (abonenta datu izpaušana) attiecībā uz noteiktiem piekļuves numuru veidiem, ja šāda izpaušana būtu pretrunā to iekšzemes tiesību sistēmas pamatprincipiem.

[32] Ļaujot Pusēm deklarēt, ka rīkojumu saskaņā ar 7. panta 1. punktu (abonenta datu izpaušana) izdod prokurors vai cita tiesu iestāde vai arī to izdod prokurora vai citas tiesu iestādes uzraudzībā, vai arī to izdod citā neatkarīgā uzraudzībā.

[33] Ļaujot Pusēm paziņot Eiropas Padomes ģenerālsekretāram, ka gadījumos, kad rīkojums saskaņā ar 7. panta 1. punktu (abonenta datu izpaušana) ir izdots pakalpojumu sniedzējam to teritorijā, Puse visos gadījumos vai konkrētos apstākļos pieprasa vienlaicīgu rīkojuma paziņošanu, papildu informāciju un faktu kopsavilkumu saistībā ar izmeklēšanu vai tiesvedību.

[34] Ļaujot Pusēm paturēt tiesības nepiemērot 8. pantu (citas Puses rīkojumu izpilde) datu plūsmas datiem.

[35] Skat. Protokola paskaidrojuma ziņojuma 147 punktu, kurā noteikts, ka "Pusei, kas patur tiesības attiecībā uz šo pantu, nav atļauts iesniegt rīkojumus par datu plūsmu citām Pusēm saskaņā ar [8. panta] 1. punktu".

[36] Ļaujot Pusēm deklarēt, ka ir vajadzīga papildu pamatojoša informācija, lai izpildītu 8. panta 1. punktā minētos rīkojumus (citas Puses rīkojumu izpilde).

[37] Ļaujot Pusēm paziņot, ka tās neizpildīs pieprasījumus, kuri iesniegti saskaņā ar 9. panta 1. punkta a. apakšpunktu (datorizētu datu paātrināta izpaušana ārkārtas situācijā) un kuros prasa izpaust tikai abonenta datus.

Visbeidzot, dalībvalstīm būtu arī jāveic vajadzīgie pasākumi saskaņā ar 14. panta 11. punkta c. apakšpunktu, lai nodrošinātu, ka saņēmēju Pusi nosūtīšanas laikā informē par pienākumu saskaņā ar Savienības tiesību aktiem sniegt paziņojumu personai, uz kuru dati attiecas[41], un par attiecīgo kontaktinformāciju, lai saņēmēja Puse varētu informēt kompetento iestādi ES dalībvalstī, tiklīdz konfidencialitātes ierobežojumi vairs nav piemērojami un var sniegt paziņojumu.

2.5. Priekšlikuma pamatojums

Protokols stāsies spēkā, tiklīdz piecas Puses būs izteikušas piekrišanu uzņemties Protokola saistības saskaņā ar 16. panta 1. un 2. punktu. Ir paredzēts, ka Protokola parakstīšanas ceremonija notiks 2022. gada martā.

ES dalībvalstīm būtu jāveic pasākumi, kas vajadzīgi, lai nodrošinātu ātru Protokola stāšanos spēkā un ratifikāciju, kas ir svarīgi, ņemot vērā vairākus faktorus.

Pirmkārt, Protokols nodrošinās, ka tiesībaizsardzības un tiesu iestādes ir labāk sagatavotas, lai iegūtu elektroniskus pierādījumus, kas nepieciešami kriminālizmeklēšanās. Ņemot vērā elektronisko pierādījumu arvien lielāko nozīmi kriminālizmeklēšanās, ir steidzami nepieciešams, lai tiesībaizsardzības un tiesu iestādēm būtu pareizie instrumenti, ar kuriem efektīvi iegūt piekļuvi elektroniskiem pierādījumiem, lai nodrošinātu, ka tās var efektīvi apkarot noziedzību tiešsaistē.

Otrkārt, Protokols nodrošinās, ka šādi pasākumi, kas paredzēti, lai iegūtu piekļuvi elektroniskiem pierādījumiem, tiks izmantoti tādā veidā, kurš dalībvalstīm ļauj ievērot pamattiesības, arī kriminālprocesuālās tiesības, tiesības uz privātumu un tiesības uz personas datu aizsardzību. Tā kā starptautiskā līmenī nav skaidru noteikumu, pašreizējā prakse var radīt problēmas saistībā ar juridisko noteiktību, pārredzamību, pārskatatbildību un aizdomās turēto pamattiesību un procesuālo garantiju ievērošanu kriminālizmeklēšanās.

Treškārt, protokols atrisinās un novērsīs tiesību normu kolīzijas, kas skar gan iestādes, gan privātā sektora pakalpojumu sniedzējus un citas struktūras, starptautiskā līmenī nodrošinot saderīgus noteikumus par pārrobežu piekļuvi elektroniskiem pierādījumiem.

Ceturtkārt, Protokols apliecinās Konvencijas kā galvenās daudzpusējās sistēmas joprojām svarīgo nozīmi cīņā pret kibernoziedzību. Tas būs ļoti svarīgi procesā, kas seko pēc Apvienoto Nāciju Organizācijas Ģenerālās asamblejas (ANO ĢA) 2019. gada decembra Rezolūcijas 74/247 par vēršanos pret informācijas un komunikācijas tehnoloģiju izmantošanu noziedzīgiem nolūkiem, ar kuru izveidoja atklātu *ad hoc* starpvaldību ekspertu komiteju, lai izstrādātu visaptverošu starptautisku konvenciju par vēršanos pret informācijas un komunikācijas tehnoloģiju izmantošanu noziedzīgiem nolūkiem.

---

[38] Ļaujot Pusēm paziņot iestādi vai iestādes, kuras attiecīgi būtu jāinformē drošības incidenta gadījumā vai ar kurām būtu jāsazinās, lai saņemtu iepriekšēju atļauju tālākas nosūtīšanas uz citu valsti vai starptautisku organizāciju gadījumā.

[39] Ļaujot Pusēm paziņot tās iestādes kontaktinformāciju, kuru tās nozīmē saņemt paziņojumus saskaņā ar 7. panta 5. punkta a. apakšpunktu un veikt 7. panta 5. punkta b., c. un d. apakšpunktā aprakstītās darbības (abonenta datu izpaušana).

[40] Ļaujot Pusēm paziņot to iestāžu kontaktinformāciju, kuras nozīmētas saņemt un iesniegt rīkojumus 8. pantā minētos rīkojumus (citas Puses rīkojumu izpilde). Atbilstīgi Regulā (ES) 2017/1939 noteiktajām prasībām dalībvalstis, kuras piedalās ciešākā sadarbībā Eiropas Prokuratūras (*EPPO*) izveidei, saziņā iekļauj *EPPO*.

[41] Sk. iepriekš 24. zemsvītras piezīmi.

3. JURIDISKAIS PAMATS, SUBSIDIARITĀTE UN PROPORCIONALITĀTE

- *Juridiskais pamats*

Savienības kompetence pieņemt tiesību aktus jautājumos par tiesu vai līdzvērtīgu iestāžu sadarbības veicināšanu tiesvedībā krimināllietās un lēmumu izpildi ir balstīta uz LESD 82. panta 1. punktu. Savienības kompetence jautājumos par personas datu aizsardzību ir balstīta uz LESD 16. pantu.

Saskaņā ar LESD 3. panta 2. punktu Savienības ekskluzīvā kompetencē ir noslēgt starptautisku līgumu tiktāl, ciktāl līguma slēgšana ietekmē Savienības kopīgos noteikumus vai maina to darbības jomu. Protokola noteikumi ietilpst jomā, uz kuru lielā mērā attiecas iepriekš 2.3. iedaļā izklāstītie kopīgie noteikumi.

Tādējādi Protokols ir Savienības ekskluzīvā ārējā kompetencē. Tādējādi dalībvalstis var ratificēt Protokolu Savienības interesēs, pamatojoties uz LESD 16. pantu, 82. panta 1. punktu un 218. panta 6. punktu.

- *Subsidiaritāte (neekskluzīvas kompetences gadījumā)*

Neattiecas.

- *Proporcionalitāte*

Ar šo priekšlikumu izvirzītos Savienības mērķus, kas izklāstīti 2.5. iedaļā, var sasniegt, tikai noslēdzot saistošu starptautisku nolīgumu, kurā paredz vajadzīgos sadarbības pasākumus un vienlaikus nodrošina pamattiesību pienācīgu aizsardzību. Protokols šo mērķi sasniedz. Protokola noteikumi ietver tikai to, kas nepieciešams tā galveno mērķu sasniegšanai. Vienpusēja rīcība nav alternatīva, jo tā nesniegtu pietiekamu pamatu sadarbībai ar valstīm, kas nav ES dalībvalstis, un nevarētu nodrošināt pamattiesību nepieciešamo aizsardzību. Turklāt tāda daudzpusēja nolīguma kā Protokols, par kuru Savienība spēja risināt sarunas, ievērošana ir efektīvāka nekā divpusēju sarunu sākšana ar atsevišķām valstīm, kas nav ES dalībvalstis. Pieņemot, ka visas 66 Konvencijas Puses un nākamās jaunās Puses Protokolu ratificēs, Protokols nodrošinās kopēju tiesisko regulējumu ES dalībvalstu sadarbībai ar svarīgākajiem starptautiskajiem partneriem cīņā pret noziedzību.

- ***Juridiskā instrumenta izvēle***

Neattiecas.

4. *EX POST* IZVĒRTĒJUMU, APSPRIEŠANOS AR IEINTERESĒTAJĀM PERSONĀM UN IETEKMES NOVĒRTĒJUMU REZULTĀTI

- Ex post *izvērtējumi / spēkā esošo tiesību aktu atbilstības pārbaudes*

Neattiecas.

- *Apspriešanās ar ieinteresētajām personām*

Eiropas Padome rīkoja sešas sabiedriskās apspriešanas kārtas saistībā ar Protokola sarunām, proti, 2018. gada jūlijā un novembrī, 2019. gada februārī un novembrī, 2020. gada decembrī un 2021. gada maijā.[42] Puses ņēma vērā šo apspriešanos gaitā saņemto informāciju.

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

Komisija kā sarunu vadītāja Savienības vārdā arī apmainījās viedokļiem ar datu aizsardzības iestādēm un 2019. un 2021. gadā organizēja mērķorientētas apspriešanās sanāksmes ar pilsoniskās sabiedrības organizācijām, pakalpojumu sniedzējiem un arodasociācijām. Komisija ņēma vērā šīs viedokļu apmaiņas gaitā saņemto informāciju.

- *Ekspertu atzinumu pieprasīšana un izmantošana*

Sarunu gaitā Komisija pastāvīgi apspriedās ar Padomes īpašo komiteju sarunām saskaņā ar Eiropas Savienības Padomes 2019. gada 6. jūnija lēmumu, ar ko Komisija tika pilnvarota Savienības vārdā piedalīties sarunās, un tas deva iespēju dalībvalstu ekspertiem dot ieguldījumu Savienības nostājas izstrādāšanas procesā. Vairāki dalībvalstu eksperti arī piedalījās sarunās paralēli Komisijai, kas piedalījās Savienības vārdā. Notika arī apspriešanās ar ieinteresētajām personām (sk. iepriekš).

- *Ietekmes novērtējums*

Ietekmes novērtējumu veica 2017.–2018. gadā, lai papildinātu Komisijas priekšlikumus par e-pierādījumiem.[43] Šajā sakarībā sarunas par nolīgumu par Budapeštas Konvencijas par kibernoziegumiem otro papildu protokolu bija vēlamā risinājuma daļa. Turklāt attiecīgā ietekme ir izklāstīta šajā paskaidrojuma rakstā.

- *Normatīvā atbilstība un vienkāršošana*

Protokols var ietekmēt konkrētas pakalpojumu sniedzēju kategorijas, arī mazos un vidējos uzņēmumus (MVU), jo saskaņā ar Protokolu uz tiem var attiekties pieprasījumi un rīkojumi par elektroniskiem pierādījumiem. Tomēr šie pakalpojumu sniedzēji bieži vien jau tagad saņem šādus pieprasījumus, kas nosūtīti, izmantojot citus pastāvošos kanālus, dažkārt ar dažādu iestāžu starpniecību, kā arī pamatojoties uz Konvenciju[44], citiem savstarpējās tiesiskās palīdzības līgumiem vai citiem regulējumiem, arī vairāku ieinteresēto personu politiku interneta pārvaldības jomā.[45] Turklāt pakalpojumu sniedzēji, arī MVU, gūs labumu no starptautiskā līmenī pastāvoša skaidra tiesiskā regulējuma un no visu Protokola pušu vienotas pieejas.

- *Pamattiesības*

Protokolā paredzētie sadarbības instrumenti var ietekmēt pamattiesības gadījumos, kad personas datus var iegūt kriminālprocesa ietvaros, t. sk., piemēram, tiesības uz taisnīgu tiesu, tiesības uz privātumu un tiesības uz personas datu aizsardzību. Protokolā ievēro tiesībām balstītu pieeju un paredz noteikumus un garantijas saskaņā ar starptautiskajiem cilvēktiesību instrumentiem, t. sk. Eiropas Padomes 1950. gada Cilvēktiesību un pamatbrīvību aizsardzības konvenciju. Protokols it īpaši paredz īpašas datu aizsardzības garantijas. Vajadzības gadījumā Protokols arī nodrošina pamatu, lai Puses varētu izdarīt konkrētas atrunas, sniegt deklarācijas vai paziņojumus, un tajā ietver pamatojumus sadarbības atteikšanai, atbildot uz pieprasījumu īpašās situācijās. Tas nodrošina Protokola saderību ar ES Pamattiesību hartu.

---

[43] SWD(2018) 118 final.

[44] Sk., piemēram, Konvencijas par kibernoziegumiem komitejas 2017. gada 1. marta norādījumus Nr. 10 par abonenta informācijas sniegšanas rīkojumiem (Budapeštas konvencijas 18. pants).

[45] Sk., piemēram, Piešķirto nosaukumu un numuru interneta kooperācijas valdes (*ICANN*) 2019. gada 15. maija rezolūciju par ieteikumiem par Pagaidu specifikāciju *gTLD* reģistrācijas datiem, kas pieejama tīmekļa vietnē www.icann.org.

5. IETEKME UZ BUDŽETU

Šis priekšlikums neietekmē Savienības budžetu. Saistībā ar Protokola īstenošanu dalībvalstīm var rasties vienreizējas izmaksas, un dalībvalstu iestādēm varētu rasties lielākas izmaksas paredzamā gadījumu skaita pieauguma dēļ.

6. CITI ELEMENTI

- *Īstenošanas plāni un uzraudzīšanas, izvērtēšanas un ziņošanas kārtība*

Īstenošanas plāns nepastāv, jo pēc Protokola parakstīšanas un ratifikācijas dalībvalstīm tas būs jāīsteno.

Attiecībā uz uzraudzību Komisija piedalīsies Konvencijas par kibernoziegumiem komitejas sanāksmēs, kurā Eiropas Savienība ir atzīta par novērotājorganizāciju.

2021/0383 (NLE)

Priekšlikums

PADOMES LĒMUMS,

ar kuru dalībvalstīm atļauj Eiropas Savienības interesēs ratificēt Konvencijas par kibernoziegumiem otro papildu protokolu par pastiprinātu sadarbību un elektronisko pierādījumu izpaušanu

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 16., 82. panta 1. punktu un 218. panta 6. punktu,

ņemot vērā Eiropas Komisijas priekšlikumu,

ņemot vērā Eiropas Parlamenta piekrišanu,

tā kā:

(1) Padome 2019. gada 9. jūnijā pilnvaroja Komisiju Savienības vārdā piedalīties sarunās par Eiropas Padomes Budapeštas konvencijas par kibernoziegumiem otro papildu protokolu.

(2) Eiropas Padomes Ministru komiteja 2021. gada 17. novembrī pieņēma Konvencijas par kibernoziegumiem otrā papildu protokola par pastiprinātu sadarbību un elektronisko pierādījumu izpaušanu (“Protokols”) tekstu, un to ir paredzēts atvērt parakstīšanai 2022. gada martā.

(3) Protokola noteikumi ietilpst jomā, uz kuru lielā mērā attiecas kopīgi noteikumi LESD 3. panta 2. punkta nozīmē, t. sk. instrumenti, kas veicina tiesu iestāžu sadarbību krimināllietās, nodrošina minimālos procesuālo tiesību standartus, kā arī datu aizsardzību un privātuma aizsardzību.

(4) Komisija arī iesniedza tiesību aktu priekšlikumus Regulai par Eiropas elektronisko pierādījumu sniegšanas un saglabāšanas rīkojumiem elektronisko pierādījumu gūšanai krimināllietās (COM(2018) 225 final) un Direktīvai, ar ko paredz saskaņotus noteikumus juridisko pārstāvju iecelšanai ar mērķi iegūt pierādījumus kriminālprocesā (COM(2018) 226 final), ar tiem tiek ieviesti saistoši pārrobežu Eiropas e-pierādījumu sniegšanas un saglabāšanas rīkojumi, kas ir tieši adresējami pakalpojumu sniedzēja pārstāvim citā dalībvalstī.

(5) Komisija, piedaloties sarunās Savienības vārdā, nodrošināja otrā papildu protokola saderību ar attiecīgajiem kopīgajiem Eiropas Savienības noteikumiem.

(6) Vairākas atrunas, deklarācijas, paziņojumi un ziņojumi ir būtiski, lai nodrošinātu Protokola saderību ar Savienības tiesību aktiem un politiku, kā arī Protokola vienādu piemērošanu ES dalībvalstu attiecībās ar valstīm, kas nav ES dalībvalstis, un Protokola efektīvu piemērošanu.

(7) Ņemot vērā to, ka Protokols paredz ātras procedūras, kas uzlabo pārrobežu piekļuvi elektroniskiem pierādījumiem un augsta līmeņa garantijas, tā stāšanās spēkā palīdzēs sekmēt cīņu pret kibernoziedzību un citiem noziedzības veidiem pasaules mērogā, šādi veicinot sadarbību starp ES dalībvalstīm, kuras ir Protokola Puses, un Protokola

Pusēm, kas nav ES dalībvalstis, nodrošinās personu augsta līmeņa aizsardzību un risinās tiesību normu kolīzijas.

(8) Ņemot vērā to, ka Protokols paredz atbilstošas garantijas saskaņā ar prasībām par personas datu starptautisku nosūtīšanu saskaņā ar Regulu (ES) 2016/679 un Direktīvu (ES) 2016/680, tā stāšanās spēkā palīdzēs veicināt Savienības datu aizsardzības standartus pasaules mērogā, atvieglos datu plūsmas starp ES dalībvalstīm, kuras ir Protokola Puses, un Protokola Pusēm, kas nav ES dalībvalstis, un nodrošinās, ka ES dalībvalstis pilda savus pienākumus saskaņā ar Savienības datu aizsardzības noteikumiem.

(9) Turklāt drīzā stāšanās spēkā arī apstiprinās Eiropas Padomes Budapeštas Konvencijas kā galvenās daudzpusējās sistēmas pozīciju cīņā pret kibernoziedzību.

(10) Eiropas Savienība nevar kļūt par Protokola pusi, jo gan Protokols, gan Eiropas Padomes Konvencija par kibernoziegumiem ir atvērta tikai valstīm.

(11) Tāpēc būtu jāatļauj dalībvalstīm ratificēt Protokolu, kopīgi rīkojoties Eiropas Savienības interesēs.

(12) Saskaņā ar Eiropas Parlamenta un Padomes Regulas (ES) 2018/1725 42. panta 1. punktu ir notikusi apspriešanās ar Eiropas Datu aizsardzības uzraudzītāju, kas [...] sniedza atzinumu.

(13) [Saskaņā ar 1. un 2. pantu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, un neskarot minētā protokola 4. pantu, Īrija nepiedalās šā lēmuma pieņemšanā, un šis lēmums tai nav saistošs un nav jāpiemēro.]

[VAI]

[Saskaņā ar 1. un 2. pantu Protokolā Nr. 21 par Apvienotās Karalistes un Īrijas nostāju saistībā ar brīvības, drošības un tiesiskuma telpu, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, un neskarot minētā protokola 4. pantu, Īrija [… vēstulē] ir paziņojusi, ka vēlas piedalīties šā lēmuma pieņemšanā un piemērošanā.]

(14) Saskaņā ar 1. un 2. pantu Protokolā Nr. 22 par Dānijas nostāju, kas pievienots Līgumam par Eiropas Savienību un Līgumam par Eiropas Savienības darbību, Dānija nepiedalās šā lēmuma pieņemšanā, un Dānijai šis lēmums nav saistošs un nav jāpiemēro,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Ar šo dalībvalstis ir pilnvarotas Eiropas Savienības interesēs ratificēt Konvencijas par kibernoziegumiem otro papildu protokolu par pastiprinātu sadarbību un elektronisko pierādījumu izpaušanu (“Protokols”).

2. pants

Ratificējot Protokolu, dalībvalstis izdara atrunas, sniedz deklarācijas, paziņojumus vai ziņojumus, kas izklāstīti pielikumā.

3. pants

Šis lēmums stājas spēkā tā pieņemšanas dienā.

4. pants

Šo lēmumu publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

5. pants

Šis lēmums ir adresēts dalībvalstīm.

Briselē,

Padomes vārdā –
priekšsēdētājs