EUROPSKA
KOMISIJA

Bruxelles, 25.11.2021.
COM(2021) 719 final

2021/0383 (NLE)

Prijedlog

ODLUKE VIJEĆA

o ovlašćivanju država članica da u interesu Europske unije ratificiraju Drugi dodatni protokol uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza

OBRAZLOŽENJE

1. PREDMET PRIJEDLOGA

Ovaj Prijedlog odnosi se na odluku o ovlašćivanju država članica da u interesu Europske unije ratificiraju Drugi dodatni protokol o pojačanoj suradnji i otkrivanju elektroničkih dokaza uz Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu („Protokol”).[1] Cilj je Protokola osigurati zajednička pravila na međunarodnoj razini radi poboljšanja suradnje u području kiberkriminaliteta i prikupljanja dokaza u elektroničkom obliku za kaznene istrage ili postupke.

Ovim Prijedlogom dopunjuje se zasebni Komisijin prijedlog odluke Vijeća Europske unije („Vijeće”) kojom se države članice ovlašćuju za potpisivanje Protokola u interesu Europske unije.

Kiberkriminalitet i dalje je velik problem za naše društvo. Bez obzira na trud koji tijela kaznenog progona i pravosudna tijela ulažu kako bi suzbila kibernapade, oni su zajedno s napadima ucjenjivačkim softverom sve učestaliji i postaju sve složeniji.[2] Konkretno, s obzirom na to da internet nema granica, istrage kiberkriminaliteta gotovo uvijek su prekogranične prirode, zbog čega je potrebna bliska suradnja među tijelima u različitim zemljama.

Elektronički dokazi sve su važniji za kaznene istrage. Komisija procjenjuje da tijela kaznenog progona i pravosudna tijela danas trebaju pristup elektroničkim dokazima u 85 % kaznenih istraga, uključujući kiberkriminalitet.[3] Pružatelji usluga u stranim jurisdikcijama sve više čuvaju dokaze o svakom kaznenom djelu u elektroničkom obliku, a za učinkovit kaznenopravni odgovor potrebne su odgovarajuće mjere za pribavljanje takvih dokaza kako bi se poštovala vladavina prava.

Ulaže se trud u poboljšanje prekograničnog pristupa elektroničkim dokazima za kaznene istrage na globalnoj i nacionalnoj razini, na razini Europske unije[4] i na međunarodnoj razini, među ostalim putem Protokola. Važno je osigurati usklađena pravila na međunarodnoj razini kako bi se izbjegli sukobi zakona kad se traži prekogranični pristup elektroničkim dokazima.

2. KONTEKST PRIJEDLOGA

2.1. Kontekst

Cilj je Budimpeštanske konvencije Vijeća Europe o kibernetičkom kriminalu (CETS br. 185) („Konvencija”) olakšati borbu protiv kaznenih djela u kojima se koriste računalne mreže. Ona sadržava (1.) odredbe kojima se usklađuju elementi nacionalnog kaznenog materijalnog prava u području kaznenih djela i povezane odredbe u području kiberkriminaliteta, (2.) u njoj se predviđaju ovlasti nacionalnog kaznenog postupovnog prava potrebne za istragu i progon takvih kaznenih djela, kao i drugih kaznenih djela počinjenih putem računalnog sustava ili za koja postoje dokazi u elektroničkom obliku te (3.) joj je cilj uspostaviti brz i učinkovit sustav međunarodne suradnje.

---

1 Tekst Protokola priložen je ovom Prijedlogu.
2 Procjena prijetnje teškog i organiziranog kriminala u Europskoj uniji za 2021. (EU SOCTA 2021.).
3 SWD(2018) 118 final.
4 COM(2018) 225 i 226 final.

Konvencija je otvorena državama članicama Vijeća Europe i zemljama koje nisu članice Vijeća Europe na poziv. Trenutačno Konvencija ima 66 zemalja stranaka, uključujući 26 država članica Europske unije.[5] Konvencijom se ne predviđa pristupanje Europske unije Konvenciji. Međutim, Europska unija priznata je kao promatračka organizacija Odbora za Konvenciju o kibernetičkom kriminalu (T-CY).[6]

Bez obzira na nastojanja da se pregovori o novoj konvenciji o kibernetičkom kriminalu odvijaju na razini Ujedinjenih naroda[7], Budimpeštanska konvencija i dalje je glavna multilateralna konvencija za borbu protiv kiberkriminaliteta. Unija dosljedno podupire Konvenciju[8], među ostalim i u okviru financiranja programa izgradnje kapaciteta.[9]

Nakon prijedloga radne skupine za pristup dokazima koji se nalaze u oblaku[10] Odbor za Konvenciju o kibernetičkom kriminalu donio je nekoliko preporuka za rješavanje problema, među ostalim i u okviru pregovora o Drugom dodatnom protokolu uz Konvenciju o kibernetičkom kriminalu o pojačanoj međunarodnoj suradnji, koji se odnose na to da se dokazi o kiberkriminalitetu i drugim kaznenim djelima sve češće nalaze kod pružatelja usluga u stranim jurisdikcijama, dok su ovlasti tijela kaznenog progona i dalje teritorijalno ograničene. U lipnju 2017. Odbor za Konvenciju o kibernetičkom kriminalu odobrio je mandat za pripremu Drugog dodatnog protokola u razdoblju od rujna 2017. do prosinca 2019.[11] S obzirom na to da je potrebno više vremena za dovršetak rasprava te uzimajući u obzir ograničenja uzrokovana pandemijom bolesti COVID-19 u 2020. i 2021., Odbor za Konvenciju o kibernetičkom kriminalu dvaput je naknadno produljio mandat, do prosinca 2020., odnosno do svibnja 2021.

Nakon poziva Europskog vijeća u zaključcima od 18. listopada 2018.[12] Komisija je 5. veljače 2019. donijela Preporuku za odluku Vijeća kojom se Komisija ovlašćuje za sudjelovanje, u ime Europske unije, u pregovorima o Drugom dodatnom protokolu uz Konvenciju Vijeća Europe o kibernetičkom kriminalu.[13] Europski nadzornik za zaštitu podataka dao je 2. travnja 2019. mišljenje o Preporuci.[14] Odlukom od 6. lipnja 2019. Vijeće Europske unije ovlastilo je Komisiju da u ime Europske unije sudjeluje u pregovorima o Drugom dodatnom protokolu.[15]

---

5 Sve države članice EU-a osim Irske, koja je potpisala, ali nije ratificirala Konvenciju, no ipak se obvezala na pristupanje.

6 Poslovnik Odbora za Konvenciju o kibernetičkom kriminalu (T-CY (2013)25 rev), dostupan na www.coe.int/cybercrime.

7 Rezolucija Opće skupštine Ujedinjenih naroda (UNGA) 74/247 o borbi protiv uporabe informacijskih i komunikacijskih tehnologija u kriminalne svrhe, prosinac 2019.

8 JOIN(2020) 81 final.

9 Vidjeti na primjer Prošireno globalno djelovanje protiv kiberkriminaliteta (GLACY)+, na https://www.coe.int/en/web/cybercrime/glacyplus.

10 Završno izvješće radne skupine za pristup dokazima koji se nalaze u oblaku Odbora za Konvenciju o kibernetičkom kriminalu pod nazivom „Pristup kaznenog pravosuđa elektroničkim dokazima u oblaku: preporuke za razmatranje T-CY-a” od 16. rujna 2016.

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

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

13 COM(2019) 71 final.

14 Mišljenje EDPS-a o sudjelovanju u pregovorima s obzirom na Drugi dodatni protokol uz Budimpeštansku konvenciju o kibernetičkom kriminalu od 2. travnja 2019., Mišljenje 3/2019.

15 Odluka Vijeća s oznakom 9116/19.

Kako je navedeno u strategiji EU-a za sigurnosnu uniju iz 2020.[16], strategiji EU-a za kibersigurnost za digitalno desetljeće iz 2020.[17] i strategiji EU-a za borbu protiv organiziranog kriminala iz 2021.[18], Komisija predano radi na brzom i uspješnom završetku pregovora o Protokolu. I Europski parlament prepoznao je potrebu za dovršenjem rada na Protokolu u svojoj Rezoluciji iz 2021. o strategiji EU-a za kibersigurnost za digitalno desetljeće.[19]

Komisija je u ime Europske unije sudjelovala u pregovorima o Protokolu u skladu s Odlukom Vijeća Europske unije. Komisija se dosljedno savjetovala s posebnim odborom Vijeća za pregovore o stajalištu Unije.

U skladu s Okvirnim sporazumom o odnosima Europskog parlamenta i Europske komisije[20], Komisija je i putem pisanih izvješća i usmenih prezentacija obavješćivala Europski parlament o pregovorima.

Na plenarnoj sjednici Odbora za Konvenciju o kibernetičkom kriminalu 28. svibnja 2021. Odbor za Konvenciju o kibernetičkom kriminalu odobrio je nacrt Protokola na svojoj razini i proslijedio ga Odboru ministara Vijeća Europe na donošenje.[21] Odbor ministara Vijeća Europe donio je Protokol 17. studenoga 2021.

2.2. Drugi dodatni protokol

Cilj je Protokola poboljšati suradnju u području kiberkriminaliteta i prikupljanja dokaza u elektroničkom obliku o kaznenom djelu za potrebe posebnih kaznenih istraga ili postupaka. Protokolom se prepoznaje potreba za povećanom i učinkovitijom suradnjom među državama i s privatnim sektorom te za većom jasnoćom i pravnom sigurnošću za pružatelje usluga i druge subjekte u pogledu okolnosti u kojima oni mogu odgovoriti na zahtjeve tijela kaznenog pravosuđa drugih stranaka za otkrivanje elektroničkih dokaza.

Protokolom se osim toga prepoznaje da su za učinkovitu prekograničnu suradnju za potrebe kaznenog pravosuđa, među ostalim između tijela javnog sektora i subjekata iz privatnog sektora, potrebni dobri uvjeti i pouzdane mjere za zaštitu temeljnih prava. U tu svrhu Protokol slijedi pristup temeljen na pravima i predviđa uvjete i zaštitne mjere u skladu s međunarodnim instrumentima za ljudska prava, uključujući Konvenciju Vijeća Europe za zaštitu ljudskih prava i temeljnih sloboda iz 1950. Budući da se elektronički dokazi često odnose na osobne podatke, Protokol uključuje i pouzdane mjere za zaštitu privatnosti i osobnih podataka.

Odredbe iz sljedećih odjeljaka od posebne su važnosti za Protokol. Protokolu je priloženo detaljno izvješće s objašnjenjima. Iako izvješće s objašnjenjima ne predstavlja instrument za vjerodostojno tumačenje Protokola, svrha mu je „ponuditi strankama smjernice i pomoć” u primjeni Protokola.[22]

---

16 COM(2020) 605 final.
17 JOIN(2020) 81 final.
18 COM(2021) 170 final.
19 Rezolucija Europskog parlamenta od 10. lipnja 2021. o strategiji EU-a za kibersigurnost za digitalno desetljeće.
20 Referentna oznaka L 304/47.
21 https://rm.coe.int/0900001680a2aa42
22 Vidjeti stavak 2. izvješća s objašnjenjima uz Protokol.

2.2.1. Zajedničke odredbe

U poglavlju I. Protokola predviđene su zajedničke odredbe. Člankom 2. utvrđuje se područje primjene Protokola u skladu s područjem primjene Konvencije: primjenjuje se na posebne kaznene istrage ili postupke koji se odnose na kaznena djela povezana s računalnim sustavima i podacima te na prikupljanje dokaza o kaznenom djelu u elektroničkom obliku.

U članku 3. navedene su definicije za „središnja tijela”, „nadležna tijela”, „hitne situacije”, „osobne podatke” i „stranke koje prenose podatke”. Te se definicije primjenjuju na Protokol, zajedno s definicijama uključenima u Konvenciju.

Člankom 4. utvrđuju se jezici na kojima stranke trebaju dostavljati naloge, zahtjeve ili obavijesti u skladu s Protokolom.

2.2.2. Mjere suradnje

U poglavlju II. Protokola predviđene su mjere za poboljšanje suradnje. Prvo, člankom 5. stavkom 1. utvrđuje se da stranke surađuju na temelju Protokola u najvećoj mogućoj mjeri. Člankom 5. stavcima od 2. do 5. utvrđuje se primjena mjera Protokola u odnosu na postojeće ugovore ili dogovore o uzajamnoj pomoći. Člankom 5. stavkom 7. utvrđuje se da mjere iz poglavlja II. ne ograničavaju suradnju između stranaka ili s pružateljima usluga ili subjektima u okviru drugih primjenjivih sporazuma, dogovora, praksi ili nacionalnog prava.

Člankom 6. osigurava se osnova za izravnu suradnju između nadležnih tijela jedne stranke i subjekata koji pružaju usluge registracije naziva domene u drugoj stranci radi otkrivanja podataka o registraciji naziva domene.

Člankom 7. osigurava se osnova za izravnu suradnju između nadležnih tijela jedne stranke i pružatelja usluga u drugoj stranci radi otkrivanja podataka o pretplatnicima.

Člankom 8. osigurava se osnova za pojačanu suradnju među tijelima u otkrivanju računalnih podataka.

Člankom 9. osigurava se osnova za suradnju među tijelima u otkrivanju računalnih podataka u hitnim situacijama.

Člankom 10. pruža se osnova za uzajamnu pravnu pomoć u hitnim situacijama.

Člankom 11. pruža se osnova za suradnju putem videokonferencije.

Člankom 12. pruža se osnova za zajedničke istrage i zajedničke istražne timove.

2.2.3. Zaštitne mjere

Protokol slijedi pristup temeljen na pravima s posebnim uvjetima i zaštitnim mjerama, od kojih su neke uključene u posebne mjere suradnje, kao i u poglavlje III. Protokola. Člankom 13. Protokola od stranaka se zahtijeva da osiguraju da ovlasti i postupci podliježu odgovarajućoj razini zaštite temeljnih prava, čime se, u skladu s člankom 15. Konvencije, osigurava primjena načela proporcionalnosti.

Člankom 14. Protokola predviđa se zaštita osobnih podataka kako je definirana u članku 3. Protokola u skladu s Protokolom o izmjeni uz Konvenciju o zaštiti pojedinaca u vezi s obradom osobnih podataka (CETS 223) (Konvencija 108+) i pravom Unije.

Na temelju toga, u članku 14. stavcima od 2. do 15. utvrđuju se temeljna načela zaštite podataka, uključujući ograničenje svrhe, pravnu osnovu, kvalitetu podataka i pravila koja se primjenjuju na obradu posebnih kategorija podataka, obveze koje se primjenjuju na voditelje obrade, među ostalim u pogledu zadržavanja, vođenja evidencije, sigurnosti i u pogledu daljnjih prijenosa, izvršiva prava pojedinaca, među ostalim na obavješćivanje, pristup, ispravljanje i automatizirano donošenje odluka, neovisni i učinkoviti nadzor jednog ili više tijela te administrativnu i sudsku zaštitu. Zaštitne mjere obuhvaćaju sve oblike suradnje utvrđene u Protokolu, uz prilagodbe prema potrebi kako bi se uzele u obzir posebne značajke izravne suradnje (npr. u kontekstu obavješćivanja o povredi). Ostvarivanje određenih prava pojedinaca može se odgoditi, ograničiti ili odbiti ako je to potrebno i razmjerno radi ostvarivanja važnih ciljeva od javnog interesa, posebno radi sprečavanja rizika za istrage kaznenog progona koje su u tijeku, što je isto tako u skladu s pravom Unije.

Članak 14. Protokola trebalo bi tumačiti i u vezi s člankom 23. Protokola. Člankom 23. jača se učinkovitost zaštitnih mjera iz Protokola tako što se predviđa da će Odbor za Konvenciju o kibernetičkom kriminalu procijeniti provedbu i primjenu mjera poduzetih u nacionalnom zakonodavstvu kako bi se provele odredbe Protokola. Konkretno, u članku 23. stavku 3. izričito se potvrđuje da će se provedba članka 14. od strane stranaka procjenjivati nakon što deset stranaka Konvencije izrazi svoj pristanak da budu obvezane Protokolom.

Kao dodatnu zaštitnu mjeru, u skladu s člankom 14. stavkom 15., ako stranka ima bitne dokaze da druga stranka sustavno ili materijalno krši zaštitne mjere utvrđene Protokolom, može nakon savjetovanja (što nije potrebno u hitnom slučaju) suspendirati prijenos osobnih podataka toj stranci. Osobni podaci preneseni prije suspenzije i dalje se obrađuju u skladu s Protokolom.

Naposljetku, s obzirom na multilateralnu narav Protokola, člankom 14. stavkom 1. točkama (b) i (c) Protokola strankama se omogućuje da se u svojim bilateralnim odnosima pod određenim uvjetima dogovore o alternativnim načinima osiguravanja zaštite osobnih podataka koji se prenose na temelju Protokola. Iako se zaštitne mjere iz članka 14. stavaka od 2. do 15. automatski primjenjuju na stranke koje primaju osobne podatke, na temelju članka 14. stavka 1. točke (b), stranke koje su uzajamno obvezane međunarodnim sporazumom o uspostavi sveobuhvatnog okvira za zaštitu osobnih podataka u skladu s primjenjivim zahtjevima zakonodavstva predmetnih stranaka također se mogu osloniti na taj okvir. To se primjerice odnosi na Konvenciju 108+ (za one stranke koje dopuštaju prijenos podataka drugim strankama u skladu s tom konvencijom) ili Krovni sporazum između EU-a i SAD-a (u okviru njegova područja primjene, tj. za prijenos osobnih podataka između nadležnih tijela i, u kombinaciji s posebnim dogovorom o prijenosu između SAD-a i EU-a, za izravnu suradnju između nadležnih tijela i pružatelja usluga). Osim toga, na temelju članka 14. stavka 1. točke (c), stranke mogu i uzajamno odrediti da se prijenos osobnih podataka izvršava na temelju drugih sporazuma ili dogovora između predmetnih stranaka. Kad je riječ o državama članicama EU-a, takav alternativni sporazum ili dogovor može se upotrijebiti samo za prijenose podataka na temelju Protokola ako su ti prijenosi u skladu sa zahtjevima prava Unije o zaštiti podataka, odnosno poglavlja V. Direktive (EU) 2016/680 (Direktiva o zaštiti podataka za potrebe kaznenog progona) i (za izravnu suradnju između tijela i pružatelja usluga na temelju članaka 6. i 7. Protokola) poglavlja V. Uredbe (EU) 2016/679 (Opća uredba o zaštiti podataka).

2.2.4. Završne odredbe

U poglavlju IV. Protokola predviđene su završne odredbe. Među ostalim, člankom 15. stavkom 1. točkom (a) osigurava se da stranke mogu urediti svoje odnose u pogledu pitanja

navedenih u Protokolu drukčije, u skladu s člankom 39. stavkom 2. Konvencije. Člankom 15. stavkom 1. točkom (b) osigurava se da države članice EU-a koje su stranke Protokola mogu nastaviti primjenjivati pravo Unije u svojim međusobnim odnosima. Člankom 15. stavkom 2. utvrđuje se i da se članak 39. stavak 3. Konvencije primjenjuje na Protokol.

U članku 16. stavku 3. navodi se da će Protokol stupiti na snagu nakon što pet stranaka Konvencije izrazi suglasnost da budu obvezane Protokolom.

Člankom 19. stavkom 1. predviđa se da stranke mogu koristiti rezerve u vezi s člankom 7. stavkom 9. točkama (a) i (b), člankom 8. stavkom 13. i člankom 17. Člankom 19. stavkom 2. predviđa se da stranke mogu davati izjave u vezi s člankom 7. stavkom 2. točkom (b) i stavkom 8., člankom 8. stavkom 11., člankom 9. stavkom 1. točkom (b) i stavkom 5., člankom 10. stavkom 9., člankom 12. stavkom 3. i člankom 18. stavkom 2. Člankom 19. stavkom 3. utvrđuje se da stranka daje izjave, obavijesti ili priopćenja iz članka 7. stavka 5. točaka (a) i (e), članka 8. stavka 4. i stavka 10. točaka (a) i (b), članka 14. stavka 7. točke (c) i stavka 10. točke (b) te članka 17. stavka 2.

Člankom 23. stavkom 1. pruža se osnova za savjetovanje među strankama, među ostalim u okviru Odbora za Konvenciju o kibernetičkom kriminalu, u skladu s člankom 46. Konvencije. Osim toga, člankom 23. stavkom 2. pruža se osnova za procjenu primjene i provedbe odredaba Protokola. Člankom 23. stavkom 3. osigurava se da procjena primjene i provedbe članka 14. o zaštiti podataka počinje nakon što deset stranaka izrazi suglasnost da budu obvezane Protokolom.

2.3. Pravo i politika Unije u tom području

Područje uređeno Protokolom u velikoj je mjeri obuhvaćeno zajedničkim pravilima koja se temelje na članku 82. stavku 1. i članku 16. UFEU-a. Trenutačni pravni okvir Europske unije posebno uključuje instrumente o izvršavanju zakonodavstva i pravosudnoj suradnji u kaznenim stvarima, kao što su Direktiva 2014/41/EU o Europskom istražnom nalogu u kaznenim stvarima, Konvencija o uzajamnoj pomoći u kaznenim stvarima među državama članicama Europske unije i Okvirna odluka Vijeća 2002/465/PUP o zajedničkim istražnim timovima. Na vanjskom planu Europska unija sklopila je niz bilateralnih sporazuma između Unije i trećih zemalja, kao što su sporazumi o uzajamnoj pravnoj pomoći između Europske unije i Sjedinjenih Američkih Država, između Europske unije i Japana te između Europske unije i Norveške i Islanda. Postojeći okvir Europske unije obuhvaća i Uredbu Vijeća (EU) 2017/1939 o provedbi pojačane suradnje u vezi s osnivanjem Ureda europskog javnog tužitelja („EPPO”). Države članice koje sudjeluju u pojačanoj suradnji trebale bi osigurati da EPPO pri izvršavanju svojih nadležnosti kako je predviđeno člancima 22., 23. i 25. Uredbe (EU) 2017/1939 može tražiti suradnju na temelju Protokola na isti način kao i nacionalni tužitelji tih država članica. Ti instrumenti i sporazumi posebno se odnose na članke 8., 9., 10., 11. i 12. Protokola.

Nadalje, Unija je donijela nekoliko direktiva kojima se jačaju postupovna prava osumnjičenih i optuženih osoba.[23] Ti se instrumenti posebno odnose na članke 6., 7., 8., 9., 10., 11., 12. i 13.

[23] Direktiva 2010/64/EU Europskog parlamenta i Vijeća od 20. listopada 2010. o pravu na tumačenje i prevođenje u kaznenim postupcima, SL L 280, 26.10.2010., str. 1.; Direktiva 2012/13/EU Europskog parlamenta i Vijeća od 22. svibnja 2012. o pravu na informiranje u kaznenom postupku, SL L 142, 1.6.2012., str. 1.; Direktiva 2013/48/EU Europskog parlamenta i Vijeća od 22. listopada 2013. o pravu na pristup odvjetniku u kaznenom postupku i u postupku na temelju europskog uhidbenog naloga te o pravu na obavješćivanje treće strane u slučaju oduzimanja slobode i na komunikaciju s trećim osobama i konzularnim tijelima, SL L 294, 6.11.2013., str. 1.; Direktiva (EU) 2016/1919 Europskog parlamenta i Vijeća od

Protokola. Poseban skup zaštitnih mjera odnosi se na zaštitu osobnih podataka, što je temeljno pravo sadržano u Ugovorima EU-a i Povelji Europske unije o temeljnim pravima. Osobni podaci mogu se obrađivati samo u skladu s Uredbom (EU) 2016/679 (Opća uredba o zaštiti podataka) i Direktivom (EU) 2016/680 (Direktiva o zaštiti podataka za potrebe kaznenog progona). Temeljno pravo svakoga na poštovanje privatnog i obiteljskog života, doma i komuniciranja uključuje poštovanje privatnosti komunikacije kao ključnog elementa. Elektronički komunikacijski podaci mogu se obrađivati samo u skladu s Direktivom 2002/58/EZ (Direktiva o e-privatnosti). Ti se instrumenti posebno odnose na članak 14. Protokola.

Člankom 14. stavcima od 2. do 15. Protokola predviđaju se odgovarajuće mjere zaštite podataka u smislu pravila Unije o zaštiti podataka, posebno članka 46. Opće uredbe o zaštiti podataka i članka 37. Direktive o zaštiti podataka za potrebe kaznenog progona te relevantne sudske prakse Suda Europske unije. U skladu sa zahtjevima prava Unije[24] i kako bi se zajamčila učinkovitost zaštitnih mjera iz članka 14. Protokola, države članice trebale bi osigurati obavješćivanje pojedinaca čiji su podaci preneseni, podložno određenim ograničenjima, npr. kako bi se izbjeglo ugrožavanje istraga u tijeku. Člankom 14. stavkom 11. točkom (c) Protokola državama članicama pruža se osnova za ispunjavanje tog zahtjeva.

Usklađenost članka 14. stavka 1. Protokola s pravilima Unije o zaštiti podataka podrazumijeva i da države članice razmotre sljedeće u pogledu mogućih alternativnih načina osiguravanja odgovarajuće zaštite osobnih podataka koji se prenose u skladu s Protokolom. U pogledu drugih međunarodnih sporazuma kojima se uspostavlja sveobuhvatan okvir za zaštitu osobnih podataka u skladu s primjenjivim zahtjevima zakonodavstva predmetnih stranaka, u skladu s člankom 14. stavkom 1. točkom (b) države članice trebale bi uzeti u obzir da je za izravnu suradnju Krovni sporazum između EU-a i SAD-a potrebno dopuniti dodatnim zaštitnim mjerama, koje treba odrediti u posebnom dogovoru o prijenosu između SAD-a i EU-a / njegovih država članica, kojima se uzimaju u obzir jedinstveni zahtjevi za prijenos elektroničkih dokaza izravno od strane pružatelja usluga, a ne među tijelima.[25]

---

26. listopada 2016. o pravnoj pomoći za osumnjičenike i okrivljenike u kaznenom postupku i za tražene osobe u postupku na temelju europskog uhidbenog naloga, SL L 297, 4.11.2016., str. 1. Direktiva (EU) 2016/800 Europskog parlamenta i Vijeća od 11. svibnja 2016. o postupovnim jamstvima za djecu koja su osumnjičenici ili optuženici u kaznenim postupcima, SL L 132, 21.5.2016., str. 1. Direktiva (EU) 2016/343 Europskog parlamenta i Vijeća od 9. ožujka 2016. o jačanju određenih vidova pretpostavke nedužnosti i prava sudjelovati na raspravi u kaznenom postupku SL L 65, 11.3.2016., str. 1.; Direktiva 2012/13/EU Europskog parlamenta i Vijeća od 22. svibnja 2012. o pravu na informacije u kaznenim postupcima.

[24] Vidjeti Mišljenje 1/15 Suda Europske unije (veliko vijeće), ECLI:EU:C:2017:592, točka 220. Vidjeti i doprinos Europskog odbora za zaštitu podataka savjetovanju o nacrtu drugog dodatnog protokola uz Konvenciju Vijeća Europe o kibernetičkom kriminalu (Budimpeštanska konvencija), 13. studenoga 2019., str. 6. („Važno je da nadležna nacionalna tijela kojima je odobren pristup podacima o tome obavijeste dotične osobe, u okviru primjenjivih nacionalnih postupaka, čim takva obavijest ne može ugroziti istragu koju vode ta tijela. ... Ta obavijest je potrebna kako bi se dotičnim osobama omogućilo, među ostalim, ostvarivanje prava na pravni lijek i pravo na zaštitu njihovih podataka u vezi s obradom njihovih podataka”).

[25] Zbog toga Odluka Vijeća od 21. svibnja 2019. o odobravanju otvaranja pregovora u cilju sklapanja sporazuma između Europske unije i Sjedinjenih Američkih Država o prekograničnom pristupu elektroničkim dokazima za potrebe pravosudne suradnje u kaznenim stvarima (9114/19) u svojim pregovaračkim smjernicama sadržava niz dodatnih mjera za zaštitu podataka. Konkretno, u pregovaračkim smjernicama navodi se da „sporazumom bi trebalo dopuniti Krovni sporazum dodatnim zaštitnim mjerama kojima se u obzir uzimaju razina osjetljivosti dotičnih kategorija podataka i jedinstveni zahtjevi za prijenos elektroničkih dokaza koji izravno provode pružatelji usluga te se on ne provodi između tijela i prijenose od nadležnih tijela izravno do pružatelja usluga.”

Isto tako, u skladu s člankom 14. stavkom 1. točkom (b) Protokola, države članice trebale bi smatrati da za države članice EU-a koje su stranke Konvencije 108+ ta konvencija sama po sebi ne pruža odgovarajuću osnovu za prekogranične prijenose podataka na temelju Protokola drugim strankama te konvencije. U tom pogledu trebale bi razmotriti zadnju rečenicu članka 14. stavka 1. Konvencije br. 108+[26].

Naposljetku, s obzirom na druge sporazume ili dogovore iz članka 14. stavka 1. točke (c), države članice trebale bi razmotriti činjenicu da se mogu osloniti na takve druge sporazume ili dogovore samo ako je Europska komisija donijela odluku o primjerenosti u skladu s člankom 45. Opće uredbe o zaštiti podataka (EU) 2016/679 ili člankom 36. Direktive o zaštiti podataka za potrebe kaznenog progona (EU) 2016/680 za predmetnu treću zemlju koja obuhvaća dotične prijenose podataka ili ako se samim tim drugim sporazumom ili dogovorom osiguravaju odgovarajuće mjere za zaštitu podataka u skladu s člankom 46. Opće uredbe o zaštiti podataka ili člankom 37. stavkom 1. Direktive o zaštiti podataka za potrebe kaznenog progona.

Potrebno je uzeti u obzir ne samo pravo Unije u postojećem obliku u predmetnom području nego i njegov budući razvoj, u mjeri u kojoj je to predvidivo u vrijeme analize. Područje obuhvaćeno Protokolom od izravne je važnosti za predvidivi budući razvoj prava Unije. U tom pogledu treba napomenuti prijedloge Komisije iz travnja 2018. o prekograničnom pristupu elektroničkim dokazima.[27] Ti se instrumenti posebno odnose na članke 6. i 7. Protokola.

Komisija je sudjelovanjem u pregovorima u ime Unije osigurala potpunu usklađenost Protokola s pravom Unije i obvezama država članica koje iz njega proizlaze. Konkretno, Komisija je osigurala da odredbe Protokola omogućuju državama članicama poštovanje temeljnih prava, sloboda i općih načela prava Unije kako su utvrđena u Ugovorima EU-a i Povelji o temeljnim pravima, uključujući proporcionalnost, postupovna prava, pretpostavku nedužnosti i pravo na obranu osoba koje podliježu kaznenom postupku, kao i privatnost i zaštitu osobnih podataka i elektroničkih komunikacijskih podataka kad se takvi podaci obrađuju, uključujući prijenos tijelima kaznenog progona u zemljama izvan Europske unije te sve obveze tijela kaznenog progona i pravosudnih tijela u tom pogledu. Komisija je uzela u obzir i mišljenje Europskog nadzornika za zaštitu podataka[28] i Europskog odbora za zaštitu podataka.[29]

Nadalje, Komisija je osigurala da su odredbe Protokola i prijedlozi Komisije o e-dokazima kompatibilni, među ostalim s obzirom na to da se nacrt zakonodavstva mijenjao u raspravama sa suzakonodavcima, i da Protokol ne izaziva sukobe zakona. Konkretno, Komisija je osigurala da Protokol uključuje odgovarajuće mjere zaštite podataka i privatnosti, kojima se

[26] Vidjeti i Izvješće s objašnjenjima uz Protokol o izmjeni Konvencije o zaštiti pojedinaca s obzirom na automatsku obradu osobnih podataka, 10. listopada 2018., točke 106.–107.

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

[28] Mišljenje EDPS-a o sudjelovanju u pregovorima s obzirom na Drugi dodatni protokol uz Budimpeštansku konvenciju o kibernetičkom kriminalu od 2. travnja 2019., Mišljenje 3/2019.

[29] Uključujući „Doprinos EDPB-a savjetovanju o nacrtu drugog dodatnog protokola uz Konvenciju Vijeća Europe o kibernetičkom kriminalu („Budimpeštanska konvencija") od 13. studenoga 2019.; „Izjava 02/201 o novom nacrtu odredaba drugog dodatnog protokola uz Konvenciju Vijeća Europe o kibernetičkom kriminalu (Budimpeštanska konvencija) kako je donesena 2. veljače 2021."; „Doprinos EDPB-a šestom krugu savjetovanja o nacrtu Drugog dodatnog protokola uz Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu od 4. svibnja 2021.".

pružateljima usluga iz EU-a omogućuje da poštuju svoje obveze u skladu s propisima EU-a o zaštiti podataka i privatnosti, u mjeri u kojoj Protokol pruža pravnu osnovu za prijenose podataka kao odgovor na naloge ili zahtjeve koje je izdalo tijelo stranke Protokola koja nije država članica EU-a i kojima se od voditelja obrade ili izvršitelja obrade iz EU-a zahtijeva otkrivanje osobnih podataka ili elektroničkih komunikacijskih podataka.

2.4. Rezerve, izjava, obavijest i priopćenja te druga razmatranja

Protokolom se strankama pruža osnova za korištenje određenih rezervi te za davanje izjava, obavijesti ili priopćenja u vezi s određenim člancima. Države članice trebale bi zauzeti jedinstven pristup određenim rezervama i izjavama, obavijestima i priopćenjima kako je utvrđeno u Prilogu ovoj Odluci. Kako bi se osiguralo da provedba Protokola bude usklađena s pravom Unije, države članice EU-a trebale bi u pogledu tih rezervi i izjava zauzeti stajalište navedeno u nastavku. Ako je Protokolom predviđena osnova za druge rezerve, izjave, obavijesti ili priopćenja, ovim se Prijedlogom države članice ovlašćuju da razmotre i izraze svoje rezerve, izjave, obavijesti ili priopćenja.

Kako bi se osigurala usklađenost odredaba Protokola s relevantnim pravom i politikama Unije, države članice ne bi trebale koristiti rezerve u skladu s člankom 7. stavkom 9. točkama (a)[30] i (b)[31]. Osim toga, države članice trebale bi dati izjavu u skladu s člankom 7. stavkom 2. točkom (b)[32] i obavijest u skladu s člankom 7. stavkom 5. točkom (a)[33]. Nekorištenje tih rezervi i podnošenje izjave i obavijesti važni su kako bi se osigurala usklađenost Protokola s Komisijinim zakonodavnim prijedlozima o e-dokazima, uključujući rasprave o nacrtima zakonodavstva.

Osim toga, kako bi države članice EU-a tijekom suradnje sa strankama koje nisu države članice EU-a ujednačeno primjenjivale Protokol, države članice potiče se da ne koriste rezervu u skladu s člankom 8. stavkom 13.[34], među ostalim i zato što bi takva rezerva imala recipročni učinak[35]. Države članice trebale bi dati izjavu u skladu s člankom 8. stavkom 4. kako bi osigurale da se nalog može provesti u slučaju da su potrebne dodatne popratne informacije, npr. o okolnostima predmetnog slučaja kako bi se procijenile proporcionalnost i nužnost.[36]

---

[30] Omogućivanje strankama da zadrže pravo da ne primjenjuju članak 7. (otkrivanje podataka o pretplatnicima).

[31] Omogućivanje strankama da zadrže pravo da ne primjenjuju članak 7. (otkrivanje podataka o pretplatnicima) na određene vrste pristupnih brojeva ako to ne bi bilo u skladu s temeljnim načelima njihova nacionalnog pravnog sustava.

[32] Omogućivanje strankama da izjave da se nalog u skladu s člankom 7. stavkom 1. (otkrivanje podataka o pretplatnicima) mora izdati od strane ili pod nadzorom tužitelja ili drugog pravosudnog tijela ili se mora izdati na neki drugi način pod neovisnim nadzorom.

[33] Omogućivanje strankama da obavijeste glavnog tajnika Vijeća Europe da, kad se u skladu s člankom 7. stavkom 1. (otkrivanje podataka o pretplatnicima) izdaje nalog pružatelju usluga na njihovu državnom području, stranka zahtijeva, u svakom slučaju ili u utvrđenim okolnostima, istodobnu obavijest o nalogu, dopunske informacije i sažetak činjenica povezanih s istragom ili postupkom.

[34] Omogućivanje strankama da zadrže pravo da ne primjenjuju članak 8. (izvršavanje naloga druge stranke) na podatke o prometu.

[35] Vidjeti stavak 147. izvješća s objašnjenjima uz Protokol kojim se utvrđuje da „[a] stranka koja primjenjuje rezervu na ovaj članak ne smije drugim strankama dostavljati naloge za podatke o prometu na temelju [članka 8.] stavka 1.”.

[36] Omogućivanje strankama da izjave da su potrebne dodatne popratne informacije za izvršenje naloga u skladu s člankom 8. stavkom 1. (izvršavanje naloga druge stranke).

Države članice potiče se i da se suzdrže od davanja izjave u skladu s člankom 9. stavkom 1. točkom (b)[37] kako bi se osigurala učinkovita primjena Protokola.

Države članice trebale bi slati obavijesti iz članka 7. stavka 5. točke (e)[38], članka 8. stavka 10. točaka (a) i (b)[39], članka 14. stavka 7. točke (c) i stavka 10. točke (b) kako bi se osigurala sveukupna učinkovita primjena Protokola.[40]

Konačno, države članice trebale bi poduzeti i potrebne mjere u skladu s člankom 14. stavkom 11. točkom (c) kako bi osigurale da je stranka koja prima podatke obaviještena u trenutku prijenosa obveze na temelju prava Unije da dostavi obavijest osobi na koju se podaci odnose[41] te odgovarajuće podatke za kontakt kako bi se stranci koja prima podatke omogućilo da obavijesti nadležno tijelo u državi članici EU-a nakon što se prestanu primjenjivati ograničenja povjerljivosti i obavješćivanje postane moguće.

2.5. Razlozi prijedloga

Protokol će stupiti na snagu nakon što pet stranaka izrazi svoju suglasnost da budu obvezane Protokolom u skladu s odredbama članka 16. stavaka 1. i 2. Svečanost potpisivanja Protokola predviđena je za ožujak 2022.

Države članice EU-a trebale bi poduzeti potrebne korake kako bi osigurale brzo stupanje na snagu i ratifikaciju Protokola, što je važno s obzirom na niz čimbenika.

Prvo, Protokolom će se osigurati bolja opremljenost tijela kaznenog progona i pravosudnih tijela za pribavljanje elektroničkih dokaza potrebnih za kaznene istrage. S obzirom na sve veću važnost elektroničkih dokaza za kaznene istrage nužno je da tijela kaznenog progona i pravosudna tijela imaju odgovarajuće instrumente za učinkovito dobivanje pristupa elektroničkim dokazima kako bi se uspješno borila protiv kriminala na internetu.

Drugo, Protokolom će se osigurati da se takve mjere za dobivanje pristupa elektroničkim dokazima upotrebljavaju na način kojim se državama članicama omogućuje da poštuju temeljna prava, uključujući kaznena postupovna prava, pravo na privatnost i pravo na zaštitu osobnih podataka. Budući da nema jasnih pravila na međunarodnoj razini, postojeće prakse mogu biti problematične u pogledu pravne sigurnosti, transparentnosti, odgovornosti i poštovanja temeljnih prava i postupovnih jamstava osumnjičenika u kaznenim istragama.

---

[37] Omogućivanje strankama da izjave da neće izvršavati zahtjeve iz članka 9. stavka 1. točke (a) (brzo otkrivanje računalnih podataka u hitnim slučajevima) u kojima se traži samo otkrivanje podataka o pretplatnicima.

[38] Omogućivanje strankama da priopće podatke za kontakt tijela koje su imenovale za primanje obavijesti iz članka 7. stavka 5. točke (a) i obavljanje radnji opisanih u članku 7. stavku 5. točkama (b), (c) i (d) (otkrivanje podataka o pretplatnicima).

[39] Omogućivanje strankama da priopće podatke za kontakt tijela koja su imenovale za slanje i primanje naloga u skladu s člankom 8. (izvršavanje naloga druge stranke). U skladu sa zahtjevima iz Uredbe (EU) 2017/1939 države članice koje sudjeluju u pojačanoj suradnji u vezi s osnivanjem Ureda europskog javnog tužitelja (EPPO) uključuju EPPO u komunikaciju.

[40] Omogućivanje strankama da navedu tijela koja bi trebalo obavijestiti u slučaju sigurnosnog incidenta odnosno s kojima bi trebalo stupiti u kontakt kako bi se zatražilo prethodno odobrenje u slučaju daljnjih prijenosa drugoj državi ili međunarodnoj organizaciji.

[41] Vidjeti bilješku 24.

Treće, Protokolom će se riješiti i spriječiti sukobi zakona, koji utječu i na nadležna tijela i na pružatelje usluga u privatnom sektoru i na druge subjekte, tako što će se na međunarodnoj razini osigurati kompatibilna pravila za prekogranični pristup elektroničkim dokazima.

Četvrto, Protokolom će se potkrijepiti kontinuirana važnost Konvencije kao glavnog multilateralnog okvira za borbu protiv kiberkriminaliteta. To će biti presudno u postupku nakon Rezolucije Opće skupštine Ujedinjenih naroda (UNGA) 74/247 iz prosinca 2019. o borbi protiv uporabe informacijskih i komunikacijskih tehnologija u kriminalne svrhe kojom je osnovan otvoreni *ad hoc* međuvladin odbor stručnjaka radi izrade sveobuhvatne međunarodne konvencije o borbi protiv uporabe informacijskih i komunikacijskih tehnologija u kriminalne svrhe.

3. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

- *Pravna osnova*

Nadležnost Unije da donosi zakonodavstvo o pitanjima olakšavanja suradnje među sudskim ili drugim odgovarajućim tijelima u vezi s kaznenim postupcima i izvršenjem odluka temelji se na članku 82. stavku 1. UFEU-a. Nadležnost Unije za pitanja zaštite osobnih podataka temelji se na članku 16. UFEU-a.

U skladu s člankom 3. stavkom 2. UFEU-a Unija ima isključivu nadležnost za sklapanje međunarodnog sporazuma u mjeri u kojoj bi njegovo sklapanje moglo utjecati na zajednička pravila EU-a ili izmijeniti njihov opseg. Odredbe Protokola dio su područja koje je u velikoj mjeri obuhvaćeno zajedničkim pravilima kako je prethodno navedeno u odjeljku 2.3.

Protokol je stoga u isključivoj vanjskoj nadležnosti Unije. Države članice mogu ratificirati Protokol u interesu Unije na temelju članka 16., članka 82. stavka 1. i članka 218. stavka 6. UFEU-a.

- *Supsidijarnost (za neisključivu nadležnost)*

Nije primjenjivo.

- *Proporcionalnost*

Ciljevi Unije u pogledu ovog Prijedloga, kako su navedeni u odjeljku 2.5., mogu se postići samo sklapanjem obvezujućeg međunarodnog sporazuma kojim se predviđaju potrebne mjere suradnje uz istodobno osiguravanje odgovarajuće zaštite temeljnih prava. Protokolom se postiže taj cilj. Odredbe Protokola ograničene su na ono što je potrebno za ostvarivanje njegovih glavnih ciljeva. Jednostrano djelovanje nije rješenje jer se na taj način ne bi osigurala dostatna osnova za suradnju sa zemljama izvan EU-a i ne bi se mogla osigurati potrebna zaštita temeljnih prava. Osim toga, pristupanje multilateralnom dogovoru kao što je Protokol o kojem je pregovarala Unija učinkovitije je od otvaranja pregovora na bilateralnoj razini s pojedinačnim zemljama koje nisu članice EU-a. Pod pretpostavkom da će svih 66 stranaka, kao i buduće nove stranke Konvencije ratificirati Protokol, Protokolom će se osigurati zajednički pravni okvir za suradnju država članica EU-a s njihovim najvažnijim međunarodnim partnerima u borbi protiv kriminala.

- ***Odabir instrumenta***

Nije primjenjivo.

4. REZULTATI *EX POST* EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINKA

- *Ex post evaluacije/provjere primjerenosti postojećeg zakonodavstva*

Nije primjenjivo.

- *Savjetovanja s dionicima*

Vijeće Europe organiziralo je šest krugova javnih savjetovanja u vezi s pregovorima o Protokolu, u srpnju i studenome 2018., veljači i studenome 2019. te u prosincu 2020. i svibnju 2021.[42] Stranke su uzele u obzir informacije dobivene u okviru tih savjetovanja.

Komisija je, u svojstvu pregovarača u ime Unije, razmijenila mišljenja i s tijelima za zaštitu podataka te je tijekom 2019. i 2021. organizirala ciljane savjetodavne sastanke s organizacijama civilnog društva, pružateljima usluga i trgovinskim udruženjima. Komisija je uzela u obzir informacije dobivene na temelju tih razmjena.

- *Prikupljanje i primjena stručnog znanja*

Tijekom pregovora Komisija se dosljedno savjetovala s posebnim odborom Vijeća za pregovore u skladu s Odlukom Vijeća Europske unije od 6. lipnja 2019. o ovlašćivanju Komisije za sudjelovanje u pregovorima u ime Unije, čime se stručnjacima iz država članica pružila prilika da doprinesu postupku oblikovanja stajališta Unije. Nekoliko stručnjaka iz država članica nastavilo je sudjelovati i u pregovorima, zajedno s Komisijom koja je predstavljala Uniju. Održana su i savjetovanja s dionicima (vidjeti prethodno navedeno).

- *Procjena učinka*

Procjena učinka provedena je 2017. i 2018. te je priložena Komisijinim prijedlozima o e-dokazima.[43] U tom kontekstu pregovori o Drugom dodatnom protokolu uz Budimpeštansku konvenciju o kibernetičkom kriminalu bili su dio najpoželjnije opcije. Osim toga, relevantni učinci predstavljeni su u ovom obrazloženju.

- *Primjerenost i pojednostavnjenje propisa*

Protokol može utjecati na određene kategorije pružatelja usluga, uključujući mala i srednja poduzeća (MSP), jer se na njih mogu primjenjivati zahtjevi i nalozi za elektroničke dokaze u skladu s Protokolom. Međutim, na te će se pružatelje usluga često već primjenjivati takvi zahtjevi putem drugih postojećih kanala, ponekad preko različitih tijela, među ostalim na temelju Konvencije[44], drugih ugovora o uzajamnoj pravnoj pomoći ili drugih okvira, uključujući politike upravljanja internetom s više dionika.[45] Isto tako, pružatelji usluga, uključujući mala i srednja poduzeća, imat će koristi od jasnog pravnog okvira na međunarodnoj razini i zajedničkog pristupa svih stranaka Protokola.

- *Temeljna prava*

---

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

[43] SWD(2018) 118 final.

[44] Vidjeti, na primjer, Smjernice Odbora za Konvenciju o kibernetičkom kriminalu br. 10 od 1. ožujka 2017. o nalozima za dostavljanje informacija o pretplatnicima (članak 18. Budimpeštanske konvencije).

[45] Vidjeti, na primjer, Rezoluciju Odbora za internetsku organizaciju za dodijeljene nazive i brojeve (ICANN) od 15. svibnja 2019. o Preporukama o privremenoj specifikaciji za registracijske podatke za generičke vršne domene, dostupno na www.icann.org.

Instrumenti suradnje u okviru Protokola vjerojatno će utjecati na temeljna prava ako se podaci o osobi mogu dobiti u okviru kaznenog postupka, među ostalim npr. na pravo na pošteno suđenje, pravo na privatnost i pravo na zaštitu osobnih podataka. Protokol slijedi pristup temeljen na pravima i predviđa uvjete i zaštitne mjere u skladu s međunarodnim instrumentima za ljudska prava, uključujući Konvenciju Vijeća Europe za zaštitu ljudskih prava i temeljnih sloboda iz 1950. Konkretno, Protokolom su predviđene posebne mjere zaštite podataka. Protokolom se prema potrebi strankama pruža i osnova za korištenje određenih rezervi, davanje izjava ili obavijesti te se navode razlozi za odbijanje suradnje kao odgovor na zahtjev u posebnim situacijama. Time se osigurava usklađenost Protokola s Poveljom EU-a o temeljnim pravima.

5. UTJECAJ NA PRORAČUN

Prijedlog nema utjecaj na proračun EU-a. Države članice mogu imati jednokratne troškove provedbe Protokola, a zbog očekivanog porasta broja slučajeva mogli bi nastati veći troškovi za tijela država članica.

6. DRUGI ELEMENTI

- *Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja*

Ne postoji plan provedbe jer će nakon njegova potpisivanja i ratifikacije države članice morati provesti Protokol.

U pogledu praćenja Komisija će sudjelovati na sastancima Odbora za Konvenciju o kibernetičkom kriminalu na kojima je Europska unija priznata kao promatračka organizacija.

2021/0383 (NLE)

Prijedlog

ODLUKE VIJEĆA

o ovlašćivanju država članica da u interesu Europske unije ratificiraju Drugi dodatni protokol uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 16., članak 82. stavak 1 i članak 218. stavak 6.,

uzimajući u obzir prijedlog Europske komisije,

uzimajući u obzir suglasnost Europskog parlamenta,

budući da:

(1) Vijeće je 9. lipnja 2019. ovlastilo Komisiju da u ime Unije sudjeluje u pregovorima o Drugom dodatnom protokolu uz Budimpeštansku konvenciju Vijeća Europe o kibernetičkom kriminalu.

(2) Tekst Drugog dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza („Protokol”) donio je Odbor ministara Vijeća Europe 17. studenoga 2021. te se predviđa da će biti otvoren za potpisivanje u ožujku 2022.

(3) Odredbe Protokola dio su područja koje je u velikoj mjeri obuhvaćeno zajedničkim pravilima u smislu članka 3. stavka 2. UFEU-a, uključujući instrumente za olakšavanje pravosudne suradnje u kaznenim stvarima, osiguravanje minimalnih standarda za postupovna prava te mjere za zaštitu podataka i privatnosti.

(4) Komisija je podnijela i zakonodavne prijedloge uredbe o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima (COM(2018) 225 final) i direktive o utvrđivanju usklađenih pravila za imenovanje pravnih zastupnika za potrebe prikupljanja dokaza u kaznenim postupcima kojima se uvode obvezujući prekogranični europski nalozi za dostavljanje i čuvanje dokaza koji se izravno upućuju predstavniku pružatelja usluga u drugoj državi članici (COM(2018) 226 final).

(5) Sudjelovanjem u pregovorima u ime Unije Komisija je osigurala usklađenost Drugog dodatnog protokola s relevantnim zajedničkim pravilima Europske unije.

(6) Kako bi se osigurala usklađenost Protokola s pravom i politikama Unije, kao i ujednačena primjena Protokola među državama članicama EU-a u odnosima sa strankama koje nisu članice EU-a te učinkovita primjena Protokola, važan je niz rezervi, izjava, obavijesti i priopćenja.

(7) S obzirom na to da su Protokolom predviđeni brzi postupci za poboljšanje prekograničnog pristupa elektroničkim dokazima i visoka razina zaštitnih mjera, stupanje na snagu doprinijet će borbi protiv kiberkriminaliteta i drugih oblika kriminala na globalnoj razini olakšavanjem suradnje između stranaka Protokola iz

država članica EU-a i stranaka iz zemalja koje nisu države članice EU-a, te će osigurati visoku razinu zaštite pojedinaca i uklanjanje sukoba zakona.

(8) S obzirom na to da su Protokolom predviđene odgovarajuće zaštitne mjere u skladu sa zahtjevima za međunarodne prijenose osobnih podataka na temelju Uredbe (EU) 2016/679 i Direktive (EU) 2016/680, njegovim stupanjem na snagu doprinijet će se promicanju standarda Unije za zaštitu podataka na globalnoj razini, olakšat će se protok podataka između stranaka Protokola iz država članica EU-a i stranaka iz zemalja koje nisu države članice EU-a te će se osigurati da države članice EU-a poštuju svoje obveze koje proizlaze iz pravila Unije o zaštiti podataka.

(9) Brzim stupanjem na snagu potvrdit će se i važnost Budimpeštanske konvencije Vijeća Europe kao glavnog multilateralnog okvira za borbu protiv kiberkriminaliteta.

(10) Europska unija ne može postati stranka Protokola jer su i Protokol i Konvencija Vijeća Europe o kibernetičkom kriminalu otvoreni samo za države.

(11) Države članice trebale bi stoga biti ovlaštene ratificirati Protokol, djelujući zajednički u interesu Europske unije.

(12) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća te je on dao mišljenje …

(13) [U skladu s člancima 1. i 2. Protokola br. 21 o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područje slobode, sigurnosti i pravde, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, i ne dovodeći u pitanje članak 4. navedenog protokola, Irska ne sudjeluje u donošenju ove Odluke te ona za nju nije obvezujuća niti se na nju primjenjuje.]

[ILI]

[U skladu s člancima 1. i 2. Protokola br. 21 o stajalištu Ujedinjene Kraljevine i Irske s obzirom na područje slobode, sigurnosti i pravde, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, i ne dovodeći u pitanje članak 4. navedenog protokola, Irska je [pismom od ...] obavijestila da želi sudjelovati u donošenju i primjeni ove Odluke.]

(14) U skladu s člancima 1. i 2. Protokola br. 22 o stajalištu Danske, priloženog Ugovoru o Europskoj uniji i Ugovoru o funkcioniranju Europske unije, Danska ne sudjeluje u donošenju ove Odluke te ona za nju nije obvezujuća niti se na nju primjenjuje,

DONIJELO JE OVU ODLUKU:

Članak 1.

Države članice ovlašćuju se u interesu Europske unije za ratifikaciju Drugog dodatnog protokola uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza („Protokol”).

Članak 2.

Pri ratifikaciji Protokola države članice izražavaju rezerve i daju izjave, obavijesti ili priopćenja navedena u Prilogu.

Članak 3.

Ova Odluka stupa na snagu na dan donošenja.

Članak 4.

Ova Odluka objavljuje se u *Službenom listu Europske unije*.

Članak 5.

Ova je Odluka upućena državama članicama.

Sastavljeno u Bruxellesu,

Za Vijeće
Predsjednik