Europski parlament
2014-2019

Odbor za građanske slobode, pravosuđe i unutarnje poslove

1.4.2019

ŠESTI RADNI DOKUMENT (B)

o Prijedlogu uredbe o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima (2018/0108 (COD)) – Zaštitne mjere i pravni lijekovi

Odbor za građanske slobode, pravosuđe i unutarnje poslove

Izvjestiteljica: Birgit Sippel

Suautor: Romeo Franz

II. *Ex ante* zaštitne mjere

Nakon analize Prijedloga u pogledu obavješćivanja ispitanika, ovim se radnim dokumentom razmatraju one zaštitne mjere koje moraju biti zajamčene prije prikupljanja podataka i njihova prosljeđivanja državi izdavateljici (takozvane *ex ante* zaštitne mjere).

Budući da se o pitanju prethodne autentifikacije EPOC-PR-a koju provodi pružatelj usluga (kojom se jamči da je EPOC-PR zaista izdalo nadležno pravosudno tijelo) već detaljno raspravljalo u 3. radnom dokumentu[1], ovaj je dokument usmjeren samo na *ex ante* zaštitne mjere koje se odnose na treće strane te na zaštitne mjere povezane s postupkom izvršenja.

1. Uključene treće strane[2]

Gotovo je neizbježno da će čak i upotreba ciljanih EPOC-ova rezultirati slučajnim prikupljanjem podataka o osobama s kojima je komunicirao prvotno predviđeni ispitanik, tj. osumnjičenik/okrivljenik. Neki od tih podataka mogli bi biti važni za istragu, a neki ne. Prema tome, čuvanje, dostavljanje i širenje podataka ne samo ciljanih osoba nego i podataka trećih osoba (uključujući sigurnost podataka) mora biti uređeno strogim pravilima, čime će se osigurati potpuno jamčenje temeljnih prava i načela zaštite podataka. Međutim, takva pitanja povezana sa zadržavanjem, širenjem i sigurnošću prikupljenih podataka do sada nisu razmatrana ni rješavana na primjeren način. Osim zaista osnovnog zajedničkog dogovora da bi podatke trebalo primjereno zaštititi od hakera i drugih zločinaca, postoji potreba za jasnim skupom pravila i postupaka u pogledu vremenskog razdoblja u kojem se podaci prije samog prikupljanja podataka i njihova prijenosa državi izdavateljici mogu zadržati te s kime se smiju dijeliti i u koje svrhe.

2. Obavješćivanje i moguća reakcija nadležnih tijela u državi izvršiteljici

Drugi važan element u pogledu *ex ante* zaštitnih mjera odnosi se na pitanje veće uključenosti nadležnih tijela države izvršiteljice, uključujući iscrpnu obavijest o EPOC-PR-u i mogućnost značajne reakcije ili čak prethodnog odobrenja. To je pitanje već naglašeno u nekoliko prethodnih radnih dokumenata. Takvo automatsko pravo tijela izvršitelja na reakciju trenutačno nije predviđeno Prijedlogom uredbe. Iako članak 14. stavak 4. točka (f) i stavak 5. točka (f) sadržavaju odredbu prema kojoj pružatelj usluga ne mora postupiti u skladu s EPOC-PR-om ako je „očito da se njime krši Povelja ili da je očito uvredljiv”, pretpostavlja se da pružatelj usluga nije postupio u skladu s EPOC-PR-om. Tek tada bi nadležna tijela države izvršiteljice imala aktivnu ulogu.

Ipak, veće se uključenje država izvršiteljica čini jedinim razumnim rješenjem za jamčenje sadašnje sudske prakse Europskog suda za ljudska prava i obveza država članica.[3] Takva se mogućnost obavješćivanja i reakcija može temeljiti na članku 31. Direktive o EIN-u i razlozima za nepriznavanje navedenima u članku 11. Direktive o EIN-u te bi se mogla

[1] Vidi i dokument BRAK-a (Bundesrechtsanwaltskammer – Njemačka savezna odvjetnička komora) br. 28/2018 u kojem se isto tako upućuje na potrebu za širim skupom podataka koji bi trebalo slati pružateljima usluga po uzoru na članak 5. Direktive o EIN-u.

[2] Za svaki pristup podacima o trećim stranama koje nisu osumnjičene postrožit će se uvjeti, kao što je ograničeni pristup ili samo izniman pristup, primjerice za zaštitu ključnih interesa nacionalne sigurnosti, obrane ili javne sigurnosti.

[3] Vidi 3. radni dokument.

prilagoditi različitim kategorijama podataka.

U pogledu podataka o pretplatniku i pristupu, takvim bi se većim uključenjem moglo odrediti da se EPOC-PR automatski i istodobno šalje pružatelju usluga i nadležnom tijelu države izvršiteljice, a nadležno tijelo države izvršiteljice imalo bi određeno vremensko ograničenje za prigovor na EPOC-PR na temelju razloga za nepriznavanje iz članka 11. Direktive o EIN-u.[4] Na taj način, umjesto da se od nadležnih tijela države izvršiteljice zahtijeva potvrda EPOC-PR-a, EPOC-PR za podatke o pretplatniku i pristupu predviđa pravo države izvršiteljice na negativnu reakciju.

U pogledu osjetljivijih kategorija podataka, odnosno podataka o transakcijama i sadržaju, sustavom veće uključenosti mogu se zahtijevati strože obveze, primjerice, pozitivna odluka države izvršiteljice, a time i potvrda EPOC-PR-a prije dostavljanja/čuvanja podataka.[5]

Nadalje, u pogledu teksta odredbe o temeljnim pravima, umjesto primjene vrlo nepreciznog teksta iz Prijedloga Komisije, odnosno „očito se krši Povelja o temeljnim pravima Europske unije", upotrebljava se definicija iz članka 11. stavka 1. točke (f) Direktive o EIN-u („postoje opravdani razlozi za sumnju da bi izvršenje istražne mjere navedene u EIN-u bilo nepodudarno s obvezama države izvršiteljice u skladu s člankom 6. UEU-a i Poveljom").

Čini se da je preuzimanje istog teksta kao u Direktivi o EIN-u još i važnije radi rješavanja sadašnje neusklađenosti odredaba iz različitih pravnih instrumenata EU-a za uzajamno priznavanje i sudske prakse Suda Europske unije.[6] Iako je s vremenom postalo očito da je jasna odredba o temeljnim pravima neophodna za jamčenje obveza u pogledu temeljnih prava, praksa je ipak bila uvođenje različitih odredaba za svaki instrument za uzajamno priznavanje s jasnom namjerom nekih da ga se ograniči ili učini neprimjenjivim.[7] Stoga odredba o temeljnim pravima mora biti dovoljno opsežna kako bi je sudac mogao po potrebi upotrijebiti (sudac ili sutkinja dužni su štititi temeljna prava), mora se odnositi na sva prava (ne samo na katalog prava)[8] te upućuje na članak 6. UEU-a.[9] Samo se na taj način mogu izbjeći buduća

---

[4] U pogledu upotrebe članka 11. Direktive o EIN-u, vidi i stajalište Vijeća odvjetničkih komora Europe od 19. listopada 2010. o prijedlogu Komisije.

[5] Opći pristup Vijeća ne rješava problem uvođenjem novog članka 7.a s obavješćivanjem u pogledu podataka o sadržaju kada je osoba iz države izvršiteljice. Nije u potpunosti jasno je li država izvršiteljica ovlaštena intervenirati bilo u negativnom (određeni rok za reakciju), bilo u pozitivnom smislu (odluka o odobrenju). Država izdavateljica uzima u obzir sve moguće nedoumice (u vrlo ograničenom broju slučajeva). Vidi i preporuke Vijeća odvjetničkih komora Europe o elektroničkim dokazima, 28. veljače 2019.

[6] Vidi, primjerice, samo opće upućivanje u članku 1. stavku 3. Okvirne odluke Vijeća o europskom uhidbenom nalogu 2002/584/PUP i izričite odredbe u nekoliko država članica u prenesenom tekstu; članak 20. stavak 3. Okvirne odluke Vijeća 2005/214/PUP od 24. veljače 2005. o primjeni načela uzajamnog priznavanja na novčane kazne; članak 11. stavak 1. točka (f) Direktive o EIN-u; članak 8. stavak 1. točka (f) i članak 19. stavak 1. točka (h) Uredbe (EU) 2018/1805 o uzajamnom priznavanju naloga za zamrzavanje i naloga za oduzimanje te *Aranyosi i Căldăraru*, spojeni predmeti C-404/15 i C-659/15 PPU, i *Minister for Justice and Equality protiv LM-a*, predmet C-216/18 PPU.

[7] Primjerice, upotrebom termina „očito uskraćivanje sudske zaštite" (pojam Europskog suda za ljudska prava koji se uglavnom upotrebljava u pogledu izručenja trećim zemljama) koji je Europski parlament izričito odbio u pregovorima u vezi s EIN-om zbog njegovih iznimnih ograničenja.

[8] Neke su države članice željele ograničiti kategorije prava obuhvaćene tim razlozima u pogledu uzajamnog priznavanja naloga za zamrzavanje i naloga za oduzimanje. Međutim, Europski parlament snažno se protivio ograničenju samo nekih prava. Vidi i Europski odbor za zaštitu podataka, ibid. koji navodi (str. 17.): *„Čak i osnova za odbijanje izvršenja naloga na temelju toga što se njime krši Povelja pojavljuje se iznad klasičnog praga koji se odnosi na kršenje temeljnih prava dotične osobe. Sukladno s time, ... nacrtom Uredbe trebalo bi barem predvidjeti minimalno klasično odstupanje da bi, ako postoje osnovani razlozi za pretpostavku da bi izvršenje naloga rezultiralo kršenjem temeljnog prava dotične osobe i da bi država izvršiteljica zanemarila svoje obveze u pogledu zaštite temeljnih prava..."*

upućivanja na sud i napetosti u pogledu temeljnih prava.[10]

3. Obavješćivanje *uključene* države

Pristup iznesen u prijedlogu Komisije da se nadležnim tijelima države izdavateljice daju izravne pravne ovlasti nad pružateljima usluga (a time i podacima građana) uz samo ograničeno ili naknadno informiranje uključenih osoba, dovodi do situacije u kojoj uključena osoba nema učinkovitu mogućnost osporavanja zakonitosti, proporcionalnosti ili nužnosti naloga pred sudom koji joj je dostupan u državi u kojoj ima prebivalište. Time se izravno utječe na pravo na pošteno suđenje i pravo na obranu. Stoga takozvani parametar lokalizacije ciljane osobe, pri čemu bi trebalo uzeti u obzir lokaciju ispitanika (uz mjesto kaznenog progona), neće biti uključen u prijedlog Komisije.[11]

Jedan način na koji se može osigurati djelotvorno ostvarivanje temeljnih prava uključene osobe, uključujući imunitet i povlastice (tj. za novinare, liječnike ili odvjetnike) bio bi uspostava mehanizma obavješćivanja kojim bi država izdavateljica obavijestila uključenu državu ili tražila njezino odobrenje prije izdavanja naloga državi izvršiteljici ili pružatelju usluga. Time bi se zaštita temeljnih prava podigla na uspostavljene standarde pravosudne suradnje, a uključenoj državi bi se omogućilo da ispuni svoje obveze u pogledu zaštite temeljnih prava.

Međutim, postavlja se glavno pitanje, a to je koja će država biti obaviještena, država u kojoj su pohranjeni podaci, država u kojoj je imenovan pravni zastupnik pružatelja usluge, država u kojoj uključena osoba ima prebivalište[12] ili/i država čije državljanstvo ima uključena osoba?[13] Pitanje postaje još složenije uvođenjem pojma zastupnika iz usporedno donesene Direktive, gdje bi se zastupnik mogao razlikovati od sjedišta pružatelja usluga u EU-u i mjesta u EU-u u kojem su pohranjeni podaci.[14] Teoretski, čini se da bi svi oni trebali biti obaviješteni ako se želi postupiti u skladu s obvezama EU-a i Europske konvencije o temeljnim pravima u pogledu temeljnih prava/zaštite podataka. Kako bi se potrebni napor smanjio, postoji mogućnost imenovanja pravnog zastupnika samo za pružatelje usluga iz trećih zemalja; za pružatelje usluga iz EU-a bio bi prikladniji sadašnji sustav u skladu s kojim sjedište pružatelja usluga/lokacija podataka služi kao kontaktna točka. U tom pogledu, upitno je nastoji li se

[9] Upućivanje na članak 6. UEU-a važno je jer se odnosi na tri sloja zaštite temeljnih prava, a to su Europska konvencija o ljudskim pravima, Povelja i zajedničke ustavne tradicije. Takvim se upućivanjem može izbjeći i potencijalni sukob nacionalnih ustava i prava EU-a (kakav se dogodio u slučaju „Solange") u pogledu zaštite temeljnih prava.

[10] Instrumenti uzajamnog priznavanja često se u državama članicama prenose u posebne zakone. Nema smisla i sudac ne može na taj način raditi ako se za svaki posebni postupak uzajamnog priznavanja upotrebljava različita odredba o temeljnim pravima (bilo šira, bilo ograničena), primjerice, jedna za europski uhidbeni nalog, jedna za oduzimanje, a jedna za dokaze. Sudac tako ne sudi niti ocjenjuje predmete na taj način, već ili prepoznaje rizik za temeljna prava ili ga ne prepoznaje.

[11] Vidi, primjerice, radni dokument Vijeća 3901/2017, prijedlog Belgije za radnu metodologiju u kojem se navodi: „Smatramo da predstavlja najvažniji ‚čimbenik povezivanja' uz razlog za kazneni progon", pri čemu se predlaže pojam lociranje mjesta na kojem ciljana osoba uobičajeno upotrebljava usluge.

[12] Za ovu mogućnost vidi T. Christakis, Forum za prekogranične podatke, „Velika odstupanja u mišljenjima" o elektroničkim dokazima u Vijeću EU-a: Prijedlog za rješavanje problema obavješćivanja.

[13] Ibid.

[14] Vidi članak 3. predložene e-Direktive („Pravni zastupnik boravi ili ima poslovni nastan u jednoj od država članica u kojima pružatelj usluga ima poslovni nastan ili nudi usluge."). Sustav bi bio logičan za pružatelje usluga koji nemaju poslovni nastan u EU-u, ali u EU-u nude usluge. Međutim, time se za pružatelje usluga s poslovnim nastanom u EU-u mijenjaju sadašnja praksa i funkcionalni sustav suradnje. To je naglasilo Njemačko udruženje sudaca, vidi Deutscher Richterbund, Stellungnahme br. 6/18.

općim pristupom Vijeća o Direktivi o elektroničkim dokazima od 8. ožujka 2019.[15] proširiti, kako se čini, pojam pravnog zastupnika (i sva pitanja povezana s time u pogledu obavješćivanja) na druge postojeće instrumente, kao što je EIN. Takvim bi se potencijalnim proširivanjem doveo u pitanje postojeći funkcionalni i uspostavljeni sustav u pogledu pružatelja usluga iz EU-a.[16]

Uz pitanje potrebnih adresata za iscrpno obavješćivanje, postoji još jedan važan aspekt mogućih posljedica takvog obavješćivanja. Takvo obavješćivanje mora barem za neke kategorije podataka uključivati mogućnost reakcije barem na negativan način (tj. blokiranje mjere na određeno vrijeme na temelju predloška iz članka 31. Direktive o EIN-u) kako bi se omogućile odgovornosti države izvršiteljice u okviru sustava Europskog suda za ljudska prava te radi osjetljive prirode podataka u skladu sa sudskom praksom Suda Europske unije (posebno u pogledu vrlo niskog praga kojim se Komisija koristi za, primjerice, podatke o trgovanju ljudima).[17]

4. Različite sigurnosne mjere za različite kategorije podataka (članak 2.)

Komisija je u svojem prijedlogu uvela četiri kategorije podataka: (a) podaci o pretplatniku, (b) podaci o pristupu, (c) podaci o transakcijama i (d) podaci o sadržaju. Prijedlogom se daju različiti zahtjevi ovisno o kategorijama u koje pripadaju podaci koje zahtijevaju nadležna tijela. Dok je za podatke o pretplatniku i pristupu potrebna samo ovjera tužitelja i može im se pristupiti za potrebe svih kaznenih djela, podacima o transakcijama i sadržaju može se pristupiti samo uz prethodnu potvrdu suca i to za kaznena djela kažnjiva maksimalnom zatvorskom kaznom od najmanje tri godine, za kaznena djela usklađena u Okvirnoj odluci Vijeća 2001/413/PUP, Direktivi 2011/93/EU i Direktivi 2013/40/EU te kaznena djela terorizma navedena u Direktivi 2017/541/EU.

Pojavljuju se dva pitanja u vezi s novim kategorijama podataka: (1.) definicije se djelomično preklapaju (vidi definicije podataka o pristupu i podataka o transakcijama) te bi mogle onemogućiti tijelima kaznenog progona da pravedno upotrebljavaju instrumente; (2.)

---

[15] Vijeće, dok. 6946/19.

[16] Vidi uvodnu izjavu 8. navedenog općeg pristupa u kojoj se navodi: *„Dotični pravni zastupnik trebao bi služiti kao adresat za domaće naloge i odluke te naloge i odluke na temelju pravnih instrumenata Unije koji su obuhvaćeni područjem primjene glave V. poglavlja 4. Ugovora o funkcioniranju Europske unije u pogledu prikupljanja dokaza u kaznenim stvarima, među ostalim kada se ti nalozi i odluke prenose u obliku certifikata. To uključuje i instrumente u okviru kojih je moguća izravna dostava naloga pružatelju usluga u prekograničnim situacijama ili njegovom pravnom zastupniku, kao što je [Uredba o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima (dalje u tekstu „Uredba")[6]], i druge instrumente za pravosudnu suradnju primjenjive među državama članicama, posebno one obuhvaćene područjem primjene glave V. poglavlja 4., kao što su Direktiva o Europskom istražnom nalogu[7] i Konvencija o uzajamnoj pravnoj pomoći iz 2000.[8]. Angažiranje pravnog zastupnika trebalo bi biti u skladu s postupcima utvrđenima u instrumentima i zakonodavstvu koji se primjenjuju na sudske postupke. Nadležna tijela države članice u kojoj pravni zastupnik boravi ili ima poslovni nastan trebala bi djelovati u skladu s ulogom koja je za njih utvrđena u odgovarajućem instrumentu, ako i kada je predviđeno njihovo sudjelovanje."*

[17] Europski odbor za zaštitu podataka kritizirao je „pojednostavljeni" zaključak Komisije iz predmeta o zadržavanju podataka jer Komisija smatra dopuštenim sve što Sud nije izričito spomenuo/zabranio. Europski odbor za zaštitu podataka, mišljenje 23/2018 u kojem se navodi (str. 14.): *„Europski odbor za zaštitu podataka posebno žali što se najniži prag kojim se tijelima kaznenog progona daje mogućnost traženja pristupa podacima o pretplatniku ili sadržaju za bilo koje kazneno djelo temelji na a contrario tumačenju sudske prakse Suda Europske unije..."* Vidi i Deutscher Richterbund, br. 6/18 i Europska komora za kazneno pravo, Mišljenje o elektroničkim dokazima, kojim se zahtijeva smisleno obavješćivanje uz moguću reakciju u određenom vremenskom roku.

kategorizacija odstupa od definicija kategorija podataka iz postojećeg europskog zakonodavstva[18] u području zaštite podataka i privatnosti elektroničkih komunikacija, kao i međunarodnih ugovora[19], što dovodi do rizika od nepodudarnosti i neusklađenosti sa sudskom praksom Suda Europske unije i Europskog suda za ljudska prava.[20]

[18] Članak 10. stavak 2. točka (e) Direktive 2014/41/EU o EIN-u, članak 4. stavak 3. točka (c) prijedloga Uredbe o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (COM(2017)10).
[19] Konvencija Vijeća Europe o kibernetičkom kriminalu.
[20] Vidi 2. radni dokument o području primjene, posebno u pogledu pitanja dinamičkih IP adresa.