UDK 343.7(4)
004.3/.4(4)
Primljeno 19. rujna 2022.
Izvorni znanstveni rad
DOI 10.54070/hljk.29.2.7

Dr. sc. Ivan Glavić *

NEPOSREDNA MEĐUNARODNA SURADNJA PREMA DRUGOM DODATNOM PROTOKOLU UZ KONVENCIJU O KIBERNETIČKOM KRIMINALU

U ovom radu analiziraju se odredbe o neposrednoj suradnji tijela otkrivanja i progona kaznenih djela s pružateljima usluga u stranoj državi koje proizlaze iz Drugog dodatnog protokola uz Konvenciju Vijeća Europe o kibernetičkom kriminalu. Svrha je navedenog međunarodnog izvora pojednostavniti i poboljšati razmjenu podataka nužnih za utvrđivanje identiteta počinitelja, uz visoku razinu zaštite prava korisnika usluga. Naglasak u radu stavljen je na različitost pristupa navedenoj problematici u postojećim pravnim sustavima članica Europske unije i Sjedinjenih Američkih Država te na povezanost razvoja nacionalnih zakonodavstava s čl. 32. Konvencije o neposrednom prekograničnom pristupu javno dostupnim i dobrovoljno otkrivenim podacima. Rezultati rada upućuju na to da Protokol daje osnovu potencijalnim članicama da ga implementiraju u skladu sa svojim postojećim pravnim sustavom ne narušavajući pritom načelo uzajamnosti međunarodne suradnje.

Ključne riječi: neposredna međunarodna suradnja, pružatelji internetskih usluga, pretplatnički podaci, privatnost računalne komunikacije, proširena pretraga računalnog sustava

1. UVOD

Konvencija Vijeća Europe o kibernetičkom kriminalu (u daljnjem tekstu Konvencija)[1] kao prvi obvezujući međunarodnopravni instrument kojim su definirana kaznena djela računalnog kriminaliteta te procesni mehanizmi nužni za njihovo otkrivanje i kazneni progon donesena je u Budimpešti 23. studenog 2001., a stupila je na snagu 1. srpnja 2004. Trenutačno je ratificirana od strane 67 država, gotovo svih članica Vijeća Europe (osim Irske), ali i brojnih

* Dr. sc. Ivan Glavić, zamjenik državnog odvjetnika u Županijskom državnom odvjetništvu u Zagrebu; ivan.glavic@zdozg.dorh.hr; ORCID iD: https://orcid.org/0000-0003-4055-3286

[1] Narodne novine, Međunarodni ugovori, br. 9/2002.

izvaneuropskih država, primjerice Sjedinjenih Američkih Država, Australije, Kanade, Japana.[2] Uz Konvenciju je 28. siječnja 2003. donesen i Dodatni protokol o inkriminiranju djela rasističke i ksenofobne naravi počinjenih pomoću računalnih sustava, kojim su dopunjene njezine materijalne odredbe.[3]

Digitalizacija društva i globalizacija trgovine prouzročili su eksponencijalni rast kaznenih djela povezanih s računalnim sustavom, uz internacionalizaciju kaznenopravnih postupaka, često i kada mjesta djelovanja počinitelja te napadnutog računalnog sustava ili žrtve ostaju u okviru granica jedne države. Mrežni prijenos podataka naime pretpostavlja cijeli niz poslovnih subjekata koji svoje usluge pružaju i izvan granica države u kojoj se nalaze, bilo da se radi o pristupu mreži ili raznim aplikacijama kao što su društvene mreže, internetska trgovina, elektronička pošta, bilo da je posrijedi samo pohranjivanje podataka u ime korisnika računala ili drugog pružatelja usluge.

Povezanost računalnog i organiziranog kriminaliteta, olakšan pristup žrtvi, s posljedičnim povećavanjem razmjera štete, uporaba malicioznih programa i mreže zaraženih računala (botneta) te korištenje raznih alata za prikrivanje i lažno prikazivanje izvorišta komunikacije, samo su neki od čimbenika koji utječu na to da konvencijske odredbe protekom vremena više ne mogu pružiti dovoljno učinkovit odgovor na intenzitet i kvalitetu kaznenih djela povezanih s uporabom računala.[4] Dvadeset godina od donošenja Konvencije, 12. svibnja 2022., u Vijeću Europe otvoren je za potpisivanje Drugi dodatni protokol uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza (u daljnjem tekstu Protokol),[5] popraćen odlukom Europske unije da ga njezine članice potpišu, u interesu Europske unije, što je prije moguće.[6] Trenutačno su ga potpisale 24 države, uključujući četrnaest članica Europske unije, Sjedinjene Američke Države i Japan.[7]

[2] Council of Europe, Chart of signatures and ratifications of Treaty 185, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185 (10. rujna 2022.).

[3] Narodne novine, Međunarodni ugovori, br. 4/2008.

[4] Opširnije u Maurushat, A., *Australia's accession to the Cybercrime Convention: Is the Convention still relevant in combating cybercrime in the era of botnets and obfuscation crime tools,* University of New South Wales Law Journal, vol. 33, issue 2 (2010), str. 432–441; Spiezia, F.*, International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime,* ERA Forum (2022) 23, str. 101–103.

[5] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence, https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224 (10. rujna 2022.).

[6] Odluka Vijeća (EU) 2022/722 od 5. travnja 2022. o ovlašćivanju država članica da u interesu Europske unije potpišu Drugi dodatni protokol uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza, Službeni list Europske unije, br. L. 134, od 11. svibnja 2022.

[7] Council of Europe, Chart of signatures and ratifications of Treaty 224, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=224 (10. rujna 2022.).

Svrha je Protokola jačanje međunarodne suradnje u kaznenim stvarima uspostavom brzog i učinkovitog pristupa elektroničkim dokazima u inozemstvu, uz visoku razinu zaštitnih mjera. Pored mehanizama pravne pomoći pojednostavljenom komunikacijom između državnih tijela (čl. 8.–12.), koji nisu predmet ovog rada, Protokol određuje i mjere neposredne suradnje između tijela kaznenog progona jedne s pružateljima usluga iz druge članice. Riječ je o radikalnom zaokretu u odnosu na klasičnu međunarodnu pravnu pomoć budući da zahtjeve i naloge stranih država izravno izvršavaju privatni poslovni subjekti koji nisu specijalizirani za pitanja međunarodnih pravnih odnosa i zaštite temeljnih interesa države, uključujući i prava okrivljenika i općenito korisnika interneta. Pritom neke od stranaka Konvencije o kibernetičkom kriminalu, a time potencijalno i Protokola, čija tijela mogu uputiti navedene zahtjeve i naloge nisu demokratske.

Ovim radom analiziraju se odredbe Protokola o neposrednoj suradnji s pružateljima usluga, osobito u pogledu načina osiguranja kontrole i odgovornosti državnih tijela na čijem su području poslovni subjekti koji izvršavaju strane zahtjeve i naloge u svrhu zaštite privatnosti korisnika interneta, slobode izražavanja i drugih temeljnih ljudskih prava. U tom smislu navedeni međunarodni izvor bilo je nužno staviti u kontekst same Konvencije i nastojanja njezinih članica da u skladu s njezinim odredbama ili mimo njih u svojem zakonodavstvu pojednostavne prekograničnu dostupnost računalnih podataka. Naglasak je pritom stavljen na države Europske unije te Sjedinjene Američke Države, u kojima se nalazi većina pružatelja usluga.

2. PREKOGRANIČNI PRISTUP PODACIMA PREMA KONVENCIJI O KIBERNETIČKOM KRIMINALU

Određivanje u članku 1. Konvencije računalnog sustava kao naprave ili grupe povezanih naprava od kojih barem jedna temeljem programa obavlja automatsku obradu podataka, pri čemu povezivanje podrazumijeva i ono putem interneta,[8] ima za posljedicu da počinitelj kaznenog djela može upotrebljavati računalni sustav čiji su dijelovi na različitim mjestima te u vlasništvu ili pod kontrolom različitih osoba – korisnika i pružatelja usluge. Prekine li se ta veza prestankom korištenja usluge, takav računalni sustav više ne postoji, ali to ne znači da su podaci o prethodnoj komunikaciji obrisani i da je pružatelj usluge izgubio podatke koji upućuju na identitet korisnika. Posljedično, radnje prikupljanja dokaza mogu se podijeliti na one koje se provode istodobno s komu-

[8] Council of Europe, *Explanatory Report to the Convention on Cybercrime*, 23. XI. 2001., odjeljak 24., str. 5.

nikacijom (presretanje podataka, prikupljanje podataka u realnom vremenu) te one nakon što komunikacija prestane (nalog za dostavu podataka, pretraga računalnog sustava).

Konvencijom su opisane tri kategorije podataka relevantnih za progon kaznenih djela – pretplatnički podaci, podaci o prometu te podaci sadržaju komunikacije – pri čemu su razvrstani prema stupnju miješanja u privatnost korisnika usluge. Pretplatnički podaci u smislu čl. 18. st. 3. Konvencije određeni su kao oni koji se odnose na pretplatnika, a nisu podaci o prometu ili sadržaju komunikacije, te temeljem kojih može biti utvrđena vrsta korištene usluge, tehničke mjere i razdoblje pružanja te pretplatnikov identitet, odnosno podaci iz kojih se on može utvrditi – poštanska ili zemljopisna adresa, broj telefona i drugi pristupni broj, podaci za slanje računa te o plaćanju i mjestu gdje je instalirana oprema. Navedene podatke pružatelji usluga prikupljaju već pri sklapanju pretplatničkog ugovora, uključujući pritom i registraciju usluge putem sučelja na internetu.

Osnovna svrha dohvata navedenih podataka utvrđivanje je identiteta korisnika računala koje se dovodi u vezu s počinjenjem kaznenog djela te, posljedično, poduzimanje daljnjih radnji, kao što su ispitivanje te osobe, pretraga računalnog sustava ili presretanje računalne komunikacije. *Ratio* izdvajanja pretplatničkih podataka kao posebne kategorije oslanja se na okolnost da se radi o niskoj razini miješanja u pravo na privatnost, uslijed čega bi i manje intruzivne mjere, poput pribavljanja bez sudskog naloga ili omogućivanje primjene za sva kaznena djela u zakonodavstvima članica, ispunjavale uvjet proporcionalnosti legitimnom cilju progona kaznenih djela. Prema obrazloženju uz Konvenciju riječ je o „fleksibilnoj mjeri, koju policija može koristiti u mnogim slučajevima, osobito umjesto mjera koje su nametljivije ili više ograničavajuće“.[9] Stoga ih sukladno čl. 18. st. 1.b Konvencije nadležna tijela pribavljaju od pružatelja usluga pukim nalogom za dostavu podataka.

Prikupljanje ostalih podataka o komunikaciji u posjedu ili pod kontrolom pružatelja usluga, kao i presretanje protoka podataka između korisnika i pružatelja usluge, izdvojeno je u posebne odredbe Konvencije: čl. 17. (Hitno očuvanje i djelomično otkrivanje podataka o prometu), čl. 19. (Pretraga i oduzimanje pohranjenih računalnih podataka), čl. 20. (Prikupljanje podataka o prometu u realnom vremenu) i čl. 21. (Presretanje podataka o sadržaju). Time je zakonodavcima članica ostavljen prostor da za mjere intenzivnijeg miješanja u privatnost korisnika osiguraju dodatne zaštitne mehanizme. Ujedno, sukladno čl. 19. Konvencije, članice su dužne domaća tijela kaznenog progona ovlastiti na poduzimanje pretrage svakog dijela računalnog sustava radi pristupa pohranjenim podacima; pa i proširiti je na drugi računalni sustav ako imaju

[9] Ibid., odjeljak 171., str. 29

razloga vjerovati da su traženi podaci u njemu ili u njegovu dijelu pohranjeni i zakonito dostupni iz početnog računalnog sustava.

Sve prethodno navedene mjere odnose se na pristup računalnom sustavu, njegovu dijelu ili mediju za pohranu podataka smještenima unutar jedne države, odnosno na upućivanje naloga za dostavu pružatelju koji usluge nudi na području te države. Konvencija ne određuje pretragu ili njezino proširenje na podatke pohranjene na računalu u drugoj državi, neposredne naloge pružatelju usluga registriranom u drugoj državi za dostavu bilo kakvih podataka o korisnicima, dopuštenje članice da strana tijela izravno dohvaćaju podatke s naprava na njezinu području ili se obraćaju njezinim pružateljima usluga, čak i postupanje te ovlasti tijela kaznenog progona kada im je nepoznata lokacija naprave na kojoj su pohranjeni podaci. Naime tim međunarodnim izvorom predviđen način prikupljanja podataka pohranjenih na prostoru druge članice jest klasična međunarodna pravna pomoć, uz mogućnost da se, do njezina izvršenja ili odbijanja, putem mreže stalno dostupnih kontakata u smislu čl. 16. stranom pružatelju usluga privremeno zabrani brisanje, promjena ili drugo narušavanje cjelovitosti pohranjenih podataka.

Iznimno, člankom 32. određena su dva slučaja neposrednog, jednostranog prekograničnog dohvata ili pribavljanja pohranjenih računalnih podataka – javno dostupnih, neovisno o njihovoj lokaciji, te pohranjenih na području druge države – ako je pribavljen zakonit i dobrovoljan pristanak osobe ovlaštene ih otkriti. Premda je već u postupku donošenja Konvencije razmatrana mogućnost sveobuhvatnog reguliranja neposrednog prekograničnog dohvata, zaključeno je kako se pristup podacima bez ovlaštenja i obavještavanja članice na čijem su području pohranjeni treba zadržati na javnim i dobrovoljno predanim podacima zbog nepostojanja prakse i ovisnosti prikladnog rješenja o konkretnim okolnostima svakog slučaja. Obrazloženje Konvencije nije čak ponudilo ni definiciju ili primjere javno dostupnih podataka, dok su kao primjer ovlaštenika na dobrovoljno otkrivanje pohranjenih podataka navedeni sami korisnici elektroničke pošte i drugih usluga, tj. osobe čiji se podaci pribavljaju.[10]

Inicijalna razmatranja u postupku donošenja Konvencije o osnivanju međunarodne policije za kibernetički kriminalitet ili dodjeljivanju nacionalnim zakonodavcima univerzalne jurisdikcije nad tim kaznenim djelima odmah su odbijena zato što većina država nije bila spremna odreći se svojeg suvereniteta ili prihvatiti da međunarodni istražitelji provode istrage na njezinu području.[11] Unatoč tome usvojene odredbe o izravnom prekograničnom pristupu, kao i

[10] Ibid., odjeljak 293., str. 53.

[11] Cangemi, D., *Procedural Law Provisions of the Council of Europe Convention on Cybercrime*, International Review of Law, Computers & Technology, vol. 18, issue 2 (2004), str. 167.

računalni kriminalitet općenito, nakon donošenja Konvencije intenzivirali su rasprave o jurisdikciji kao integralnom dijelu teritorijalnog suvereniteta. Među ostalim, upozorava se na problematiku višestrukih istovremenih lokacija računalnih podataka, primjerice zbog kontinuiranih prijenosa s jednog na drugi poslužitelj (server), kopiranja podataka zbog sigurnosnih razloga i razloga dostupnosti, ili web-stranica sačinjenih od podataka iz više povezanih izvora.[12] U pravnom smislu moguće je da pružatelj usluge ima sjedište u jednoj jurisdikciji, da se na njega primjenjuje pravni sustav druge jurisdikcije, a da su podaci pohranjeni u trećoj.[13] Premda navedene dileme završavaju zaključkom o „gubitku lokacije", okosnica problema ipak nije u tome da je samo mjesto počinjenja kaznenog djela postalo virtualno, jer počinitelj mora djelovati s određene lokacije, napadnuti sustav ili žrtva moraju se nalaziti na određenoj lokaciji, a računalni podaci moraju biti pohranjeni na medij na određenoj lokaciji. Međutim u lancu počinitelj – pružatelj(i) usluge pristupa internetu – pružatelj(i) usluge elektroničke pošte, prodaje robe, društvenih mreža i slično – pružatelj(i) usluge pohrane podataka – napadnuti sustav ili žrtva nastojanja da se pribave podaci o identitetu korisnika, uključenim računalima ili samoj komunikaciji nailaze na brojne zapreke pravne i tehnološke prirode.

Jednostrani prekogranični pristup iz članka 32. Konvencije ipak se primarno zadržao na javnim i dobrovoljno predanim podacima zbog kompleksnosti garancije prava korisnika usluga, osobito poštivanja osobnog i obiteljskog života. U tom smislu Konvencijom određen neposredan prekogranični pristup nije sporan jer podrazumijeva da je pohranjeni računalni podatak izgubio svojstvo privatnog prije postojanja interesa tijela kaznenog progona zbog prethodne odluke zakonodavca članice ili ovlaštenika prava da se učini široko dostupnim (javno objavljeni podaci), a nakon postojanja interesa tijela kaznenog progona, povodom njihove zamolbe, zbog odricanja od prava na privatnost ovlaštene osobe (dobrovoljni pristanak).

[12] Council of Europe, Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, *Transborder access and jurisdiction: What are the options?* (Report), 6 december 2012, str. 10.

[13] Council of Europe, Cybercrime Convention Committee (T-CY), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY* (Final report), 16 September 2016, str. 15; Kleijssen, J., Perri, P.: *Cybercrime, Evidence and Territoriality, Issues and Options*, u M. Kuijer, M., Werner, W. (ur.), *Netherlands Yearbook of International Law (The Changing Nature of Territoriality in International Law)*, br. 47/2016, str. 158.

3. PREKOGRANIČNI PRISTUP PODACIMA U PRAVU ČLANICA KONVENCIJE O KIBERNETIČKOM KRIMINALU

Razvoj tehnologije i nacionalnih pravnih sustava tijekom dvadeset godina od donošenja Konvencije stvorili su preduvjete za daljnje širenje instituta prekograničnog pristupa. Paradoksalno, razjašnjavanje tehnološko-pravnih implikacija ipak nije dovelo do približavanja zakonodavstava članica. Uz nerazmjer u količini podataka izravno dohvaćenih iz inozemstva i onih izravno dohvaćenih s njihovih područja, države su različito normirale i same institute javno dostupnih te pretplatničkih i podataka o prometu, kao i krug ovlaštenika dobrovoljnog pristanka na otkrivanje pohranjenih podataka.

3.1. Javno dostupni podaci

Osnovna kategorija javno objavljenih podataka jesu oni učinjeni takvima iz razloga transparentnosti ili u drugom društvenom interesu, što ovisi o konkretnom nacionalnom pravnom sustavu. Najčešće je riječ o telefonskim imenicima, podacima iz zemljišnih knjiga, sudskim i komorskim registrima poslovnih subjekata, provedenim javnim nabavama. Podaci o fizičkim i pravnim osobama koje su registrirale web-stranice i upravljaju njima te o drugim internetskim domenama (registranti) tradicionalno su bili dostupni pukim unosom naziva u javne preglednike[14] te su i dalje takvi u većini država. Tijela kaznenog progona stoga ih slobodno mogu dohvatiti, bilo da je registrant osoba koja se povezuje s kaznenim djelom bilo da od njega treba zatražiti podatke o pristupateljima domeni (npr. onima koji su na njoj objavili zabranjeni sadržaj ili su je koristili za komunikaciju s napadnutim računalnim sustavom i žrtvom).

Stupanjem na snagu Opće uredbe o zaštiti podataka (u daljnjem tekstu GDPR)[15] 25. svibnja 2018. registrari (osobe koje drugima pružaju uslugu registracije domena) i voditelji registra vršnih domena iz Europske unije[16] bili su u obvezi ukloniti sve dotad postojeće javno dostupne podatke o registrantima fizičkim osobama i ne objavljivati ih ubuduće.[17] Posljedično, tijela kaznenog

[14] Npr. preglednik domena na stranicama ICAAN-a (Internet Corporation for Assigned Names and Numbers) na: https://lookup.icann.org/en (10. rujna 2022.).

[15] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ, Službeni list Europske unije, br. L 119/1, 4. svibnja 2016.

[16] Npr. CARNET (za domenu .hr), usp. Pravilnik o ustrojstvu i upravljanju vršnom nacionalnom internetskom domenom (Narodne novine, br. 38/2010, 81/2015, 5/2017, 76/2022).

[17] Usp. Politiku privatnosti CARNET-a, https://domene.hr/portal/files/Obavijest_o_privatnosti_Registar_domena_hr.pdf?20200709-1 (10. rujna 2022.).

progona članica Europske unije mogu slobodno dohvatiti takve podatke izvan Europske unije, međutim to nije dohvat podataka utemeljen na uzajamnosti jer tijela drugih država dostavljanje podataka iz Europske unije mogu zatražiti isključivo putem međunarodne pravne pomoći.

Suštinski privatni podaci također mogu postati javni odrekne li se ovlaštenik prava na anonimnost računalne komunikacije, primjerice objavom sadržaja na društvenim mrežama, forumima i platformama za dijeljenje datoteka pristupačnim većem broju ljudi.

Prema hrvatskoj sudskoj praksi redarstvene vlasti navedene objave mogu slobodno dohvatiti i to ne predstavlja pretragu uređaja koji služi prikupljanju, pohrani ili prijenosu podataka, pa nije potrebno primijeniti odredbe članaka 257., 262. i 263. Zakona o kaznenom postupku, već se radi o dokazu pribavljenom na zakonit način sukladno Pravilniku o načinu postupanja policijskih službenika i Zakonu o policijskim poslovima i ovlastima.[18] Ipak, ne radi se o dokaznoj radnji koja proizlazi isključivo iz policijskih propisa. Uostalom, to bi za posljedicu imalo da javno objavljeni sadržaj na internetu ne bi bili ovlašteni dohvatiti državno odvjetništvo, privatni tužitelj ili sud koji vodi postupak. Riječ je o privremenom oduzimanju predmeta iz čl. 263. st. 1. i 3. u svezi s čl. 261. st. 1. Zakona o kaznenom postupku, odnosno elektroničkog (digitalnog) dokaza iz čl. 331. u svezi s čl. 263. st. 1. i 3. Zakona o kaznenom postupku, tehničkim snimanjem podataka pohranjenih na poslužitelju (serveru) lociranom u stranoj državi, u posjedu ili pod kontrolom pružatelja usluge društvene mreže. Priroda javno dostupnih podataka pritom isključuje primjenu prisilnih mjera, kao što su upućivanje zahtjeva za predaju podataka i kažnjavanje za nepostupanje po njemu u smislu čl. 261. st. 2. i 3. i čl. 263. st. 2. Zakona o kaznenom postupku.

Javnost objavljenog sadržaja nije u korelaciji s javnošću identiteta korisnika, primjerice kada je profil anoniman, izmišljen ili kreiran korištenjem tuđih osobnih podataka. Ujedno ne predstavlja, *eo ipso,* odricanje od legitimnog očekivanja korisnika da će njegova elektronička komunikacija ostati privatna. Europski sud za ljudska prava naime, polazeći od toga da je zaštitom prava na osobni i obiteljski život, među ostalim, obuhvaćeno i pravo na identitet i osobni razvoj, pa time i pravo uspostavljanja i razvijanja veza s drugim ljudima i vanjskim svijetom, zauzima shvaćanje da postoji zona interakcije s drugima, čak i u javnom kontekstu, koja pripada području privatnog života. Stoga je, procjenjujući da se unatoč javnosti sadržaja mrežne komunikacije ona ipak odvijala uz visok stupanj anonimnosti, uzimao u obzir da korisnik nije u bilo kojem trenutku otkrivao svoj stvarni identitet i da

[18] Usp. Županijski sud u Zagrebu, broj Kž-1143/2019-3, 14. siječnja 2020.

ga nije bilo moguće identificirati putem podataka (ostavljenih) u korisničkom računu ili za potrebe kontakta.[19]

Pored toga nalaganje intruzivnih mjera pukim oslanjanjem na objavljeno ime ili sliku neke osobe na profilu, bez dužne pažnje i provjere je li ta osoba doista kreirala korisnički račun ili je povezana s njim, predstavljalo bi nerazmjerno upletanje u ljudska prava. Prema shvaćanju Europskog suda za ljudska prava, pretraga doma i oduzimanje računala kao miješanje u pravo na privatan i obiteljski život mora biti utemeljena na postojanju razumne sumnje da se provodi nad počiniteljem kaznenog djela kako bi bio ispunjen uvjet nužnosti u demokratskom društvu.[20]

Detalji o stvarnim korisnicima društvenih mreža, javnog ili ograničenog pristupa, kao i elektroničke pošte, trgovine i sličnih usluga utvrdivi su i provjerljivi ukoliko tijela kaznenog progona raspolažu podatkom o dodijeljenom broju računalu na internetu, IP adresi, bilo da je ona pribavljena temeljem materijala koji je dostavila žrtva bilo da se do nje došlo pretragom računalnog sustava ili drugim dokaznim radnjama. Tijela kaznenog progona temeljem čl. 32. Konvencije mogu utvrditi stranog pružatelja usluge koji raspolaže konkretnom IP adresom pod uvjetom da se radi o javno dostupnim podacima,[21] za razliku od imena ili naziva korisnika kojem je IP adresa dalje dodijeljena.

Registranti domena također imaju položaj pružatelja usluga drugome jer se radi o djelatnosti omogućavanja pristupa i razmjene informacija. Bez obzira na to što je sadržaj ostavljen na domeni u pravilu javan, oni, kao i drugi pružatelji usluga iz Europske unije, ne mogu dobrovoljno dostavljati osobne podatke korisnika fizičkih osoba (uključujući i ime i prezime te IP adresu) bez njihove privole, osim što iznimno mogu nadležna tijela upozoriti na moguća kaznena djela (ili prijetnje javnoj sigurnosti).[22] Međutim domašaj navedene iznimke ograničen je time što registranti u pravilu nisu obvezni kontrolirati na domeni objavljen sadržaj, pa eventualna saznanja o počinjenim kaznenim djelima pristupatelja crpe zaprimanjem prigovora oštećenika i trećih osoba.[23] Stoga su tijela kaznenog progona iz Europske unije u pravilu upućena od registranata zatražiti osobne podatke pristupatelja koristeći prisilne mjere sukladno po-

[19] Usp. Europski sud za ljudska prava, Benedik protiv Slovenije (2018); analiza odluke u: Pirc Musar, N., *Benedik v Slovenia: Dynamic IP and Communication Privacy*, European Data Protection Law Review, vol. 4, issue 4 (2018), str. 556–559.

[20] Usp. Europski sud za ljudska prava, Yuditskaya i drugi protiv Rusije, 12. veljače 2015.

[21] Usp. preglednik https://lookup.icann.org/en (10. rujna 2022.).

[22] Usp. obrazloženje odjeljka 50. uvoda GDPR-a.

[23] Usp. Tosza, S., *Internet service providers as law enforcers and adjudicators. A public role of private actors.*, Computer Law & Security Review, 43 (2021), str. 3–7.

sebnoj direktivi[24] i nacionalnom zakonodavstvu (u Republici Hrvatskoj kroz dokaznu radnju privremenog oduzimanja predmeta), a tijela kaznenog progona izvan Europske unije putem međunarodne pravne pomoći.

3.2. Pretplatnički i prometni podaci

3.2.1. Sjedinjene Američke Države

Povodom spora nastalog odbijanjem Microsofta da kao poslovni subjekt sa sjedištem u Sjedinjenim Američkim Državama postupi po domaćem nalogu za dostavu podataka o komunikaciji korisnika pohranjenih izvan državnog područja[25] u ožujku 2018. donesen je tzv. CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*), dopuna Zakona o pohranjenoj komunikaciji.[26] Pored razjašnjavanja ovlasti domaćih tijela u dohvatu računalnih podataka lociranih u inozemstvu navedenim propisom normirane su i ovlasti drugih država za izravno upućivanje naloga za otkrivanje podataka američkim pružateljima usluga. Načelno, oni su dužni postupiti u skladu s obvezama „očuvanja, izrade kopije ili otkrivanja sadržaja žičane ili elektroničke komunikacije i bilo kojeg zapisa ili drugog podatka koji se odnosi na korisnika ili pretplatnika, a koji su u posjedu, čuvanju ili pod kontrolom pružatelja usluga, neovisno o tome je li takva komunikacija, zapis ili drugi podatak lociran unutar ili izvan područja Sjedinjenih Američkih Država".[27] Nalog im, osim domaćih tijela, mogu izravno uputiti i „kvalificirane" strane vlasti, tj. tijela one države koja sa Sjedinjenim Američkim Državama ima potpisan poseban sporazum.[28] Navedena mjera obrazložena je potrebom brzog pristupa računalnim podacima koje drže američki pružatelji globalnih usluga, ključnih u istraživanju ozbiljnih kaznenih djela, od strane država koje imaju zajamčen sustav zaštite privatnosti i

[24] Direktiva (EU) 2016/680 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka od strane nadležnih tijela u svrhe sprečavanja, istrage, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Okvirne odluke Vijeća 2008/977/PUP, Službeni list Europske unije, L. 119/89, 4. svibnja 2016.

[25] Usp. Daskal, J., *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, Stanford Law Review (Online), vol. 71 (2018), https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/ (10. rujna 2022.); Maillart, JB., *The limits of subjective territorial jurisdiction in the context of cybercrime*, ERA Forum 19, 375–390 (2019), https://doi.org/10.1007/s12027-018-0527-2 (10. rujna 2022.); Davis, F. T., Gressel, A. R., *Storm Clouds or Silver Linings*?, Litigation, vol. 45, no. 1 (2018), str. 48–52.

[26] Stored Communication Act, U. S. Code, title 18, chapter 121.

[27] U. S. Code, title 18, chapter 121, section 2713.

[28] U. S. Code, title 18, chapter 121, section 2703(h)(5).

građanskih sloboda.[29] Sporazumi su trenutačno potpisani s Ujedinjenim Kraljevstvom[30] i Australijom,[31] dok su u tijeku pregovori s Europskom unijom[32] i Kanadom.[33]

Različito od dostavljanja podataka temeljem CLOUD Acta, koje je prisilno, američkim pružateljima usluga dopušteno je i dobrovoljno otkrivanje, među ostalim temeljem zahtjeva domaćih i stranih tijela kaznenog progona. Navedenu fleksibilnost omogućuju odredbe Zakona o pohranjenoj komunikaciji iz 1986.[34] Navedeni propis opisuje i dvije vrste podataka koji bi u smislu Konvencije odgovarali pojmovima pretplatničkih podataka i podataka o prometu komunikacije. Tako pojam „osnovni pretplatnički podaci", pored imena/naziva, podataka o konekciji, trajanju i vrsti usluge te sredstvima plaćanja, podrazumijeva i mrežnu adresu (tj. IP adresu kod korištenja interneta) privremeno dodijeljenu korisniku. Ekstenzivni podaci o prijenosu podataka, uključujući i one koji bi otkrili osobe s kojima je korisnik komunicirao i uopće odredište komunikacije, normirani su kao „zapisi i drugi podaci koji se odnose na klijente i pretplatnike".[35]

Dobrovoljno otkrivanje podataka o uslugama dostupnim javnosti ovisi o vrsti podataka o kojima je riječ. Zakonom su propisane samo iznimke pod kojima je ono dopušteno, pri čemu su one za osnovne pretplatničke podatke i podatke koji se odnose na klijente i pretplatnike razmjerno široke, različito od podataka o sadržaju komunikacije.[36] Posljedično, dostavljanje tih podataka

[29] U. S. Department of Justice, *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* (White Paper), April 2019, str. 2, 5, 10, 11.

[30] Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on Access to Electronic Data for the Purpose of Countering Serious Crime, October 3, 2019, https://www.justice.gov/dag/cloud-act-agreement-between-governments-us-united-kingdom-great-britain-and-northern-ireland (10. rujna 2022.).

[31] Agreement between the Government of the United States of America and the Government of Australia on Access to Electronic Data for the Purpose of Countering Serious Crime, Deceber 15, 2021, https://www.justice.gov/dag/cloud-act-agreement-between-governments-us-and-australia (10. rujna 2022.).

[32] European Commission, Joint statement on the launch of EU-U.S. negotiations to facilitate access to electronic evidence, 26 September 2019, https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_19_5890 (10. rujna 2022).

[33] U. S. Department of Justice, United States and Canada Welcome Negotiations of a CLOUD Act Agreement, 22 March 2022, https://www.justice.gov/opa/pr/united-states-and-canada-welcome-negotiations-cloud-act-agreement (10. rujna 2022.).

[34] U. S. Code, title 18, chapter 121, section 2702, 2703.

[35] Executive Office for United States Attorneys, Office of Legal Education, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 3. izdanje, str. 121–122. https://www.justice.gov/file/442111/download (10. rujna 2022.).

[36] Usp. U. S. Code, title 18, chapter 121, section 2702.

podložno je slobodnoj ocjeni pružatelja usluga, međutim u praksi to znači arbitrarnost. Naime oni samostalno odlučuju hoće li uopće, u koje vrijeme i na koji način udovoljiti traženju, pa čak i hoće li o činjenici dostavljanja podataka obavijestiti samog klijenta, što dovodi do različitog postupanja čak i kada je riječ o istom pružatelju usluga.[37] Međutim odbijanja dobrovoljnog otkrivanja podataka česta su i kada njihovo traženje prisilnim mjerama putem međunarodne pravne pomoći ne bi imalo učinka jer bi udovoljenje zaprimljenoj zamolnici vlasti Sjedinjenih Američkih Država (temeljem čl. 27. st. 4.b Konvencije) odbile pozivajući se na zaštitu slobode govora kao bitnog interesa države. To se osobito odnosi na slučajeve koji bi u hrvatskom pravu bili podvedivi pod kazneno djelo javnog poticanja na nasilje i mržnju iz čl. 325. Kaznenog zakona, a koji su prema praksi Vrhovnog suda Sjedinjenih Američkih Država kažnjivi samo kada predstavljaju istinsku prijetnju (usmjereni na poticanje ili izazivanje neposredno prijeteće protupravne radnje i vjerojatno je da bi potakli ili izazvali takvu radnju) ili odgovaraju borbenim izrazima (suštinski nanose povredu ili teže poticanju neposrednog narušavanja mira).[38] Zaštita slobode govora koja proizlazi iz Prvog amandmana na Ustav pritom se odnosi i na mrežne objave putem američkih pružatelja usluga, čak i kada je sadržaj dostupan ili usmjeren korisnicima iz drugih država u kojima je zabranjen kao rasistički ili kao govor mržnje.[39]

Institut dobrovoljnog otkrivanja pretplatničkih i podataka o prometu koristi se relativno često. Tijekom 2015. Apple, Facebook, Google, Microsoft, Twitter i Yahoo zaprimili su 227 962 traženja za takvim otkrivanjem podataka, pretežito iz inozemstva (138 612 traženja), a ostatak od američkih vlasti. Dvije trećine slučajeva rezultiralo je dostavom zatraženih pretplatničkih i podataka o prometu komunikacije.[40]

[37] Usp. Council of Europe, Cybercrime Convention Committee (T-CY), Cloud evidence group, *Criminal justice access to dana in the cloud: Cooperation with „foreign" service providers* (Background paper), 3 May 2016, str. 22, 24, 25.

[38] Van Blarcum, C. D., *Internet Hate Speech: The European Framework and the Emerging American Haven*, 62 Wash. & Lee L. Rev. 781 (2005), str. 809–814.

[39] Usp. Banks, J., *Regulating hate speech online,* International Review of Law, Computers & Technology, vol. 24, no. 3 (2010), str. 234–237; Murphy, S. D., *Contemporary practice of the United States relating to international law*, The American Journal of International Law, vol. 96, no. 4 (2002), str. 973–975.

[40] Council of Europe, Cybercrime Convention Committee (T-CY), *Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY* (Final report), op. cit. (13), str. 25.

3.2.2. Članice Europske unije

Osim ograničenjima koja proizlaze iz GDPR-a i odnose se isključivo na korisnike fizičke osobe, zaštita privatnosti računalne komunikacije u pravu Europske unije detaljno je razrađena Direktivom 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama), izmijenjenom Direktivom 2009/136/EZ od 25. studenoga 2009.[41] Različito od Konvencije, kojom su razdvojene kategorije pretplatničkih i prometnih podataka, člankom 2. Direktive obuhvaćeni su samo podaci o prometu, oni koji se obrađuju u svrhu prijenosa komunikacije na elektroničkoj komunikacijskoj mreži ili za njezino naplaćivanje. Člankom 6. stavkom 1. Direktive određeno je da se takvi podaci koji se odnose na pretplatnike i korisnike moraju obrisati ili anonimizirati od strane pružatelja usluga kada više nisu potrebni u svrhu prijenosa komunikacije, osim u slučaju iznimki određenih Direktivom.

Direktiva ne sadrži odredbe o obvezama ili suradnji pružatelja usluga u Europskoj uniji s tijelima kaznenog progona, osim što kao iznimku od obveznog brisanja ili anonimiziranja podataka o prometu u čl. 15. st. 1. općenito omogućuje članicama donošenje zakonskih mjera ograničenja obveza pružatelja usluge kada ono predstavlja nužnu, prikladnu i razmjernu mjeru unutar demokratskog društva, među ostalim s ciljem sprečavanja, istrage, otkrivanja i progona kaznenih djela. To pretpostavlja i mogućnost donošenja zakona kojima se omogućuje zadržavanje podataka tijekom ograničenog razdoblja. Nastojanje da se takva iznimka unificira predstavljala je Direktiva Europskog parlamenta i Vijeća 2006/24/EZ od 15. ožujka 2006. (tzv. Direktiva o zadržavanju podataka),[42] kojom su članice bile dužne osigurati da pružatelji usluga u roku koji ne može biti kraći od šest mjeseci ni dulji od dvije godine prikupljaju i čuvaju sve podatke o izvoru, odredištu, nadnevku, trajanju i vrsti komunikacije, kao i identifikaciju i lokaciju korištene opreme, kako bi se ti podaci mogli koristiti za progon počinitelja teških kaznenih djela ili poslove nacionalne sigurnosti. Međutim odlukom Suda Europske unije iz 2014.[43] Direktiva je proglašena ništavnom zbog povrede načela razmjernosti. Pritom je zauzeto stajalište da podaci koje su pružatelji usluga bili obvezni zadržati, uzeti zajedno, omogućuju donošenje vrlo preciznih zaključaka o privatnom životu korisnika, kao što su svakodnevne navike, mjesta trajnih ili privremenih boravaka, dnevna ili druga kretanja, obavljane aktivnosti, društveni odnosi i društvene sredine koje su te

[41] Službeni list Europske unije, br. L. 201, 31. srpnja 2002., br. L. 337, 18. prosinca 2009.
[42] Službeni list Europske unije, br. L. 105, 15. ožujka 2006.
[43] Predmet br. C-293/12 i C-594/12 od 8. travnja 2014.

osobe posjećivale. Među razlozima poništenja bilo je i neodređivanje kruga teških kaznenih djela za koje se podaci mogu zatražiti.

Posljedično, uređenje instituta zadržavanja podataka o prometu komunikacije prepušteno je nacionalnim zakonodavcima pod uvjetima iz čl. 15. st. 1. Direktive o privatnosti i elektroničkim komunikacijama. Sud Europske unije ocijenio je kako navedenu normu treba tumačiti na način da joj se protive nacionalne zakonske mjere kojima se preventivno, u svrhu borbe protiv teških kaznenih djela, predviđa opće i neselektivno zadržavanje podataka o prometu i lokaciji komunikacije. Međutim navedeno se ne odnosi na opće i neselektivno zadržavanje podataka o dodijeljenim IP adresama korisnicima u svrhu borbe protiv teških kaznenih djela i kada je razdoblje zadržavanja ograničeno na strogo nužno te na opće i neselektivno zadržavanje podataka o građanskom identitetu korisnika elektroničkih komunikacijskih sredstava u svrhu borbe protiv kaznenih djela općenito. Osim toga čl. 15. st. 1. Direktive ne predstavlja zapreku za nacionalne zakonske mjere kojima se omogućuje, u svrhu borbe protiv teških kaznenih djela, izdavanje naloga pružateljima elektroničkih komunikacijskih usluga da u određenom trajanju provedu *a fortiori* hitno zadržavanje podataka o prometu i lokaciji komunikacije, pod uvjetom da je takav nalog izdan u obliku odluke nadležnog tijela koja podliježe djelotvornom sudskom nadzoru.[44]

U hrvatskom pravu zadržavanje podataka o prometu kroz razdoblje od godinu dana od ostvarene komunikacije obveza je pružatelja usluga sukladno čl. 53. i čl. 54. Zakona o elektroničkim komunikacijama.[45] Dohvat tih podataka određen je kao dokazna radnja uspostavljanja telekomunikacijskog kontakta iz čl. 339.a. Zakona o kaznenom postupku, koju nalaže sudac istrage ili u hitnim slučajevima državni odvjetnik, uz naknadno odobrenje suca istrage, za kataloški nabrojena teška kaznena djela. Zatražiti se mogu isključivo svi zadržani podaci, uključujući pritom i one irelevantne za utvrđivanje identiteta korisnika, kao što su trajanje komunikacije, serijski broj uređaja ili vrsta korištene usluge.

Odlukom Suda Europske unije iz 2018.[46] ocijenjeno je kako članak 15. stavak 1. Direktive o privatnosti i elektroničkim komunikacijama valja tumačiti „na način da pristup državnih tijela podacima o identitetu nositelja SIM kartica aktiviranih ukradenim mobilnim telefonom, poput imena, prezimena i, prema potrebi, adrese tih nositelja, predstavlja zadiranje u njihova temeljna prava priznata navedenim člancima Povelje o temeljnim pravima koje nije tako ozbiljno da bi taj pristup, u okviru sprečavanja, istrage, otkrivanja i progona kaznenih djela, trebalo odobriti samo kad je riječ o borbi protiv teškog kriminaliteta.“ U

[44] Predmeti br. C511/18, C512/18 i C520/18 od 6. listopada 2020., C-140/20 od 5. travnja 2022., C-793/19 i C-794/19 od 20. rujna 2022.

[45] Narodne novine, br. 76/2022.

[46] Predmet br. C-207/16 od 2. listopada 2018.

hrvatskom pravu takva mogućnost da se zatraže samo zadržani podaci potrebni za početno utvrđivanje identiteta korisnika usluge neovisno o težini kaznenog djela i mimo sudskog naloga nije iskorištena.

Sukladno predloženim intervencijama u (Komisijin) Prijedlog Uredbe Europskog parlamenta i Vijeća o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima,[47] podaci o računalnoj komunikaciji podijelili bi se na pretplatničke, podatke o prometu te podatke o sadržaju. Pretplatnički podaci bili bi pritom oni koji su prikupljeni tijekom uobičajenog poslovanja, a odnose se na ime, datum rođenja, poštansku ili zemljopisnu adresu, podatke za plaćanje, broj telefona ili adresu elektroničke pošte kojima se identificira pretplatnik ili klijent te vrstu pružene usluge i trajanje ugovora s pružateljem usluga, koji su strogo nužni radi isključive svrhe identifikacije korisnika usluge. IP adrese dodijeljene korisniku pripadale bi kategoriji pretplatničkih ili podataka o prometu, ovisno u svakom pojedinačnom slučaju o svrsi za koju se traže (početna identifikacija korisnika ili prikupljanje daljnjih dokaza o kaznenom djelu). Tijela kaznenog progona bila bi ovlaštena zahtjev za dostavljanje podataka uputiti izravno pravnom zastupniku pružatelja usluge u drugoj članici Europske unije, međutim samu odluku o dostavljanju pretplatničkih podataka ili IP adresa sa svrhom identifikacije korisnika bio bi ovlašten, pored suda, donijeti ili odobriti i tužitelj za sva kaznena djela; a podataka o prometu i sadržaju isključivo sudbena vlast za kaznena djela za koja je propisana kazna zatvora od barem tri godine ili za određena kataloški nabrojena teža kaznena djela. Predloženi koncept neposredne komunikacije tijela jedne s pružateljem usluga iz druge članice izazvao je određene kritike, među ostalim da čl. 82. st. 1. Ugovora o funkcioniranju Europske unije zahtijeva suradnju među tijelima članica koja obavljaju pravosudnu funkciju, što pružatelji usluga nisu,[48] da se odbacuju mehanizmi sudske kontrole i ispitivanja, a na privatne pružatelje usluga neprimjereno prebacuje odgovornost za zaštitu temeljnih ljudskih prava,[49] da nije adekvatno riješena situacija suprotstavljenih obveza u kojima se pružatelj usluge nalazi ako istodobno mora postupiti po zahtjevu članice za dostavom podataka, a pravo treće države (npr. one na čijem

[47] Usp. Nacrt zakonodavne rezolucije Europskog parlamenta o Prijedlogu uredbe Europskog parlamenta i Vijeća o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima (COM(2018)0225 – C8-0155/2018 – 2018/0108(COD), prosinac 2020., https://www.europarl.europa.eu/doceo/document/A-9-2020-0256_HR.html#_section3 (10. rujna 2022.).

[48] Usp. Spiezia, F., op. cit. (4), str. 106.

[49] Usp. Mitsilegas, V., *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, Maastricht Journal of European and Comparative Law, vol. 25, issue 3 (2018), str. 264–265.

su području podaci pohranjeni) zabranjuje takav prijenos.[50] Stupi li navedena Uredba na snagu, primjenjivat će se u međusobnim odnosima članica Europske unije budući da je samim Drugim dodatnim protokolom uz Konvenciju (čl. 15.) određeno da je on supsidijarne naravi.

Prema čl. 48. GDPR-a sudske ili upravne odluke tijela trećih država kojima se od voditelja obrade osobnih podataka u Europskoj uniji (što obuhvaća i pružatelje usluga) zahtijeva otkrivanje osobnih podataka mogu biti priznate ili izvršive samo ako se temelje na međunarodnom sporazumu koji je na snazi između države koja je podnijela zahtjev i članice Europske unije. Premda su propisane i određene iznimke od tog pravila, one nisu primjenjive na kaznene postupke u trećoj državi. Članice Europske unije potpisnice su nekih konvencija i sporazuma koji se odnose na obradu osobnih podataka, primjerice Konvencije Vijeća Europe za zaštitu osoba glede automatizirane obrade osobnih podataka od 28. siječnja 1981., s dodatnim Protokolom od 8. studenoga 2001.,[51] te Sporazuma između Sjedinjenih Američkih Država i Europske unije o zaštiti osobnih informacija u vezi sa sprečavanjem, istragom, otkrivanjem i progonom kaznenih djela.[52] Međutim navedeni izvori uređuju načela obrade osobnih podataka, a ne neposrednu komunikaciju između tijela kaznenog progona trećih država i domaćih pružatelja usluga koja bi u smislu čl. 48. GDPR-a rezultirala dostavljanjem pretplatničkih podataka.

Pored ograničenja neposrednog prekograničnog pristupa pretplatničkim podacima proizašlih iz prava Europske unije, s obzirom na to da su njezine članice ujedno i članice Vijeća Europe, postoje i ona vezana uz Europsku konvenciju za zaštitu ljudskih prava i temeljnih sloboda. Europski sud za ljudska prava otprije je zauzeo stajalište kako je privatnost komunikacije kategorija šira od samog prenesenog sadržaja. Podaci o osobama koje uspostavljaju telefonsku komunikaciju, ispis prometa, kao i podaci o vremenu te duljini poziva predstavljaju integralni element komunikacije te su, posljedično, uz sadržaj objekt prava na poštovanje privatnog i obiteljskog života kao zaštićene vrijednosti iz čl. 8. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda.[53] Razvojem tehnologije navedeno stajalište prošireno je i na uporabu računala i interneta neovisno o tome koristi li se pritom netko privatnim ili službenim računalom.[54]

[50] Usp. Brière, C., EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments, *European Papers*, vol. 6, no 1 (2021), str. 501–502.

[51] Narodne novine, Međunarodni ugovori, br. 4/2005.

[52] Službeni list Europske unije, br. L. 336, 10. prosinca 2016.

[53] Malone protiv Ujedinjenog Kraljevstva (1985) i Valenzuela Contreras protiv Španjolske (1998).

[54] Copland protiv Ujedinjenog Kraljevstva (2007).

U predmetu razmjene sadržaja putem računalnih aplikacija zauzeto je stajalište da podaci kojima teleoperater raspolaže o korisniku kojem je dodijelio IP adresu također uživaju zaštitu privatnosti. Pritom se okolnost da korisnik nije tehničkim putem sakrio ili prikrio IP adresu sama za sebe ne smatra svjesnim izlaganjem javnosti i odricanjem od prava na privatnost jer se navedeni podatak, kada je i vidljiv ostalim korisnicima na mreži, ne može povezati s određenim računalom bez traženja podataka od teleoperatera.[55]

Praksa Suda stoga ne podržava mogućnost da se članica Vijeća Europe oslobodi obveze zaštite prava na osobni i obiteljski život pukim prepuštanjem pružateljima usluga da bez kontrole tijela javne vlasti slobodno odlučuju o uvjetima i načinu suradnje s tijelima drugih država u otkrivanju podataka korisnika. Navedeno vrijedi za sve vrste podataka – pretplatničke, prometne i sadržaj komunikacije. Pružatelji usluga kao poslovni subjekti naime nisu ovlašteni odreći se prava na privatnost u ime korisnika. Međutim jednako tako ne mogu biti jedini garant zaštite prava klijenata jer se pozitivna obveza države da učinkovito istraži povrede prava na privatnost računalne komunikacije odnosi i na kršenja počinjena od strane privatnih osoba.[56] U konačnici, država je odgovorna za povredu prava iz čl. 8. Europske konvencije za zaštitu ljudskih prava i temeljenih sloboda u svezi s računalnom komunikacijom i samom činjenicom da u svojem zakonodavstvu nije osigurala mjere učinkovite zaštite pojedinaca.[57]

Osim toga država na čijem području djeluju pružatelji usluga ne može odgovornost za zaštitu prava korisnika izbjeći prebacujući je na državu koja je zatražila podatke. Naime sukladno čl. 1. Europske konvencije za zaštitu ljudskih prava i temeljnih sloboda država osigurava svakoj osobi pod svojom jurisdikcijom konvencijska prava i obveze. Posljedično, čak i prilikom izvršavanja inozemne zamolnice za pretragu računalnog sustava od strane njezinih pravosudnih tijela država je odgovorna za zaštitu prava na osobni i privatni život koja proizlazi iz službenih radnji poduzetih na njezinu teritoriju.[58] Stoga nema osnove da se članica oslobodi garantne obveze tako da međunarodnu pravnu pomoć nadomjesti zakonom koji bi dopustio stranoj državi da neposredno i mimo znanja državnih tijela od domaćih pružatelja usluga pribavlja pohranjene podatke.

[55] Usp. Benedik protiv Slovenije (2018).

[56] Usp. Buturugă protiv Rumunjske (2020).

[57] Usp. K. U. protiv Finske (2008).

[58] Usp. Wieser and Bicos Beteiligungen GmbH protiv Austrije (2008).

3.3. Proširenje pretrage računalnog sustava na računalo u inozemstvu

3.3.1. Sjedinjene Američke Države

Odlučivanje o pretrazi računala za federalna kaznena djela u nadležnosti je okružnih sudova. Načelno, nalog može obuhvatiti proširivanje te dokazne radnje s jednog računalnog sustava na drugi s njim povezani sustav, na različitoj lokaciji, međutim ne samo pod uvjetom da su oba smještena na području Sjedinjenih Američkih Država već i unutar istog okruga. U protivnom sud svakog od okruga morao bi izdati zaseban nalog za pretragu računala smještenog na njegovu području. Od 2016. godine normirane su dvije iznimke od navedenog pravila. Okružni sud na čijem su području počinjene radnje kaznenog djela može izdati nalog za udaljeni pristup u svrhu pretrage medija na kojem su pohranjeni elektronički podaci i njihova kopiranja bez obzira na to nalaze li se unutar ili izvan tog okruga: a) ako je uporabom tehnologije prikriveno mjesto na kojemu se nalaze medij ili podaci; b) ako je riječ o istrazi neovlaštenog nanošenja štete zaštićenim računalima smještenim na području pet ili više okruga,[59] što se uglavnom odnosi na kaznena djela počinjena uporabom tzv. botneta, mreže zaraženih računala.[60]

3.3.2. Članice Europske unije

Kao što pozitivno pravo Europske unije ne pruža podlogu za izravnu suradnju između teleoperatera u jednoj te tijela kaznenog progona u drugoj državi, unutar ili izvan Europske unije, ne predviđa ni proširenje pretrage s jednog računalnog sustava na drugi smješten u različitoj državi. Nacionalna zakonodavstva članica po su tom pitanju različita.

Proširenje pretrage računalnog sustava na drugi s njim povezan sustav, bez obzira na lokaciju potonjeg, izmjenama belgijskog Zakona o kaznenom postupku iz 2000. omogućeno je nalogom suca istrage. Prema obrazloženju danom u postupku donošenja propisa, uz rizik gubitka dokaza, osnovni razlog normiranja bila je nemogućnost *a priori* utvrđivanja mjesta gdje treba obaviti pretragu, relevantne dokumente ili čak geografske lokacije računala.[61] Nakon što je Ustavni sud poništio zakonodavne izmjene iz 2016. kojima je ovlast izda-

[59] Federal Rules of Criminal Procedure, Rule 41 (b) (6).

[60] Usp. Federal Rules of Criminal Procedure, Rule 41*, Committee Notes on Rules—2016 Amendment* https://www.law.cornell.edu/rules/frcrmp/rule_41 (10. rujna 2022.).

[61] Chambre des représentants de belgique, *Projet de loi relatif á la criminalité informatique*, N° 213/1, N° 214/1 (résumé), 3 novembre 1999.

vanja naloga za proširenu pretragu računalnog sustava dana državnom odvjetniku,[62] mjera je ponovno vraćena u nadležnost suca istrage. Može se odrediti samo u odnosu na udaljeno računalo kojem korisnik obuhvaćen mjerom ima pristup te ako je nužna za utvrđivanje istine o kaznenom djelu koje je predmet pretrage i ako su druge mjere nerazmjerne ili postoji rizik gubitka dokaza bez njezina proširenja. Nalaze li se podaci izvan Belgije, mogu se samo kopirati, a ako se država na čijem su području pohranjeni može razumno utvrditi, sudac istrage u svrhu obavještavanja nadležnih tijela te države mora bez odlaganja o poduzimanju mjere obavijestiti belgijsku službu nadležnu za pravosuđe.[63]

Francuski Zakon o kaznenom postupku omogućuje pristup podacima relevantnima za tekuću istragu pohranjenim na računalnom sustavu smještenom u domu gdje se obavlja pretraga (ili policijskoj stanici ako se obavlja pretraga oduzetog računala), kao i u drugom računalnom sustavu ako su podaci dostupni iz ili za početni računalni sustav. Međutim zna li se unaprijed da se podaci iz tog drugog računalnog sustava nalaze izvan francuskog područja, mogu se prikupiti samo ako to omogućuje međunarodni sporazum koji je na snazi.[64] Istovremeno posebnim zakonom zabranjeno je francuskim fizičkim i pravnim osobama na bilo koji način razmijeniti dokumente ili podatke gospodarske, trgovinske, industrijske, financijske ili tehničke prirode koji bi bili dokaz za ili u svezi sa stranim sudskim ili upravnim postupcima ako to ne proizlazi iz međunarodnih ugovora ili sporazuma.[65]

Zakonodavstva ostalih članica Europske unije uglavnom nemaju odredbe o proširenju pretrage na drugi računalni sustav, a ako i imaju, svode se na normiranje pretrage početnog računala zajedno s povezanim računalom ili s podacima iz tog računala ako su dostupni iz ili za početno računalo, bez posebne reference na problematiku lokacije drugog računala.[66] Premda se u po-

[62] Cour constitutionnelle, arrêt n° 174/2018 du 6 décembre 2018.

[63] Code d'instruction criminelle, Art. 88ter http://www.droitbelge.be/codes.asp#ins (10. rujna 2022.).

[64] Code de procédure pénale, Article 57-1, https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006151876/?anchor=LEGIARTI000032655328#LEGIARTI000032655328 (10. rujna 2022.).

[65] Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, Art. 1 bis, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326/ (10. rujna 2022.).

[66] Hrvatski Zakon o kaznenom postupku, čl. 257. st. 1.; španjolski Ley de Enjuiciamiento Criminal, Art. 588 sexies c (3)., https://noticias.juridicas.com/base_datos/Penal/lecr.html (10. rujna 2022.); portugalski Lei do Cibercrime, Lei n.° 109/2009, Art. 15.° (5), https://dre.pt/dre/legislacao-consolidada/lei/2009-128879174 (10. rujna 2022.); njemačko i nizozemsko pravo, usp. u Osula, A. M., *Remote search and seizure in domestic criminal procedure: Estonian case study*, International Journal of Law and Information Technology, vol. 24, issue 4 (2016), str. 366–371.

jedinim državama pojavljuju i tumačenja da takve općenite norme omogućuju proširenje pretrage računalnog sustava neovisno o lokaciji računala i podataka,[67] izvan iznimki određenih čl. 32. Konvencije (osobito pristanka osobe nad kojom se provodi pretraga) nije postignut opći konsenzus o dopustivosti proširenja pretrage na inozemna računala i u njima pohranjene podatke bez izričite zakonske ovlasti.

4. NEPOSREDNA PREKOGRANIČNA SURADNJA S PRUŽATELJIMA USLUGA PREMA DRUGOM DODATNOM PROTOKOLU UZ KONVENCIJU O KIBERNETIČKOM KRIMINALU

Odjeljkom naziva „Postupci poboljšanja neposredne suradnje s pružateljima usluga i subjektima u drugim državama" opisana su dva opširna instituta – zahtjev za podatke o registraciji naziva domene (čl. 6.) i otkrivanje pretplatničkih podataka (čl. 7.). Premda tijela kaznenog progona jedne države, primjenjujući navedene institute, formalno doista neposredno komuniciraju s privatnim subjektima u drugoj, riječ je o nastojanju da se međunarodnim pravom reguliraju već postojeći odnosi nastali u nacionalnim zakonodavstvima nakon donošenja Konvencije, a da se istodobno ne naruši uzajamnost u mogućnosti dohvata podataka o računalnoj komunikaciji. Tijelu kaznenog progona zatražene podatke formalno će i dostaviti privatni subjekti iz druge države kojima je upućen zahtjev ili nalog. Međutim suštinski nijedan od navedenih instituta nije se promijenio u odnosu na temeljne postavke konvencijskih odredbi o prekograničnom pristupu javnim i dobrovoljno predanim podacima, odnosno o (klasičnoj) međunarodnoj pomoći, pri čemu je na samoj članici Protokola da se opredijeli za rješenje primjereno njezinu pravnom sustavu.

4.1. Zahtjev za podatke o registraciji naziva domene

Člankom 6. Protokola članice su dužne osigurati zakonodavne i druge mjere kojima bi njihova nadležna tijela u svrhu otkrivanja počinitelja i vođenja postupaka za kaznena djela: a) bila ovlaštena od pružatelja usluge registracije domena u drugoj članici zatražiti podatke koje posjeduju ili kontroliraju u svrhu utvrđivanja ili kontaktiranja registranta domene, te b) dopustila subjektima na svojem području da otkriju te podatke na zahtjev stranih tijela u skladu s razumnim uvjetima osiguranim u domaćem pravu.

[67] Verdelho, P., *Obtaining digital evidence in the global world*, UNIO – EU Law Journal, vol. 5, no. 2 (2019), str. 141–143.

Zahtjevom se može naznačiti uputa o načinu izvršavanja, uključujući i neotkrivanje postojanja zahtjeva registrantu.[68] Zbog nejavne prirode kaznenih postupaka opis i klasifikacija kaznenih djela ne pripada u obvezan sadržaj zahtjeva, već samo izjava da je izdan sukladno Protokolu te da je zatraženo potrebno i bit će upotrijebljeno zbog otkrivanja ili postupka za konkretno kazneno djelo. Međutim pružatelj usluge registracije domena ovlašten je od stranog tijela koje je izdalo zahtjev zatražiti takve podatke.[69] Naime zahtjev ne predstavlja obvezujuću mjeru i „ne utječe na dobrovoljnu prirodu međunarodne suradnje" prema čl. 6. Protokola.[70] Posljedično, nisu predviđene posljedice nepostupanja, osim što se od pružatelja usluge registracije domena kojem je dostavljen zahtjev može zatražiti obrazloženje uskraćivanja podataka, a od nadležnog tijela članice na čijem je području i konzultacije radi utvrđivanja drugih dostupnih mjera za prikupljanje podataka.

Navedena mjera nepotrebna je za dohvat podataka iz država u kojima su podaci o registrantima domena općenito javno dostupni, a iz članica Europske unije ukoliko se radi o javnim podacima registranata pravnih osoba. Međutim kada je i riječ o upućivanju zahtjeva za otkrivanjem osobnih podataka registranata fizičkih osoba u Europskoj uniji, čl. 6. Protokola ne predstavlja suštinski odmak od neposrednog prekograničnog pristupa u smislu čl. 32. Konvencije. U osnovi radi se o pribavljanju temeljem dobrovoljnog pristanka stranog pružatelja usluge registracije domena (registrara ili voditelja registra vršnih domena). Formalna je razlika u tome što se takav pristanak u smislu čl. 32. Konvencije u nacionalnom pravu određuje slobodno, a u smislu čl. 6. Protokola u skladu „s razumnim uvjetima osiguranim u domaćem pravu". Potonja sintagma pretpostavlja i ovlast unutarnjim pravom propisati uvjete uskraćivanja podataka,[71] međutim ne u smislu zaštite prava okrivljenika u kaznenom postupku jer ona tom mjerom nisu dovedena u pitanje. Naime pretežito se radi samo o osnovi za utvrđivanje osobe kojoj treba uputiti daljnji zahtjev za otkrivanjem pretplatničkih podataka klijenata.

Osnovnu prepreku u članicama Europske unije za dobrovoljno otkrivanje podataka o registrantima domena fizičkim osobama ipak predstavlja čl. 48. GDPR-a o zabrani izvršenja stranih odluka za otkrivanjem osobnih podataka bez postojanja međunarodnog sporazuma. Međutim nije li na snazi neki drugi međunarodni izvor o zaštiti osobnih podataka, sam Protokol predstavlja taj međunarodni sporazum. Čl. 14. određeni su strogi uvjeti pod kojima članice

[68] Usp. Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, 12. V. 2022., odjeljak 84., str. 16.

[69] Ibid., odjeljak 85., str. 16.

[70] Ibid., odjeljak 77. str. 14.

[71] Ibid., odjeljak 82., str. 15.

Protokola moraju obrađivati primljene osobne podatke, kao i mogućnost da jedna članica suspendira prijenos osobnih podataka u drugu ako ima dostatne dokaze o sustavnom ili znatnom kršenju uvjeta za obradu osobnih podataka ili da je znatno kršenje neposredno predstojeće. Smatra se da članicama Protokola navedeno daje ovlast provjeravati i preispitivati usklađenost zakonodavstva druge članice s preuzetim međunarodnim obvezama zaštite osobnih podataka.[72]

4.2. Otkrivanje pretplatničkih podataka

Člankom 7. Protokola članice su dužne osigurati zakonodavne i druge mjere kojima bi njihova nadležna tijela u svrhu otkrivanja počinitelja i vođenja postupaka za kaznena djela: a) bila ovlaštena pružatelju usluge u drugoj članici naložiti da otkrije pohranjene pretplatničke podatke potrebne za pokretanje konkretne kaznene istrage ili postupka, te b) pružateljima usluga na svojem području osigurati da otkriju te podatke stranim tijelima.

Različito od pribavljanja podataka o registrantima domena, mjera otkrivanja pretplatničkih podataka ipak predstavlja miješanje u pravo na privatnost korisnika mrežnih usluga. Protokolom se članicama ostavlja izbor između nekoliko modela. U tom smislu članica prilikom ratifikacije, prihvaćanja ili pristupanja Protokolu može dati izjavu da: a) koristi pravo na neprimjenjivanje instituta neposrednog pristupa pretplatničkim podacima uopće; b) koristi pravo na neprimjenjivanje navedenog instituta samo u odnosu na pojedine vrste pristupnih brojeva; c) institut primjenjuje, ali pod uvjetom da je nalog za dostavu pretplatničkih podataka upućen njezinu pružatelju usluga izdan od ili pod kontrolom stranog tužitelja ili drugog pravosudnog tijela ili na drugi način pod neovisnim nadzorom; te u bilo kojem trenutku dati izjavu da: d) zahtijeva da se u svakom slučaju ili pod određenim okolnostima uz dostavu naloga njezinu pružatelju usluga istodobno dostavi i obavijest njezinu imenovanom državnom tijelu.

Europska unija opredijelila se za rješenje da su njezine članice dužne prihvatiti institut neposrednih naloga za pretplatničke podatke, uz obvezno davanje izjava prethodno opisanih pod c) i d), koje se primjenjuje u svakom slučaju. Izjavu pod b) članice Europske unije mogu dati, ali samo u odnosu na pristupne brojeve koji nisu potrebni isključivo u svrhu identifikacije pretplatnika.[73] Time se formalno nalozi trećih država upućuju pružateljima usluga iz Europske unije, čime je udovoljeno načelu uzajamnosti u međunarodnim odnosima,

[72] Ibid., odjeljak 282., str. 53.

[73] Odluka Vijeća (EU) 2022/722 od 5. travnja 2022. o ovlašćivanju država članica da u interesu Europske unije potpišu Drugi dodatni protokol uz Konvenciju o kibernetičkom kriminalu o pojačanoj suradnji i otkrivanju elektroničkih dokaza, op. cit. (6)

ali suštinski o njihovoj opravdanosti odluku donosi državno tijelo koje stranka Protokola imenuje i o tome obavještava Vijeće Europe, koje vodi popis kontaktnih točaka.

Imenovano državno tijelo naime nakon zaprimanja obavijesti treće države da je izdala nalog pružatelju usluga ili nakon što je od njega domaći pružatelj usluga zatražio konzultacije, ovlašteno je bez odlaganja pružatelju usluge naložiti da ne dostavi pretplatničke podatke ako bi to moglo omesti domaće istrage i postupke ili bi postojali Konvencijom propisani razlozi za odbijanje pravne pomoći da je one zatražena (odbijanje određeno domaćim pravom ili primjenjivim ugovorom o međunarodnoj suradnji, političko kazneno djelo, izvršenje zahtjeva dovodi u pitanje suverenitet, sigurnost, javni red ili bitni interes države). Pored toga kada je pretplatnik fizička osoba, postoji mogućnost suspenzije prijenosa osobnih podataka u državu izdavateljicu naloga u skladu s čl. 14. Protokola. Različito od razloga za odbijanje pravne pomoći, koji ovise o nacionalnom pravu, predvidivo je da će iz razloga usklađenosti u pitanjima zajedničkog prava eventualne odluke o suspenziji biti koordinirane jedinstveno na razini Europske unije, iako ih formalno donosi svaka članica Protokola zasebno.

Nalog za dostavu pretplatničkih podataka mora sadržavati i opis kaznenog djela koje je predmet kaznene istrage ili postupka te podatke o primjenjivim kaznama, čime je ocjena (ne)postojanja razloga za odbijanje u pravilu već omogućena. Međutim radi razjašnjenja relevantnih okolnosti imenovano državno tijelo može zatražiti i dodatne podatke od države izdavateljice ne obavještavajući o tome pružatelja usluge bez pristanka te države. Naredi li pružatelju usluge da ne otkrije pretplatničke podatke, dužno je o tome obavijestiti državu izdavateljicu naloga navodeći pritom razloge takvoj odluci.

Kako će državna tijela članica Europske unije uvijek biti obaviještena o postojanju inozemnog naloga upućenog pružatelju usluge na njihovu području, a dužna su osigurati zaštitu prava na privatnost komunikacije, kojeg su pretplatnički podaci integralni dio, ona ne mogu biti pasivna i time prepustiti pružatelju usluge da samovoljno odlučuje o izvršenju stranog naloga. Stoga se u pogledu ovlasti za donošenje odluke o (ne)izvršenju naloga navedeni proces neće razlikovati od klasične međunarodne pravne pomoći (pogotovo ako članice kao izabrano državno tijelo prema Protokolu imenuju ono koje je i inače nadležno za izvršenje stranih zamolnica).

Svaka članica Protokola dužna je osigurati pružateljima usluga da postupe po dostavljenim nalozima drugih država osiguravajući im da neće snositi pravne posljedice samo zato što su u dobroj vjeri izvršili nalog za koji je država izdavateljica potvrdila da je izdan u skladu s Protokolom.[74] Međutim odgovor-

[74] Usp. Council of Europe, *Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, op. cit. (68), odjeljak 100., str. 19.

nost pružatelja usluga može proizaći iz kršenja dodatnih uvjeta koje je, također u skladu s Protokolom, ovlašten donijeti zakonodavac ili drugo tijelo članice iz koje je pružatelj usluga. Primjerice pored donošenja odluke o suspenziji prijenosa osobnih podataka u drugu državu članica ima pravo propisati uvjete pod kojima su njezini pružatelji usluga dužni zatražiti konzultacije. U okviru toga moguće je osigurati i izbjegavanje nesporazuma između pružatelja usluga i imenovanog državnog tijela u pogledu (ne)postojanja razloga za uskratu dostavljanja pretplatničkih podataka u inozemstvo, ali i kažnjavanje pružatelja usluga zbog izvršenja naloga prije ili protivno odluci imenovanog državnog tijela, odnosno propuštanja traženja obvezne konzultacije.

Članice Protokola izvan Europske unije, čiji pružatelji usluge već u smislu čl. 32. Konvencije dobrovoljno otkrivaju pohranjene pretplatničke i prometne podatke klijenata neposrednom komunikacijom s inozemnim tijelima kaznenog progona, mogu zadržati postojeće rješenje već pukim davanjem izjave o neprimjenjivanju neposrednog otkrivanja pretplatničkih podataka iz čl. 7. Protokola. Međutim ovlaštene su i odlučiti se za primjenu tog instituta ne izjavljujući da države izdavateljice naloga moraju dostaviti istodobnu obavijest njihovu imenovanom državnom tijelu ili izjavljujući da je moraju dostaviti iznimno ako su ostvareni određeni uvjeti. Pružatelj usluge s njihova područja tada u pravilu neposredno obavještava državu izdavateljicu naloga o uskrati otkrivanja pretplatničkih podataka, traži od nje eventualna dodatna pojašnjenja, ali jednako tako može (ili mora) pod uvjetima propisanim u nacionalnom pravu zatražiti konzultacije sa svojim imenovanim državnim tijelom i time mu prepustiti daljnju odluku. Potonje rješenje primjerenije je od dobrovoljnog otkrivanja pretplatničkih podataka u smislu čl. 32. Konvencije jer osigurava ubrzanje postupka i izvjesnost u obvezama uključenih subjekata kroz standardiziranje sadržaja naloga, mogućnost davanja upute da se njegovo postojanje ne otkrije pretplatniku te određivanje rokova za izvršenje i ovlasti države izdavateljice prema stranom pružatelju usluga.

Država izdavateljica naloga nema ovlast prisilnih mjera prema inozemnom pružatelju usluga bez obzira na koje se rješenje država čiji pružatelji usluga zaprimaju nalog odlučila. Ona može, u slučaju da od pružatelja usluga ili imenovanog državnog tijela druge države nije dobila povratnu informaciju u roku od trideset dana od dostave naloga ili datuma naznačenog u nalogu, od pružatelja usluge zatražiti objašnjenje nepostupanja. Ako objašnjenjem nije zadovoljna ili ga ne dobije, jedini način na koji može dalje postupiti jest traženje klasične međunarodne pravne pomoći sastavljanjem i upućivanjem zamolnice inozemnom državnom tijelu. Međutim to ne utječe na ovlast države iz koje dolaze pružatelji usluga da u svojem unutarnjem pravu propiše uvjete pod kojima oni moraju izvršiti inozemni nalog za dostavu pretplatničkih podataka (uključujući i postojanje posebnog sporazuma s drugom državom, kao što su oni između

Sjedinjenih Američkih Država i Ujedinjenog Kraljevstva te Australije, sklopljeni temeljem CLOUD Acta) te pravne posljedice propuštanja te obveze.

U konačnici, neposredna suradnja sa stranim pružateljima usluga institut je koji pojednostavnjuje postupak prekograničnog protoka informacija, a da pritom članice Protokola samostalno određuju u kojoj će mjeri prepustiti pružateljima usluga slobodu neometanog komuniciranja sa stranim tijelima kaznenog progona, a u kojoj će takva „sloboda" biti podvrgnuta kontrolnim mehanizmima.

4.3. Proširenje pretrage računalnog sustava na računalo u inozemstvu

Premda je u postupku donošenja Protokola razmatrano reguliranje prekograničnog proširenja pretrage računalnog sustava, od toga se odustalo uz obrazloženje da područje zahtijeva dodatni posao, vrijeme i konzultacije sa zainteresiranim stranama.[75] Suštinu problema predstavlja okolnost da bi se od države koja bi putem međunarodnog prava nastojala omogućiti svojim tijelima kaznenog progona jednostrano proširenje pretrage na računalo u inozemstvu očekivalo odgovarajuće ekvivalentno rješenje po kojem bi i ona dopustila stranim tijelima kaznenog progona pretraživanje računala na njezinu teritoriju.

Protokolom predviđena neposredna suradnja takve je prirode da članica čijem je pružatelju usluga upućen inozemni zahtjev/nalog ima prostora zaštititi svoj pravni poredak mjerama koje sprječavaju otkrivanje podataka. Isto je s prekograničnim pristupom pohranjenim podacima određenim Konvencijom jer članica sama odlučuje koje podatke učiniti javnima i kome dati ovlast na dragovoljno otkrivanje. Nasuprot tome kod proširene pretrage računalnog sustava pristup podacima spremljenim na računalo u inozemstvu trenutačan je, pri čemu tijelo koje je provodi prethodno, a često i tijekom provođenja mjere, ne zna kakve će podatke pronaći ni u kojoj se državi nalazi računalo na kojem su pohranjeni. Posljedično, država u kojoj je lociran udaljeni objekt pretrage nije u mogućnosti na vrijeme provjeriti bi li postojali uvjeti za odbijanje međunarodne pravne pomoći da je ona zatražena. S druge strane eventualna naknadna konvalidacija inozemne pretrage bila bi odluka donesena nakon što je zadiranje u privatnost i druga prava korisnika računalne komunikacije već ostvareno. Priroda proširene pretrage na drugi računalni sustav stoga zahtijeva daleko kompleksnije kompromise od onih već postignutih u Konvenciji i Protokolu, ako su kompromisi uopće mogući.

[75] Ibid., odjeljak 24., str. 5.

5. ZAKLJUČNA RAZMATRANJA

Dvadeset godina od donošenja Konvencije njezin drugi Protokol na putu je da postane prvi međunarodni obvezujući sporazum o pojednostavnjenoj suradnji u prekograničnom pribavljanju digitalnih dokaza. Njime su obuhvaćena sva kaznena djela povezana s računalnim sustavima, bilo da su napadnuti bilo da su korišteni kao sredstvo počinjenja, komunikacije ili pribavljanja protupravne imovinske koristi, te u tom smislu zadire u područje u kojem nužno postoje razlike među državama u pitanju granice dopuštenog i onog što predstavlja kazneno djelo.

Razvoj tehnologije i digitalizacije društva, u kombinaciji sa slobodom međunarodne razmjene roba i usluga, doveo je do kolateralnog porasta kaznenih djela takva intenziteta da Konvencijom predviđen dohvat podataka u svrhu utvrđivanja počinitelja više nije bio brz, učinkovit i racionalan. U zajedničkom interesu država i pružatelja usluga bilo je pronaći alternativna rješenja kojima bi se spriječilo da pružanje digitalnih usluga u inozemstvo ne preraste u nesmetano korištenje interneta za počinjenje kaznenih djela te vremenom posljedično dovede do ograničavanja slobode trgovine.

Protokolom se nastoji unijeti pravna sigurnost i izvjesnost, formaliziranjem procesa koji je prethodno već započeo u nacionalnim pravnim sustavima kao nastavak na Konvenciju, na način da razlike u unutarnjim pravima članica ne postanu zapreka uzajamnosti u međunarodnim odnosima. Protokol se ujedno i zaustavlja na razini na kojoj su trenutačno nacionalna rješenja, ne prelijevajući se na područje prekograničnog proširenja pretraga računalnog sustava.

Jedan vid pojednostavnjene suradnje opisan Protokolom jest izravna komunikacija tijela kaznenog progona i pružatelja usluga u drugoj državi. Premda se razina zaštite temeljnih prava sudionika računalne komunikacije nastoji unaprijediti, uključivanje treće osobe (pružatelja usluga) u proces pribavljanja podataka koji se inače odvijao neposredno između državnih tijela samo po sebi predstavlja latentnu opasnost ugrožavanja legitimnih interesa ne samo države koja traži podatke već i one iz koje dolazi pružatelj usluge. Privatni poslovni subjekti svojim radnjama mogu ugroziti prikupljanje dokaza, ali i prava svojih klijenata, neovisno o tome je li to rezultat nepoznavanja propisa i međunarodnih odnosa, nesporazuma sa stranom ili vlastitom državom, ili sukoba interesa uslijed ekonomske ovisnosti o klijentu.

Problematika položaja pružatelja usluga nadilazi puku garanciju da oni ne mogu snositi pravne posljedice samo zato što su u dobroj vjeri izvršili strani zahtjev ili nalog. Izvršenje obveze, pa i zakonito, može imati implikacije na financije pružatelja usluge, njegov odnos s klijentom ili ravnopravnost u tržišnoj utakmici. Realno je da će svoje obveze učinkovito i bez nerazmjernog ekonomskog tereta moći podnijeti snažni poslovni subjekti usmjereni na glo-

balno tržište. Oni mogu racionalizirati svoje troškove neposredne suradnje i osigurati zakonitost svog postupanja korištenjem posebnih računalnih programa, zapošljavanjem ili angažiranjem pravnih stručnjaka za odnose sa stranim uputiteljima zahtjeva i naloga, domaćim koordinativnim tijelima ili trećom državom, prema kojoj također mogu imati obveze. U tom smislu nema zapreke da se znatan dio prekograničnog dohvata pretplatničkih podataka učinkovito i uz poštovanje prava klijenata riješi neposrednom suradnjom s pružateljima usluga.

Međutim Protokolom predviđena obveza međunarodne suradnje obuhvatila bi poslovne subjekte bez obzira na njihov opseg poslovanja i resurse, potencijalno čak i one koji svoje usluge ne nude u inozemstvo i poduzimaju razumne mjere radi blokiranja stranih korisnika. Buduće detaljno normiranje položaja ekonomski slabijih pružatelja usluga u nacionalnim zakonodavstvima ključno je ne samo za nesmetano odvijanje gospodarskih odnosa i slobode pružanja usluga već i za zaštitu prava korisnika jer osoba na kojoj je teret izvršavanja neposredne međunarodne suradnje objektivno mora biti u mogućnosti taj teret podnijeti.

Na državama koje namjeravaju potpisati i ratificirati Protokol složen je zadatak odabrati ono rješenje koje najbolje odgovara njihovu pravnom sustavu. U konačnici, uspješnost Protokola i prednost neposredne međunarodne suradnje s pružateljima usluga u odnosu na klasičnu putem državnih tijela vrednovat će se prema utjecaju tog izvora na nacionalna prava i njihovu primjenu u praksi.

LITERATURA

1. Banks, J., *Regulating hate speech online,* International Review of Law, Computers & Technology, vol. 24, o. 3 (2010), str. 233–239.
2. van Blarcum, C. D., *Internet Hate Speech: The European Framework and the Emerging American Haven*, 62 Wash. & Lee L. Rev. 781 (2005), str. 781–830.
3. Brière, C., *EU Criminal Procedural Law onto the Global Stage: The e-Evidence Proposals and Their Interaction with International Developments*, European Papers, vol. 6, no 1 (2021), str. 493–511.
4. Cangemi, D., *Procedural Law Provisions of the Council of Europe Convention on Cybercrime*, International Review of Law, Computers & Technology, vol. 18, issue 2 (2004), str. 165–172.
5. Daskal, J., *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0*, Stanford Law Review (Online), vol. 71 (2018), https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/.
6. Davis, F. T., Gressel, A.R., *Storm Clouds or Silver Linings*?, Litigation, vol. 45, no. 1 (2018), str. 47–52.
7. Executive Office for United States Attorneys, Office of Legal Education, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations,* 3. izdanje, https://www.justice.gov/file/442111/download (10. rujna 2022.).

8. Kleijssen, J., Perri, P.: *Cybercrime, Evidence and Territoriality, Issues and Options*, u: M. Kuijer, M., Werner, W. (ur.), *Netherlands Yearbook of International Law (The Changing Nature of Territoriality in International Law)*, br. 47/2016, str. 147–173.
9. Maillart, J. B., *The limits of subjective territorial jurisdiction in the context of cybercrime*, ERA Forum (2019) 19, str. 375–390., https://doi.org/10.1007/s12027-018-0527-2 (10. rujna 2022.).
10. Maurushat, A., *Australias accession to the Cybercrime Convention : is the Convention still relevant in combating cybercrime in the era of botnets and obfuscation crime tools*, University of New South Wales Law Journal, vol. 33, issue 2 (2010), str. 431–473.
11. Mitsilegas, V., *The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence*, Maastricht Journal of European and Comparative Law, vol. 25, issue 3 (2018), str. 263–265.
12. Murphy, S. D., *Contemporary practice of the United States relating to international law*, The American Journal of International Law, vol. 96, no. 4 (2002), str. 956–983.
13. Osula, A. M., *Remote search and seizure in domestic criminal procedure: Estonian case study*, *International Journal of Law and Information Technology,* vol. 24, issue 4 (2016), str. 343–373.
14. Pirc Musar, N., *Benedik v Slovenia: Dynamic IP and Communication Privacy*, European Data Protection Law Review, vol. 4, issue 4 (2018), str. 554–562.
15. Spiezia, F., International cooperation and protection of victims in cyberspace: welcoming Protocol II to the Budapest Convention on Cybercrime, ERA Forum (2022) 23, str. 101–108.
16. Tosza, S., *Internet service providers as law enforcers and adjudicators. A public role of private actors.,* Computer Law & Security Review, 43 (2021), 105614, str. 1–17.
17. Verdelho, P., *Obtaining digital evidence in the global world*, UNIO – EU Law Journal, vol. 5, no. 2 (2019), str. 136–145.

Summary

Ivan Glavić, PhD *

DIRECT INTERNATIONAL COOPERATION ACCORDING TO THE SECOND ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBER CRIME

This paper analyses the provisions on the direct cooperation of authorities in charge of revealing and prosecuting criminal offences with the service providers in a foreign country, deriving from the Council of Europe Second Additional Protocol to the Convention on Cybercrime. The purpose of the aforementioned international source is to simplify and improve the exchange of data necessary for revealing the identity of perpetrators, with a high level of protection of the rights of service users. Emphasis is placed on the diversity of approaches to the mentioned issue in the existing legal systems of EU countries and the United States of America, and the connection of the development of national legislation with Art. 32 of the Convention, on direct cross-border access to publicly available and voluntarily disclosed data. The results of the work indicate that the Protocol provides a basis for potential members to implement it in accordance with their existing legal system, without disrupting the principle of reciprocity of international cooperation.

Keywords: direct international cooperation, Internet service providers, subscriber data, privacy of computer communication, extended search of computer system

* Ivan Glavić, PhD, Deputy State Attorney at the County State Attorney's Office in Zagreb; ivan.glavic@zdozg.dorh.hr; ORCID iD: https://orcid.org/0000-0003-4055-3286.