Mišljenje 23/2018 o prijedlozima Komisije o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima (članak 70. stavak 1. točka (b))

Doneseno 26. rujna 2018.

Sadržaj

Europski odbor za zaštitu podataka

uzimajući u obzir članak 70. stavak 1. točku (b) Uredbe 2016/679/EU 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,

DONIO JE SLJEDEĆE MIŠLJENJE:

Uvod

U travnju 2018. Komisija je predstavila prijedlog Uredbe o europskom nalogu za dostavljanje i europskom nalogu za čuvanje elektroničkih dokaza u kaznenim stvarima i prijedlog Direktive o utvrđivanju usklađenih pravila za imenovanje pravnih zastupnika za potrebe prikupljanja dokaza u kaznenim postupcima. Ta se dva prijedloga (COM(2018) 225 final i COM(2018) 226 final) međusobno dopunjuju. Opći je cilj Komisije poboljšati suradnju između tijela država članica i pružatelja usluga, uključujući one sa sjedištem u zemljama izvan EU-a, i predložiti rješenja za problem utvrđivanja i izvršavanja nadležnosti u kiberprostoru.

Nacrtom Uredbe predviđeni su pravila i postupci za izdavanje, dostavljanje i izvršenje naloga za dostavljanje i čuvanje upućenih pružateljima usluga elektroničke komunikacije, a nacrtom Direktive utvrđena su minimalna pravila za imenovanje pravnog zastupnika pružatelja usluga koji nemaju poslovni nastan u EU-u.

U studenome 2017.[1], prije nego što je Komisija predstavila nacrte zakonodavnih instrumenata, Radna skupina iz članka 29. (WP29) podsjetila je da treba osigurati da svi zakonodavni prijedlozi budu u potpunosti u skladu s postojećom pravnom stečevinom EU-a o zaštiti podataka te općenito s pravom EU-a i sudskom praksom.

Konkretno, Radna skupina iz članka 29. upozorila je na opasnost od ograničenja prava na zaštitu podataka i privatnosti u pogledu podataka koje obrađuju pružatelji telekomunikacijskih usluga i usluga informacijskog društva, posebice kad ih dodatno obrađuju tijela za izvršavanje zakonodavstva, podsjetila da je važno osigurati dosljednost svih instrumenata EU-a s postojećom Budimpeštanskom konvencijom Vijeća Europe o kibernetičkom kriminalu i Direktivom EU-a o Europskom istražnom nalogu (EIN) i preporučila da se objasne odgovarajuća postupovna pravila kojima je uređen pristup elektroničkim dokazima na nacionalnoj razini i razini EU-a kako bi se osiguralo da novim instrumentom tijelima vlasti neće biti dodijeljene nove ovlasti koje interno ne bi imale. Uz te opće primjedbe Radna skupina iz članka 29. komentirala je zakonodavne opcije koje je Komisija tada razmatrala u pogledu obuhvaćenih kategorija podataka i odgovarajućih zaštitnih mjera za pristup tim podacima, mogućnosti upućivanja zahtjeva/naloga za dostavljanje kako bi se pružatelje usluga primoralo da dostave podatke smještene izvan EU-a te materijalne i postupovne zahtjeve kao nužne zaštitne mjere u pogledu izravnog pristupa podacima.

Kako su sad predstavljeni konkretni prijedlozi o elektroničkim dokazima, Odbor želi iznijeti podrobniju analizu predloženih pravnih instrumenata sa stajališta zaštite podataka.

[1] Vidjeti izjavu Radne skupine iz članka 29. (http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48801)

1. Pravna osnova prijedloga Uredbe (članak 82. UFEU-a)

Predložena pravna osnova za nacrt Uredbe o elektroničkim dokazima je članak 82. stavak 1. UFEU-a o pravosudnoj suradnji u kaznenim stvarima, koji glasi:

> 1. Pravosudna suradnja u kaznenim stvarima u Uniji temelji se na načelu uzajamnog priznavanja presuda i sudskih odluka te uključuje usklađivanje zakona i drugih propisa država članica u područjima iz stavka 2. i članka 83.
>
> Europski parlament i Vijeće, odlučujući u skladu s redovnim zakonodavnim postupkom, usvajaju mjere za:
>
> (a) utvrđivanje pravila i postupaka kojima se osigurava priznavanje svih oblika presuda i sudskih odluka u čitavoj Uniji;
>
> (b) sprečavanje i rješavanje sukoba nadležnosti među državama članicama;
>
> (c) potporu osposobljavanju sudaca i sudskog osoblja;
>
> (d) olakšavanje suradnje među sudskim ili drugim odgovarajućim tijelima država članica u vezi s kaznenim postupcima i izvršenjem odluka.

Kako je Komisija istaknula u procjeni učinka koja je priložena prijedlozima: „U članku 82. stavku 1. utvrđeno je da se pravosudna suradnja u kaznenim stvarima temelji na načelu uzajamnog priznavanja. Ta bi pravna osnova obuhvatila moguće zakonodavstvo o izravnoj suradnji s pružateljima usluga u skladu s kojim bi tijelo u državi članici izdavateljici izravno kontaktiralo sa subjektom (pružateljem usluga) u državi izvršiteljici te mu čak nametnulo obveze. Time bi se uvela nova dimenzija uzajamnog priznavanja izvan tradicionalne suradnje u Uniji, koja se dosad temeljila na postupcima u kojima sudjeluju dva pravosudna tijela, jedno u državi izdavateljici a drugo u državi izvršiteljici.”(naknadno istaknuto)

Kako je upotreba te pravne osnove u kontekstu izravnih zahtjeva koje javna tijela upućuju privatnim subjektima novost, Odbor žali što Komisija nije dostavila dodatne analize ili procjene.

Naime, kako je Radna skupina već istaknula u svojoj prethodnoj izjavi, Odbor i dalje iznosi sumnje o prikladnosti te pravne osnove koje podupiru analiza Suda i nezavisnog odvjetnika iznesena u Mišljenju 1/15. U okviru razmatranja o valjanosti članka 82. kao pravne osnove za Prijedlog sporazuma između Kanade i EU-a o popisu imena putnika Sud je naglasio da kanadsko nadležno tijelo *nije ni sudsko ni drugo odgovarajuće tijelo*[2]. Kako je Komisija navela, čini se da je jedan od glavnih ciljeva u kontekstu prijedloga o elektroničkim dokazima izbjeći „pretjerano zahtjevnu” pravosudnu suradnju. Stoga se prijedlog temelji na načelu da bi se suradnja trebala odvijati između tijela vlasti i pružatelja usluga, a ne između dvaju tijela vlasti. U predviđenom postupku privatni subjekti bili bi prvenstveno primatelji i odgovarali na zahtjeve koje upućuju pravosudna tijela.

Odbor naglašava da bi postupak izvršenja naloga za dostavljanje i naloga za čuvanje mogao podrazumijevati sudjelovanje tijela primatelja u situaciji da pružatelj usluge koji je primatelj naloga ne izvrši svoje obveze pa je stoga potrebno tražiti *ex-post* izvršenje naloga. Međutim, kako je glavni cilj utvrđenog postupka upravo isključivanje tijela primatelja, Odbor sumnja da bi taj sporedni postupak opravdao upotrebu članka 82. kao jedine pravne osnove zakonodavnog instrumenta.

[2] Vidjeti točku 103. Mišljenja 1/15 i točku 108. mišljenja nezavisnog odvjetnika u tom predmetu.

Stoga Odbor smatra da članak 82. može biti pravna osnova ako se glavni postupovni koraci suradnje odvijaju između dva pravosudna tijela, a za ovu vrstu suradnje potrebna je druga pravna osnova.

2. Nužnost prijedloga o elektroničkim dokazima u odnosu na MLAT i EIN

Odbor napominje da je Komisija predana preispitivanju prepreka u kaznenim istragama, posebice u odnosu na pristup elektroničkim dokazima. U obrazloženju Komisija navodi kontekst prijedloga i ističe nestabilnu prirodu elektroničkih dokaza, njihovu međunarodnu dimenziju te potrebu da se mehanizmi suradnje prilagode digitalnom dobu. Prijedlozi Uredbe i Direktive o pristupanju elektroničkim dokazima i njihovu prijenosu nisu zamišljeni kao zamjena za prethodne instrumente suradnje u kaznenim stvarima kao što su Budimpeštanska konvencija, ugovor o uzajamnoj pravnoj pomoći (MLAT) i Europski istražni nalog (EIN). Komisija je iznijela da je cilj zakonodavnih prijedloga o elektroničkim dokazima poboljšati pravosudnu suradnju u kaznenim stvarima između tijela vlasti i pružatelja usluga u Europskoj uniji i u trećim zemljama, posebice u Sjedinjenim Američkim Državama.

Budući da će ti novi dodatni alati biti posebno namijenjeni za pristup elektroničkim dokazima i njihov prijenos, Odbor će ocijeniti dodanu vrijednost tih instrumenata u odnosu na Direktivu o EIN-u i MLAT.

a) Nužnost elektroničkih dokaza u odnosu na zaštitne mjere utvrđene MLAT-om i EIN-om

Glavni argument koji je Komisija iznijela u korist zakonodavnih prijedloga o elektroničkim dokazima je ubrzavanje postupka osiguravanja i pribavljanja elektroničkih dokaza koje čuvaju i/ili posjeduju pružatelji usluga s poslovnim nastanom u drugoj jurisdikciji.

Međutim, Odbor izražava žaljenje što potreba za uvođenjem novog instrumenta za organiziranje pristupa elektroničkim dokazima nije prikazana u procjeni učinka. Naime, u prijedlozima nije prikazano da nije moglo biti upotrijebljeno nijedno manje intruzivno sredstvo da bi se ostvario cilj prijedloga o elektroničkim dokazima, iako su mogla biti razmotrena alternativna rješenja. Primjerice, moglo se razmotriti izmjenjivanje i poboljšavanje Direktive o EIN-u, čime bi se ispunio i zahtjev iz same Direktive da se do 21. svibnja 2019. provede procjena potrebe za izmjenama teksta[3]. Druga je mogućnost mogla biti upotreba naloga za čuvanje za „zamrzavanje" podataka dok ne bude izdan službeni zahtjev na temelju MLAT-a. Tim bi se mogućnostima omogućilo zadržavanje zaštitnih mjera navedenih u tim instrumentima, a istodobno onemogućilo brisanje traženih osobnih podataka.

Odbor ističe da su rokovi utvrđeni u Direktivi o EIN-u dulji od rokova iz prijedloga o elektroničkim dokazima. Naime, tijelo izvršitelj ima 30 dana za donošenje odluke o priznavanju zahtjeva[4] i zatim treba izvršiti zahtjev u roku od 90 dana[5]. Odbor smatra da je davanje tijelima izvršiteljima EIN-a 30 dana za razmatranje ključna zaštitna mjera kojom im se omogućuje da razmotre je li zahtjev za izvršenje utemeljen i poštuju li se njime svi uvjeti za izdavanje i prosljeđivanje EIN-a[6].

[3] Vidjeti članak 37. Direktive o EIN-u.
[4] Članak 12. stavak 3. Direktive o EIN-u.
[5] Članak 12. stavak 4. Direktive o EIN-u.
[6] Članak 6. Direktive o EIN-u.

Odbor je zabrinut da se propisivanjem desetodnevnog roka u prijedlozima o elektroničkim dokazima za izvršenje potvrde europskog naloga za dostavljanje (EPOC) bez dodatnog vremena za razmatranje sprečava prikladna procjena ispunjava li EPOC sve kriterije i je li pravilno popunjen.

Stoga Odbor preporučuje da se primatelju EPOC-a omogući više vremena za utvrđivanje treba li nalog izvršiti ili ne.

Odbor napominje da kod potvrde europskog naloga za čuvanje (EPOC-PR) nema jamstva da će čuvanje podataka biti ograničeno na podatke koje treba dostaviti. K tome, trajanje čuvanja podataka može premašiti 60 dana jer nije naveden rok u kojem tijelo izdavatelj treba obavijestiti adresata da povlači nalog za dostavljanje ili da ga neće izdati. Stoga Odbor preporučuje da se barem odredi rok u kojem tijelo izdavatelj mora povući ili odustati od izdavanja naloga za dostavljanje kako bi se poštovalo načelo smanjenja količine podataka utvrđeno u Općoj uredbi o zaštiti podataka[7].

Na kraju, Odbor ističe da je Direktivom o EIN-u propisano da država izdavateljica vraća dokaze tijelu izvršitelju[8]. Međutim, ta se mogućnost ne spominje u prijedlogu Uredbe o elektroničkim dokazima. Nije jasno što se zbiva s elektroničkim dokazima nakon što budu preneseni tijelu izdavatelju.

Stoga Odbor preporučuje da se u prijedlogu Uredbe navede više informacija o upotrebi elektroničkih dokaza nakon njihova prijenosa tijelu izdavatelju kako bi se poštovali Opća uredba o zaštiti podataka i načelo transparentnosti[9], kao i načelo specifičnosti utvrđeno u MLAT-ovima.

b) Napuštanje načela dvostruke kažnjivosti

Odbor priznaje da uzajamno priznavanje ovisi o primjeni načela dvostruke kažnjivosti, a na taj način države članice mogu zadržati suverenitet. Međutim, dvostruka kažnjivost sve se češće smatra preprekom neometanoj pravosudnoj suradnji. Države članice sve su spremnije na suradnju, čak i ako se istražne mjere odnose na djelo koje se u njihovu nacionalnom pravu ne smatra kaznenim djelom. Međutim, Odbor podsjeća da je cilj načela dvostruke kažnjivosti osigurati dodatnu zaštitnu mjeru kako bi se zajamčilo da se država članica ne može osloniti na pomoć druge države članice za primjenu kaznene sankcije koja ne postoji u pravu druge države. Time se primjerice sprečava neku državu da zatraži pomoć druge države kako bi lišila slobode neku osobu zbog njezinih političkih uvjerenja ako ta uvjerenja nisu kriminalizirana u državi kojoj se podnosi zahtjev ili da sudi nekoj osobi zbog pobačaja ako ta osoba boravi u drugoj državi u kojoj pobačaj nije protuzakonit. Načelo dvostruke kažnjivosti često prate i druga ograničenja ili zaštitne mjere u pogledu sankcija ako se one uvelike razlikuju između države koja podnosi zahtjev i države izvršiteljice. Glavni je primjer obveza neizvršavanja smrtne kazne u nekim MLAT-ovima ako ona ne postoji u pravu jedne od stranaka.

Odbor primjećuje da je načelo dvostruke kažnjivosti izostavljeno iz prijedloga Uredbe o elektroničkim dokazima. Međutim, rezultat toga nije samo ukidanje uobičajenih formalnosti uzajamnog priznavanja, nego i ukidanje zaštitnih mjera povezanih sa samim načelom dvostruke kažnjivosti.

Naime, Odbor je uočio da nema upućivanja na pravo države u kojoj pružatelj usluga kojem je upućen zahtjev ima poslovni nastan, te da se čuvanje svih podataka, kao i dostavljanje podataka o pretplatnicima i podataka o pristupu, može naložiti za sva kaznena djela[10] bez obzira na to postoje li slična kaznena djela u drugim državama članicama ili ne.

[7] Članak 5. stavak 1. točka (c) Opće uredbe o zaštiti podataka.
[8] Članak 13. stavci 3. i 4. Direktive o EIN-u.
[9] Članak 5. stavak 1. točka (a) Opće uredbe o zaštiti podataka.
[10] Članak 5. stavak 3. i članak 6. stavak 2. predložene Uredbe o elektroničkim dokazima.

Međutim, nalog za dostavljanje može se izdati i izvršiti samo ako je slična mjera dostupna za isto kazneno djelo u usporedivoj domaćoj situaciji u državi izdavateljici[11]. K tome, kako je Komisija objasnila u obrazloženju prijedloga Uredbe, podaci o transakcijama i podaci o sadržaju specifični su jer se smatraju podacima osjetljivije prirode. Naime, nalozi koji se odnose na podatke o transakcijama i podatke o sadržaju temelje se na pragu maksimalne kazne od najmanje tri godine zatvora kako bi se osiguralo poštovanje proporcionalnosti i prava obuhvaćenih osoba[12]. Međutim, Odbor naglašava da na razini EU-a još nisu usklađena kaznena djela kažnjiva maksimalnom kaznom od najmanje tri godine zatvora.

Odbor se protivi napuštanju načela dvostruke kažnjivosti, čija je svrha osigurati da država ne može primijeniti nacionalno kazneno pravo izvan svojeg državnog područja uz pomoć države koja ne dijeli isti pristup, posebice uzimajući u obzir nestanak drugih tradicionalnih većih zaštitnih mjera u području kaznenog prava (vidjeti točku 3. o kriterijima lokacije i točku 7.(g) o mogućim sukobima sa zakonima trećih zemalja).

c) Posljedice izravnog upućivanja naloga poduzećima

Odbor prihvaća da su elektronički dokazi sve češće dostupni na privatnoj infrastrukturi i da se mogu nalaziti izvan zemlje koja provodi istragu te u vlasništvu pružatelja usluga.

Odbor je svjestan da, nakon odluka u predmetima *Yahoo!*[13] i *Skype*[14] u Belgiji te u kontekstu terorističkih napada postoji potreba za jednostavnijom i bržom suradnjom javnih i privatnih subjekata. U procjeni učinka Komisija upućuje na tri vrste postupovnih instrumenata kojima su obuhvaćeni i javna tijela i pružatelji usluga. To su pravosudna suradnja, izravna suradnja i izravni pristup. U prvom instrumentu odgovornost za izvršenje EIN-a ne počiva na pružatelju usluge nego na tijelu izvršitelju[15], a drugi instrument (izravna suradnja) temelji se na suradnji pružatelja usluga. Sa stanovišta pružatelja usluga najnametljiviji je izravni pristup jer javna tijela mogu pristupiti podacima bez pomoći posrednika.

Stoga Odbor strahuje da, kad im se nalog uputi izravno, pružatelji usluga neće osigurati zaštitu osobnih podataka jednako učinkovito kao što to javna tijela mogu i moraju, te naglašava da će to rezultirati neprimjenjivošću određenih postupovnih jamstava predviđenih u kontekstu pravosudne suradnje za pojedince, kao i za sama poduzeća[16]. Primjerice, pružatelj usluga koji primi zahtjev morao bi na sudu druge države (članice) pobijati nalog, dok bi u kontekstu pravosudne suradnje to mogao učiniti pred tijelima vlastite države. Odbor preporučuje da se u prijedlog Uredbe uvrste dodatne osnove kojima bi se potvrdilo da će pružatelji usluga štititi pojedina temeljna prava kao što su pravo na zaštitu osobnih podataka i poštovanje privatnog i obiteljskog života, kao i informacije o nadležnom tijelu za zaštitu podataka kako bi se osigurala mogućnost kontrole.

3. Nova osnova za jurisdikciju i takozvani nestanak kriterija lokacije

[11] Članak 5. stavak 2. predložene Uredbe o elektroničkim dokazima.
[12] Članak 5. stavak 4. točka (a) predložene Uredbe o elektroničkim dokazima.
[13] Hof van Cassatie of Belgium, YAHOO! Inc., br. P.13.2082.N od 1. prosinca 2015.
[14] Correctionele Rechtbank van Antwerpen, afdeling Mechelen of Belgium, br. ME20.F1.105151-12 od 27. listopada 2016. (Skype se žalio na odluku).
[15] Članci od 10. do 16.
[16] Iz perspektive međunarodne zaštite podataka vidjeti i „Radni dokument o standardima zaštite podataka i osobne privatnosti u prekograničnim zahtjevima za podatke za potrebe kaznenog progona", Međunarodna radna skupina za zaštitu podataka u telekomunikacijama, 63. sjednica, 9.–10. travnja 2018., Budimpešta (Mađarska).

Odbor primjećuje da Komisija ističe da je jedna od glavnih izmjena uvedena prijedlozima instrumenata nestanak kriterija lokacije i mogućnost da nadležna tijela zatraže čuvanje i dostavljanje podataka bez obzira na to gdje su podaci zapravo pohranjeni.

Sa stajališta zaštite podataka nije novost da se pravo EU-a o zaštiti podataka primjenjuje bez obzira na to gdje su podaci dotičnih osoba pohranjeni. Naime, primjenjivost Opće uredbe o zaštiti podataka ovisi ili o činjenici da voditelj obrade ili izvršitelj obrade imaju poslovni nastan u EU-u ili o tome jesu li obrađeni podaci ispitanika iz EU-a, čak i ako voditelj obrade ili izvršitelj obrade nemaju poslovni nastan na području EU-a[17], u kojem slučaju moraju imenovati pravnog zastupnika u EU-u [18]. Sa stajališta zaštite podataka važno je napomenuti da je cilj proširenog teritorijalnog obuhvata osigurati potpuniju zaštitu ispitanicima iz EU-a bez obzira na to gdje poduzeće koje obrađuje njihove podatke ima poslovni nastan.

Stoga, iako bi nestanak kriterija lokacije mogao biti novost u području kaznenog prava, sa stajališta zaštite podataka to se ne doima kao velika promjena. K tome, Odbor je primijetio da i dalje postoji poveznica s područjem EU-a jer samo pružatelji usluga koji nude usluge u Uniji spadaju u područje djelovanja prijedloga instrumenata, a činjenica da se zahtjevi mogu uputiti samo u kontekstu kaznenih istraga podrazumijevaju poveznicu s EU-om (bilo zato što je kazneno djelo počinjeno na državnom području države članice ili zato što su žrtva ili zločinac državljani države članice).

Ako se nestanak kriterija lokacije sad primijeni u kaznenom pravu, prema mišljenju Odbora najvažnije je pitanje kako osigurati da taj pomak ne ugrozi zaštitu podataka i postupovna prava ispitanika i pružatelja usluga kojima je zahtjev upućen u kaznenim postupcima. S tog stajališta Odbor priznaje da su u EU-u postupovne zaštitne mjere barem djelomično usklađene i potrebno ih je osigurati u skladu s Europskom konvencijom o ljudskim pravima. Stoga bi se moglo zaključiti da bi nestanak kriterija lokacije vjerojatno imao ograničenije učinke kad se dokazi traže unutar EU-a u odnosu na obratnu situaciju, odnosno ako tijela iz trećih zemalja zahtijevaju podatke od društava s poslovnim nastanom u EU-u pod istim uvjetima koji su utvrđeni u nacrtu Uredbe o elektroničkim dokazima. Odbor je posebno zabrinut da bi to moglo dovesti do brojnih problematičnijih situacija. U tom kontekstu tijela iz treće zemlje gdje se u kaznenom pravu primjenjuju drukčije i potencijalno slabije postupovne zaštitne mjere imala bi pristup podacima koji bi u EU-u bili obuhvaćeni dodatnim zaštitnim mjerama. U tom kontekstu Odbor ponovno ističe svoju zabrinutost zbog dvostrukih standarda i slabljenja temeljnih prava ako pružatelji usluga i ispitanici nemaju koristi od postupovnih zaštitnih mjera prava EU-a kad zahtjev dolazi od tijela treće zemlje.

Nadalje, kako je nova osnova za jurisdikciju „bez obzira na lokaciju podataka" kombinirana s postupkom koji se uglavnom oslanja na izravne zahtjeve koje nadležna tijela upućuju pružateljima usluga, Odbor je zabrinut da privatna poduzeća koja prime zahtjeve i koja nisu obvezana pravnim instrumentom poput MLAT-a, kojim se tradicionalno uređuje razmjena podataka među pravosudnim tijelima i osiguravaju zaštitne mjere, možda neće primjenjivati mjere za zaštitu podataka. Konkretno, u kontekstu MLAT-ova minimalne mjere za zaštitu podataka uključuju primjerice obvezu povjerljivosti i načelo specifičnosti koje podrazumijeva da podaci neće biti obrađivani u neku drugu svrhu.

Stoga Odbor ponavlja da bi se trebale primjenjivati zaštitne mjere utvrđene u Direktivi 2016/680, pa i na prijenose podataka, a posebice članak 39. ako pružatelj usluga ima poslovni nastan u trećoj zemlji bez odluke o primjerenosti u tom području. Konkretno, Odbor ističe da ta odredba posebice podrazumijeva obavješćivanje nadležnog tijela za zaštitu podataka u državi članici tijela izdavatelja o

[17] Vidjeti članak 3., posebno stavak 2.
[18] Vidjeti članak 27.

nalogu/nalozima i dokumentiranje prijenosa, uključujući opravdanje o neučinkovitosti ili neprikladnosti prijenosa nadležnom tijelu treće zemlje.

4. Pojam „pružatelji usluga" trebao bi biti ograničen ili dopunjen dodatnim zaštitnim mjerama za prava ispitanika

U pogledu pružatelja usluga Odbor pozdravlja široku definiciju kojom se omogućuje uključivanje i komunikacijskih usluga i *Over-The-Top* (OTT) usluga, koje su funkcionalno jednakovrijedne, pa bi stoga predviđene mjere mogle imati sličan utjecaj na pravo na privatnost i pravo na tajnost komunikacija, kako je naglašeno u izjavi Radne skupine iz članka 29. i prethodno u mišljenju 01/2017 o predloženoj Uredbi o e-privatnosti. Naime, prijedlog Uredbe o elektroničkim dokazima obuhvaća pružatelje usluga koji pružaju elektroničke komunikacijske usluge kako su definirane u članku 2. stavku 4. Direktive o Europskom zakoniku elektroničkih komunikacija, usluge informacijskog društva kako su definirane u članku 1. stavku 1. točki (b) Direktive (EU) 2015/1535 „u pogledu kojih je pohranjivanje podataka ključna komponenta usluge koja se pruža korisniku, uključujući usluge društvenih mreža, internetskih trgovina koje olakšavaju transakcije između njihovih korisnika i pružatelje ostalih usluga smještanja na poslužitelju" ili usluge naziva internetskih domena i izdavanja brojeva za IP adrese „kao što su pružatelji IP adresa, registri naziva domena, pružatelji usluga registracije naziva domena i povezane usluge privatnosti i posredovanja"[19].

Međutim, kako je u smislu nacrta Uredbe pružatelj usluga „bilo koja fizička ili pravna osoba koja pruža jednu ili više sljedećih kategorija usluga", Odbor je zabrinut da bi taj instrument mogao obuhvatiti i voditelje obrade i izvršitelje obrade u smislu Opće uredbe o zaštiti podataka. Konkretno, kako „pružanje usluga" kako je definirano u članku 2. stavku 4. nacrta Uredbe obuhvaća i omogućivanje pravnim ili fizičkim osobama u jednoj ili više država članica da se koriste navedenim uslugama i postojanje bitne veze s državom članicom ili državama članicama, te bi aktivnosti mogle obuhvaćati aktivnosti koje izvršitelj obrade vrši za voditelja obrade, primjerice pohranjivanje podataka.

Stoga Odbor strahuje da će, ako se ne uvedu ograničenja za pružatelje usluga koji djeluju kao voditelji obrade u smislu Opće uredbe o zaštiti podataka ili posebne obveze izvršitelja obrade da obavijeste voditelja obrade kad zaprime nalog za dostavljanje ili nalog za čuvanje, prava ispitanika biti zanemarena. To posebno vrijedi jer se u kontekstu mogućih proturječnih obveza koje sprečavaju adresata da postupi po primljenim nalozima u nacrtu Uredbe pravosudna tijela upućuje da se obrate najprikladnijem akteru bez obzira na primjenjiva pravila zaštite podataka, posebice jer se mogu zatražiti svi podaci, a ne samo osobni podaci obuhvaćeni Općom uredbom o zaštiti podataka[20].

Prema Općoj uredbi o zaštiti podataka izvršitelj obrade djeluje isključivo na temelju uputa dobivenih od voditelja obrade. Stoga je odgovornost voditelja obrade osigurati poštovanje prava ispitanika i pružiti ispitanicima relevantne informacije, uključujući informacije o primateljima njihovih podataka, primjerice u kontekstu ostvarivanja njihova prava na pristup informacijama. Izvršitelj obrade neće primiti te zahtjeve od ispitanika i neće biti u položaju da na njih odgovori ako to voditelj obrade izričito ne zatraži.

Prema tome, ako njihova prava nisu ograničena primjenom Opće uredbe o zaštiti podataka, Odbor naglašava da ispitanici obuhvaćeni tom Uredbom možda neće moći učinkovito ostvarivati svoja prava

[19] Članak 2. stavak 3. točka (c) predložene Uredbe o elektroničkim dokazima.
[20] Vidjeti članak 7. stavke 3. i 4.

ako voditelj obrade nije u mogućnosti dati potpune informacije. Odbor naglašava da je vjerojatnost nedostatka informacija još veća ako se izvršitelju obrade ne nametne specifična obveza da obavijesti voditelja obrade kad se traženi podaci odnose na ispitanike koji nemaju koristi od zaštite zajamčene Općom uredbom o zaštiti podataka. U tom slučaju pravosudna tijela koja traže podatke neće nužno biti obvezna obavijestiti ispitanike o vlastitoj daljnjoj obradi tih podataka. Odbor stoga traži ograničenje opsega u pogledu voditelja obrade u smislu Opće uredbe o zaštiti podataka ili uvođenje odredbe kojom se objašnjava da, ako pružatelj usluga kojem je upućen nalog nije voditelj obrade podataka, on o tome obavješćuje voditelja obrade.

5. Pojmove „poslovni nastan” i „pravni zastupnik” u kontekstu prijedloga instrumenata trebalo bi jasno razlikovati od istih pojmova iz Opće uredbe o zaštiti podataka

Zbog neprimjenjivosti kriterija lokacije u odnosu na podatke, adresati naloga za dostavljanje i naloga za čuvanje u okviru predložene Uredbe ograničeni su na pružatelje usluga koji pružaju usluge u Uniji, bez obzira na to imaju li poslovni nastan u EU-u ili ne, koji su obvezni imenovati pravnog zastupnika u skladu s pravilima predloženima u nacrtu Direktive. Pojmovi „poslovni nastan” i „pravni zastupnik” stoga su definirani u nacrtima instrumenata.

Odbor ističe da se ti pojmovi pojavljuju i u kontekstu drugih instrumenata EU-a, a posebice u kontekstu Opće uredbe o zaštiti podataka. Prema tome, trebalo bi uključiti objašnjenje o definiciji i razgraničenju tih pojmova u kontekstu prijedloga instrumenata i u kontekstu Opće uredbe o zaštiti podataka.

a) Poslovni nastan

Odbor ističe i da pojam „poslovni nastan” u kontekstu nacrta Uredbe ne bi trebalo zamjenjivati s istim pojmom u kontekstu Opće uredbe o zaštiti podataka. Naime, pojam poslovnog nastana kako je za potrebe nacrta Uredbe definiran u članku 2. stavku 5. širi je od definicije u Općoj uredbi o zaštiti podataka jer uključuje „stvarno obavljanje gospodarske djelatnosti na neodređeno vrijeme s pomoću stabilne infrastrukture iz koje se obavlja djelatnost pružanja usluga”, bez obzira na to vrši li se obrada osobnih podataka u kontekstu djelatnosti tog poslovnog nastana ili ne. Stoga, iako je „poslovni nastan” u smislu Opće uredbe o zaštiti podataka nedvojbeno obuhvaćen definicijom u nacrtu Uredbe, obratno to nije slučaj.

Odbor stoga upozorava da poslovni nastani pružatelja usluga u smislu nacrta Uredbe ne podrazumijevaju nužno da su uvjeti za primjenu Opće uredbe o zaštiti podataka u skladu s člankom 3. stavkom 1. ispunjeni. U tom kontekstu voditelji obrade i izvršitelji obrade trebali bi provjeriti proizlazi li primjenjivost Opće uredbe o zaštiti podataka iz članka 3. stavka 2., što bi podrazumijevalo imenovanje pravnog zastupnika u EU-u i nepostojanje jedinstvenog mehanizma.

b) Pravni zastupnik

U svojoj izjavi Radna skupina istaknula je da bi trebalo izbjeći mogućnost zamjene obveze imenovanja pravnog zastupnika iz članka 27. Opće uredbe o zaštiti podataka s pravnim zastupnikom predviđenim u nacrtu Uredbe o elektroničkim dokazima.

Na temelju podnesenog prijedloga Odbor bi želio ponovno istaknuti tu preporuku te posebno naglasiti da se, prema shvaćanju Odbora, pravni zastupnik u smislu nacrta Direktive o imenovanju pravnih

zastupnika u kontekstu prijedloga instrumenata o elektroničkim dokazima imenuje u svakom slučaju, dodjeljuju mu se specifične funkcije neovisno o mandatu koji mu daje pružatelj usluga, ima ovlasti odgovarati na zahtjeve i djelovati u ime pružatelja usluga te ima veću odgovornost od pravnog zastupnika u kontekstu Opće uredbe o zaštiti podataka.

Nadalje, Odbor naglašava da se obveza imenovanja pravnog zastupnika u svakom slučaju na temelju prijedloga instrumenata o elektroničkim dokazima, bez obzira na to ima li pružatelj usluga poslovni nastan u EU-u ili ne, mogućnost imenovanja čak nekoliko pravnih zastupnika istog pružatelja usluga u skladu s nacrtom Direktive o elektroničkim dokazima i obveza obavješćivanja tijela države članice o imenovanju pravnog zastupnika razlikuju od Opće uredbe o zaštiti podataka, kojom nisu propisani obveza obavješćivanja o imenovanom pravnom zastupniku, iznimke od imenovanja i ograničene odgovornosti pravnog zastupnika.

Stoga, zbog važnih razlika uloga, odgovornosti i odnosa s drugim poslovnim nastanima pružatelja usluge s jedne strane i voditelja obrade ili izvršitelja obrade s druge strane, Odbor preporučuje da se, ako pružatelj usluge nema poslovni nastan u EU-u, ali je obuhvaćen i Općom uredbom o zaštiti podataka u skladu s člankom 3. stavkom 2. i Uredbom o elektroničkim dokazima, imenuju dva zasebna pravna zastupnika s jasnim funkcijama u skladu s instrumentima na temelju kojih su imenovani.

6. Nove kategorije podataka

U članku 2. predložene Uredbe definiraju se različite kategorije podataka: podaci o pretplatniku, podaci o pristupu, podaci o transakcijama i podaci o sadržaju. U uvodnoj izjavi 20. prijedloga Komisije dodatno je objašnjeno: *Kategorije podataka iz ove Uredbe uključuju podatke o pretplatnicima, podatke o pristupu, podatke o transakcijama (te se tri kategorije nazivaju „podaci koji se ne odnose na sadržaj") i podatke o sadržaju. Ta razlika, osim u pogledu podataka o pristupu, postoji u zakonima mnogih država članica i u trenutačnom pravnom okviru SAD-a kojim se pružateljima usluga dopušta da podatke koji se ne odnose na sadržaj dobrovoljno dijele sa stranim tijelima kaznenog progona.*

U tom kontekstu Odbor prvenstveno napominje da sve četiri navedene kategorije podataka treba smatrati osobnim podacima u skladu s pravom EU-a o zaštiti podataka jer sadržavaju informacije koje se odnose na identificiranu fizičku osobu ili fizičku osobu koju se može identificirati, bez obzira je li ona u predloženoj Uredbi nazvana „pretplatnik" ili „korisnik". Slično tome, treba naglasiti da „elektronički dokazi" kako su definirani u članku 2. točki 6. prijedloga Komisije obuhvaćaju sve četiri kategorije podataka i stoga se odnose na osobne podatke. Stoga se predloženom Uredbom umjesto utvrđivanja pravila pristupa dokazima definiranima i kvalificiranima u skladu s nacionalnim pravom i sudskim postupcima utvrđuju novi materijalni i postupovni uvjeti povezani s pristupom osobnim podacima.

Iako se predloženom Uredbom utvrđuju nove potkategorije osobnih podataka na koje se primjenjuju različiti postupovni uvjeti pristupa, Odbor podsjeća da, u skladu s relevantnom sudskom praksom Suda Europske unije, da bi se moglo utvrditi zadiranje u temeljno pravo na privatnost nije važno imaju li dotične informacije o privatnom životu osjetljiv karakter, odnosno jesu li zainteresirane osobe zbog tog zadiranja pretrpjele eventualne neugodnosti.

Nadalje, u odnosu na „podatke koji se ne odnose na sadržaj", a koji u skladu s prijedlogom Komisije uključuju podatke o pretplatnicima, podatke o pristupu i podatke o transakcijama, Odbor podsjeća da je Sud Europske unije u spojenim predmetima C-203/15 i C-698/15 *Tele2 Sverige AB* presudio da metapodaci kao što su podaci o prometu i podaci o lokaciji omogućuju utvrđivanje profila predmetnih

osoba, što je jednako osjetljiva informacija s obzirom na pravo na poštovanje privatnog života, kao i sam sadržaj komunikacija[21].

Kako je već navedeno u izjavi Radne skupine o aspektima zaštite podataka i privatnosti u prekograničnom pristupanju elektroničkim dokazima od 29. studenoga 2017., Odbor ponovno izražava sumnju i zabrinutost u pogledu razgraničenja „podataka koji se ne odnose na sadržaj" i podataka o sadržaju, kao i u pogledu četiri kategorije osobnih podataka utvrđene u prijedlogu Uredbe. Naime, čini se da četiri predložene kategorije nisu jasno razgraničene, a definicija „podataka o pristupu" nejasna je u usporedbi s drugim kategorijama. Odbor stoga izražava žaljenje što Komisija u procjeni učinka i prijedlogu nije dodatno potkrijepila stvaranje tih novih potkategorija osobnih podataka i zabrinutost u odnosu na različite razine jamstava u pogledu materijalnih i postupovnih uvjeta za pristup kategorijama osobnih podataka, posebice uzimajući u obzir poteškoće s ocjenjivanjem u praksi kojoj kategoriji podataka pripadaju zatraženi podaci. Primjerice, IP adrese mogle bi se kategorizirati i kao podaci o transakcijama i kao podaci o pretplatniku.

U tom kontekstu Odbor podsjeća i da je u uvodnoj izjavi 14. prijedloga Uredbe o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama (Uredba o e-privatnosti) Komisija navela da „elektroničke komunikacijske podatke trebalo bi definirati dovoljno široko i tehnološki neutralno kako bi se obuhvatile sve informacije o sadržaju koji se prenosi ili razmjenjuje (sadržaj elektroničkih komunikacija) i informacije o krajnjem korisniku elektroničkih komunikacijskih usluga koje se obrađuju u svrhu prijenosa, distribucije ili omogućavanja razmjene sadržaja elektroničkih komunikacija, uključujući podatke za praćenje i identifikaciju izvora i odredišta komunikacije, zemljopisnu lokaciju te datum, vrijeme, trajanje i vrstu komunikacije". Budući da će se postojeći i budući okvir za e-privatnost, kao i povezana ograničenja prava na privatnost, primjenjivati na pravila kojima se uređuje pristup tijela za izvršavanje zakonodavstva elektroničkim dokazima, Odbor preporučuje da se u predloženu Uredbu uvrsti šira definicija podataka o elektroničkim komunikacijama kako bi se osiguralo da se primjerenim zaštitnim mjerama i uvjetima za dobivanje pristupa dosljedno obuhvaćaju i „podaci koji se ne odnose na sadržaj" i „podaci o sadržaju".

7. Analiza postupaka za europski nalog za čuvanje i europski nalog za dostavljanje

Općenito govoreći, čini se da je postupak za upućivanje naloga za dostavljanje ili naloga za čuvanje sljedeći:

- Ovisno o vrsti traženih podataka i vrsti naloga, nadležno pravosudno tijelo – tijelo izdavatelj – izdaje nalog u skladu s (oskudnim) uvjetima nabrojanima u člancima 5. i 6., šalje ga pomoću usklađene potvrde adresatu – pravnom zastupniku pružatelja usluge ili bilo kojem poslovnom nastanu pružatelja usluge u EU-u.
- Po primitku potvrde adresat izvršava nalog, odnosno prenosi podatke u roku od 10 dana ili 6 sati u hitnim slučajevima ili ih čuva najviše 60 dana – osim ako to nije moguće jer je potvrda nepotpuna, zbog više sile, zbog *de facto* nemogućnosti adresata ili zato što adresat odbija izvršiti nalog na temelju proturječnih obveza, bilo u odnosu na temeljna prava ili temeljne interese treće zemlje, ili na drugim temeljima.

[21] Presuda Suda Europske unije od 21. prosinca 2016., točka 99.

- Ako adresat nije postupio u skladu s primljenim nalogom, a da nije naveo razloge koje je tijelo izdavatelj prihvatilo, predviđeni su postupci za izvršenje naloga koje provodi nadležno tijelo za izvršenje u državi članici u kojoj pružatelj usluge ima predstavnika ili poslovni nastan, osim ako se primjenjuju ograničeni temelji za odbijanje i ako se tijelo izvršitelj protivi priznavanju ili izvršenju naloga.
- Ako je adresat izdao obrazloženi prigovor na nalog na temelju proturječnih obveza, tijelo izdavatelj upućuje predmet nadležnom sudu u svojoj državi članici koji će biti zadužen za rješavanje mogućeg sukoba i za provedbu naloga u slučaju nepostojanja sukoba. U slučaju sukoba nadležni sud obraća se središnjim tijelima u trećoj zemlji putem nacionalnih središnjih tijela s rokom od 15 dana za odgovor, koji se može produljiti za 30 dana na temelju obrazloženog zahtjeva, u slučaju proturječnih obveza u pogledu temeljnih prava ili temeljnih interesa treće zemlje, ili sam utvrđuje treba li provesti ili povući nalog zbog drugih osnova za odbijanje na koje se adresat pozvao.
- Ne dovodeći u pitanje pravne lijekove koji su raspoloživi u skladu s Općom uredbom o zaštiti podataka i Direktivom o zaštiti podataka pri izvršavanju zakonodavstva, osobe čiji su podaci dobiveni na temelju naloga za dostavljanje imaju pravo i na djelotvoran pravni lijek protiv tog naloga.

Odbor je ocijenio predviđene postupke i zaštitne mjere sadržane u nacrtu Uredbe koji prate različite korake i za svaki od aspekata navedenih u nastavku preporučuje sljedeće zaštitne mjere i izmjene.

a) Pragovi za izdavanje naloga trebali bi biti povišeni, a naloge izdavati ili ovjeravati sudovi

Kad je riječ o uvjetima za izdavanje naloga, Odbor pozdravlja načelo većih zaštitnih mjera za pristup podacima o transakcijama ili podacima o sadržaju. Međutim, Odbor napominje da, kako kaznene sankcije nisu u potpunosti usklađene među državama članicama, upućivanje na „kaznena djela kažnjiva u državi izdavateljici maksimalnom zatvorskom kaznom od najmanje tri godine”[22] i dalje podrazumijeva različite pragove i odstupanja u zaštiti podataka ispitanika unutar EU-a.

Nadalje, Odbor naglašava da se navedeni prag, posebice imajući na umu široku definiciju podataka o pretplatnicima, doima izrazito niskim za naloge za čuvanje i naloge za dostavljanje podataka o pretplatnicima ili podataka o pristupu, jer se u načelu izdavanje takvih naloga može opravdati svim kaznenim djelima. Slično tome, tijela kojima je dopušteno izdavati takve naloge ograničenija su u kontekstu naloga za dostavljanje podataka o transakcijama ili podataka o sadržaju nego u kontekstu izdavanja naloga za čuvanje ili naloga za dostavljanje podataka o pretplatniku ili podataka o pristupu jer tužitelji mogu izdati ili odobriti samo ove zadnje dok svaki sudac, sud ili istražni sudac može izdati ili odobriti bilo koji nalog.

Konkretno, Odbor izražava žaljenje što je najniži prag kojim se tijelima za izvršavanje zakonodavstva omogućuje da zatraže pristup podacima o pretplatniku i podacima o pristupu za bilo koje kazneno djelo temelji na tumačenju *a contrario* sudske prakse Suda Europske unije (koja se prvenstveno odnosi na druge podatke) za određivanje pripadajućih zaštitnih mjera. Naime, Sud je posebno naglasio da je pristup nadležnih tijela podacima o prometu i podacima o lokaciji ograničen isključivo na borbu protiv

[22] Vidjeti članak 5. stavak 3. točku (a).

teških kaznenih djela[23]. Odbor može razumjeti da bi prijedlog omogućio traženje pristupa najosnovnijim informacijama koje bi omogućile samo identifikaciju osobe bez otkrivanja bilo kakvih podataka o komunikaciji bez prethodnog odobrenja suda. Međutim, Odbor izražava žaljenje zbog Komisijina širokog tumačenja *a contrario* te presude i poziva na uvođenje većih zaštitnih mjera kako bi se ograničile osnove za pristup drugim podacima o pretplatnicima i podacima o pristupu. Odbor predlaže ograničavanje pristupa tim podacima ili na popis kaznenih djela naveden u nacrtu Uredbe ili barem na „teška kaznena djela", posebice imajući na umu predviđeni nizak prag za prethodno odobrenje za te podatke.

K tome, Odbor naglašava da to tumačenje *a contrario* dovodi i do toga da se prijedlogom otvara mogućnost tužiteljima da izdaju ili odobravaju izdavanje naloga. Odbor smatra da je to, osim u slučaju zahtjeva za najosnovnije informacije koje bi omogućile samo identifikaciju osobe bez otkrivanja bilo kakvih podataka o komunikaciji, nazadovanje u odnosu na sudsku praksu Suda o pristupu podacima o komunikaciji. Doista, u sudskoj praksi o pristupu podacima o komunikaciji za potrebe izvršavanja zakonodavstva Sud je uvjetovao da mogućnost davanja takvog pristupa, među ostalim kriterijima te *osim u valjano opravdanim hitnim slučajevima*[24], ovisi o *prethodnom nadzoru suda ili neovisnog upravnog tijela* i to *nakon obrazloženog zahtjeva nacionalnih tijela podnesenog osobito u okviru postupaka sprečavanja, otkrivanja ili progona kaznenih djela*[25].

Odbor podsjeća da je pojam „sud" autonomni pojam prava EU-a te da je Sud Europske unije stalno naglašavao i isticao kriterije koje treba ispuniti da bi se tijelo kvalificiralo kao sud, uključujući kriterij neovisnosti[26] koji se ne primjenjuje na tužitelje, kako je istaknuo i Europski sud za ljudska prava u svojoj sudskoj praksi[27].

Sukladno tome, iz članka 4. stavka 1. točaka (a) i (b) i članka 4. stavka 3. točaka (a) i (b) proizlaze postupci sa znatno slabijim zaštitnim mjerama za podatke o pretplatniku i podatke o pristupu jer će tužitelj moći sam zatražiti podatke bez daljnje kontrole tijela države u kojoj se nalaze traženi podaci ili tijela države u kojoj se nalazi pravni zastupnik poduzeća od kojeg su podaci zatraženi, kao i bez kontrole neovisnog upravnog tijela.

Nadalje, Odbor je primijetio takozvanu dodatnu zaštitnu mjeru iz članka 5. stavka 2. kojom se mogućnost izdavanja naloga za dostavljanje ograničava na slučaj kad je slična mjera dostupna za isto kazneno djelo u usporedivoj domaćoj situaciji. Međutim, Odbor ističe kontraproduktivne učinke te odredbe: umjesto da se njome osiguraju dodatne zaštitne mjere, čini se da se odredbom potiče države članice da prošire svoje nacionalne mogućnosti za traženje podataka o pretplatniku ili podataka o pristupu kako bi osigurale da se mogu izdati nalozi za dostavljanje u skladu s Uredbom.

b) Rokovi za dostavljanje podataka trebali bi biti opravdani

Odbor je uočio da se na europske naloge za dostavljanje odgovara najkasnije u roku od 10 dana od primitka potvrde, osim ako tijelo izdavatelj navede razloge za ranije otkrivanje, te najkasnije u roku od 6 sati u hitnim slučajevima, kako je propisano člankom 9. stavcima 1. i 2.

Međutim, Odbor nije pronašao nikakve kriterije kojima se uobličuje obveza tijela da dokažu hitnost dostavljanja podataka, čak ni naknadno, kako bi se omogućila kontrola upotrebe tog vrlo brzog postupka, a rok od šest sati podrazumijeva da bi pružatelj usluga prije dostavljanja podataka izvršio

[23] Vidjeti predmet 203/15, točka 125.
[24] Vidjeti predmet 203/15, točka 120.
[25] Vidjeti spojene predmete C-293/12 i C-594/12, točka 62.
[26] Vidjeti primjerice predmet C 203/14.
[27] Vidjeti primjerice Moulin protiv Francuske, 23.11.2010.

vrlo površnu kontrolu ili da je ne bi izvršio. U procjeni učinka naglašeno je da nadležna tijela moraju imati pravovremeni pristup podacima. Međutim, svi primjeri navedeni u procjeni učinka tiču se dokaza potrebnih u slučaju počinjenja teških kaznenih djela (teroristički napadi s taocima, seksualno zlostavljanje djece koje je u tijeku), no opravdanje temeljeno na nepostojanosti dokaza nije dobro ako nema specifičnog hitnog slučaja osim te potencijalne nepostojanosti dokaza. K tome, nepostojanost dokaza nije dodatno opravdanje u smislu proporcionalnosti da bi se odobrio pristup podacima s manje zaštitnih mjera u situacijama kad je jedino opravdanje za hitnost nepostojanost podataka.

K tome, Odbor sumnja da je nužno utvrditi rok od šest sati i istodobno navesti da se taj rok ne primjenjuje dok tijelo izdavatelj ne navede dodatna objašnjenja „u roku od pet dana" ako pružatelj usluge ne može ispuniti svoju obvezu.

Odbor stoga traži uvođenje dodatnih elemenata u procjenu učinka kako bi se opravdala potreba za tim rokovima u slučaju da kazneno djelo koje je počinjeno ili koje se istražuje nije teško te, ako ti podrobni elementi nisu navedeni, izričite kriterije za opravdavanje hitnosti ako su izdani EPOC-ovi. Primjerice, mogao bi se predvidjeti isti model kao u Direktivi o EIN-u. Direktivom o EIN-u omogućen je kraći rok kad je to opravdano „zbog postupovnih rokova, težine kaznenog djela ili drugih posebno hitnih okolnosti" (vidjeti članak 12. stavak 2.) ili 24-satni rok za odlučivanje o privremenoj mjeri (vidjeti članak 32. stavak 2.). U procjeni učinka nacrta Uredbe nisu navedena detaljna obrazloženja zašto ti rokovi nisu odgovarajući, nego je samo istaknuto da su pravosudna tijela „zatrpana" velikim brojem poslanih zahtjeva i da zato ne mogu poštovati rokove.

c) Europski nalog za dostavljanje i europski nalog za čuvanje ne upotrebljavaju se za traženje podataka o ispitaniku iz druge države članice bez barem obavješćivanja nadležnih tijela te države članice, posebice za podatke o sadržaju

Odbor ističe da je u postojećim instrumentima osigurana pravosudna suradnja, a time i dodatne zaštitne mjere, posebice za kontrolu nužnosti i proporcionalnosti zahtjeva, te naglašava da su te zaštitne mjere posebno opravdane u slučajevima kad se traže podaci o sadržaju koji podrazumijevaju veća ograničenja prava ispitanika na zaštitu osobnih podataka i privatnosti. U tom pogledu Odbor podsjeća da je Direktivom o EIN-u omogućeno presretanje telekomunikacija uz tehničku pomoć druge države članice (vidjeti članak 30.) kao i obveza obavješćivanja nadležnog tijela druge države članice na čijem se državnom području ispitanik nalazi ili će se nalaziti o presretanju podataka ako tehnička pomoć nije potrebna (vidjeti članak 31.).

Odbor ne pronalazi opravdanje za postupak predviđen u nacrtu Uredbe o elektroničkim dokazima kojim bi se omogućilo dostavljanje podataka o sadržaju bez uključivanja barem nadležnih tijela države članice u kojoj se nalazi ispitanik.

d) Europski nalog za čuvanje ne smije se upotrebljavati za zaobilaženje obveza pružatelja usluga u pogledu zadržavanja podataka

Odbor ističe da je glavni cilj europskog naloga za čuvanje spriječiti brisanje podataka.

Iako Odbor priznaje da to u nekim slučajevima može biti nužno i razmjerno, ipak izražava žaljenje zbog nedostatka zaštitnih mjera u pogledu izdavanja takvih naloga. Konkretno, Odbor preporučuje da, ako su nalozi za čuvanje izdani samo za specifične podatke, iako se čini da se nacrtom dopuštaju i zahtjevi širokog opsega, te ako se ti nalozi izdaju za podatke čije je brisanje planirano u skladu s načelom

zadržavanja podataka, nalog nikad ne smije biti osnova da bi pružatelj usluge obrađivao podatke nakon izvornog datuma brisanja. Drugim riječima, podaci bi trebali biti „zamrznuti".

K tome, poveznicu između naloga za čuvanje i naknadnog zahtjeva za dostavljanje podataka, bio on europski nalog za dostavljanje, zahtjev za EIN ili zahtjev za uzajamnu pravnu pomoć, trebalo bi ojačati kako bi se osiguralo izdavanje europskih naloga za čuvanje samo u slučajevima kad je izdavanje drugog zahtjeva sigurno (a ne da se o njemu razmišlja kao o mogućnosti) te da valjanost naloga za čuvanje istječe ako drugi zahtjev bude odbijen, umjesto da se čeka 60 dana[28] ako je naknadni zahtjev ranije odbijen.

e) Povjerljivost i informacije o korisnicima

Odbor je uočio da je u nacrt Uredbe uvršten poseban članak[29] koji se odnosi na povjerljivost upućenih naloga. Kako bi se izbjegle sve nejasnoće i mogući nesporazumi u pogledu prava na zaštitu podataka, Odbor podsjeća da, iako je Općom uredbom o zaštiti podataka predviđeno da ograničenje prava ispitanika zbog zaštite sprečavanja, istrage, otkrivanja ili progona kaznenih djela bude propisano zakonom i stoga javno[30] i da te zakonske mjere sadržavaju specifične odredbe o pravu ispitanika da budu obaviješteni o ograničenju, osim ako to može biti štetno za svrhu ograničenja[31], njome nije propisana obveza obavješćivanja pojedinačnih ispitanika o svakom zahtjevu za pristup podacima koji podnesu tijela za izvršavanje zakonodavstva.

Međutim, u međuvremenu Odbor podsjeća da je Direktivom o zaštiti podataka predviđeno pravo ispitanika na informacije od samih nadležnih tijela, osim ako je to pravo ograničeno, za sve ispitanike, odnosno bez ograničenja prava samo na ispitanike koji borave na području EU-a.

f) Postupak za izvršenje naloga ako ga pružatelj usluga odbije provesti

Odbor je uočio da članak 14. nacrta Uredbe propisuje postupak za osiguravanje izvršenja naloga ako adresat ne postupi u skladu s njim oslanjajući se na pravosudnu suradnju između tijela izdavatelja i nadležnog tijela u državi izvršiteljici.

Međutim, čini se da taj postupak ne omogućuje tijelu izvršitelju da odbije provesti preneseni nalog osim na isključivo postupovnoj osnovi (istoj kao za adresata, koja se uglavnom odnosi na nedostatak dostavljenih informacija ili stvarnu nemogućnost dostavljanja podataka), ako su predmetni podaci zaštićeni imunitetom ili povlasticom u skladu s njegovim nacionalnim pravom ili ako bi njihovo otkrivanje moglo naštetiti njegovim temeljnim interesima kao što su nacionalna sigurnost i obrana[32].

Odbor stoga ponovno izražava zabrinutost i u pogledu uklanjanja svih dvostrukih provjera prenesenog naloga koje bi provelo nadležno tijelo primatelj u odnosu na druge instrumente. Čak i osnova za odbijanje izvršenja naloga na osnovi toga što se njime krši Povelja pojavljuje se iznad klasičnog praga koji se odnosi na kršenje temeljnih prava dotične osobe. Sukladno tome, slijedeći primjer europskog uhidbenog naloga kojim se omogućuju i obvezni i neobvezni razlozi za odbijanje izvršenja, ili barem Direktive o EIN-u kojom je općenito propisano da je pretpostavka „stvaranje područja slobode, sigurnosti i pravde unutar Unije temelji se na uzajamnom povjerenju i pretpostavci sukladnosti drugih država članica s pravom Unije i, posebno, s temeljnim pravima" osporiva[33], nacrtom Uredbe trebalo bi

[28] Vidjeti članak 10. stavak 1.
[29] Vidjeti članak 11.
[30] Vidjeti članak 23. stavak 1. točku (d).
[31] Vidjeti članak 23. stavak 1. točku (h).
[32] Vidjeti članak 14. stavak 2.
[33] Vidjeti uvodnu izjavu 19. Direktive o EIN-u.

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 priznatih Poveljom, izvršenje naloga trebalo biti odbijeno.

g) Izvršenje naloga i proturječne obveze u skladu sa zakonima treće zemlje (članci 15. – 16.)

Odbor pozdravlja mogućnost iz nacrta Uredbe da adresati odbiju nalog na temelju činjenice da se on kosi s temeljnim pravima jer se time osiguravaju zaštitne mjere u slučaju proturječnih pravnih obveza. Čini se nužnim i da se u prijedlogu predvidi savjetovanje s tijelima treće zemlje, barem u slučaju sukoba, kao i obveza povlačenja naloga ako tijelo treće zemlje uloži prigovor.

Stoga bi predviđeni postupak za odbijanje izvršenja naloga na temelju proturječnih obveza koje proizlaze iz zakona treće zemlje trebalo znatno poboljšati.

Prvo, Odbor je uočio da se nacrtom Uredbe privatnom poduzeću kao adresatu naloga za dostavljanje povjerava procjena je li nalog u sukobu s primjenjivim zakonima treće zemlje kojima se zabranjuje otkrivanje traženih podataka. Poduzeće mora uložiti obrazloženi prigovor koji sadržava sve relevantne pojedinosti o pravu treće zemlje, o njegovoj primjenjivosti na predmetni slučaj i o prirodi proturječnih obveza.

Što je najvažnije, Odbor je zabrinut da će, kad bude uložen takav prigovor, nadležni sud države članice tijela izdavatelja sam ocjenjivati postoji li sukob, jer se u kontakt s tijelima treće zemlje stupa samo ako sud utvrdi postojanje sukoba. Nadležnom sudu iz EU-a stoga se u tom kontekstu daje nadležnost za konačno tumačenje prava treće zemlje, a da on nije nužno specijaliziran za tu materiju. Odbor stoga smatra da je u prijedlogu Uredbe obveza savjetovanja s nadležnim tijelima treće zemlje previše ograničena. U području zaštite podataka Odbor želi zakonodavcima istaknuti činjenicu da, iako bi nadležni sud treće zemlje tumačio Opću uredbu o zaštiti podataka kako bi ocijenio je li ona proturječna njegovim zahtjevima, tijela EU-a za zaštitu podataka i nadležni sudovi i dalje bi bili nadležni za ocjenjivanje zakonitosti prijenosa na temelju presude suda ili odluke upravnog tijela treće zemlje kojom se traži prijenos ili otkrivanje osobnih podataka u području primjene Opće uredbe o zaštiti podataka[34].

K tome, Odbor naglašava da se ocjena prava treće zemlje koju provodi nadležni sud države članice koja je podnijela zahtjev mora temeljiti na objektivnim elementima te je obuhvaćena kriterijima koje nadležna tijela trebaju uzeti u obzir pri ocjeni prava treće zemlje u skladu s člankom 15. stavkom 4. i člankom 16. stavkom 5. točkom (a) nacrta Uredbe. Naime, sud bi trebao utvrditi činjenicu da se „umjesto zaštite temeljnih prava ili temeljnih interesa treće zemlje povezanih s nacionalnom sigurnošću ili obranom" pravom treće zemlje nastoje „očito zaštititi drugi interesi ili je usmjereno na zaštitu nezakonitih aktivnosti u okviru zahtjeva tijela kaznenog progona u kontekstu kaznenih istraga" ili „interesa koji se štite mjerodavnim pravom treće zemlje, uključujući interesa treće zemlje za sprječavanje otkrivanja podataka". Primjerice, iako bi za tu procjenu zbog mogućeg utjecaja te odluke trebalo provesti procjenu na temelju dokaza u pogledu svih raspoloživih informacija, u najmanju ruku je fraza „ili je usmjeren" nejasna i trebalo bi je prilagoditi („ima za cilj").

Odbor izražava žaljenje što se s tijelima treće zemlje savjetuje o izvršenju naloga za dostavljanje (i ona mogu izreći prigovor) samo ako nadležni sud države članice smatra da postoji relevantan sukob i ako dostavi sve elemente središnjim tijelima predmetne treće zemlje, a središnje tijelo te treće zemlje

[34] Vidjeti članak 48. Opće uredbe o zaštiti podataka.

može izreći prigovor u kratkom roku od najviše 50 dana (15 dana za odgovor, moguće produljenje za 30 dana i zatim podsjetnik s pet dodatnih dana). U svim drugim slučajevima nadležni sud mogao bi potvrditi nalog za dostavljanje i izreći novčanu kaznu pružatelju usluge koji odbija izvršiti nalog. Stoga Odbor izražava zabrinutost da nadležni sudovi EU-a neće imati širu obvezu savjetovanja s nadležnim tijelima dotičnih trećih zemalja kako bi osigurali da će se postupkom sustavnije jamčiti uzimanje u obzir argumenata obiju strana te pokazati veće poštovanje prava trećih zemalja.

Kako je već istaknuto u izjavi Radne skupine iz članka 29. i prethodno u tekstu, Odbor podsjeća da bi posebnu pozornost trebalo pridati donošenju sličnih instrumenata u trećim zemljama koji utječu na prava ispitanika i njihovo pravo na privatnost unutar EU-a, a posebice opasnosti da bi slični instrumenti bili u izravnom sukobu s pravom EU-a o zaštiti podataka.

K tome, Odbor naglašava da nadležno tijelo države članice izdavatelja možda nije nadležan sud za provođenje naloga kako je predviđeno u članku 14. nacrta Uredbe, čime bi se dodatno povećao rizik od proturječnih postupaka i nedostatka provjere u slučaju sukoba zakona. To je rezultat činjenice da u nekim slučajevima mogu biti obuhvaćene tri zemlje: država tijela koje izdaje nalog, treća zemlja pružatelja usluge i država članica u kojoj se nalazi pravni zastupnik pružatelja usluge u EU-u te u kojoj bi nalog trebao biti izvršen. Sukladno tome, primjenjujući predviđeni postupak sud podnositelja zahtjeva u državi članici A mogao bi donijeti svoje tumačenje prava treće zemlje B pružatelja usluga, a da ne zatraži mišljenje tijela te treće zemlje (iako bi ona podnijela prigovor na nalog) i zatražiti od suda države članice C da izvrši njegovu odluku bez mogućnosti prigovora.

Osim toga, Odbor pozdravlja i uvođenje posebnih pravnih lijekova protiv naloga za dostavljanje uz pravne lijekove koji su raspoloživi u skladu s Općom uredbom o zaštiti podataka i Direktivom o zaštiti podataka. Radna skupina je u prethodnoj izjavi već zatražila takve zaštitne mjere. Međutim, Odbor izražava žaljenje što takvi pravni lijekovi nisu predviđeni i protiv naloga za čuvanje, jer se i tim nalozima mogu ograničiti temeljna prava pojedinaca čiji se podaci zadržavaju. Naime, na temelju naloga za čuvanje podaci mogu biti zadržani dulje nego što je to propisano pravilima o zaštiti podataka. Stoga nalog za čuvanje sam po sebi izaziva ograničavanje temeljnih prava dotičnog ispitanika, a opravdanje za to podliježe preispitivanju i posebnim pravnim lijekovima, posebice u slučajevima ako je nalog za čuvanje izdan zajedno s nalogom za dostavljanje podataka. Kako je Radna skupina iz članka 29. preporučila u svojem izvješću, treba predvidjeti pravne lijekove barem jednakovrijedne onima koji su na raspolaganju u nacionalnim slučajevima.

h) Sigurnost prijenosa podataka pri odgovaranju na nalog

Odbor ističe da su nacrtom Uredbe obuhvaćeni samo nalozi koji se šalju adresatima unutar Europske unije te stoga nisu predviđeni nikakvi posebni kanali za prijenos podataka između adresata i pružatelja usluga smještenih izvan Europske unije.

Iako pozdravlja činjenicu da nema daljnjih odstupanja od općeg okvira EU-a za zaštitu podataka, Odbor podsjeća da svaki nalog poslan adresatu koji podrazumijeva prijenos izvan EU-a treba biti u skladu s pravnim okvirom propisanim Općom uredbom o zaštiti podataka. Naime, zaobilaženje pravnog okvira pravosudne suradnje, kojim je propisano poštivanje mjera za zaštitu podataka, ne bi smjelo izazvati da adresat naloga za dostavljanje ili naloga za čuvanje zaobilazi zahtjeve za prijenos podataka.

K tome, iako pozdravlja činjenicu da nema odredbe kojom se nameće obveza dešifriranja enkribiranih podataka[35], Odbor izražava zabrinutost jer nacrtima zakonodavnih instrumenata nisu predviđeni nikakvi posebni zahtjevi da adresati provjere vjerodostojnost dostavljenih podataka, naglašava da je ta

[35] Vidjeti uvodnu izjavu 19. i stranicu 240. procjene učinka.

procjena upravo dodana vrijednost tradicionalnih instrumenata koji se oslanjaju na pravosudnu suradnju te upozorava da bez takve procjene raste rizik za obuhvaćene ispitanike.

Zaključci

Na temelju ove procjene Odbor želi uputiti sljedeće preporuke suzakonodavcima:

1) Pravna osnova Uredbe ne bi trebao biti članak 82. stavak 1. UFEU-a.
2) Potreba za novim instrumentom u usporedbi s postojećom Direktivom o EIN-u ili MLAT-ovima trebala bi biti bolje opravdana, među ostalim i podrobnom analizom manje nametljivih sredstava u pogledu temeljnih prava kao što su izmjene postojećih instrumenata ili ograničenje područja primjene ovog instrumenta na naloge za dostavljanje u kombinaciji s drugim postojećim postupcima za traženje pristupa podacima.
3) Uredbom bi trebalo propisati dulji rok kako bi se pružatelju usluge koji izvršava nalog omogućilo da osigura poštovanje dodatnih zaštitnih mjera u pogledu zaštite temeljnih prava.
4) Trebalo bi zadržati načelo dvostruke kažnjivosti, posebice ako se ne koristi kriterij lokacije podataka, kako bi se sačuvala obveza uzimanja u obzir zaštitnih mjera u obje države (državi tijela izdavatelja i državi u kojoj se nalazi pružatelj usluge).
5) Područje primjene Uredbe trebalo bi ograničiti na voditelje obrade u smislu Opće uredbe o zaštiti podataka ili uvrstiti odredbu da, ako pružatelj usluge kojem je upućen nalog nije voditelj nego izvršitelj obrade, on mora obavijestiti voditelja obrade.
6) Uredba bi trebala sadržavati zaštitne mjere za prijenos podataka ako pružatelj usluge ima poslovni nastan u trećoj zemlji za koju nije donesena odluka o primjerenosti u tom području ili upućivanje na Direktivu 2016/680 jer bi te zaštitne mjere bile primjenjive.
7) Budući da obvezno imenovanje pravnog zastupnika odstupa od Opće uredbe o zaštiti podataka, u Uredbi bi trebalo navesti da se pravni zastupnik imenovan u skladu s Uredbom o elektroničkim dokazima razlikuje od zastupnika imenovanog u skladu s člankom 3. stavkom 2. Opće uredbe o zaštiti podataka.
8) Uredba bi trebala sadržavati širu definiciju podataka o elektroničkim komunikacijama kako bi se osiguralo da prikladne zaštitne mjere i uvjeti za dobivanje pristupa obuhvaćaju i podatke o sadržaju i podatke koji se ne odnose na sadržaj.
9) U Uredbi bi trebalo podići pragove za izdavanje naloga, a naloge trebaju izdavati ili odobravati sudovi, osim za podatke o pretplatnicima, pod uvjetom da se definicija te kategorije podataka drastično suzi na najosnovnije informacije koje omogućuju samo identifikaciju osobe bez obuhvaćanja pristupa bilo kakvim podacima o komunikaciji.
10) U Uredbi bi pristup podacima o pretplatnicima i podacima o pristupu trebalo ograničiti na strogo određen popis kaznenih djela ili barem na „teška kaznena djela”.
11) Rok za dostavljanje podataka, posebno u hitnim slučajevima, trebalo bi bolje opravdati u Uredbi, a mogućnost upotrebe brzog šestosatnog postupka trebala bi obuhvaćati obvezu tijela izdavatelja da dokaže hitnost zbog koje se upotrebljava taj postupak, čak i *a posteriori*, kako bi se omogućila kontrola upotrebe takvih iznimnih ovlasti.
12) Trebalo bi odustati od postupka za dostavljanje podataka o sadržaju bez uključivanja tijela države članice u kojoj se nalazi ispitanik.
13) U Uredbi bi trebalo poboljšati zaštitne mjere u pogledu izdavanja europskih naloga za čuvanje.
14) Uredba bi trebala sadržavati barem 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 priznatih Poveljom, izvršenje naloga trebalo biti odbijeno.

15) Uredbom bi trebalo predvidjeti širu obvezu savjetovanja s nadležnim tijelima treće zemlje u kojoj se nalazi pružatelj usluga kojem je naloženo da dostavi podatke zbog mogućeg sukoba zakona kako bi se izbjeglo subjektivno tumačenje jednog suda.
16) Valjanost i trajanje naloga za čuvanje trebali bi biti povezaniji s nalozima za dostavljanje koji su im priloženi.
17) Trebalo bi bolje jamčiti sigurnost prijenosa podataka.
18) Trebalo bi predvidjeti provjeru vjerodostojnosti podataka, posebice ako se mogu dostaviti enkribirani podaci.

Za Europski odbor za zaštitu podataka

Predsjednica

(Andrea Jelinek)