RADNA SKUPINA ZA ZAŠTITU PODATAKA IZ ČLANKA 29.

17/HR

WP 247

Mišljenje 01/2017 o prijedlogu Uredbe o e-privatnosti (2002/58/EZ)

doneseno 4. travnja 2017.

RADNA SKUPINA ZA ZAŠTITU POJEDINAČNIH KORISNIKA U VEZI S OBRADOM OSOBNIH PODATAKA

uspostavljena Direktivom 95/46/EZ Europskog parlamenta i Vijeća od 24. listopada 1995.,

uzimajući u obzir članke 29. i 30. te Direktive,

uzimajući u obzir njezin poslovnik,

DONIJELA JE OVO MIŠLJENJE:

SAŽETAK

Radna skupina pozdravlja prijedlog Europske komisije od 10. siječnja 2017. za uredbu o e-privatnosti. Radna skupina pozdravlja **odabir uredbe** kao regulatornog instrumenta. Time se osiguravaju ujednačena pravila u cijelom EU-u te jasnoća za organizacije i nadzorne tijela. To pomaže i u osiguravanju usklađenosti s Općom uredbom o zaštiti podataka. Toj usklađenosti dodatno pridonosi i odluka da **isto tijelo koje je odgovorno za praćenje usklađenosti s Općom uredbom o zaštiti podataka (OUZP)** bude odgovorno i za provedbu pravila o e-privatnosti.

Istodobno, odabir (zadržavanje) **dopunskog pravnog instrumenta** pozitivna je odluka. Zaštita povjerljive komunikacijske i terminalne opreme ima posebne značajke koje nisu obuhvaćene OUZP-om. Stoga su za te vrste usluga potrebne dopunske odredbe kako bi se osigurala odgovarajuća zaštita temeljnog prava na privatnost i povjerljivost komunikacija, uključujući povjerljivost terminalne opreme. U tom pogledu Radna skupina snažno podržava **načelni pristup** koji je odabran u predloženoj Uredbi, a uključuje **opsežne zabrane i ograničena izuzeća** te **ciljanu primjenu pojma privole**.

Radna skupina pozdravlja proširenje područja primjene predložene Uredbe radi **uključivanja pružatelja OTT usluga**, tj. usluga koje su funkcionalno istovjetne tradicionalnijim sredstvima komunikacije te stoga mogu na sličan način utjecati na privatnost i pravo na tajnost komunikacija ljudi u EU-u. Pozitivno je i to što su predloženom Uredbom jasno obuhvaćeni **sadržaj i povezani metapodaci** te što se njome priznaje da se **na temelju metapodataka mogu otkriti vrlo osjetljivi podaci.**

Međutim, Radna skupina isto tako smatra da postoje četiri područja koja izazivaju **ozbiljnu zabrinutost**. Kad je riječ o **praćenju lokacije terminalne opreme, uvjetima pod kojima je dopuštena analiza sadržaja i metapodataka, zadanim postavkama terminalne opreme i softvera te „zidovima za praćenje",** predloženom Uredbom snizila bi se razina zaštite koja se pruža OUZP-om. U ovom Mišljenju Radna skupina daje konkretne prijedloge kako bi se osiguralo da će se Uredbom o e-privatnosti jamčiti ista ili viša razina zaštite primjerena osjetljivoj prirodi komunikacijskih podataka (sadržaja i metapodataka).

Kad je riječ o **praćenju putem mreže WiFi**, ovisno o okolnostima i svrhama prikupljanja podataka, u skladu s OUZP-om za takvo će praćenje vjerojatno biti potrebna privola ili će se moći provoditi samo ako se prikupljeni osobni podaci anonimiziraju. U potonjem slučaju moraju biti ispunjena sljedeća četiri uvjeta: svrha prikupljanja podataka iz terminalne opreme ograničena je na puko statističko brojanje, praćenje je ograničeno vremenski i prostorno koliko je nužno potrebno za tu svrhu, podaci će potom biti odmah izbrisani ili anonimizirani te postoje učinkovite mogućnosti izuzeća. Europsku komisiju poziva se da promiče razvoj tehničkog standarda za mobilne uređaje tako da mogu automatski signalizirati prigovor na takvo praćenje.

Kad je riječ o **analizi sadržaja i metapodataka**, polazište bi trebalo biti u tome da je zabranjena obrada komunikacijskih podataka bez privole svih krajnjih korisnika (pošiljatelja i primatelja). Kako bi se pružateljima usluga omogućilo pružanje usluga koje je izričito zatražio korisnik, kao što su, na primjer, funkcija pretraživanja i indeksiranja ili usluge

pretvaranja teksta u govor, trebalo bi postojati domaće izuzeće za obradu sadržaja i metapodataka u isključivo osobne svrhe samog korisnika.

Kad je riječ o **privoli za praćenje**, Radna skupina zalaže se za izričitu zabranu „zidova za praćenje", to jest uvjeta kojim se korisnike prisiljava na davanje privole za praćenje ako žele imati pristup usluzi.

Naposljetku, Radna skupina preporučuje da terminalna oprema i softver moraju **imati integrirane postavke za zaštitu privatnosti** te korisnicima jasno nuditi mogućnosti potvrđivanja ili mijenjanja tih integriranih postavki tijekom instaliranja. Postavke moraju biti lako dostupne tijekom upotrebe. Korisnici moraju imati mogućnost signalizirati posebnu privolu preko svojih postavki preglednika. Postavke privatnosti ne bi trebale biti ograničene na zadiranje trećih osoba ili na kolačiće. Radna skupina snažno preporučuje da primjena standarda „Ne prati" bude obvezna.

Radna skupina utvrdila je i ostala problematična područja koja se odnose, na primjer, na područje primjene, zaštitu terminalne opreme i izravni marketing. Naposljetku, Radna skupina utvrdila je pitanja koja je potrebno pojasniti radi bolje zaštite krajnjih korisnika i uvođenja veće pravne sigurnosti za sve uključene dionike.

SADRŽAJ

1. UVOD

1. Radna skupina za zaštitu podataka iz članka 29. (Radna skupina ili Radna skupina iz članka 29.) pozdravlja prijedlog uredbe o e-privatnosti Europske komisije (EK) (predložena Uredba, prijedlog uredbe ili Uredba o e-privatnosti) [1], kojom se namjerava zamijeniti Direktiva o e-privatnosti (ePD)[2].

2. Predložena Uredba u brojnim je aspektima pozitivna i njezinim je uvođenjem Europska komisija poduzela važan korak. Međutim, ona se može dodatno poboljšati. Time bi se pridonijelo ne samo boljoj zaštiti krajnjih korisnika, nego bi se omogućilo i uvođenje veće pravne sigurnosti za sve uključene dionike.

3. Radna skupina stoga je utvrdila nekoliko problematičnih područja i donijela preporuke za pojašnjenja koje Europski parlament i Vijeće ministara trebaju riješiti u raspravi o predloženoj Uredbi. U ovom će se Mišljenju prvo razmotriti pozitivni aspekti predložene Uredbe, a potom istaknuti pitanja koja izazivaju zabrinutost te područja koja je potrebno pojasniti.

2. POZITIVNI ASPEKTI PREDLOŽENE UREDBE

USKLAĐIVANJE NA RAZINI EU-A, USKLAĐIVANJE NOVČANIH KAZNI TE PROVEDBA KOJU OSTVARUJU ISKLJUČIVO TIJELA ZA ZAŠTITU PODATAKA

4. Radna skupina pozdravlja **odabir uredbe kao regulatornog instrumenta**. Time se osiguravaju ujednačena pravila u cijelom EU-u (uz određena izuzeća o kojima se raspravlja u nastavku) te pruža jasnoća organizacijama i nadzornim tijelima. Osim toga, s obzirom na ključnu ulogu koju Opća uredba o zaštiti podataka (OUZP)[3] ima u predloženoj Uredbi, tim se izborom pridonosi usklađenosti između tih dvaju instrumenata. Istodobno, **odabir (zadržavanje) dopunskog pravnog instrumenta** pozitivna je odluka. Zaštita povjerljive komunikacijske i terminalne opreme ima posebne značajke koje nisu obuhvaćene OUZP-om. Stoga su potrebne dopunske odredbe o tim vrstama usluga kako bi se osigurala odgovarajuća zaštita tog temeljnog prava. U tom kontekstu Radna skupina **podržava i načelni pristup koji je odabran u predloženoj Uredbi, a uključuje opsežne zabrane i ograničena izuzeća** te

[1] Prijedlog uredbe Europskog parlamenta i Vijeća o poštovanju privatnog života i zaštiti osobnih podataka u elektroničkim komunikacijama te stavljanju izvan snage Direktive 2002/58/EZ (Uredba o privatnosti i elektroničkim komunikacijama), 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

[2] Direktiva 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), SL L 201, 31.7.2002., str. 37.–47., url: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:32002L0058.

[3] 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 (Opća uredba o zaštiti podataka), SL L 119/1, 4.5.2016., str. 1.–88., url: http://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX%3A32016R0679.

vjeruje da bi trebalo izbjegavati uvođenje neograničenih izuzeća u okviru članka 6. OUZP-a, a posebno članka 6. točke (f) OUZP-a (legitimni interes).

5. Usklađenosti između tih dvaju instrumenata dodatno pridonosi i odluka da **isto tijelo koje je odgovorno za praćenje usklađenosti s OUZP-om bude odgovorno i za provedbu navedenih pravila**. S obzirom na odnos između zaštite osobnih podataka i zaštite povjerljive komunikacijske i terminalne opreme, korisno je povjeriti izvršenje odredaba predložene Uredbe istom nadzornom tijelu koje izvršava OUZP (uvodna izjava 38. i članak 18. predložene Uredbe). Osim toga, sudskom praksom Suda Europske unije[4] potvrđeno je da je bitno da nadzorno tijelo bude neovisno, kako je propisano člankom 7. Povelje. Međutim, to bi na operativnoj razini rezultiralo znatnim dodatnim poslom za tijela za zaštitu podataka, čije izvršenje nije zajamčeno ako se ne dobiju dodatna sredstva. Tijela za zaštitu podataka stoga pozdravljaju uvodnu izjavu 38. predložene Uredbe, u kojoj se ističe da bi svakom nadzornom tijelu trebalo osigurati dodatne financijske i ljudske resurse, prostorije i infrastrukturu koji su potrebni za učinkovitu provedbu zadaća na temelju nove Uredbe. Pozdravlja se i činjenica da je člankom 18. stavkom 2. osigurana pravna osnova za suradnju između nadzornih tijela iz predložene Uredbe i nacionalnih regulatornih tijela iz predložene Direktive o Europskom zakoniku elektroničkih komunikacija („EECC")[5].

6. Budući da su predložena Uredba i OUZP usko povezani, pozdravlja se i **usklađivanje novčanih kazni predviđenih predloženom Uredbom s onima iz OUZP-a.** Aktivnosti koje su obuhvaćene područjem primjene predložene Uredbe vrlo su osjetljive i, među ostalim, uključuju zadiranje u povjerljivu komunikacijsku i terminalnu opremu. Visina novčanih kazni trebala bi biti razmjerna tom osjetljivom kontekstu. Zbog tog je konteksta važno i usklađivanje na razini EU-a kako bi se osigurala ista visoka razina zaštite u cijeloj regiji. Člankom 23. predložene Uredbe predviđaju se učinkovite novčane kazne za povrede Uredbe čija je visina slična visini novčanih kazni utvrđenih za povredu pravila iz OUZP-a, osim u nekim slučajevima (vidjeti točku 38.).

7. Treba pozdraviti i to da su iz ovog propisa **uklonjena pravila o posebnom obavješćivanju o povredi podataka** kako bi se spriječilo nepotrebno preklapanje sa zahtjevima u pogledu povrede podataka iz OUZP-a.

8. Isto se tako **pozdravlja i to što je pozornost usmjerena na pružanje jednake razine zaštite svim krajnjim korisnicima**, jer je iz predložene Uredbe izostavljeno razlikovanje „pretplatnika" i ostalih korisnika elektroničkih komunikacijskih usluga.

PROŠIRENJE PODRUČJA PRIMJENE U USPOREDBI S DIREKTIVOM O E-PRIVATNOSTI

[4] Vidjeti npr. točku 41. presude Suda od 6. listopada 2015. u predmetu C-362/14 (*sigurna luka*), i točku 123. presude Suda od 21. prosinca 2016. u predmetima C-203/15 i C-698/15 (*Tele2/Watson*).

[5] Prijedlog direktive Europskog parlamenta i Vijeća o Europskom zakoniku elektroničkih komunikacija (preinačeno) 2016/0288 (COD), 12.10.2016., url: http://eur-lex.europa.eu/legal-content/HR/ALL/?uri=comnat:COM_2016_0590_FIN.

9. Radna skupina pozdravlja **proširenje područja primjene predložene Uredbe radi uključivanja pružatelja OTT usluga**, tj. usluga koje su funkcionalno istovjetne tradicionalnijim sredstvima komunikacije te stoga mogu na sličan način utjecati na privatnost i pravo na tajnost komunikacija građana EU-a. Radna skupina posebno pozdravlja to što su sada sve OTT kategorije (OTT0, OTT1 i neki OTT2)[6] obuhvaćene područjem primjene Uredbe, jer ona ne obuhvaća samo tradicionalna sredstva komunikacije (OTT0), nego i funkcionalno istovjetne usluge (OTT1) kako je navedeno u članku 8. stavku 1. točki (c) predložene Uredbe. Pozitivno je i to što su, uz definicije na temelju EECC-a, uključeni i neki OTT2 kada omogućuju pomoćnu interpersonalnu i interaktivnu komunikaciju koja je neraskidivo povezana s njihovom uslugom, kao što su igre, aplikacije za dogovaranje ljubavnih sastanaka ili *web*-mjesta za recenzije (članak 4. stavak 2. predložene Uredbe). Slično tomu, pozdravlja se i **pojašnjenje da zaštita obuhvaća i interakciju između strojeva.** U uvodnoj izjavi 12. jasno se navodi da su uređaji koji međusobno komuniciraju obuhvaćeni područjem primjene zaštite koja se pruža predloženom Uredbom. To je poželjno jer takve komunikacije često sadržavaju informacije koje su zaštićene pravima na privatnost. Međutim, primjenjivost bi se mogla pojasniti (vidjeti točku 40. podtočku (h)).

10. Pozitivno je i to što **predložena Uredba jasno obuhvaća sadržaj i povezane metapodatke.** U uvodnoj izjavi 14. jasno se navodi da je definicija za „elektroničke komunikacijske podatke" iz članka 4. stavka 3. točke (a) predviđena da bude dovoljno široka da obuhvati *sav* sadržaj i povezane metapodatke, bez obzira na, na primjer, način prijenosa signala. Međutim, u točki 39. Radna skupina napominje da zabrinjava to što je trenutačna definicija za „elektroničke komunikacijske podatke" još uvijek predmet rasprave. U skladu s navedenim proširenjem područja primjene, Radna skupina smatra da je ključan dodatak to što se **priznaje da se na temelju metapodataka mogu otkriti vrlo osjetljivi podaci** (vidjeti stavak 2.2. Obrazloženja; uvodna izjava 2.). Radna skupina pozdravlja činjenicu da je Europska komisija time uzela u obzir razmatranja Suda Europske unije u predmetima *Digital Rights Ireland* i *Tele2/Watson*. Radna skupina iz članka 29. isto tako cijeni to što **se priznaje da je analiza sadržaja visokorizična obrada podataka**. Uvodnom izjavom 19. i člankom 6. stavkom 3. točkom (b) utvrđuje se logična pravna pretpostavka da je pregledavanje sadržaja visokorizična obrada podataka na temelju članka 35. OUZP-a te da, očito bez obzira na postojanje rezidualnog visokog rizika, zahtijeva prethodno savjetovanje s (vodećim) tijelom za zaštitu podataka. Istodobno, Radna skupina izražava zabrinutost u pogledu područja primjene definicije „metapodataka" i činjenice da analiza metapodataka ne podliježe istom obveznom zahtjevu za provođenje procjene učinka na zaštitu podataka (vidjeti točke 33. i 46.).

[6] Za dodatno objašnjenje ovih pojmova vidjeti BEREC, *Izvješće o OTT uslugama*, BoR (16) 35, 29. siječnja 2016., str. 15. i 16., url: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. Vidjeti i napomenu u izvješću u kojoj se navodi da su kategorije pojmovi koji su predviđeni za upotrebu u raspravi o reviziji i nisu pravni pojmovi.

11. Pozdravlja se i kontinuirano **priznavanje važnosti anonimizacije.** Već u Direktivi o e-privatnosti mjere anonimizacije imale su ulogu u osiguravanju usklađenosti (na primjer članak 6. stavak 1. Direktive o e-privatnosti u kojem se navodi da se podaci o prometu moraju izbrisati ili učiniti anonimnima kada više nisu potrebni u svrhu prijenosa komunikacije). Člankom 6. stavkom 2. točkom (c) i člankom 6. stavkom 3. točkom (b) predložene Uredbe dopušta se izuzeće od zabrane obrade metapodataka i sadržaja na temelju privole, pod uvjetom da se predmetna svrha ili predmetne svrhe „*ne mogu ispuniti obradom informacija koje su anonimizirane*". Propisivanjem takvih mjera zaštite privatnosti i traženjem privole korisnika te se korisnike štiti od neopravdane obrade. Međutim, Radnu skupinu istodobno ozbiljno zabrinjava to što se uvođenje takvih tehnika anonimizacije ne zahtijeva pri praćenju lokacije korisnika preko njihove mobilne opreme (vidjeti točku 17.). Osim toga, čak i kad se primjenjuju mjere anonimizacije, pružatelji usluga trebali bi uvijek provesti procjenu učinka na zaštitu podataka (DPIA) (vidjeti točke 33. i 46.), a Radna skupina poziva na uvođenje dodatne obveze javnog objavljivanja načina na koji se podaci anonimiziraju i agregiraju (vidjeti točku 42. pod (b)).

12. Pozitivna je i **široka formulacija zaštite terminalne opreme**. U uvodnoj izjavi 20. i članku 8. utvrđuje se da tehnologije koje se upotrebljavaju za pristup terminalnoj opremi nisu relevantne: za svako zadiranje u terminalnu opremu, uključujući upotrebu njezina kapaciteta za obradu, potrebna je privola krajnjeg korisnika (uz određena izuzeća). EK je sada korisno potvrdio da je tom odredbom obuhvaćeno i prikupljanje informacija o uređaju u svrhu njegove identifikacije i praćenja (eng. *device fingerprinting*). Osim toga, Radna skupina pozdravlja to da su odabiri koje je pojedinac definirao **postavkama preglednika izvršivi** u pogledu treće osobe koja se ne pridržava tih izbora, kako je opisano u uvodnoj izjavi 22. To je korisno za situacije kada treća strana (npr. oglašivačka mreža) ne poštuje te postavke. Međutim, to bi trebalo utvrditi i u relevantnoj odredbi predložene Uredbe.

13. Konačno, treba pozdraviti i kontinuirano **uključivanje pravnih osoba u područje primjene predložene Uredbe** (vidjeti stavak 2.2. Obrazloženja; uvodne izjave 3., 33. i 42.; članak 1., članak 15. i članak 16. stavak 5.). To je već učinjeno u slučaju Direktive o e-privatnosti, ali s obzirom na to da će tijela za zaštitu podataka biti zadužena za izvršavanje novih pravila, korisno je to posebno naglasiti. Time se tijelima za zaštitu podataka omogućuje da poduzmu mjere u slučajevima kada su pravne osobe žrtve povrede pravila, na primjer kad korporacije primaju neželjene elektroničke poruke ili kad se njihove komunikacije prikriveno prate. Međutim, za Radnu je skupinu zabrinjavajuće i to što primjena privole na pravne osobe nije jasna (vidjeti točku 41. podtočku (a) te nije jasno što se misli pod „legitimnim interesom" pravnih osoba u slučaju izravnog marketinga (vidjeti točku 43. podtočku (c)).

CILJANA PRIMJENA POJMA PRIVOLE

14. Radna skupina pozdravlja i poboljšanja povezana s primjenom i tumačenjem pojma privole. Prvo, pozdravlja se **pojašnjenje da su pristup internetu i (mobilna) telefonija bitne usluge te pružatelji tih usluga ne mogu „prisiliti" svoje potrošače na davanje privole za obradu podataka koja nije nužna za pružanje same bitne usluge**. Posebno se u uvodnoj izjavi 18. navodi da se osnovne usluge širokopojasnog pristupa internetu i govorne komunikacije trebaju smatrati bitnim uslugama, što znači, s obzirom na ovisnost ljudi o pristupu tim uslugama, da privola za obradu njihovih komunikacijskih podataka za dodatne svrhe (npr. obrada u svrhe oglašavanja ili marketinga) ne može biti valjana. Istodobno je za Radnu skupnu zabrinjavajuće to što je navedeno pojašnjenje previše ograničeno. Usluge određenih pružatelja OTT usluga mogu se također smatrati bitnim uslugama pa bi Uredbom o e-privatnosti trebalo izričito zabraniti opcije „uzmi ili ostavi" u drugim okolnostima (vidjeti točku 20.).

15. Osim toga, pozitivno je i to što je **usklađen zahtjev u pogledu privole za uvrštavanje osobnih podataka fizičkih osoba u imenike**. Na temelju članka 15. predložene Uredbe obrada podataka iz javno dostupnih imenika dopuštena je samo ako su fizičke osobe dale privolu ili ako pravne osobe imaju mogućnost uložiti prigovor. To je dodatno objašnjeno u uvodnoj izjavi 31., u kojoj se navodi da je za posebne kategorije osobnih podataka koje se namjerava uvrstiti u imenik potrebna posebna privola. Međutim, Radna skupina napominje da je jedno od problematičnih pitanja i to što bi se u predloženoj Uredbi moglo jasnije utvrditi da je za pretraživanje i obrnuto pretraživanje potrebna posebna, odvojena privola (vidjeti točku 37.).

16. Cijeni se i uvođenje **novog ciljanog izuzeća za zadiranje u terminalnu opremu kojim se ne narušava privatnost**. Radna skupina iz članka 29. smatra korisnim to što se u predloženoj Uredbi pojašnjava da se zabrana ne primjenjuje na mjerenje internetskog prometa (pod uvjetom da takvo mjerenje provodi pružatelj usluge informacijskog društva koju je zatražio krajnji korisnik, usp. članak 8. stavak 1. točku (d) predložene Uredbe). Vidjeti i uvodnu izjavu 21. Radna skupina međutim predlaže da se upotrijebi tehnološki neutralnija definicija te pojasni primjenjivost navedenog uvjeta (vidjeti točku 25.).

3. PITANJA KOJA IZAZIVAJU OZBILJNU ZABRINUTOST

ZAŠTITA NA TEMELJU OUZP-A NARUŠENA JE PREDLOŽENOM UREDBOM

Kako je prethodno navedeno, predloženom se Uredbom uvodi niz ključnih poboljšanja. Postoje međutim i pitanja koja izazivaju zabrinutost različitog stupnja ozbiljnosti. U ovom odjeljku Radna skupina raspravlja o četiri problema zbog kojih je **duboko zabrinuta**. To su odredbe kojima se **narušava razina zaštite koja se pruža OUZP-om**:

17. **Obveze koje su Uredbom propisane u pogledu praćenja lokacije terminalne opreme trebale bi biti usklađene sa zahtjevima iz OUZP-a**. Kad je riječ o prikupljanju informacija koje odašilje terminalna oprema, člankom 8. stavkom 2. točkom (b) predložene Uredbe propisuje se samo obveza isticanja obavijesti i provedbe sigurnosnih mjera. U istom članku 8. stavku 2. točki (b) dalje se navodi da osoba koja je odgovorna za prikupljanje tih informacija mora navesti sve mjere koje krajnji korisnici mogu poduzeti kako bi smanjili ili zaustavili prikupljanje. Time članak 8. stavak 2. točka (b) ostavlja dojam da organizacije mogu prikupljati informacije koje odašilje terminalna oprema kako bi pratile fizičko kretanje pojedinaca (kao što su praćenje putem mreže WiFi ili praćenje putem Bluetootha) bez privole predmetnog pojedinca. Očito je da bi stranka koja prikuplja te podatke mogla ispuniti navedenu obvezu s pomoću obavijesti u kojoj krajnje korisnike obavješćuje da isključe svoje uređaje ako ne žele da ih se prati. Takav bi pristup bio suprotan temeljnom cilju telekomunikacijske politike Europske komisije, a to je prekogranično pružanje vrlo brze mobilne internetske veze uz strogu zaštitu privatnosti i niske troškove za sve Europljane.

Osim toga, predloženom se Uredbom ne uvode jasna ograničenja u pogledu opsega prikupljanja podataka i njihove kasnije obrade. U tom bi kontekstu trebalo napomenuti da su MAC adrese osobni podaci, čak i nakon primjene sigurnosnih mjera kao što je sažimanje (eng. *hashing*). Zbog neuvođenja dodatnih zahtjeva ili ograničenja razina zaštite tih osobnih podataka na temelju predložene Uredbe znatno je smanjena u odnosu na onu iz OUZP-a, prema kojoj bi takvo praćenje moralo biti pošteno, zakonito i transparentno. U uvodnoj izjavi 25. nepotrebno se navodi da neke funkcionalnosti praćenja putem mreže WiFi ne podrazumijevaju visoke rizike za privatnost, dok druge – kao što je praćenje pojedinaca tijekom vremena – to podrazumijevaju. Iako Radna skupina cijeni priznanje da su u potonjem slučaju prisutni visoki rizici za privatnost, nije korisno unaprijed odlučiti, bez dodatne procjene okolnosti i proporcionalnosti obrade podataka, da kod nekih drugih funkcionalnosti ti rizici ne postoje. Navedenu bi procjenu trebalo provesti uzimajući u obzir sljedeće uvjete u pogledu neanonimiziranog praćenja putem mreže WiFi.

Ovisno o okolnostima i svrhama prikupljanja podataka, u skladu s OUZP-om za takvo će praćenje vjerojatno biti potrebna privola ili će se moći provoditi samo ako se prikupljeni osobni podaci anonimiziraju. Poželjno je da se anonimizacija izvrši odmah nakon prikupljanja. Ako anonimizaciju nije moguće odmah izvršiti s obzirom na svrhe u koje su podaci prikupljeni, ti se podaci mogu obraditi u razdoblju dok nisu anonimizirani jedino pod sljedećim uvjetima: i. svrha prikupljanja podataka mora biti ograničena na puko statističko brojanje (vidjeti primjere u nastavku), ii. praćenje je ograničeno vremenski i prostorno koliko je nužno potrebno za tu svrhu, iii. podaci se odmah potom brišu ili anonimiziraju te iv. mora postojati učinkovita mogućnost izuzeća. U svim okolnostima voditelji obrade moraju ispuniti obvezu pružanja odgovarajućih informacija.

Radna skupina izražava zabrinutost zbog toga što bi moguća ponuda pojedinačnog izuzeća po organizaciji koja prikuplja te podatke predstavljala neprihvatljivo opterećenje za građane s obzirom na povećanje upotrebe takvih tehnologija praćenja od strane organizacija kako iz privatnog tako i javnog sektora. Stoga Radna skupina

poziva europskog zakonodavca da promiče razvoj tehničkih standarda za uređaje kako bi automatski signalizirali prigovor na takvo praćenje te da osigura provedivost obveze pridržavanja takvog signala.

Primjerice, na temelju OUZP-a privola bi vjerojatno bila potrebna ako voditelj obrade podataka prikuplja i pohranjuje MAC adrese uređaja (WiFi ili Bluetooth) koje se neizravno mogu prepoznati te izračunava lokaciju korisnika kako bi pratio korisnikovu lokaciju tijekom vremena, na primjer u većem broju prodavaonica. To je posebno slučaj kada se tako praćenje provodi na javnim mjestima na kojima korisnici imaju legitimna očekivanja da neće biti identificirani ili praćeni, ali gdje se ipak prikupljaju MAC adrese prolaznika. Takva se privola može dobiti, na primjer, s pomoću aplikacije kojom se korisnike poziva da dopuste praćenje njihove lokacije u određenim prostorima u zamjenu za komercijalne ponude ili tako da se unutar posebnih lokacija ponude prijavna mjesta ili s pomoću modula privole na javnim WiFi pristupnim točkama.

Samo bi se u ograničenom broju okolnosti voditeljima obrade podataka moglo dopustiti da informacije koje odašilje terminalna oprema obrađuju radi praćenja njihova fizičkog kretanja bez privole predmetnog pojedinca. To bi, na primjer, mogao biti slučaj kada se broje kupci unutar određene lokacije ili kada se prikupljaju odašiljani podaci na obje strane sigurnosne kontrolne točke kako bi se prikazalo vrijeme čekanja. Međutim, u oba primjera podaci bi se trebali izbrisati ili anonimizirati čim se ispuni statistička svrha. To znači da se MAC adrese uređaja posjetitelja unutar određene lokacije, kao što je prodavaonica, moraju anonimizirati odmah nakon prikupljanja, bez ikakvog trajnog pohranjivanja MAC adresa, i to tako da je tehnički isključena mogućnost njihova ponovnog prepoznavanja. U slučaju izračunavanja vremena čekanja, MAC adrese morale bi se izbrisati ili anonimizirati čim podaci nisu više relevantni za izračunavanje vremena čekanja (jer je posjetitelj stigao na drugu stranu sigurnosne kontrolne točke ili je napustio red).
Osim toga, voditelj obrade podataka morao bi ispunjavati zahtjeve u pogledu smanjenja količine podataka (na primjer, ne pratiti 24 sata na dan, sedam dana u tjednu ako je svrha ograničena na radno vrijeme prodavaonica i/ili uzorkovati u određenim vremenskim razmacima). Voditelji obrade podataka moraju poduzeti i ostale mjere za ublažavanje rizika kako bi osigurali da utjecaj na prava na privatnost korisnika bude neznatan ili da ga uopće nema, na primjer zaštititi privatnost ljudi koji žive u blizini točke prikupljanja.

Zahtjev da je potrebno samo istaknuti obavijest, kako je predviđeno člankom 8. stavkom 2., još više začuđuje s obzirom na zaključak u uvodnoj izjavi 20. da se informacije povezane s uređajem krajnjeg korisnika mogu prikupljati i daljinski u svrhu identifikacije i praćenja te da se takvom obradom – u skladu s predloženom Uredbom – može ozbiljno zadrijeti u privatnost tih krajnjih korisnika. Osim toga, navedena obveza nije šira od obveze obavješćivanja koja je već predviđena člancima 13. i 14. OUZP-a. Problem ozbiljnog narušavanja privatnosti zbog praćenja dodatno pogoršava mogući pristup drugih osoba prikupljenim podacima, kao što je mogućnost da tijela za izvršavanje zakonodavstva identificiraju krajnje korisnike na temelju pohranjenih MAC adresa koje su emitirali njihovi mobilni uređaji.

18. **Moraju se razraditi uvjeti pod kojima je dopuštena analiza sadržaja i metapodataka.**

Člankom 6. predložene Uredbe predviđaju se različite razine zaštite metapodataka i sadržaja. Radna skupina iz članka 29. ne podržava takvo razlikovanje: obje su kategorije podatka vrlo osjetljive te bi stoga za metapodatke i sadržaj trebalo predvidjeti istu razinu zaštite. Polazište bi trebalo biti u tome da je zabranjena obrada metapodataka i sadržaja bez privole svih krajnjih korisnika (tj. pošiljatelja i primatelja).

Međutim, ovisno o svrhama, određena se obrada može dopustiti i bez privole ako je nužno potrebna za te svrhe:

- Pružatelji usluga mogu obrađivati elektroničke komunikacijske podatke u svrhe navedene u članku 6. stavku 1. točkama (a) i (b) te članku 6. stavku 2. točkama (a) i (b) predložene Uredbe[7].
- Trebalo bi pojasniti da se i neke tehnike otkrivanja/filtriranja neželjenih elektroničkih poruka i ublažavanja botneta mogu smatrati nužnima za otkrivanje ili zaustavljanje zlouporabe elektroničkih komunikacijskih usluga (članak 6. stavak 2. točka (b)). Kad je riječ o filtriranju neželjenih elektroničkih poruka, korisnicima koji primaju takve poruke trebalo bi ponuditi, ako je to tehnički moguće, precizno definirane mogućnosti izuzeća.
- Trebalo bi pojasniti da i analiza elektroničkih komunikacijskih podataka u svrhe pružanja usluga korisnicima može biti obuhvaćena izuzećem „ako je to nužno za naplatu" (usp. članak 6. stavak 2. točka (b)). Relevantni metapodaci mogu se čuvati do kraja razdoblja u kojemu se može zakonito osporiti račun ili izvršiti plaćanje u skladu s nacionalnim pravom. Relevantni podaci (kao što su URL adrese) mogu se zadržati samo na zahtjev krajnjeg korisnika, a i tada samo onoliko dugo koliko je nužno potrebno za rješavanje spora u pogledu računa (što znači da bi članak 7. stavak 3. trebalo dopuniti).
- Trebalo bi omogućiti obradu elektroničkih komunikacijskih podataka u svrhe pružanja usluga koje je izričito zatražio krajnji korisnik, kao što su funkcija pretraživanja i indeksiranja, virtualni pomoćnici, program za pretvaranje teksta u govor i usluge prevođenja. To zahtijeva uvođenje izuzeća za analizu takvih podataka za isključivo osobnu (kućnu) upotrebu, kao i za osobnu upotrebu povezanu s poslom[8]. Ta bi analiza dakle bila moguća bez privole svih krajnjih korisnika, ali bi se mogla izvršiti samo ako je privolu dao krajnji

[7] Kad je riječ o potrebnom ispunjavanju obveznih zahtjeva u pogledu kvalitete usluga, kako je navedeno u članku 6. stavku 2. točki (a) predložene Uredbe, pružatelji usluga trebali bi uzeti u obzir uvjete opisane u Uredbi (EU) 15/2120 (EECS), a posebno u njezinu članku 3., uvodnoj izjavi 10. i uvodnim izjavama od 13. do 15. Na temelju te odredbe, od pružatelja usluga može se zahtijevati da obrađuju komunikacijske podatke radi otkrivanja zlonamjernog ili špijunskog softvera te im se može dopustiti komprimiranje podataka.

[8] Iako su uvodnom izjavom 13. predložene Uredbe korporativne mreže izričito isključene iz područja primjene Uredbe, tim bi se novim izuzećem koje se odnosi na pojedinačnu upotrebu riješilo i pitanje usluga u oblaku koje zaposlenici upotrebljavaju u svrhe povezane s poslom, kao što je pretraživanje njihove elektroničke pošte.

korisnik koji je zatražio predmetnu uslugu. Takva posebna privola spriječila bi pružatelja usluge da se koristi tim podacima u druge svrhe.

To znači da je za analizu sadržaja i/ili metapodataka za sve ostale svrhe, kao što su analitika, izrada profila, bihevioralno oglašavanje ili druge svrhe u (komercijalnu) korist pružatelja usluge, potrebna privola svih krajnjih korisnika čiji bi se podaci obrađivali. U pogledu takvih situacija, u predloženoj Uredbi trebalo bi objasniti da sam čin slanja elektroničke pošte ili druga vrsta osobne komunikacije od druge usluge prema krajnjem korisniku koji je osobno dao privolu na obradu njegova sadržaja ili metapodataka (na primjer tijekom registriranja za korištenje uslugom slanja pošte), ne predstavlja valjanu privolu pošiljatelja.

Konačno, trebalo bi pojasniti da obrada podataka osoba koje nisu krajnji korisnici (npr. slika ili opis treće osobe u okviru razmjene informacija između dvoje ljudi) treba isto tako biti u skladu sa svim relevantnim odredbama OUZP-a

19. **Terminalna oprema i softver moraju *imati zadane postavke* kojima se obeshrabruje, sprečava i zabranjuje nezakonito zadiranje u njih te pružati informacije o mogućnostima koje se nude**. Iako se predloženom Uredbom pružatelje softvera za elektroničke komunikacije obvezuje da „ponude mogućnost" sprečavanja ograničenog oblika zadiranja u terminalnu opremu te da, nakon instalacije softvera, zahtijevaju od krajnjeg korisnika privolu za postavke (članak 10. stavci 1. i 2.), takav odabir nije istovjetan *integriranoj zaštiti privatnosti*. Osim toga, „mogućnost" sprečavanja određenog zadiranja već postoji, ali do sada se njome nije uspjelo u dovoljnoj mjeri riješiti problem neopravdanog praćenja. Upravo je zbog toga u okviru OUZP-a svjesno donesena odluka politike da se uvedu načela tehničke i integrirane zaštite podataka i privatnosti (članak 25. OUZP-a). Predloženom se Uredbom ta načela narušavaju u pogledu podataka iz komunikacija iz uređaja. Istodobno se Direktivom 2014/53/EU o radijskoj opremi[9] (koja se spominje u uvodnoj izjavi 10.) predviđa jedino vrlo ograničena sigurnosna obveza kojom se zahtijeva da radijska oprema ima ugrađene „zaštitne mehanizme radi osiguranja zaštite osobnih podataka te privatnosti korisnika i pretplatnika" (članak 3. stavak 3. točka (e)). To ne može zamijeniti posebne zadane postavke za zaštitu privatnosti koje su predviđene predloženom Uredbom. U tom pogledu vrijedi napomenuti da se u anketi Eurobarometra o e-privatnosti koja je objavljena u prosincu 2016. navodi da se „[g]otovo sedam od deset osoba (69 %) u potpunosti slaže da bi zadanim postavkama preglednika trebalo zaustaviti dijeljenje njihovih informacija"[10]. Radna skupina izražava posebnu zabrinutost u pogledu postavki preglednika i definicije „trećih strana". Vidjeti točku 24. Osim toga, trebalo bi imati na umu da se ta odredba ne odnosi samo na preglednike koji se upotrebljavaju u računalima, nego obuhvaća i druge vrste softvera koje omogućuju komunikaciju (uključujući operativne sustave, aplikacije i softverska sučelja za uređaje spojene na internet stvari). Naposljetku, terminalna oprema i softver moraju imati *integrirane* postavke za zaštitu privatnosti

[9] Direktiva 2014/53/EU o radijskoj opremi.

[10] Vidjeti Flash Eurobarometer 443, Izvješće o e-privatnosti (objavljeno u prosincu 2016.), str. 5.

te u konfiguracijskom izborniku nuditi korisniku mogućnosti odstupanja od tih zadanih postavki nakon instaliranja. Konfiguracijski izbornik mora uvijek biti lako dostupan tijekom upotrebe. Radna skupina potiče europskog zakonodavca da u tom smislu pojasni područje primjene članka 10.

20. **Uredbom o e-privatnosti trebali bi se izričito zabraniti „zidovi za praćenje"**, tj. praksa odbijanja pristupa *web*-mjestu ili usluzi ako pojedinac ne pristane da bude praćen na drugim *web*-mjestima ili uslugama. Kako je već navedeno u prethodnim mišljenjima Radne skupine o Direktivi o e-privatnosti[11], takvi pristupi „uzmi ili ostavi" rijetko su zakoniti[12]. Kada upotreba kapaciteta terminalne opreme za obradu ili pohranu ili prikupljanje informacija koje odašilje terminalna oprema korisnika omogućuju praćenje aktivnosti korisnika tijekom vremena ili u nekoliko usluga (npr. različitih *web*-mjesta ili aplikacija), takvim se aktivnostima obrade može ozbiljno zadrijeti u privatnost tih korisnika. S obzirom na veliku važnost koju internet ima u omogućavanju ostvarivanja temeljnog prava na slobodu izražavanja, uključujući pravo na pristup informacijama, mogućnost pojedinaca da pristupe sadržaju putem interneta ne smije ovisiti o pristajanju na praćenje aktivnosti na uređajima i *web*-mjestima/aplikacijama. U budućoj uredbi o e-privatnosti trebalo bi stoga utvrditi da se pristup sadržajima na, na primjer, *web*-mjestima ili aplikacijama ne smije uvjetovati pristajanjem na aktivnosti obrade kojima se narušava privatnost, bez obzira na primijenjenu tehnologiju praćenja, kao što su kolačići, prikupljanje informacija o uređaju u svrhu njegove identifikacije i praćenja (eng. *device fingerprinting*), ubacivanje jedinstvenih identifikatora ili druge tehnike praćenja. Na nužnost takve zabrane ukazuje i nedavna Eurobarometrova anketa o e-privatnosti u kojoj su „[g]otovo dvije trećine ispitanika navele da je neprihvatljivo da im se aktivnosti na internetu prate u zamjenu za neograničen pristup određenom *web*-mjestu (64 %)".

21. Ukratko, u pogledu četiri prethodno navedene točke, **predložena Uredba trebala bi ispuniti svoju svrhu i osigurati razinu zaštite koja je jednaka onoj iz OUZP-a ili veća od nje**. U uvodnoj izjavi 5. izravno se navodi da se predloženom Uredbom ne smanjuje razina zaštite koja se pruža na temelju OUZP-a. Međutim, prema trenutačnoj verziji predložene Uredbe to nije točno, posebno kad je riječ o praćenju uređaja (točka 17.), nedostatku načela integrirane zaštite privatnosti (točka 19.) te privoli (točka 18.). To je posebno važno jer se u istoj uvodnoj izjavi navodi da će predložena Uredba biti *lex specialis* u odnosu na GDPR te će se [njome] preciznije utvrditi i dopuniti GDPR u pogledu elektroničkih komunikacijskih podataka koji se smatraju osobnim podacima". Radna skupina predlaže da se, kao minimum, u tekstu Uredbe o e-privatnosti pojasni da

    i. zabrane iz Uredbe o e-privatnosti imaju prednost nad dopuštenjima iz OUZP-a (npr. zabrana zadiranja u podatke na temelju članka 5. Uredbe o e-privatnosti ima prednost nad pravima pružatelja elektroničkih komunikacijskih usluga na daljnju obradu podataka na temelju članka 5. stavka 1. točke (b) i članka 6. stavka 4. OUZP-a);

[11] Vidjeti npr. WP240 (preispitivanje e-privatnosti), str. 16.; WP 208 (izuzeće za privolu za kolačiće), str. 5.

[12] Ovim se stajalištem ne dovodi u pitanje članak 7. stavak 4. OUZP-a, kojim se mogu spriječiti odluke „uzmi ili ostavi" u drugim situacijama u kojima je to primjereno.

ii. ako je obrada dopuštena na temelju bilo kojeg izuzeća (uključujući privolu) od zabrana na temelju Uredbe o e-privatnosti, ta obrada, ako se odnosi na osobne podatke, mora ipak biti u skladu sa svim relevantnim odredbama OUZP-a;

iii. ako je obrada dopuštena na temelju bilo kojeg izuzeća od zabrana na temelju Uredbe o e-privatnosti, zabranjena je svaka druga obrada na temelju OUZP-a, uključujući obradu za drugu svrhu na temelju članka 6. stavka 4. OUZP-a. To ne bi sprečavalo voditelje obrade da traže dodatnu privolu za nove postupke obrade. Ne bi sprečavalo ni zakonodavce da propišu dodatna, ograničena i posebna izuzeća u Uredbi o e-privatnosti, na primjer, da dopuste obradu u znanstvene ili statističke svrhe na temelju članka 89. OUZP-a ili u svrhu zaštite „ključnih interesa" pojedinaca u skladu s člankom 6. točkom (d) OUZP-a.

Osim toga, Uredbu o e-privatnosti trebalo bi tumačiti tako da se osigura da pruža barem istu razinu zaštite kao i OUZP, a prema potrebi i veću.

4. OSTALA PITANJA KOJA IZAZIVAJU ZABRINUTOST

Uz prethodno navedena pitanja, Radna skupina iz članka 29. **izražava zabrinutost** i zbog sljedećega.

POTREBNO JE PROŠIRITI TERITORIJALNO I MATERIJALNO PODRUČJE PRIMJENE

22. **Pojam „metapodaci" preusko je definiran**. Definiran je u članku 4. točki (c) kao „podaci koji su obrađeni u elektroničkoj komunikacijskoj mreži u svrhe prijenosa, distribucije ili razmjene sadržaja elektroničkih komunikacija" (podcrtavanje je dodano). Čini se da upotreba riječi „mreže" upućuje na to da bi se jedino podaci koji su generirani tijekom pružanja usluge u „nižem" sloju mreže mogli smatrati metapodacima. To bi moglo značiti da se iz tog područja primjene izuzimaju podaci generirani tijekom pružanja OTT usluge. To bi bilo nepoželjno, a vjerojatno to i nije bila namjera s obzirom na predviđeno proširenje područja primjene predložene Uredbe na pružatelje OTT usluga. Da bi se taj problem riješio, definiciju za „elektroničke komunikacijske podatke" trebalo bi izmijeniti tako da obuhvati sve podatke koji se obrađuju u svrhe prijenosa, distribucije ili razmjene sadržaja elektroničkih komunikacija.

23. Osim toga, problematično je i to što su **u pogledu organizacija koje nemaju poslovni nastan u EU-u teritorijalnim područjem primjene predložene Uredbe obuhvaćeni samo pružatelji elektroničkih komunikacijskih usluga**. Na temelju predložene Uredbe pružatelj elektroničke komunikacijske usluge koji nema poslovni nastan u EU-u mora pisanim putem imenovati predstavnika u Uniji (članak 3. stavak 2.). U uvodnoj izjavi 9. navodi se da bi Uredbu trebalo primjenjivati na obradu koju provode pružatelji elektroničkih komunikacijskih usluga bez obzira na to gdje se obrada provodi. Radna skupina pozdravlja to pojašnjenje. Međutim, s obzirom na to da se u tekstu navode samo pružatelji elektroničkih komunikacijskih usluga, nejasno je u kojoj su mjeri tim teritorijalnim područjem obuhvaćene ostale vrste stranaka (na primjer, stranke koje zadiru u informacije što ih odašilje terminalna oprema krajnjih

korisnika ili koje prikupljaju takve informacije, usp. članak 3. stavak 1. točku (c) i članak 8. predložene Uredbe). Stoga Radna skupina predlaže da se članak 3. stavak 2. i članak 3. stavak 5. izmijene kako bi obuhvatili i pružatelje javno dostupnih imenika, pružatelje softvera za elektroničke komunikacije te osobe koje šalju izravne marketinške komercijalne komunikacije ili prikupljaju (ostale) informacije povezane s terminalnom opremom krajnjih korisnika ili informacije pohranjene na takvoj opremi, kad god su njihove aktivnosti usmjerene na korisnike u EU-u (usp. uvodnu izjavu 8. predložene Uredbe)[13].

POTREBNO JE POJAČATI ZAŠTITU TERMINALNE OPREME

Problematično pitanje je i nedovoljna zaštita terminalne opreme u predloženoj Uredbi.

24. Prvo, **iz predložene Uredbe pogrešno proizlazi da se valjana privola može dati s pomoću općih postavki preglednika.** Radna skupina slaže se s prosudbom da su krajnji korisnici trenutačno prezasićeni zahtjevima za davanje privole (uvodna izjava 22.). Postavke preglednika (i usporedivog softvera) imaju važnu ulogu u rješavanju ovog problema. Međutim, s obzirom na to da opće postavke preglednika nisu predviđene za primjenu tehnologije praćenja u jednom pojedinačnom slučaju, nisu prikladne za davanje privole u skladu s člankom 7. i uvodnom izjavom 32. OUZP-a (jer privola nije dovoljno informirana i specifična).
Krajnji korisnik mora biti u mogućnosti za svako *web*-mjesto ili aplikaciju dati zasebnu privolu za praćenje u različite svrhe (kao što su dijeljenje na društvenim medijima ili oglašavanje). Voditelj obrade podataka koji je odgovoran za više *web*-mjesta ili aplikacija može zatražiti privolu i za sva ostala *web*-mjesta ili aplikacije koje su pod njegovom kontrolom, pod uvjetom da taj zahtjev za davanje privole bude zaseban.
Osim toga, voditelj obrade mora ispuniti sve ostale obveze u pogledu privole, uključujući obvezu pružanja odgovarajućih informacija korisnicima. To znači, kako za preglednike tako i za voditelje obrade podataka, da bi bilo nevaljano kad bi nudili jedino opciju „Prihvati sve kolačiće" jer tako ne bi omogućili korisnicima davanje potrebne precizno definirane privole. Međutim, preglednici bi trebali omogućivati korisnicima donošenje informirane i svjesne odluke o prihvaćanju svih kolačića kako bi spriječili sve buduće zahtjeve za davanje privole s *web*-mjesta koja budu posjećivali.
Radna skupina snažno preporučuje da se Uredbom o e-privatnosti za preglednike propiše obveza primjene tehničkih mehanizama, kao što je standard „Ne prati", kako

[13] Vidjeti članak 3. stavak 2. OUZP-a: *Ova se Uredba primjenjuje na obradu osobnih podataka ispitanikâ u Uniji koju obavlja voditelj obrade ili izvršitelj obrade bez poslovnog nastana u Uniji, ako su aktivnosti obrade povezane s: (a) nuđenjem robe ili usluga takvim ispitanicima u Uniji, neovisno o tome treba li ispitanik izvršiti plaćanje; ili (b) praćenjem njihovih postupaka dokle god se oni odvijaju unutar Unije.* Ta bi obveza mogla uključivati i izuzeća u skladu s člankom 27. stavkom 2. OUZP-a.

bi se korisnicima osigurala stvarna mogućnost izbora te kontrola nad zadiranjem u njihove uređaje[14].

Još važnije, Uredbom o e-privatnosti trebalo bi osigurati da odluku o pohranjivanju informacija na uređaju i signal „Ne prati" koji šalje preglednik svi voditelji obrade podataka prihvaćaju kao pravno obvezujuću naznaku davanja ili odbijanja davanja privole. Time se ne dovode u pitanje daljnje smjernice Radne skupine o usklađenosti standarda „Ne prati" sa, među ostalim, načelom ograničavanja svrhe, kada taj standard bude završen (planirano za kraj 2017.).

Implicitne vrste „privole", kao što su klik na *web*-mjesto ili pomicanje stranice, nemaju prednost nad odlukama u pogledu pohrane i signalom „Ne prati". Važna je prednost upotrebe ovog standarda u tome da nije ograničen na tehnologiju praćenja kolačićima, nego se odnosi i na druge vrste praćenja, kao što je prikupljanje informacija u svrhu identifikacije i praćenja (eng. *fingerprinting*).

Propisivanjem da primjena tog standarda bude pravna obveza riješit će se još jedan problem, a to je trenutačna upotreba izraza „treće strane" u članku 10. *Web*-mjesto ili aplikacija obično sadržavaju brojne elemente, kako one sa samog *web*-mjesta tako i vanjske. U kontekstu posjećenog mjesta može biti aktivan neki vanjski kod koji šalje podatke na server treće strane. Kolačiće za praćenje može slati prva strana kada korisnik posjećuje na primjer *web*-mjesto za društveno umrežavanje. Ta društvena mreža može biti i treća strana kada korisnik posjećuje drugo *web*-mjesto koje sadržava interakciju s *web*-mjestom te društvene mreže. U svim navedenim slučajevima, neovisno o tome je li riječ o „pristupu" informacijama ili njihovoj „pohrani" na uređaju krajnjeg korisnika, radi se o zadiranju u uređaj za koje je potrebna privola (osim ako se primjenjuje jedno od izuzeća). Kod standarda „Ne prati" to je pitanje riješeno s pomoću pojmova „na razini *web*-mjesta" i „na razini mreže". Stoga bi, radi bolje pravne sigurnost svih dionika, upućivanje na „treće strane" u Uredbi o e-privatnosti trebalo preinačiti tako da obuhvaća sve subjekte s kojima uređaj dolazi u interakciju (jer oni pohranjuju informacije na uređaju ili im pristupaju).

Kako bi standard „Ne prati" bio usklađen s visokom razinom zaštite povjerljivosti komunikacija i zaštite podataka koja se pruža Poveljom, u Uredbi o e-privatnosti trebalo bi utvrditi da se zahtjevi za praćenje na razini interneta, za razliku od praćenja na razini *web*-mjesta, moraju predočiti odvojeno te da bi korisnici trebali moći slobodno odlučivati hoće li prihvatiti ili odbiti takve zahtjeve. Osim toga, kako bi se korisnike zaštitilo od učestalih zahtjeva za davanje privole, Uredbom o e-privatnosti trebalo bi osigurati da nakon što korisnik odbije (preko standarda „Ne prati" ili zasebne crne liste) zahtjev neke organizacije za praćenje na razini interneta, ta organizacija ne bi smjela upućivati zahtjeve za davanje privole u razdoblju od najmanje šest mjeseci. To pravilo ne sprečava predmetnu organizaciju da, u slučaju kada je korisnik izravno posjeti (tj. kao prva strana), zatraži od njega privolu na vlastitom *web*-mjestu (tj. zahtjev za davanje privole na razini *web*-mjesta). To u praksi znači, na primjer, da *web*-mjesto za videoprijenos koje se koristi kolačićima za

[14] Vidjeti URL: https://www.w3.org/TR/tracking-compliance/. U stavku 7. objašnjava se model izuzeća te razlika između izuzeća na razini *web*-mjesta i izuzeća na razini mreže. Stavak 6. sadržava strojno čitljive informacije koje voditelji obrade podataka mogu pružiti kako bi ispunili zahtjev u pogledu informiranja radi dobivanje privole.

praćenje može zatražiti privolu kada korisnik posjeti to *web*-mjesto, ali ne smije ponovno zatražiti privolu u razdoblju od šest mjeseci ako taj korisnik odbije dati privolu i posjeti druga *web*-mjesta koja sadržavaju videosadržaj upućen s *web*-mjesta koje ga prenosi.

25. Osim toga, **izuzeće za „mjerenje broja posjetitelja *web*-mjesta" neprecizno je formulirano.** Člankom 8. stavkom 1. točkom (d) predložene Uredbe predviđa se izuzeće za mjerenje broja posjetitelja *web*-mjesta. Prvo je problematično to što je navedena formulacija neodređena i može se brkati s izradom profila korisnika. U definiciji bi trebalo jasno navesti da se to izuzeće ne može upotrijebiti u svrhe izrade profila. Izuzeće bi se trebalo primjenjivati isključivo na analizu posjećenosti *web*-mjesta koja je potrebna za analizu uspješnosti pružanja usluge koju je zatražio korisnik, a ne bi se smjelo primjenjivati na analizu korisnika (tj. analizu ponašanja korisnika čiji se identitet može utvrditi, a koji posjećuju *web*-mjesto ili se koriste aplikacijom ili uređajem). Stoga se to izuzeće ne može upotrijebiti u okolnostima u kojima se podaci mogu povezati s podacima koji se odnose na korisnika čiji se identitet može utvrditi, a koje obrađuje pružatelj usluge ili drugi voditelji obrade podataka. Osim toga, opis izuzeća upućuje na primjenu koja zahtijeva vrlo specifičnu tehnologiju. Izraz „mjerenje broja posjetitelja *web*-mjesta" trebalo bi stoga promijeniti u tehnološki neutralan izraz kako bi uključivao i slične analitičke informacije o korištenju dobivene iz aplikacija, nosivih uređaja i uređaja spojenih na internet stvari.

Radna skupina predlaže da se to učini po ugledu na nizozemsko izuzeće, koje se primjenjuje ako je nužno radi dobivanja informacija o tehničkoj kvaliteti ili učinkovitosti isporučene usluge informacijskog društva te ne utječe ili neznatno utječe na privatnost uključenih pretplatnika ili krajnjih korisnika (usp. članak 11.7a stavak 3. točku (b) nizozemskog Zakona o telekomunikacijama). Kod tog je izuzeća uzeta u obzir činjenica da većina podataka prikupljenih *web*-analitikom ili analitikom aplikacija predstavlja osobne podatke. To znači da i obrada tih podataka podliježe OUZP-u. To na primjer podrazumijeva da bi analitiku upotrebe mogla provoditi i vanjska organizacija, ali samo ako su ispunjeni sljedeći uvjeti:
i. ta organizacija djeluje kao izvršitelj obrade podataka;
ii. s izvršiteljem obrade sklopljen je ugovor u skladu s OUZP-om;
iii. upotrijebljenom analitičkom tehnologijom sprečava se ponovno utvrđivanje identiteta, uključujući, među ostalim, s pomoću anonimizacije IP adresa korisnika;
iv. posebni kolačići ili drugi podaci upotrijebljeni za analitiku mogu se upotrijebiti jedino za to konkretno *web*-mjesto, aplikaciju ili nosivi uređaj te se ne mogu povezati s ostalim podacima na temelju kojih je moguće utvrditi identitet;
v. korisnici imaju pravo izuzeća (vidjeti i točke 17. i 50. ovog Mišljenja).

Iako privola ne bi bila potrebna ako su ti uvjeti ispunjeni, voditelji obrade podataka ipak moraju pružiti korisnicima odgovarajuće informacije, na primjer u rubrikama koje se odnose na status praćenja u standardu „Ne prati"[15].

[15] Vidjeti: *Tracking Preference Expression (DNT)*, nacrt urednika, 7. ožujka 2016.

26. Uredbom o e-privatnosti **trebalo bi osigurati uska i precizno formulirana izuzeća od zahtjeva u pogledu privole.** Tekst kojim se opisuje izuzeće od zahtjeva u pogledu privole za zadiranje u uređaje u članku 8. stavku 1. točki (c) gotovo je identičan trenutačnom tekstu u članku 5. stavku 3. Direktive o e-privatnosti, *strogo nužno kako bi se pružila neka usluga informacijskog društva koju je pretplatnik ili korisnik izričito zatražio*, ali je bez ikakva objašnjenja izostavljena ključna riječ „strogo". To je problematično zbog dvaju razloga. Prvo, navedena odredba Direktive o e-privatnosti već je dovela do opsežne rasprave o njezinu području primjene među nadzornim tijelima i organizacijama, a izostavljanje riječi „strogo" dovest će do još manje pravne sigurnosti. To je problematično i zbog toga što je Radna skupina već dala smjernice o tumačenju izraza „strogo" u tom kontekstu. Radna skupina predložila je sljedeće pojašnjenje u Mišljenju o kolačićima koji su izuzeti od zahtjeva za privolu (WP 194):
Kolačić je nužno potreban za osiguravanje određene funkcionalnosti korisniku (ili pretplatniku): ako su kolačići onemogućeni, funkcionalnost neće biti dostupna, a tu je funkcionalnost korisnik (ili pretplatnik) izričito zatražio u okviru usluge informacijskog društva.[16]

Osim toga, Radna je skupina pojasnila da:

kolačići „trećih strana" obično nisu „nužno potrebni" korisniku koji posjećuje web-*mjesto jer su ti kolačići obično povezani s uslugom koja se razlikuje od usluge koju je korisnik „izričito zatražio"*[17].
Radna skupina dodala je da se upotreba dodataka za društvene mreže namijenjenih onima koji nisu korisnici platforme ili *web*-mjesta isto tako ne bi smatrala nužno potrebnom.

Nadalje, dok se člankom 6. stavkom 1. točkom (b) predložene Uredbe dopušta obrada elektroničkih komunikacijskih podataka ako je to „potrebno" u sigurnosne svrhe, u uvodnoj izjavi 49. OUZP-a zahtijeva se da to bude nužno potrebno. Izostavljanje riječi „nužno" možda nije bilo namjerno jer se u uvodnoj izjavi 21. predložene Uredbe navodi da privolu za zadiranje ne bi trebalo tražiti ako je to zadiranje „nužno" potrebno. Unatoč tome, predložena Uredba pruža mogućnost da se dodatno pojasni da bi test nužnosti u kontekstu ove uredbe trebalo usko tumačiti u pogledu svih izuzeća. Radna skupina stoga predlaže da se kod svih izuzeća u članku 6. i članku 8. stavku 1. predložene Uredbe iza riječ „nužno" doda riječ „potrebno".

S druge strane, Uredbom o e-privatnosti trebalo bi izričito dopustiti zadiranje u opremu koje se provodi radi instaliranja sigurnosnog ažuriranja. Slanje sigurnosnog ažuriranja putem interneta poželjna je metoda instaliranja sigurnosnog ažuriranja u većinu uređaja krajnjih korisnika. Instaliranje ažuriranja smatra se zadiranjem u terminalnu opremu. Postoji legitiman interes da se osigura da sigurnost tih uređaja

[16] Radna skupina iz članka 29., WP 294, Mišljenje 04/2012 o kolačićima koji su izuzeti od zahtjeva za privolu, doneseno 7. lipnja 2012., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf.

[17] Ibidem

bude ažurirana. Stoga bi pružatelj sigurnosnih zakrpa trebao općenito biti u mogućnosti instalirati nužno potrebna sigurnosna ažuriranja bez privole krajnjeg korisnika. Međutim, nejasno je može li se na takvo zadiranje primijeniti izuzeće od zabrane zadiranja koje se odnosi na „informacijsko društvo" (članak 8. stavak 1. točka (c)). Trebalo bi pojasniti da je instaliranje sigurnosnog ažuriranja dopušteno u skladu s tim izuzećem, ali samo i. ako su sigurnosna ažuriranja u zasebnom paketu i ni na koji način ne mijenjaju funkcionalnost softvera u opremi (uključujući interakciju s drugim softverom ili postavkama koje je odabrao korisnik), ii. ako se krajnjeg korisnika unaprijed obavijesti svaki put kad se instalira ažuriranje te iii. ako krajnji korisnik ima mogućnost isključiti funkciju automatskog instaliranja tih ažuriranja.

IZRAVNI MARKETING

Problematično pitanje je i nedovoljna zaštita protiv izravnog marketinga.

27. Prvo, problematično je to što je **opseg izravnog marketinga previše ograničen**. U članku 4. stavku 3. točki (f) predložene Uredbe „izravne marketinške komunikacije" definiraju se kao „svaki oblik oglašavanja, neovisno o tome je li u pisanom ili usmenom obliku, koji se šalje jednom ili više krajnjih korisnika elektroničkih komunikacijskih usluga čiji je identitet utvrđen ili se može utvrditi". Upotreba riječi „koji se šalje" podrazumijeva upotrebu tehnoloških komunikacijskih sredstava koja nužno uključuju prenošenje komunikacije, dok većina oglašavanja na internetu (preko platformi društvenih medija ili na *web*-mjestima) ne uključuje „slanje" oglasa u strogom smislu te riječi. To je dodatno naglašeno primjerima navedenima u definiciji (SMS, elektronička pošta) te u uvodnoj izjavi 33. Sve se to odnosi na prilično tradicionalne oblike marketinške komunikacije, pa čak i tada upotreba – prilično tradicionalnih – sustava pozivanja možda nije obuhvaćena područjem primjene. Taj članak i uvodnu izjavu trebalo bi izmijeniti tako da se obuhvate svi oblici oglašavanja *koji se šalju, upućuju ili prikazuju* jednom ili više krajnjih korisnika čiji je identitet utvrđen ili se može utvrditi. Osim toga, potrebno je osigurati da se i bihevioralno oglašavanje (koje se temelji na profilima krajnjih korisnika) smatra izravnim marketinškim komunikacijama usmjerenima na „jednog ili više krajnjih korisnika čiji je identitet utvrđen ili se može utvrditi" (s obzirom na to da su ti oglasi namijenjeni posebnim korisnicima čiji se identitet može utvrditi).

Nadalje, u skladu s predloženim područjem primjene „izravnih marketinških komunikacija", zaštita iz članka 16. stavka 1. bila bi ograničena na poruke koje sadržavaju reklamni materijal te se njome pojedinci ne bi štitili od drugih poruka koje se šalju, upućuju ili prikazuju u marketinške svrhe (kao što su poruke o stvaranju popisa potencijalnih klijenata u kojima se traži privola, promicanje političkih gledišta ili glasačkih preferencija, promicanje humanitarnih ili drugih neprofitnih organizacija ili opće stvaranje identiteta (brendiranje) organizacije). Osim toga, u definiciji nisu navedeni telefaks uređaji iako se oni još uvijek upotrebljavaju kao metoda izravnog marketinga. Članak 4. stavak 3. točka (f) trebao bi stoga obuhvatiti svaki oblik oglašavanja, anketiranja ili promidžbe, uključujući i za neprofitne organizacije, te bi uz elektroničku poštu i SMS trebalo izričito navesti i telefaks uređaje (vidjeti i

prijedlog za pojašnjenje u točki 43. podtočki (a)). Konačno, u uvodnoj izjavi 32. navodi se da izravni marketing uključuje i poruke koje šalju političke stranke radi vlastite promidžbe. To bi trebalo ažurirati tako da uključuje političare i kandidate na izborima koji promiču svoju kandidaturu.

28. Drugo, **povlačenje privole za izravni marketing nije besplatno ni lako kao davanje privole.** Potrebno je pojasniti mogućnost povlačenja privole na temelju predložene Uredbe kako bi se osigurala dosljednost i poboljšala zaštita primatelja. Člankom 16. stavkom 6. predložene Uredbe trenutačno se predviđa da se primateljima izravnih marketinških komunikacija moraju pružiti „informacije potrebne kako bi ostvarili svoje pravo na jednostavno povlačenje privole za primanje daljnjih marketinških komunikacija" (podcrtavanje dodano). To je potvrđeno u uvodnoj izjavi 34. Međutim, iz uvodne izjave 70. OUZP-a proizlazi da bi ispitanici na temelju OUZP-a trebali imati ne samo pravo da na jednostavan način ulože prigovor na obradu podataka u svrhu izravnog marketinga, nego i da to učine „besplatno". Taj se izraz upotrebljava i u članku 16. stavku 2. predložene Uredbe, ali samo u pogledu izuzeća od izravnog marketinga na temelju kontaktnih podataka dobivenih u kontekstu prodaje.

Člankom 7. stavkom 3. OUZP-a predviđa se da povlačenje privole mora biti jednako jednostavno kao i njezino davanje te da bi pojedinci trebali moći u svakom trenutku povući svoju privolu. Osim toga, Radna skupina već je u svojem Mišljenju 04/2010 o FEDMA-i (WP174) priznala važnost nuđenja „jednostavne, učinkovite, besplatne, izravne i lako dostupne metode odjave" od primanja izravnih marketinških komunikacija[18]. Taj standard povlačenja privole trebalo bi ugraditi u pravila za izravni marketing u predloženoj Uredbi. Isto vrijedi i za zahtjev iz članka 7. stavka 3. OUZP-a da bi u svakom trenutku povlačenje privole trebalo biti jednako jednostavno kao i njezino davanje.

29. S tim u vezi, **trebalo bi pojasniti način povlačenja privole ili izuzeća od izravnih marketinških poziva**. Na temelju članka 16. stavka 4. predložene Uredbe, države članice mogu odlučiti primjenjivati režim izuzeća za govorne izravne marketinške pozive. Uredbom o e-privatnosti trebalo bi pobliže utvrditi postupke povlačenja privole i postupke izuzeća za marketinške pozive. U uvodnoj izjavi 36. utvrđuje se da bi države članice *trebale imati mogućnost* uspostave i/ili održavanja nacionalnih sustava izuzeća. Na temelju te odredbe, države članice mogle bi čak dopustiti situaciju u kojoj bi korisnik morao koristiti izuzeće u odnosu na pojedinačne pružatelje komunikacija. Takvom se provedbom korisnici ne štite od uznemiravanja neželjenim komunikacijama[19] niti se osigurava mehanizam lakog povlačenja privole

18 Radna skupina iz članka 29., WP174, Mišljenje 04/2010 o europskom kodeksu ponašanja FEDMA-e pri upotrebi osobnih podataka u izravnom marketingu, doneseno 13. srpnja 2010., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_en.pdf.

19 Na primjer, u Ujedinjenoj Kraljevini telekomunikacijski operater BT zabilježio je 31 milijun uznemirujućih poziva u tjedan dana. Vidjeti: http://www.bbc.com/news/business-38635921.

u svakom trenutku koji je u skladu s OUZP-om. Stoga bi Uredbom trebalo utvrditi da države članice *moraju* uspostaviti nacionalni registar „Ne zovi". Osim toga, Uredbom bi trebalo utvrditi da bi primateljima govornih izravnih poziva trebalo dati dvije mogućnosti povlačenja privole: za buduće pozive od predmetnog poduzeća ili organizacije te mogućnost da se tijekom tih poziva registriraju u nacionalni registar „Ne zovi".

30. Problematično je i to što **nije izričito zabranjena upotreba lažnih identiteta pri slanju izravnih marketinških komunikacija**. U uvodnoj izjavi 34. navodi se da je potrebno zabraniti „maskiranje identiteta i uporabu lažnih identiteta, lažnih povratnih adresa ili brojeva pri slanju nezatraženih komercijalnih komunikacija u svrhe izravnog marketinga". Međutim, u članku 16. stavku 4. samo se navodi da se krajnje korisnike obavješćuje o „identitetu pravne ili fizičke osobe u čije ime se komunikacija prenosi". Tu obvezu obavješćivanja primatelja o identitetu trebalo bi dopuniti jasnom zabranom upotrebe maskiranih ili lažnih kontaktnih adresa u svrhe izravnog marketinga.

31. Ova se točka odnosi na još jedno pitanje koje izaziva zabrinutost: **zahtjev za navođenje predbroja za izravni marketing navodi se kao alternativa zahtjevu za navođenje broja za kontakt**. U skladu s člankom 16. stavkom 3. izravni marketinški pozivi dopušteni su ako pozivatelj ili i. navede broj na koji se može kontaktirati fizička ili pravna osoba koja upućuje poziv (članak 16. stavak 3. točka (a)) ili ii. upotrebljava posebni kod/predbroj na temelju kojeg se može utvrditi da je poziv marketinške prirode (članak 16. stavak 3. točka (b)). Iako Radna skupina pozdravlja obvezu upotrebe predbroja iz članka 16. stavka 3. točke (b), vjeruje da se tim zahtjevom ne rješava isti problem koji se rješava obvezom navođena broja za kontakt iz članka 16. stavka 3. točke (a). Dok je svrha zahtjeva za navođenje predbroja omogućiti primatelju da odmah utvrdi da je poziv marketinške prirode (te da poduzme mjere za blokiranje tih poziva), svrha je zahtjeva za navođenje broja za kontakt osigurati način na koji primatelji (i nadzorna tijela) mogu identificirati i kontaktirati pokretača marketinške aktivnosti. To je posebno bitno u slučaju automatskih poziva kod kojih postoji velika neravnoteža između mogućnosti prodavatelja usluge ili proizvoda da uputi uznemirujući poziv i mogućnosti primatelja da izbjegne te pozive. Ti zahtjevi stoga ne bi smjeli biti alternativa jedan drugome, nego bi se trebali nadopunjavati.

VREMENSKI RASPORED

32. Radna skupina iz članka 29. pohvaljuje to što Europska komisija priznaje potrebu da predložena Uredba stupi na snagu zajedno s OUZP-om u svibnju 2018. kako bi se izbjegle nedosljednosti između tih dvaju zakonodavnih akata. Međutim, takav ambiciozan rok ipak izaziva zabrinutost jer zahtijeva završetak izrade Europskog zakonika elektroničkih komunikacija. Radna skupina iz članka 29. stoga zahtijeva da se svi sudionici u zakonodavnom postupku obvežu pridržavati se roka, a to je svibanj 2018.

OSTALA PROBLEMATIČNA PITANJA

U ovom se odjeljku razmatra niz dodatnih problematičnih pitanja.

33. Prvo, Radna skupina iz članka 29. izražava zabrinutost zbog toga što se **navodi na zaključak da su mjere čuvanja podataka koje nisu ciljano usmjerene prihvatljive.** U Obrazloženju se navodi da na temelju predložene Uredbe države članice mogu zadržati ili stvoriti nacionalne okvire za čuvanje podataka kojima su propisane, među ostalim, ciljane mjere čuvanja (točka 1.3.). Nakon presude u predmetu *Tele2/Watson*[20], jasno je da okviri za čuvanje podataka kojima se predviđa bilo što drugo osim ciljanog čuvanja nisu dopušteni na temelju Povelje (a čak i kada predviđaju samo ciljano čuvanje podataka podliježu važnim uvjetima kao što je nadzor) te da se opći pristup metapodacima mora smatrati povredom bitnog sadržaja članka 7. na isti način kao i opći pristup sadržaju elektroničke komunikacije (usp. Sud Europske unije, Schrems, i točka 94. navedene presude). Način na koji je rečenica sročena navodi na zaključak da je u pogledu mjera čuvanja podataka državama članicama ostavljen određeni manevarski prostor, koji ne postoji. S tim je povezana i činjenica da predloženom Uredbom **nije osigurana dovoljna razina zaštite metapodataka**. Kako je navedeno u točki 10., Radna skupina iz članka 29. pozdravlja priznanje da se na temelju metapodataka mogu otkriti vrlo osjetljivi podaci. Međutim, predloženom Uredbom nije osigurana ona razina zaštite metapodataka koja bi trebala proizlaziti iz tog priznanja. S obzirom na osjetljivost metapodataka, posebno prije analize na temelju članka 6. stavka 2. točke (c), trebalo bi provesti procjenu učinka na zaštitu podataka (vidjeti i točku 46.).

34. Drugo, **predloženom Uredbom nepotrebno bi se proširile mogućnosti čuvanja podataka**. U članku 11. predložene Uredbe upućuje se na članak 23. stavak 1. točke (a) do (e) OUZP-a pri opisivanju svrha u koje države članice mogu ograničiti obveze i prava koji su predviđeni člancima 5. do 8. Uredbe. OUZP-om nisu predviđena takva ograničenja u pogledu posebnih kategorija podataka, u skladu s visokim rizicima za ispitanike. Iako je člankom 15. Direktive o e-privatnosti trenutačno dopušteno slično ograničenje, svrhe su ograničenije. Novom predloženom Uredbom omogućila bi se nova ograničenja u svrhe „izvršavanja kaznenopravnih sankcija, uključujući zaštitu od prijetnji javnoj sigurnosti i njihovo sprečavanje" (članak 23. stavak 1. točka (d) OUZP-a) i „drugih važnih ciljeva od općeg javnog interesa Unije ili države članice, posebno važnog gospodarskog ili financijskog interesa Unije ili države članice, što uključuje monetarna, proračunska i porezna pitanja, javno zdravlje i socijalnu sigurnost" (članak 23. stavak 1. točka (e) OUZP-a). Ne samo da su te svrhe nove u usporedbi s Direktivom o e-privatnosti, nego su zadnja svrha iz članka 23. stavka 1. točke (d) i cijela svrha iz članka 23. stavka 1. točke (e) iznimno široko formulirane. Stoga se predlaže da se upućivanje na članak 23. stavak 1. točke (a) do (e) OUZP-a briše te da se umjesto toga navedu samo svrhe koje su trenutačno navedene u članku 15. Direktive o e-privatnosti.

35. **Obveza obavješćivanja korisnikâ o sigurnosnim rizicima ima previše ograničeno područje primjene**. Radna skupina pozdravlja činjenicu da pružatelji usluga moraju

[20] ECLI:EU:C:2016:970, URL: http://curia.europa.eu/juris/celex.jsf?celex=62015CJ0203.

obavijestiti korisnike o sigurnosnim rizicima i mjerama za rješavanje tih rizika, kao što je enkripcija (članak 17. i uvodna izjava 37.). Međutim, naslov odredbe glasi: „Informacije o otkrivenim sigurnosnim rizicima". Činjenica da se u naslovu navode otkriveni rizici upućuje na to da se odredba odnosi samo na (potencijalne) povrede sigurnosti, dok su odredba i uvodna izjava sročene tako da više upućuju na opću edukaciju krajnjih korisnika. Na primjer, ako pružatelj usluge otkrije da je uređaj korisnika zaražen zlonamjernim softverom i da je postao dio botneta, čini se da se tom odredbom pružatelj usluge izravno obvezuje da obavijesti korisnika o rizicima koji iz toga proizlaze. Međutim, područje primjene te odredbe moglo bi se pojasniti te ne bi smjelo biti ograničeno na taj konkretan scenarij. Odredbom bi trebali biti obuhvaćeni barem otkriveni sigurnosni rizici u svoj opremi koju pružatelj usluge osigurava krajnjem korisniku u okviru pretplate, kao što su na primjer usmjernici i mobilni uređaji, te bi trebala uključivati i edukaciju o rizicima koji nastaju u slučaju mijenjanja postavki za zaštitu privatnosti zadanih u skladu s načelom tehničke zaštite privatnosti.

Radna skupina preporučuje da se područje primjene proširi kako bi se obuhvatilo pružatelje softvera za elektroničke komunikacije (usp. uvodnu izjavu 8.) te prema mogućnosti i novu kategoriju: pružatelje tehnologije koja je bitna za sigurne komunikacije, a koji nisu pružatelji usluga (npr. pružatelje enkripcijske tehnologije). Kad je riječ o proširenju u potonjem slučaju trebalo bi voditi računa o tome da se ta obveza ne preklapa s obvezama obavješćivanja o povredi sigurnosti iz drugih instrumenata, kao što je Direktiva NIS,[21] te drugih pravnih instrumenata koji se odnose na pružatelje certifikata. S obzirom na to da potonja kategorija pružatelja tehnologije obično nema izravan kontakt s krajnjim korisnicima, mora se objasniti i način na koji oni mogu ispuniti svoju obvezu obavješćivanja na temelju te uredbe.

36. Radna skupina pozdravlja odredbe članaka 2. i 13. koje će se primjenjivati na brojevno utemeljene interpersonalne komunikacijske usluge. Međutim, nije odmah očito zašto **slična razina zaštite privatnosti ne bi bila dostupna i za funkcionalno istovjetne OTT usluge pozivanja.**

37. Radna skupina izražava zabrinutost i zbog **nedostatka jasnoće u pogledu precizno definirane privole za obrnuto pretraživanje imenika**. Člankom 15. stavkom 2. predložene Uredbe od pružatelja se zahtijeva da od krajnjih korisnika dobiju privolu prije nego što aktiviraju funkcije pretraživanja koje se odnose na podatke (vidjeti i uvodnu izjavu 31.). Radna skupina pozdravlja usklađivanje zahtjeva za privolu u pogledu uključivanja imenika, ali sa žaljenjem navodi da ne nije predviđena mogućnost preciznog definiranja privole za različite vrste pretraživanja. Trenutačnom Direktivom o e-privatnosti državama članicama dopušta se da zahtijevaju zaseban zahtjev za privolu za obrnuto pretraživanje, na temelju članka 12. stavka 3. U tom se članku navodi da *države članice mogu zahtijevati da se od pretplatnika traži dodatni pristanak za bilo koju svrhu javnog telefonskog imenika, osim traženja kontaktnih*

[21] Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, SL L 194, 19.7.2016., str. 1.–30., url: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

podataka o osobama na temelju njihovog imena te, gdje je to potrebno, minimuma drugih indikatora. Na temelju te odredbe u mnogim se državama članicama zahtijeva zasebna privola za funkcionalnosti obrnutog pretraživanja, uzimajući u obzir različite razine do kojih se s pomoću tih dviju funkcionalnosti može utvrditi identitet osobe, a time i narušiti njezina privatnost.

38. S formalnog aspekta, **visina novčanih kazni nije usklađena za sve povrede Uredbe**. U predloženoj se Uredbi predviđa da države članice utvrđuju pravila o sankcijama za povrede članka 23. stavka 4., članka 23. stavka 6. i članka 24. predložene Uredbe. Bilo bi dosljednije da se ovo pitanje riješi i u samoj Uredbi o e-privatnosti.

39. Konačno**, predložena Uredba oslanja se na definicije koje mogu postati „pokretne mete"**. Za niz ključnih pojmova u predloženoj se Uredbi upućuje na drugi pravni instrument koji je trenutačno u obliku nacrta: predloženi EECC (vidjeti, na primjer, članak 4. stavak 1. točku (b)). Dva važna primjera za to su definicija „krajnjeg korisnika", koja trenutačno obuhvaća fizičke i pravne osobe, te definicije „elektroničkih komunikacijskih usluga" i „interpersonalnih komunikacijskih usluga", koje se navode u članku 4. stavku 1. točki (b) predložene Uredbe, pri čemu se potonja preciznije određuje u članku 4. stavku 2. kako bi se obuhvatile i vrste usluga koje su izričito isključene u EECC-u.[22] Ovo se Mišljenje temelji na definicijama onakvima kakve su trenutačno, međutim velika je vjerojatnost da će se predloženi EECC i/ili njegovi ključni pojmovi promijeniti. To bi imalo izravne posljedice i za Uredbu o e-privatnosti. U idealnom bi slučaju sve pojmove iz EECC-a trebalo neovisno definirati u Uredbi o e-privatnosti ili bi barem u predloženoj Uredbi trebalo navesti pojašnjenje za pojmove čija definicija odstupa od one u EECC-u (npr. prethodno navedeno uključenje „pomoćnih usluga" u definiciju „interpersonalnih komunikacijskih usluga"). Međutim, ako to nije moguće, Radna skupina htjela bi predložiti da sve strane koje su uključene u zakonodavni postupak osiguraju da će se o predloženoj Uredbi i EECC-u raspravljati i glasovati istodobno kako bi se dionicima omogućilo da ispravno procijene područje primjene i posljedice novih instrumenata.

5. PRIJEDLOZI ZA POJAŠNJENJA RADI OSIGURAVANJA PRAVNE SIGURNOSTI

Osim prethodno razmatranih pitanja, Radna skupina isto tako želi istaknuti neke odredbe predložene Uredbe koje bi bilo dobro pojasniti. Smatra se da su ta pojašnjenja potrebna kako bi se svim dionicima pružila pravna sigurnost da će Uredba o e-privatnosti biti shvaćena i primijenjena na ujednačen način u cijelom EU-u.

POJAŠNJENJA PODRUČJA PRIMJENE

[22] Na primjer, u članku 4. stavku 2. predložene Uredbe navodi se da interpersonalne komunikacijske usluge „uključuju usluge kojima se omogućuje interpersonalna i interaktivna komunikacija samo kao manja pomoćna funkcija koja je neraskidivo povezana s drugom uslugom", dok su u članku 2. stavku 5. EECC-a takve usluge izričito isključene iz te definicije. (U EECC-u je „interpersonalna komunikacijska usluga" uključena u širu kategoriju „elektroničke komunikacijske usluge" u članku 2. stavku 4.).

40. U pogledu područja primjene predložene Uredbe Radna skupina iz članka 29. predlaže sljedeća pojašnjenja:

    a. **Pojam „krajnji korisnik" trebao bi uključivati sve pojedinačne korisnike**. U članku 2. stavku 14. EECC-a „krajnji korisnik" definira se kao korisnik koji ne daje na korištenje javne komunikacijske usluge ili ne pruža javno dostupne elektroničke komunikacijske usluge. Trebalo bi pojasniti da pojedinci koji pridonose mreži – na primjer isprepletenoj mreži svojim WiFi usmjernicima – nisu isključeni iz područja primjene zaštite iz predložene Uredbe.
    b. **Trebalo bi pojasniti da su teritorijalnim područjem primjene obuhvaćeni svi krajnji korisnici u Uniji**. Člankom 3. stavkom 1. točkom (a) predviđa se da se predložena Uredba primjenjuje na pružanje elektroničkih komunikacijskih usluga krajnjim korisnicima „u Uniji", dok se člankom 3. stavkom 1. točkom (c) predviđa da se ona primjenjuje na zaštitu terminalne opreme krajnjih korisnika „koji se nalaze u Uniji" (podcrtavanje je dodano). To se razlikuje u različitim prijevodima. Njemačka verzija ne sadržava tu razliku, dok je druge verzije, na primjer francuska i danska, sadržavaju. Iz uvodne izjave 9. jasno proizlazi da je predviđeno široko teritorijalno područje primjene, bez obzira na to pružaju li se usluge izvan Unije odnosno odvija li se obrada u Uniji. Stoga se predlaže da se u članku 3. stavku 1. točki (c) uklone riječi „koji se nalaze" kako bi se naglasilo to široko područje primjene.
    c. **Čini se da se predloženom Uredbom povjerljive komunikacije štite samo dok se *prenose*, a ne i dok su *pohranjene***. Trenutačni je pristup u predloženoj Uredbi usredotočiti se na zaštitu prijenosa komunikacija. Vidjeti, na primjer, uvodnu izjavu 15., u kojoj se navodi da bi zabranu presretanja podataka o komunikacijama trebalo primjenjivati tijekom njihova prijenosa, odnosno dok predviđeni primatelj ne primi sadržaj komunikacije. Područje primjene te zaštite temelji se na zastarjelom koncepcijskom okviru za komunikacije. Većina komunikacijskih podatka čak i nakon primitka ostaje pohranjena kod pružatelja usluga te bi trebalo osigurati da povjerljivost tih podataka i dalje bude zaštićena. Osim toga, komunikacija između pretplatnika istih usluga u oblaku (na primjer pružatelja usluga internetske pošte) često uključuje vrlo malo prijenosa: slanje pošte uglavnom se odražava u bazi podataka pružatelja usluge i ne sastoji se od stvarnog slanja komunikacija između dviju stranaka. Neuvjerljiva je tvrdnja da bi to bilo obuhvaćeno OUZP-om: upravo je i svrha predložene Uredbe zaštititi sve povjerljive komunikacije, bez obzira na tehnička sredstva takve komunikacije. Moguće je da je riječ o pogrešnoj formulaciji jer se zabrana u članku 5. odnosi na „pohranjivanje" i „obradu".
    d. **Sve javne pristupne točke za bežični pristup internetu trebale bi biti obuhvaćene područjem primjene**. S obzirom na to da je upotreba bežičnih pristupnih točaka uobičajena, sasvim je logično da ne bi smjelo biti nikakve dvojbe o tome je li povjerljivost komunikacija koje se prenose putem takvih pristupnih točaka zaštićena. Međutim, pokušaj da se to pojasni u ovoj Uredbi nije uspio jer je područje primjene prošireno na mreže čije se usluge pružaju

„nedefiniranoj skupini krajnjih korisnika" (uvodna izjava 13.). Potrebno je definirati izraze „nedefinirana skupina krajnjih korisnika" i „zatvorena skupina krajnjih korisnika". Posebno bi trebalo pojasniti da su i sigurne bežične mreže (tj. one sa zaporkom) obuhvaćene područjem primjene, ako se ta zaporka daje teoretski neodređenoj skupini korisnika čiji se identitet ne može odrediti unaprijed (npr. gostima u kafiću, posjetiteljima u zračnoj luci). U tom je kontekstu temeljno načelo da, u skladu s prethodnim mišljenjem Radne skupine iz članka 29. o preispitivanju Direktive o e-privatnosti, *jedino usluge do kojih dolazi u službenom kontekstu ili u kontekstu zaposlenja isključivo u službene svrhe ili u svrhe povezane s poslom, ili tehnička komunikacija između tijela koja nisu javna ili između javnih tijela isključivo radi kontrole radnih ili poslovnih procesa, kao i korištenje uslugama isključivo u domaće svrhe, mogu se izuzeti iz instrumenta o e-privatnosti*. (str. 8.).

e. **Predloženom Uredbom trebalo bi obuhvatiti podatke prikupljene tijekom nuđenja usluga digitalne radiodifuzije.** S obzirom na to da su navike gledatelja osjetljive prirode jer otkrivaju osobne interese i karakteristike gledatelja, Uredbom o e-privatnosti trebalo bi pobliže utvrditi (možda u uvodnoj izjavi) da isključivanje usluga pružanja „sadržaja koji se prenosi korištenjem elektroničkih komunikacijskih mreža" iz definicije „elektroničke komunikacijske usluge" ne znači da pružatelji usluga koji nude i elektroničke komunikacijske usluge i usluge sadržaja nisu obuhvaćeni područjem primjene odredaba Uredbe o e-privatnosti koja je usmjerena na pružatelje elektroničkih komunikacijskih usluga. To je posebno bitno jer je pružanje usluga pružanja „sadržaja koji se prenosi korištenjem elektroničkih komunikacijskih mreža" isključeno iz definicije „elektroničke komunikacijske usluge" na temelju predloženog EECC-a (članak 2. stavak 4.).

f. **Komunikacijski podaci uglavnom su osobni podaci**. U uvodnoj izjavi 4. navodi se da komunikacijski podaci mogu uključivati osobne podatke. Međutim, većina komunikacijskih podataka osobni su podaci[23] i većim je dijelom riječ o podacima prilično intimne i osjetljive prirode te bi tu uvodnu izjavu trebalo izmijeniti tako da se navede da su komunikacijski podaci uglavnom osobni podaci.

g. **Povjerljiva komunikacija uključuje poruke na platformama**. U uvodnoj izjavi 1. objašnjava se da se načelo povjerljivosti primjenjuje na „sadašnja i buduća sredstva komunikacije". Potom se navode primjeri tih sredstava, među ostalim i „razmjena osobnih poruka preko društvenih medija". Time se vjerojatno namjeravalo obuhvatiti osobne poruke između korisnika neke društvene mreže (npr. Facebooka ili Twittera) ili poruke objavljene na

[23] Vidjeti, na primjer, presudu Suda Europske unije od 6. studenoga 2003. u predmetu C-101/01, t. 24. (u pogledu telefonskog broja), presudu Suda Europske unije od 19. listopada 2016. u predmetu C-582/14 (*Breyer*), t. 49. (u pogledu dinamične IP adrese) i presudu Suda Europske unije od 8. travnja 2014. u predmetima C-239/12 i C-594/12 (*Digital Rights Ireland*), t. 26.–27. (u pogledu osjetljivosti metapodataka).

vremenskoj crti koje su dostupne ograničenom broju osoba, ali tekst nije dovoljno jasno sročen.

h. **Kako se Uredba o e-privatnosti primjenjuje na interakciju između strojeva.** Kako je navedeno u točki 9., Radna skupina pozdravlja proširenje zaštite na interakciju između strojeva. Međutim, to se spominje samo u uvodnoj izjavi 12., a ne i u odgovarajućem članku. Ta je zaštita poželjna jer takve komunikacije često sadržavaju informacije koje su zaštićene pravima na privatnost. S druge strane, usku kategoriju puke komunikacije između strojeva trebalo bi izuzeti ako ne utječe na privatnost ili na povjerljivost komunikacija, kao što je na primjer slučaj kada se takva komunikacija provodi pri izvršavanju prijenosnog protokola između elemenata mreže (npr. servera, prespojnika) radi međusobnog izvješćivanja o statusu aktivnosti.
Posebno je potrebno pojasniti primjenu Uredbe o e-privatnosti u području inteligentnih prometnih sustava. Predviđeno je da vozila kontinuirano putem radija šalju podatke koji sadržavaju jedinstveni identifikator. Bez dodatne zaštite u Uredbi o e-privatnosti u pogledu komunikacijskih podataka to bi moglo dovesti do stalnog praćenja vozačkih navika, planova putovanja i brzine vozača. Međutim, članak 2. stavak 1. EECC-a sadržava novu i proširenu definiciju komunikacijskih mreža. One uključuju sustave prijenosa koji nemaju centralizirani upravljački kapacitet i koji omogućuju prijenos signala putem radija U uvodnoj izjavi 14. Uredbe o e-privatnosti utvrđuje se da su takvi podaci elektronički komunikacijski podaci. Na temelju članka 5. predložene Uredbe zabranjen je svaki oblik presretanja, praćenja ili pohranjivanja tih komunikacijskih podataka, osim ako se primjenjuje jedno od izuzeća. Ipak, postoji interes da se ti podaci obrađuju kako bi se predmeti kao što su automobili bez vozača i autonomni uređaji međusobno upozoravali o svojoj blizini ili o drugim rizicima. Postavlja se pitanje koje bi se izuzeće primjenjivalo u tom slučaju. Privola krajnjih korisnika nije izvedivo izuzeće jer može biti potrebno uvijek moći obraditi te podatke. Pružatelji bi stoga trebali biti u mogućnosti osloniti se na posebno izuzeće, a to je omogućivanje predmetima kao što su automobili bez vozača i autonomni uređaji da se međusobno upozoravaju o svojoj blizini ili o drugim rizicima.

POJAŠNJENJA POJMA I PRIMJENE PRIVOLE

41. U pogledu pojma i primjene privole u trenutačnoj predloženoj Uredbi Radna skupina iz članka 29. predlaže sljedeća pojašnjenja:

    a. **Kako bi pojam privole trebalo primjenjivati u kontekstu pravnih osoba.** U uvodnoj izjavi 3. navodi se da bi Uredbom trebalo osigurati primjenu odredbi OUZP-a i na krajnje korisnike koji su pravne osobe. To u skladu s tom uvodnom izjavom uključuje definiciju privole na temelju OUZP-a (vidjeti i uvodnu izjavu 18.). Kako je navedeno u točki 13., Radna skupina pozdravlja izričito uključivanje pravnih osoba u područje primjene Uredbe. Nije međutim jasno kako bi se to načelo trebalo primjenjivati u praksi. U skladu s definicijom privole u OUZP-u privola mora biti „informirana", a izražavanje želja ispitanika mora biti „izjavom ili jasnom potvrdnom

radnjom" (članak 4. stavak 11. OUZP-a). Potrebno je pojasniti kada se zapravo može smatrati da je pravna osoba „informirana" i kada postoji takvo izražavanje želja pravne osobe.

b. U tom kontekstu vrijedi napomenuti da poslodavac u većini okolnosti ne može dati privolu u ime svojih zaposlenika jer kada poslodavac traži privolu od zaposlenika i kada, s obzirom na nejednaku ravnotežu moći, nedavanje privole može prouzročiti stvarnu ili moguću štetu za zaposlenika, takva privola nije valjana jer nije dana dobrovoljno[24]. U pogledu **poduzeća koja ustupaju uređaje ili opremu pojedincima, predložena Uredba ne sadržava (prikladno) izuzeće** od zabrane zadiranja. Primjer je za to slučaj kada poslodavac želi ažurirati telefon koji je poduzeće ustupilo. Drugi je primjer kada poslodavac nudi zaposlenicima unajmljene automobile te u administrativne svrhe dopušta trećoj strani da prikuplja podatke o lokaciji preko uređaja ugrađenog u automobil. U oba slučaja poslodavac ima interes da zadire u te uređaje.

   Zadiranje se ne može smatrati nužnim za pružanje usluge informacijskog društva (članak 8. stavak 1. točka (c)) ili nužnim za mjerenje broja posjetitelja *web*-mjesta (članak 8. stavak 1. točka (d)). To bi se moglo riješiti tako da se uvede novo izuzeće kako bi se uključila situacija kada i. poslodavac pruža određenu opremu u kontekstu radnog odnosa, ii. zaposlenik je korisnik te opreme, i iii. zadiranje je nužno potrebno za funkcioniranje opreme kojom se koristi zaposlenik (što podrazumijeva primjenu načela proporcionalnosti i supsidijarnosti u pogledu prikupljanja podataka). Jedino ako su ispunjeni ti uvjeti, poslodavac bi mogao zadirati u uređaj krajnjeg korisnika.

c. **Poboljšanje kontrola za zaustavljanje automatskog prosljeđivanja poziva**. Člankom 14. predviđa se važna kontrola krajnjih korisnika za zaustavljanje automatskog prosljeđivanja poziva treće strane. Ta se zaštita može dodatno poboljšati tako da se od krajnjeg korisnika traži privola za pokretanje prosljeđivanja poziva.

POJAŠNJENJA O PODACIMA O LOKACIJI I DRUGIM METAPODACIMA

42. Radna skupina predlaže da se pojasne sljedeća pitanja u pogledu podataka o lokaciji i drugih metapodataka:

    a. **Trebalo bi pojasniti značenje „podataka o lokaciji koji nisu generirani u kontekstu pružanja usluga elektroničkih komunikacija" u uvodnoj izjavi 17**. Nije jasno odnosi li se to na podatke o lokaciji prikupljene, na primjer, preko aplikacija koje upotrebljavaju podatke iz GPS funkcionalnosti u pametnim uređajima i/ili generiraju podatke o lokaciji na temelju obližnjih WiFi usmjernika, i/ili podatke o lokaciji prikupljene s pomoću ugrađenih navigacijskih aplikacija i/ili na druge načine generiranja podataka o lokaciji. Zbog nedostatka jasnoće nastaje pravna nesigurnost u pogledu područja

[24] Vidjeti Mišljenje 15/2011 o definiciji privole (WP 187), Mišljenje 8/2001 o obradi osobnih podataka u kontekstu zaposlenja (WP48) i novo Mišljenje o obradi podataka na radnom mjestu (doneseno istodobno kad i ovo Mišljenje).

primjene obveze. U svakom slučaju, podaci o lokaciji terminalnog uređaja fizičke osobe osobni su podaci te stoga obrada tih podataka podliježe obvezama iz OUZP-a.

b. Trebalo bi pojasniti da **za većinu zakonite obrade podataka o lokaciji i drugih metapodataka <u>nije</u> potreban jedinstveni identifikator**. U uvodnoj izjavi 17. navode se toplinske mape (eng. *heatmaps*) kao primjer komercijalne uporabe elektroničkih komunikacijskih metapodataka od strane pružatelja elektroničkih komunikacijskih usluga. Međutim, da bi se stvorila osnovna toplinska mapa, nisu potrebni jedinstveni identifikatori, nego je dovoljno samo statističko brojanje. Drugi primjer koji se navodi u toj uvodnoj izjavi, a to je upotreba infrastrukture i pritisak na nju, može se isto tako brojati s pomoći određenih mjernih točaka, na primjer stvaranjem agregiranih statističkih podataka o upotrebi tornjeva za praćenje prometa kako bi se saznalo koliki je pritisak na određenu lokaciju u određenom trenutku, a da pri tom nije potrebno znati identitet spojenih osoba.

   Osim toga, u uvodnoj se izjavi kao primjer navodi prikaz kretanja prometa u određenim smjerovima tijekom određenog razdoblja kod kojeg bi bio potreban jedinstveni identifikator za povezivanje položaja pojedinaca u određenim vremenskim intervalima. Čini se da se u uvodnoj izjavi tim primjerom daje legitimitet daljnjoj obradi tih podataka koja se provodi da bi se potkrijepila analitika „velikih podataka". U skladu s predloženom Uredbom jedini je uvjet za tu vrstu obrade obvezno provođenje procjene učinka na zaštitu podataka, ako *je vjerojatno da će se obradom prouzročiti visoki rizik za prava i slobode fizičkih osoba*. Taj je uvjet nedostatan. Isto je tako u suprotnosti s obvezom iz članka 6. da se ta vrsta obrade može provoditi jedino uz privolu korisnika i jedino ako se podaci ne mogu anonimizirati, to jest bez ikakvog jedinstvenog identifikatora. Korisnici često ne mogu odbiti da njihove geolokacijske podatke prikupljaju pružatelji elektroničkih komunikacijskih usluga ako je takvo prikupljanje tehnički potrebno za prijenos komunikacije korisniku ili ako je takva obrada potreba za isporuku tražene (na primjer navigacijske) usluge. U svojim je prethodnim mišljenjima Radna skupina zaključila da su takvi podaci o lokaciji iz pametnih uređaja osobni podaci osjetljive prirode te da koristi od analize tih podataka nemaju prednost nad pravima korisnika na zaštitu povjerljivosti svojih komunikacijskih metapodataka niti imaju prednost nad općim pravima na zaštitu podataka na temelju OUZP-a. Stoga se u toj uvodnoj izjavi mora barem utvrditi da pružatelji moraju ispunjavati obveze iz članka 25. OUZP-a u slučaju daljnje obrade podataka o lokaciji ili drugih metapodataka. To podrazumijeva da se moraju poduzeti barem sljedeće mjere:

   i. upotreba privremenih pseudonima;
   ii. brisanje svake tablice u kojoj su pseudonimi povezani s izvornim identificirajućim podacima;
   iii. agregacija do razine na kojoj se pojedinačni korisnici ne mogu identificirati na temelju njihovih posebnih itinerera i
   iv. brisanje netipičnosti kod kojih bi identifikacija i dalje bila moguća (sve je navedene mjere potrebno primijeniti zajedno).

Konačno, Uredba o e-privatnosti mora obvezati strane uključene u obradu podataka o lokaciji i drugih metapodataka da objave svoje metode anonimizacije i daljnje agregacije, ne dovodeći u pitanje tajnost zajamčenu zakonom. To će nadzornim tijelima i javnosti omogućiti da lako provjere je li izabrana metoda primjerena.

POJAŠNJENJA O NEZATRAŽENIM KOMUNIKACIJAMA

43. Radna skupina predlaže da se pojasne sljedeća pitanja u pogledu nezatraženih komunikacija:
    a. **Tekst zabrane izravnog marketinga bez privole**. U članku 16. stavku 1. predložene Uredbe sada se navodi da se elektroničke komunikacijske usluge „mogu" upotrebljavati za slanje izravnih marketinških komunikacija (uz privolu), ali ne sadržava izričitu zabranu slanja (upućivanja ili prikazivanja) izravnih marketinških komunikacija bez privole. To je u suprotnosti s pristupom u drugim odredbama u kojima je prvo formulirana zabrana te su nakon nje navedena određena posebna izuzeća. Trenutačna formulacija upućuje na popustljiviji pristup (a to najvjerojatnije nije bila namjera). Radna skupina predlaže da se tekst trenutačnog članka 13. stavka 1. Uredbe o e-privatnosti donekle izmijeni: „Upotreba elektroničkih komunikacijskih usluga, uključujući govorne pozive, automatizirane sustave pozivanja i komunikacijske sustave, uključujući poluatomatizirane sustave koji povezuju primatelja s pojedincem, telefaksove, elektroničku poštu, ili drugi način upotrebe elektroničkih komunikacijskih usluga u svrhu prikazivanja izravnih marketinških komunikacija krajnjim korisnicima može se dopustiti fizičkim i pravnim osobama isključivo u odnosu na one krajnje korisnike koji su prethodno dali svoju privolu."
    b. **Područje primjene odredaba o marketinškim komunikacijama i pozivima postojećim kontaktima.** Člankom 16. stavkom 2. predviđa se da ako fizička ili pravna osoba od svojeg potrošača pribavi kontaktne podatke za elektroničku poštu, može se služiti tim podacima za daljnji izravni marketing svojih proizvoda i usluga ako u trenutku prikupljanja i u svakoj poruci jasno ponudi mogućnost besplatnog i jednostavnog prigovora. To se trenutačno odnosi samo na komercijalne kontaktne podatke pribavljene „u kontekstu prodaje proizvoda ili usluge" te za daljnji komercijalni marketing vlastitih proizvoda ili usluga. S obzirom na to da se odredbe o izravnom marketingu jednako primjenjuju i na nekomercijalne promotivne aktivnosti (npr. humanitarnih organizacija ili političkih stranaka), tu bi odredbu trebalo izmijeniti kako bi se jednako primjenjivala i na nekomercijalne organizacije koje kontaktiraju prijašnje pristalice pri promicanju vlastitih sličnih ciljeva ili ideja te bi se na izravne marketinške pozive trebalo primjenjivati isto pravo na prigovor. Osim toga, trebalo bi odrediti rok valjanosti „postojećih potrošača za kontakt" u elektroničkim komunikacijama u komercijalne, humanitarne ili političke svrhe te bi se taj rok trebao primjenjivati i na izravne marketinške pozive. Ako je država članica odlučila primjenjivati sustav prigovora na govorne marketinške pozive, postojanje odnosa s

„postojećim potrošačima za kontakt" ima prednost pred upisom u registar „Ne zovi¨. U tim okolnostima krajnji korisnici nemaju učinkovitu mogućnost spriječiti uznemirujuće pozive koje im upućuju poduzeća ili organizacija s kojima su nekada bili u kontaktu, ali s kojima ne žele više surađivati. Stoga bi, kao osnovno pravilo, Uredbom trebalo utvrditi da izuzeće „postojeći potrošač" vrijedi jednu ili dvije godine, ovisno o legitimnim očekivanjima predmetnih krajnjih korisnika

c. **Primjena pravila o izravnom marketingu na pravne osobe**. Člankom 16. stavkom 5. predložene Uredbe predviđa se da države članice osiguravaju dovoljnu zaštitu legitimnog interesa krajnjih korisnika koji su pravne osobe u pogledu nezatraženih komunikacija. U članku 13. stavku 5. trenutačne Direktive o e-privatnosti opisuju se legitimni interesi pretplatnika koji nisu fizičke osobe. Nejasno je koje su posljedice te promjene u tekstu. U uvodnim izjavama trebalo bi pojasniti da ta promjena ne odražava namjeru pružanja niže razine zaštite. S tim u vezi, zabrana izravnog marketinga bez privole odnosi se na „krajnje korisnike koji su fizičke osobe i koji su dali svoju privolu" (podcrtavanje dodano). Trebalo bi pojasniti da to uključuje fizičke osobe *koje rade za* pravne osobe. S druge strane, privola ne bi bila potrebna za pristupanje pravnim osobama preko generičkih kontaktnih podataka koje su one objavile u tu svrhu (kao što je „info@companyname.eu").

d. **Primjena pravila o izravnom marketingu na one koji djeluju u svojstvu (političkog) predstavnika.** Kako je formuliran, članak 16. može spriječiti da izabranim predstavnicima budu poslane neke komunikacije u kojima se navode komercijalni problemi ili interesi. Trebalo bi pojasniti da se Uredbom ne sprečavaju takve komunikacije.

POJAŠNJENJA O PRIMJENI INSTRUMENATA O TEMELJNIM PRAVIMA

44. **Primjenu Povelje i EKLJP-a na nacionalne zakone o čuvanju podataka** trebalo bi dodatno pojasniti. U uvodnoj izjavi 26. predviđa se da sve mjere država članica za zaštitu javnog interesa, kao što su mjere zakonitog presretanja, moraju biti u skladu s Poveljom (osim s EKLJP-om). To je poželjno jer je u skladu s obrazloženjem u predmetu *Tele2/Watson* da sva nacionalna izuzeća od zaštite koja se pravom EU-a osigurava pri obradi podataka podliježu Povelji (pa se povrede putem nacionalnih propisa mogu stoga uputiti Europskom sudu). Međutim, u članku 11. predložene Uredbe samo se navodi da se ograničenjima područja primjene članaka 5. do 8. predložene Uredbe mora poštovati bit temeljnih prava i sloboda te da ona moraju biti nužna i proporcionalna mjera. Tu bi trebalo navesti izričito upućivanje na Povelju i EKLJP.

45. **Povjerljivost komunikacija zaštićena je i člankom 8. EKLJP-a**. U stavku 1.1. Obrazloženja te u uvodnoj izjavi 1. objašnjava se da se predloženom Uredbom provodi članak 7. Povelje. To je ponovljeno u uvodnoj izjavi 19. Međutim, temeljno pravo na povjerljivost komunikacija nije zaštićeno samo tom odredbom, nego i člankom 8. EKLJP-a. Uključivanjem izričitog upućivanja u članku predložene Uredbe dodatno bi se potvrdilo da će se pri ocjenjivanju (konačne) uredbe morati

uzeti u obzir i sva relevantna sudska praksa Europskog suda za ljudska prava. To je upućivanje već uključeno u uvodnu izjavu 20. (koja se odnosi na terminalnu opremu) i uvodnu izjavu 26. (koja se odnosi na nezakonito presretanje) te je dodatno potkrijepljeno u stavku 2.1. Obrazloženja (o odnosu između Povelje i EKLJP u kontekstu pravnih osoba), ali nije uključeno ni u jedan relevantan članak, kao što je članak 11. stavak 1.

OSTALA POJAŠNJENJA

46. Trebalo bi pojasniti da **su obveze na temelju OUZP-a, kao što su obveze u pogledu režima koji se odnosi na povrede podataka i one u pogledu analiza učinka na zaštitu podataka, i dalje primjenjive** kada stranke obrađuju osobne podatke u kontekstu elektroničkih komunikacijskih podataka. Kao što se u uvodnoj izjavi 5. navodi da je predložena Uredba *lex specialis* u odnosu na OUZP te da bi obradu elektroničkih komunikacijskih podataka trebalo dopustiti samo u skladu s predloženom Uredbom, moglo bi se postaviti pitanje primjenjuju li se određene obveze iz OUZP-a i u kontekstu predložene Uredbe. To je posebno slučaj onda kada bi se predloženu Uredbu moglo tumačiti na način da se njome uvode određene obveze, iako ih obuhvaća i OUZP. Indikativni su primjeri sljedeći:
    (i) predloženom Uredbom propisuje se obveza obavješćivanja o „otkrivenim" sigurnosnim rizicima (članak 17.) (vidjeti i točku 35.), ali OUZP sadržava režim obavješćivanja o povredi podataka (članci 33. i 34.);
    (ii) u predloženoj Uredbi navodi se da je u određenim okolnostima obvezno provođenje analize učinka na zaštitu podataka te savjetovanje s nadzornim tijelom u skladu s OUZP-om (uvodne izjave 17. i 19. i članak 6. stavak 3. točka (b)), iako je OUZP-om već utvrđeno kada se mora provesti analiza učinka na zaštitu podataka, a kada je potrebno savjetovanje (članci 35. i 36.) i
    (iii) nije navedeno da ako netko ispunjuje potrebne uvjete za izuzeće od zabrane obrade na temelju članka 5. predložene Uredbe, ipak mora ispuniti sve relevantne obveze na temelju OUZP-a kad je riječ o obradi osobnih podataka te je na temelju OUZP-a svaki drugi oblik obrade zabranjen. Trebalo bi pojasniti da se stoga ne primjenjuje test sukladnosti utvrđen u članku 6. stavku 4. OUZP-a.
    (iv) Predloženom Uredbom o e-privatnosti ne predviđaju se mehanizmi certificiranja slični onima iz članaka 42. i 43. OUZP-a. S obzirom na to da je područje primjene članka 42. OUZP-a u strogom smislu ograničeno na uspostavljanje mehanizama certificiranja zaštite podataka te žigova i oznaka za dokazivanje usklađenosti s OUZP-om, trebalo bi razmotriti bi li trebalo uvesti usporedivu odredbu kako bi se omogućilo da se za postupke obrade, standarde, proizvode ili usluge izdaje certifikat o usklađenosti s Uredbom o e-privatnosti.

    Kako bi se osiguralo da se taj nedostatak jasnoće ne upotrebljava kao argument za smanjenje razine zaštite na temelju predložene Uredbe, trebalo bi jasno navesti da u svim tim slučajevima i voditelji obrade podataka moraju biti u skladu s OUZP-om.

47. Nadalje, trebalo bi pojasniti da se **zahtjev u pogledu povlačenja privole primjenjuje i u kontekstu zadiranja u terminalnu opremu**. Člankom 8.

stavkom 1. točkom (b) predložene Uredbe predviđa se mogućnost zadiranja u terminalnu opremu krajnjeg korisnika uz privolu. Člankom 9. stavkom 3. zahtijeva se da se krajnjim korisnicima da mogućnost da u svakom trenutku povuku svoju privolu, ali to se primjenjuje samo na privolu za analizu metapodataka i sadržaja. Trebalo bi pojasniti da se ta obveza odnosi i na zadiranje u terminalnu opremu.

48. S tim u vezi, trebalo bi pojasniti da **se podsjećanje na mogućnost povlačenja privole primjenjuje i na privolu danu preko postavki preglednika.** Člankom 9. stavkom 3. zahtijeva se da se krajnje korisnike u periodičnim intervalima od šest mjeseci podsjeća na mogućnost povlačenja privole u svakom trenutku. Iako Radna skupina vjeruje da opće postavke preglednika i drugi softver, uključujući operativne sustave, aplikacije i softverska sučelja za uređaje spojene na internet stvari (tj. ne na temelju posebnih precizno definiranih kontrola) ne mogu biti valjana mjera za davanje privole, s obzirom na to da opće postavke nisu primjeren za davanje posebne privole za posebne scenarije (vidjeti točku 24.), zadane postavke trebale bi korisniku biti lake za upotrebu (vidjeti točku 19.). *Ako* to ostane tako u predloženoj Uredbi, postavke moraju biti dovoljno precizno definirane da kontroliraju svu obradu podataka za koju korisnik daje privolu te da obuhvaćaju svaku funkcionalnost opreme koja može dovesti do obrade podataka. Dodatno, krajnjeg bi korisnika trebalo barem u periodičnim intervalima (od šest mjeseci) podsjećati na mogućnost da promijeni te postavke.

49. Pozdravlja se činjenica da se predloženom Uredbom zahtijeva da softver koji je već stavljen na tržište obavješćuje krajnjeg korisnika o mogućnostima postavki privatnosti (članak 10.). **Međutim, nejasno je kako se to može učinkovito primijeniti na proizvode koji su već na tržištu** i na one proizvode za koje više ne postoji podrška. Osim toga, trebalo bi pojasniti kako će se ta obveza primjenjivati na softver otvorenog koda koji je razvijen na otvoren i decentraliziran način.

50. Trebalo bi pojasniti da **nuđenje mogućnosti blokiranja kolačića (treće strane) na temelju članka 10. predložene Uredbe ima prednost pred izuzećem koje se odnosi na mjerenje broja posjetitelja *web*-mjesta** na temelju članka 8. stavka 1. točke (d). Ili drugim riječima: čak i ako neko *web*-mjesto možda primjenjuje analitiku za mjerenje broja posjetitelja na temelju članka 8. stavka 1. točke (d), korisnici bi ipak trebali imati pravo blokiranja tih tehnologija praćenja u svojim preglednicima.

51. **Trebalo bi pojasniti definiciju (polu)automatiziranih sustava pozivanja i komunikacijskih sustava**. Definicija tog pojma u članku 4. stavku 3. točki (h) predložene Uredbe sadržava upućivanje na sam pojam u drugom dijelu rečenice („uključujući pozive uz uporabu automatiziranih sustava pozivanja i komunikacijskih sustava koji povezuju primatelja s pojedincem"). Predlaže se da se iz definicije izbriše zadnja rečenica te da se definicija u članku 4. stavku 3. promijeni kako bi obuhvaćala pozive s pomoću poluautomatiziranih komunikacijskih sustava, kao što su automatski pozivatelji, koji povezuju primatelja poziva s pojedincem.

52. **Trebalo bi pojasniti informacije koje su „dio pretplate na uslugu"**. U uvodnoj izjavi 14. navodi se da elektronički komunikacijski metapodaci „mogu uključivati informacije koje su dio pretplate na uslugu kada se takve informacije obrađuju u

svrhe prijenosa, distribucije ili razmjene sadržaja elektroničkih komunikacija". Nejasno je što se namjeravalo postići ovom formulacijom.

53. Trebalo bi pojasniti **primjenjivost mehanizama konzistentnosti i suradnje.** U uvodnoj izjavi 38. navodi se da se predložena Uredba oslanja na mehanizam konzistentnosti iz OUZP-a. Osim toga, člankom 18. stavkom 1. predviđa se da se poglavlja VI. i VII. OUZP-a primjenjuju *mutatis mutandis*. U članku 19. navodi se da Europski odbor za zaštitu podataka obavlja zadaće utvrđene u članku 70. OUZP-a. Iako je primjena tih odredaba relativno jasna, ne može se isključiti da će se pojaviti problemi u tumačenju u pogledu ključnih pojmova mehanizama konzistentnosti i suradnje na temelju OUZP-a. Na primjer, mehanizam vodećeg tijela primjenjuje se u onim slučajevima u kojima postoji „prekogranična obrada" (članak 56. stavak 1. OUZP-a): nejasno je kako se to primjenjuje u slučaju zadiranja u terminalnu opremu ili analizu sadržaja ili metapodataka na temelju predložene Uredbe. Stoga se preporučuje pojasniti primjenu tih ključnih pojmova u uvodnoj izjavi te naglasiti da će se sva preostala pitanja u pogledu primjenjivosti navedenih poglavlja OUZP-a u kontekstu predložene Uredbe rješavati tumačenjem odredaba tih poglavlja u skladu s njihovom namjenom. Osim toga, preporučuje se pojasniti da se članak 70. primjenjuje *mutatis mutandis* na Europski odbor za zaštitu podataka u kontekstu predložene Uredbe (to sad nije navedeno u uvodnoj izjavi).

*** * ***