



17/SL

WP 247

**Mnenje št. 01/2017 o
predlogu uredbe o zasebnosti in elektronskih komunikacijah (2002/58/ES)**

Sprejeto 4. aprila 2017

Ta delovna skupina je bila ustanovljena v skladu s členom 29 Direktive 95/46/ES. Je neodvisen evropski svetovalni organ na področju varstva podatkov in zasebnosti. Naloge skupine so opredeljene v členu 30 Direktive 95/46/ES in členu 15 Direktive 2002/58/ES.

Naloge sekretariata opravlja Direktorat C (Temeljne pravice in pravna država) Evropske komisije, Generalni direktorat za pravosodje in potrošnike, B-1049 Bruselj, Belgija, pisarna št. MO-59 05/035.

Spletišče: http://ec.europa.eu/justice/data-protection/index_en.htm

DELOVNA SKUPINA ZA VARSTVO POSAMEZNIKOV PRI OBDELAVI OSEBNIH PODATKOV,

ustanovljena z Direktivo Evropskega parlamenta in Sveta 95/46/ES z dne 24. oktobra 1995, je –

ob upoštevanju členov 29 in 30 Direktive,

ob upoštevanju Poslovnika delovne skupine –

SPREJELA NASLEDNJE MNENJE:

POVZETEK

Delovna skupina pozdravlja predlog Evropske komisije z dne 10. januarja 2017 za uredbo o zasebnosti in elektronskih komunikacijah. Pozdravlja tudi, da je bila kot regulativni instrument **izbrana uredba**. To zagotavlja enotna pravila po vsej EU ter jasnost tako za nadzorne organe kot za organizacije. Prispeva tudi k zagotavljanju skladnosti s Splošno uredbo o varstvu podatkov. K tej skladnosti prispeva tudi odločitev, da bo za izvrševanje pravil o zasebnosti in elektronskih komunikacijah **pooblaščen isti organ, ki je že odgovoren za spremljanje skladnosti s Splošno uredbo o varstvu podatkov**.

Pozitivna je tudi odločitev glede (ohranitve) **dopolnilnega pravnega instrumenta**. Varstvo zaupne komunikacije in terminalske opreme ima posebne značilnosti, ki v Splošni uredbi o varstvu podatkov niso obravnavane. Zato so potrebne dopolnilne določbe v zvezi s tovrstnimi storitvami, ki bodo zagotovile ustrezno varstvo temeljne pravice do zasebnosti in zaupnosti komunikacij, vključno z zaupnostjo terminalske opreme. Delovna skupina v zvezi s tem odločno podpira **načelni pristop široko opredeljenih prepovedi in ozko opredeljenih izjem**, ki je bil uporabljen v predlogu uredbe, in **ciljno usmerjeno uporabo pojma privolitve**.

Delovna skupina pozdravlja razširitev področja uporabe predloga uredbe, da bi **vkjučevala ponudnike povrhnjih spletnih storitev (v nadaljnjem besedilu: OTT)**, ki so funkcionalno enakovredne bolj tradicionalnim komunikacijskim sredstvom in lahko zato podobno vplivajo na zasebnost državljanov EU in njihovo pravico do zaupnih komunikacij. Pozitivno je tudi, da so v predlogu uredbe jasno obravnavani **vsebina in povezani metapodatki** ter da je priznано, da **lahko metapodatki razkrijejo zelo občutljive podatke**.

Kljub temu delovna skupina opozarja na štiri **zelo problematična** področja. Predlog uredbe bi znižal raven varstva, ki jo zagotavlja Splošna uredba o varstvu podatkov, v zvezi s **sledenjem lokaciji terminalske opreme, pogoji, pod katerimi je dovoljena analiza vsebine in metapodatkov, privzetimi nastavitvami terminalske opreme in programske opreme ter zidovi sledenja**. Delovna skupina v tem mnenju predstavlja posebne predloge za zagotovitev, da bo uredba o zasebnosti in elektronskih komunikacijah zagotavljala enako ali višjo raven varstva, ki bo ustrezala občutljivi naravi komunikacijskih podatkov (vsebine in metapodatkov).

Sledenje prek Wi-Fi v skladu s Splošno uredbo o varstvu podatkov se bo glede na okoliščine in namene zbiranja podatkov verjetno izvajalo na podlagi privolitve ali le, če bodo zbrani osebni podatki anonimizirani. V zadnjem primeru morajo biti izpolnjeni naslednji štirje pogoji: namen zbiranja podatkov iz terminalske opreme je omejen na golo statistično štetje, sledenje je časovno in prostorsko omejeno na obseg, ki je izrecno potreben za ta namen, podatki se izbrišejo ali anonimizirajo takoj za tem in na voljo so učinkovite možnosti zavrnitve. Evropska komisija naj spodbuja tehnični standard za mobilne naprave, da bi samodejno opozarjale na nasprotovanje takemu sledenju.

Analiza vsebine in metapodatkov bi morala temeljiti na tem, da je obdelava komunikacijskih podatkov brez privolitve vseh končnih uporabnikov (pošiljatelj in prejemnik) prepovedana. Da bi ponudnikom omogočili zagotavljanje storitev, ki jih izrecno zahteva uporabnik, kot so na primer funkcionalnost iskanja in indeksiranja ali storitve

pretvorbe besedila v govor, bi bilo treba uvesti domačo izjemo za obdelavo vsebine in metapodatkov v izključno osebne namene uporabnika.

V zvezi s **privolitvijo v sledenje** delovna skupina poziva k izrecni prepovedi zidov sledenja, tj. možnosti „vzemi ali pusti“, ki uporabnike silijo, da privolijo v sledenje, če želijo uporabljati storitev.

Delovna skupina poleg tega priporoča, naj terminalska oprema in programska oprema **privzeto ponudita nastavitve, ki varujejo zasebnost**, in uporabnikom jasno omogočita, da te privzete nastavitve med nameščanjem potrdijo ali spremenijo. Nastavitve morajo biti med uporabo lahko dostopne. Uporabnikom je treba omogočiti, da svojo izrecno privolitev izrazijo v okviru nastavitve brskalnika. Nastavitve zasebnosti ne bi smele biti omejene na posege tretjih strani ali piškotke. Delovna skupina močno priporoča, naj upoštevanje standarda *brez sledenja* postane obvezno.

Delovna skupina je opredelila tudi druga problematična področja, na primer v zvezi s področjem uporabe, zaščito terminalske opreme in neposrednim trženjem. Ne nazadnje je delovna skupina opredelila vprašanja, ki bi jih bilo treba pojasniti, da bi bolje zaščitili končne uporabnike in vzpostavili večjo pravno varnost za vse udeležene zainteresirane strani.

KAZALO

1. UVOD.....	6
2. POZITIVNI VIDIKI PREDLOGA UREDBE	6
<i>Uskladitev na ravni EU, uskladitev upravnih glob in izključno izvrševanje s strani organov za varstvo podatkov.....</i>	<i>6</i>
<i>Razširitev področja uporabe v primerjavi z Direktivo o zasebnosti in elektronskih komunikacijah</i>	<i>8</i>
<i>Ciljno usmerjena uporaba pojma privolitve</i>	<i>10</i>
3. ZELO PROBLEMATIČNA PODROČJA	10
<i>Predlog uredbe spodkopava varstvo v skladu s Splošno uredbo o varstvu podatkov.</i>	<i>10</i>
4. DRUGA PROBLEMATIČNA PODROČJA	16
<i>Razširiti je treba ozemeljsko in vsebinsko veljavnost</i>	<i>16</i>
<i>Okrepiti je treba zaščito terminalske opreme</i>	<i>17</i>
<i>Neposredno trženje</i>	<i>21</i>
<i>Časovni razpored.....</i>	<i>23</i>
<i>Drugi pomisleki</i>	<i>23</i>
5. PREDLOGI ZA POJASNILA ZA ZAGOTOVITEV PRAVNE VARNOSTI	26
<i>Pojasnilo o področju uporabe</i>	<i>26</i>
<i>Pojasnilo o pojmu in uporabi privolitve</i>	<i>29</i>
<i>Pojasnilo o podatkih o lokaciji in drugih metapodatkih.....</i>	<i>30</i>
<i>Pojasnilo o nepovabljenih sporočilih</i>	<i>31</i>
<i>Pojasnilo o uporabi instrumentov na področju temeljnih pravic</i>	<i>33</i>
<i>Druga pojasnila</i>	<i>33</i>

1. UVOD

1. Delovna skupina za varstvo podatkov iz člena 29 (v nadaljnjem besedilu: delovna skupina ali delovna skupina iz člena 29) pozdravlja predlog Evropske komisije za uredbo o zasebnosti in elektronskih komunikacijah (v nadaljnjem besedilu: predlog uredbe ali uredba o zasebnosti in elektronskih komunikacijah) ¹, katere cilj je nadomestiti Direktivo o zasebnosti in elektronskih komunikacijah ².
2. Mnogi vidiki predloga uredbe so pozitivni in Evropska komisija je z uvedbo predloga uredbe naredila pomemben korak, vendar je mogoče to uredbo dodatno izboljšati. To bi pripomoglo k boljšemu varstvu končnih uporabnikov in večji pravni varnosti za vse udeležene zainteresirane strani.
3. Delovna skupina je zato opredelila več problematičnih področij in pripravila priporočila za pojasnila, ki jih morata Evropski parlament in Svet ministrov obravnavati na razpravi o predlogu uredbe. V tem mnenju bodo najprej obravnavani pozitivni vidiki predloga uredbe, nato pa poudarjena problematična področja in področja, ki jih je treba pojasniti.

2. POZITIVNI VIDIKI PREDLOGA UREDBE

USKLADITEV NA RAVNI EU, USKLADITEV UPRAVNIH GLOB IN IZKLJUČNO IZVRŠEVANJE S STRANI ORGANOV ZA VARSTVO PODATKOV

4. Delovna skupina pozdravlja, **da je bila kot regulativni instrument izbrana uredba**. To zagotavlja enotna pravila po vsej EU (z nekaterimi izjemami, ki so obravnavane v nadaljevanju). To zagotavlja jasnost za nadzorne organe in organizacije. Poleg tega to glede na ključno vlogo Splošne uredbe o varstvu podatkov ³ v predlogu uredbe pomaga zagotavljati usklajenost obeh instrumentov. Pozitivna je tudi **odločitev glede (ohranitve) dopolnilnega pravnega instrumenta**. Varstvo zaupne komunikacije in terminalske opreme ima posebne značilnosti, ki v Splošni uredbi o varstvu podatkov niso obravnavane. Zato so potrebne dopolnilne določbe v zvezi s tovrstnimi storitvami, ki bodo zagotovile ustrezno varstvo te temeljne pravice. Delovna skupina v zvezi s tem **podpira tudi načelni pristop široko opredeljenih prepovedi in ozko**

¹ Predlog Uredba Evropskega parlamenta in Sveta o spoštovanju zasebnega življenja in varstvu osebnih podatkov na področju elektronskih komunikacij ter razveljavitvi Direktive 2002/58/ES (uredba o zasebnosti in elektronskih komunikacijah), 2017/0003 (COD), URL: <http://eur-lex.europa.eu/legal-content/SL/TXT/PDF/?uri=CELEX:52017PC0010&qid=1508854426717&from=SL>.

² Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah), UL L 201, 31.7.2002, str. 37–47, URL: <http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=celex:32002L0058>.

³ Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov), UL L 119, 4.5.2016, str. 1–88, URL: <http://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679>.

opredeljenih izjem, ki je bil uporabljen v predlogu uredbe, in meni, da bi bilo treba preprečiti uvedbo nedoločenih izjem v skladu s členom 6 Splošne uredbe o varstvu podatkov in zlasti členom 6(f) navedene uredbe (razlog zakonitega interesa).

5. Dejstvo, da bo **ta pravila izvrševal isti organ, ki je že odgovoren za spremljanje skladnosti s Splošno uredbo o varstvu podatkov**, bo dodatno prispevalo k usklajenosti obeh instrumentov. Glede na povezavo med varstvom osebnih podatkov ter varstvom zaupne komunikacije in terminalske opreme je koristno, da se za izvrševanje določb iz predloga uredbe pooblasti isti nadzorni organ, ki je že odgovoren za izvajanje Splošne uredbe o varstvu podatkov (uvodna izjava 38 in člen 18 predloga uredbe). Poleg tega Sodišče Evropske unije⁴ v sodni praksi potrjuje, da mora biti nadzorni organ nujno neodvisen, kot je predpisano v členu 7 Listine EU o temeljnih pravicah (v nadaljnjem besedilu: Listina). V praksi pa bi to povzročilo veliko dodatnega dela za organe za varstvo podatkov, ki ne bodo mogli jamčiti za izpolnjevanje svojih dolžnosti, če ne bodo pridobljena dodatna proračunska sredstva. Zato pozdravljajo uvodno izjavo 38 predloga uredbe, v kateri je poudarjeno, da bi bilo treba vsakemu nadzornemu organu zagotoviti dodatne finančne in človeške vire, prostore in infrastrukturo, ki jih potrebuje za učinkovito opravljanje nalog na podlagi nove uredbe. Pozdravljajo tudi, da člen 18(2) zagotavlja pravno podlago za sodelovanje med nadzornimi organi iz predloga uredbe in nacionalnimi regulativnimi organi iz predloga direktive o Evropskem zakoniku o elektronskih komunikacijah⁵.
6. Glede na tesno povezavo med predlogom uredbe in Splošno uredbo o varstvu podatkov je treba pozdraviti tudi **uskladitev upravnih glob iz predloga uredbe z upravnimi globami iz Splošne uredbe o varstvu podatkov**. Dejavnosti, ki spadajo na področje uporabe predloga uredbe, so precej občutljive in med drugim vključujejo poseganje v zaupno komunikacijo in terminalsko opremo. Višina upravnih glob bi morala biti sorazmerna s tem občutljivim okvirom. Prav zaradi tega je pomembna usklajenost na ravni EU, da bi zagotovili enako raven varstva po vsej regiji. Člen 23 predloga uredbe predvideva učinkovite upravne globe za kršitev njenih določb, ki so podobno visoke kot upravne globe, določene za kršitev pravil iz Splošne uredbe o varstvu podatkov, razen za nekatere točke (glej odstavek 38).
7. Pozdraviti je treba tudi **izključitev posebnih pravil glede obveščanja o kršitvah varstva osebnih podatkov** iz te zakonodaje, s katero se bo preprečilo nepotrebno prekrivanje z zahtevami glede kršitev varstva osebnih podatkov iz Splošne uredbe o varstvu podatkov.
8. **Pozitivno je tudi, da je pozornost zdaj namenjena zagotavljanju enakovredne ravni varstva vsem končnim uporabnikom**, saj se s predlogom uredbe odpravlja

⁴ Glej npr. Sodišče Evropske unije, 6. oktober 2015, C-362/14 (varni pristan), točka 41, in Sodišče Evropske unije, 21. december 2016, C-203/15 in C-698/15 (Tele2/Watson), točka 123.

⁵ Predlog Direktiva Evropskega parlamenta in Sveta o Evropskem zakoniku o elektronskih komunikacijah (prenovitev), 2016/0288 (COD), 12.10.2016, URL: http://eur-lex.europa.eu/legal-content/SL/ALL/?uri=comnat:COM_2016_0590_FIN.

pojem razlikovanja med „naročniki“ in drugimi uporabniki elektronskih komunikacijskih storitev.

RAZŠIRITEV PODROČJA UPORABE V PRIMERJAVI Z DIREKTIVO O ZASEBNOSTI IN ELEKTRONSKIH KOMUNIKACIJAH

9. Delovna skupina pozdravlja **razširitev področja uporabe predloga uredbe, da bi vključevala ponudnike povrhnjih spletnih storitev**, ki so funkcionalno enakovredne bolj tradicionalnim komunikacijskim sredstvom in lahko zato podobno vplivajo na zasebnost državljanov EU in njihovo pravico do zaupnih komunikacij. Delovna skupina zlasti pozdravlja, da na področje uporabe uredbe zdaj spadajo vse kategorije povrhnjih spletnih storitev (OTT0, OTT1 in nekatere OTT2)⁶, saj ne zajema le tradicionalnih komunikacijskih sredstev (OTT0), temveč tudi funkcionalno enakovredne storitve (OTT1), kot je navedeno v členu 8(1)(c) predloga uredbe. Pozitivno je tudi, da so poleg opredelitev iz Evropskega zakonika o elektronskih komunikacijah vključene nekatere storitve OTT2, kadar zagotavljajo pomožno medosebno in interaktivno komunikacijo, ki je dejansko povezana z drugo storitvijo, na primer v igrah, aplikacijah za zmenke ali na spletiščih za recenzije (člen 4(2) predloga uredbe). Podobno je treba pozdraviti tudi **pojasnilo, da varstvo zajema tudi interakcijo stroj-stroj**. V uvodni izjavi 12 je pojasnjeno, da naprave, ki komunicirajo med sabo, spadajo v obseg varstva, ki ga zagotavlja predlog uredbe. To je zaželeno, saj take komunikacije pogosto vsebujejo informacije, zaščitene v okviru pravic do zasebnosti. Pojasnila pa bi se lahko uporaba (glej odstavek 40h).
10. Pozitivno je tudi, da so **v predlogu uredbe jasno obravnavani vsebina in povezani metapodatki**. V uvodni izjavi 14 je pojasnjeno, da mora biti opredelitev „elektronskih komunikacijskih podatkov“ iz člena 4(3)(a) dovolj široka, da bi zajela vso vsebino in povezane metapodatke ne glede na, na primer, način prenosa signalov. Vendar delovna skupina v odstavku 39 z zaskrbljenostjo poudarja, da se o tej obstoječi opredelitvi „elektronskih komunikacijskih podatkov“ še vedno razpravlja. V skladu s to razširitvijo področja uporabe je po mnenju delovne skupine nujno, da se doda **priznanje, da lahko metapodatki razkrijejo zelo občutljive podatke** (glej odstavek 2.2 obrazložitvenega memoranduma in uvodno izjavo 2). Delovna skupina pozdravlja, da Evropska komisija s tem upošteva premisleke Sodišča Evropske unije v zadevah Digital Rights Ireland in Tele2/Watson. Delovna skupina iz člena 29 tudi ceni **priznanje, da je analiza vsebine obdelava z velikim tveganjem**. V uvodni izjavi 19 in členu 6(3)(b) je določena logična pravna domneva, da je skeniranje vsebine obdelava z velikim tveganjem v skladu s členom 35 Splošne uredbe o varstvu podatkov in da očitno ne glede na obstoj velikega preostalega tveganja vedno zahteva predhodno posvetovanje z (glavnim) organom za varstvo podatkov. Poleg tega je

⁶ Dodatna razlaga teh pojmov je na voljo v poročilu BEREC o povrhnjih spletnih storitvah (*Report on OTT*

Services), BoR (16) 35, 29. januar 2016, str. 15 in 16, URL:

http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services.

Upoštevati je treba tudi pripombo v poročilu, da so kategorije le pojmi za uporabo v razpravi o pregledu, in ne pravni pojmi.

delovna skupina zaskrbljena glede področja uporabe opredelitve „metapodatkov“ in dejstva, da za analizo metapodatkov ne veljajo enake obvezne zahteve glede ocene učinka v zvezi z varstvom podatkov (glej odstavek 33 in 46).

11. Pozdraviti je treba tudi nadaljnje **priznavanje pomena anonimizacije**. V Direktivi o zasebnosti in elektronskih komunikacijah je že bila priznana pomembna vloga ukrepov anonimizacije pri zagotavljanju združljivosti (v členu 6(1) navedene direktive je na primer navedeno, da morajo biti podatki o prometu izbrisani ali predelani v anonimne, potem ko niso več potrebni za namen prenosa sporočila). V členu 6(2)(c) in 6(3)(b) predloga uredbe je izjema od prepovedi obdelave metapodatkov in vsebine dovoljena na podlagi privolitve, če *zadevnega namena ali namenov ne bi bilo mogoče izpolniti z obdelavo anonimiziranih informacij*. Zahteva po takih ukrepih, ki varujejo zasebnost, poleg obvezne privolitve uporabnikov te uporabnike varuje pred neupravičeno obdelavo. Kljub temu je delovna skupina hkrati zelo zaskrbljena, da se sprejetje takih tehnik anonimizacije ne bi zahtevalo pri sledenju lokaciji uporabnikov prek mobilne opreme (glej odstavek 17). Tudi v primeru izvedbe ukrepov anonimizacije bi morali ponudniki vedno izvesti oceno učinka v zvezi z varstvom podatkov (glej odstavek 33 in 46), zato delovna skupina poziva k uvedbi dodatne obveznosti objave, kako se podatki anonimizirajo in združujejo (glej odstavek 42b).
12. Še ena pozitivna stran je **široka zasnova varstva terminalske opreme**. V uvodni izjavi 20 in členu 8 je določeno, da tehnologije, ki se uporabljajo za dostop do terminalske opreme, niso ustrezne: za vsako poseganje v terminalsko opremo, vključno z uporabo njenih obdelovalnih zmogljivosti, je potrebna privolitev končnega uporabnika (z nekaterimi izjemami). Evropska komisija je kolegialno potrdila, da v to določbo spada „zajem prstnega odtisa naprave“. Delovna skupina pozdravlja tudi, da je neupoštevanje osebnih preferenc, ki jih je posameznik izrazil v **nastavitvah brskalnika**, s strani tretje osebe **izvršljivo** proti njej, kot je opisano v uvodni izjavi 22. To je koristno v primerih, v katerih tretja oseba (npr. oglaševalsko omrežje) teh nastavitvev ne upošteva. Tudi to bi bilo treba določiti v ustrezni določbi predloga uredbe.
13. Nazadnje je treba pozdraviti tudi nadaljnjo **vključenost pravnih oseb v področje uporabe predloga uredbe** (glej odstavek 2.2 obrazložitvenega memoranduma, uvodne izjave 3, 33 in 42 ter člena 1 in 15 ter člen 16(5)). To že velja v okviru Direktive o zasebnosti in elektronskih komunikacijah, vendar ker bodo organi za varstvo podatkov pooblaščen za izvajanje novih pravil, je koristno, da se to posebej poudari. To organom za varstvo podatkov omogoča, da ukrepajo, kadar so pravne osebe žrtve kršitve, na primer kadar družbe prejmejo neželeno elektronsko pošto ali kadar se njihova komunikacija neopazno nadzoruje. Delovna skupina z zaskrbljenostjo poudarja tudi, da ni jasna uporaba privolitve za pravne osebe (glej odstavek 41a). Poleg tega ni jasno, kaj pomeni „zakoniti interes“ pravnih oseb v primeru neposrednega trženja (glej odstavek 43c).

14. Delovna skupina pozdravlja dodatno kategorijo izboljšanj, povezanih z uporabo in razlago pojma privolitve. Pozdraviti je treba **pojasnilo, da sta dostop do spleta in (mobilna) telefonija osnovni storitvi ter da ponudniki teh storitev svojih strank ne smejo „siliti“, da privolijo v obdelavo podatkov, ki ni potrebna za zagotovitev osnovne storitve**. Zlasti v uvodni izjavi 18 je poudarjeno, da je treba osnovni širokopasovni dostop do spleta in govorne komunikacijske storitve šteti za osnovne storitve, kar glede na odvisnost ljudi od dostopa do teh storitev pomeni, da privolitev v obdelavo njihovih komunikacijskih podatkov za take dodatne namene (npr. obdelava za oglaševanje ali trženje) ne more biti veljavna. Hkrati je delovna skupina zaskrbljena, da je to pojasnilo preveč omejeno. Za osnovne storitve se lahko štejejo tudi storitve nekaterih ponudnikov povrhnjih spletnih storitev, zato bi bilo treba v uredbi o zasebnosti in elektronskih komunikacijah izrecno prepovedati možnosti „vzemi ali pusti“ tudi v drugih okoliščinah (glej odstavek 20).
15. Pozitivno je tudi, da **je usklajena zahteva glede privolitve v vključitev osebnih podatkov fizičnih oseb v direktorije**. V skladu s členom 15 predloga uredbe je obdelava podatkov v javnih direktorijih dovoljena le, če fizične osebe vanjo privolijo in če je pravnim osebam omogočeno, da ji nasprotujejo. To je podrobneje pojasnjeno v uvodni izjavi 31, v kateri je navedeno, da je treba pri tej privolitvi določiti, katere kategorije osebnih podatkov bodo vključene v direktorij. Vendar delovna skupina z zaskrbljenostjo ugotavlja, da bi bilo lahko v predlogu uredbe jasneje določeno, da bo za iskanje in povratno iskanje potrebno posebno soglasje (glej odstavek 37).
16. Cenjena je tudi **nova namenska izjema za nevsiljivo poseganje v terminalsko opremo**. Delovna skupina iz člena 29 meni, da je koristno, da je v predlogu uredbe pojasnjeno, da prepoved ne velja za merjenje spletnega prometa (z ozko izjemo, da tako merjenje izvaja ponudnik storitve informacijske družbe, ki jo je zahteval končni uporabnik, glej člen 8(1)(d) predloga uredbe). Glej tudi uvodno izjavo 21. Vendar delovna skupina predlaga, da se uporabi tehnološko nevtralnejša opredelitev in pojasni uporaba te izjeme (glej odstavek 25).

3. ZELO PROBLEMATIČNA PODROČJA

PREDLOG UREDBE SPODKOPAVA VARSTVO V SKLADU S SPLOŠNO UREDBO O VARSTVU PODATKOV.

Kot je navedeno zgoraj, predlog uredbe vsebuje številne ključne izboljšave. Kljub temu pa obstajajo tudi različno tehtna problematična področja. Delovna skupina v tem oddelku obravnava štiri področja, v zvezi s katerimi je **resno zaskrbljena**. Naslednje določbe **spodkopavajo raven varstva, ki jo zagotavlja Splošna uredba o varstvu podatkov**:

17. Obveznosti glede sledenja lokaciji terminalske opreme iz predloga uredbe bi morale biti usklajene z zahtevami Splošne uredbe o varstvu podatkov.

Člen 8(2)(b) predloga uredbe kot pogoj za zbiranje informacij, ki jih oddaja terminalska oprema, zahteva le objavo obvestila in izvedbo varnostnih ukrepov. V tem členu je določeno tudi, da mora oseba, odgovorna za to zbiranje, navesti vse ukrepe, ki jih lahko končni uporabniki sprejmejo, da zbiranje čim bolj omejijo ali preprečijo. Ta člen tako daje vtis, da lahko organizacije zbirajo informacije, ki jih oddaja terminalska oprema, za sledenje fizičnemu gibanju posameznikov (kot je „sledenje prek Wi-Fi“ ali „sledenje prek tehnologije Bluetooth“) brez privolitve zadevnega posameznika. Oseba, ki zbira te podatke, bi zahteve očitno lahko izpolnjevala tako, da bi uporabnike obvestila, naj izklopijo naprave, kadar ne želijo, da jim sledi. Tak pristop bi bil v nasprotju z osnovnim ciljem telekomunikacijske politike Evropske komisije, ki je vsem Evropejcem po nizki ceni zagotoviti čezmejno mobilno spletno povezavo visokih hitrosti z močnim varstvom zasebnosti.

Poleg tega predlog uredbe ne uvaja nobenih jasnih omejitev glede področja uporabe zbiranja podatkov ali poznejših dejavnosti obdelave. V zvezi s tem bi bilo treba poudariti, da so ti naslovi MAC osebni podatki tudi po izvedbi varnostnih ukrepov, kot je zgoščevanje. Ker niso bile uvedene dodatne zahteve ali omejitve, je raven varstva teh osebnih podatkov v okviru predloga uredbe precej nižja kot v okviru Splošne uredbe o varstvu podatkov, v skladu s katero bi morale biti tako sledenje pošteno, zakonito in pregledno. V uvodni izjavi 25 je nekoristno poudarjeno, da nekatere od funkcionalnosti sledenja prek Wi-Fi ne pomenijo velikih tveganj za zasebnost, druge pa, na primer tiste, ki zajemajo sledenje posameznikom v daljšem časovnem obdobju. Čeprav delovna skupina ceni priznanje, da zadnjenavedene funkcionalnosti pomenijo velika tveganja za zasebnost, ni koristno, da se brez nadaljnje ocene okoliščin in sorazmernosti obdelave že vnaprej določi, da pri nekaterih drugih funkcionalnostih ni tako. Tako oceno bi bilo treba izvesti ob upoštevanju naslednjih pogojev v zvezi z neanonimiziranim sledenjem prek Wi-Fi.

Sledenje v skladu s Splošno uredbo o varstvu podatkov se bo glede na okoliščine in namene zbiranja podatkov verjetno izvajalo na podlagi privolitve ali le, če bodo zbrani osebni podatki anonimizirani. Zaželeno je, da se ta anonimizacija izvede takoj po zbiranju. Če podatkov zaradi namenov njihovega zbiranja ni mogoče takoj anonimizirati, se lahko v obdobju, v katerem niso anonimizirani, obdelujejo le pod naslednjimi pogoji: (i) namen zbiranja podatkov iz terminalske opreme je omejen na golo statistično štetje (glej primere v nadaljevanju), (ii) sledenje je časovno in prostorsko omejeno na obseg, ki je izrecno potreben za ta namen, (iii) podatki se izbrišejo ali anonimizirajo takoj za tem in (iv) na voljo je učinkovita možnost zavrnitve. Upravljavci morajo seveda v vseh okoliščinah izpolnjevati zahtevo glede zagotavljanja ustreznih informacij.

Delovna skupina je zaskrbljena, da bi morebitna zagotovitev možnosti zavrnitve po posamezni organizaciji, ki te podatke zbira, glede na povečanje uporabe takih tehnologij sledenja, ki ga izvajajo organizacije zasebnega in javnega sektorja, nesprejemljivo obremenila državljane. Zato evropskega zakonodajalca poziva, naj spodbuja razvoj tehničnih standardov za naprave, da bi samodejno opozarjale na nasprotovanje takemu sledenju, in zagotovi izvršljivost upoštevanja tega opozorila.

Privolitev v skladu s Splošno uredbo o varstvu podatkov bi bila na primer verjetno potrebna, kadar upravljavec podatkov zbira in hrani naslove MAC naprav, ki so posredno določljivi (prek Wi-Fi ali tehnologije Bluetooth), in izračuna lokacijo uporabnika, da bi sledil njegovi lokaciji v daljšem časovnem obdobju, na primer v več trgovinah. To zlasti velja, kadar se tako sledenje izvaja na javnih mestih, kjer uporabniki legitimno pričakujejo, da ne bodo določeni ali izsledeni, vendar se prav tam zbirajo naslovi MAC mimoidočih. Taka privolitev se na primer lahko pridobi z aplikacijo, ki uporabnike poziva, naj omogočijo sledenje svoji lokaciji na nekaterih območjih v zameno za komercialne ponudbe, z zagotovitvijo prijavnih točk na nekaterih lokacijah ali prek modula privolitve na dostopnih točkah Wi-Fi.

Upravljalci podatkov lahko informacije, ki jih oddaja terminalska oprema, za namene sledenja fizičnemu gibanju zadevnih posameznikov brez njihove privolitve obdelujejo le v nekaterih okoliščinah, na primer pri štetju strank na neki lokaciji ali zbiranju oddanih podatkov na obeh straneh varnostne kontrolne točke za prikaz čakalne dobe. V obeh primerih pa je treba podatke izbrisati ali anonimizirati takoj, ko je izpolnjen statistični namen. To pomeni, da morajo biti naslovi MAC naprav obiskovalcev na neki lokaciji, kot je trgovina, anonimizirani takoj, ko so zbrani, pri čemer se naslovi MAC ne smejo trajno shraniti, in tako, da je ponovna določitev tehnično izključena. Pri izračunavanju čakalne dobe bi bilo treba naslove MAC izbrisati ali anonimizirati takoj, ko podatki niso več pomembni za izračun čakalne dobe (na primer, ker je obiskovalec prispel na drugo stran kontrolne točke ali je zapustil vrsto).

Poleg tega bi moral upravljavec podatkov izpolnjevati zahteve glede najmanjšega obsega podatkov (na primer, da se sledenje ne izvaja 24 ur na dan sedem dni v tednu, kadar je namen omejen na delovni čas trgovine in/vzorčenje v intervalih). Upravljalci podatkov morajo sprejeti tudi druge blažilne ukrepe za zagotovitev, da učinka na pravice uporabnikov do zasebnosti ne bo ali bo zelo majhen, na primer zaradi varstva zasebnosti ljudi, ki živijo v bližini zbirnega mesta.

Dejstvo, da je v členu 8(2) predloga uredbe predvidena le objava obvestila, je toliko bolj nenavadno glede na ugotovitev iz uvodne izjave 20, da se lahko informacije, povezane z napravo končnega uporabnika, za namene določitve in sledenja zbirajo tudi na daljavo ter da lahko taka obdelava v skladu s predlogom uredbe resno posega v zasebnost teh končnih uporabnikov. Poleg tega ta obveznost ne presega obveznosti glede informacij, ki je že predvidena v členih 13 in 14 Splošne uredbe o varstvu podatkov. Resnost posega v zasebnost s sledenjem še dodatno povečuje morebitni dostop drugih do zbranih podatkov, na primer to, da lahko organi pregona končne uporabnike določijo na podlagi shranjenega(-ih) naslova(-ov) MAC, ki ga (jih) oddajajo njihove mobilne naprave.

18. Pogoje, pod katerimi je dovoljena analiza vsebine in metapodatkov, je treba podrobneje opredeliti.

V členu 6 predloga uredbe so za metapodatke in vsebino predvidene različne ravni varstva. Delovna skupina iz člena 29 te razlike ne podpira, saj sta zelo občutljivi obe kategoriji podatkov. Za metapodatke in vsebino bi bilo torej treba predvideti enako

visoko raven varstva. Izhajati bi bilo treba iz tega, da je obdelava metapodatkov in vsebine brez privolitve vseh končnih uporabnikov (tj. pošiljatelja in prejemnika) prepovedana.

Določena obdelava brez privolitve pa se lahko dovoli, če je nujno potrebna za naslednje namene:

- Ponudniki lahko elektronske komunikacijske podatke obdelujejo za namene iz člena 6(1)(a) in (b) ter 6(2)(a) in (b) predloga uredbe⁷.
- Pojasniti bi bilo treba, da se lahko za odkrivanje ali preprečevanje zlorabe elektronskih komunikacijskih storitev (člen 6(2)(b)) štejejo kot nujno potrebne tudi nekatere tehnike za odkrivanje/filtriranje neželene elektronske pošte in odpravljanje botnetov. V zvezi s filtriranjem neželene elektronske pošte bi bilo treba končnim uporabnikom, ki prejemajo to pošto, omogočiti posamezno zavrnitev, če je to tehnično izvedljivo.
- Pojasniti bi bilo treba, da lahko v okvir izjeme „potrebno zaradi zaračunavanja“ (glej člen 6(2)(b)) spada tudi analiza elektronskih komunikacijskih podatkov za namene storitev za stranke. Zadevni metapodatki se lahko shranijo do konca obdobja, med katerim se lahko obračun zakonito izpodbija ali sprožijo postopki za pridobitev plačila v skladu z nacionalno zakonodajo. Zadevni podatki (kot so naslovi URL) se lahko hranijo le na zahtevo končnega uporabnika in le za obdobje, ki je nujno potrebno za rešitev spora glede obračuna (kar pomeni, da bi bilo treba spremeniti člen 7(3)).
- Omogočiti bi bilo treba obdelavo elektronskih komunikacijskih podatkov za namene zagotavljanja storitev, ki jih je izrecno zahteval končni uporabnik, kot so funkcionalnost iskanja ali indeksiranja ključnih besed, virtualni pomočniki, pretvorniki besedila v govor in prevajalske storitve. Zato bi bilo treba uvesti izjemo za analizo takih podatkov za povsem individualno (domačo) uporabo in individualno uporabo, povezano z delom⁸. Ta analiza bi bila torej mogoča brez privolitve vseh končnih uporabnikov, toda s privolitvijo končnega uporabnika, ki je storitev zahteval. Taka posebna privolitev bi poleg tega ponudniku preprečila uporabo teh podatkov za druge namene.

To pomeni, da je za analizo vsebine in/ali metapodatkov za vse druge namene, kot so analitika, oblikovanje profilov, oglaševanje na podlagi vedenjskih vzorcev ali drugi nameni za (tržno) korist ponudnika, potrebna privolitev vseh končnih uporabnikov,

⁷ Glede potrebe po izpolnjevanju zahtev v zvezi s kakovostjo storitve, kot je določeno v členu 6(2)(a) predloga uredbe, bi morali ponudniki upoštevati pogoje, opisane v Uredbi (EU) 2015/2120, zlasti členu 3 ter uvodnih izjavah 10 in od 13 do 15. Na podlagi te določbe se lahko od ponudnikov zahteva, da komunikacijske podatke obdelujejo za odkrivanje in filtriranje zlonamerne in vohunske programske opreme, in se jim omogoči, da te podatke stisnejo.

⁸ Čeprav so v skladu z uvodno izjavo 13 predloga uredbe korporacijska omrežja izrecno izključena z njenega področja uporabe, bi bilo treba pri tej novi izjemi za individualno uporabo upoštevati tudi, da storitve v oblaku uporabljajo zaposleni pri delu, na primer z iskanjem po elektronski pošti.

katerih podatki bodo obdelani. V zvezi s temi primeri bi bilo treba v predlogu uredbe pojasniti, da le dejanje pošiljanja e-pošte ali druge vrste osebnega sporočila iz druge naprave končnemu uporabniku, ki je osebno privolil v obdelavo svoje vsebine in metapodatkov (na primer pri vpisovanju v poštno storitev), ne pomeni veljavne privolitve pošiljatelja.

Poleg tega bi bilo treba pojasniti, da je treba vse ustrezne določbe Splošne uredbe o varstvu podatkov upoštevati tudi pri obdelavi podatkov oseb, ki niso udeleženi končni uporabniki (npr. slika ali opis tretje osebe v izmenjavi med dvema osebama).

19. **Terminalska oprema in programska oprema morata *privzeto* omejevati, preprečevati in prepovedovati nezakonito poseganje vanjo ter zagotavljati informacije o možnostih.** Čeprav morajo ponudniki programske opreme, ki omogoča elektronsko komunikacijo, v skladu s predlogom uredbe „ponujati možnost“, da se prepreči omejena oblika poseganja v terminalsko opremo, ob namestitvi pa morajo od končnega uporabnika zahtevati, da privoli v nastavitve (člen 10(1) in (2)), ta možnost ni enaka *privzeti zasebnosti*. Poleg tega „možnost“ preprečevanja določenega poseganja že obstaja, vendar doslej ni prispevala k zadostni obravnavi težave neupravičenega sledenja. Ravno zaradi tega je bila v okviru Splošne uredbe o varstvu podatkov sprejeta zavestna politična odločitev o uvedbi načel vgrajenega in privzetega varstva podatkov ter vgrajene in privzete zasebnosti (člen 25 navedene uredbe). Predlog uredbe spodkopava ta načela v zvezi s komunikacijskimi podatki in podatki naprav. Ob tem Direktiva 2014/53/EU o radijski opremi⁹ (omenjena v uvodni izjavi 10) predvideva zelo omejeno varnostno obveznost, in sicer da ima radijska oprema vgrajeno „zaščito za zagotavljanje varstva osebnih podatkov ter zasebnosti uporabnikov in naročnikov“ (člen 3(3)(e)). To ne more nadomestiti posebnih nastavitvev privzete zasebnosti iz predloga uredbe. V zvezi s tem velja omeniti še, da je v raziskavi Eurobarometer o zasebnosti in elektronskih komunikacijah, ki je bila objavljena decembra 2016, poudarjeno, da se skoraj sedem od desetih oseb (69 %) popolnoma strinja, da bi morale privzete nastavitve njihovega brskalnika preprečevati delitev njihovih informacij¹⁰. Delovna skupina je posebej zaskrbljena glede nastavitvev brskalnika in opredelitve „tretjih oseb“. Glej odstavek 24. Poleg tega je treba upoštevati, da ta določba ne zadeva le brskalnikov, ki se uporabljajo na računalnikih, temveč zajema tudi druge vrste programske opreme, ki dovoljuje komunikacijo (vključno z operacijskimi sistemi, aplikacijami in vmesniki za programsko opremo za naprave, povezane v internet stvari). Na kratko, terminalska oprema in programska oprema morata *privzeto* zagotavljati nastavitve, ki varujejo zasebnost, in uporabnike voditi skozi konfiguracijske menije, v katerih lahko ob namestitvi te privzete nastavitve spremenijo. Ti konfiguracijski meniji bi morali biti med uporabo vedno lahko dostopni. Delovna skupina spodbuja evropskega zakonodajalca, naj pojasni področje uporabe člena 10 v zvezi s tem.

⁹ Direktiva 2014/53/EU o radijski opremi.

¹⁰ Glej poročilo o raziskavi Flash Eurobarometer 443 o zasebnosti in elektronskih komunikacijah (objavljena decembra 2016), str. 5.

20. **Uredba o zasebnosti in elektronskih komunikacijah bi morala izrecno prepovedovati zidove sledenja**, tj. prakso, pri kateri se dostop do spletišča ali storitve zavrne, če se posamezniki ne strinjajo s sledenjem na drugih spletiščih ali pri drugih storitvah. Kot je delovna skupina poudarila že v prejšnjih mnenjih o Direktivi o zasebnosti in elektronskih komunikacijah¹¹, so taki pristopi „vzemi ali pusti“ redko zakoniti¹². Kadar uporaba obdelovalnih in pomnilniških zmogljivosti terminalske opreme ali zbiranje informacij s terminalske opreme končnih uporabnikov omogoča sledenje dejavnostim uporabnika v daljšem časovnem obdobju ali pri več storitvah (npr. razna spletišča ali aplikacije), lahko take dejavnosti obdelave resno posegajo v zasebnost teh uporabnikov. Glede na pglavitni pomen svetovnega spleta pri uveljavljanju temeljne svobode izražanja, vključno s pravico dostopa do informacij, sposobnost posameznikov za dostop do spletne vsebine ne bi smela biti odvisna od strinjanja s sledenjem dejavnostim v napravah in na spletiščih ali v aplikacijah. V prihodnji uredbi o zasebnosti in elektronskih komunikacijah bi bilo zato treba določiti, da dostop do vsebine, na primer na spletiščih in v aplikacijah, ne bi smel biti pogojen s sprejetjem takih vsiljivih dejavnosti obdelave ne glede na uporabljeno tehnologijo sledenja, kot so piškotki, zajem prstnega odtisa naprave, vrivanje enotnih identifikatorjev ali druge tehnike spremljanja. Nujnost te prepovedi je bila poudarjena v najnovejši raziskavi Eurobarometer o zasebnosti in elektronskih komunikacijah, v kateri je navedeno, da je po mnenju skoraj dveh tretjin anketirancev nesprejemljivo, da se njihove spletne dejavnosti spremljajo v zameno za neomejen dostop do nekega spletišča (64 %).
21. Na kratko, **predlog uredbe bi moral** v zvezi s štirimi navedenimi problematičnimi področji **izpolniti obljubo, da bo zagotovil enakovredno ali višjo raven varstva kot Splošna uredba o varstvu podatkov**. V uvodni izjavi 5 je dejansko poudarjeno, da predlog uredbe ne znižuje ravni varstva, ki jo posamezniki uživajo v okviru Splošne uredbe o varstvu podatkov. Glede na sedanjo obliko predloga uredbe pa to ne drži, zlasti ne v zvezi s sledenjem napravam (odstavek 17), manjkajočim načelom privzete zasebnosti (odstavek 19) in privolitvijo (odstavek 18). To je pomembno predvsem zato, ker je v isti uvodni izjavi poudarjeno, da bo predlog uredbe „*lex specialis*“ glede na splošno uredbu o varstvu podatkov ter jo bo podrobno opredelil in dopolnil na področju elektronskih komunikacijskih podatkov, ki se štejejo za osebne podatke“. Delovna skupina predlaga, naj besedilo uredbe o zasebnosti in elektronskih komunikacijah pojasnjuje vsaj, da
- (i) imajo prepovedi iz uredbe o zasebnosti in elektronskih komunikacijah prednost pred dovoljenji iz Splošne uredbe o varstvu podatkov (npr. prepoved poseganja iz člena 5 uredbe o zasebnosti in elektronskih komunikacijah ima prednost pred pravicami ponudnikov elektronskih komunikacijskih storitev do nadaljnje obdelave osebnih podatkov iz členov 5(1)(b) in 6(4) navedene uredbe);

¹¹ Glej npr. WP 240 (pregled zasebnosti in elektronskih komunikacij), str. 16, in WP 208 (izvzetje iz privolitve), str. 5.

¹² To stališče ne posega v člen 7(4) Splošne uredbe o varstvu podatkov, v skladu s katerim se lahko „možnosti vzemi ali pusti“ po potrebi preprečijo tudi v drugih primerih.

(ii) kadar je obdelava dovoljena v skladu s katero koli izjemo (vključno s privolitvijo) od prepovedi iz uredbe o zasebnosti in elektronskih komunikacijah, je treba pri tej obdelavi, če zadeva osebne podatke, še vedno upoštevati vse ustrezne določbe iz Splošne uredbe o varstvu podatkov;

(iii) kadar je obdelava dovoljena v skladu s katero koli izjemo od prepovedi iz uredbe o zasebnosti in elektronskih komunikacijah, je prepovedana vsaka druga obdelava na podlagi Splošne uredbe o varstvu podatkov, vključno z obdelavo za drug namen v skladu s členom 6(4) navedene uredbe. To upravljavcem ne bi preprečilo, da za nova dejanja obdelave zahtevajo dodatno privolitev. Poleg tega zakonodajalcem ne bi preprečilo, da v uredbi o zasebnosti in elektronskih komunikacijah predvidijo dodatne, omejene in posebne izjeme, da bi na primer dovolili obdelavo v znanstvene ali statistične namene iz člena 89 Splošne uredbe o varstvu podatkov ali zaščitili „življenjske interese“ posameznikov, na katere se nanašajo osebni podatki, v skladu s členom 6(d) navedene uredbe.

Poleg tega bi bilo treba uredbo o zasebnosti in elektronskih komunikacijah razlagati tako, da bi zagotovili, da bo predvidevala vsaj enako in po potrebi višjo raven varstva kot Splošna uredba o varstvu podatkov.

4. DRUGA PROBLEMATIČNA PODROČJA

Poleg navedenih področij je delovna skupina iz člena 29 **zaskrbljena** glede naslednjih področij.

RAZŠIRITI JE TREBA OZEMELJSKO IN VSEBINSKO VELJAVNOST

22. **Izraz „metapodatki“ je preozko opredeljen.** Po opredelitvi iz člena 4(3)(c) izraz pomeni „podatke, ki se obdelajo v elektronskem komunikacijskem omrežju za namene prenašanja, razširjanja ali izmenjave vsebine elektronskih komunikacij“ (dodan poudarek). Iz uporabe besede „omrežje“ bi lahko sklepali, da se med „metapodatke“ uvrščajo samo podatki, ustvarjeni med zagotavljanjem storitev na „nižji“ ravni omrežja. To bi lahko pomenilo, da bi bili s tega področja uporabe izključeni podatki, ustvarjeni med zagotavljanjem povrhnjih spletnih storitev. To ne bi bilo zaželeno in verjetno tudi ne načrtovano glede na to, da se področje uporabe predloga uredbe namerava razširiti na ponudnike povrhnjih spletnih storitev. Da bi to težavo odpravili, bi bilo treba spremeniti opredelitev „elektronskih komunikacijskih podatkov“, da bi vključevala vse podatke, ki se obdelajo za namene prenašanja, razširjanja ali izmenjave vsebine elektronskih komunikacij.

23. Še eno problematično področje je, da **ozemeljska veljavnost predloga uredbe v zvezi z organizacijami, ki nimajo sedeža v EU, zajema samo ponudnike elektronskih komunikacijskih storitev.** Predlog uredbe določa, da kadar ponudnik elektronske komunikacijske storitve nima sedeža v EU, pisno imenuje predstavnika v Uniji (člen 3(2)). Poleg tega je v uvodni izjavi 9 navedeno, da bi se uredba uporabljala za obdelavo, ki jo izvajajo ponudniki elektronskih komunikacijskih storitev ne glede na kraj obdelave. Delovna skupina pozdravlja to pojasnilo. Ker pa je besedilo omejeno na ponudnike elektronskih komunikacijskih storitev, ni gotovo, v

kolikšnem obsegu ta ozemeljska veljavnost zadeva druge vrste oseb (na primer osebe, ki posegajo v terminalsko opremo končnih uporabnikov ali zbirajo informacije, ki jih ta oddaja (glej člen 3(1)(c) in člen 8 predloga uredbe). Zato delovna skupina predlaga, da se člen 3(2) in 3(5) spremeni tako, da bo vključeval ponudnike javno dostopnih direktorijev, ponudnike programske opreme, ki omogoča elektronsko komunikacijo, in osebe, ki pošiljajo komercialna sporočila za namene neposrednega trženja ali zbirajo (druge) informacije v zvezi s terminalsko opremo končnih uporabnikov oziroma informacij, ki so na njej shranjene, kadar koli so njihove dejavnosti usmerjene v uporabnike v EU (glej uvodno izjavo 8 predloga uredbe)¹³.

OKREPITI JE TREBA ZAŠČITO TERMINALSKE OPREME

Problematična je tudi nezadostna zaščita terminalske opreme v predlogu uredbe.

24. Predlog uredbe napačno predpostavlja, da je mogoče veljavno privolitev izraziti z nespecifičnimi nastavitvami brskalnika. Delovna skupina priznava premislek, da so končni uporabniki prenasršeni s pozivi k privolitvi (uvodna izjava 22). Pri odpravi te težave imajo pomembno vlogo nastavitve brskalnika (in primerljive programske opreme). Ker pa uporaba splošnih nastavitvev brskalnika ni predvidena za uporabo tehnologije sledenja v vsakem posameznem primeru, prek njih ni mogoče izraziti ustrezne privolitve v skladu s členom 7 in uvodno izjavo 32 Splošne uredbe o varstvu podatkov (ker privolitev ni informirana in dovolj specifična).

Končnemu uporabniku je treba omogočiti, da prek spletišča ali aplikacije ločeno privoli v sledenje za različne namene (kot je delitev prek družbenih medijev ali oglaševanje). Upravljaec podatkov, odgovoren za več spletišč ali aplikacij, lahko zahteva privolitev tudi za vsa preostala spletišča ali aplikacije, ki jih nadzoruje, če to zahtevo za privolitev predloži ločeno.

Poleg tega mora upravljavec izpolnjevati vse druge obveznosti, povezane s privolitvijo, vključno z obveznostjo, da uporabnikom zagotovi ustrezne informacije. To tako za brskalnike kot za upravljavce podatkov pomeni, da le z zagotovitvijo možnosti „sprejetja vseh piškotkov“ ne bi izpolnili obveznosti, saj s tem uporabnikom ne bi omogočili zagotovitve zahtevane posamezne privolitve. Vendar bi bilo treba poskrbeti za to, da bodo brskalniki uporabnikom omogočali sprejetje informirane in zavestne odločitve, da sprejmejo vse piškotke in tako preprečijo morebitne prihodnje zahteve spletišč, ki jih obiščejo, za posebno privolitev.

Delovna skupina močno priporoča, naj uredba o zasebnosti in elektronskih komunikacijah od brskalnikov zahteva, da uvedejo tehnične mehanizme, kot je

¹³ Glej člen 3(2) Splošne uredbe o varstvu podatkov: *Ta uredba se uporablja za obdelavo osebnih podatkov posameznikov, na katere se nanašajo osebni podatki in ki so v Uniji, s strani upravljavca ali obdelovalca, ki nima sedeža v Uniji, kadar so dejavnosti obdelave povezane: (a) z nudenjem blaga ali storitev takim posameznikom v Uniji, ne glede na to, ali je potrebno plačilo posameznika, na katerega se nanašajo osebni podatki, ali (b) s spremljanjem njihovega vedenja, kolikor to poteka v Uniji.* Ta obveznost bi lahko vključevala tudi izjeme v skladu s členom 27(2) Splošne uredbe o varstvu podatkov.

standard *brez sledenja*, da bi uporabnikom zagotovili resnično možnost izbire in nadzor nad poseganjem v njihove naprave¹⁴.

Še pomembnejše pa je, da bi morala uredba o zasebnosti in elektronskih komunikacijah zagotoviti, da vsi upravljavci podatkov tako odločitev glede hrambe informacij v napravi kot signal *brez sledenja* iz brskalnika priznajo kot pravno zavezujoč znak privolitve ali zavrnitve. To ne posega v dodatna navodila delovne skupine o tem, da mora biti standard *brez sledenja*, ko bo dokončno oblikovan (predvidoma konec leta 2017), med drugim usklajen z načelom omejitve namena.

Implicitne oblike „privolitve“, kot je klik na spletišče ali pomikanje po spletni strani, ne morejo razveljaviti odločitev glede hrambe in signala *brez sledenja*. Pomembna prednost uporabe tega standarda je, da ni omejena na tehnologijo sledenja s piškotki, temveč zajema tudi druge vrste sledenja, kot je zajem prstnega odtisa.

Če bo upoštevanje tega standarda postalo pravno zavezujoče, bo to rešilo tudi težavo v zvezi s sedanjo uporabo izraza „tretje osebe“ v členu 10. Spletna stran ali aplikacija na splošno vsebuje več elementov tako s spletišča kot zunanje elemente. V ozadju obiskanega spletišča se lahko izvaja tudi zunanja koda, ki poroča strežniku tretje osebe. Ponudnik lahko uporabniku, ko na primer obišče spletišče za socialno mreženje, ponudi sledilni piškotek. To spletišče za socialno mreženje bi lahko bila tudi tretja oseba, in sicer kadar navedeni uporabnik obišče drugo spletišče, ki vzajemno deluje z navedenim spletiščem za socialno mreženje. Ne glede na to, ali gre za „dostop do“ informacij v napravi končnega uporabnika ali njihovo „hrambo“, to v vseh teh primerih pomeni poseganje v napravo, za katero je potrebna privolitev (razen če se uporablja ena od izjem). Pri standardu *brez sledenja* je ta težava rešena z uporabo izrazov „na ravni spletišča“ in „na ravni svetovnega spleta“. Da bi se izboljšala pravna varnost za vse zainteresirane strani, bi bilo treba sklic na „tretje osebe“ v uredbi o zasebnosti in elektronskih komunikacijah preoblikovati, da bi zajemale vse subjekte, s katerimi naprava vzajemno deluje (ker dostopajo do informacij v napravi ali jih vanjo shranjujejo).

Da bi zagotovili združljivost standarda *brez sledenja* z visoko ravno varstva zaupnosti komunikacij in varstva podatkov, ki jo zagotavlja Listina, bi bilo treba v uredbi o zasebnosti in elektronskih komunikacijah določiti, da je treba zahteve za sledenje na ravni svetovnega spleta v nasprotju s sledenjem na ravni spletišča predložiti ločeno, pri tem pa bi morali imeti uporabniki možnost svobodnega odločanja, ali bodo te zahteve sprejeli ali zavrnili. Da bi uporabnike zaščitili pred pogostimi zahtevami za privolitev, bi morala uredba o zasebnosti in elektronskih komunikacijah zagotavljati, da če neka organizacija zavrne sledenje na ravni svetovnega spleta (prek standarda *brez sledenja* ali ločenega črnega seznama), tej organizaciji preprečuje pošiljanje nadaljnjih zahtev za privolitev vsaj šest mesecev. To pravilo ne preprečuje, da organizacija, če jo uporabnik (tj. kot ponudnik) neposredno obišče, zahteva privolitev na svojem spletišču (tj. zahteva za privolitev na ravni spletišča). To v praksi pomeni, da lahko na primer spletišče za pretakanje videov, ki uporablja sledilne piškotke, od uporabnika zahteva privolitev, ko jo ta

¹⁴ Glej URL: <https://www.w3.org/TR/tracking-compliance/>. V odstavku 7 sta razložena model izjem in razlika med izjemo na ravni spletišča in izjemo na ravni spleta. V odstavku 6 so navedene strojno berljive informacije, ki jih upravljavci podatkov lahko zagotovijo v okviru zahteve po informacijah za pridobitev privolitve.

obišče, vendar privolitve od njega ne sme zahtevati šest mesecev, če privolitev zavrne in obišče druga spletišča, ki vsebujejo videe, ki jih ponuja navedeno spletišče za pretakanje videov.

25. **Nenatančno je opredeljena tudi izjema za „merjenje spletnega občinstva“.** V členu 8(1)(d) predloga uredbe je predvidena izjema za merjenje spletnega občinstva. Prvi pomislek je, da ta izraz ni opredeljen in se lahko zamenjuje z oblikovanjem profilov uporabnikov. V opredelitvi bi bilo treba pojasniti, da te izjeme ni mogoče uporabiti za namene oblikovanja profilov. Izjema bi se morala uporabljati samo za analizo uporabe, ki je potrebna za analizo izvajanja storitve, ki jo je zahteval uporabnik, in ne za analizo uporabnikov (tj. analizo vedenja določljivih uporabnikov spletišča, aplikacije ali naprave). Zato se izjema ne more uporabljati, kadar se lahko podatki povežejo s podatki določljivega uporabnika, ki jih obdelujejo ponudnik ali drugi upravljavci podatkov. Poleg tega njen opis kaže na zelo tehnološko specifično uporabo. Zato bi bilo treba izraz „merjenje spletnega občinstva“ znova opredeliti na tehnološko nevtralen način, da bo vključeval tudi podobne analitične informacije o uporabi, pridobljene iz aplikacij, nosljivih naprav in naprav, povezanih v internet stvari.

Delovna skupina predlaga zgledovanje po nizozemski izjemi, ki se uporablja, če je nujno potrebna za pridobitev informacij o tehnični kakovosti ali učinkovitosti zagotovljene storitve informacijske družbe in malo ali sploh ne vpliva na zasebnost udeleženega naročnika ali končnega uporabnika (glej člen 11.7a(3)(b) nizozemskega zakona o telekomunikacijah). Ta izjema upošteva, da je večina podatkov, zbranih prek spletne ali aplikacijske analitike, še vedno osebnih. To pomeni, da tudi za obdelavo teh podatkov velja Splošna uredba o varstvu podatkov in da bi na primer analizo uporabe lahko izvajala tudi zunanja organizacija, a le, če:

- (i) ta organizacija nastopa kot obdelovalec podatkov;
- (ii) je z obdelovalcem sklenjen sporazum v skladu s Splošno uredb o varstvu podatkov;
- (iii) uporabljena analitična tehnologija preprečuje ponovno določanje, kar med drugim vključuje anonimizacijo naslovov IP uporabnikov;
- (iv) se lahko posebni piškotki ali drugi podatki, uporabljeni za analizo, uporabljajo samo za specifično spletno mesto, aplikacijo ali nosljivo napravo in jih ni mogoče povezati z drugimi določljivimi podatki;
- (v) imajo uporabniki pravico do zavrnitve (glej tudi odstavek 17 in 50 v tem mnenju).

Če so ti pogoji izpolnjeni, privolitev ni potrebna, vendar morajo upravljavci podatkov uporabnikom še vedno zagotoviti ustrezne informacije, na primer prek polj s prikazom statusa sledenja v možnosti *brez sledenja*¹⁵.

26. Uredba o zasebnosti in elektronskih komunikacijah **bi morala zagotoviti ozke in natančno opredeljene izjeme o zahtevah za privolitve**. Besedilo opredelitve izjeme od zahteve za privolitev v poseganje v naprave iz člena 8(1)(c) je skoraj enako

¹⁵ Glej: Izražanje preferenc sledenja (DNT) (Tracking Preference Expression (DNT)), urednikov osnutek, 7. marec 2016.

obstoječemu besedilu v členu 5(3) Direktive o zasebnosti in elektronskih komunikacijah: *nujno potrebno za zagotovitev storitve informacijske družbe, ki jo naročnik ali uporabnik izrecno zahtevata*. Ključna beseda „nujno“ je izpuščena brez pojasnila. To je problematično iz dveh razlogov. Prvič, v zvezi s področjem uporabe določbe v Direktivi o zasebnosti in elektronskih komunikacijah so že obsežno razpravljali nadzorni organi in organizacije in črtanje besede „nujno“ bo še bolj zmanjšalo pravno varnost. Drugič, delovna skupina je že zagotovila smernice o razlagi izraza „nujno“ v zvezi s tem. V mnenju o piškotkih, ki so izvzeti iz zahteve po soglasju (WP 194), je predlagala naslednje pojasnilo:

*piškotek je potreben za zagotavljanje določene možnosti uporabniku (ali naročniku): če so piškotki onemogočeni, storitev ni na voljo; [...] to možnost je izrecno zahteval uporabnik (ali naročnik) v sklopu storitve informacijske družbe.*¹⁶

Delovna skupina je poleg tega pojasnila, da

*piškotki „tretjih strank“ običajno niso „nujno potrebni“ za uporabnika, ki si ogleduje spletno stran, saj so ti piškotki običajno povezani s storitvijo, ki se razlikuje od storitve, ki jo je uporabnik „izrecno zahteval“*¹⁷.

Delovna skupina je dodala, da se za nujno potrebno ne bi štela tudi uporaba družbenih vtičnikov, usmerjena v neuporabnike platforme ali spletišča.

Čeprav je v skladu s členom 6(1)(b) predloga uredbe obdelava elektronskih komunikacijskih podatkov dovoljena, če je to „potrebno“ iz varnostnih razlogov, mora biti to v skladu z uvodno izjavo 49 Splošne uredbe o varstvu podatkov nujno potrebno. Izpust besede „nujno“ morda ni bil nameren, saj je v uvodni izjavi 21 predloga uredbe omenjeno, da se privolitve v poseganje ne bi smela zahtevati, če je to „nujno“ potrebno. Predlog uredbe kljub temu zagotavlja priložnost za dodatno pojasnilo, da bi bilo treba preizkus nujnosti v okviru te uredbe razlagati ozko za vse izjeme. Delovna skupina zato predlaga, da bi bilo treba v zvezi z vsemi izjemami iz člena 6 in člena 8(1) predloga uredbe pred besedo „potrebno“ dodati besedo „nujno“.

Po drugi strani bi morala uredba o zasebnosti in elektronskih komunikacijah izrecno dovoljevati poseganje v opremo zaradi namestitve varnostnih posodobitev. Zaželeno metoda za nameščanje varnostnih posodobitev v večino naprav končnih uporabnikov je pošiljanje teh posodobitev prek svetovnega spleta. Nameščanje posodobitev se šteje za poseganje v terminalsko opremo. Vendar gre tu za zakoniti interes, da varnost teh naprav ostane posodobljena. Zato bi bilo treba ponudniku varnostnih popravkov na splošno omogočiti, da brez privolitve končnega uporabnika namesti nujno potrebne varnostne posodobitve. Ni pa gotovo, ali lahko temu poseganju koristi izjema od prepovedi poseganja zaradi opravljanja storitve „informacijske družbe“ (člen 8(1)(c)). Pojasniti bi bilo treba, da je nameščanje varnostnih posodobitev v skladu s to izjemo dovoljeno, vendar le če (i) so varnostne posodobitve diskretno

¹⁶ Delovna skupina iz člena 29, WP 194, Mnenje 04/2012 o piškotkih, ki so izvzeti iz zahteve po soglasju, sprejeto 7. junija 2012, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_sl.pdf.

¹⁷ Prav tam.

pakirane in na noben način ne spreminjajo funkcionalnosti programske opreme v opremi (vključno z vzajemnim delovanjem z drugo programsko opremo ali nastavitvami, ki jih je izbral uporabnik), (ii) je končni uporabnik vnaprej obveščen ob vsaki namestitvi posodobitve in (iii) lahko končni uporabnik zavrne samodejno namestitvev teh posodobitev.

NEPOSREDNO TRŽENJE

Še eno problematično področje je nezadostna zaščita pred neposrednim trženjem.

27. Prvič, **področje uporabe neposrednega trženja je preveč omejeno**. V členu 4(3)(f) predloga uredbe „sporočila za namene neposrednega trženja“ pomenijo „vsako obliko oglaševanja v pisni ali govorni obliki, ki je bilo poslano enemu ali več določenim ali določljivim končnim uporabnikom elektronskih komunikacijskih storitev“. Uporaba besede „poslan“ kaže na uporabo tehnološkega komunikacijskega sredstva, ki nujno vključuje prenos sporočila, medtem ko večina oglaševanja na spletu (prek platform družbenih medijev ali na spletiščih) ne vključuje „pošiljanja“ oglasov v ozkem smislu. To je dodatno poudarjeno s primeri, navedenimi v tej opredelitvi (kratka sporočila SMS, elektronska pošta) in uvodni izjavi 33. Vsi se nanašajo na precej tradicionalne oblike sporočil za namene trženja, vendar na predlagano področje uporabe domnevno ne spada uporaba precej tradicionalnih klicnih sistemov. Člen in uvodno izjavo bi bilo treba spremeniti, da bi vključevala vse oglase, ki se *pošljejo, so namenjeni ali se predložijo* enemu ali več določenim ali določljivim končnim uporabnikom. Poleg tega bi bilo treba zagotoviti, da se za sporočila za neposredno trženje, usmerjena v enega ali več določenih ali določljivih končnih uporabnikov, šteje tudi vedenjsko oglaševanje (na podlagi profilov končnih uporabnikov), saj je tako oglaševanje usmerjeno v posebne določljive uporabnike.

V skladu s predlaganim področjem uporabe „sporočil za neposredno trženje“ bi bilo varstvo iz člena 16(1) omejeno na sporočila, ki vsebujejo oglaševalski material, in posameznikov ne bi ščitilo pred drugimi sporočili, ki se pošljejo, so namenjena ali se predložijo za trženje (kot so sporočila za pridobivanje novih strank, katerih namen je pridobitev privolitve, promocija političnih mnenj ali volilnih preferenc, promocija dobrodelnih ustanov ali drugih neprofitnih organizacij ali splošno znamčenje organizacije). Poleg tega se kot metoda neposrednega trženja še vedno uporabljajo telefaksi, čeprav niso navedeni v opredelitvi. Zato bi moral člen 4(3)(f) vključevati vse oblike oglaševanja, agitiranja ali promocije, tudi za neprofitne organizacije, poleg elektronske pošte in kratkih sporočil SMS pa izrecno zajemati tudi telefakse (glej tudi predlog za pojasnilo v odstavku 43(a)). V uvodni izjavi 32 je navedeno, da neposredno trženje vključuje sporočila, ki jih pošiljajo politične stranke za svojo promocijo. To bi bilo treba posodobiti, da bi vključevalo tudi nosilce političnega odločanja in kandidate za volitve, ki promovirajo svojo kandidaturo.

28. Drugič, **preklic privolitve za neposredno trženje ni brezplačen in privolitve ni mogoče enako lahko preklicati kot dati**. Možnost preklica privolitve v skladu s predlogom uredbe je treba pojasniti, da bi zagotovili skladnost in izboljšali varstvo prejemnikov. Člen 16(6) predloga uredbe določa, da se morajo prejemnikom

neposrednega trženja zagotoviti „informacije, ki jih prejemniki potrebujejo za enostavno uveljavljanje svoje pravice do preklica privolitve k sprejemanju nadaljnjih sporočil za namene trženja“ (dodan poudarek). To je potrjeno v uvodni izjavi 34. Iz uvodne izjave 70 Splošne uredbe o varstvu podatkov pa sledi, da bi morali imeti posamezniki iz navedene uredbe, na katere se nanašajo osebni podatki, pravico, da ugovarjajo obdelavi za namene neposrednega trženja enostavno in „brezplačno“. Ta izraz se uporablja tudi v členu 16(2) predloga uredbe, vendar le v zvezi z zavrnitvijo neposrednega trženja na podlagi kontaktnih podatkov, pridobljenih v okviru prodaje.

Člen 7(3) Splošne uredbe o varstvu podatkov določa, da je privolitev enako enostavno preklicati kot dati in da bi bilo treba posameznikom omogočiti, da privolitev kadar koli prekličejo. Poleg tega je delovna skupina v Mnenju 04/2010 o FEDMA (WP 174) že potrdila, kako pomembno je, da se zagotovi „preprosta, učinkovita, brezplačna, neposredna in lahko dostopna odjava“ od neposrednega trženja¹⁸. Ta standard preklica privolitve bi bilo treba vključiti v pravila za neposredno trženje v predlogu uredbe. Enako velja za zahtevo iz člena 7(3) Splošne uredbe o varstvu podatkov, da bi morale biti privolitve mogoče kadar koli enako lahko preklicati kot dati.

29. V zvezi s tem **bi bilo treba pojasniti način preklica privolitve ali zavrnitve klicev za namene neposrednega trženja**. Države članice lahko na podlagi člena 16(4) predloga uredbe izberejo sistem zavrnitve za govorno-govorne klice za namene trženja. V uredbi o zasebnosti in elektronskih komunikacijah bi bilo treba določiti ureditve za preklic privolitve in zavrnitev klicev na namene trženja. V uvodni izjavi 36 je določeno, da bi države članice *morale imeti možnost*, da vzpostavijo in/ali ohranijo nacionalne sisteme zavrnitve. Na podlagi te določbe bi lahko države članice dopustile celo primere, v katerih bi moral uporabnik zavrniti posamezne ponudnike komunikacij. Tako izvajanje uporabnikov niti ne ščiti pred nadležno neupravičeno komunikacijo¹⁹ niti ne zagotavlja mehanizma, usklajenega s Splošno uredbo o varstvu podatkov, s katerim bi bilo mogoče privolitve lahko in kadar koli preklicati. Zato bi bilo treba v uredbi določiti, da *mora* vsaka država članica vzpostaviti nacionalni register neželenih klicev. Poleg tega bi bilo treba v uredbi določiti, da bi bilo treba prejemnikom govorno-govornih klicev zagotoviti dve možnosti preklica privolitve: za prihodnje klice določenega podjetja ali organizacije ter z vključitvijo neželenih klicev v nacionalni register že v času njihovega trajanja.

30. Problematično je tudi, da **ni izrecno prepovedana uporaba lažnih identitet pri pošiljanju sporočil za neposredno trženje**. V uvodni izjavi 34 je poudarjeno, da je „zakrivanje identitete in uporabo lažnih identitet, lažnih povratnih naslovov ali števil

¹⁸ Delovna skupina za varstvo podatkov iz člena 29, WP 174, Mnenje 04/2010 o evropskem kodeksu ravnanja Evropske federacije združenj za direktni marketing (FEDMA) pri uporabi osebnih podatkov v neposrednem trženju, sprejeto 13. julija 2010, URL: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_sl.pdf.

¹⁹ V Združenem kraljestvu je na primer telekomunikacijski operater BT v enem tednu zaznal 31 milijonov nadležnih klicev. Glej: <http://www.bbc.com/news/business-38635921>.

pri pošiljanju nepovabljenih komercialnih sporočil za neposredno trženje“ prepovedano. V členu 16(4) pa je navedeno le, da morajo biti končni uporabniki obveščeni o „identiteti pravne ali fizične osebe, v katere imenu se sporočilo prenaša“. To obveznost obveščanja prejemnikov o identiteti bi bilo treba dopolniti z jasno prepovedjo uporabe prikritih ali napačnih kontaktnih naslovov za namene neposrednega trženja.

31. To področje je povezano z drugim pomislekom: **obvezna predpona pri klicih za namene neposrednega trženja je predstavljena kot alternativa zahtevi glede identifikacije priključka za stik**. V skladu s členom 16(3) so klici za namene neposrednega trženja dovoljeni, če klicatelj bodisi (i) prikaže identiteto priključka, na katerem je kličoča fizična ali pravna oseba dosegljiva (člen 16(3)(a)), bodisi (ii) uporabi posebno kodo/predpono, iz katere je razvidno, da je klic tržne narave (člen 16(3)(b)). Čeprav delovna skupina pozdravlja obveznost iz člena 16(3)(b) glede uporabe predpone, po njenem mnenju ta zahteva ne zadeva istega vprašanja kot obveznost identifikacije priključka za stik iz člena 16(3)(a). Cilj zahteve glede predpone je prejemniku omogočiti, da klic že vnaprej prepozna kot klic za namene trženja (in izvede ukrepe za blokiranje teh klicev), cilj zahteve glede identifikacije priključka za stik prejemnikom (in nadzornim organom) pa je zagotoviti sredstva za identifikacijo in vzpostavitev stika s pobudnikom trženja. To je zlasti pomembno za avtomatizirane klice, pri katerih je veliko neravnovesje med možnostmi, da trgovec opravi nadležne klice, in možnostmi, da se prejemnik tem klicem izogne. Zahteve zato ne smejo druga drugo nadomeščati, temveč se morajo dopolnjevati.

ČASOVNI RAZPORED

32. Delovna skupina iz člena 29 želi pohvaliti Evropsko komisijo, ker je pritrdila potrebi po tem, da predlog uredbe začne veljati maja 2018, skupaj s Splošno uredbo o varstvu podatkov, da bi preprečili neskladnosti med zakonodajnim aktoma. Še vedno pa je problematično, da je to ambiciozen časovni okvir, ki zahteva tudi dokončanje osnutka Evropskega zakonika o elektronskih komunikacijah. Delovna skupina iz člena 29 zato zahteva, da vse zainteresirane strani v zakonodajnem postopku upoštevajo rok, ki je maj 2018.

DRUGI POMISLEKI

V tem oddelku je obravnavanih več dodatnih pomislekov.

33. Prvič, delovna skupina iz člena 29 je zaskrbljena zaradi **domneve, da so neusmerjeni ukrepi za hrambo podatkov sprejemljivi**. V obrazložitvenem memorandumu predloga uredbe je poudarjeno, da države članice lahko ohranijo ali oblikujejo nacionalne okvire za hrambo podatkov, ki med drugim zagotavljajo usmerjene ukrepe za hrambo (odstavek 1.3). Na podlagi odločbe v zadevi Tele2/Watson²⁰ je jasno, da okviri za hrambo, ki ne zagotavljajo usmerjenih ukrepov

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

za hrambo, v skladu z Listino niso dovoljeni (in tudi drugače zanje veljajo pomembni pogoji, kot je nadzor) in da bo treba splošen dostop do metapodatkov obravnavati kot kršitev bistva člena 7 tako kot splošen dostop do vsebine elektronskih komunikacij (glej Sodišče Evropske unije, Schrems, in uvodno izjavo 94). Na podlagi besedila tega stavka je mogoče sklepati, da imajo države članice nekaj manevrskega prostora v zvezi z ukrepi za hrambo podatkov, ki pa ne obstaja. V zvezi s tem v predlogu uredbe za **metapodatke ni zagotovljena zadostna raven varstva**. Kot je poudarjeno v odstavku 10, delovna skupina iz člena 29 pozdravlja priznanje, da lahko metapodatki razkrijejo zelo občutljive podatke. Vendar za metapodatke v predlogu uredbe ni zagotovljeno varstvo, ki bi moralo temeljiti na tem priznanju. Zlasti glede na občutljivost metapodatkov bi bilo treba pred analizo iz člena 6(2)(c) izvesti oceno učinka v zvezi z varstvom podatkov (glej tudi odstavek 46).

34. Drugič, **predlog uredbe bi neželeno razširil možnosti za hrambo podatkov.**

Člen 11 predloga uredbe se sklicuje na člen 23(1)(a) do (e) Splošne uredbe o varstvu podatkov pri opisovanju namenov, za katere lahko države članice omejijo obveznosti in pravice iz členov od 5 do 8 Uredbe. V Splošni uredbi o varstvu podatkov zaradi velikega tveganja za posameznike, na katere se nanašajo osebni podatki, take omejitve v zvezi s posebnimi kategorijami podatkov niso predvidene. Člen 15 Direktive o zasebnosti in elektronskih komunikacijah trenutno omogoča podobno omejitev, vendar so nameni bolj omejeni. Novi predlog uredbe bi omogočil nove omejitve za namene „izvrševanja kazenskih sankcij, vključno z varovanjem pred grožnjami javni varnosti in njihovim preprečevanjem“ (člen 23(1)(d) Splošne uredbe o varstvu podatkov), in „drugih pomembnih ciljev v splošnem javnem interesu Unije ali države članice, zlasti pomembnega gospodarskega ali finančnega interesa Unije ali države članice, vključno z denarnimi, proračunskimi in davčnimi zadevami, javnim zdravjem in socialno varnostjo“ (člen 23(1)(e) Splošne uredbe o varstvu podatkov). Ne le, da so ti nameni novi v primerjavi z Direktivo o zasebnosti in elektronskih komunikacijah, zadnji namen iz člena 23(1)(d) in celoten namen iz člena 23(1)(e) sta zasnovana precej široko. Zato se predlaga, da se črta sklicevanje na člen 23(1)(a) do (e) Splošne uredbe o varstvu podatkov in namesto tega navedejo le nameni, ki jih trenutno vsebuje člen 15 Direktive o zasebnosti in elektronskih komunikacijah.

35. **Obseg obveznosti obveščanja uporabnikov o varnostnih tveganjih je minimalističen.**

Delovna skupina pozdravlja, da morajo ponudniki storitev uporabnike obvestiti o varnostnih tveganjih in ukrepih za njihovo odpravo, kot je šifriranje (člen 17 in uvodna izjava 37). Naslov te določbe se glasi: „Informacije o odkritih varnostnih tveganjih“. Dejstvo, da so v naslovu navedena odkrita tveganja, kaže na to, da je ta določba povezana samo z (morebitnimi) kršitvami varnosti, medtem ko je besedilo določbe in uvodne izjave bolj usmerjeno v splošno obveščanje končnih uporabnikov. Če na primer ponudnik storitve odkrije, da je naprava uporabnika okužena z zlonamerno programsko opremo in je postala del botneta, se zdi, da ta določba od ponudnika neposredno zahteva, da uporabnika obvesti o nastalih tveganjih. Področje uporabe te določbe bi bilo treba pojasniti in ne bi smelo biti omejeno na točno ta primer. Določba bi morala zajemati vsaj odkrita varnostna tveganja v vsej opremi, ki jo ponudnik zagotovi končnemu uporabniku kot del naročnine, kot so na primer usmerjevalniki in mobilne naprave, in obveščanje o

tveganjih spreminjanja nastavitvev, ki so bile v skladu z načelom vgrajene zasebnosti nastavljene tako, da varujejo zasebnost.

Delovna skupina priporoča, da se področje uporabe razširi, tako da bo vključevalo ponudnike programske opreme, ki omogoča elektronsko komunikacijo (glej uvodno izjavo 8), in morda tudi novo kategorijo: ponudnike tehnologije, bistvene za varno komunikacijo, ki niso ponudniki storitev (npr. ponudniki tehnologije šifriranja). V primeru te zadnje razširitve bi bilo treba poskrbeti za to, da se ta obveznost ne bo prekrivala z obveznostmi glede obvestila o kršitvi varnosti v drugih instrumentih, kot je direktiva o varnosti omrežij in informacijskih sistemov²¹, in drugih pravnih instrumentih v zvezi s ponudniki potrdil. Ker zadnja kategorija ponudnikov tehnologije običajno nima neposrednega stika s končnimi uporabniki, je treba pojasniti tudi, kako lahko izpolnjujejo obveznost glede informacij v skladu s to določbo.

36. Delovna skupina pozdravlja določbe členov 2 in 13, ki se bodo uporabljale za medosebne komunikacijske storitve na podlagi številke. Ni pa takoj očitno, zakaj **podobna raven varstva zasebnosti ne bi smela biti na voljo tudi za funkcionalno enakovredne klicne storitve povrhnjih spletnih storitev.**
37. Delovna skupina je zaskrbljena tudi zaradi **pomanjkanja jasnosti glede posamezne privolitve v povratno iskanje v direktorijih.** V skladu s členom 15(2) predloga uredbe morajo ponudniki pridobiti privolitev končnih uporabnikov, preden omogočijo iskalne funkcije v zvezi z njihovimi podatki (glej tudi uvodno izjavo 31). Delovna skupina pozdravlja uskladitev zahteve za privolitev v zvezi z vključitvijo v direktorije, vendar obžaluje pomanjkanje razčlenjenosti v zvezi z različnimi vrstami iskanj. Direktiva o zasebnosti in elektronskih komunikacijah v obstoječi obliki državam članicam na podlagi člena 12(3) omogoča, da zahtevajo ločeno privolitev v povratno iskanje. V tem členu je navedeno: *Države članice lahko zahtevajo, da se lahko za kateri koli namen javnega imenika, razen za iskanje podatkov o osebah na podlagi njihovega imena in, kjer je potrebno, minimalnega števila drugih identifikatorjev, zahteva dodatna privolitev naročnikov.* Na podlagi te določbe je v več državah članicah za funkcionalnosti povratnega iskanja potrebna ločena privolitev, pri čemer se upoštevajo različne ravni določljivosti in s tem ravni poseganja obeh funkcionalnosti.
38. Bolj formalni pomislek je, da **višina upravnih glob ni usklajena za vse kršitve uredbe.** Države članice v skladu s predlogom uredbe določijo predpise o kaznih za kršitve člena 23(4), člena 23(6) in člena 24 predloga uredbe. Večjo usklajenost bi dosegli, če bi to uredili tudi v uredbi o zasebnosti in elektronskih komunikacijah.
39. Nazadnje je treba poudariti, da **predlog uredbe temelji na opredelitvah, ki lahko postanejo „premični cilji“.** V zvezi s številnimi ključnimi koncepti se predlog

²¹ Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji, UL 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.SLV

uredbe sklicuje na drug pravni instrumenti, ki je še v obliki osnutka: predlog Evropskega zakonika o elektronskih komunikacijah (glej na primer člen 4(1)(b)). Dva pomembna primera sta opredelitev „končnega uporabnika“, ki trenutno vključuje fizične in pravne osebe, ter opredelitev „elektronske komunikacijske storitve“ in „medosebne komunikacijske storitve“, ki sta vključeni v člen 4(1)(b) predloga uredbe, zadnji navedeni pa je podrobneje opredeljen v členu 4(2), da bi vključeval vrste storitve, ki so v Evropskem zakoniku o elektronskih komunikacijah izrecno izključene²². To mnenje temelji na obstoječih opredelitvah, vendar je precej verjetno, da se bodo predlog Evropskega zakonika o elektronskih komunikacijah in/ali njegovi ključni koncepti spremenili. To bi imelo neposredne posledice tudi za uredbo o zasebnosti in elektronskih komunikacijah. V najboljšem primeru bi morali biti v uredbi o zasebnosti in elektronskih komunikacijah vsi izrazi, ki izhajajo iz Evropskega zakonika o elektronskih komunikacijah, neodvisno opredeljeni. Predlog uredbe bi moral pri izrazih, katerih opredelitve odstopajo od opredelitev iz Evropskega zakonika o elektronskih komunikacijah, vključevati vsaj pojasnilo (npr. zgoraj omenjena vključitev „pomožnih storitev“ v opredelitev „medosebne komunikacijske storitve“). Če to ni mogoče, delovna skupina predlaga, da vse strani, udeležene v zakonodajnem postopku, zagotovijo, da bosta obravnava predloga uredbe in Evropskega zakonika o elektronskih komunikacijah in glasovanje o njiju potekala hkrati, da bi lahko zainteresirane strani pravilno proučile področje uporabe in posledice novih instrumentov.

5. PREDLOGI ZA POJASNILA ZA ZAGOTOVITEV PRAVNE VARNOSTI

Poleg obravnavanih vprašanj želi delovna skupina poudariti tudi nekatere določbe v predlogu uredbe, ki bi jih bilo koristno pojasniti. Taka pojasnila se štejejo za potrebna za povečanje pravne varnosti za vse zainteresirane strani, da se bo uredba o zasebnosti in elektronskih komunikacijah razlagala in uporabljala enotno po vsej EU.

POJASNILO O PODROČJU UPORABE

40. Delovna skupina iz člena 29 v zvezi s področjem uporabe predloga uredbe predlaga naslednja pojasnila:

- a. **Izraz „končni uporabnik“ bi moral vključevati vse posamezne uporabnike.** V členu 2(14) Evropskega zakonika o elektronskih komunikacijah je „končni uporabnik“ opredeljen kot uporabnik, ki ne zagotavlja javnih komunikacijskih omrežij ali javnosti dostopnih elektronskih komunikacijskih storitev. Pojasniti bi bilo treba, da posamezniki, ki prispevajo k omrežjem, na primer k prepletenim omrežjem s svojim

²² V členu 4(2) predloga uredbe je navedeno, da medosebna komunikacijska storitev „vključuje storitve, ki omogočajo medosebno in interaktivno komunikacijo le kot manjši pomožni del storitve, ki je dejansko povezan z drugo storitvijo“, člen 2(5) Evropskega zakonika o elektronskih komunikacijah pa take storitve iz te opredelitve izrecno izključuje (Evropski zakonik o elektronskih komunikacijah „medosebno komunikacijsko storitev“ uvršča v širšo kategorijo „elektronske komunikacijske storitve“ iz člena 2(4)).

usmerjevalnikom Wi-Fi, niso izključeni iz obsega varstva v skladu s predlogom uredbe.

- b. **Pojasniti bi bilo treba, da ozemeljska veljavnost zajema vse končne uporabnike v Uniji.** Člen 3(1)(a) določa, da se predlog uredbe uporablja za zagotavljanje elektronskih komunikacijskih storitev končnim uporabnikom „v Uniji“, člen 3(1)(c) pa določa, da se uporablja za varstvo terminalske opreme končnih uporabnikov, „ki se nahajajo v Uniji“ (dodan poudarek). To se razlikuje v več prevodih. Nemški prevod med tem ne razlikuje, druge jezikovne različice, npr. francoska, španska in nizozemska, pa. Iz uvodne izjave 9 je razvidno, da naj bi bila ozemeljska veljavnost široka in da pri tem ni pomembno, ali se storitve zagotavljajo iz držav zunaj Unije in ali obdelava poteka v Uniji ali zunaj nje. Zato se predlaga, da se izraz „se nahajajo“ v členu 3(1)(c) črta, da bi poudarili to široko veljavnost.
- c. **Zdi se, da predlog uredbe varuje zaupne komunikacije le takrat, ko so v tranzitu, ne pa takrat, ko so shranjene.** Zdajšnji pristop v predlogu uredbe je osredotočenost na varstvo prenosa komunikacij. Glej na primer uvodno izjavo 15, v kateri je navedeno, da bi se morala prepoved prestrezanja podatkov v zvezi s komunikacijami uporabljati med njihovim prenosom, tj. dokler naslovnik ne prejme vsebine komunikacije. Obseg tega varstva temelji na zastarelem konceptualnem okviru komunikacij. Večino komunikacijskih podatkov tudi po prejemu hranijo ponudniki storitev. Zagotoviti bi bilo treba, da zaupnost teh podatkov ostane zaščitena. Poleg tega komunikacija med naročniki istih storitev v oblaku (na primer ponudniki spletne pošte) pogosto vključuje le manjši prenos; pošiljanje pošte večinoma vključuje vnos v podatkovno zbirko ponudnika in ne dejanskega pošiljanja sporočil med stranema. Trditev, da je to zajeto že v Splošni uredbi o varstvu podatkov, ni prepričljiva: cilj predloga uredbe je zaščititi vso zaupno komunikacijo ne glede na njena tehnična sredstva. Morda je to le vsebinska napaka, saj se prepoved iz člena 5 nanaša na „shranjevanje“ in „obdelavo“.
- d. **V ta sklop bi morale spadati vse javne brezžične točke dostopa do svetovnega spleta.** Ker je uporaba brezžičnih dostopnih točk splošno razširjena, je logično, da bi morala biti zaupnost komunikacije, ki se opravlja prek takih dostopnih točk, nedvomno zaščitena. Poskus, da bi to v uredbi pojasnili, pa ni bil uspešen, saj področje uporabe zajema le omrežja, ki se zagotavljajo „neopredeljeni skupini končnih uporabnikov“ (uvodna izjava 13). Opredeliti je treba izraza „neopredeljena skupina končnih uporabnikov“ in „zaprta skupina končnih uporabnikov“. Zlasti bi bilo treba pojasniti, da na področje uporabe spadajo tudi varna brezžična omrežja, tj. z geslom, če je to geslo zagotovljeno teoretično neopredeljeni skupini uporabnikov, katerih identitete ni mogoče določiti vnaprej (npr. stranke kavarne, obiskovalci letališča). V skladu s prejšnjim mnenjem delovne skupine iz člena 29 o Direktivi o zasebnosti in elektronskih komunikacijah je temeljno načelo v zvezi s tem, *da se lahko iz instrumenta o zasebnosti in elektronskih komunikacijah izvzamejo samo storitve, ki se v uradnem ali delovnem okolju zagotavljajo samo za delovne ali uradne namene, ali tehnična komunikacija med nejavnimi ali javnimi organi, namenjena samo nadzoru delovnih ali poslovnih procesov, in uporaba storitev za izključno domače namene* (str. 8).

- e. **Predlog uredbe bi moral zajemati podatke, zbrane v okviru zagotavljanja digitalnih radiodifuzijskih storitev.** Glede na občutljivo naravo vedenja gledalcev, ki razkriva njihove osebne interese in značilnosti, bi bilo treba v uredbi o zasebnosti in elektronskih komunikacijah opredeliti (morda v uvodni izjavi), da izključitev storitev, ki zagotavljajo „vsebine, ki se pošiljajo po elektronskih komunikacijskih omrežjih“, iz opredelitve „elektronske komunikacijske storitve“ ne pomeni, da so ponudniki storitev, ki zagotavljajo tako elektronske komunikacijske storitve kot storitve vsebin, izključeni s področja uporabe določb uredbe o zasebnosti in elektronskih komunikacijah, ki je usmerjena v ponudnike elektronskih komunikacijskih storitev. To je pomembno zlasti za to, ker je opravljanje storitev, ki zagotavljajo „vsebine, ki se pošiljajo po elektronskih komunikacijskih omrežjih“, v skladu s predlogom Evropskega zakonika o elektronskih komunikacijah (člen 2(4)) izključeno iz opredelitve „elektronske komunikacijske storitve“.
- f. **Komunikacijski podatki so na splošno osebni.** V uvodni izjavi 4 je poudarjeno, da komunikacijski podatki lahko vključujejo osebne podatke. Vendar je večina komunikacijskih podatkov osebnih²³ ter precej intimnih in občutljivih, zato bi bilo treba besedilo te uvodne izjave spremeniti, da bi vključevala navedbo, da so ti podatki na splošno osebni.
- g. **Zaupna komunikacija vključuje sporočila platforme.** V uvodni izjavi 1 je pojasnjeno, da se načelo zaupnosti uporablja za „sedanja in prihodnja komunikacijska sredstva“. Ta uvodna izjava se nadaljuje s seznamom primerov takih sredstev, vključno z „osebnim sporočanjem prek družbenih medijev“. To naj bi verjetno vključevalo zasebna sporočila med uporabniki družabnega omrežja (npr. Facebook ali Twitter) ali sporočila, objavljena na časovnici, ki so dostopna omejenemu številu oseb, vendar besedilo ni dovolj jasno.
- h. **Kako se uredba o zasebnosti in elektronskih komunikacijah uporablja za interakcijo stroj-stroj.** Kot je navedeno v odstavku 9, delovna skupina pozdravlja razširitev varstva na interakcijo stroj-stroj. Vendar je to omenjeno le v uvodni izjavi 12, in ne v ustreznem členu. To varstvo je zaželeno, saj take komunikacije pogosto vsebujejo informacije, zaščitene v okviru pravic do zasebnosti. Po drugi strani bi morala biti ozka kategorija le komunikacije stroj-stroj izvzeta, če ne vpliva niti na zasebnost niti na zaupnost komunikacij, na primer, kadar taka komunikacija poteka med izvajanjem protokola prenosa med omrežnimi elementi (npr. strežniki, stikala), namenjenega medsebojnemu obveščanju o statusu aktivnosti. Posebno področje v zvezi z uporabo uredbe o zasebnosti in elektronskih komunikacijah, ki bi ga bilo treba pojasniti, je področje inteligentnih prometnih sistemov. Vozila bodo podatke, ki vsebujejo enotni identifikator,

²³ Glej na primer Sodišče Evropske unije, 6. november 2003, zadeva C-101/01, točka 24 (v zvezi s telefonsko številko), Sodišče Evropske unije, 19. oktober 2016, zadeva C-582/14 (Breyer), točka 49 (v zvezi z dinamičnimi IP-naslovi), in Sodišče Evropske unije, 8 april 2014, zadevi C-239/12 in C-594/12 (Digital Rights Ireland), točki 26 in 27 (v zvezi z občutljivostjo metapodatkov).

predvidoma še naprej oddajala prek radijskih valov. Če uredba o zasebnosti in elektronskih komunikacijah ne bi zagotavljala dodatnega varstva v zvezi s komunikacijskimi podatki, bi to lahko povzročilo stalno sledenje voznim navadam, itinerarjem in hitrosti voznikov. Člen 2(1) Evropskega zakonika o elektronskih komunikacijah pa vsebuje novo in razširjeno opredelitev komunikacijskih omrežij. Vključujejo prenosne sisteme, ki nimajo centralizirane upravne zmogljivosti in ki omogočajo prenos signalov prek radijskih valov. V uvodni izjavi 14 uredbe o zasebnosti in elektronskih komunikacijah je določeno, da so taki podatki elektronski komunikacijski podatki. Na podlagi člena 5 predloga uredbe je vsaka vrsta prestrezanja, spremljanja ali shranjevanja teh komunikacijskih podatkov prepovedana, razen če se uporablja ena od izjem. Vseeno obstaja interes za obdelavo teh podatkov, saj objektom, kot so avtonomni avtomobili in naprave, omogoča, da se medsebojno opozarjajo o bližini ali drugih tveganjih. Vprašljivo je, katera izjema bi se uporabljala v tem primeru. Privolitev končnih uporabnikov ni izvedljiva izjema, ker bi se lahko pojavila potreba po tem, da bi bila obdelava teh podatkov možna v vsakem trenutku. Zato bi bilo treba ponudnikom omogočiti, da uporabijo posebno izjemo, ki objektom, kot so avtonomni avtomobili in naprave, omogoča, da se medsebojno opozarjajo o bližini ali drugih tveganjih.

POJASNILO O POJMU IN UPORABI PRIVOLITVE

41. V zvezi s pojmom in uporabo privolitve v obstoječem predlogu uredbe delovna skupina iz člena 29 predlaga naslednja pojasnila:

- a. **Uporaba pojma privolitve v zvezi s pravnimi osebami.** V uvodni izjavi 3 je poudarjeno, da bi morala uredba zagotavljati, da se določbe Splošne uredbe o varstvu podatkov uporabljajo tudi za končne uporabnike, ki so pravne osebe. To v skladu z uvodno izjavo vključuje opredelitev privolitve v skladu s Splošno uredbo o varstvu podatkov (glej tudi uvodno izjavo 18). Kot je poudarjeno v odstavku 13, delovna skupina pozdravlja izrecno vključitev pravnih oseb v področje uporabe uredbe. Uporaba tega načela v praksi pa ni jasna. V skladu s opredelitvijo v Splošni uredbi o varstvu podatkov mora biti privolitev „informirana“ izjava volje posameznika, na katerega se nanašajo osebni podatki, izražena „z izjavo ali jasnim pritrdilnim dejanjem“ (člen 4(11) Splošne uredbe o varstvu podatkov). Pojasniti je treba, kdaj se lahko pravna oseba dejansko šteje za „informirano“ in kdaj obstaja taka izjava volje pravne osebe.
- b. V zvezi s tem velja omeniti, da delodajalec v večini primerov ne more dati privolitve v imenu svojih zaposlenih, ker kadar delodajalec potrebuje privolitev zaposlenega in glede na neenakopravno razmerje moči obstaja dejanska ali potencialna pomembna škoda, ki nastane, če zaposleni ne privoli,

taka privolitve ni veljavna, ker ni dana prostovoljno²⁴. V zvezi s **podjetji, ki posameznikom izdajajo naprave ali opremo, predlog uredbe ne vsebuje (primerne) izjeme** od prepovedi poseganja. En primer je, ko delodajalec želi posodobiti telefon, ki ga je izdalo podjetje. Drug primer je, ko delodajalec zaposlenim ponudi zakupljene avtomobile in tretji osebi za upravne namene dovoli, da zbira podatke o lokaciji prek naprave, vgrajene v avtomobil. V obeh primerih ima delodajalec interes za poseganje v te naprave.

To poseganje se ne more šteti za potrebno zaradi opravljanja storitve informacijske družbe (člen 8(1)(c)) ali zaradi merjenja spletnega občinstva (člen 8(1)(d)). To bi lahko rešili z uvedbo nove izjeme, ki bo vključevala naslednje primere: (i) delodajalec zagotavlja določeno opremo v okviru delovnega razmerja, (ii) zaposleni je uporabnik te opreme in (iii) poseganje je nujno potrebno za delovanje opreme zaposlenega (kar pomeni uporabo načel sorazmernosti in subsidiarnosti v zvezi z zbiranjem podatkov). Delodajalec bi lahko posegal v napravo končnih uporabnikov samo, če so izpolnjeni ti pogoji.

- c. **Povečanje nadzora za onemogočanje avtomatičnega posredovanja klica.** Člen 14 zagotavlja pomemben nadzor za končne uporabnike, v okviru katerega se onemogoča avtomatično posredovanje klica tretje osebe. To varstvo se lahko dodatno izboljša tako, da se tudi od končnih uporabnikov že takoj zahteva privolitev v začetek posredovanja klica.

POJASNILO O PODATKIH O LOKACIJI IN DRUGIH METAPODATKIH

42. Delovna skupina predlaga, da se v zvezi s podatki o lokaciji in drugimi metapodatki pojasni naslednje:

- a. **Pojasniti bi bilo treba** pomen „**podatk[ov] o lokaciji, ki se generirajo drugače kot v okviru zagotavljanja elektronskih komunikacijskih storitev**“ v **uvodni izjavi 17**. Nejasno je, ali se to nanaša na podatke o lokaciji, zbrane na primer prek aplikacij, ki uporabljajo podatke, pridobljene prek funkcije GPS v pametnih napravah, in/ali podatke o lokaciji ustvarijo na podlagi bližnjih usmerjevalnikov Wi-Fi, in/ali podatke o lokaciji, zbrane z vgrajenimi navigacijskimi pomočniki in/ali drugimi načini ustvarjanja podatkov o lokaciji. To pomanjkanje jasnosti ustvarja pravno negotovost v zvezi z obsegom obveznosti. Podatki o lokaciji terminalske naprave fizične osebe so osebni podatki, zato za obdelavo teh podatkov veljajo obveznosti iz Splošne uredbe o varstvu podatkov.
- b. Pojasniti bi bilo treba, da **za zakonito obdelavo podatkov o lokaciji in drugih metapodatkov večinoma ni potreben enotni identifikator**. V uvodni izjavi 17 so omenjeni toplotni zemljevidi kot primer, kako ponudniki elektronskih komunikacijskih storitev uporabljajo elektronske komunikacijske metapodatke. Vendar za ustvarjanje osnovnega toplotnega

²⁴ Glej Mnenje 15/2011 o opredelitvi privolitve (WP 187), Mnenje 8/2001 o obdelavi osebnih podatkov v delovnem okolju (WP 48) in novo mnenje o obdelavi podatkov na delovnem mestu (sprejeto hkrati s tem mnenjem).

zemljevida niso potrebni enotni identifikatorji, temveč zadostuje golo statistično štetje. V tej uvodni izjavi je naveden še en primer, tj. uporaba infrastrukture in pritisk nanjo, ki ju je tudi mogoče šteti z nekaterimi merilnimi točkami, na primer z ustvarjanjem zbirnih statističnih podatkov o uporabi prometnih stolpov, ki kažejo pritisk na neki lokaciji ob določenem času, ne da bi bilo treba poznati identiteto povezanih oseb.

Poleg tega je v uvodni izjavi kot primer navedeno prikazovanje gibanja prometa v določene smeri v določenem obdobju, pri katerem bi bil potreben enotni identifikator, ki poveže položaje posameznikov v določenih časovnih presledkih. Zdi se, da želi uvodna izjava s tem primerom upravičiti nadaljnjo obdelavo teh podatkov za podpiranje analitike „velepodatkov“. V predlogu uredbe je edini pogoj za tovrstno obdelavo obveznost izvedbe ocene učinka v zvezi z varstvom podatkov, če bo obdelava *verjetno precej ogrožala pravice in svoboščine fizičnih oseb*. Ta pogoj ni zadosten. Poleg tega je v nasprotju z obveznostjo iz člena 6, da se tovrstna obdelava lahko izvede le s privolitvijo uporabnikov in če podatkov ni mogoče anonimizirati, tj. brez enotnih identifikatorjev. Uporabniki pogosto ne morejo zavrniti zbiranja podatkov o geografski lokaciji s strani ponudnikov elektronskih komunikacijskih storitev, pri katerih je tako zbiranje tehnično potrebno za prenos sporočila uporabniku ali kadar je taka obdelava potrebna za zagotovitev zahtevane storitve (na primer navigacije). Delovna skupina je v prejšnjih mnenjih ugotovila, da so taki podatki o lokaciji s pametnih naprav občutljivi osebni podatki in da koristi analize teh podatkov ne prevladajo niti nad pravicami uporabnikov do varstva zaupnosti svojih komunikacijskih metapodatkov niti nad splošnimi pravicami do varstva podatkov v skladu s Splošno uredbo o varstvu podatkov. Zato je treba v uvodni izjavi opredeliti vsaj to, da morajo ponudniki v primeru nadaljnje obdelave podatkov o lokaciji ali drugih metapodatkov izpolnjevati obveznosti iz člena 25 Splošne uredbe o varstvu podatkov. To vključuje izvedbo vsaj naslednjih ukrepov:

- (i) uporabo začasnih psevdonimov;
- (ii) izbris vseh tabel za povratno iskanje med temi psevdonimi in prvotnimi identifikacijskimi podatki;
- (iii) združevanje na raven, na kateri posameznih uporabnikov ni mogoče več identificirati prek njihovih posebnih itinerarjev, in
- (iv) izbris vrednosti izven območja, v zvezi s katerimi bi bila identifikacija še vedno mogoča (vse te ukrepe je treba uporabljati skupaj).

Poleg tega mora uredba o zasebnosti in elektronskih komunikacijah od oseb, vključenih v obdelavo podatkov o lokaciji in drugih metapodatkov, zahtevati, da svoje metode anonimizacije in nadaljnjega združevanja objavijo brez poseganja v tajnost, ki je zagotovljena z zakonodajo. To bi tako nadzornim organom kot širši javnosti omogočilo, da zlahka preverijo, ali je izbrana metoda ustrezna.

43. Delovna skupina predlaga, da se v zvezi z nepovabljenimi sporočili pojasni naslednje:

- a. **Besedilo prepovedi neposrednega trženja brez privolitve.** V členu 16(1) predloga uredbe je trenutno navedeno, da se elektronske komunikacijske storitve „lahko“ uporabljajo za namene pošiljanja sporočil za neposredno trženje (s privolitvijo), ne vsebuje pa izrecne prepovedi pošiljanja (namenjanja ali predložitve) sporočil za neposredno trženje brez privolitve. To je v nasprotju s pristopom v drugih določbah, v katerih je naprej oblikovana prepoved, nato pa ji sledijo nekatere posebne izjeme. Obstoječe besedilo izraža bolj popustljiv pristop (ki domnevno ni načrtovan). Delovna skupina predlaga nekoliko spremenjeno besedilo obstoječega člena 13(1) Direktive o zasebnosti in elektronskih komunikacijah: „Uporaba elektronskih komunikacijskih storitev, vključno z govorno-govornimi klici, avtomatiziranih klicnih in komunikacijskih sistemov, vključno s polavtomatiziranimi sistemi, ki klicanega povežejo s posameznikom, faksom in elektronske pošte ali druga uporaba elektronskih komunikacijskih storitev za namene predstavitve sporočil neposrednega trženja končnim uporabnikom je dovoljena samo za končne uporabnike, ki dajo za to predhodno privolitev.“
- b. **Področje uporabe določb o sporočilih za namene trženja in klicanje obstoječih stikov.** Člen 16(2) določa, da kadar oseba pridobi podatke o elektronskem naslovu za elektronsko pošto obstoječe stranke, lahko te podatke uporabi za nadaljnjo neposredno trženje lastnih proizvodov in storitev le, če je strankam pri zbiranju in ko se pošlje sporočilo dana jasna, brezplačna in enostavna možnost, da nasprotujejo takšni uporabi. To je trenutno omejeno na komercialne stike, pridobljene „v okviru prodaje proizvoda ali storitve“, in za nadaljnje komercialno trženje podobnih lastnih proizvodov ali storitev. Glede na to, da se določbe o neposrednem trženju uporabljajo tudi za nekomercialne promocijske dejavnosti (npr. dobrodelnih organizacij ali političnih strank), bi bilo treba to določbo spremeniti, da bi se uporabljala tudi za nekomercialne organizacije, da bi pri promociji podobnih lastnih ciljev ali idealov vzpostavile stike s prejšnjimi podporniki, za klice za namene neposrednega trženja pa bi morala veljati enaka pravica do ugovora. Poleg tega bi bilo treba določiti obdobje veljavnosti „stikov z obstoječimi strankami“ v elektronskih komunikacijah za komercialni, dobrodelni ali politični namen, ki bi moralo veljati tudi za klice za namene neposrednega trženja. Kadar se države članice odločijo za sistem ugovora proti govorno-govornim klicem za namene trženja, prisotnost razmerja „stikov z obstoječimi strankami“ razveljavi vpis v register neželenih klicev. V tem primeru končni uporabniki nimajo učinkovite možnosti za preprečevanje nadležnih klicev podjetij ali organizacij, s katerimi so bili včasih v stiku, vendar ne želijo več sodelovati z njimi. Splošno gledano bi bilo zato treba v uredbi ob upoštevanju legitimnih pričakovanj udeleženih končnih uporabnikov določiti veljavnost te izjeme „obstoječe stranke“, ki bi na primer trajala eno ali dve leti.
- c. **Uporaba pravil o neposrednem trženju za pravne osebe.** Člen 16(5) predloga uredbe določa, da države članice zagotovijo, da so legitimni interesi končnih uporabnikov, ki so pravne osebe, glede nepovabljenih sporočil ustrezno zaščiteni. V členu 13(5) veljavne Direktive o zasebnosti in

elektronskih komunikacijah so opisani legitimni interesi naročnikov, ki niso fizične osebe. Ni jasno, kakšne so posledice te spremembe besedila. V uvodnih izjavah bi bilo treba pojasniti, da ta sprememba ne izraža namena zagotoviti nižjo raven varstva. V zvezi s tem se prepoved neposrednega trženja brez privolitve nanaša na „končn[e] uporabnik[e], ki so fizične osebe in ki so v to privolili“ (dodan poudarek). Pojasniti bi bilo treba, da to vključuje fizične osebe, ki *delajo* za pravne osebe. Po drugi strani privolitev ne bi bila potrebna za vzpostavitev stika s pravnimi osebami prek splošnih kontaktnih podatkov, ki so jih objavile v ta namen (na primer „info@imepodjetja.eu“).

- d. **Uporaba pravil o neposrednem trženju za osebe, ki opravljajo vlogo (političnih) predstavnikov:** osnutek člena 16 v sedanji obliki lahko prepreči pošiljanje nekaterih sporočil izbranim predstavnikom, v katerih so opisani komercialni pomisleki ali interesi. Pojasniti bi bilo treba, da uredba ne preprečuje takih sporočil.

POJASNILO O UPORABI INSTRUMENTOV NA PODROČJU TEMELJNIH PRAVIC

44. Dodatno bi bilo treba pojasniti **uporabo Listine in Konvencije o varstvu človekovih pravic in temeljnih svoboščin (v nadaljnjem besedilu: EKČP) v okviru nacionalne zakonodaje na področju hrambe podatkov**. V uvodni izjavi 26 je določeno, da morajo biti vsi ukrepi držav članic za zaščito javnih interesov, na primer ukrepi zakonitega prestrežanja, v skladu z Listino (poleg EKČP). To je zaželeno, saj je v skladu z razlogovanjem v zadevi Tele2/Watson, tj. da se za vse nacionalne izjeme od varstva pri obdelavi podatkov v skladu s pravom EU uporablja Listina (in da je zato mogoče v zvezi s kršitvami nacionalnega prava sprožiti postopek pred Sodiščem Evropske unije). V členu 11 predloga uredbe pa je navedeno le, da mora omejitev področja uporabe členov od 5 do 8 predloga uredbe spoštovati bistvo temeljnih pravic in svoboščin ter mora biti potreben in sorazmeren ukrep. V ta sklop bi bilo treba vključiti tudi izrecno sklicevanje na Listino in EKČP.
45. **Da je zaupnost komunikacij zaščiten tudi v skladu s členom 8 EKČP.** V odstavku 1.1 memoranduma in uvodni izjavi 1 je pojasnjeno, da predlog uredbe izvaja člen 7 Listine. To se ponovi v uvodni izjavi 19. Temeljna pravica do zaupnih komunikacij pa ni zaščiten le v tej določbi, temveč tudi v skladu s členom 8 EKČP. Vključitev izrecnega sklicevanja v člen predloga uredbe bi dodatno potrdila, da bo treba pri ocenjevanju (končne) uredbe upoštevati tudi vso ustrezno sodno prakso Evropskega sodišča za človekove pravice. To sklicevanje je že vključeno v uvodni izjavi 20 (v zvezi s terminalsko opremo) in 26 (v zvezi z zakonitim prestrežanjem) ter dodatno podprto s premisleki v odstavku 2.1 memoranduma (o razmerju med Listino in EKČP v zvezi s pravnimi osebami), ne pa v ustrezne člene, kot je člen 11(1).

DRUGA POJASNILA

46. Pojasniti bi bilo treba, da **obveznosti v skladu s Splošno uredbo o varstvu podatkov, na primer v zvezi s sistemom za kršitve varstva osebnih podatkov in**

ocenami učinka v zvezi z varstvom podatkov, še naprej veljajo, kadar stranke obdelujejo osebne podatke v okviru elektronskih komunikacijskih podatkov. Ker je v uvodni izjavi 5 navedeno, da je predlog uredbe *lex specialis* glede na Splošno uredbo o varstvu podatkov in da bi morala biti obdelava elektronskih komunikacijskih podatkov dovoljena le v skladu s predlogom uredbe, se postavlja vprašanje, ali se nekatere obveznosti iz Splošne uredbe o varstvu podatkov uporabljajo tudi v okviru predloga uredbe. To zlasti velja, kadar bi se predlog uredbe lahko razlagal v smislu, da ureja neko obveznost, ki jo zajema tudi Splošna uredba o varstvu podatkov. Okvirni primeri vključujejo:

- (i) predlog uredbe zahteva določeno obveščanje o „odkritih“ varnostnih tveganjih (člen 17) (glej tudi odstavek 35), vendar Splošna uredba o varstvu podatkov vsebuje sistem obveščanja o kršitvah varstva osebnih podatkov (člena 33 in 34);
- (ii) v predlogu uredbe je navedeno, da sta izvajanje ocene učinka v zvezi z varstvom podatkov in posvetovanje z nadzornim organom v skladu s Splošno uredbo o varstvu podatkov v nekaterih primerih obvezna (uvodni izjavi 17 in 19 ter člen 6(3)(b)), v Splošni uredbi o varstvu podatkov pa je že določeno, kdaj je treba izvesti oceno učinka v zvezi z varstvom podatkov in kdaj je potrebno posvetovanje (člena 35 in 36), in
- (iii) ni opredeljeno, da je treba poleg izpolnjevanja potrebnih pogojev za izjemo od prepovedi obdelave v skladu s členom 5 predloga uredbe izpolnjevati tudi vse ustrezne obveznosti iz Splošne uredbe o varstvu podatkov, kadar zadeva obdelavo osebnih podatkov in je vsaka druga obdelava v skladu s Splošno uredbo o varstvu podatkov prepovedana. Pojasniti bi bilo treba, da se glede na to ne uporablja preskus združljivosti iz člena 6(4) Splošne uredbe o varstvu podatkov in
- (iv) predlog uredbe o zasebnosti in elektronskih komunikacijah ne predvideva mehanizma potrjevanja, ki bi bil podoben tistemu iz členov 42 in 43 Splošne uredbe o varstvu podatkov. Ker je področje uporabe člena 42 Splošne uredbe o varstvu podatkov strogo gledano omejeno na vzpostavitev mehanizmov potrjevanja za varstvo podatkov ter pečatov in označb za varstvo podatkov za dokazovanje skladnosti s Splošno uredbo o varstvu podatkov, bi bilo treba razmisliti o tem, da se primerljiva določba ne bi uvedla, da bi omogočili potrjevanje skladnosti dejanj obdelave, standardov, proizvodov ali storitev z uredbo o zasebnosti in elektronskih komunikacijah.

Da bi zagotovili, da se to pomanjkanje jasnosti ne bo uporabilo kot argument za znižanje ravni varstva v skladu s predlogom uredbe, bi bilo treba pojasniti, da morajo upravljavci v vseh teh primerih upoštevati tudi Splošno uredbo o varstvu podatkov.

47. Pojasniti bi bilo treba tudi, da **zahteva glede preklica privolitve velja tudi v okviru poseganja v terminalske opreme**. Člen 8(1)(b) predloga uredbe predvideva možnost poseganja v terminalske opreme končnih uporabnikov z njihovo privolitvijo. Člen 9(3) zahteva, da morajo imeti končni uporabniki možnost, da kadar koli prekličejo svojo privolitev, vendar to velja samo za privolitev v analizo metapodatkov in vsebine. Pojasniti bi bilo treba, da ta obveznost zajema tudi poseganje v terminalske opreme.

48. V zvezi s tem bi bilo treba pojasniti, da **opominjanje o možnosti preklica privolitve velja tudi za privolitev prek nastavitev brskalnika**. Člen 9(3) zahteva, da se končne uporabnike o možnosti, da privolitev kadar koli prekličejo, opominja v rednih šestmesečnih intervalih. Ob tem ko po mnenju delovne skupine splošne nastavitve brskalnikov in druge programske opreme, vključno z operacijskimi sistemi, aplikacijami in vmesniki za programsko opremo za naprave, povezane v internet stvari (tj. ne na podlagi posebnega podrobnega nadzora), ne morejo biti veljaven ukrep za zagotovitev privolitve, saj v okviru splošnih nastavitev ni mogoče dati posebne privolitve v posebne scenarije (glej odstavek 24), bi morale biti privzete nastavitve uporabnikom prijazne (glej odstavek 19). Če se bo to v predlogu uredbe ohranilo, morajo biti nastavitve dovolj podrobne, da bodo omogočile nadzor vseh vrst obdelave podatkov, v katere je uporabnik privolil, in zajemale vse funkcionalnosti opreme, ki bi lahko povzročile obdelavo podatkov. Poleg tega bi bilo treba končne uporabnike vsaj v rednih (šestmesečnih) intervalih opominjati o tem, da lahko te nastavitve spremenijo.
49. Pozdravlja se, da predlog uredbe zahteva, da programska oprema, ki je že bila dana na trg, končnega uporabnika obvesti o možnostih nastavitve zasebnosti (člen 10). **Nejasno pa je, kako se lahko to dejansko uporabi za obstoječe proizvode** in druge proizvode, ki niso več podprti. Poleg tega bi bilo treba dodatno pojasniti, kako se bo ta obveznost uporabljala za odprtokodno programsko opremo, ki je razvita odprto in decentralizirano.
50. Pojasniti bi bilo treba, da ima **zagotavljanje možnosti onemogočanja piškotkov (tretjih strank) iz člena 10 predloga uredbe prednost pred izjemo za merjenje spletnega občinstva** iz člena 8(1)(d). Ali povedano drugače: čeprav lahko spletišče uporablja analizo za merjenje spletnega občinstva iz člena 8(1)(d), bi morali imeti uporabniki še vedno pravico, da v brskalniku onemogočijo te tehnologije sledenja.
51. **Pojasniti bi bilo treba opredelitev (pol)avtomatiziranih klicnih in komunikacijskih sistemov**. Opredelitev tega izraza v členu 4(3)(h) predloga uredbe se v drugem delu povedi sklicuje na sam izraz („vključno s klici, pri katerih se z uporabo avtomatiziranih klicnih in komunikacijskih sistemov klicano osebo poveže s posameznikom“). Predlaga se, da se iz opredelitve črta ta zadnji stavek in spremeni opredelitev v členu 4(3)(g), da bi vključevala klice, opravljene s polavtomatiziranimi komunikacijskimi sistemi, kot so na primer avtomatični klicalniki, ki klicano osebo povežejo s posameznikom.
52. **Pojasniti bi bilo treba informacije, ki „spadajo v naročnino na storitev“**. V uvodni izjavi 14 je omenjeno, da elektronski komunikacijski metapodatki „lahko vključujejo informacije, ki spadajo v naročnino na storitev, kadar se take informacije obdelujejo za namene prenašanja, razširjanja ali izmenjave vsebine elektronskih komunikacij“. Namen tega besedila ni jasen.
53. Pojasniti bi bilo treba **uporabo mehanizmov za skladnost in sodelovanje**. V uvodni izjavi 38 je poudarjeno, da predlog uredbe temelji na mehanizmu za skladnost iz Splošne uredbe o varstvu podatkov. Poleg tega člen 18(1) določa, da se poglavji VI in VII Splošne uredbe o varstvu podatkov uporabljata smiselno. V členu 19 je

poudarjeno še, da Evropski odbor za varstvo podatkov opravlja naloge iz člena 70 Splošne uredbe o varstvu podatkov. Čeprav je uporaba teh določb sorazmerno jasna, ni mogoče izključiti, da se ne bodo pojavila vprašanja glede razlage ključnih pojmov mehanizmov za skladnost in sodelovanje iz Splošne uredbe o varstvu podatkov. Mehanizem vodilnega organa se na primer uporablja v primerih, ko se „obdelav[a] [...] izvaja [...] na čezmejni ravni“ (člen 56(1) Splošne uredbe o varstvu podatkov): ni jasno, kako se to uporablja v primeru poseganja v terminalsko opremo ali analize vsebine ali metapodatkov v skladu s predlogom uredbe. Zato se priporoča, da se v uvodni izjavi pojasni uporaba teh ključnih pojmov in poudari, da bodo vsa preostala vprašanja v zvezi z uporabo teh poglavij Splošne uredbe o varstvu podatkov v okviru predloga uredbe rešena z razlago določb teh poglavij v skladu z njihovim namenom. Poleg tega je priporočljivo pojasniti, da se člen 70 za Evropski odbor za varstvo podatkov v okviru predloga uredbe uporablja smiselno (to zdaj v uvodni izjavi manjka).

* * *