



**17/LV**

**WP 247**

**Atzinums 01/2017 par  
priekšlikumu E-privātuma regulai (2002/58/EK)**

**Pieņemts 2017. gada 4. aprīlī**

Šī darba grupa izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas padomdevēja institūcija datu aizsardzības un privātuma jautājumos. Tās uzdevumi ir aprakstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā.

Sekretariāta pakalpojumus nodrošina Eiropas Komisijas Tiesiskuma un patērētāju ģenerāldirektorāta C direktorāts (Pamattiesības un tiesiskums), B-1049 *Brussels, Belgium*, birojs Nr. MO-59 05/035.

Tmekļa vietne: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

**DARBA GRUPA PERSONU AIZSARDZĪBAI ATTIECĪBĀ UZ PERSONAS DATU APSTRĀDI,**

kas izveidota ar Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK,

ņemot vērā tās 29. un 30. pantu,

ņemot vērā darba grupas reglamentu,

**IR PIEŅĒMUSI ŠO ATZINUMU.**

## KOPSAVILKUMS

Darba grupa atzinīgi vērtē Eiropas Komisijas 2017. gada 10. janvāra priekšlikumu E-privātuma regulai. Darba grupa atzinīgi vērtē **regulas** kā reglamentējošā instrumenta **izvēli**. Tādējādi tiek nodrošināti vienādi noteikumi visā ES un skaidrība gan uzraudzības iestādēm, gan organizācijām. Tas arī palīdz nodrošināt atbilstību Vispārējai datu aizsardzības regulai. Šādu atbilstību vēl vairāk apstiprina izvēle par atbildīgo e-privātuma noteikumu izpildei nozīmēt **to pašu iestādi, kas ir atbildīga par VDAR atbilstības uzraudzību**.

Vienlaicīgi pozitīvi vērtējama **papildu juridiskā instrumenta** (saglabāšanas) izvēle. Konfidencialas saziņas un galiekārtu aizsardzībai ir īpašas iezīmes, kuras nav aplūkotas VDAR. Tāpēc ir vajadzīgi papildu noteikumi attiecībā uz šiem pakalpojumu veidiem, lai nodrošinātu pamattiesību uz privāto dzīvi un saziņas konfidencialitātes, tostarp galiekārtu konfidencialitātes, pienācīgu aizsardzību. Šajā sakarā darba grupa stingri atbalsta **principiālo pieeju**, kas izvēlēta ierosinātajā regulā, ar **plašu aizliegumu un šauru izņēmumu izmantošanu, kā arī mērķtiecīgu piekrišanas jēdziena piemērošanu**.

Darba grupa atzinīgi vērtē ierosinātās regulas darbības jomas paplašināšanu, **iekļaujot *Over-The-Top* (OTT) pakalpojumu sniedzējus**, pakalpojumus, kas ir funkcionāli līdzvērtīgi tradicionālākiem saziņas līdzekļiem, un tādējādi tiem ir līdzīgs potenciāls ietekmēt privātumu un tiesības uz ES iedzīvotāju saziņas slepenību. Tāpat ir pozitīvi, ka ierosinātajā regulā ir skaidri ietverts **saturs un saistītie metadati**, un atzīts, ka **metadati var atklāt ļoti sensitīvus datus**.

Tomēr darba grupa arī atzīmē četrus apsvērumus, kas raisa **nopietnas bažas**. Attiecībā uz **galiekārtu atrašanās vietas izsekošanu, nosacījumiem, saskaņā ar kuriem ir atļauta satura un metadatu analīze, galiekārtu un programmatūras noklusējuma iestatījumiem un attiecībā uz izsekošanas sienām** šī ierosinātā regula samazinātu VDAR paredzēto aizsardzības līmeni. Šajā atzinumā darba grupa sniedz konkrētus ieteikumus, lai nodrošinātu, ka E-privātuma regula garantēs tādu pašu vai augstāku aizsardzības līmeni, kas atbilst sakaru datu (gan satura, gan metadatu) sensitīvajam raksturam.

Attiecībā uz **WiFi izsekošanu** atkarībā no datu vākšanas apstākļiem un mērķiem šādai izsekošanai saskaņā ar VDAR, iespējams, ir nepieciešama piekrišana vai to var veikt tikai tad, ja vāktie personas dati ir anonimizēti. Pēdējā gadījumā ir jānodrošina atbilstība šādiem četriem nosacījumiem: datu vākšanas no galiekārtām mērķis ir tikai statistikas uzskaitē, izsekošana ir ierobežota laikā un telpā, ciktāl tas ir noteikti nepieciešams šim nolūkam, dati tiks dzēsti vai anonimizēti tūlīt pēc tam, un pastāv iedarbīgas nepiekrišanas iespējas. Eiropas Komisija tiek aicināta veicināt tehnisko standartu mobilajām ierīcēm, lai automātiski brīdinātu par šādu izsekošanu.

Attiecībā uz **satura un metadatu analīzi** izejas punktam vajadzētu būt tādām, ka ir aizliegts apstrādāt sakaru datus bez visu galalietotāju (sūtītāju un saņēmēju) piekrišanas. Lai ļautu pakalpojumu sniedzējiem nodrošināt lietotāja skaidri pieprasītus pakalpojumus, piemēram, meklēšanas un indeksēšanas funkcionalitāti vai teksta-runas pakalpojumus, būtu jāizmanto vietējs izņēmums satura un metadatu apstrādei tikai paša lietotāja personīgajām vajadzībām.

Attiecībā uz **piekrišanu izsekošanai** darba grupa aicina nepārprotami aizliegt izsekošanas sienas, tas ir, tādas izvēles iespējas, kas liek lietotājiem piekrist izsekošanai, ja viņi vēlas piekļūt pakalpojumam.

Visbeidzot, bet ne mazāk svarīgi, darba grupa iesaka, ka galiekārtām un programmatūrai **pēc noklusējuma jāpiedāvā privātuma aizsardzības iestatījumi** un jāpiedāvā lietotājiem skaidras iespējas šos noklusējuma iestatījumus apstiprināt vai mainīt uzstādīšanas laikā. Iestatījumiem lietošanas laikā ir jābūt viegli pieejamiem. Izmantojot pārlūka iestatījumus, lietotājam jābūt iespējai sniegt konkrētu piekrišanu. Vēlmēm attiecībā uz privātumu nevajadzētu aprobežoties tikai ar trešo personu iejaukšanos vai sīkdatnēm. Darba grupa stingri iesaka noteikt obligātu “neizsekošanas” standarta ievērošanu.

Darba grupa ir arī norādījusi citus jautājumus, kas rada bažas, piemēram, darbības jomu, galiekārtu aizsardzību un tiešo tirgvedību. Visbeidzot, bet ne mazāk svarīgi, darba grupa ir norādījusi jautājumus, kuriem nepieciešams paskaidrojums, lai labāk aizsargātu galalietotājus un ieviestu lielāku tiesisko noteiktību visām ieinteresētajām personām.

## SATURS

|  |           |
|--|-----------|
| <b>1. IEVADS.....</b>  | <b>6</b>  |
| <b>2. IEROSINĀTĀS REGULAS POZITĪVIE ASPEKTI .....</b>  | <b>6</b>  |
| <i>ES mēroga saskaņošana, sodu pielīdzināšana un izpildes panākšana tikai datu aizsardzības iestāžu kompetencē .....</i> | <i>6</i>  |
| <i>Darbības jomas paplašināšana, salīdzinot ar E-privātuma direktīvu .....</i>   | <i>7</i>  |
| <i>Pieņemšanas jēdziena mērķtiecīga piemērošana .....</i>  | <i>10</i> |
| <b>3. JAUTĀJUMI, KAS RAISA NOPIETNAS BAŽAS.....</b>  | <b>10</b> |
| <i>Ierosinātā regula apdraud VDAR paredzēto aizsardzību.....</i>   | <i>10</i> |
| <b>4. CITI JAUTĀJUMI, KAS RADA BAŽAS .....</b>   | <b>16</b> |
| <i>Ir jāpaplašina teritoriālā un materiālā darbības joma .....</i>   | <i>16</i> |
| <i>Ir jāstiprina galiekārtu aizsardzība .....</i>  | <i>17</i> |
| <i>Tiešā tirgvedība .....</i>  | <i>20</i> |
| <i>Grafiks .....</i>   | <i>23</i> |
| <i>Citi jautājumi, kas raisa bažas .....</i>   | <i>23</i> |
| <b>5. IEROSINĀJUMI PRECIZĒJUMIEM, LAI NODROŠINĀTU TIESISKO NOTEIKTĪBU .....</b>  | <b>25</b> |
| <i>Darbības jomas precizējumi .....</i>  | <i>26</i> |
| <i>Pieņemšanas jēdziena un piemērošanas precizējumi.....</i>   | <i>28</i> |
| <i>Atrašanās vietas un citu metadatu precizējumi.....</i>  | <i>29</i> |
| <i>Precizējumi par nepasūtītiem paziņojumiem .....</i>   | <i>30</i> |
| <i>Precizējumi par pamattiesību instrumentu piemērošanu.....</i>   | <i>32</i> |
| <i>Citi precizējumi.....</i>   | <i>32</i> |

## 1. IEVADS

1. 29. panta datu aizsardzības darba grupa (darba grupa vai DG29) atzinīgi vērtē Eiropas Komisijas (EK) priekšlikumu par E-privātuma regulu (regulas priekšlikums, ierosinātā regula vai E-privātuma regula)<sup>1</sup>, kuras mērķis ir aizstāt E-privātuma direktīvu (ePD)<sup>2</sup>.
2. Daudzi ierosinātās regulas aspekti ir pozitīvi, un Eiropas Komisija ir spērusi svarīgu soli, iesniedzot šo regulas priekšlikumu. Tomēr regulas priekšlikumu var uzlabot. Tādējādi tiktu ne tikai labāk aizsargāti galalietotāji, bet arī ieviesta lielāka tiesiskā noteiktība visām ieinteresētajām personām.
3. Tāpēc darba grupa ir norādījusi vairākus punktus, kas rada bažas, un ieteikumus precizējumiem, kurus Eiropas Parlamentam un Ministru padomei jāizskata, apspriežot ierosināto regulu. Šajā atzinumā vispirms tiks apskatīti ierosinātās regulas pozitīvie aspekti un pēc tam tiks izcelti jautājumi, kas rada bažas, kā arī jautājumi, kuri jāprecizē.

## 2. IEROSINĀTĀS REGULAS POZITĪVIE ASPEKTI

*ES MĒROGA SASKAŅOŠANA, SODU PIELĪDZINĀŠANA UN IZPILDES PANĀKŠANA TIKAI DATU AIZSARDZĪBAS IESTĀŽU KOMPETENCĒ*

4. Darba grupa atzinīgi vērtē **regulas kā reglamentējošā instrumenta izvēli**. Tas nodrošina, ka noteikumi ir vienādi visā ES (ar dažiem izņēmumiem, kas tiks apspriesti turpmāk). Tas nodrošina skaidrību gan uzraudzības iestādēm, gan arī organizācijām. Turklāt, ņemot vērā būtisko lomu, kāda Vispārīgajai datu aizsardzības regulai (VDAR)<sup>3</sup> ir paredzēta ierosinātajā regulā, tas palīdz nodrošināt atbilstību starp abiem instrumentiem. Vienlaicīgi pozitīvi vērtējama **papildu juridiskā instrumenta** (saglabāšanas) izvēle. Konfidencialas saziņas un galiekārtu aizsardzībai ir īpašas iezīmes, kuras nav aplūkotas VDAR. Tāpēc ir vajadzīgi papildu noteikumi attiecībā uz šiem pakalpojumu veidiem, lai nodrošinātu pienācīgu šīs pamattiesības aizsardzību. Šajā kontekstā darba grupa arī **atbalsta principiālo pieeju, kas izraudzīta ierosinātajā regulā, par plašu aizliegumu un šauru izņēmumu**

<sup>1</sup> Priekšlikums Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā un ar ko atceļ Direktīvu 2002/58/EK (Privātuma un elektronisko sakaru regula), 2017/0003 (COD), tīmekļa vietne: [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=41241](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241).

<sup>2</sup> Eiropas Parlamenta un Padomes Direktīva 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektronisko komunikāciju), (OV L 201, 31.7.2002., 37.-47. lpp.: <http://eur-lex.europa.eu/legal-content/LV/TXT/HTML/?uri=CELEX:32002L0058>).

<sup>3</sup> Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula), OV L 119/1, 4.5.2016., 1.-88. lpp.: <http://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:32016R0679>

**izmantošanu**, un uzskata, ka būtu jāizvairās no atvērtu izņēmumu ieviešanas saskaņā ar VDAR 6. pantu un jo īpaši VDAR 6. panta f) apakšpunktu (likumīgās intereses pamats).

5. **Par šo noteikumu izpildes panākšanu atbild tā pati iestāde, kas ir atbildīga par VDAR atbilstības uzraudzību**, kas ļaus tālāk nodrošināt atbilstību starp abiem instrumentiem. Ņemot vērā saikni starp personas datu aizsardzību un konfidencialas saziņas un galiekārtu aizsardzību, ir lietderīgi saskaņā ar ierosināto regulu paredzēto noteikumu izpildes panākšanu uzticēt tai pašai uzraudzības iestādei, kura īsteno VDAR (ierosinātās regulas 38. apsvērums un 18. pants). Turklāt Eiropas Savienības Tiesas (EST)<sup>4</sup> judikatūrā ir apstiprināts, ka uzraudzības iestādes neatkarība ir būtiska, kā tas paredzēts Hartas 7. pantā. Tomēr praksē tas nozīmētu papildu darbu datu aizsardzības iestādēm, negarantējot izpildi, ja netiek piešķirti papildu budžeta līdzekļi. Tādēļ datu aizsardzības iestādes atzinīgi vērtē ierosinātās regulas 38. apsvērumu, kurā uzsvērts, ka katrai uzraudzības iestādei jānodrošina papildu finanšu resursi, cilvēkresursi, telpas un infrastruktūra, kas nepieciešama efektīvai uzdevumu veikšanai saskaņā ar jauno regulu. Tāpat ir atzinīgi vērtējams, ka 18. panta 2. punkts nodrošina juridisko pamatu sadarbībai starp ierosinātās regulas uzraudzības iestādēm un ierosinātās direktīvas par Eiropas Elektronisko sakaru kodeksa (EESK) izveidi valstu regulatīvajām iestādēm<sup>5</sup>.
6. Ņemot vērā ciešo saikni starp ierosināto regulu un VDAR, tiek arī atzinīgi vērtēta **ierosinātajā regulā paredzētā naudas sodu pielīdzināšana VDAR**. Ierosinātās regulas darbības jomā ietvertās darbības ir diezgan sensitīvas un ietver cita starpā iekļaušanos konfidencialā saziņā un galiekārtās. Naudas sodiem jābūt samērīgiem ar šo sensitīvo kontekstu. Šis konteksts ir arī iemesls, kādēļ ir svarīga saskaņošana visā ES, lai nodrošinātu vienādu augsta līmeņa aizsardzību visā reģionā. Ierosinātās regulas 23. pantā ir paredzēti efektīvi naudas sodi par regulas pārkāpšanu, kas līdzinās naudas sodu apmēram, kāds noteikts par VDAR noteikumu pārkāpumiem, izņemot dažus punktus (skatīt 38. piezīmi).
7. Atzinīgi vērtējama arī **konkrētu noteikumu par paziņošanu par personas datu pārkāpumu svīturošana** no šī tiesību akta, lai novērstu nevajadzīgu pārklāšanos ar VDAR datu aizsardzības pārkāpumu prasībām.
8. **Atzinīgi vērtējams arī, ka tagad uzmanība tiek pievērsta visiem galalietotājiem vienāda aizsardzības līmeņa nodrošināšanai**, jo ierosinātajā regulā netiek izdalīta atšķirība starp “abonentiem” un citiem elektronisko sakaru pakalpojumu lietotājiem.

*DARBĪBAS JOMAS PAPLAŠINĀŠANA, SALĪDZINOT AR E-PRIVĀTUMA DIREKTĪVU*

<sup>4</sup> Skatīt, piem., EST 2015. gada 6. oktobra spriedumu lietā C-362/14 (*Safe Harbor*), 41. punkts, un EST 2016. gada 21. decembra spriedumu lietās C-203/15 un C-698/15 (*Tele2/Watson*), 123. punkts.

<sup>5</sup> Priekšlikums Eiropas Parlamenta un Padomes direktīvai, ar ko izveido Eiropas Elektronisko sakaru kodeksu (pārstrādāta redakcija), 2016/0288 (COM), 12.10.2016., tīmekļa vietne: [http://eur-lex.europa.eu/legal-content/tv/ALL/?uri=comnat:COM\\_2016\\_0590\\_FIN](http://eur-lex.europa.eu/legal-content/tv/ALL/?uri=comnat:COM_2016_0590_FIN)

9. Darba grupa atzinīgi vērtē **ierosinātās regulas darbības jomas paplašināšanu, iekļaujot *Over-The-Top (OTT)* pakalpojumu sniedzējus**, pakalpojumus, kas ir funkcionāli līdzvērtīgi tradicionālākiem saziņas līdzekļiem, un tādējādi tiem ir līdzīgs potenciāls ietekmēt privātumu un tiesības uz ES pilsoņu saziņas slepenību. Darba grupa īpaši atzinīgi vērtē, ka visas *OTT* kategorijas (*OTT0*, *OTT1* un daži *OTT2*)<sup>6</sup> tagad ir ietvertas regulas darbības jomā, jo tā attiecas ne tikai uz tradicionālajiem saziņas līdzekļiem (*OTT0*), bet arī funkcionāli līdzvērtīgiem pakalpojumiem (*OTT1*), kā minēts ierosinātās regulas 8. panta 1. punkta c) apakšpunktā. Tāpat ir pozitīvi, ka papildus EESK definīcijām ir iekļauti daži *OTT2* gadījumi, kad tie nodrošina interaktīvu starppersonu saziņu, kas ir būtiski saistīta ar to sniegto pakalpojumu, piemēram, spēlēs, iepazīšanās lietotnēs vai pārskatīšanas vietnēs (ierosinātās regulas 4. panta 2. punkts). Līdzīgi, atzinīgi vērtējams arī **precizējums, ka aizsardzība attiecas arī uz mašīnas-mašīnas mijiedarbību**. 12. apsvērumā skaidri norādīts, ka ierīces ar savstarpēju saziņu ietilpst ierosinātajā regulā paredzētajā aizsardzības piemērošanas jomā. Tas ir vēlams, jo šāda saziņa nereti satur informāciju, kuru aizsargā tiesības uz privātumu. Tomēr piemērojamību varētu precizēt (skatīt 40.h. piezīmi).
10. Ir arī pozitīvi, ka **ierosinātā regula nepārprotami attiecas uz saturu un saistītajiem metadatiem**. 14. apsvērumā ir skaidri noteikts, ka "Elektronisko sakaru datu" definīcija 4. panta 3. punkta a) apakšpunktā ir paredzēta pietiekami plaša, lai aptvertu *visu* saturu, kā arī saistītos metadatus, neatkarīgi no, piemēram, signālu nodošanas līdzekļiem. Tomēr darba grupa kā jautājumu, kas raisa bažas, 39. piezīmē atzīmē, ka pašreizējā "elektronisko sakaru datu" definīcija joprojām tiek apspriesta. Atbilstoši darbības jomas paplašināšanai darba grupa **konstatē, ka metadati var atklāt ļoti sensitīvus datus** (skatīt Paskaidrojuma raksta 2.2. punktu, 2. apsvērumu), kas ir būtisks papildinājums. Darba grupa atzinīgi vērtē faktu, ka Eiropas Komisija šādā veidā iekļauj EST apsvērumus lietās *Digital Rights Ireland* un *Tele2/Watson*. DG29 arī novērtē **atzinumu, ka satura analīze ir augsta riska apstrāde**. 19. apsvērumā un 6. panta 3. punkta b) apakšpunktā izklāstīts loģisks juridiskais pieņēmums, ka satura skenēšana ir augsta riska apstrāde saskaņā ar VDAR 35. pantu, un, acīmredzot, neatkarīgi no tā, vai pastāv augsts nenovērstais risks, vienmēr ir nepieciešama iepriekšēja apspriešanās ar (vadošo) datu aizsardzības iestādi. Vienlaicīgi darba grupai ir bažas par metadatu definīcijas tvērumu un to, ka uz metadatu analīzi neattiecas tā pati obligātā DAIN prasība (skatīt 33. un 46. piezīmi).
11. Tiek novērtēta arī **anonimizācijas nozīmes atzīšanas** pagarināšana. E-privātuma direktīvā anonimizācijas pasākumi jau bija saistīti ar saderības nodrošināšanu (piemēram, E-privātuma direktīvas 6. panta 1. punkts, kurā teikts, ka informācija par datu plūsmu ir jādzēš vai jāpadara anonīma, kad tā vairs nav nepieciešama sakaru

<sup>6</sup> Sīkāk šo terminu skaidrojumu skatīt BEREC, Ziņojums par OTT pakalpojumiem, BoR (16) 35, 2016. gada 29. janvāris, 15. un 16. lpp., tīmekļa vietne: [http://berec.europa.eu/eng/document\\_register/subject\\_matter/berec/reports/5751-berec-report-on-ott-services](http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services). Lūdzu, ņemiet vērā arī ziņojumā pausto komentāru, ka šīs kategorijas ir paredzētas kā jēdzieni, ko izmantot diskusijās par pārskatīšanu, un tie nav paredzēti kā tiesiski jēdzieni.



pārraidīšanas nolūkam). Ierosinātās regulas 6. panta 2. punkta c) apakšpunktā un 6. panta 3. punkta b) apakšpunktā tiek pieļauts metadatu un satura apstrādes aizlieguma izņēmums, balstoties uz piekrišanu, ar nosacījumu, ka attiecīgo nolūku vai nolūkus “nevar sasniegt, apstrādājot anonimizētu informāciju”. Šādu privātuma aizsardzības pasākumu pieprasīšana papildus prasībai pēc lietotāju piekrišanas aizsargā šos lietotājus no nepamatotas apstrādes. Tomēr vienlaikus darba grupai ir nopietnas bažas, ka šādu anonimizācijas metožu pieņemšana nebūtu nepieciešama, izsekojot lietotāju atrašanās vietu ar mobilo iekārtu palīdzību (skatīt 17. piezīmi). Turklāt pat tad, ja ir jāpiemēro anonimizācijas pasākumi, pakalpojumu sniedzējiem vienmēr būtu jāveic datu aizsardzības ietekmes novērtējums (DAIN) (skatīt 33. un 46. piezīmi), un darba grupa aicina noteikt papildu pienākumu publiskot, kādā veidā dati ir anonimizēti un apkopoti (skatīt 42.b piezīmi).

12. Vēl viens pozitīvs aspekts ir **plašais galiekārtu aizsardzības formulējums**. 20. apsvērumā un 8. pantā noteikts, ka tehnoloģijas, kas tiek izmantotas, lai piekļūtu galiekārtām, nav būtiskas: jebkāda iejaukšanās attiecībā uz galiekārtām, ieskaitot to apstrādes iespēju izmantošanu, pieprasa galalietotāja piekrišanu (ar dažiem izņēmumiem). EK tagad ir izpalīdzīgi apstiprinājusi, ka šis noteikums attiecas uz “ierīču ciparnospiedumiem”. Turklāt darba grupa atzinīgi vērtē faktu, ka trešās personas nespējai ievērot indivīda **pārlūkprogrammas iestatījumos** noteiktās vēlmes **piemērojama izpilde**, kā aprakstīts 22. apsvērumā. Tas ir noderīgi situācijās, kad trešā persona (piemēram, reklāmas tīkls) neievēro šos iestatījumus. Tomēr tas būtu jānosaka arī attiecīgajā ierosinātās regulas noteikumā.
13. Visbeidzot, atzinīgi vērtējama **juridisko personu** pastāvīga **iekļaušana ierosinātās regulas darbības jomā** (skatīt Paskaidrojuma raksta 2.2. punktu; 3., 33. un 42. apsvērumi; 1., 15. un 16. panta 5. punkts). Tas jau notiek saskaņā ar E-privātuma direktīvu, bet, tā kā datu aizsardzības iestādēm būs jāuzliek pienākums piemērot jaunus noteikumus, ir lietderīgi to īpaši uzsvērt. Tas ļauj datu aizsardzības iestādēm rīkoties gadījumos, kad juridiskas personas ir pārkāpuma upuris, piemēram, ja korporācijas saņem surogātpastu vai to saziņa tiek slepeni pārraudzīta. Tomēr darba grupa kā jautājumu, kas rada bažas, arī norāda, ka piekrišanas piemērošana juridiskām personām ir neskaidra (skatīt 41.a piezīmi) un nav skaidrs, kas ir domāts ar juridisku personu “likumīgajām interesēm” tiešās tirgvedības gadījumā (skatīt 43.c piezīmi).

14. Darba grupa atzinīgi vērtē vēl vienu uzlabojumu kategoriju saistībā ar piekrišanas jēdziena piemērošanu un interpretāciju. Pirmkārt, atzinīgi vērtējams **skaidrojums, ka interneta piekļuve un (mobilā) telefonija ir būtiski pakalpojumi un šo pakalpojumu sniedzēji nevar “piespiest” klientus piekrist datu apstrādei, kas nav nepieciešama pamatpakalpojumu sniegšanai**. Jo īpaši 18. apsvērumā ir atzīmēts, ka pamata platjoslas interneta piekļuves un balss sakaru pakalpojumi ir uzskatāmi par būtiskiem pakalpojumiem, kas nozīmē, ka, ņemot vērā cilvēku atkarību no piekļuves šiem pakalpojumiem, šī piekrišana viņu sakaru datu apstrādei šādiem papildu nolūkiem (piemēram, apstrāde reklāmas vai tirgvedības vajadzībām) nevar būt spēkā esoša. Vienlaikus darba grupai ir bažas, ka šis skaidrojums ir pārāk ierobežojošs. Dažu OTT pakalpojumu sniedzēju pakalpojumus var uzskatīt arī par būtiskiem pakalpojumiem, un E-privātuma regulā arī būtu īpaši jāaizliedz tādas “pieņemt tādu, kā piedāvāts” izvēles citos apstākļos (skatīt 20. piezīmi).
15. Turklāt ir pozitīvi, ka **piekrišanas prasība attiecībā uz fizisko personu personas datu iekļaušanu abonentu sarakstos ir saskaņota**. Saskaņā ar ierosinātās regulas 15. pantu datu apstrāde publiskajos abonentu sarakstos ir atļauta tikai ar fizisku personu piekrišanu un juridiskām personām ir jābūt iespējai iebilst pret to. Tas ir sīkāk izklāstīts 31. apsvērumā, kurā norādīts, ka šādi piekrišanai jābūt konkrētai attiecībā uz konkrētām personas datu kategorijām, kuras jāiekļauj abonentu sarakstā. Tomēr darba grupa atzīmē bažas, ka ierosinātajā regulā varētu precīzāk noteikt, ka meklēšanas un reversās meklēšanas nolūkā būs vajadzīga konkrēta atsevišķa piekrišana (skatīt 37. piezīmi).
16. Ir novērtēts arī **jauns mērķtiecīgs izņēmums attiecībā uz neuzbāzīgas iejaukšanās gadījumiem ar galiekārtām**. DG29 uzskata par lietderīgu, ka ierosinātā regula precīzē, ka aizliegums neattiecas uz tīmekļa datplūsmas mērīšanu (saskaņā ar šauru izņēmumu, ka šādus mērījumus veic informācijas sabiedrības pakalpojuma sniedzējs un kuru pieprasa galalietotājs, skatīt ierosinātās regulas 8. panta 1. punkta d) apakšpunktu). Skatīt turpmāk 21. apsvērumu. Tomēr darba grupa ierosina izmantot tehnoloģiski neitrālu definīciju un precizēt šī izņēmuma piemērojamību (skatīt 25. piezīmi).

### 3. JAUTĀJUMI, KAS RAISA NOPIETNAS BAŽAS

#### *IEROSINĀTĀ REGULA APDRAUD VDAR PAREDZĒTO AIZSARDZĪBU*

Kā minēts iepriekš, ierosinātajā regulā ir vairāki būtiski uzlabojumi. Tomēr ir arī aspekti, kas raisa dažādas nopietnības pakāpes bažas. Šajā sadaļā darba grupa apskata četrus jautājumus, kas tai raisa **nopietnas bažas**. Tie ir noteikumi, kas **mazina VDAR piešķirto aizsardzības līmeni**:

17. **Regulā paredzētajām saistībām attiecībā uz galiekārtu atrašanās vietas izsekošanu ir jāatbilst VDAR prasībām.** Ierosinātās regulas 8. panta 2. punkta b) apakšpunktā tiek pieprasīta paziņojuma parādīšana un drošības pasākumu ieviešana, lai vāktu galiekārtu emitēto informāciju. 8. panta 2. punkta b) apakšpunktā tālāk norādīts, ka personai, kura ir atbildīga par šo vākšanu, jānorāda jebkurš pasākums, ko galalietotājs var veikt, lai līdz minimumam mazinātu vai apturētu šādu informācijas vākšanu. Tādējādi 8. panta 2. punkta b) apakšpunkts rada iespaidu, ka organizācijas var vākt informāciju, kuru emitē galiekārtas, lai izsekotu individu fizisko kustību (piemēram, “WiFi izsekošana” vai “Bluetooth izsekošana”) bez attiecīgās personas piekrišanas. Persona, kura vāc šos datus, acīmredzot var ievērot šo prasību, informējot lietotājus, ka tiem jāatslēdz ierīces, kad tās nevēlas tikt izsekotas. Šāda pieeja būtu pretrunā ar Eiropas Komisijas telekomunikāciju politikas pamatmērķi nodrošināt ātrgaitas mobilā interneta savienojamību ar stingru privātuma aizsardzību ar zemām izmaksām visiem Eiropas iedzīvotājiem.

Turklāt ierosinātajā regulā nav paredzēti nekādi skaidri ierobežojumi attiecībā uz datu vākšanas vai turpmāko apstrādes darbību apjomu. Šajā kontekstā jāatzīmē, ka šīs MAC adreses ir personas dati pat tad, ja tiek veikti drošības pasākumi, piemēram, jaukšana. Neuzliekot papildu prasības vai ierobežojumus, šo personas datu aizsardzības līmenis saskaņā ar ierosināto regulu ir ievērojami zemāks nekā VDAR paredzētais, saskaņā ar kuru šādai izsekošanai jābūt godīgai un likumīgai, kā arī pārredzamai. Turklāt 25. apsvērumā nelietderīgi atzīmēts, ka dažas no WiFi izsekošanas funkciju iespējām nerada augstu risku saistībā ar privātuma neaizskaramību, savukārt citas, piemēram, individu izsekošana ilgākā laika posmā, rada. Lai gan darba grupa atzinīgi novērtē to, ka pēdējām ir augsts risks saistībā ar privātuma neaizskaramību, nav lietderīgi jau no paša sākuma izlemt, ka dažas citas funkciju iespējas nerada risku, neveicot papildu novērtējumu par apstākļiem un apstrādes samērīgumu. Šāds novērtējums jāveic, ņemot vērā šādus nosacījumus attiecībā uz neanonimizētu WiFi izsekošanu.

Atkarībā no datu vākšanas apstākļiem un mērķiem šādai izsekošanai saskaņā ar VDAR, iespējams, ir nepieciešama piekrišana vai to var veikt tikai tad, ja vāktie personas dati ir anonimizēti. Šādu anonimizāciju vēlams veikt uzreiz pēc vākšanas. Ja tūlītēja anonimizācija nav iespējama, ņemot vērā nolūkus, kādiem dati tiek vākti, šos datus var apstrādāt laikposmā, kurā tie nav anonimizēti, tikai ar šādiem nosacījumiem: i) datu vākšanas mērķis ir tikai statistikas uzskaitē (skatīt piemērus turpmāk), ii) izsekošana ir ierobežota laikā un telpā, ciktāl tas ir noteikti nepieciešams šim nolūkam, iii) dati tiks dzēsti vai anonimizēti tūlīt pēc tam, un iv) pastāv rezultatīvas nepieņemšanas iespēja. Jebkuros apstākļos datu apstrādātājiem, protams, ir jāievēro prasība sniegt atbilstošu informāciju.

Darba grupa pauž bažas, ka iespējama individuāla nepieņemšanas piedāvājums vienai organizācijai, kas apkopo šos datus, radītu nepieņemamu slogu iedzīvotājiem, ņemot vērā, ka gan privātā, gan valsts sektora organizācijas palielina šādu izsekošanas tehnoloģiju ieviešanu. Tāpēc darba grupa aicina Eiropas likumdevēju veicināt tādu tehnisko standartu izstrādi, lai ierīces automātiski brīdinātu par iebildumu pret šādu izsekošanu, un nodrošināt, ka šāda signāla ievērošanas izpilde ir īstenojama.

Piemēram, piekrišana VDAR ietvaros, visticamāk, būs nepieciešama, ja datu apstrādātājs vāc un uzglabā ierīču netieši identificējamās (WiFi vai *Bluetooth*) MAC adreses un aprēķina lietotāja atrašanās vietu, lai izsekotu lietotāja atrašanās vietu ilgākā laika posmā, piemēram, vairākos veikalos. Tas jo īpaši attiecas uz gadījumiem, kad šāda izsekošana notiek sabiedriskajās vietās, kur lietotājiem ir tiesiskā pašlāvība, ka tie netiek identificēti vai izsekoti, kamēr tiek vāktas garāmgājēju MAC adreses. Piemēram, šāda piekrišana var tikt iegūta, izmantojot lietotni, kas aicina lietotājus atļaut noteikt to atrašanās vietu noteiktās zonās apmaiņā pret komerciāliem piedāvājumiem vai piedāvājot reģistrācijas punktus noteiktās atrašanās vietās, vai izmantojot piekrišanas moduli WiFi tīklajos.

Tikai ierobežotos apstākļos datu apstrādātāji drīkstētu apstrādāt galiekārtu emitēto informāciju, lai izsekotu fizisko pārvietošanos bez attiecīgās personas piekrišanas. Piemēram, tas varētu būt gadījumā, kad tiek uzskaitīts klientu skaits konkrētā atrašanās vietā vai apkopojot emitētos datus abās drošības pārbaudes punkta pusēs, lai parādītu gaidīšanas laiku. Tomēr abos piemēros dati būtu jādzēš vai jāpadara anonīmi, tiklīdz būs iespējams izpildīt statistisko mērķi. Tas nozīmē, ka apmeklētāju ierīču MAC adreses konkrētā atrašanās vietā, piemēram, veikalā, nekavējoties pēc to savākšanas tiek anonimizētas, neuzglabājot MAC adreses pastāvīgi un tādā veidā, lai tehniski identificēšana no jauna nav iespējama. Gaidīšanas laika aprēķināšanas gadījumā MAC adreses būtu jādzēš vai jāpadara anonīmas, tiklīdz dati vairs nav būtiski gaidīšanas laika aprēķināšanai (piemēram, tāpēc, ka apmeklētājs atrodas otrpus drošības pārbaudei vai tāpēc, ka viņš vai viņa ir atstājis rindu).

Turklāt datu apstrādātājiem būtu jāievēro datu minimizācijas prasības (piemēram, neveikt izsekošanu 24 stundas diennaktī, ja mērķis ir tikai izsekošana veikala darba laikā un/vai paraugu ņemšana intervālos). Datu apstrādātājiem ir jāveic arī citi pasākumi, lai novērstu vai mazinātu ietekmi uz lietotāju tiesībām uz privātumu, piemēram, lai aizsargātu personu, kura dzīvo blakus vākšanas vietai, privātumu.

Izvēle ierosinātās regulas 8. panta 2. punktā noteikt tikai paziņošanas prasību ir vēl jo vairāk nozīmīga, ņemot vērā 20. apsvērumā iekļauto secinājumu, ka ar galalietotāju ierīci saistītā informācija var tikt vākta arī attālināti identificēšanas un izsekošanas nolūkā un ka šādas apstrāde — saskaņā ar ierosināto regulu, var nopietni pārkāpt šo galalietotāju privātumu. Turklāt šis pienākums neattiecas tikai uz pienākumu sniegt informāciju, kas jau ir paredzēts VDAR 13. un 14. pantā. Šo nopietno privātuma pārkāpumu papildus vēl vairāk pastiprina trešo personu iespējamā piekļuve savāktajiem datiem, piemēram, iespējai tiesībaizsardzības iestādēm identificēt galalietotājus, pamatojoties uz uzglabāto MAC adresi(-ēm), ko pārraida to mobilās ierīces.

**18. Ir jāizstrādā nosacījumi, saskaņā ar kuriem ir atļauta satura un metadatu analīze.**

Ierosinātās regulas 6. pantā metadatiem un saturam tiek piešķirti dažādi aizsardzības līmeņi. DG29 neatbalsta šo atšķirību: abas datu kategorijas ir ļoti sensitīvas. Tādēļ gan metadatiem, gan saturam būtu jāpiešķir vienādi augsts aizsardzības līmenis.

Tāpēc izejas punktam vajadzētu būt tādām, ka ir aizliegts apstrādāt metadatus, kā arī saturu bez visu galalietotāju piekrišanas (t. i., sūtītāja un saņēmēja).

Atkarībā no nolūkiem tomēr var tikt atļauta noteikta apstrāde bez piekrišanas, ja tas ir noteikti nepieciešams šādiem nolūkiem:

- Pakalpojumu sniedzēji var apstrādāt elektronisko sakaru datus ierosinātās regulas 6. panta 1. punkta a) un b) apakšpunktā, 6. panta 2. punkta a) un b) apakšpunktā paredzētajiem nolūkiem.<sup>7</sup>
- Jāprecizē, ka dažus surogātpasta atklāšanas/filtrēšanas un robottiklu mazināšanas paņēmienus var arī uzskatīt par absolūti nepieciešamiem, lai atklātu vai apturētu ļaunprātīgu elektronisko sakaru pakalpojumu izmantošanu (6. panta 2. punkta b) apakšpunkts). Attiecībā uz surogātpasta filtrēšanu galalietotājiem, kuri saņem surogātpastu, būtu jāpiedāvā, ja tehniski iespējams, granulāras nepiekrišanas iespējas.
- Jāprecizē, ka elektronisko sakaru datu analīze klientu apkalpošanas nolūkiem var būt attiecināma uz “rēķinu izrakstīšanai nepieciešamo informāciju” (izņēmumu) (skatīt 6. panta 2. punkta b) apakšpunktu). Būtiskos metadatus var glabāt līdz perioda beigām, kura laikā rēķinu var likumīgi apstrīdēt vai var veikt maksājumu saskaņā ar valsts tiesību aktiem. Būtiskos datus (piemēram, vietražus URL) var saglabāt tikai pēc galalietotāja pieprasījuma un tad tikai laikposmā, kas noteikti nepieciešams, lai atrisinātu strīdu par rēķinu (tas nozīmē, ka ir jāgroza 7. panta 3. punkts).
- Jābūt iespējai apstrādāt elektronisko sakaru datus, lai nodrošinātu galalietotāju nepārprotami pieprasītos pakalpojumus, piemēram, meklēšanas vai atslēgvārdu indeksēšanas funkcionalitāti, virtuālos palīgus, tekstrunas ierīces un tulkošanas pakalpojumus. Tam ir nepieciešams ieviest atbrīvojumu šādu datu analīzei tīri individuālai (mājsaimniecības) izmantošanai, kā arī individuālam darba lietojumam.<sup>8</sup> Tādējādi to būtu iespējams veikt bez visu galalietotāju piekrišanas, bet tikai ar tā galalietotāja piekrišanu, kurš pieprasa pakalpojumu. Šāda īpaša piekrišana arī liedz pakalpojumu sniedzējam izmantot šos datus citiem nolūkiem.

Tas nozīmē, ka satura un/vai metadatu analīzei visiem citiem nolūkiem, piemēram, analīzei, profilēšanai, reklāmai, kas balstīta uz uzvedību, vai citiem nolūkiem pakalpojuma sniedzēja (komerciālajam) guvumam, ir nepieciešama visu to galalietotāju, kuru dati tiks apstrādāti, piekrišana. Attiecībā uz šīm situācijām ierosinātajā regulā būtu jāpaskaidro, ka vienkārši e-pasta nosūtīšana vai cita veida

<sup>7</sup> Attiecībā uz nepieciešamību ievērot obligātās pakalpojumu kvalitātes prasības, kā norādīts ierosinātās regulas 6. panta 2. punkta a) apakšpunktā, pakalpojumu sniedzējiem jāņem vērā Regulā (ES) 15/2120 (EESK) aprakstītie nosacījumi, jo īpaši 3. pants un 10. un 13.-15. apsvērumi. Pamatojoties uz šo noteikumu, pakalpojumu sniedzējiem var būt nepieciešams apstrādāt sakaru datus, lai atklātu un filtrētu ļaunprogrammatūru un spieģļprogrammatūru, un tiem var ļaut saspiest datus.

<sup>8</sup> Kaut arī ierosinātās regulas 13. apsvērumā korporatīvie tīkli tiek nepārprotami izslēgti no regulas darbības jomas, šim jaunajam individuālajam lietošanas izņēmumam būtu jāattiecas arī uz mākoņpakalpojumiem, ko darbinieki izmanto saistībā ar darbu, piemēram, veicot meklēšanu savā e-pastā.

personiskās saziņas no cita pakalpojuma galalietotājam, kurš ir personīgi piekritis sava satura un metadatu apstrādei (piemēram, pierakstoties uz pasta pakalpojumu), neveido spēkā esošu sūtītāja piekrišanu.

Visbeidzot, ir jāprecizē, ka personu, kuri nav galalietotāji, datu apstrādē (piemēram, trešās personas attēla vai apraksta apmaiņā starp diviem cilvēkiem) ir jāievēro arī visi attiecīgie VDAR noteikumi.

**19. Galiekārtām un programmatūrai *pēc noklusējuma* ir jāattur, jānovērš un jāaizliedz pret to vērsti nelikumīgi traucējumi, kā arī jāsniedz informācija par iespējām.** Lai gan ierosinātā regula paredz, ka programmatūras nodrošinātājiem, kuri ļauj elektroniskajiem sakariem “piedāvāt iespēju”, ir jānovērš ierobežota veida iejaukšanās galiekārtās, un pēc uzstādīšanas uzliek par pienākumu programmatūras nodrošinātājiem pieprasīt no galalietotāja piekrišanu iestatījumam (10. panta 1. un 2. punkts), šāda izvēle nediskriminē privātumu pēc noklusējuma. Turklāt šobrīd jau pastāv “iespēja” novērst noteiktu iejaukšanos, un līdz šim tā nav pietiekami novērsusi nepamatotas izsekošanas problēmu. Tieši tādēļ VDAR ietvaros ir veikta apzināta politikas izvēle, lai ieviestu datu aizsardzības un integrētus privātās dzīves, un privātās dzīves pēc noklusējuma aizsardzības principus (VDAR 25. pants). Ierosinātā regula apdraud šos principus attiecībā uz sakaru un ierīču datiem. Tajā pašā laikā Radioiekārtu direktīvā 2014/53/ES<sup>9</sup> (minēta 10. apsvērumā) paredzēts tikai ļoti ierobežots drošības pienākums, prasot radioiekārtām iekļaut “drošības pasākumus, kas nodrošina lietotāja un abonenta personas datu un privātuma aizsardzību” (3. panta 3. punkta e) apakšpunkts). Ar to nevar aizstāt konkrētos noklusētā privātuma iestatījumus saskaņā ar ierosināto regulu. Šajā sakarā ir arī vērts atzīmēt, ka Eiropas Komisijas pētījumā, kas publicēts 2016. gada decembrī, ir norādīts, ka “gandrīz septiņi no desmit (69 %) pilnībā piekrīt, ka to pārlūkprogrammas noklusējuma iestatījumiem jāaptur to informācijas dalīšana”<sup>10</sup>. Darba grupu atsevišķi nodarbina jautājums par pārlūkprogrammas iestatījumiem un “trešo personu” definīciju. Skatīt 24. piezīmi. Turklāt jāpatur prātā, ka šis noteikums attiecas ne tikai uz datoros izmantojamām pārlūkprogrammām, bet arī uz citiem programmatūras veidiem, kas ļauj sazināties (tostarp operētājsistēmām, lietotnēm un programmatūras saskarnēm ar lietu internetu savienotām ierīcēm). Kopumā galiekārtām un programmatūrām *pēc noklusējuma* jāpiedāvā privātuma aizsardzības iestatījumi un jāvada lietotāji, izmantojot konfigurācijas izvēlni, lai pēc uzstādīšanas novirzītu no šiem noklusējuma iestatījumiem. Šai konfigurācijas izvēlnei vienmēr jābūt viegli pieejamai lietošanas laikā. Darba grupa mudina Eiropas likumdevēju šajā sakarā precizēt 10. panta darbības jomu.

**20. E-privātuma regulā būtu nepārprotami jāaizliedz izsekošanas sienas, t. i., prakse, saskaņā ar kuru piekļuve vietnei vai pakalpojumam tiek liegta, ja vien personas nesniedz piekrišanu tikt izsekotas citās tīmekļa vietnēs vai pakalpojumos.** Kā jau minēts iepriekšējos darba grupas atzinumos par E-

<sup>9</sup> Radio aprīkojuma direktīva 2014/53/ES.

<sup>10</sup> Skatīt *Flash Eurobarometer 443*, Ziņojums par e-privātumu (publicēts 2016. gada decembrī), 5. lpp.

privātuma direktīvu<sup>11</sup>, šādas “pieņemt tādu, kā piedāvāts” pieejas reti ir pamatotas<sup>12</sup>. Ja galiekārtu apstrādes un uzglabāšanas spējas vai informācijas iegūšana no galalietotāju galiekārtām ļauj izsekot lietotāja darbības ilgākā laika posmā vai vairākos pakalpojumos (piemēram, dažādās tīmekļa vietnēs vai lietotnēs), šādas apstrādes darbības var nopietni pārkāpt šo lietotāju privātās dzīves neaizskaramību. Ņemot vērā interneta būtisko nozīmi vārda brīvības pamattiesību, tostarp tiesību piekļūt informācijai, nodrošināšanā, indivīdu iespēja piekļūt tiešsaistes saturam nedrīkst būt atkarīga no tā, vai viņš/ viņa pieņem izsekošanas darbības, kas tiek veiktas dažādās ierīcēs un tīmekļa vietnēs/lietotnēs. Turpmākajā e-privātuma regulējumā būtu jānosaka, ka piekļuve saturam, piemēram, vietnēs un lietotnēs, nedrīkst būt atkarīga no šādu uzmācīgu apstrādes darbību pieņemšanas neatkarīgi no izmantotās izsekošanas tehnoloģijas, piemēram, sīkdatnēm, ierīču ciparnospiedumiem, unikāliem identifikatoriem vai citām uzraudzības metodēm. Šī aizlieguma nepieciešamība ir uzsvērtā nesenajā Eiropas Komisijas aptaujā par e-privātumu, kurā norādīts, ka “gandrīz divas trešdaļas respondentu uzskata, ka ir nepieņemami uzraudzīt viņu tiešsaistes darbības apmaiņā pret neierobežotu piekļuvi noteiktai tīmekļa vietnei (64 %)”.

21. Kopumā attiecībā uz četriem iepriekš minētajiem punktiem **ierosinātajai regulai jāpilda solījums nodrošināt vienādu vai augstāku aizsardzības līmeni nekā VDAR**. 5. apsvērumā ir teikts, ka ierosinātā regula nemazina VDAR paredzēto aizsardzības līmeni. Tas neatbilst pašreizējai ierosinātās regulas versijai, jo īpaši attiecībā uz ierīču izsekošanu (17. piezīme), jo trūkst privātuma (19. piezīme) pēc noklusējuma un piekrišanas (18. piezīme) princips. Tas ir īpaši svarīgi, jo tajā pašā apsvērumā ir norādīts, ka ierosinātajai regulai būs “VDAR *lex specialis*, un tas konkretizēs un papildinās VDAR attiecībā uz elektronisko sakaru datiem, kuri kvalificējami kā personas dati”. Darba grupa ierosina vismaz precizēt šādus jautājumus E-privātuma regulas tekstā:

i) E-privātuma regulā paredzētajiem aizliegumiem ir prioritāte pār VDAR piešķirtajām atļaujām (piemēram, E-privātuma regulas 5. pantā minētais ierīču izsekošanas aizliegums ir prioritārs pār elektronisko komunikāciju pakalpojumu sniedzēju tiesībām turpināt apstrādāt personas datus saskaņā ar VDAR 5. panta 1. punkta b) apakšpunktu un 6. panta 4. punktu);

ii) ja apstrāde ir atļauta saskaņā ar jebkādiem izņēmumiem (tostarp piekrišanu) attiecībā uz E-privātuma regulā paredzētajiem aizliegumiem, šāda apstrāde, ja tā skar personas datus, joprojām atbilst visiem attiecīgajiem VDAR noteikumiem;

iii) ja apstrāde ir atļauta saskaņā ar jebkuru izņēmumu attiecībā uz E-privātuma regulā paredzētajiem aizliegumiem, ir aizliegta jebkura cita apstrāde, pamatojoties uz VDAR, tostarp apstrāde citam nolūkam saskaņā ar VDAR 6. panta 4. punktu. Tas neliegtu datu apstrādātājiem pieprasīt papildu piekrišanu jaunām apstrādes darbībām. Tas arī neliegtu likumdevējiem paredzēt E-privātuma regulā papildu, ierobežotus un īpašus izņēmumus,

<sup>11</sup> Skatīt, piem., WP240 (e-privātuma pārskats), 16. lpp.; WP208 (atbrīvojums no piekrišanas), 5. lpp.

<sup>12</sup> Šī nostāja neietekmē VDAR 7. panta 4. punktu, kas var arī liegt “pieņemt vai atstāt” izvēles citās situācijās, kad tas ir atbilstoši.

piemēram, lai atļautu apstrādi zinātniskos vai statistikas nolūkos saskaņā ar VDAR 89. pantu vai aizsargātu personu “vitālās intereses” saskaņā ar VDAR 6. panta d) apakšpunktu.

Turklāt E-privātuma regula jāinterpretē tā, lai nodrošinātu, ka tā sniedz vismaz tādu pašu un — attiecīgajā gadījumā — augstāku aizsardzības līmeni nekā VDAR

#### 4. CITI JAUTĀJUMI, KAS RADA BAŽAS

Papildus iepriekš minētajiem jautājumiem 29. panta darba grupai **bažas rada** šādi jautājumi.

##### *IR JĀPAPLAŠINA TERITORIĀLĀ UN MATERIĀLĀ DARBĪBAS JOMA*

22. **Termins “metadati” ir definēts pārāk šauri.** Tas tagad ir definēts 4. panta c) apakšpunktā kā “dati, kas elektronisko sakaru tīklā tiek apstrādāti nolūkā tos pārraidīt, izplatīt vai veikt elektronisko sakaru satura apmaiņu” (izcēlums pievienots). Vārda “tīkls” izmantošana, šķiet, liek domāt, ka tikai dati, kas iegūti, sniedzot pakalpojumus tīkla “apakšējā” slānī, būtu klasificējami kā “metadati”. Tas varētu nozīmēt to, ka *OTT* pakalpojuma sniegšanas gaitā iegūtie dati tiktu izslēgti no šīs darbības jomas. Tas būtu nevēlami un, iespējams, arī nebija paredzēts, ņemot vērā nodomu paplašināt ierosinātās regulas darbības jomu attiecībā uz *OTT* pakalpojumu sniedzējiem. Lai to novērstu, ir jāgroza “elektronisko sakaru metadatu” definīcija, iekļaujot visus datus, kas apstrādāti elektronisko sakaru satura pārraidīšanas, izplatīšanas vai apmaiņas nolūkiem.

23. Turklāt bažas rada tas, ka **ierosinātās regulas teritoriālā darbības joma attiecībā uz organizācijām, kuras neatrodas ES, attiecas tikai uz elektronisko sakaru pakalpojumu sniedzējiem.** Saskaņā ar ierosināto regulu elektronisko sakaru pakalpojumu sniedzējs, kas neatrodas ES, rakstiski nozīmē savu pārstāvi Savienībā (3. panta 2. punkts). 9. apsvērumā ir minēts arī tas, ka regulu piemērotu apstrādei, ko veic elektronisko sakaru pakalpojumu sniedzēji neatkarīgi no apstrādes vietas. Darba grupa šādu precizējumu vērtē atzinīgi. Tomēr, tā kā formulējums attiecas tikai uz elektronisko sakaru pakalpojumu sniedzējiem, nav skaidrs, cik lielā mērā šī teritoriālā darbības joma attiecas uz cita veidu personām (piemēram, personām, kuras iejaucas vai apkopo informāciju, ko pārraida galalietotāju galiekārtas, skatīt ierosinātās regulas 3. panta 1. punkta c) apakšpunktu un 8. pantu). Tāpēc darba grupa ierosina grozīt 3. panta 2. punktu un 3. panta 5. punktu, iekļaujot publiski pieejamu abonentu sarakstu nodrošinātājus, programmatūras piegādātājus, kas ļauj elektronisko saziņu, un personas, kuras sūta tiešās tirgvedības komerciālos paziņojumus vai vāc (citu) informāciju, kas saistīta ar galalietotāju galiekārtām vai tiek uzglabāta to galiekārtās, ja vien to darbības ir vērstas uz lietotājiem ES (skatīt ierosinātās regulas 8. apsvērumu)<sup>13</sup>.

<sup>13</sup> Skatīt VDAR 3. panta 2. punktu: “Šo regulu piemēro Savienībā esošu datu subjektu personas datu apstrādei, ko veic pārzinis vai apstrādātājs, kas neveic uzņēmējdarbību Savienībā, ja apstrādes darbības ir saistītas ar: a) preču vai pakalpojumu piedāvāšanu šādiem datu subjektiem Savienībā, neatkarīgi no tā, vai no datu subjekta tiek prasīta samaksa; vai b) viņu uzvedības novērošanu, ciktāl viņu uzvedība notiek Savienībā.” Šis pienākums var ietvert arī izņēmumus saskaņā ar VDAR 27. panta 2. punktu.



Vēl viena jautājumu kategorija ir saistīta ar nepietiekamu galiekārtu aizsardzību ierosinātajā regulā.

24. Pirmkārt, **ierosinātajā regulā nepareizi norādīts, ka spēkā esošu piekrišanu var sniegt, izmantojot nekonkrētus pārlūka iestatījumus.** Darba grupa atzīst apsvērumu, ka galalietotājus pašlaik pārslogo ar pieprasījumiem sniegt piekrišanu (22. apsvērums). Pārlūkprogrammu (un salīdzināmās programmatūras) iestatījumiem ir svarīga nozīme šīs problēmas risināšanā. Tomēr, tā kā vispārējos pārlūka iestatījumus nav paredzēts piemērot izsekošanas tehnoloģijas lietojumam vienā atsevišķā gadījumā, tie nav piemēroti, lai sniegtu piekrišanu saskaņā ar VDAR 7. pantu un 32. apsvērumu (jo piekrišana nav apzināta un pietiekami konkrēta).

Galalietotājam jābūt iespējai sniegt atsevišķu piekrišanu katrai vietnei vai lietotnei izsekošanai dažādiem mērķiem (piemēram, sociālo mediju apmaiņai vai reklāmai). Ja datu apstrādātājs atbild par vairākām vietnēm vai lietotnēm, tas var arī pieprasīt piekrišanu visām citām tā kontrolē esošajām lietotnēm un vietnēm, ja vien šis piekrišanas pieprasījums tiek parādīts atsevišķi.

Turklāt datu apstrādātājam ir jāievēro visi pārējie ar piekrišanu saistītie pienākumi, tostarp pienākums sniegt lietotājiem atbilstošu informāciju. Attiecībā gan uz pārlūkprogrammām, gan uz datu apstrādātājiem tas nozīmē, ka piekrišana būtu spēkā neesoša, ja tie piedāvātu tikai iespēju “pieņemt visas sīkdatnes”, jo tas neļaus lietotājiem sniegt nepieciešamo granulāro piekrišanu. Tomēr pārlūkprogrammām vajadzētu būt iespējai ļaut lietotājiem izdarīt apzinātu izvēli pieņemt visas sīkdatnes, tādējādi novēršot turpmākus atsevišķus piekrišanas pieprasījumus to apmeklētajās vietnēs.

Darba grupa stingri iesaka E-privātuma regulā pārlūkprogrammām obligāti ieviest tādus tehniskos mehānismus kā neizsekošanas standartu, lai nodrošinātu lietotājiem patiesu izvēli un kontroli pār iekļaušanos to ierīcēs<sup>14</sup>.

Vēl svarīgāk, E-privātuma regulā būtu jānodrošina, ka gan izvēle attiecībā uz ierīces datu glabāšanu, gan DNT signālu no pārlūkprogrammas tiek pieņemta kā juridiski saistoša, norādot uz visu datu apstrādātāju piekrišanu vai atteikumu. Tas neskar turpmākas darba grupas pamatnostādnes DNT standarta ievērošanai, cita starpā nolūka ierobežojuma principu, kad šis standarts būs pabeigts (paredzēts 2017. gada beigās).

Neskaidri “piekrišanas” veidi, piemēram, klikšķis uz vietnes vai lapas ritināšana, nevar atcelt izvēles iespējas attiecībā uz uzglabāšanu un DNT signālu. Svarīgs ieguvums no šī standarta izmantošanas ir tas, ka tas neaprobežojas tikai ar sīkdatņu izsekošanas tehnoloģiju, bet attiecas arī uz citiem izsekošanas veidiem, piemēram, ierīču ciparnospiedumiem.

Ja šī standarta ievērošana būtu juridiski saistoša, tas atrisinātu vēl vienu problēmu termina “trešās personas” 10. pantā pašreizējā izmantojumā. Tīmekļa vietnē vai

<sup>14</sup> Skatīt tīmekļa vietni: <https://www.w3.org/TR/tracking-compliance/>. 7. punktā ir izskaidrots izņēmuma modelis un atšķirība starp vietņu mēroga un tīmekļa mēroga izņēmumiem. 6. punktā ir iekļauta mašīnlasāmā informācija, ko datu apstrādātāji var sniegt attiecībā uz informācijas prasību piekrišanas iegūšanai.

lietotnē parasti ir daudz elementu gan no pašas vietnes, gan no ārējiem elementiem. Un ārējais kods var darboties arī apmeklētās vietnes kontekstā, bet tiek nosūtīts atpakaļ trešās personas serverim. Pirmā persona var nodrošināt izsekošanas sīkdatni, kad lietotājs apmeklē, piemēram, sociālā tīkla vietni. Šī sociālā tīkla vietne var kļūt par trešo personu, kad šis lietotājs apmeklē citu vietni, kurai ir mijiedarbība ar šo sociālā tīkla vietni. Visos šajos gadījumos, neskatoties uz to, vai tas attiecas uz lietotāja piekļuvi informācijai vai informācijas glabāšanu galalietotāja ierīcē, tā ir iejaukšanās ierīcē, kam ir nepieciešama piekrišana (ja vien nav spēkā kāds no izņēmumiem). DNT standartā tas tiek risināts, izmantojot terminus “visā vietnē” un “visā internetā”. Tādēļ, lai uzlabotu visu ieinteresēto personu tiesisko noteiktību, E-privātuma regulā atsauce uz trešām personām būtu jāpārformulē, lai tā aptvertu visas organizācijas, ar kurām ierīce mijiedarbojas (jo tās glabā vai piekļūst informācijai ierīcē).

Lai neatbilstības standarts būtu saderīgs ar augsto saziņas un datu aizsardzības konfidencialitātes aizsardzības līmeni, kas piešķirts saskaņā ar Hartu, E-privātuma regulā būtu jānorāda, ka pieprasījumi izsekošanai visā internetā, ne tikai vietnē, ir jāuzrāda atsevišķi, un lietotājiem jābūt tiesīgiem pieņemt vai noraidīt šādus pieprasījumus. Turklāt, lai aizsargātu lietotājus no biežiem piekrišanas pieprasījumiem, E-privātuma regulā jānodrošina, ka atteikums pieņemt izsekošanu visā internetā no kādas konkrētas organizācijas (izmantojot neizsekošana standartu vai atsevišķu melno sarakstu) neļauj šai organizācijai veikt turpmākus piekrišanas pieprasījumus vismaz sešus mēnešus. Šis noteikums neliedz šai organizācijai gadījumā, kad lietotājs to tieši apmeklē (t. i., kā pirmajai personai), pieprasīt piekrišanu savā tīmekļa vietnē (t. i., pieprasījums vietnes atļaujas saņemšanai). Praksē tas nozīmē, ka, piemēram, video straumēšanas vietne, kas izmanto izsekošanas sīkdatnes, var lūgt piekrišanu, ja šis lietotājs apmeklē video straumēšanas vietni, taču tā vairs nevar lūgt piekrišanu sešu mēnešu garumā, ja šis lietotājs ir atteicies piekrist un apmeklē citas vietnes, kurās ir videoklipi, kas tiek rādīti no šīs straumēšanas vietnes.

25. Turklāt **izņēmums “tīmekļa auditorijas mērījumiem” ir neprecīzi formulēts.** Ierosinātās regulas 8. panta 1. punkta d) apakšpunktā ir sniegts izņēmums tīmekļa auditorijas mērījumiem. Pirmā problēma ir tāda, ka šis termins nav definēts un to var sajaukt ar lietotāju profilu veidošanu. Definīcijai ir skaidri jānorāda, ka šo izņēmumu nevar izmantot nekādiem profilēšanas nolūkiem. Izņēmums attiecas tikai uz lietojuma analīzi, kas nepieciešama, lai analizētu lietotāja pieprasīto pakalpojuma sniegumu, bet ne lietotāju analīzei (t. i., tīmekļa vietnes, lietotnes vai ierīces identificējamo lietotāju darbības izpētei). Tādēļ izņēmumu nevar izmantot apstākļos, kad datus var saistīt ar identificējamām lietotāja datiem, kurus apstrādā pakalpojumu sniedzējs vai citi datu apstrādātāji. Turklāt tā aprakstā ir minēts attiecībā uz tehnoloģijām ļoti specifisks pielietojums. Tāpēc jēdziens “tīmekļa auditorijas mērījumi” ir jādefinē no jauna tehnoloģiski neitrālā veidā, tajā iekļaujot līdzīgu analītisko lietojuma informāciju, kas iegūta no lietojumprogrammām, valkājamām ierīcēm un lietu interneta ierīcēm.

Darba grupa ierosina smelties iedvesmu no Nīderlandes izņēmuma, kas ir spēkā tikai tad, ja tas ir absolūti nepieciešams, lai iegūtu informāciju par piegādātās informācijas sabiedrības pakalpojuma tehnisko kvalitāti vai efektivitāti, un tam nav vai ir neliela

ietekme uz iesaistīto abonentu vai galalietotāju (skatīt Nīderlandes telekomunikāciju likuma 11. panta 7. punkta a) apakšpunkta 3. punkta b) apakšpunktu). Šis izņēmums ņem vērā to, ka lielākā daļa datu, kas iegūti, izmantojot tīmekļa vai lietotņu analīzi, joprojām ir personas dati. Tas nozīmē, ka uz šo datu apstrādi arī attiecas VDAR. Piemēram, tas nozīmē, ka lietojuma analīzi var veikt arī ārēja organizācija, bet tikai tad, ja:

- i) šī organizācija darbojas kā datu apstrādātājs;
- ii) tiek noslēgts VDAR prasībām atbilstošs procesora līgums;
- iii) izmantotā analīzes tehnoloģija novērš atkārtotu identifikāciju, tostarp lietotāju IP adresu anonimizēšanu;
- iv) konkrētas sīkdatnes vai citus datus, kas izmantoti analīzē, var izmantot tikai konkrētajai vietnei, lietotnei vai valkājamām ierīcēm, un tos nevar piesaistīt citiem identificējamiem datiem;
- v) lietotājiem ir tiesības atteikties (skatīt arī šī atzinuma 17. un 50. piezīmi).

Pat ja piekrišana nebūtu nepieciešama, ja šie nosacījumi ir izpildīti, datu apstrādātājiem joprojām jāsniedz lietotājiem pietiekama informācija, piemēram, izmantojot izsekošanas statusa reprezentācijas laukus neizsekošanas standartā<sup>15</sup>.

26. E-privātuma regulai **būtu jānodrošina šauri un precīzi formulēti izņēmumi attiecībā uz piekrišanas prasībām**. Piekrišanas prasības izņēmuma formulējums attiecībā uz ieviešanu ierīcē 8. panta 1. punkta c) apakšpunktā ir gandrīz identisks pašreizējam E-privātuma direktīvas 5. panta 3. punkta formulējumam: “nepieciešama, lai sniegtu informācijas sabiedrības pakalpojumu, ko skaidri pieprasa abonents vai lietotājs”, taču bez paskaidrojuma ir izlaists būtiskais vārds “noteikti”. Tas rada bažas divu iemeslu dēļ: Pirmkārt, E-privātuma direktīvas norma jau ir izraisījusi plašas diskusijas par tās tvērumu uzraudzības iestādēs un organizācijās, un vārda “noteikti” svīturošana sniegs vēl mazāku tiesisko noteiktību. Tas rada arī bažas, jo darba grupa jau ir sniegusi norādes par termina “noteikti” interpretāciju šajā kontekstā. Atzinumā par sīkdatņu atbrīvošanu no prasības par piekrišanu (WP 194) darba grupa ierosināja šādu precizējumu:

*“Sīkdatne ir vajadzīga, lai nodrošinātu konkrētu funkciju lietotājam (vai abonentam): ja sīkdatnes ir atspējotas, funkcija nebūs pieejama, un šo funkciju ir skaidri pieprasījis lietotājs (vai abonents) kā daļu no informācijas sabiedrības pakalpojuma.”*<sup>16</sup>

Papildus darba grupa precizēja, ka:

<sup>15</sup> Skatīt: Izsekošanas vēlmju izpaušme (DNT), redaktora projekts, 2016. gada 7. marts.

<sup>16</sup> 29. panta darba grupa, WP 294, Atzinums 04/2012 par sīkdatņu atbrīvošanu no prasības par piekrišanu, pieņemts 2012. gada 7. jūnijā, tīmekļa vietne: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194\\_lv.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_lv.pdf)

*„trešo personu sīkdatnes” parasti nav “noteikti nepieciešamas” lietotājam, kas apmeklē tīmekļa vietni, jo šīs sīkdatnes parasti ir saistītas ar pakalpojumu, kas atšķiras no pakalpojuma, kuru lietotājs ir „skaidri pieprasījis”<sup>17</sup>.*

Darba grupa piebilda, ka tādu sociālo spraudņu izmantošana, kas paredzēta platformas vai tīmekļa vietnes lietotājiem, kuri nav lietotāji, arī netiks uzskatīta par noteikti nepieciešamām.

Turklāt, lai gan ierosinātās regulas 6. panta 1. punkta b) apakšpunkts ļauj elektronisko sakaru datus apstrādāt, ja tas ir “nepieciešams” drošības nolūkos, VDAR 49. apsvērums pieprasa, ka tam jābūt noteikti nepieciešamam. Vārda “noteikti” dzēšana, iespējams, nav tīša, jo ierosinātās regulas 21. apsvērumā ir minēts, ka piekrišana iejaukšanās gadījumam nav jāpieprasa tad, ja tas ir “noteikti” nepieciešams. Tomēr ierosinātā regula dod iespēju vēl vairāk precizēt, ka šīs regulas kontekstā vajadzības tests būtu jāinterpretē šauri attiecībā uz jebkādiem izņēmumiem. Tādēļ darba grupa ierosina, ka attiecībā uz visiem 6. pantā un 8. panta 1. punktā minētajiem izņēmumiem pirms vārda “nepieciešams” jāpievieno vārdu “noteikti”.

No otras puses, E-privātuma regulā skaidri jāparedz iejaukšanās iekārtās drošības atjauninājumu uzstādīšanai. Drošības atjauninājumu nosūtīšana, izmantojot internetu, ir vēlamā metode drošības atjauninājumu uzstādīšanai lielākajā daļā galalietotāju ierīču. Atjauninājumu uzstādīšana tiek uzskatīta par iejaukšanos galiekārtā. Pastāv likumīga interese nodrošināt, ka šo ierīču drošība ir atjaunināta. Tādēļ drošības ielāpu nodrošinātājam jāspēj uzstādīt noteikti nepieciešamos drošības atjauninājumus bez galalietotāja piekrišanas. Tomēr nav skaidrs, vai šāda iejaukšanās var gūt labumu no “informācijas sabiedrības” izņēmuma iejaukšanās aizliegumam (8. panta 1. punkta c) apakšpunkts). Jāprecizē, ka drošības atjauninājumu uzstādīšana ir atļauta saskaņā ar šo izņēmumu, bet tikai, ciktāl i) drošības atjauninājumi ir nemanāmi iepakoti un nekādā veidā nemaina programmatūras funkcionalitāti iekārtā (ieskaitot mijiedarbību ar citu lietotāja izvēlētu programmatūru vai iestatījumiem); ii) galalietotājs tiek iepriekš informēts katru reizi, kad tiek uzstādīts atjauninājums, un iii) galalietotājam ir iespēja atslēgt šo atjauninājumu automātisku uzstādīšanu.

## ***TIEŠĀ TIRGVEDĪBA***

Vēl viena jautājumu kategorija ir saistīta ar nepietiekamu aizsardzību pret tiešo tirgvedību.

27. Pirmkārt, bažas rada tas, **ka tiešās tirgvedības darbības joma ir pārāk ierobežota.** Ierosinātās regulas 4. panta 3. punkta f) apakšpunktā “tiešās tirgvedības paziņojumi” ir definēti kā “katra rakstiska vai mutiska reklāma, ko nosūta vienam vai vairākiem identificētiem vai identificējamiem elektronisko sakaru pakalpojumu galalietotājiem”. Vārda “nosūta” lietojums norāda uz tehnoloģiskās saziņas līdzekļu izmantošanu, kas obligāti ietver saziņas nodošanu, lai gan lielākā daļa reklāmu tīmeklī (izmantojot sociālo mediju platformas vai tīmekļa vietnes) neietver reklāmu sūtīšanu tiešā nozīmē. To vēl vairāk uzsver piemēri, kas uzskaitīti šajā definīcijā (SMS, e-pasts) un

---

<sup>17</sup> Turpat.

33. apsvērumā. Tie visi atsaucas uz samērā tradicionālām tirgvedības saziņas formām, un pat tad tradicionālo zvanīšanas sistēmu izmantošana neapšaubāmi neietilpst darbības jomā. Pants un apsvēruma jāgroza, iekļaujot visu reklāmu, kas *nosūtīta, ko vērš vai parāda* vienam vai vairākiem identificētiem vai identificējamiem galalietotājiem. Turklāt būtu arī jānodrošina, ka uz uzvedību balstītas reklāmas (pamatojoties uz tiešo lietotāju profiliem) arī tiek uzskatītas par tiešās tirgvedības paņēmumiem, kas vērsti uz “vienu vai vairākiem identificētiem vai identificējamiem galalietotājiem” (jo reklāmas ir vērstas uz konkrētiem, identificējamiem lietotājiem).

Turklāt saskaņā ar ierosināto “tiešās tirgvedības paņēmumu” tvērumu, 16. panta 1. punktā paredzētā aizsardzība attiecas tikai uz paņēmumiem, kuros ir reklāmas materiāls, un tie neaizsargā individuus no citām ziņām, kas tiek sūtītas, vērstas vai parādītas tirgvedības nolūkos (piemēram, klientu piesaistīšanas ziņojumi, kam nepieciešama piekrišana, politisko uzskatu popularizēšana vai balsošanas preferences, labdarības veicināšana vai citu bezpeļņas organizāciju vai organizācijas vispārējā zīmola pārstāvēšana). Turklāt faksa aparāti joprojām tiek izmantoti kā tiešās tirgvedības metode, lai gan definīcijā tie nav minēti. Tāpēc 4. panta 3. punkta f) apakšpunktā būtu jāietver jebkāda veida reklāma, aģitācija vai popularizēšana arī bezpeļņas organizācijām, un skaidri jānorāda faksa aparāti līdzās e-pastam un īsziņām (skatīt arī precizējuma ieteikumu 43.a piezīmē). Visbeidzot 32. apsvērumā ir teikts, ka politisko partiju nosūtītie paņēmumi savu partiju popularizēšanai arī ietilpst tiešajā tirgvedībā. Šis apsvēruma būtu jāatjaunina, iekļaujot politiskus un vēlēšanu kandidātus, kuri reklamē savu kandidatūru.

28. Otrkārt, **tiešās tirgvedības piekrišanas atsaukšana nav bez maksas, nedz arī tik vienkārša kā piekrišanas sniegšana.** Jāprecizē iespēja izņemt piekrišanu saskaņā ar ierosināto regulu, lai nodrošinātu atbilstību un uzlabotu saņēmēju aizsardzību. Patlaban ierosinātās regulas 16. panta 6. punktā ir noteikts, ka tiešās tirgvedības saņēmējiem ir jāsniedz “informāciju, kas saņēmējiem ir vajadzīga, lai izmantotu savas tiesības vienkāršā veidā atsaukt savu piekrišanu attiecībā uz turpmāku tirgvedības paņēmumu saņemšanu” (izcēlums ir pievienots). To apstiprina 34. apsvēruma. Tomēr no VDAR 70. apsvēruma izriet, ka VDAR datu subjektiem ne tikai jābūt tiesībām vienkāršā veidā vērsties pret apstrādi tiešās tirgvedības nolūkā, bet arī jābūt iespējai to darīt “bez maksas”. Šo terminu izmanto arī ierosinātās regulas 16. panta 2. punktā, bet tikai attiecībā uz atteikšanos no tiešās tirgvedības, kas tiek veikta, pamatojoties uz pārdošanas kontekstā iegūtajiem kontaktu datiem.

VDAR 7. panta 3. punktā paredzēts, ka piekrišanas atsaukšanai ir jābūt tikpat vienkāršai kā piekrišanas došanai un ka indivīdiem jebkurā laikā jābūt iespējai atsaukt piekrišanu. Turklāt savā atzinumā 04/2010 par *FEDMA* (WP174) darba grupa jau ir atzinusi, ka ir svarīgi, lai būtu “vienkārša, efektīva, bezmaksas, tieša un viegli pieejama metode”<sup>18</sup>, kā atteikties no tiešās tirgvedības. Šis piekrišanas atsaukšanas

---

18 29. panta darba grupa, WP174, Atzinums Nr. 4/2010 par *FEDMA* Eiropas rīcības kodeksu personas datu izmantošanai tiešajā tirdzniecībā, pieņemts 2010. gada 13. jūlijā, tīmekļa vietne: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174\\_lv.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_lv.pdf)

standarts ir jāiekļauj ierosinātās regulas tiešās tirgvedības noteikumos. Tas pats attiecas uz VDAR 7. panta 3. punkta prasību, ka jebkurā laikā piekrišanas atsaukšanai ir jābūt tikpat vienkāršai kā tās sniegšanai.

29. Saistībā ar to **būtu jāprecizē veids, kā atsaukt savu piekrišanu vai atteikties no tiešās tirgvedības izsaukumiem.** Pamatojoties uz ierosinātās regulas 16. panta 4. punktu, dalībvalstis var izvēlēties atteikšanās režīmu tiešās tirgvedības balss izsaukumiem. E-privātuma regulā būtu jānosaka kārtība, kādā atsaukt piekrišanu un atteikties no tiešās tirgvedības balss izsaukumiem. 36. apsvērumā ir precizēts, ka dalībvalstīm *vajadzētu būt iespējai* izveidot un/vai saglabāt nacionālās atteikšanās sistēmas. Pamatojoties uz šo noteikumu, dalībvalstis tādējādi varētu pat pieļaut situāciju, kad lietotājam būtu jāatsakās no atsevišķiem sakaru sniedzējiem. Šāda īstenošana neaizsargā lietotājus pret nepamatotas saziņas traucējumiem<sup>19</sup> un nenodrošina VDAR atbilstošu mehānismu vienkāršai piekrišanas atsaukšanai jebkurā laikā. Tādēļ regulā būtu jānorāda, ka katrai dalībvalstij *jāizveido* valsts bloķēto numuru reģistrs. Turklāt regulā būtu jānorāda, ka balss izsaukumu saņēmējiem jāsniedz divas iespējas viņu piekrišanas atsaukšanai: iespēju attiecībā uz turpmākajiem izsaukumiem no šī uzņēmuma vai organizācijas un iespēju šo izsaukumu laikā reģistrēties valsts bloķēto numuru reģistrā.
30. Cits jautājums, kas raisa bažas, ir apstāklis, ka **tiešās tirgvedības paziņojumu sūtīšanā nav nepārprotami aizliegta neīstu identitāšu izmantošana.** 34. apsvērumā ir norādīts, ka “tiešās tirgvedības nolūkos sagatavotu nepasūtītu komercpaziņojumu izsūtīšanā slēpt identitāti un izmantot viltus identitāti, viltus atpakaļ adresi vai viltus numurus” ir aizliegts. Tomēr 16. panta 4. punktā ir tikai noteikts, ka galalietotājus informē par “tās juridiskās vai fiziskās personas identitāti, kuras vārdā šie paziņojumi tiek pārraidīti”. Šis pienākums informēt saņēmējus par identitāti jāpapildina ar skaidru aizliegumu izmantot slēptas vai nepatiesas kontaktu adreses tiešās tirgvedības nolūkos.
31. Šis punkts ir saistīts ar citu jautājumu, kas raisa bažas: **prefiksu prasība tiešās tirgvedības izsaukumiem tiek piedāvāta kā alternatīva kontaktu līnijas identifikācijas prasībai.** Saskaņā ar 16. panta 3. punktu tiešās tirgvedības izsaukumi ir atļauti gadījumos, kad zvanītājs vai nu i) uzrāda tā tiešā numura identifikatoru, kuru izmantojot, var sazināties ar attiecīgo personu (16. panta 3. punkta a) apakšpunkts), vai ii) uzrāda īpašu kodu vai prefiksu, kas norāda uz to, ka tas ir tirgvedības izsaukums (16. panta 3. punkta b) apakšpunkts). Lai gan darba grupa atzinīgi vērtē regulas 16. panta 3. punktā b) apakšpunktā noteikto pienākumu izmantot prefiksu, tā uzskata, ka šī prasība nerisina to pašu jautājumu, uz kuru attiecas kontaktu līnijas identifikācijas pienākums saskaņā ar 16. panta 3. punkta a) apakšpunktu. Tā kā prefiksu prasība ir paredzēta, lai dotu iespēju saņēmējam iepriekš identificēt izsaukumu kā tirgvedības izsaukumu (un īstēnot pasākumus, lai bloķētu šos izsaukumus), kontaktpersonu identifikācijas prasības mērķis ir nodrošināt saņēmējiem (un uzraudzības iestādēm) iespējas identificēt un sazināties ar

<sup>19</sup> Piemēram, Lielbritānijā telekomunikāciju operators *BT* vienā nedēļā reģistrēja 31 miljonu traucējošo zvanu. Skatīt: <http://www.bbc.com/news/business-38635921>.

tirgvedības ierosinātāju. Tas jo īpaši attiecas uz automatizētiem izsaukumiem, kur pastāv nopietna nelīdzsvarotība starp tirgotāju iespējām raidīt traucējošus zvanus un saņēmēja iespējām no tiem izvairīties. Tāpēc prasības nedrīkst būt alternatīvas, bet gan savstarpēji papildinošas.

#### GRAFIKS

32. 29. panta darba grupa atzinīgi vērtē Eiropas Komisijas atziņu, ka ierosinātai regulai jāstājas spēkā vienlaikus ar VDAR 2018. gada maijā, lai izvairītos no pretrunām starp abiem šiem tiesību aktiem. Tomēr joprojām pastāv bažas, ka šis grafiks ir pārāk ambiciozs, jo nepieciešams izstrādāt arī EESK projektu. Tādēļ DG29 aicina visas likumdošanas procesā iesaistītās puses apņemties ievērot noteikto 2018. gada maija termiņu.

#### CITI JAUTĀJUMI, KAS RAISA BAŽAS

Šajā sadaļā ir apskatīti vairāki papildu jautājumi.

33. Pirmkārt, DG29 pauž bažas par **ieteikumu, ka datu saglabāšanas pasākumi, kuri nav mērķtiecīgi, ir pieņemami**. Paskaidrojuma rakstā ir norādīts, ka saskaņā ar ierosināto regulu dalībvalstīm joprojām ir tiesības saglabāt vai izveidot valsts datu saglabāšanas sistēmas, kas cita starpā paredz mērķtiecīgus saglabāšanas pasākumus (1.3. punkts). Pēc lēmuma lietā *Tele2/Watson*<sup>20</sup> ir skaidrs, ka saskaņā ar Hartu ir atļauta tikai mērķtiecīga saglabāšanas sistēma (un pat tad uz to attiecas tādi svarīgi nosacījumi kā pārraudzība) un ka vispārēja piekļuve metadatiem, tāpat kā vispārēja piekļuve elektronisko sakaru saturam, būs jāuzskata par 7. panta būtības pārkāpumu (skatīt EST spriedumu lietā *Schrems* un 94. apsvērumu). Tādējādi šī teikuma formulējums norāda uz noteiktu iespēju dalībvalstīm attiecībā uz datu saglabāšanas pasākumiem, kas nepastāv. Saistībā ar to **ierosinātajā regulā metadatiem netiek piešķirts pietiekams aizsardzības līmenis**. Kā norādīts 10. piezīmē, 29. panta darba grupa novērtē atzinumu, ka metadati var atklāt ļoti sensitīvus datus. Tomēr ierosinātajā regulā metadati nesaņem aizsardzību, kas izriet no šī atzinuma. Ņemot vērā metadatu sensitivitāti, jo īpaši pirms analīzes saskaņā ar 6. panta 2. punkta c) apakšpunktu, ir jāveic DAIN (skatīt arī 46. piezīmi).

34. Otrkārt, **ierosinātā regula nevēlami paplašinātu datu saglabāšanas iespējas**. Ierosinātās regulas 11. pantā ir atsauce uz VDAR 23. panta 1. punkta a) līdz e) apakšpunktu, aprakstot nolūkus, kādiem dalībvalstis var ierobežot regulas 5.-8. pantā paredzētās saistības un tiesības. VDAR neparedz šādus ierobežojumus attiecībā uz īpašām datu kategorijām, ievērojot datu subjektu lielo risku. Kamēr E-privātuma direktīvas 15. panta nosacījumi pašlaik pieļauj līdzīgu ierobežojumu, nolūki ir vairāk ierobežoti. Jaunā ierosinātā regula varētu radīt jaunus ierobežojumus, lai nodrošinātu “kriminālsodu izpildi, tostarp aizsardzību pret sabiedriskās drošības

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

apdraudējumiem un to novēršanu” (VDAR 23. panta 1. punkta d) apakšpunkts) un “citus svarīgus Savienības vai dalībvalsts vispārējo sabiedrības interešu mērķus, jo īpaši Savienībai vai dalībvalstij svarīgas ekonomiskās vai finanšu intereses, tostarp monetāros, budžeta un nodokļu jautājumus, sabiedrības veselību un sociālo nodrošinājumu” (VDAR 23. panta 1. punkta d) apakšpunkts). Šie mērķi ir ne tikai jauni salīdzinājumā ar E-privātuma direktīvu, bet pēdējais 23. panta 1. punkta d) apakšpunktā norādītais nolūks un viss 23. panta 1. punkta e) apakšpunkta nolūks ir ļoti plaši formulēti. Tādēļ tiek ierosināts svītrot atsauci uz VDAR 23. panta 1. punkta a) līdz e) apakšpunktu un tā vietā minēt tikai tos nolūkus, kas pašlaik minēti E-privātuma direktīvas 15. pantā.

35. **Pienākumam informēt lietotājus par drošības riskiem ir minimāls tvērums.** Darba grupa atzinīgi vērtē faktu, ka pakalpojumu sniedzējiem ir jāinformē lietotāji par drošības riskiem un pasākumiem šos risku novēršanai, piemēram, šifrēšanu (17. pants un 37. apsvērums). Tomēr normas virsraksts ir formulēts šādi: “Informācija par konstatētajiem drošības riskiem”. Fakts, ka nosaukums attiecas uz konstatētajiem riskiem, liecina, ka šī norma attiecas tikai uz (iespējamajiem) drošības pārkāpumiem, savukārt normas formulējums un apsvērums vairāk attiecas uz galalietotāju vispārējo izglītošanu. Piemēram, ja pakalpojumu sniedzējs konstatē, ka lietotāja ierīce ir inficēta ar ļaunprogrammatūru un ir kļuvusi par robottīkla daļu, šķiet, ka šī norma uzliek pakalpojumu sniedzējam tiešu pienākumu informēt lietotāju par radītajiem riskiem. Tomēr šīs normas piemērošanas jomu varētu precizēt, un to nevajadzētu attiecināt tikai uz šo īpašo scenāriju. Noteikumā jāiekļauj vismaz aptvertie drošības riski visās iekārtās, ko pakalpojuma sniedzējs piegādā galalietotājam abonēšanas ietvaros, piemēram, maršrutētājus un mobilās ierīces, un jāietver izglītošanu par privātuma aizsardzības iestatījumu maiņas riskiem saskaņā ar integrēta privātuma principu.

Darba grupa iesaka paplašināt piemērošanas jomu, iekļaujot tajā programmatūras piegādātājus, kuri pieļauj elektroniskos sakarus (skatīt 8. apsvērums) un, iespējams, arī jaunu kategoriju: sakaru nodrošināšanai svarīgu tehnoloģiju piegādātāji, kuri nav pakalpojumu sniedzēji (piemēram, šifrēšanas tehnoloģiju piegādātāji). Šīs pēdējās paplašināšanas gadījumā būtu jāņem vērā, ka šis pienākums nepārkļājas ar drošības pārkāpumu paziņošanas pienākumiem, kas paredzēti citos instrumentos, piemēram, NIS direktīvā<sup>21</sup> un citos juridiskajos instrumentos attiecībā uz sertifikātu sniedzējiem. Tā kā pēdējās kategorijas tehnoloģiju piegādātājiem parasti nav tieša kontakta ar galalietotājiem, ir arī jāpaskaidro, kā tie var izpildīt savus pienākumus sniegt informāciju saskaņā ar šo noteikumu.

36. Darba grupa atzinīgi vērtē 2. un 13. panta noteikumus par numuratkarīgiem starppersonu sakaru pakalpojumiem. Tomēr nav uzreiz skaidrs, kādēļ **līdzīga līmeņa privātuma aizsardzība nebūtu pieejama arī funkcionāli līdzvērtīgiem OTT izsaukuma pakalpojumiem.**

<sup>21</sup> Eiropas Parlamenta un Padomes Direktīva (ES) 2016/1148 (2016. gada 6. jūlijs) par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1.-30. lpp., tīmekļa vietne: [http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.194.01.0001.01.ENG](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG)



37. Darba grupai ir arī bažas par **skaidrības trūkumu attiecībā uz granulāro piekrišanu reversās meklēšanas veikšanai abonentu sarakstos**. Ierosinātās regulas 15. panta 2. punktā noteikts, ka pakalpojumu sniedzējiem jāsaņem galalietotāju piekrišana, pirms tiek veiktas ar datiem saistītas meklēšanas funkcijas (skatīt arī 31. apsvērumu). Darba grupa atzinīgi vērtē piekrišanas prasības saskaņošanu attiecībā uz iekļaušanu abonentu sarakstos, taču pauž nožēlu par to, ka trūkst granularitātes dažādu veidu meklējumos. Spēkā esošā E-privātuma direktīva ļauj dalībvalstīm pieprasīt atsevišķu piekrišanu attiecībā uz reverso meklēšanu, pamatojoties uz 12. panta 3. punktu. Pantā noteikts, ka “dalībvalstis var pieprasīt, ka, izmantojot publiski pieejama abonentu sarakstu tādām nolūkam, kas nav personu kontaktinformācijas meklēšana, pamatojoties uz to vārdiem vai nosaukumiem un nepieciešamības gadījumā uz citu minimālo identifikācijas informāciju, ir jāsaņem papildu piekrišana no abonentiem”. Pamatojoties uz šo noteikumu, daudzās dalībvalstīs ir nepieciešama atsevišķa piekrišana reversās meklēšanas funkcijām, ņemot vērā atšķirīgos identifikācijas līmeņus un tādējādi abu funkciju iejaukšanos.
38. Attiecībā uz formu janorāda, ka **naudas sodu līmenis nav saskaņots attiecībā uz visiem regulas pārkāpumiem**. Ierosinātā regula paredz, ka dalībvalstis nosaka noteikumus sankcijām par ierosinātās regulas 23. panta 4. punkta, 23. panta 6. punkta un 24. panta pārkāpumiem). Atbilstošāk būtu to noteikt pašā E-privātuma regulā.
39. Visbeidzot, **ierosinātā regula balstās uz definīcijām, kuras var kļūt par “kustīgajiem mērķiem”**. Attiecībā uz vairākiem tā galvenajiem jēdzieniem ierosinātajā regulā ir atsauce uz citu juridisku instrumentu, kas šobrīd ir projekta stadijā: ierosinātais EESK (piemēram, 4. panta 1. punkta b) apakšpunkts). Divi svarīgi piemēri šajā sakarā ir “galalietotāja” definīcija, kurā pašlaik ietilpst fiziskas un juridiskas personas, kā arī definīcijas “elektronisko sakaru pakalpojums” un “starppersonu sakaru pakalpojums”, kas ierosinātajā regulā ietverti 4. panta 1. punkta b) apakšpunktā, un pēdējā gadījumā sīkāk izstrādāts 4. panta 2. punktā, iekļaujot pakalpojumu veidus, kas izslēgti EESK.<sup>22</sup> Šis atzinums ir balstīts uz pašreiz spēkā esošajām definīcijām, tomēr, iespējams, ka ierosinātais EESK un/vai tā galvenie jēdzieni mainīsies. Tas nekavējoši ietekmētu arī E-privātuma regulu. Ideālā gadījumā visus terminus, kas izriet no EESK, vajadzētu atsevišķi definēt E-privātuma regulā; vai vismaz ierosinātajā regulā jāiekļauj skaidrojums, ja ir termini, kuru definīcijas atšķiras no EESK iekļautajām definīcijām (piemēram, “papildpakalpojumu” iekļaušana “starppersonu sakaru pakalpojuma” definīcijā). Tomēr, ja tas nav iespējams, darba grupa vēlētos ierosināt visām likumdošanas procesā iesaistītajām pusēm nodrošināt, ka gan ierosinātā regula, gan EESK tiek apspriesti un par tiem balso vienlaicīgi, ļaujot ieinteresētajām personām pareizi novērtēt jauno instrumentu darbības jomu un ietekmi.

---

<sup>22</sup> Piemēram, ierosinātās regulas 4. panta 2. punktā ir teikts, ka “definīcijā “starppersonu sakaru pakalpojums” ietilpst pakalpojumi, kuros interaktīva starppersonu saziņa ir tikai ar citu pakalpojumu saistīta sīka palīgfunckcija”, savukārt EESK 2. panta 5. punkts īpaši izslēdz šādus pakalpojumus no šīs definīcijas. (EESK ietver 2. panta 4. punkta plašo “elektronisko sakaru pakalpojumu” kategoriju “starppersonu sakaru pakalpojumus”).

## 5. IEROSINĀJUMI PRECIZĒJUMIEM, LAI NODROŠINĀTU TIESISKO NOTEIKTĪBU

Papildus iepriekš apskatītajiem jautājumiem darba grupa arī vēlas uzsvērt dažus ierosinātās regulas noteikumus, kurus būtu vēlams precizēt. Šādi precizējumi tiek uzskatīti par nepieciešamiem, lai uzlabotu visu ieinteresēto personu tiesisko noteiktību, ka visā Eiropas Savienībā būs vienota izpratne par E-privātuma regulu un tās piemērošana.

### DARBĪBAS JOMAS PRECIZĒJUMI

40. Attiecībā uz ierosinātās regulas darbības jomu 29. darba grupa ierosina turpmāk izklāstītos precizējumus.

- a. **Terminā “galalietotājs” būtu jāiekļauj visi individuālie lietotāji.** EESK 2. panta 14. punktā “galalietotājs” ir lietotājs, kas nenodrošina publiskos sakaru tīklus vai publiski pieejamus elektronisko sakaru pakalpojumus. Būtu jāprecizē, ka no ierosinātās regulas aizsardzības jomas nav izslēgtas personas, kuras piedalās tīklos, piemēram, režģītīklos ar WiFi maršrutētāju.
- b. **Būtu jāprecizē, ka teritoriālā darbības joma attiecas uz visiem galalietotājiem Savienībā.** 3. panta 1. punkta a) apakšpunktā noteikts, ka priekšlikums regulai attiecas uz elektronisko sakaru pakalpojumu sniegšanu galalietotājiem “Savienībā”, savukārt 3. panta 1. punkta c) apakšpunktā noteikts, ka tas attiecas uz “Savienībā esošo” galalietotāju galiekārtu aizsardzību (izcēlums pievienots). Pastāv atšķirības dažādos tulkojumos. Vācu valodas tulkojumā nav šādas atšķirības, savukārt citos — franču, spāņu un nīderlandiešu, ir. No 9. apsvēruma izriet, ka teritoriālā darbības joma ir plaša neatkarīgi no tā, vai pakalpojumi tiek sniegti ārpus Savienības, vai arī apstrāde notiek Savienībā. Tādēļ tiek ierosināts svītrot terminu “esošo” 3. panta 1. punkta c) apakšpunktā, lai uzsvērtu plašo darbības jomu.
- c. **Šķiet, ka ierosinātā regula aizsargā tikai konfidencialus sakarus *tranzītā*, nevis *uzglabājot*.** Pašreizējā pieeja ierosinātajā regulā ir vērsta uz sakaru pārraides aizsardzību. Skatīt, piemēram, 15. apsvērumu, kurā noteikts, ka sakaru datu pārtveršanas aizliegums būtu jāpiemēro to nodošanas laikā, t. i., līdz brīdim, kad saņēmējs saņem paziņojuma saturu. Šis aizsardzības tvērums ir balstīts uz novecojušu sakaru konceptuālo sistēmu. Lielāko daļu sakaru datu pakalpojumu sniedzēji glabā pat pēc to saņemšanas. Jānodrošina, ka šo datu konfidencialitāte joprojām tiek aizsargāta. Turklāt sakari starp viena mākonī balstīta pakalpojuma (piemēram, tīmekļa pasta pakalpojumu sniedzēji) abonentiem bieži vien rada tikai nelielu pārraidi: pasta nosūtīšana lielākoties ietvers to atspoguļošanu pakalpojuma sniedzēja datubāzē, nevis tiešu saziņu starp abām pusēm. Arguments, ka VDAR to jau aptver, nav pārliecinošs: viss ierosinātās regulas nolūks ir aizsargāt visu konfidencialo saziņu neatkarīgi no tā, kādi tehniskie līdzekļi šādai saziņai tiek izmantoti. Iespējams, ka tā ir tikai izstrādes kļūda, jo 5. pantā minētais aizliegums attiecas uz “uzglabāšanu” un “apstrādi”.
- d. **Visiem publiskajiem bezvadu interneta pieslēguma punktiem vajadzētu būt iekļautiem darbības jomā.** Tā kā bezvadu piekļuves

punktu izmantošana ir izplatīta, ir loģiski, ka nevajadzētu pastāvēt šaubām par to, vai saziņas, izmantojot šādus piekļuves punktus, konfidencialitāte ir aizsargāta. Regula tiecas to neseekmīgi noskaidrot, jo darbības joma tiek paplašināta tikai attiecībā uz tīkliem, kas tiek nodrošināti “nenoteiktai galalietotāju grupai” (13. apsvēruma). Ir jādefinē termini “nenoteikta galalietotāju grupa” un “slēgta galalietotāju grupa”. Jo īpaši jāprecizē, ka darbības jomā ietverti arī droši bezvadu tīkli (t. i., ar paroli), ja šī parole tiek sniegta teorētiski nenoteiktai lietotāju grupai, kuru identitāti iepriekš nevar noteikt (piemēram, kafejnīcas klienti, lidostu apmeklētāji). Pamatprincips šajā kontekstā ir tāds, ka saskaņā ar WP29 iepriekšējo atzinumu par ePD pārskatīšanu “tikai tie pakalpojumi, kas notiek oficiālā vai nodarbinātības situācijā tikai ar darbu saistītiem vai oficiāliem nolūkiem, vai tehniska saziņa starp iestādēm, kas nav valsts iestādes, vai starp valsts iestādēm vienīgi, lai kontrolētu darba vai uzņēmējdarbības procesus, kā arī pakalpojumu izmantošanu tikai vietējiem nolūkiem, var tikt atbrīvoti no e-privātuma instrumenta piemērošanas.” (8. lpp.).

- e. **Ierosinātajā regulā būtu jāiekļauj dati, kas iegūti, piedāvājot ciparu apraides pakalpojumus.** Ņemot vērā skatīšanās uzvedības sensitīvo raksturu, atklājot skatītāju personiskās intereses un īpašības, E-privātuma regulā būtu jāprecizē (iespējams, apsvērumā), ka pakalpojumu sniegšana, kas nodrošina “saturu, kas pārraidīts, izmantojot elektronisko sakaru tīklus” no “elektronisko sakaru pakalpojuma” definīcijas, nenozīmē, ka uz pakalpojumu sniedzējiem, kas piedāvā gan ECS, gan satura pakalpojumus, neattiecas E-privātuma regulas noteikumi, kas attiecas uz ECS pakalpojumu sniedzējiem. Tas jo īpaši būtiski, jo pakalpojumu sniegšana, kas nodrošina “saturu, kas pārraidīts, izmantojot elektronisko sakaru tīklus” ir izslēgta no “elektronisko sakaru pakalpojuma” definīcijas ierosinātajā EESK (2. panta 4. punkts).
- f. **Sakaru dati parasti ir personas dati.** 4. apsvērumā ir norādīts, ka sakaru dati var saturēt personas datus. Tomēr lielākā daļa sakaru datu ir personas dati<sup>23</sup> un liela daļa datu ir diezgan intīmi un sensitīvi, tādēļ formulējums būtu jāgroza, lai norādītu, ka tie parasti ir personas dati.
- g. **Konfidenciāla saziņa ietver sevī ziņojumus platformas iekšienē.** 1. apsvērumā ir paskaidrots, ka konfidencialitātes princips attiecas uz gan “tagad izmantotajiem saziņas līdzekļiem, gan tiem, kas tiks izmantoti nākotnē”. Apsvērumā turpmāk sniegti šādu līdzekļu piemēri, tostarp “privātā ziņapmaiņa sociālajos medijos”. Iespējams, ir paredzēts iekļaut privātos ziņojumus starp sociālā tīkla lietotājiem (piemēram, *Facebook* vai *Twitter*) vai laikrakstā publicētām ziņām, kas ir pieejamas ierobežotam personu skaitam, bet formulējums nav pietiekami skaidrs.
- h. **Kā E-privātuma regula piemērojama mijiedarbībai starp mašīnām.** Kā minēts 9. punktā, darba grupa atbalsta mehānisma un mijiedarbības aizsardzības paplašināšanu. Tomēr tas ir minēts tikai 12. apsvērumā, nevis

<sup>23</sup> Skatīt, piemēram, EST 2003. gada 6. novembra spriedumu lietā C-101/01, 24. punkts (attiecībā uz tālruņa numuru), EST 2016. gada 19. oktobra spriedumu lietā C-582/14 (*Breyer*), 49. punkts (attiecībā uz dinamiskām IP adresēm) un EST 2014. gada 8. aprīļa spriedumu lietās C-239/12 un C-594/12 (*Digital Rights Ireland*, 26.-27. punkts (attiecībā uz metadatu sensitivitāti)).

attiecīgajā pantā. Šī aizsardzība ir vēlama, jo šāda saziņa nereti satur informāciju, kuru aizsargā tiesības uz privātumu. No otras puses, atbrīvojums būtu jāpiemēro šaurai “mašīna-mašīna” saziņas kategorijai, ja tas neietekmē ne privātu, ne konfidenciālu saziņu, piemēram, tādus gadījumus, kad šāda saziņa tiek veikta, izpildot pārvades protokolu starp tīkla elementiem (piemēram, serveriem, slēdžiem), lai viens otru informētu par to darbības statusu.

Viens konkrēts konteksts, kurā E-privātuma regulas piemērošana jāprecizē, ir intelektisko transporta sistēmu joma. Ir paredzēts, ka transportlīdzekļi, izmantojot radio, nepārtraukti pārsūtīs datus, kas satur unikālu identifikatoru. Bez papildu aizsardzības E-privātuma regulā attiecībā uz sakaru datiem tas varētu novest pie braukšanas paradumu, maršrutu un braucēju ātruma nepārtrauktas izsekošanas. Tomēr EESK 2. panta 1. punktā ir ietverta jauna un paplašināta sakaru tīklu definīcija. Tajos ietilpst pārvades sistēmas, kurām nav centralizētas administrēšanas iespējas un kas ļauj raidīt signālus. E-privātuma regulas 14. apsvērumā precizēts, ka šādi dati ir elektronisko sakaru dati. Pamatojoties uz ierosinātās regulas 5. pantu, jebkāda veida šo pārraižu datu pārtveršana, uzraudzība vai glabāšana ir aizliegta, ja vien nav spēkā kāds no izņēmumiem. Tomēr ir interesanti apstrādāt šos datus, ļaujot objektiem, piemēram, bezvadītāja automašīnām un ierīcēm, brīdināt vienu otru par apkārtējiem apstākļiem vai citiem riskiem. Jautājums, kāds izņēmums būtu piemērojams šajā gadījumā. Galalietotāju piekrišana nav īstenojams izņēmums, jo, iespējams, vienmēr būs jāspēj apstrādāt šādus datus. Pakalpojuma sniedzējiem tādēļ būtu jāspēj paļauties uz konkrētu izņēmumu, ļaujot objektiem, piemēram, bezvadītāja automašīnām un ierīcēm, brīdināt vienu otru par apkārtējiem apstākļiem vai citiem riskiem.

#### *PIEKRIŠANAS JĒDZIENA UN PIEMĒROŠANAS PRECIZĒJUMI*

41. Attiecībā uz piekrišanas jēdzienu un piemērošanu pašreizējā ierosinātajā regulā 29. darba grupa ierosina šādus precizējumus:

- a. **Kā piekrišanas jēdziens piemērojams juridisko personu kontekstā.**  
3. apsvērumā norādīts, ka regulai jānodrošina, ka VDAR noteikumi attiecas arī uz tiem lietotājiem, kuri ir juridiskas personas. Tas saskaņā ar apsvērumu ietver arī VDAR piekrišanas definīciju (skatīt arī 18. apsvērumu). Kā atzīmēts 13. piezīmē, darba grupa atzinīgi vērtē to, ka juridisko personu regulējums ir skaidri iekļauts regulas darbības jomā. Tomēr šī principa praktiskā piemērošana ir neskaidra. VDAR piekrišanas definīcija prasa, lai tā būtu “apzināta”, un norādēm uz datu subjekta vēlmēm jābūt “paziņojuma vai skaidri apstiprinošas darbības veidā” (VDAR 4. panta 11. punkts). Jāprecizē, kad juridisku personu patiesībā var uzskatīt par “apzinātu” un kādos gadījumos ir šāda juridiska persona gribas izpausme.
- b. Šajā kontekstā ir vērts atzīmēt, ka darba devējs lielākajā daļā gadījumu var nesniegt piekrišanu saviem darbiniekiem, jo, ja darba devējam ir nepieciešama darbinieka piekrišana, un, ņemot vērā nevienlīdzīgo varas līdzsvaru, ir reāls vai iespējams kaitējums, kas izriet no piekrišanas

nesniegšanas, šāda piekrišana nav spēkā, jo tā nav sniegta no brīvas gribas<sup>24</sup>. Attiecībā uz **uzņēmumiem, kas izsniedz ierīces vai aprīkojumu privātpersonām, ierosinātā regula nesatur (piemērotu) izņēmumu** iejaukšanās aizliegumam. Viens piemērs ir gadījums, kad darba devējs vēlas atjaunināt uzņēmuma izsniegto tālruni. Otrs piemērs — ja darba devējs piedāvā darbiniekiem nomas automašīnas, un administratīviem mērķiem trešā persona var vākt datus par atrašanās vietu, izmantojot automašīnas vienību. Abos gadījumos pastāv darba devēja interese iejaukties šajās ierīcēs.

Šo iejaukšanos nevar uzskatīt par nepieciešamu informācijas sabiedrības pakalpojuma sniegšanai (8. panta 1. punkta c) apakšpunkts) vai vajadzīgu tīmekļa auditorijas mērīšanai (8. panta 1. punkta d) apakšpunkts). To varētu atrisināt, radot jaunu izņēmumu, lai iekļautu situāciju, kad i) darba devējs nodrošina noteiktas iekārtas darba attiecību kontekstā, ii) darbinieks ir šī aprīkojuma lietotājs un iii) iejaukšanās ir kas noteikti nepieciešams, lai darbinieks varētu strādāt ar iekārtu (tas nozīmē, ka tiek piemēroti samērīguma jeb proporcionālītātes un subsidiaritātes principi attiecībā uz datu vākšanu). Tikai tad, ja ir izpildīti šie nosacījumi, darba devējam varētu ļaut iejaukties galalietotāju ierīcē.

- c. **Automātiskas izsaukumu pāradresācijas apturēšanas kontroles uzlabošana** 14. pants paredz galalietotājiem svarīgu kontroli pār trešās personas automātiskas izsaukumu pāradresācijas pārtraukšanu. Šo aizsardzību var vēl vairāk uzlabot, pieprasot arī galalietotāja piekrišanu pirms izsaukuma pāradresācijas.

#### *ATRAŠANĀS VIETAS UN CITU METADATU PRECIZĒJUMI*

42. Darba grupa iesaka precizēt šādus datus attiecībā uz atrašanās vietas datiem un citiem metadatiem:

- a. **Būtu jāprecizē 17. apsvērumā izteikuma “atrašanās vietas datiem, dati, kas nav ģenerēti elektronisko sakaru pakalpojumu sniegšanas saistībā”** nozīmi. Nav skaidrs, vai tas attiecas uz atrašanās vietas datiem, kas iegūti, piemēram, no lietotnēm, kuras izmanto viedo ierīču GPS funkcionalitātes datus un/vai ģenerē atrašanās vietas datus, kuru pamatā ir netālu esošie WiFi maršrutētāji, un/vai atrašanās vietas datus, kas vākti ar ierīces navigācijas palīdzību un/vai citiem atrašanās vietas datu ģenerēšanas veidiem. Šī neprecizitāte rada tiesisku neskaidrību par pienākuma tvērumu. Jebkurā gadījumā fiziskās personas galaierīces atrašanās vietas dati ir personas dati, un tādējādi uz šo datu apstrādi attiecas VDAR paredzētie pienākumi.
- b. Būtu jāprecizē, ka **lielākajai daļai leģitimās atrašanās vietas datu un citu metadatu apstrādei nav nepieciešams unikāls identifikators**. 17. apsvērumā minētas intensitātes kartes kā elektronisko sakaru pakalpojumu sniedzēju elektronisko sakaru metadatu komerciālas

<sup>24</sup> Skatīt Atzinumu 15/2011 par piekrišanas definīciju (WP 187), Atzinumu 8/2001 par personas datu apstrādi nodarbinātības jomā (WP48) un jauno Atzinumu par datu apstrādi darbā (pieņemts vienlaikus ar šo atzinumu).

izmantošanas piemērs. Tomēr intensitātes kartes izveidei nav nepieciešami unikālie identifikatori, tikai statistiska uzskaitē. Citā piemērā, kas minēts apsvērumā, infrastruktūras izmantošana un slodze uz to var tikt ņemti vērā arī noteiktos mērīšanas punktos, piemēram, izveidojot apkopotu statistiku par satiksmes torņu izmantošanu, lai identificētu slodzi noteiktā atrašanās vietā noteiktā laikposmā, bez nepieciešamības arī uzzināt saistīto personu identitāti.

Papildus apsvērumā minēts piemērs satiksmes plūsmas atspoguļošanai noteiktos virzienos noteiktā laika periodā, kur vajadzīgs unikāls identifikators, lai sasaistītu personu pozīcijas noteiktos laika intervālos. Ar šo piemēru apsvērumā, šķiet, tiek domāts par turpmāku šo datu apstrādi, lai atbalstītu "lielo datu" analīzi. Vienīgais nosacījums saskaņā ar ierosināto regulu šāda veida apstrādei ir pienākums veikt datu aizsardzības ietekmes novērtējumu, ja apstrāde *varētu radīt lielu risku fizisku personu tiesībām un brīvībām*. Šis nosacījums ir nepietiekams. Tas arī ir pretrunā 6. panta prasībai, ka šāda veida apstrāde var tikt veikta tikai ar lietotāju piekrišanu un tikai tad, ja datus nevar anonimizēt, tas ir, bez unikāliem identifikatoriem. Elektronisko sakaru pakalpojumu sniedzēji bieži vien nevar atteikties no to ģeogrāfiskās atrašanās vietas datu vākšanas, ja šāda vākšana ir tehniski nepieciešama, lai pārraidītu saziņu lietotājam vai ja šāda apstrāde ir nepieciešama pieprasītā (piemēram, navigācijas) pakalpojuma sniegšanai. Iepriekšējos atzinumos darba grupa secināja, ka šādi atrašanās vietas dati no viedajām ierīcēm ir sensitīvi personas dati un ka šo datu analīzes priekšrocības nav prioritāras attiecībā uz lietotāju tiesībām aizsargāt savu sakaru metadatu konfidencialitāti, nedz arī tie ir prioritāti attiecībā uz to vispārējām tiesībām uz datu aizsardzību saskaņā ar VDAR. Tādēļ apsvērumā ir vismaz jānorāda, ka pakalpojumu sniedzējiem ir jāievēro saistības, kas izriet no VDAR 25. panta, ja tālāk tiek apstrādāti atrašanās vietas dati vai citi metadati. Tas nozīmē, ka ir jāveic vismaz šādi pasākumi.

- i) pagaidu pseidonīmu izmantošana;
- ii) jebkādu reverso atsauču tabulu dzēšana starp šiem pseidonīmiem un oriģinālajiem identificējošajiem datiem;
- iii) apkopošana līdz līmenim, kurā atsevišķus lietotājus vairs nevar identificēt, izmantojot savus konkrētos maršrutus; un
- iv) izslēgto personu, attiecībā uz kurām identifikācija joprojām būtu iespējama, dzēšana (visi šie pasākumi jāpiemēro kopā).

Visbeidzot E-privātuma regulai ir jāuzliek par pienākumu personām, kuras iesaistītas atrašanās vietas apstrādē un citos metadatos, publiskot anonimizācijas un turpmākās apkopošanas metodes, neskarot ar likumu aizsargāto slepenību. Tas ļautu gan uzraudzības iestādēm, gan plašākai sabiedrībai viegli pārbaudīt, vai izvēlēta metode ir atbilstoša.

#### PRECIZĒJUMI PAR NEPASŪTĪTIEM PAZIŅOJUMIEM

43. Darba grupa iesaka precizēt šādus datus attiecībā uz nepasūtītiem paziņojumiem:

- a. **Tiešās tirgvedības bez piekrišanas aizlieguma formulējums.** Tagad ierosinātās regulas 16. panta 1. punktā norādīts, ka elektronisko sakaru

pakalpojumus var "izmantot", lai nosūtītu tiešo tirgvedību (ar piekrišanu), taču tajā nav tieša aizlieguma būt (vērst vai parādīt) tiešu tirgvedību bez piekrišanas. Tas ir pretrunā pieejai citos noteikumos, kur vispirms ir formulēts aizliegums un pēc tam tiek veikta turpmāka uzraudzība ar dažiem īpašiem izņēmumiem. Pašreizējais formulējums liecina par saudzīgāku pieeju (kas, iespējams, nav paredzēta). Darba grupa ierosina nedaudz mainīt pašreizējo E-privātuma direktīvas 13. panta 1. punkta redakciju: "Fiziskām vai juridiskām personām izmantojot elektronisko sakaru pakalpojumu, tostarp balss izsaukumus, automātisko izsaukuma un sakaru sistēmu, ieskaitot pusautomātiskas sistēmas, kas savieno izsaukto personu ar individu, faksus, elektronisko pastu vai citus elektroniskās saziņas līdzekļus, pakalpojumi tiešo tirgvedības paziņojumu parādīšanas galalietotājiem nolūkiem var tikt atļauti tikai attiecībā uz lietotājiem, kuri tam ir devuši iepriekšēju piekrišanu."

- b. **Noteikumu darbības joma attiecībā uz tirgvedības paziņojumiem un izsaukumiem esošajiem kontaktiem.** Saskaņā ar 16. panta 2. punktu, ja persona no esoša klienta saņem elektroniskās vēstules kontakthinformāciju, tā var izmantot šīs ziņas savām precēm un pakalpojumiem turpmākajai tiešai tirgvedībai, ja vākšanas laikā un katrā paziņojumā tiek sniegta skaidra, bezmaksas un vienkārša iespēja iebilst. Šobrīd tas attiecas tikai uz komerciāliem kontaktiem, kas iegūti "saistībā ar produkta vai pakalpojuma pārdošanu", kā arī par savu līdzīgu produktu vai pakalpojumu komerciālu tirgvedību. Ņemot vērā, ka tiešās tirgvedības noteikumi vienādi attiecas uz nekomerciālām veicināšanas darbībām (piemēram, labdarības organizācijām vai politiskajām partijām), šis noteikums būtu jāgroza, vienādi piemērojot nekomerciālām organizācijām saziņai ar iepriekšējiem atbalstītājiem, tām veicinot līdzīgus mērķus vai ideālus, un būtu jāpiemēro tādas pašas tiesības izteikt iebildumus, kas attiecas uz tiešās tirgvedības izsaukumiem. Papildus tam ir jānosaka termiņš elektronisko sakaru "esošo klientu kontaktu" derīgumam komerciālos, labdarības vai politiskos nolūkos, un šis termiņš jāattiecinā arī uz tiešās tirgvedības izsaukumiem. Ja dalībvalstis izvēlējušās iebildumu sistēmu attiecībā uz tiešās tirgvedības balss izsaukumiem, "esošā klientu kontakta" esība neļauj reģistrēties bloķēto zvanu reģistrā. Šādos apstākļos galalietotājiem nav efektīvas iespējas novērst traucējošos zvanus no uzņēmumiem vai organizācijām, ar kurām tie kādreiz ir sazinājušies, bet vairs nevēlas saistīties. Tādēļ regulā būtu jāprecizē šī "esošā klienta" izņēmuma spēkā esības termiņš, piemēram, viens vai divi gadi, saistībā ar attiecīgo galalietotāju tiesisko palāvību.

- c. **Tiešās tirgvedības noteikumu piemērošana juridiskai personai.** Ierosinātās regulas 16. panta 5. punktā paredzēts, ka dalībvalstis nodrošina, ka galalietotāju, kas ir juridiskas personas, likumīgas intereses attiecībā uz nevēlamiem paziņojumiem ir pietiekami aizsargātas. Pašreizējās E-privātuma direktīvas 13. panta 5. punktā ir aprakstītas abonenti, kas nav fiziskas personas, likumīgās intereses. Nav skaidra formulējuma maiņas ietekme. Apsvērumos ir jāprecizē, ka šīs izmaiņas neatspoguļo nodomu nodrošināt zemāku aizsardzības līmeni. Saistībā ar to tiešās tirgvedības bez piekrišanas aizliegums attiecas uz "galalietotājiem, kas ir fiziskas personas, kuras tam sniegušas piekrišanu" (izcēlums pievienots). Ir jāprecizē, ka tas ietver arī

fiziskas personas, kuras *strādā pie* juridiskajām personām. No otras puses, piekrišana nebūtu nepieciešama, lai vērstos pie juridiskām personām, izmantojot vispārīgu kontaktinformāciju, ko tās šim nolūkam ir publiskojušas (piemēram, "info@companyname.eu").

- d. **Tiešās tirgvedības noteikumu piemērošana tiem, kas darbojas (politiskas) pārstāvības līmenī:** 16. pants esošajā redakcijā var liegt dažus paziņojumus, kas tiek sūtīti ievēlētajiem pārstāvjiem, izklāstot komerciālas bažas vai intereses. Jāprecizē, ka regula neaizliedz šādus paziņojumus.

#### PRECIZĒJUMI PAR PAMATTIESĪBU INSTRUMENTU PIEMĒROŠANU

44. Papildus būtu jāprecizē **Hartas un ECTK piemērošana valsts datu saglabāšanas tiesību aktiem.** 26. apsvērumā noteikts, ka visiem dalībvalstu pasākumiem sabiedrības interešu aizsardzībai, piemēram, likumīgiem pārtveršanas pasākumiem, jābūt saskaņā ar Hartu (papildus ECTK). Tas ir vēlams, jo atbilst argumentācijai lietā *Tele2/Watson*, saskaņā ar kuru uz Hartu attiecas visi valstu izņēmumi no ES tiesību aktu datu apstrādes aizsardzības (un tādēļ valstu tiesību aktu pārkāpumus var iesniegt ES tiesā). Tomēr ierosinātās regulas 11. pantā ir tikai norādīts, ka ierosinātās regulas 5.-8. Panta tvēruma ierobežojumiem ir jāievēro pamattiesību un brīvību būtība un veiktajam pasākumam jābūt nepieciešamam un samērīgam. Šeit būtu jāiekļauj skaidra atsauce uz Hartu un ECTK.
45. **Ka paziņojumu konfidencialitāte ir aizsargāta arī saskaņā ar ECTK 8. pantu.** Paskaidrojuma raksta 1.1. punktā un 1. apsvērumā ir paskaidrots, ka ierosinātā regula īsteno hartas 7. pantu. Tas tiek atkārtots 19. apsvērumā. Tomēr pamattiesības uz paziņojumu konfidencialitāti tiek aizsargātas ne tikai šajā noteikumā, bet arī saskaņā ar ECTK 8. pantu. Iekļaujot ierosinātās regulas pantā tiešu atsauci, vēl vairāk apstiprinās, ka, izvērtējot (galīgo) regulu, būs jāņem vērā arī jebkura attiecīgā Eiropas Cilvēktiesību tiesas prakse. Starp citu, šī atsauce jau ir iekļauta 20. apsvērumā (attiecībā uz galiekārtām) un 26. pantā (kas attiecas uz likumīgu pārtveršanu), un to papildina apsvērumi, kas minēti Paskaidrojuma raksta 2.1. punktā (par attiecībām starp Hartu un ECTK juridisko personu kontekstā), bet ne kādā no attiecīgajiem pantiem, piemēram, 11. panta 1. punktā.

#### CITI PRECIZĒJUMI

46. Būtu jāprecizē, ka, apstrādājot personas datus saistībā ar elektronisko sakaru datiem, **turpina piemērot VDAR saistības, piemēram, attiecībā uz datu aizsardzības pārkāpumu režīmu un DAIN.** Tā kā 5. apsvērumā minēts, ka ierosinātā regula ir VDAR *lex specialis* un elektronisko sakaru datu apstrāde būtu atļauta tikai saskaņā ar ierosināto regulu, varētu apšaubīt, vai konkrēti VDAR ietvertie pienākumi ir piemērojami arī ierosinātās regulas kontekstā. Tas jo īpaši attiecas uz gadījumu, kad ierosinātā regula varētu tikt interpretēta, ka tā uzliek noteiktu pienākumu, kuru aptver arī VDAR. Indikatīvi piemēri:



- (i) ierosinātā regula uzliek pienākumu informēt par “atklātajiem” drošības riskiem (17. pants) (skatīt arī 35. piezīmi), bet VDAR satur paziņojumu par datu aizsardzības pārkāpumiem (33. un 34. pants);
- (ii) ierosinātajā regulā ir minēts, ka DAIN veikšana un apspriešanās ar uzraudzības iestādi saskaņā ar VDAR ir obligāta noteiktos apstākļos (17. un 19. apsvērums un 6. panta 3. punkta b) apakšpunkts), savukārt VDAR jau nosaka, kad DAIN ir jāveic un ir nepieciešama apspriešanās (35. un 36. pants), un;
- (iii) nav skaidri noteikts, ka, nodrošinot atbilstību nosacījumiem apstrādes aizlieguma izņēmumam saskaņā ar ierosinātās regulas 5. pantu, joprojām ir jāievēro visi attiecīgie pienākumi saskaņā ar VDAR, ja tas attiecas uz personas datu apstrādi, un jebkura cita apstrāde saskaņā ar VDAR ir aizliegta. Jāprecizē, ka VDAR 6. panta 4. punktā noteiktā atbilstības pārbaude līdz ar to nav piemērojama;
- (iv) ierosinātajā E-privātuma regulā nav paredzēti sertifikācijas mehānismi līdzīgi VDAR 42. un 43. pantā paredzētajiem. Tā kā VDAR 42. panta darbības joma stingri attiecas tikai uz datu aizsardzības sertifikācijas mehānismu un datu aizsardzības zīmogu un zīmju izveidi, lai parādītu atbilstību VDAR, jāapsver, vai nevajadzētu ieviest salīdzināmu noteikumu, nodrošinot apstrādes darbību, standartu, produktu vai pakalpojumu sertifikāciju, lai ievērotu E-privātuma regulas nosacījumus.

Lai nodrošinātu, ka šis skaidrības trūkums netiek izmantots kā arguments, lai samazinātu aizsardzības līmeni saskaņā ar ierosināto regulu, būtu skaidri jānosaka, ka visos šajos gadījumos arī datu apstrādātājiem ir jāievēro VDAR.

47. Turklāt būtu jāprecizē, ka **prasība par piekrišanas atsaukšanu attiecas arī uz galiekārtu traucējumiem**. Ierosinātās regulas 8. panta 1. punkta b) apakšpunkts paredz iespēju iejaukties galalietotāju galiekārtās ar to piekrišanu. 9. panta 3. punktā noteikts, ka galalietotājiem jebkurā laikā ir jādod iespēja atsaukt savu piekrišanu, bet tas attiecas tikai uz piekrišanu metadatu un satura analīzei. Būtu jāprecizē, ka šis pienākums attiecas arī uz iejaukšanos galiekārtās.
48. Saistībā ar to būtu jāprecizē, ka **atgādinājums par iespēju atsaukt piekrišanu attiecas arī uz piekrišanu, izmantojot pārlūka iestatījumus**. 9. panta 3. punkta nosacījumi pieprasa, lai galalietotājiem periodiski, ik pēc sešiem mēnešiem tiktu atgādināts par iespēju atsaukt savu piekrišanu jebkurā laikā. Lai gan darba grupa uzskata, ka vispārīgie pārlūkprogrammu un citas programmatūras iestatījumi, tostarp operētājsistēmas, lietotnes un programmatūras saskarnes ar lietu internetu savienotām ierīcēm (t. i., nevis, pamatojoties uz īpašām granulārām pārbaudēm), nevar būt pamatojums, lai sniegtu piekrišanu, jo vispārējie iestatījumi nav piemēroti, lai sniegtu konkrētu piekrišanu konkrētiem scenārijiem (skatīt 24. piezīmi), noklusējuma iestatījumiem jābūt lietotājam draudzīgiem (skatīt 19. piezīmi). Ja ierosinātajā regulā tiek saglabāts šis nosacījums, tad iestatījumiem jābūt pietiekami precīziem, lai kontrolētu visu datu apstrādi, kurai lietotājs piekrīt, un jāaptver visas iekārtas funkciju iespējas, kas var izraisīt datu apstrādi. Turklāt galalietotājam vismaz periodiski (no sešiem mēnešiem) būtu jāatgādina par iespēju mainīt šos iestatījumus.

49. Ir atzinīgi vērtējams, ka saskaņā ar ierosināto regulu programmatūrai, kas jau ir laista tirgū, ir jāinformē galalietotājs par tā konfidencialitātes iestatījumiem (10. pants). **Tomēr nav skaidrs, kā to var efektīvi piemērot mantotajiem produktiem un citiem produktiem**, kuriem vairs netiek nodrošināts atbalsts. Turklāt būtu jāprecizē, kā šis pienākums attieksies uz atvērtā koda programmatūru, kas tiek izstrādāta atklātā un decentralizētā veidā.
50. Būtu jāprecizē, ka **piedāvātā iespēja bloķēt (trešo personu) sīkdatnes saskaņā ar ierosinātās regulas 10. pantu ir prioritāra, salīdzinot ar 8. panta 1. punkta d) apakšpunktā paredzēto tīmekļa auditorijas mērījumu izņēmumu**. Vai, citiem vārdiem sakot: kaut arī vietnē var izmantot analītiskus tīmekļa auditorijai, kas tiek mērīta saskaņā ar 8. panta 1. punkta d) apakšpunktu, lietotājiem joprojām vajadzētu būt tiesībām bloķēt šīs izsekošanas tehnoloģijas savā pārlūkprogrammā.
51. **Būtu jāprecizē (pus-) automātisko izsaukumu un sakaru sistēmu definīcijas**. Šī termina definīcijā ierosinātās regulas 4. panta 3. punkta h) apakšpunktā ir ietverta atsauce uz pašu terminu teikuma otrajā daļā (“tostarp izsaukumus, ko veic automatizētā izsaukšanas un saziņas sistēma, kas izsaukto personu savieno ar citu personu”). Tiek ierosināts dzēst šo pēdējo teikumu no definīcijas un mainīt definīciju 4. panta 3. punkta g) apakšpunktā, iekļaujot izsaukumus, kas veikti, izmantojot daļēji automatizētas sakaru sistēmas, piemēram, automātiskās zvanītājprogrammas, kas savieno izsaukto personu ar individu.
52. **Būtu jāprecizē informācija, kas ir “pakalpojuma abonēšanas daļa”**. 14. apsvērumā ir minēts, ka elektronisko sakaru metadati “var ietvert informāciju, kura sniegta saistībā ar pakalpojuma abonēšanu, ja šādu informāciju apstrādā nolūkā to pārraidīt, izplatīt vai veikt elektronisko sakaru satura apmaiņu”. Nav skaidrs, kas ir domāts ar šo formulējumu.
53. Būtu jāprecizē **atbilstības un sadarbības mehānismu piemērojamība**. 38. apsvērumā ir atzīmēts, ka ierosinātā regula balstīta VDAR saskaņošanas mehānismā. Turklāt 18. panta 1. punkts paredz, ka VDAR VI un VII nodaļu piemēro *mutatis mutandis*. 19. pantā ir arī atzīmēts, ka Eiropas Datu aizsardzības kolēģija (EDAK) pilda VDAR 70. pantā noteiktos uzdevumus. Lai gan šo noteikumu piemērošana ir salīdzinoši skaidra, nevar izslēgt, ka radīsies interpretācijas jautājumi saistībā ar pamatnostādnēm par saskaņotību un sadarbības mehānismiem VDAR ietvaros. Piemēram, vadošās iestādes mehānisms tiek piemērots gadījumos, kad notiek “pārrobežu apstrāde” (VDAR 56. panta 1. punkts): nav skaidrs, kā tas piemērojams galiekārtu traucējumiem vai satura vai metadatu analīzei saskaņā ar ierosināto regulu. Tādēļ ir ieteicams precizēt šo galveno jēdzienu piemērošanu apsvērumā un uzsvērt, ka visi atlikušie jautājumi par šo VDAR nodaļu piemērojamību ierosinātās regulas kontekstā tiks atrisināti, interpretējot šo nodaļu noteikumus saskaņā ar to nodomu. Turklāt ir ieteicams paskaidrot, ka 70. pants EDAK ir piemērojams *mutatis mutandis* ierosinātās regulas kontekstā (tas šobrīd trūkst apsvērumā).

\* \* \*