



17/ET

WP 247

**Arvamus 01/2017
e-privaatsuse määruse (2002/58/EÜ) ettepaneku kohta**

Vastu võetud 4. aprillil 2017

Töörühm on asutatud direktiivi 95/46/EÜ artikli 29 alusel. Tegemist on Euroopa sõltumatu nõuandeorganiga andmekaitse ja eraelu puutumatuse küsimustes. Töörühma ülesandeid on kirjeldatud direktiivi 95/46/EÜ artiklis 30 ja direktiivi 2002/58/EÜ artiklis 15.

Sekretariaaditeenused tagab Euroopa Komisjoni õigus- ja tarbijaküsimuste peadirektoraadi direktoraat C (põhiõigused ja õigusriik), B-1049 Brüssel, Belgia, kabinet nr MO-59 05/035.

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

TÖÖRÜHM ÜKSIKISIKUTE KAITSEKS SEOSIS ISIKUANDMETE TÖÖTLEMISEGA,

mis on asutatud Euroopa Parlamendi ja nõukogu 24. oktoobri 1995. aasta direktiiviga 95/46/EÜ,

võttes arvesse nimetatud direktiivi artikleid 29 ja 30,

võttes arvesse oma kodukorda,

ON VASTU VÕTNUD KÄESOLEVA ARVAMUSE:

KOKKUVÕTE

Töörühm väljendab heameelt Euroopa Komisjoni 10. jaanuaril 2017. aastal esitatud e-privaatsuse määruse ettepaneku üle. Töörühm kiidab heaks asjaolu, et reguleerimisvahendiks **valiti määrus**. See tagab ühtsed eeskirjad kogu ELis ja annab selgust nii järelevalveasutustele kui ka organisatsioonidele. Samuti aitab see tagada järjepidevuse isikuandmete kaitse üldmäärusega. Seda järjepidevust toetab omalt poolt otsus määrata e-privaatsuse eeskirjade täitmisele pööramise eest vastutajaks **sama asutus, kes vastutab isikuandmete kaitse üldmääruse järgimise järelevalve eest**.

Samal ajal on positiivne, et otsustati **täiendava õigusakti** (säilitamise) kasuks. Konfidentsiaalse teabevahetuse ja lõppseadmete kaitsmisel on spetsiifilised eripärad, mida isikuandmete kaitse üldmäärus ei käsitle. Seetõttu on vaja selliste teenuste kohta lisaetteid, mis tagaksid eraelu puutumatuse põhiõiguse ja teabevahetuse konfidentsiaalsuse, sealhulgas lõppseadmete konfidentsiaalsuse piisava kaitse. Sellega seoses toetab töörühm määruse ettepanekus valitud **põhimõttelist lähenemist laiade keeldude ja kitsaste erandite kohta ning nõusoleku mõiste sihipärasest rakendamist**.

Töörühm kiidab heaks määruse ettepaneku kohaldamisala laiendamise nii, et see hõlmab ka **OTT-teenuste osutajaid** – need teenused on funktsionaalsuse poolest samaväärsed traditsioonilisemate suhtlusvahenditega ning võivad seetõttu samamoodi mõjutada ELi kodanike eraelu ja õigust teabevahetuse konfidentsiaalsusele. Samuti on positiivne, et määruse ettepanek käsitleb selgelt **sisu ja seotud metaandmeid** ning tunnistab, et **metaandmed võivad paljastada väga tundlikke andmeid**.

Siiski toob töörühm välja neli **äärmiselt murettekitavat punkti**. **Lõppseadme asukoha jälgimise, sisu ja metaandmete analüüsi lubatavuse tingimuste, lõppseadmete ja tarkvara vaikeseadete ning jälitusmüüride** valdkonnas langetaks määruse ettepanek isikuandmete kaitse üldmääruses pakutava kaitse taset. Oma arvamuses esitab töörühm konkreetseid ettepanekuid eesmärgiga tagada, et e-privaatsuse määrus tagaks samaväärse või kõrgema tasemega kaitse, mis vastab sideandmete (nii sisu kui ka metaandmete) tundlikule iseloomule.

Mis puudutab **kohtvõrgus jälgimist**, siis olenevalt asjaoludest ja andmete kogumise eesmärkidest nõuab selline jälgimine isikuandmete kaitse üldmääruse kohaselt tõenäoliselt nõusolekut või on lubatud üksnes juhul, kui kogutavad isikuandmed anonüümitakse. Viimasel juhul tuleb täita järgmised neli tingimust: lõppseadme andmete kogumise eesmärk piirub üksnes statistilise loendusega; jälgimine on ajaliselt ja ruumiliselt piiratud rangelt selle eesmärgi saavutamiseks; pärast seda kustutatakse või anonüümitakse andmed viivitamata; olemas on toimivad võimalused andmete kogumisest keeldumiseks. Kutsume Euroopa Komisjoni üles toetama mobiilseadmete jaoks mõeldud tehnilise standardi kehtestamist, mis võimaldaks anda automaatselt märku sellisest jälgimisest keeldumisest.

Mis puudutab **sisu ja metaandmete analüüsi**, siis tuleks lähtuda sellest, et kui puudub kõigi lõppkasutajate (saatjate ja vastuvõtjate) nõusolek, on sideandmete töötlemine keelatud. Et teenuseosutajatel oleks võimalik osutada just neid teenuseid, mida kasutaja on sõnaselgelt soovinud, näiteks otsimis- ja indekseerimisfunktsioon või kõnesünteesiteenused, peaks

liikmesriik kehtestama erandi sisu ja metaandmete töötlemiseks üksnes kasutaja isiklikul eesmärgil.

Mis puudutab **nõusolekut jälgimiseks**, kutsub töörühm üles selgelt keelustama jälitusmüürid ehk võta-või-jäta-valikud, mis sunnivad kasutajad jälgimisega nõustuma, juhul kui nad soovivad teenusele juurdepääsu.

Viimaks soovib töörühm, et lõppseadmete ja tarkvara **vaikeseaded peavad kaitsma eraelu puutumatust** ning pakkuma kasutajatele selgeid võimalusi neid vaikeseadeid paigaldamise ajal kinnitada või muuta. Need seaded peavad kasutamise ajal olema hõlpsasti juurdepääsetavad. Kasutajatel peab olema võimalik anda brauseri seadete kaudu konkreetne märguanne nõusoleku kohta. Eraelu puutumatusega seotud eelistused ei tohiks piirduda kolmandate isikute sekkumise ega küpsistega. Töörühm soovib tungivalt muuta jälgimiskeelu (Do Not Track) standardi järgimise kohustuslikuks.

Samuti on töörühm leidnud muid murepunkte, mis on seotud näiteks kohaldamisala, lõppseadmete kaitsmise ja otseturundusega. Ühtlasi on töörühm esile tõstnud teemasid, mis vajaksid täpsustamist, et lõppkasutajaid paremini kaitsta ning pakkuda kõigile kaasatud sidusrühmadele suuremat õiguskindlust.

SISUKORD

1. SISSEJUHATUS.....	6
2. MÄÄRUSE ETTEPANEKU POSITIIVSED TAHUD	6
<i>Üleliiduline ühtlustamine, trahvide vastavusse viimine ja andmekaitseasutustele täitmisele pööramise ainuõiguse andmine</i>	<i>6</i>
<i>Kohaldamisala laiendamine võrreldes e-privaatsuse direktiiviga.....</i>	<i>8</i>
<i>Nõusoleku mõiste sihipärane kohaldamine.....</i>	<i>10</i>
3. TÕSISED MUREPUNKTID.....	10
<i>Määruse ettepanek kahjustab isikuandmete kaitse üldmäärusest tulenevat kaitset</i>	<i>10</i>
4. MUUD MUREPUNKTID	16
<i>Territoriaalset ja materiaaloiguslikku kohaldamisala tuleb laiendada.....</i>	<i>16</i>
<i>Lõppseadmete kaitset tuleb tugevdada</i>	<i>17</i>
<i>Otseturundus.....</i>	<i>21</i>
<i>Ajakava</i>	<i>23</i>
<i>Muud mured.....</i>	<i>23</i>
5. TÄPSUSTAMISETTEPANEKUD ÕIGUSKINDLUSE TAGAMISEKS	26
<i>Täpsustused seoses kohaldamisalaga</i>	<i>26</i>
<i>Täpsustused seoses nõusoleku mõiste ja kohaldamisega.....</i>	<i>29</i>
<i>Täpsustused seoses asukoha ja muude metaandmetega</i>	<i>30</i>
<i>Täpsustused seoses mittetellitud teadaannetega.....</i>	<i>31</i>
<i>Selgitused põhiõigusi käsitlevate õigusaktide kohaldamise kohta.....</i>	<i>33</i>
<i>Muud täpsustused</i>	<i>33</i>

1. SISSEJUHATUS

1. Artikli 29 alusel asutatud andmekaitse töörühm (edaspidi: töörühm või artikli 29 töörühm) väljendab heameelt Euroopa Komisjoni e-privaatsuse määruse ettepaneku üle (edaspidi: määruse ettepanek või e-privaatsuse määrus)¹, millega soovitakse asendada e-privaatsuse direktiiv².
2. Paljud selle määruse ettepaneku tahud on kiiduväärt ja Euroopa Komisjon on määruse ettepaneku esitamise astunud olulise sammu edasi. Siiski on määruse ettepanekut võimalik veelgi paremaks muuta. See võimaldaks nii lõppkasutajaid paremini kaitsta kui ka kõigile kaasatud sidusrühmadele rohkem õiguskindlust pakkuda.
3. Seetõttu toob töörühm välja mitu murepunkti ja täpsustamissoovitust, mida Euroopa Parlament ja ministrite nõukogu peaksid oma arutelus määruse ettepaneku üle käsitlema. Oma arvamuses käsitleme esmalt määruse ettepaneku positiivseid tahke ning seejärel tõstame esile murepunktid ja täpsustamist vajavad kohad.

2. MÄÄRUSE ETTEPANEKU POSITIIVSED TAHUD

ÜLELIIDULINE ÜHTLUSTAMINE, TRAHVIDE VASTAVUSSE VIIMINE JA ANDMEKAITSEASUTUSTELE TÄITMISELE PÕÖRAMISE AINUÕIGUSE ANDMINE

4. Töörühm kiidab heaks asjaolu, et reguleerimisvahendiks **valiti määrus**. See tagab eeskirjade ühtsuse kogu ELis (teatavate eranditega, mida käsitletakse allpool). Samuti annab see selgust nii järelevalveasutustele kui ka organisatsioonidele. Arvestades isikuandmete kaitse üldmääruse³ kesket rolli määruse ettepanekus, aitab see ühtlasi tagada mõlema instrumendi järjepidevuse. Samal ajal on positiivne, et otsustati **täiendava õigusakti (säilitamise)** kasuks. Konfidentsiaalse teabevahetuse ja lõppseadmete kaitsmisel on spetsiifilised eripärad, mida isikuandmete kaitse üldmäärus ei käsitle. Seetõttu on vaja selliste teenuste kohta lisaettepanekuid, mis tagaksid selle põhiõiguse piisava kaitse. Selles kontekstis toetab töörühm ka määruse ettepanekus valitud **põhimõttelist lähenemist, et keelud peaksid olema laiad ja erandid kitsad**, ning usub, et vältida tuleks piiritlemata erandite kehtestamist

¹ Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus), 2017/0003 (COD), veebiaadress: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

² Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (EÜT L 201, 31.7.2002, lk 37–47), veebiaadress: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:32002L0058>.

³ Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus) (ELT L 119/1, 4.5.2016, lk 1–88, veebiaadress: <http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679>).

isikuandmete kaitse üldmääruse artikli 6, eriti artikli 6 lõike f (tuginemine õigustatud huvile) eeskujul.

5. Asjaolu, et **neid eeskirju jõustab sama ametiasutus, kes vastutab isikuandmete kaitse üldmääruse järgimise järelevalve eest**, toetab nende kahe instrumendi omavahelist järjepidevust veelgi. Arvestades isikuandmete kaitse ning konfidentsiaalse teabevahetuse ja lõppseadmete kaitse omavahelist seost, tuleb kasuks, et määruse ettepaneku sätete jõustamine usaldatakse samale järelevalveasutusele, kes jõustab ka isikuandmete kaitse üldmäärust (määruse ettepaneku põhjendus 38 ja artikkel 18). Samuti kinnitab Euroopa Liidu Kohtu praktika⁴, et järelevalveasutus peab kindlasti olema sõltumatu, nagu on ette nähtud Euroopa Liidu põhiõiguste harta artiklis 7. Praktilisel tasandil aga tooks see andmekaitseasutustele olulisel määral lisatööd, kuid selle tegemine ei ole tagatud, kui eelarvet ei suurendata. Seetõttu kiidavad andmekaitseasutused heaks määruse ettepaneku põhjenduse 38, milles on esile tõstetud, et igale järelevalveasutusele tuleks tagada täiendavad rahalised vahendid ja töötajad, ruumid ja taristu, mis on vajalikud nende uuest määrusest tulenevate ülesannete tulemuslikuks täitmiseks. Samuti on kiiduväärt, et artikli 18 lõikes 2 on antud õiguslik alus koostööks määruse ettepanekus nimetatud järelevalveasutuste ja Euroopa elektroonilise side seadustiku direktiivi ettepanekus⁵ nimetatud riiklike reguleerivate asutuste vahel.
6. Arvestades määruse ettepaneku ja isikuandmete kaitse üldmääruse tihedat seost, kiidame heaks ka **määruse ettepaneku kohaselt määratavate trahvide ühtlustamist isikuandmete kaitse üldmäärusega**. Määruse ettepaneku kohaldamisalasse kuuluvad toimingud on üsnagi tundlikud, hõlmates muu hulgas kokkupuudet konfidentsiaalse side ja lõppseadmetega. Trahvide suurus peaks vastama sellele tundlikule kontekstile. Samuti on just see kontekst põhjus, miks on ühtlustamine kogu ELis oluline selleks, et tagada kogu piirkonnas ühesugune kõrge kaitstuse tase. Määruse ettepaneku artiklis 23 on sätestatud tõhusad trahvid määruse rikkumise eest, mis on samalaadsel tasemel nagu isikuandmete kaitse üldmääruse eeskirjade rikkumise eest kehtestatud trahvid, välja arvatud mõnes aspektis (vt märkus 38).
7. Samuti kiidame heaks sellest õigusaktist **konkreetsete andmete puutumatuse rikkumisest teavitamise põhimõtete kõrvalejätmise**, sest nii on välistatud tarbetu kattumine isikuandmete kaitse üldmääruses sätestatud andmete puutumatuse rikkumisega seotud nõuetega.
8. Ühtlasi on **kiiduväärt, et tähelepanu on nüüd koondunud kõigile lõppkasutajatele võrdse kaitstuse taseme tagamisele**, sest määruse ettepanekus on lõpetatud „abonentide“ ja teiste elektrooniliste sideteenuste kasutajate eristamine.

⁴ Vt näiteks kohtuotsus, Euroopa Kohus, 6.10.2015, C-362/14 (Safe Harbour), punkt 41 ja kohtuotsus, Euroopa Kohus, 21.12.2016, C-203/15 ja C-698/15 (Tele2/Watson), punkt 123.

⁵ Ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, millega luuakse Euroopa elektroonilise side seadustik (uuesti sõnastatud), 2016/0288 (COD), 12.10.2016, veebiaadress: http://eur-lex.europa.eu/legal-content/ET/ALL/?uri=omnat:COM_2016_0590_FIN.

9. Töörühm kiidab heaks **määruse ettepaneku kohaldamisala laiendamise ka OTT-teenuste osutajatele** – need teenused on funktsionaalselt samaväärsed traditsioonilisemate suhtlusvahenditega ning võivad seetõttu samamoodi mõjutada ELi kodanike eraelu ja õigust teabevahetuse konfidentsiaalsusele. Eelkõige tunnustab töörühm asjaolu, et kõik OTT-teenuste kategooriad (OTT0, OTT1 ja mõned OTT2-teenused)⁶ kuuluvad nüüd määruse kohaldamisalasse, kuna see ei hõlma mitte üksnes traditsioonilisi suhtlusvahendeid (OTT0), vaid ka funktsionaalselt samaväärseid teenuseid (OTT1), nagu on nimetatud määruse ettepaneku artikli 8 lõike 1 punktis c. Samuti on positiivne, et peale Euroopa elektroonilise side seadustikus toodud määratluste on sisse arvatud ka mõned OTT2-teenused, mis võimaldavad kõrvalteenusena isikutevahelist interaktiivset suhtlust, mis on nende teenusega olemuslikult seotud, näiteks mängudes, kohtingurakendustes või arvustussaitidel (määruse ettepaneku artikli 4 lõige 2). Samamoodi avaldame poolehoidu **täpsustusele, et kaitse hõlmab ka masinatevahelist suhtlust**. Põhjenduses 12 on selgeks tehtud, et üksteisega sidet pidavad seadmed kuuluvad määruse ettepanekus pakutava kaitse kohaldamisalasse. See on soovitatav, kuna selline side sisaldab sageli teavet, mida kaitstakse eraelu puutumatusega seotud õigusega. Siiski võiks kohaldatavust täpsustada (vt märkus 40h).
10. Samuti on positiivne, et määruse ettepanekus käsitletakse selgelt **sisu ja seotud metaandmeid**. Põhjenduses 14 on selgelt välja toodud, et artikli 4 lõike 3 punktis a esitatud „elektroonilise side andmete“ määratlus peaks olema piisavalt lai, et see hõlmaks *kogu* sisu ja kõiki seotud metaandmeid, olenemata näiteks sellest, milline on signaalide edastamise viis. Siiski toob töörühm märkuses 39 murepunktina välja asjaolu, et praegune „elektroonilise side andmete“ määratlus on ikka veel vaieldav. Kooskõlas kohaldamisala sellise laiendamisega peab töörühm **selle asjaolu tunnustamist, et metaandmed võivad avaldada väga tundlikku teavet** (vt seletuskirja punkt 2.2 ja põhjendus 2), oluliseks täienduseks. Töörühm kiidab heaks asjaolu, et seeläbi inkorporeerib Euroopa Komisjon Euroopa Liidu Kohtu kaalutlused kohtuotsustes Digital Rights Ireland ja Tele2/Watson. Samuti avaldab artikli 29 töörühm tunnustust sellele, et on **teadvustatud asjaolu, et sisu analüüsimine on suure riskitasemega töötlemine**. Põhjenduses 19 ja artikli 6 lõike 3 punktis b on sätestatud loogiline õiguslik eeldus, et sisu skannimine on suurt ohtu tekitav isikuandmete töötlemine isikuandmete kaitse üldmääruse artikli 35 alusel ning nõuab ilmselt olenemata sellest, kas kõrge jääkrisk esineb või mitte, alati eelnevat konsulteerimist (juhtiva) andmekaitseasutusega. Samal ajal tunneb töörühm muret mõiste „metaandmed“ ulatuse pärast ja asjaolu pärast, et metaandmete analüüsile ei kohaldata samasugust kohustuslikku andmekaitsealase mõjuhinnangu tegemise nõuet (vt märkused 33 ja 46).

⁶ Nende terminite täpsemat selgitust vt BEREC, *Report on OTT Services*, BoR (16) 35, 29. jaanuar 2016, lk 15 ja 16, veebiaadress: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. Palun pöörake tähelepanu ka aruandes olevale kommentaarile, et need kategooriad on mõeldud mõistetena, mida saaks kasutada raamistiku läbivaatamist puudutavas arutelus, mitte õigusmõistetena.

11. Samuti on kiiduväärt see, et endiselt **tunnistatakse anonüümimise tähtsust**. Juba e-privatsuse direktiivis oli anonüümimismeetmel oluline roll ühilduvuse tagamisel (vt näiteks e-privatsuse direktiivi artikli 6 lõiget 1, milles on sätestatud, et liiklusandmed tuleb kustutada või muuta anonüümseks, kui neid ei ole enam vaja side edastamiseks). Määruse ettepaneku artikli 6 lõike 2 punktis c ja artikli 6 lõike 3 punktis b on nõusoleku andmise korral lubatud teha erand metaandmete ja sisu töötlemise keelule, tingimusel et kõnealust eesmärki või kõnealuseid eesmärke „ei saa saavutada anonüümitud teabe töötlemisega“. Selliste eraelu puutumatust kaitsvate meetmete nõudmine lisaks kasutajate nõusoleku küsimisele kaitseb kasutajaid soovimatu isikuandmete töötlemise eest. Siiski on töörühmal samal ajal suur mure, et selliste anonüümimisvahendite kasutuselevõtt ei tohiks olla nõutav juhul, kui kasutajate asukohta jälgitakse nende mobiilseadmete vahendusel (vt märkus 17). Samuti peaksid teenuseosutajad alati, isegi anonüümimismeetmete võtmise korral, tegema andmekaitsealase mõjuhinnangu (vt märkused 33 ja 46) ning töörühm kutsub üles kehtestama lisakohustuse avalikustada andmete anonüümimise ja koondamise viis (vt märkus 42b).
12. Veel üks positiivne aspekt on **lõppseadmete kaitse lai sõnastus**. Põhjenduses 20 ja artiklis 8 on määratletud, et lõppseadmetele juurde pääsemiseks kasutatav tehnoloogia ei ole oluline: igasugune lõppseadet puudutav sekkumine, sealhulgas selle töötlemisfunktsiooni kasutamine, nõuab lõppkasutaja nõusolekut (teatavate eranditega). EK on nüüd abivalmilt kinnitanud, et selle sätte alla kuulub ka seadmetuvastus. Samuti kiidab töörühm heaks, et kui kolmas isik ei järgi isiku **brauseri seadetes väljendatud eelistusi, on need jõustatavad**, nagu kirjeldatakse põhjenduses 22. Sellest on kasu sellistes olukordades, kus kolmas isik (näiteks mõni reklaamivõrgustik) neid seadeid ei arvesta. Siiski peaks see olema sätestatud ka mõnes määruse ettepaneku asjaomases sättes.
13. Viimaks avaldame poolehoidu sellele, et **juriidilised isikud kuuluvad endiselt määruse ettepaneku kohaldamisalasse** (vt seletuskirja punkt 2.2; põhjendused 3, 33 ja 42; artiklid 1 ja 15 ning artikli 16 lõige 5). See oli nii juba e-privatsuse direktiivi puhul, kuid et andmekaitseasutused saavad ülesande uusi eeskirju jõustada, on kasulik seda spetsiaalselt rõhutada. See võimaldab andmekaitseasutustel võtta meetmeid olukorras, kus rikkumise ohvriks satuvad juriidilised isikud, näiteks juhul, kui ettevõtetele saadetakse rämpsposti või kui nende suhtlust salaja jälgitakse. Siiski toob töörühm murepunktidena välja, et nõusoleku kohaldamine juriidilistele isikutele ei ole selge (vt märkus 41a), samuti ei ole selge, mida mõeldakse juriidiliste isikute „õigustatud huvi“ all otseturunduse korral (vt märkus 43c).

14. Töörühm kiidab heaks uut liiki täiendused, mis on seotud nõusoleku mõiste kohaldamise ja tõlgendamisega. Kõigepealt on kiiduväärt **täpsustus, et internetiühendus ja (mobiil)telefoniside on hädavajalikud teenused ning nende teenuste osutajad ei tohi oma kliente sundida andma oma nõusolekut selliseks isikuandmete töötlemiseks, mis ei ole hädavajaliku teenuse enda osutamiseks vajalik**. Eriti just põhjenduses 18 on märgitud, et lairibaühenduse ja kõneside baasteenuseid tuleb käsitada hädavajalike teenustena, mis arvestades inimeste sõltumist ligipääsust neile teenustele tähendab seda, et nõusolek sideandmete töötlemiseks nimetatud lisaeesmärkidel (nt töötlemiseks reklaami või turunduse eesmärgil) ei saa olla kehtiv. Samas on töörühm mures, et see täpsustus on liiga kitsas. Ka teatavaid OTT-teenuseid võib käsitada hädavajalike teenustena ning e-privatsuse määruses tuleks sõnaselgelt keelata võta-või-jäta-valikud ka teistes olukordades (vt märkus 20).
15. Samuti on positiivne, et **ühtlustatakse nõue saada nõusolek füüsiliste isikute isikuandmete lisamiseks kataloogidesse**. Määruse ettepaneku artikli 15 kohaselt on andmete töötlemine üldkasutatavates kataloogides lubatud üksnes füüsiliste isikute nõusoleku korral ja juriidilistele isikutele tuleb anda võimalus keelduda. Seda on veelgi täpsustatud põhjenduses 31, kus on öeldud, et selles nõusolekus peaks olema konkreetselt märgitud, millise kategooria isikuandmed kataloogi lisatakse. Siiski toob töörühm murepunktina välja, et määruse ettepanekus võiks olla selgemalt väljendatud, et otsingu ja pöördotsingu jaoks on vaja konkreetset eraldiseisvat nõusolekut (vt märkus 37).
16. Samuti avaldatakse tunnustust asjaolule, et **kehtestatud on uus sihipärane erand lõppseadmetega seotud mittepealetükkivale sekkumisele**. Artikli 29 töörühma arvates tuleb kasuks määruse ettepanekus esitatud selgitus, et keeldu ei kohaldata veebiliikluse mõõtmisele (selle kitsa erandiga, et kõnealust mõõtmist teostab lõppkasutaja soovitud infoühiskonna teenuse osutaja, vt määruse ettepaneku artikli 8 lõike 1 punkt d). Vt täpsemalt põhjendus 21. Töörühm soovib siiski kasutada tehnoloogia suhtes neutraalsemat määratlust ja täpsustada selle erandi kohaldatavust (vt märkus 25).

3. TÕSISED MUREPUNKTID

MÄÄRUSE ETTEPANEK KAHJUSTAB ISIKUANDMETE KAITSE ÜLDMÄÄRUSEST TULENEVAT KAITSET

Nagu eespool nimetatud, on määruse ettepanekus palju olulisi edasiminekuid. Kuid samuti on selles eri raskusastmega murepunkte. Selles jaotises käsitleb töörühm nelja teemat, mille pärast ta on **sügavalt mures**. Need on sätted, mis **kahjustavad isikuandmete kaitse üldmäärusest tulenevat kaitset**.

17. **Määruses sätestatud kohustus seoses lõppseadmete asukoha jälgimisega peaks vastama isikuandmete kaitse üldmääruses sätestatud nõuetele.** Määruse ettepaneku artikli 8 lõike 2 punktis b on nõutud üksnes selge teabe kuvamist ja turvameetmete võtmist selleks, et koguda lõppseadmelt eetrisse antavat teavet. Samuti on artikli 8 lõike 2 punktis b märgitud, et kogumise eest vastutav isik peab andma teavet mis tahes meetmete kohta, mida lõppkasutaja saab teabe kogumise peatamiseks või minimeerimiseks võtta. Sellega jäetakse artikli 8 lõike 2 punktis b mulje, et organisatsioonid võivad isikute füüsilise liikumise jälgimiseks koguda lõppseadmelt eetrisse antavat teavet (näiteks kohtvõrgus või Bluetoothi abil jälgimine) ilma asjaomase isiku nõusolekuta. Tundub, et andmeid koguv isik võib määrust järgida sellega, et ta teavitab kasutajaid, et kui nad ei soovi lasta end jälgida, tuleb neil oma seadmed välja lülitada. Selline lähenemine läheks vastuollu Euroopa Komisjoni telekommunikatsioonipõhimõtetega, mille kohaselt kõigile Euroopa kodanikele pakutakse kiiret ja piiriülest mobiilse interneti ühendust tugevate eraelu puutumatus
- kaitse
- põhimõtte
- alusel.

Samuti ei ole määruse ettepanekus kehtestatud ühtegi selget piirangut andmete kogumisele või sellele järgnevate töötlemistoimingute ulatusele. Sellega seoses tuleb mainida, et MAC-aadressid on isikuandmed isegi pärast turvameetmete võtmist, näiteks räsimit. Kuna määruse ettepanekus ei kehtestata muid nõudeid ega piiranguid, on nende isikuandmete kaitstuse tase määruse ettepaneku alusel oluliselt madalam kui isikuandmete kaitse üldmääruse alusel, milles on nõutud, et selline jälgimine peab olema õiglane, seaduslik ja läbipaistev. Samuti on põhjenduses 25 tarbetult märgitud, et mõned kohtvõrgus jälgimise funktsioonid ei tekita suuri privaatsusega seotud riske, teised aga küll (näiteks üksikisikute jälgimine pikema aja jooksul). Ehkki töörühm kiidab heaks teadvustamise, et viimase variandi puhul tekivad suured eraelu puutumatusse seotud riskid, ei tasu juba ennetavalt ilma asjaolude ja töötlemise proportsionaalsust süvitsi hindamata otsustada, et mõne teise funktsiooni puhul neid ei esine. Mitteenonüümitud kohtvõrgus jälgimise kohta tuleks selline hindamine teha, võttes arvesse järgmisi tingimusi.

Olenevalt andmete kogumise asjaoludest ja eesmärkidest nõuab jälgimine isikuandmete kaitse üldmääruse kohaselt tõenäoliselt kas nõusolekut või on lubatud üksnes juhul, kui kogutavad isikuandmed anonüümitakse. Anonüümimist soovitatakse teha vahetult pärast andmete kogumist. Kui vahetu anonüümimine ei ole andmete kogumise eesmärgi arvestades võimalik, saab andmeid töödelda perioodil, mil need ei ole anonüümitud, üksnes järgmiste tingimuste korral: i) isikuandmete kogumise eesmärk peab piirduma üksnes statistilise loendusega (vt alltoodud näited), ii) jälgimine on ajaliselt ja ruumiliselt piiratud selle eesmärgi saavutamiseks hädavajaliku jälgimisega, iii) pärast seda kustutatakse või anonüümitakse andmed viivitamata ning iv) isikul peab olema võimalus andmete kogumisest keelduda. Kõigil asjaoludel peavad vastutavad töötajad loomulikult järgima nõuet esitada piisavat teavet.

Töörühm on mures selle pärast, et kui pakutakse võimalust keelduda andmete kogumisest iga andmeid koguva organisatsiooni kohta eraldi, kujutaks see endast inimestele vastuvõetamatut kohustust, arvestades seda, et nii era- kui ka avaliku sektori organisatsioonid kasutavad selliseid jälgimismeetodeid järjest rohkem.

Seetõttu kutsub töörühm Euroopa seadusandjat üles edendama tehniliste standardite väljatöötamist, et seadmed saaksid automaatselt anda märku jälgimisega mittenõustumisest, ning tagama, et selliste märguannete järgimine on jõustatav.

Näiteks oleks isikuandmete kaitse üldmääruse alusel nõusolekut vaja juhul, kui andmete vastutav töötleja kogub ja salvestab seadmete kaudselt tuvastatavaid (kohtvõrgu või Bluetoothi) MAC-aadresse ning arvutab kasutaja asukoha välja eesmärgiga jälgida kasutaja asukohta pikema aja jooksul, näiteks eri kauplustes. See olukord esineb eelkõige juhul, kui selline jälgimine toimub avalikes kohtades, kus kasutajatel on õiguspärane ootus, et neid ei tuvastataks ega jälgitaks, ent kus sellest hoolimata kogutakse möödujate MAC-aadresse. Seda nõusolekut võib küsida näiteks rakenduse abil, mis kutsub kasutajaid üles lubama oma asukoha jälgimist mingis konkreetses piirkonnas reklaampakkumiste saamiseks, või võimaldades mingites konkreetses paikades registreerimispunktide kasutamist või traadita interneti pääsupunktides nõusolekumooduli abil.

Andmete vastutavatel töötlejatel võiks lõppseadmelt eetrisse antavat teavet olla lubatud koguda füüsilise liikumise jälgimiseks ilma asjaomase üksikisiku nõusolekuta üksnes piiratud juhtudel. Näiteks võiks sellega tegemist olla siis, kui loendatakse mingis konkreetses kohas viibivaid kliente või kogutakse turvakontrollipunkti kummaski otsas eetrisse antavat teavet eesmärgiga näidata ooteaega. Siiski tuleb need andmed mõlemal juhul kustutada või anonüümida niipea, kui statistiline eesmärk on täidetud. See tähendab, et konkreetses paigas, näiteks poes olevate külastajate seadmete MAC-aadressid tuleb anonüümida vahetult pärast nende kogumist ilma neid püsivalt salvestamata ning viisil, mis tehniliselt välistab nende uuesti tuvastatavuse. Ooteaja arvutamise puhul tuleb MAC-aadressid kustutada või anonüümida niipea, kui need andmed ei ole enam ooteaja arvutamiseks vajalikud (nt seetõttu, et külastaja on läbinud turvakontrolli, või seetõttu, et ta on järjekorrast lahkunud).

Samuti peab andmete vastutav töötleja järgima andmete minimeerimise nõudeid (näiteks hoiduma pidevast jälgimisest, kui eesmärk piirdub jälgimisega poe lahtiolekuajal ja/või valimi moodustamisega regulaarsete ajavahemike tagant). Samuti peavad vastutavad töötlejad võtma muid leevendusmeetmeid tagamaks, et kasutajate õigust eraelu puutumatusele ei mõjutataks või et see mõju oleks minimaalne, näiteks kaitsma andmekogumispunkti kõrval elavate inimeste eraelu puutumatust.

Määruse ettepaneku artikli 8 lõikes 2 valitud lahendus, mille kohaselt piisab üksnes teabe kuvamisest, on seda märkimisväärselt, et põhjenduses 20 on esitatud järeldus, et lõppkasutaja seadmega seotud teavet võidakse tuvastamise ja jälgimise jaoks koguda kasutaja teadmata ka kaugmeetodil ning määruse ettepaneku kohaselt võib selline töötlemine raskelt rikkuda nende lõppkasutajate privaatsust. Peale selle ei ole see kohustus suurem kui teavitamiskohustus, mis on isikuandmete kaitse üldmääruse artiklites 13 ja 14 juba ette nähtud. Jälgimisega kaasnevat rasket eraelu puutumatuse rikkumist suurendab veelgi kolmandate isikute võimalik juurdepääs kogutud andmetele, näiteks õiguskaitseasutuste võimalus tuvastada lõppkasutajaid nende mobiilseadmete eetrisse antud ja salvestatud MAC-aadressi(de) põhjal.

18. Täpsustada tuleb sisu ja metaandmete analüüsi lubatavuse tingimusi.

Määruse ettepaneku artiklis 6 on metaandmetele ja sisule antud erinev kaitstuse tase. Artikli 29 tööühm sellist eristamist ei toeta: mõlemad andmete kategooriad on väga tundlikud. Seetõttu tuleb metaandmetele ja sisule määrata ühesugune kõrge kaitstuse tase. Lähtuda tuleks sellest, et nii metaandmete kui ka sisu töötlemine on keelatud, kui puudub kõigi lõppkasutajate (st saatja ja saaja) nõusolek.

Olenevalt eesmärgist võib mingit laadi isikuandmete töötlemine olla siiski lubatud ilma nõusolekuta, kui see on nimetatud eesmärgiks hädavajalik.

- Teenuseosutajad võivad elektroonilise side andmeid töödelda eesmärkidel, mis on nimetatud määruse ettepaneku artikli 6 lõike 1 punktides a ja b ning lõike 2 punktides a ja b⁷.
- Tuleks täpsustada, et ka teatavaid rämpsposti tuvastamise/filtreerimise ja robotivõrkude toime piiramise tehnikaid võidakse käsitada hädavajalikuna elektroonilise side teenuste kuritarvitava kasutamise tuvastamiseks või peatamiseks (artikli 6 lõike 2 punkt b). Rämpsposti filtreerimisega seoses tuleks rämpsposti saavatele lõppkasutajatele pakkuda üksikasjalikke võimalusi rämpsposti saamisest keeldumiseks, kui see on tehniliselt võimalik.
- Tuleks täpsustada, et elektroonilise side andmete analüüs klienditeeninduse eesmärgil võib samuti kuuluda erandi „vajalik arveldamiseks“ alla (vt artikli 6 lõike 2 punkt b). Asjaomaseid metaandmeid võib säilitada kuni selle ajavahemiku lõpuni, mille vältel võib arve seaduslikult vaidlustada või riigi õiguse kohaselt nõuda selle tasumist. Asjaomaseid andmeid (näiteks veebiaadresse) võib säilitada üksnes lõppkasutaja taotlusel ja sellisel juhul vaid sellise ajavahemiku jooksul, mis on arvet puudutavate erimeelsuste lahendamiseks hädavajalik (mis tähendab, et artikli 7 lõiget 3 tuleks vastavalt muuta).
- Tuleks võimaldada elektroonilise side andmete töötlemist lõppkasutaja sõnaselgelt soovitud teenuste osutamise eesmärgil, milleks võivad olla näiteks otsimis- ja indekseerimisfunktsioon, virtuaalsed assistendid, kõnesünteesiteenused ning tõlketeenused. Selleks on vaja kehtestada erand selliste andmete analüüsimiseks üksnes individuaalsel (ühe majapidamisega seotud) kasutuseesmärgil, samuti individuaalsel tööga seotud kasutuseesmärgil⁸. See oleks seega võimalik ilma kõigi lõppkasutajate nõusolekuta, ent võib toimuda üksnes teenuse osutamist taotleva lõppkasutaja

⁷ Mis puudutab vajadust täita teenuse kvaliteedi kohustuslikke nõudeid, nagu on kirjeldatud artikli 6 lõike 2 punktis a, peaksid teenuseosutajad arvesse võtma tingimusi, mis on esitatud määruses (EL) 2015/2120 (rändlusteenuse määrus), eriti selle artiklis 3 ning põhjendustes 10 ja 13–15. Selle sätte alusel võidakse teenuseosutajatelt nõuda sideandmete töötlemist eesmärgiga tuvastada ning filtreerida paha- ja nuhkvara ning neile võidakse anda luba andmeid pakkida.

⁸ Ehkki määruse ettepaneku põhjenduses 13 on määruse kohaldamisalast sõnaselgelt välistatud ettevõttesised võrgud, peaks uus individuaalse kasutamise erand hõlmama ka töötajate tööks kasutatavaid pilveteenuseid, näiteks e-kirjade otsingut.

nõusolekul. Samuti ei võimaldaks selline konkreetne nõusolek teenuseosutajal neid andmeid kasutada eri eesmärkideks.

See tähendab, et sisu ja/või metaandmete analüüs kõigil muudel eesmärkidel, näiteks analüüsimine, profiilianalüüs, käitumispõhine reklaam või muud teenuseosutaja (äri)huve teenivad eesmärgid, nõuab nõusolekut kõigilt lõppkasutajatelt, kelle andmeid töödeldakse. Nimetatud olukordadega seoses peaks määruse ettepanekus olema selgitatud, et pelgalt e-kirja või muu teenuse kaudu isikliku sõnumi saatmine sellisele lõppkasutajale, kes on avaldanud nõusolekut oma sisu ja metaandmete töötlemiseks (näiteks e-postiteenuse lepingu sõlmimise käigus), ei tähenda saatja kehtivat nõusolekut.

Viimaks tuleks täpsustada, et ka muude kui asjaomaste lõppkasutajate isikuandmete (näiteks kolmanda isiku pilt või kirjeldus kahe inimese vestluses) töötlemine peab vastama kõigile isikuandmete kaitse üldmääruse asjaomastele sätetele.

19. **Lõppseadmed ja tarkvara peavad *vaikimisi* ära hoidma, ennetama ja keelama ebaseaduslikku sekkumist ning andma teavet valikuvõimaluste kohta.** Ehkki määruse ettepanekus kohustatakse elektroonilist sidet võimaldava tarkvara pakkujaid „pakkuma võimalust“ keelata piiratud sekkumine seoses lõppseadmega ning kohustatakse tarkvara pakkujaid installimise ajal nõudma lõppkasutajalt nõustumist ühe seade kasutamise (artikli 10 lõiked 1 ja 2), ei ole selline valik võrdsustatav *eraelu puutumatuse tagamisega vaikimisi*. Peale selle on „võimalus“ teatavat sekkumist takistada olemas juba praegu, kuid see ei ole tänini suutnud piisavalt lahendada soovimatu jälgimise probleemi. Just seetõttu on isikuandmete kaitse üldmääruses tehtud teadlik poliitiline valik kehtestada andmete ja eraelu puutumatuse lõimitud ja vaikimisi kaitse põhimõtted (isikuandmete kaitse üldmääruse artikkel 25). Määruse ettepanekus rikutakse neid põhimõtteid seoses side- ja seadmete andmetega. Samas on raadioseadmete direktiivis 2014/53/EL⁹ (mida on mainitud põhjenduses 10) üksnes väga piiratud infoturbealane kohustus: selles on nõutud, et raadioseadmed peavad sisaldama „turvaseadmeid, et tagada kasutajate ja abonentide isikuandmete ja eraelu puutumatuse kaitse“ (artikli 3 lõike 3 punkt e). See ei saa asendada määruse ettepanekust tulenevaid konkreetseid eraelu puutumatuse vaikimisi kaitse seadeid. Sellega seoses väärib märkimist ka asjaolu, et 2016. aasta detsembris avaldatud e-privatsuse Eurobaromeetri küsitluse tulemustest selgus, et „peaaegu seitse inimest kümnest (69 %) on täiesti nõus väitega, et nende brauseri vaikeseaded peaksid peatama nende teabe jagamise“¹⁰. Samuti on töörühm mures brauseri seadete ja „kolmandate isikute“ määratluse pärast. Vt märkus 24. Pealegi tuleb mees pidada, et see säte ei puuduta mitte üksnes arvutis kasutatavaid brausereid, vaid laieneb ka teistele suhtlemist võimaldavatele tarkvaraliikidele (sealhulgas operatsioonisüsteemidele, rakendustele ja asjade internetiga ühendatud seadmete tarkvaraliidestele). Kokkuvõttes peavad lõppseadmed ja tarkvara seadmed kaitsma eraelu puutumatust *vaikimisi* ning juhendama kasutajaid installimise ajal

⁹ Raadioseadmete direktiiv 2014/53/EL.

¹⁰ Vt Flash Eurobarometer 443, e-privatsuse aruanne (avaldatud 2016. aasta detsembris), lk 5.

seadistusmenüü abil neid vaikeseadeid muutma. Need seadistusmenüüd peavad kasutamise ajal olema pidevalt hõlpsasti juurdepääsetavad. Töörühm julgustab Euroopa seadusandjat täpsustama sellel eesmärgil artikli 10 kohaldamisala.

20. **E-privatsuse määrus peaks sõnaselgelt keelustama jälitusmüürid**, st tava, mille kohaselt juurdepääs veebisaidile või teenusele on keelatud seni, kuni üksikisikud nõustuvad sellega, et neid jälgitakse teistel veebisaitidel või teisi teenuseid kasutades. Nagu töörühma varasemates arvamustes e-privatsuse direktiivi kohta juba märgitud¹¹, ei ole selline võta-või-jäta-lähenemine peaaegu kunagi õiguspärane¹². Kui lõppseadme töötlemis- ja salvestusvõimekuse kasutamine või lõppkasutajate lõppseadmetest teabe kogumine võimaldab kasutaja tegevust jälgida pikema aja jooksul või eri teenuste (näiteks eri veebisaitide või rakenduste) kasutamisel, võib selline töötlemistegevus rängalt sekkuda kõnealuste kasutajate eraellu. Arvestades interneti suurt tähtsust sõnavabaduse põhiõiguse, sealhulgas teabele juurdepääsu õiguse teostamise võimaldamisel, ei tohiks üksikisikute võimalus pääseda juurde veebis olevale sisule sõltuda sellest, kas nad on andnud heakskiidu enda tegevuse jälgimisele eri seadmetel ja veebisaitidel/rakendustel. Seetõttu peaks tulevases e-privatsuse määruks olema täpsustatud, et juurdepääsu näiteks veebisaitidel ja rakendustes olevale sisule ei tohi muuta tingimuslikuks selliste sekkuvate töötlemistoimingute heakskiitmisest, olenemata sellest, millist jälgimistehnoloogiat kohaldatakse – näiteks küpsiseid, seadmetuvastust, kordumatute tuvastustunnuste lisamist või muid jälgimismeetodeid. Selle keelu vajalikkust rõhutab hiljutine Eurobaromeetri e-privatsust käsitlev uuring, milles on märgitud, et „ligi kaks kolmandikku (64 %) vastajatest leiab, et nende veebitegevuse jälgimine vastutasuks piiramatult juurdepääsu eest teatavale veebisaidile on vastuvõetamatu“.

21. Kokkuvõttes peaks **määruse ettepanek** neljas eelnimetatud punktis **täitma selles oleva lubaduse tagada isikuandmete kaitse üldmäärusega samaväärne või kõrgem kaitstuse tase**. Põhjenduses 5 on konkreetselt sedastatud, et määruse ettepanek ei vähenda isikuandmete kaitse üldmäärusega tagatud kaitse taset. Määruse ettepaneku praeguses sõnastuses ei vasta see aga tõele, eriti seoses seadmete jälgimise (märkus 17), lõimitud eraelukaitse põhimõtte puudumise (märkus 19) ja nõusolekuga (märkus 18). See on eriti asjakohane seetõttu, et seletuskirja punktis 1.2 on märgitud, et määruse ettepaneku puhul „on tegemist isikuandmete kaitse üldmääruse suhtes erioigusaktiga (*lex specialis*) ning sellega täpsustatakse ja täiendatakse nimetatud määrust isikuandmetena käsitatavate elektroonilise side andmete suhtes“. Töörühm teeb ettepaneku, et e-privatsuse määrus peaks minimaalselt täpsustama järgmist:

i) e-privatsuse määruks sätestatud keelud on ülimuslikud isikuandmete kaitse üldmääruks sätestatud õiguste suhtes (näiteks e-privatsuse määruks artiklis 5 sätestatud sekkumise keeld on ülimuslik elektroonilise side teenuste osutajate õiguste suhtes töödelda isikuandmeid edasi isikuandmete kaitse üldmääruse artikli 5 lõike 1 punkti b ja artikli 6 lõike 4 alusel);

¹¹ Vt näiteks WP 240 (arvamus e-privatsuse direktiivi hinnangu ja läbivaatamise kohta), lk 16; WP 208 (erandid nõusolekust), lk 5.

¹² See seisukoht ei piira isikuandmete kaitse üldmääruse artikli 7 lõike 4 kohaldamist – sellega võidakse võta-või-jäta-olukord välistada ka muudes olukordades, kus see on kohane.

ii) kui andmete töötlemine on lubatud mis tahes erandi (sh nõusoleku) alusel e-privatsuse määruuses sisalduvatest keeldudest, peab selline töötlemine isikuandmeid puudutavates aspektides siiski vastama kõigile isikuandmete kaitse üldmääruse asjaomastele sätetele;

iii) kui andmete töötlemine on lubatud mis tahes erandi alusel e-privatsuse määruuses sisalduvatest keeldudest, on keelatud andmete igasugune muu töötlemine isikuandmete kaitse üldmääruse alusel, sealhulgas isikuandmete kaitse üldmääruse artikli 6 lõikes 4 sätestatud töötlemine muul eesmärgil. See ei takistaks vastutavaid töötlejaid küsimast uutele töötlemistoimingutele lisanõusolekut. Samuti ei takistaks see seadusandjaid kehtestamast e-privatsuse määruuses uusi, piiratud ja konkreetseid erandeid, näiteks võidakse lubada andmeid töödelda teadusuuringute või statistilisel eesmärgil isikuandmete kaitse üldmääruse artikli 89 alusel või üksikisikute eluliste huvide kaitsmiseks isikuandmete kaitse üldmääruse artikli 6 lõike 1 punkti d alusel.

Samuti tuleks e-privatsuse määrust tõlgendada viisil, millega on tagatud, et see annab isikuandmete kaitse üldmäärusega võrreldes vähemalt samaväärse ja vajaduse korral kõrgema kaitstuse taseme.

4. MUUD MUREPUNKTID

Peale eelnimetatud punktide on artikli 29 tööriühm **mures** ka järgmiste aspektide pärast.

TERRITORIAALSET JA MATERIAALÕIGUSLIKKU KOHALDAMISALA TULEB LAIENDADA

22. **Termin „metaandmed“ on määratletud liiga kitsalt.** Metaandmed on artikli 4 lõike 3 punktis c määratletud kui „elektroonilise side võrgus elektroonilise side sisu edastamiseks, levitamiseks või vahetamiseks töödeldavad andmed“ (rõhuasetus lisatud). Sõna „võrk“ kasutamine näib viitavat sellele, et „metaandmeteks“ saab lugeda üksnes sellised andmed, mis on loodud teenuste osutamise käigus võrgu madalamas kihis. See võib tähendada, et OTT-teenuse osutamise käigus loodud andmed jääksid mõiste kohaldamisalast välja. See ei ole soovitatav ja tõenäoliselt ka mitte taotluslik, arvestades seda, et eesmärk oli laiendada määruuse ettepaneku kohaldamisala ka OTT-teenuste osutajatele. Selle probleemi lahendamiseks tuleks „elektroonilise side metaandmete“ määratlust muuta nii, et see hõlmaks kõiki andmeid, mida töödeldakse elektroonilise side sisu edastamiseks, levitamiseks või vahetamiseks.

23. Järgmine murepunkt on asjaolu, et **selliste organisatsioonide suhtes, mis ei asu ELis, laieneb määruuse ettepaneku territoriaalne kohaldamisala üksnes elektroonilise side teenuste osutajatele.** Määruuse ettepanekus on sätestatud, et kui elektroonilise side teenuse osutaja ei asu Euroopa Liidus, siis nimetab ta kirjalikult oma esindaja Euroopa Liidus (artikli 3 lõige 2). Samuti on põhjenduses 9 mainitud, et määrust tuleks kohaldada elektroonilise side teenuste osutajate töötlemistoimingutele olenemata sellest, kus töötlemine toimub. Tööriühm kiidab selle täpsustuse heaks. Kuna aga sõnastuses on piirdutud üksnes elektroonilise side teenuste osutajatega, ei ole selge, millises ulatuses see territoriaalne kohaldamisala kehtib muud liiki isikutele

(näiteks isikutele, kes sekkuvad lõppkasutajate lõppseadmete eetrisse antud teabesse või koguvad seda, vt määruse ettepaneku artikli 3 lõike 1 punkt c koos artikliga 8). Seetõttu soovib töörühm muuta artikli 3 lõikeid 2 ja 5 nii, et need hõlmaksid ka üldkasutatavate kataloogide pakkujaid, elektroonilist sidet võimaldava tarkvara pakkujaid ning isikuid, kes saadavad otseturunduslikke ärilisi teadaandeid või koguvad lõppkasutajate lõppseadmega seotud või sinna salvestatud (muud) teavet, kui nende tegevus on suunatud ELis asuvatele kasutajatele (vt määruse ettepaneku põhjendus 8)¹³.

LÕPPSEADMETE KAITSET TULEB TUGEVDADA

Järgmine murepunktide kategooria on seotud lõppseadmete ebapiisava kaitsega määruse ettepanekus.

24. Esiteks **jäetakse määruse ettepanekus ekslikult mulje, et kehtivat nõusolekut saab anda mittespetsiifiliste brauseriseadete abil**. Töörühm mõistab, et lõppkasutajad on üle koormatud nõusoleku andmise palvetega (põhjendus 22). Seda probleemi aitavad lahendada brauseri (ja samalaadse tarkvara) seaded. Kuna aga brauseri üldised seaded ei ole mõeldud kohaldamiseks jälgimistehnoloogiale üksikjuhtudel, ei sobi need isikuandmete kaitse üldmääruse artiklis 7 ja põhjenduses 32 sätestatud nõusoleku andmiseks (kuna see nõusolek ei ole teavitatud ega piisavalt konkreetne).

Lõppkasutajal peab olema võimalus anda igale veebisaidile või rakendusele eraldi nõusolek eri eesmärkidel jälgimiseks (näiteks sotsiaalmeedias jagamiseks või reklaami pakumiseks). Andmete vastutav töötleja, kes vastutab mitme veebisaidi eest, võib küsida nõusolekut ka kõigi teiste enda kontrolli all olevate veebisaitide või rakenduste kohta, eeldusel et iga nõusolekutaotlus on esitatud eraldi.

Samuti peab vastutav töötleja järgima kõiki muid nõusolekuga seotud kohustusi, sealhulgas kohustust anda kasutajatele piisavat teavet. See tähendab nii brauserite kui ka andmete vastutavate töötlejate jaoks seda, et nõusolek on kehtetu juhul, kui nad pakuvad üksnes varianti „nõustun kõigi küpsistega“, kuna see ei võimaldaks kasutajatel anda vajalikku üksikasjalikku nõusolekut. Siiski peaksid brauserid saama anda kasutajatele võimaluse teha teavitatud ja teadlik otsus nõustuda kõigi küpsistega ning seega vältida külastatavate veebisaitide edasisi konkreetseid nõusolekutaotlusi.

Töörühm soovib tungivalt, et e-privatsuse määrus muudaks brauseritele kohustuslikuks tehniliste mehhanismide, näiteks jälgimiskeelu (Do Not Track) standardi järgimise, tagamaks, et kasutajatele antakse enda seadmetesse sekkumise suhtes reaalne valikuvõimalus ja kontroll selle üle¹⁴.

¹³ Vt isikuandmete kaitse üldmääruse artikli 3 lõige 2: „Käesolevat määrust kohaldatakse liidus asuvate andmesubjektide isikuandmete töötlemise suhtes mujal kui liidus asuva vastutava töötleja või volitatud töötleja poolt, kui andmete töötlemine on seotud a) liidus asuvatele andmesubjektidele kaupade ja teenuste pakumisega, olenemata sellest, kas andmesubjekt peab maksma tasu; või b) nende tegevuse jälgimisega, kui see tegevus toimub liidus.“ Sellel kohustusel võib olla ka erandeid kooskõlas isikuandmete kaitse üldmääruse artikli 27 lõikega 2.

¹⁴ Vt veebiaadress: <https://www.w3.org/TR/tracking-compliance/>. Punktis 7 on selgitatud erandi mudelit ning saidipõhiste ja veebiüleste erandite erinevust. Punktis 6 on esitatud masinloetavad andmed, mida andmete vastutavad töötlejad võivad kasutada, et täita nõusoleku saamist puudutava teabe kohustus.

Veelgi olulisem on see, et e-privatsuse määruks oleks tagatud, et kõik andmete vastutavad töötajad aktsepteeriks nii seadmel oleva teabe salvestamist puudutavat valikut kui ka brauserilt saadud mittejälgimise märguannet õiguslikult siduva teatena nõustumise või keeldumise kohta. See ei piira töörühmal andmast edasisi suuniseid mittejälgimise standardi järgimise kohta, näiteks seoses otstarbe piiramise põhimõttega, pärast standardi lõplikku valmimist (mis toimub kava järgi 2017. aasta lõpus).

Kaudsed nõusoleku vormid, näiteks veebisaidil klõpsamine või lehekülje edasikerimine, ei tohi tühistada salvestamise ja mittejälgimise märguandega seoses tehtud valikuid. Selle standardi kasutamise oluline eelis seisneb asjaolus, et see ei piirdu üksnes jälgimisega küpsiste abil, vaid käsitleb ka teisi jälgimisviise, näiteks seadmetuvastust.

Selle standardi järgimise seaduslikult kohustuslikuks muutmine lahendab veel ühe probleemi, mis on seotud artiklis 10 esitatud mõiste „kolmas isik“ praeguse kasutusega. Veebisait või rakendus sisaldab tavaliselt palju elemente, mis pärinevad nii veebisaidilt endalt kui ka välistelt isikutelt. Samuti võib külastataval veebisaidil töötada väline kood, mis saadab andmeid kolmanda isiku serverisse. Jälgimisküpsise võib saata vahetu suhtluspartner, näiteks siis, kui kasutaja külastab mõnda sotsiaalvõrgustiku saiti. See sotsiaalvõrgustiku sait võib aga olla ka kolmas isik, kui sama kasutaja külastab mõnda teist veebisaiti, mis sisaldab suhtlust nimetatud sotsiaalvõrgustiku saidiga. Kõigil neil juhtudel olenemata sellest, kas olukord puudutab juurdepääsu lõppkasutaja seadmes olevale teabele või selle salvestamist, on tegemist seadet puudutava sekkumisega, mis nõuab nõusolekut (välja arvatud juhul, kui sellele kohaldatakse mõnda erandit). Mittejälgimise standardis kasutatakse seda kirjeldades termineid „saidipõhine“ ja „veebiülene“. Seetõttu tuleks e-privatsuse määruks olev viide „kolmandale isikule“ kõigi sidusrühmade õiguskindluse suurendamiseks sõnastada ümber nii, et see hõlmaks kõiki isikuid, kellega seade suhtleb (kuna nad salvestavad seadmel olevat teavet või pääsevad sellele juurde).

Selleks et viia jälgimiskeelu standard vastavusse hartast tuleneva teabevahetuse konfidentsiaalsuse ja andmekaitse kõrge kaitstuse tasemega, peaks e-privatsuse määruks olema täpsustatud, et erinevalt saidipõhisest jälgimisest peavad taotlused veebiüleseks jälgimiseks olema esitatud eraldi ja kasutajatel peab olema vabadus selliste taotlustega nõustuda või need tagasi lükata. Lisaks, et kaitsta kasutajaid sagedaste nõusolekutaotluste eest, peaks e-privatsuse määruks tagama, et mingi konkreetse organisatsiooni veebiülese jälgimise taotluse tagasilükkamine (kas mittejälgimise standardi või eraldi musta nimekirja vahendusel) takistab sellel organisatsioonil esitamast edasisi nõusolekutaotlusi vähemalt kuue kuu jooksul. See nõue ei takista sellel organisatsioonil paluda nõusolekut seoses tema enda veebisaidiga (nt taotlus saidipõhise nõusoleku saamiseks) juhul, kui kasutaja seda saiti vahetult külastab. Praktikast tähendab see seda, et näiteks videoedastussait, mis saadab jälgimisküpsiseid, võib küsida nõusolekut siis, kui kasutaja külastab tema saiti, kuid ei või kuue kuu jooksul nõusolekut uuesti küsida siis, kui kasutaja on nõusoleku andmisest keeldunud ja külastab teisi veebisaiti, mis sisaldavad nimetatud videoedastussaidilt pärit videoid.

25. Samuti on „veebis külastajate arvu mõõtmist“ puudutav erand sõnastatud ebatäpselt. Määruse ettepaneku artikli 8 lõike 1 punktis d on erand, mis puudutab

veebis külastajate arvu mõõtmist. Esimene murepunkt on see, et sellel terminil puudub määratlus ja selle võib segamini ajada kasutaja profiili määramisega. Määratluses tuleks selgelt väljendada, et nimetatud erandit ei tohi kasutada profiili määramise eesmärgil. Erandit peaks saama kohaldada üksnes kasutusanalüüsiks, mis on vajalik kasutaja soovitud teenuse toimimise analüüsimiseks, kuid mitte kasutajaanalüüsiks (st veebisaidi, rakenduse või seadme tuvastatavate kasutajate käitumise analüüsiks). Seetõttu ei tohi seda erandit kasutada olukorras, kus on võimalik andmeid seostada tuvastatavate kasutajaandmetega, mida töötleb teenuseosutaja või mõni muu andmete vastutav töötleja. Peale selle viitab kirjeldus tehnoloogiast olulisel määral sõltuvale kohaldamisele. Seetõttu tuleks termin „veebis külastajate arvu mõõtmine“ ümber sõnastada tehnoloogiliselt neutraalseks, et see hõlmaks ka rakendustelt, kantavatelt seadmetelt ja asjade internetiga seotud seadmetelt saadud samalaadset analüütilist kasutusteavet.

Töörühm soovib võtta eeskuju Madalmaades kehtestatud erandist, mida kohaldatakse juhul, kui see on hädavajalik selleks, et saada teavet osutatud infoühiskonna teenuse tehnilise kvaliteedi või tõhususe kohta, ning mõjutab asjassepuutuva abonendi või lõppkasutaja privaatsust vähe või ei mõjuta seda üldse (vt Madalmaade telekommunikatsiooniseaduse artikli 11.7a lõike 3 punkt b). Selle erandi puhul võetakse arvesse asjaolu, et enamik interneti või rakenduste analüüsi käigus kogutud andmeid on siiski isikuandmed. See tähendab, et nende andmete töötlemisele kohaldatakse ka isikuandmete kaitse üldmäärust. See tähendab näiteks seda, et kasutust võib analüüsida ka väline organisatsioon, ent üksnes järgmistel tingimustel:

- i) organisatsioon tegutseb andmete volitatud töötlejana;
- ii) sõlmitud on isikuandmete kaitse üldmäärust järgiv volitatud töötleja leping;
- iii) kasutatav analüüsitehnika takistab kasutajate uuesti tuvastamist, mis muu hulgas tähendab kasutajate IP-aadresside anonüümimist;
- iv) konkreetset küpsist (konkreetsed küpsiseid) või muid analüüsiks kasutatavaid andmeid saab kasutada üksnes asjaomase veebisaidi, rakenduse või kantava seadme puhul ning neid ei saa seostada muude tuvastatavate andmetega;
- v) kasutajatel on õigus nõusoleku andmisest keelduda (vt ka arvamuse märkused 17 ja 50).

Ehkki nende tingimuste täitmise korral ei oleks nõusolek vajalik, peavad andmete vastutavad töötledjad siiski andma kasutajatele piisavat teavet, näiteks jälgimiskeelu standardis nimetatud jälgimise olekut väljendaval väljal¹⁵.

26. E-privaatsuse määruuses **tuleks tagada, et nõusoleku nõuete erandid oleksid kitsad ja täpselt sõnastatud**. Seadmetega seotud sekkumise nõusoleku nõude erandi sõnastus artikli 8 lõike 1 punktis c on peaaegu samasugune nagu praegune sõnastus e-privaatsuse direktiivi artikli 5 lõikes 3: „hädavajalik sellise infoühiskonna teenuse osutamiseks, mida abonent või kasutaja on sõnaselgelt taotlenud“, kuid ilma mingi selgituseta on sõna „hädavajalik“ asemel kasutatud sõna „vajalik“. See valmistab

¹⁵ Vt Tracking Preference Expression (DNT) (jälgimiseelistuste väljendamine), toimetaja 7. märtsi 2016. aasta kavand.

muret kahel põhjusel. Esiteks on juba e-privatsuse direktiivi säte toonud kaasa arvukaid arutelusid järelevalveasutuste ja organisatsioonide vahel seoses selle kohaldamisalaga ning täiendsõna „häda-“ kustutamine vähendab õiguskindlust veelgi. Teiseks on see probleem ka seetõttu, et töörühm on juba andnud suuniseid selleks, kuidas tõlgendada selles kontekstis sõna „hädavajalik“. Töörühm pakkus oma arvamuses, mis käsitleb vabastust küpsiste kasutamiseks nõusoleku saamise kohustusest (WP 194), järgmise täpsustuse:

„Küpsis on vajalik kasutajale (või abonendile) konkreetse funktsiooni pakkumiseks: kui küpsised on blokeeritud, siis funktsioon ei ole kättesaadav, ning kasutaja (või abonent) on nimetatud funktsiooni infoühiskonna teenuse osana sõnaselgelt taotlenud.“¹⁶

Samuti täpsustas töörühm järgmist:

„kolmanda osapoole“ küpsised [ei ole] veebisaiti külastava kasutaja jaoks enamasti „hädavajalikud“, sest nad on üldjuhul seotud teenusega, mis erineb kasutaja poolt „sõnaselgelt taotletud“ teenusest¹⁷.

Töörühm lisas, et samamoodi ei saa platvormi või veebisaidi mittekasutajatele suunatud suhtluspluginade kasutamist pidada hädavajalikuks.

Veelgi enam: kui määruse ettepaneku artikli 6 lõike 1 punkt b lubab elektroonilise side andmeid töödelda juhul, kui see on „vajalik“ turvalisuse säilitamiseks, siis isikuandmete kaitse üldmääruse põhjenduses 49 on nõutud, et see oleks „rangelt vajalik“. Sõna „rangelt“ ärajätmine ei pruukinud olla taotluslik, kuna määruse ettepaneku põhjenduses 21 on siiski nimetatud, et sekkumiseks ei ole vaja nõusolekut, kui see on „rangelt vajalik“. Ometi annab määruse ettepanek võimaluse veelgi täpsustada, et selle määruse kontekstis tuleks vajalikkuse hindamist tõlgendada kõigi erandite puhul kitsalt. Seetõttu soovib töörühm asendada kõigi määruse ettepaneku artiklis 6 ja artikli 8 lõikes 1 nimetatud erandite puhul sõna „vajalik“ sõnaga „hädavajalik“.

Teisalt peaks e-privatsuse määrus sõnaselgelt võimaldama seadmetega seotud sekkumist turbevärskenduste paigaldamiseks. Turbevärskenduste saatmine interneti kaudu on enamikule lõppkasutajate seadmetele turbevärskenduste paigaldamiseks parim meetod. Värskenduste paigaldamist käsitatakse lõppseadmetega seotud sekkumisena. Nende seadmete turvalisuse ajakohasena püsimise tagamiseks on õigustatud huvi. Seega peaks turvaaukude kõrvaldajal olema üldjuhul võimalus paigaldada hädavajalikke turbevärskendusi ilma lõppkasutaja nõusolekuta. Siiski on ebaselge, kas see sekkumine võib tugineda „infoühiskonnaga“ seotud sekkumise keelu erandile (artikli 8 lõike 1 punkt c). Tuleks täpsustada, et see erand võimaldab küll turbevärskenduste paigaldamist, kuid üksnes tingimusel, et i) turbevärskendused

¹⁶ Artikli 29 alusel asutatud andmekaitse töörühm, WP 294, aramus 04/2012, mis käsitleb vabastust küpsiste kasutamiseks nõusoleku saamise kohustusest, vastu võetud 7. juunil 2012, veebiaadress: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_et.pdf.

¹⁷ Samas.

on diskreetse pakatina ega muuda mingil moel seadmes oleva tarkvara funktsioone (sealhulgas suhtlemist muu tarkvaraga või kasutaja valitud seadeid), ii) lõppkasutajat teavitatakse värskenduse paigaldamisest iga kord ette ja iii) lõppkasutajal on võimalus nende värskenduste automaatne paigaldamine välja lülitada.

OTSETURUNDUS

Järgmine murepunktide kategooria puudutab ebapiisavat kaitset otseturunduse eest.

27. Esimene murepunkt on see, et **otseturunduse kohaldamisala on liiga piiratud**. Määruse ettepaneku artikli 4 lõike 3 punktis f on „otseturundusteedaanne“ määratletud kui „mis tahes kujul kirjalik või suuline reklaam, mis saadetakse ühele või mitmele elektroonilise side teenuse kindlakstehtud või kindlakstehtavale lõppkasutajale“. Sõna „saadetakse“ viitab tehnoloogilise suhtlusvahendi sellisele kasutamisele, mis hõlmab vältimatult teadaande edasitoimetamist, samas kui suurem osa veebireklaamist (sotsiaalmeediaplatvormidel või veebisaitidel) ei hõlma reklaamide „saatmist“ selle sõna otseses tähenduses. Seda rõhutavad veelgi näited, mis on toodud selle määratluse lõpus (SMS, elektronpost) ja põhjenduses 33. Need kõik viitavad suhteliselt traditsioonilistele turundusteedaanete vormidele ja võib väita, et sellesse kohaldamisalasse ei kuulu isegi (samuti suhteliselt traditsiooniliste) kõnevalimissüsteemide kasutamine. Artiklit ja põhjendust tuleks muuta nii, et need hõlmaksid igasugust reklaami, mida *saadetakse või näidatakse või mis on suunatud* ühele või mitmele kindlakstehtud või kindlakstehtavale lõppkasutajale. Samuti tuleks paremini tagada, et käitumispõhist reklaami (mis põhineb lõppkasutajate profiilidel) käsitatakse samuti otseturundusteedaandena, mis on suunatud ühele või mitmele kindlakstehtud või kindlakstehtavale lõppkasutajale (kuna selline reklaam on suunatud konkreetsetele ja kindlakstehtavatele kasutajatele).

Lisaks piirduks artikli 16 lõikes 1 sätestatud kaitse „otseturundusteedaanete“ pakutud ulatuse kohaselt reklaammaterjale sisaldavate teadetega ega kaitseks üksikisikuid muude teadete eest, mida saadetakse või näidatakse või mis on kasutajale suunatud turunduseesmärkidel (näiteks nõusoleku saamiseks saadetavad müügivihjed, poliitiliste seisukohtade või valimiseelistuste soovitamine, heategevusorganisatsioonide või muude mittetulundusühingute reklaamimine või üldine teavitamine mõnest organisatsioonist). Samuti kasutatakse otseturunduses ikka veel faksi, ehkki määratluses seda ei mainita. Seetõttu peaks artikli 4 lõike 3 punkt f hõlmama kõiki reklaamimise, ükselt uksele käimise või soovitamise vorme, ka mittetulundusühingute puhul, ning selles tuleks elektronposti ja SMSi kõrval sõnaselgelt ära märkida ka faksiaparaat (vt ka täpsustamissettepanek märkuse 43 punktis a). Viimaks on põhjenduses 32 märgitud, et otseturundus hõlmab ka erakondade saadetud teadaandeid oma erakonna tutvustamiseks. Seda tuleks täiendada nii, et see hõlmaks poliitikuid ja valimistel osalevaid kandidaate, kes oma kandidatuuri tutvustavad.

28. Teiseks **ei saa otseturunduseks antud nõusolekut tagasi võtta tasuta ning seda ei ole sama lihtne teha kui nõusolekut anda**. Määruse ettepanekus tuleks täpsustada nõusoleku tagasivõtmise võimalust, et tagada järjepidevus ja suurendada teadaannete

saajate kaitset. Määruse ettepaneku artikli 16 lõike 6 praeguses redaktsioonis on sätestatud, et otseturundustedaannete saajatele tuleb esitada „saajatele vajalik teave, et nad saaksid kasutada oma õigust võtta lihtsasti tagasi oma nõusolek saada edaspidi turundustedaandeid“ (rõhuasetus lisatud). Seda kinnitatakse põhjenduses 34. Siiski tuleneb isikuandmete kaitse üldmääruse põhjendusest 70, et andmesubjektidel peaks isikuandmete kaitse üldmääruse kohaselt olema õigus oma isikuandmete otseturunduse eesmärgil töötlemise suhtes vastuväiteid esitada mitte üksnes lihtsasti, vaid ka tasuta. Sama terminit kasutatakse ka määruse ettepaneku artikli 16 lõikes 2, kuid üksnes seoses müügi kontekstis saadud kontaktandmete alusel toimuvast otseturundusest loobumisega.

Isikuandmete kaitse üldmääruse artikli 7 lõikes 3 on sätestatud, et nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine ja et üksikisikutel peab olema õigus oma nõusolek igal ajal tagasi võtta. Samuti on töörühm oma arvamuses 04/2010 FEDMA kohta (WP 174) juba tunnistanud, kui oluline on pakkuda „lihtsat, tõhusat, tasuta, kergesti kättesaadavat võimalust otseturundusest loobuda“¹⁸. See nõusoleku tagasivõtmise standard tuleks lisada ka määruse ettepaneku otseturundust käsitlevatesse sätetesse. Sama kehtib isikuandmete kaitse üldmääruse artikli 7 lõikes 3 sätestatud nõude kohta, et nõusoleku tagasivõtmine peab olema sama lihtne kui selle andmine.

29. Sellega seoses **tuleks täpsustada seda, mil viisil saab nõusolekut tagasi võtta või otseturunduskõnedest loobuda**. Määruse ettepaneku artikli 16 lõike 4 kohaselt võivad liikmesriigid kehtestada otseturunduslikest häälkõnedest loobumise korra. E-privatsuse määruks peaks olema esitatud täpsem kord nõusoleku tagasivõtmiseks ja turunduslikest kõnedest keeldumiseks. Põhjenduses 36 on sätestatud, et liikmesriikidel *peaks olema võimalik* luua ja/või hoida töös riiklikke keeldumist võimaldavaid süsteeme. Selle sätte põhjal võivad liikmesriigid seega lubada isegi sellist olukorda, kus kasutajal tuleks esitada keeldumisteade igale teadaannete saatjale eraldi. Selline rakendamine ei suuda kasutajaid kaitsta häiriva soovimatute teadaannete saamise eest¹⁹ ega võimalda isikuandmete kaitse üldmäärusega kooskõlas olevat mehhanismi nõusoleku tagasivõtmiseks lihtsasti ja igal ajal. Seetõttu peaks määruks olema sätestatud, et iga liikmesriik *peab* looma riikliku kõnede mittesoovijate registri. Samuti peaks määruks olema sätestatud, et häälkõnede saajatel peaks olema oma nõusoleku tagasivõtmiseks kaks võimalust: seoses edasiste kõnedega samast äriühingust või organisatsioonist ning võimalus lasta ennast nende kõnede ajal kanda riiklikku kõnede mittesoovijate registrisse.

18 Artikli 29 töörühm, WP 174, arvamus 04/2010, mis käsitleb FEDMA Euroopa tegevusjuhendit isikuandmete kasutamiseks otseturunduses, vastu võetud 13. juulil 2010, veebiaadress: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_et.pdf.

19 Näiteks Suurbritannias registreeris sideoperaator BT 31 miljonit häirivat kõnet nädalas. Vt <http://www.bbc.com/news/business-38635921>.

30. Teine murepunkt on see, et **valeidentiteedi kasutamine otseturundusteadaannete saatmisel ei ole sõnaselgelt keelatud**. Põhjenduses 34 on märgitud, et „isikuandmete varjamine ning valeidentiteedi või vale tagasisaatmisadressi või helistaja numbri kasutamine otseturunduslike mittetellitud äriliste teadaannete saatmisel“ on keelatud. Siiski on artikli 16 lõikes 6 üksnes sedastatud, et lõppkasutajaid tuleb teavitada „sellest, millise juriidilise või füüsilise isiku nimel teadaanne edastatakse“. Sellele kohustusele teavitada saajaid isikusamasusest peaks lisanduma selge keeld kasutada otseturunduseks varjatud või valesid kontaktaadresse.
31. See punkt on seotud ühe teise murepunktiga: **otseturunduslikele kõnedele kohaldatavat eesliite nõuet esitletakse alternatiivina kontaktliini numbri esitamise nõudele**. Artikli 16 lõike 3 kohaselt on otseturunduslikud kõned lubatud juhul, kui helistaja kas i) esitab selle liini numbri, mille kaudu saab nendega ühendust võtta (artikli 16 lõike 3 punkt a), või ii) esitab konkreetse koodi ja/või eesliite, mis näitab, et tegemist on turundusliku kõnega (artikli 16 lõike 3 punkt b). Ehkki töörühm kiidab heaks artikli 16 lõike 3 punktis b sätestatud kohustuse kasutada eesliidet, usub ta siiski, et see nõue ei käsitle sama teemat nagu see, mida käsitleb ühenduse võtmise liini numbri esitamise kohustus artikli 16 lõike 3 punktis a. Kui eesliite nõude eesmärk on anda kõne saajale võimalus saada enne kõne vastuvõtmist aru, et tegemist on turundusliku kõnega (ja võtta meetmeid selliste kõnede blokeerimiseks), siis ühenduse võtmise liini nõude eesmärk on anda kõnede saajatele (ja järelvalveasutusele) võimalus tuvastada turundustegevuse algataja ning temaga ühendust võtta. See on eriti asjakohane automatiseeritud kõnede puhul, kus turundaja võimalused teha häirivaid kõnesid ja kõne saaja võimalused neid kõnesid vältida on väga ebavõrdsel tasemel. Seega ei tohi need nõuded olla mitte alternatiivsed, vaid üksteist täiendavad.

AJAKAVA

32. Artikli 29 töörühm kiidab Euroopa Komisjoni selle eest, et komisjon on teadvustanud vajadust jõustada määruse ettepanek 2018. aasta mais koos isikuandmete kaitse üldmäärusega, et vältida ebakõlasid nende kahe õigusakti vahel. Siiski valmistab muret asjaolu, et see ajakava on väga nõudlik ning eeldab ka Euroopa elektroonilise side seadustiku direktiivi eelnõu lõpliku teksti valmimist. Seetõttu palub artikli 29 töörühm, et kõik seadusandlikku protsessi kaasatud sidusrühmad peaksid kinni 2018. aasta maiks määratud tähtajast.

MUUD MURED

Selles jaotises käsitleme mitmeid teisi muresid.

33. Esiteks on artikli 29 töörühm mures **mulje pärast, et andmete mittesihetstarbelise säilitamise meetmed on lubatavad**. Seletuskirjas on märgitud, et määruse ettepaneku kohaselt on liikmesriikidel võimalik säilitada või luua riiklikke andmete säilitamise raamistikke, millega kehtestatakse muu hulgas sihtetstarbelise säilitamise

meetmed (punkt 1.3). Pärast kohtuotsust Tele2/Watson²⁰ on selge, et ükski muu säilitamisraamistik peale sihtotstarbelise säilitamise raamistike ei ole harta alusel lubatud (ja isegi neile kohaldatakse olulisi tingimusi, näiteks järelevalvet) ning et üldistatud ligipääsu metaandmetele tuleb käsitada artikli 7 sisu rikkumisena samamoodi, nagu seda on üldine tutvumine elektroonilise side sisuga (vt Euroopa Kohtu otsus, Schrems, punkt 94). Seega jääb selle lause sõnastusest mulje, et liikmesriikidel on andmete säilitamise meetmete puhul teatav otsustusvabadus, mida tegelikult ei ole. Sellega seondub asjaolu, et määruse ettepanekus **ei anta metaandmetele piisavalt suurt kaitset**. Nagu mainisime märkuses 10, kiidab artikli 29 tööriühm heaks selle asjaolu tunnustamise, et metaandmed võivad avaldada väga tundlikku teavet. Vaatamata sellele ei saa metaandmed määruse ettepanekus sellist kaitset, nagu selle tunnustamisega peaks kaasnema. Arvestades metaandmete tundlikkust, tuleks teha andmekaitsealane mõjuhindang, eriti enne artikli 6 lõike 2 punkti c alusel tehtavat analüüsi (vt ka märkus 46).

34. Teiseks **laiendaks määruse ettepanek ebasoovitavalt andmete säilitamise võimalusi**. Määruse ettepaneku artiklis 11 viidatakse isikuandmete kaitse üldmääruse artikli 23 lõike 1 punktidele a–e, kirjeldades seda, millistel eesmärkidel võivad liikmesriigid piirata määruse artiklites 5–8 sätestatud kohustusi ja õigusi. Isikuandmete kaitse üldmääruses ei ole andmete eriliikidele ette nähtud selliseid piiranguid kooskõlas andmesubjektidele avalduvate suurte riskidega. Ehkki e-privaatsuse direktiivi artiklis 15 nähakse praegu ette samalaadne piirang, on selle eesmärgid piiratumad. Uues määruse ettepanekus võimaldatakse uusi piiranguid, mille eesmärk on „kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine“ (isikuandmete kaitse üldmääruse artikli 23 lõike 1 punkt d) ning „liidu või liikmesriigi muud üldist avalikku huvi pakkuvad olulised eesmärgid, eelkõige liidu või liikmesriigi oluline majanduslik või finantshuvi, sealhulgas rahandus-, eelarve- ja maksuküsimused, rahvatervis ja sotsiaalkindlustus“ (isikuandmete kaitse üldmääruse artikli 23 lõike 1 punkt e). Peale selle, et need eesmärgid on e-privaatsuse direktiiviga võrreldes uued, on ka artikli 23 lõike 1 punktis d esitatud viimane eesmärk ja kogu artikli 23 lõike 1 punktis e nimetatud eesmärk väga laialt sõnastatud. Seetõttu soovitame kustutada viide isikuandmete kaitse üldmääruse artikli 23 lõike 1 punktidele a–e ja selle asemel mainida üksnes praegu e-privaatsuse direktiivi artiklis 15 nimetatud eesmäärke.

35. **Kohustus teavitada kasutajaid turvaohutusest on minimaalse ulatusega**. Tööriühm kiidab heaks asjaolu, et teenuseosutajad peavad kasutajaid teavitama turvaohutusest ja nende kõrvaldamiseks võetavatest meetmetest, näiteks krüpteerimisest (artikkel 17 ja põhjendus 37). Selle sätte pealkiri kõlab aga järgmiselt: „Teave tuvastatud turvariskide kohta“. Asjaolu, et pealkirjas osutatakse üksnes tuvastatud riskidele, viitab sellele, et see säte puudutab üksnes (potentsiaalset) turvalisuse rikkumist, samas kui sätte ja põhjenduste sõnastus käsitleb lõppkasutajate harimist üldisemalt. Kui teenuseosutaja näiteks avastab, et kasutaja seade on pahavaraga nakatunud ja on muutunud osaks robotivõrgust, paneb see sätte teenuseosutajale pealtnäha otsese kohustuse teavitada kasutajat sellest tulenevatest ohtudest. Siiski võiks selle sätte

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

kohaldamisala täpsustada ning see ei tohiks olla piiratud eelnimetatud konkreetse stsenaariumiga. See säte peaks hõlmama vähemalt tuvastatud turvariske kõigis seadmetes, mille teenuseosutaja on lõppkasutajale teenuse tellimuse raames tarninud, näiteks ruuterites ja mobiilseadmetes, ning kasutaja teavitamist sellest, millised ohud kaasnevad nende seadistuste muutmisega, mis on algul eraelu kavandatud puutumatus põhimõtte kohaselt määratud eraelu puutumatus kaitsvaks.

Töörühm soovib laiendada sätte kohaldamisala nii, et see hõlmaks ka elektroonilist sidet võimaldava tarkvara pakkujaid (vt põhjendus 8) ja võib-olla ka uut kategooriat, nimelt side turvalisuse tagamiseks vajaliku tehnoloogia pakkujaid, kes ei ole teenuseosutajad (nt krüpteerimistehnoloogia pakkujad). Viimati nimetatud laiendamise puhul tuleb hoolt kanda selle eest, et see kohustus ei kattuks turvarikkumistest teatamise kohustusega, mis on sätestatud teistes õigusaktides, näiteks võrgu- ja infoturbe direktiivis²¹ ning teistes sertifikaatide pakkujaid käsitlevates õigusaktides. Kuna viimati nimetatud tehnoloogiapakkujad tavaliselt ei puutu lõppkasutajatega otseselt kokku, tuleb ühtlasi selgitada, kuidas nad saavad selle sätte alusel teavitamiskohustust järgida.

36. Töörühm kiidab heaks artiklites 2 ja 13 sätestatu, mida hakatakse kohaldama numbripõhistele isikutevahelise side teenustele. Siiski ei ole esmapilgul selge, miks **ei peaks samasugune eraelu puutumatus tase kehtima funktsionaalselt samaväärsete OTT-kõneteenuste puhul.**
37. Töörühm on mures ka selle pärast, et **puudub selgus kataloogides tehtavaid pöördotsinguid puudutava üksikasjaliku nõusoleku kohta.** Määruse ettepaneku artikli 15 lõikes 2 on pakkujalt nõutud lõppkasutajate nõusoleku saamist enne, kui nad hakkavad võimaldama andmetega seotud otsingufunktsioonide kasutamist (vt ka põhjendus 31). Töörühm kiidab heaks kataloogidesse lisamist puudutava nõusoleku nõude ühtlustamise, kuid taunib vähest üksikasjalikkust seoses eri liiki otsingutega. Kehtiv e-privatsuse direktiiv võimaldab artikli 12 lõike 3 põhjal liikmesriikidel nõuda pöördotsingu puhul eraldi nõusolekut. Selles artiklis on sätestatud: „Liikmesriigid võivad nõuda, et kui üldkasutataval kataloogil on muu otstarve peale isikute kontaktandmete otsimise nende nime ja vajaduse korral üksikute muude tunnusandmete põhjal, tuleb selleks küsida abonendilt lisanõusolek.“ Selle sätte põhjal on paljudes liikmesriikides pöördotsingu funktsioonide võimaldamisele nõutud eraldi nõusolekut, võttes arvesse tuvastatavuse eri tasandeid ja seega nende kahe funktsiooni sekkuvat iseloomu.
38. Üks formaalsem murepunkt on see, et **trahvide tase ei ole kõigi määruse rikkumiste puhul ühtlustatud.** Määruse ettepaneku kohaselt kehtestavad liikmesriigid rikkumiste korral kohaldatavad karistusnormid (määruse ettepaneku artikli 23 lõiked 4 ja 6 ning artikkel 24). Oleks järjepidevam kehtestada ka need õigusnormid e-privatsuse määruandes.

²¹ Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus, ELT L 194, 19.7.2016, lk 1–30, veebiaadress: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.EST

39. Viimaks **tugineb määruse ettepanek määratlustele, millest võivad saada „liikuvad sihtmärgid“**. Mitme põhimõiste puhul viidatakse määruse ettepanekus teisele õigusaktile, mis on praegu alles eelnõu kujul, ehk Euroopa elektroonilise side seadustiku ettepanekule (vt näiteks artikli 4 lõike 1 punkt b). Kaks olulist näidet selle kohta on „lõppkasutaja“ määratlus, mis hõlmab praegu füüsilisi ja juriidilisi isikuid, ning „elektroonilise side teenuse“ ja „isikutevahelise side teenuse“ määratlused, mida kajastatakse määruse ettepaneku artikli 4 lõike 1 punktis b ja millest viimast kirjeldatakse üksikasjalikumalt artikli 4 lõikes 2, et lisada määratlusse selliseid teenuseliike, mis on Euroopa elektroonilise side seadustikust sõnaselgelt välja jäetud²². Meie arvamus põhineb praegustel määratlustel, kuid on üsna tõenäoline, et Euroopa elektroonilise side seadustiku ettepanek ja/või selle põhimõisted muutuvad. See mõjutaks vahetult ka e-privatsuse määrust. Ideaaljuhul peaksid kõik Euroopa elektroonilise side seadustikust tulenevad terminid olema e-privatsuse määruuses määratletud sõltumatult; määruse ettepanek peaks minimaalselt sisaldama selgitust nende terminite kohta, mille määratlused kalduvad kõrvale Euroopa elektroonilise side seadustikus esitatutest (näiteks eespool nimetatud „lisateenuste“ lisamine „isikutevahelise side teenuse“ määratlusse). Kui see aga ei ole võimalik, soovitab töörühm kõigil õigusloomeprotsessi kaasatud isikutel tagada, et nii määruse ettepanekut kui ka Euroopa elektroonilise side seadustiku ettepanekut arutatakse ning nende üle hääletatakse samal ajal, et sidusrühmad võiksid õigesti hinnata nende uute õigusaktide kohaldamisala ja mõju.

5. TÄPSUSTAMISEETTEPANEKUD ÕIGUSKINDLUSE TAGAMISEKS

Peale eespool käsitletud punktide soovib töörühm tõsta esile mõned määruse ettepaneku sätted, mille täpsustamine tuleks kasuks. Neid täpsustusi peetakse vajalikuks selleks, et suurendada kõigi sidusrühmade õiguskindlust selle suhtes, et kogu ELis saadakse e-privatsuse määrusest ühtemoodi aru ja kohaldatakse seda ühtselt.

TÄPSUSTUSED SEOSSES KOHALDAMISALAGA

40. Määruse ettepaneku kohaldamisalaga seoses teeb artikli 29 töörühm ettepaneku järgmisteks täpsustusteks:

- a. **Mõiste „lõppkasutaja“ peaks hõlmama kõiki üksikisikuid.** Euroopa elektroonilise side seadustiku artikli 2 punktis 14 on „lõppkasutaja“ määratletud kui kasutaja, kes ei paku üldkasutatavaid sidevõrke ega üldkasutatavaid elektroonilise side teenuseid. Tuleks täpsustada, et üksikisikud, kes osalevad võrkudes – näiteks silmusvõrkudes oma

²² Näiteks on määruse ettepaneku artikli 4 lõikes 2 sätestatud, et isikutevahelise side teenus „hõlmab teenuseid, mis võimaldavad isikutevahelist interaktiivset suhtlust teise teenusega olemuslikult seotud väikse lisafunktsioonina“, Euroopa elektroonilise side seadustiku artikli 2 lõikes 5 aga on konkreetselt välja toodud, et sellised teenused välistatakse sellest määratlusest. (Euroopa elektroonilise side seadustiku artikli 2 lõike 4 kohaselt kuulub „isikutevahelise side teenus“ laiemasse „elektroonilise side teenuse“ kategooriasse.)

juhtmevaba võrgu ruuteriga –, ei ole määruse ettepanekuga saadava kaitse kohaldamisalast välja jäetud.

- b. **Tuleks täpsustada, et territoriaalne kohaldamisala laieneb kõigile lõppkasutajatele Euroopa Liidus.** Artikli 3 lõike 1 punktis a on sätestatud, et määruse ettepaneku kohaldamisalasse kuulub lõppkasutajatele elektroonilise side teenuste osutamine „Euroopa Liidus“, artikli 3 lõike 1 punktis c on aga sätestatud, et selle kohaldamisalasse kuulub „Euroopa Liidus asuvate“ lõppkasutajate lõppseadmetega seotud teabe kaitse (rõhuasetus lisatud). See on eri tõlgetes erinev. Saksakeelses tõlkes see eristus puudub, teistes keeltes, näiteks prantsuse, hispaania ja hollandi keeles, aga on olemas. Põhjendusest 9 nähtub selgelt, et territoriaalne kohaldamisala on kavandatud laiana ja ei ole oluline, kas teenuseid osutatakse väljastpoolt Euroopa Liitu või kas töötlemine toimub Euroopa Liidus. Seetõttu soovitame eemaldada artikli 3 lõike 1 punktist c sõna „asuvate“, et seda laia kohaldamisala rõhutada.
- c. **Määruse ettepanek näib konfidentsiaalset teabevahetust kaitsvat üksnes selle edastamise ajal, mitte aga salvestatud kujul.** Määruse ettepaneku praeguses lähenemisviisis keskendutakse side edastamise kaitsele. Vt näiteks põhjendust 15, milles on märgitud, et sideandmete infopüügi keeldu tuleks kohaldada sideandmete edastamise ajal, s.o kuni elektroonilise side sisu on laekunud ettenähtud adressaadile. Selle kaitse kohaldamisala põhineb sellisel teabevahetuse kontseptuaalsel raamistikul, mis on aegunud. Enamik sideandmeid jääb teenuseosutaja salvestiste hulka ka pärast nende vastuvõtmist. Tuleks tagada, et nende andmete konfidentsiaalsus püsib kaitstuna. Samuti hõlmab sama pilvepõhise teenuse abonentide vaheline side sageli väga vähe edastamist: e-kirja saatmine tähendab enamasti selle asjaolu kajastamist teenuseosutaja andmebaasis, mitte tegelikku kirja edastamist ühelt isikult teisele. Väide, et see on isikuandmete kaitse üldmäärusega juba kaetud, ei ole veenev: määruse ettepaneku kogu eesmärk on kaitsta igasugust konfidentsiaalset teabevahetust hoolimata sellest, kuidas see teabevahetus tehniliselt toimub. Tegemist võib olla lihtsalt eelnõu koostamisel tekkinud veaga, kuna artiklis 5 sätestatud keeld hõlmab „salvestamist“ ja „töötlemist“.
- d. **Kohaldamisala peaks hõlmama kõiki avalikke traadita interneti pääsupunkte.** Kuna traadita interneti pääsupunktide kasutamine on tavaline, on üksnes loogiline, et pääsupunktide kaudu edastatava teabevahetuse konfidentsiaalsus peab olema vaieldamatult kaitstud. Määruses ei ole seda siiski suudetud täpselt väljendada, kuna määruse kohaldamisala laieneb üksnes võrkudele, mis on antud kasutamiseks „määramata lõppkasutajate rühmale“ (põhjendus 13). Terminid „määramata lõppkasutajate rühm“ ja „lõppkasutajate suletud rühm“ vajavad määratlemist. Eelkõige tuleks täpsustada, et kohaldamisalasse kuuluvad ka turvatud (st parooliga) traadita võrgud, kui parool antakse teoreetiliselt lõpmatule kasutajate rühmale, kelle identiteeti ei ole võimalik eelnevalt kindlaks määrata (näiteks kohviku kliendid või lennujaama külastajad). Selles kontekstis on aluspõhimõte see, et kooskõlas artikli 29 töörühma varasema arvamusega e-privaatsuse direktiivi läbivaatamise kohta „*võib e-privaatsuse õigusakti kohaldamisalast välja jätta üksnes teenused, mida osutatakse ameti- või töösuhtes üksnes tööga seotud või ametlikul eesmärgil või üksnes töö- või äriprotsesside kontrollimise*

eesmärgil toimuva tehnilise side era- või avalik-õiguslike asutuste vahel, samuti üksnes kodukasutuseks mõeldud teenuste kasutamise“ (lk 8).

- e. **Määruse ettepanek peaks laienema ka digitaalsete ringhäälinguteenuste osutamise käigus kogutud andmetele.** Arvestades vaatajate käitumise tundlikku olemust, kuna sellest nähtuvad vaatajate isiklikud huvid ja iseloomuomadused, peaks e-privaatsuse määruses (võib-olla mõnes selle põhjenduses) olema täpsustatud, et „elektrooniliste sidevõrkude abil edastatava sisu“ välistamine „elektroonilise side teenuste“ määratlusest ei tähenda, et teenuseosutajad, kes osutavad nii elektroonilise side teenuseid kui ka sisuteenuseid, jääksid välja e-privaatsuse määruse nende sätete kohaldamisalast, mis on suunatud elektroonilise side teenuste osutajatele. See on eriti asjakohane seepärast, et selliste teenuste osutamine, mis puudutavad „elektrooniliste sidevõrkude abil edastatavat sisu“, on Euroopa elektroonilise side seadustiku ettepanekus „elektroonilise side teenuse“ määratlusest välja jäetud (artikli 2 lõige 4).
- f. **Sideandmed on üldjuhul isikuandmed.** Põhjenduses 4 on märgitud, et sideandmed võivad hõlmata isikuandmeid. Siiski on enamik sideandmeid isikuandmed²³ ning suures osas üsnagi intiimsed ja tundlikud, seega tuleks seda sätet muuta ja sedastada, et sideandmed on üldjuhul isikuandmed.
- g. **Konfidentsiaalne teabevahetus hõlmab platvormil vahetatavaid teateid.** Põhjenduses 1 on selgitatud, et konfidentsiaalsuse põhimõtet kohaldatakse „praegu kasutusel olevate ja tulevikus kasutusele võetavate sidevahendite“ suhtes. Põhjendus jätkub loeteluga näidetest selliste vahendite kohta, mis hõlmavad ka „sotsiaalmeedia kaudu sõnumite saatmist“. Selle eesmärk on ilmselt kohaldada seda põhimõtet ka sotsiaalmeedia (nt Facebook või Twitter) kasutajate vahel saadetavatele erasõnumitele või ajajoonele postitatud sõnumitele, mida näeb piiratud hulk inimesi, kuid selle sõnastus ei ole piisavalt selge.
- h. **E-privaatsuse määruse kohaldamine masinatevahelisele suhtlusele.** Nagu märgitud punktis 9, kiidab töörihm heaks kaitse laiendamise masinatevahelisele suhtlusele. Siiski mainitakse seda üksnes põhjenduses 12, mitte aga mõnes sellekohases artiklis. See kaitse on soovitatav, kuna selline side sisaldab sageli teavet, mida kaitstakse eraelu puutumatusega seotud õiguste kohaselt. Teisalt tuleks kohaldamisalast välja jätta kitsas puhta masinatevahelise suhtluse kategooria, mis ei mõjuta ei eraelu puutumatust ega sidepidamise saladust, näiteks olukorrad, kus selline side toimub võrguelementide (nt serverid, kommutaatorid) vaheliste sideedastusprotokollide täitmisel ja selle eesmärk on teavitada üksteist oma olekust.
Üks konkreetne kontekst, millega seoses e-privaatsuse määruse kohaldamine täpsustamist vajab, on intelligentsete transpordisüsteemide valdkond.

²³ Vt näiteks Euroopa Kohtu otsus, 6.11.2003, C-101/01, punkt 24 (seoses telefoninumbriga), Euroopa Kohtu otsus, 19.10.2016, C-582/14 (Breyer), punkt 49 (seoses dñaamiliste IP-aadressidega), ning Euroopa Kohtu otsus, 8.4.2014, C-239/12 ja C-594/12 (Digital Rights Ireland), punktid 26–27 (seoses metaandmete tundlikkusega).

Eeldatakse, et sõidukid hakkavad pidevalt raadio kaudu edastama kordumatute tunnustega andmeid. Kui e-privatsuse määruses puudub sideandmete lisakaitse, võib see endaga kaasa tuua juhtide sõiduharjumuste, marsruutide ja kiiruse pideva jälgimise. Siiski on Euroopa elektroonilise side seadustiku artikli 2 lõikes 1 esitatud uus ja laiendatud sidevõrkude määratlus. Nende hulka kuuluvad ülekandesüsteemid, millel ei ole kesket juhtimist ja mis võimaldavad edastada signaale raadio teel. E-privatsuse määruse põhjenduses 14 on sätestatud, et sellised andmed on elektroonilise side andmed. Määruse ettepaneku artikli 5 kohaselt on selliste sideandmete igasugune infopüük, seire või salvestamine keelatud, välja arvatud mõne erandi kohaldumise korral. Siiski on olemas vajadus neid andmeid töödelda, et esemed, näiteks isesõitvad autod ja seadmed, saaksid üksteist enda lähedusest või muudest ohtudest hoiatada. Küsimus on selles, milline erand sellises olukorras kohalduks. Lõppkasutajate nõusolek ei ole praktiline erand, kuna võib tekkida vajadus selle järele, et neid andmeid oleks alati võimalik töödelda. Seetõttu peaksid teenuseosutajad saama tugineda konkreetsele erandile, mis võimaldaks esemetel, näiteks isesõitvatel autodel ja seadmetel, üksteist enda lähedusest või muudest ohtudest hoiatada.

TÄPSUSTUSED SEOSSES NÕUSOLEKU MÕISTE JA KOHALDAMISEGA

41. Seoses nõusoleku mõiste ja kohaldamisega praeguses määruse ettepanekus teeb artikli 29 töörühm ettepaneku lisada järgmised täpsustused.
- a. **Nõusoleku mõiste kohaldamine juriidiliste isikute puhul.** Põhjenduse 3 kohaselt tuleks määrusega tagada, et isikuandmete kaitse üldmääruse sätteid kohaldatakse ka juriidilisest isikust lõppkasutajate suhtes. Põhjenduse kohaselt hõlmab see ka isikuandmete kaitse üldmääruses esitatud nõusoleku määratlust (vt ka põhjendus 18). Nagu on märgitud märkuses 13, kiidab töörühm heaks selle, et määruse kohaldamisala hõlmab sõnaselgelt ka juriidilisi isikuid. Selle põhimõtte kohaldamine praktikas ei ole aga selge. Isikuandmete kaitse üldmääruses sätestatud määratluse kohaselt peab nõusolek olema „teadlik“ ja andmesubjekti soovide tahteavaldus peab olema „avalduse vormis või selge nõusolekut väljendav tegevus“ (isikuandmete kaitse üldmääruse artikli 4 punkt 11). Tuleks täpsustada, mis hetkest võib juriidilist isikut käsitada „teadlikuna“ ja millal on juriidilise isiku puhul tegemist tahteavaldusega.
 - b. Selles kontekstis väärib mainimist, et enamasti ei saa tööandja anda nõusolekut oma töötajate nimel, kuna olukorras, kus tööandja nõuab töötajalt nõusolekut ja ebavõrdsete võimusehete tõttu võib nõusoleku andmata jätmisest tekkida tegelik või võimalik kahju, ei ole nõusolek kehtiv, kuna see ei ole antud vabatahtlikult²⁴. Seoses **äriühingutega, kes annavad**

²⁴ Vt aramus 15/2011 nõusoleku määratluse kohta (WP 187), aramus nr 8/2001 isikuandmete töötlemise kohta töösuhetes (WP 48) ja uut arvamust andmete töötlemise kohta töökohal (vastu võetud käesoleva arvamusega ühel ajal).

üksikisikutele kasutamiseks seadmeid, ei ole määruse ettepanekus (sobivat) erandit sekkumise keelule. Üks näide on olukord, kus tööandja soovib uuendada töötajale antud töötelefoni. Teine näide on olukord, kus tööandja võimaldab töötajatel kasutada rendiautosid ja laseb kolmandal isikul koguda halduseesmärkidel asukohateavet auto pardaseadme vahendusel. Mõlemal juhul on tööandjal huvi sekkuda seoses nende seadmetega.

Sellist sekkumist ei saa pidada vajalikuks infoühiskonna teenuse osutamiseks (artikli 8 lõike 1 punkt c) ega veebis külastajate arvu mõõtmiseks (artikli 8 lõike 1 punkt d). Probleemi lahendaks uue erandi loomine, mis hõlmaks olukorda, kus i) tööandja annab töösuhte kontekstis kasutamiseks teatavad seadmed, ii) seadmeid kasutab töötaja ja iii) sekkumine on hädavajalik selleks, et seade saaks töötaja käes toimida (mis viitab sellele, et andmete kogumisele tuleb rakendada proportsionaalsuse ja subsidiaarsuse põhimõtet). Tööandja peaks saama lõppkasutajate seadmetega seoses sekkuda üksnes juhul, kui need tingimused on täidetud.

- c. **Kontrollivõimaluste parandamine kõnede automaatse suunamise peatamiseks.** Artiklis 14 antakse lõppkasutajatele oluline kontrollivõimalus kolmandate isikute kõnede automaatse suunamise peatamiseks. Seda kaitsemeetet võib veelgi parandada sellega, et nõutakse ühtlasi lõppkasutaja nõusolekut selleks, et kõne suunamist võiks üldse algatada.

TÄPSUSTUSED SEoses ASUKOHA JA MUUDE METAANDMETEGA

42. Töörühm teeb ettepaneku täpsustada asukoha- ja muude metaandmetega seoses järgmisi aspekte:

- a. **Põhjenduses 17 tuleks täpsustada fraasi „asukohaandmed, mis genereeritakse muus kontekstis kui elektroonilise side teenuste osutamine“** tähendust. Ei ole selge, kas siin on mõeldud asukohaandmeid, mis on kogutud näiteks nutiseadmete GPS-funktsioonide abil saadud andmeid kasutavate rakenduste vahendusel, ja/või asukohaandmeid, mis põhinevad läheduses asuvatel traadita interneti ruuteritel, ja/või asukohaandmeid, mis on kogutud sõidukisse paigaldatud navigatsiooniseadmete abil, ja/või muul viisil kogutud asukohaandmeid. Selline täpsuse puudumine tekitab õiguskindlusetuse selle kohustuse ulatuse suhtes. Igal juhul on füüsilise isiku lõppseadme asukohaandmed käsitatavad isikuandmetena ja seetõttu kohaldatakse nende andmete töötlemisele isikuandmete kaitse üldmääruses sätestatud kohustusi.
- b. Tuleks täpsustada, et **suurem osa asukoha- ja muude metaandmete õiguspärasest töötlemisest ei nõua kordumatut tunnust**. Põhjenduses 17 on mainitud kuumuskaarte näitena selle kohta, kuidas elektroonilise side teenuste osutajad kasutavad elektroonilise side metaandmeid ärilisel otstarbel. Lihtsa kuumuskaardi koostamiseks ei ole aga kordumatuid tunnuseid vaja, piisab statistilisest loendusest. Teine selles põhjenduses mainitud näide, taristu kasutamine (ja koormus), on samuti loendatav teatavates mõõtmispunktides, näiteks liikluse reguleerimise tornide kasutamise koondstatistika loomise abil, millest nähtub mingi paiga koormus kindlal kellal ajal, kusjuures asjasepuutuvaid isikuid ei ole vaja kindlaks teha.

Veel üks selles põhjenduses toodud näide on teatava aja jooksul teatavas suunas kulgeva liikluse kuvamine, mis nõuab identifikaatorit ehk kordumatut tunnust, mille abil seostada üksikisikute asukohad konkreetsete ajavahemike järel. Tundub, et selle näitega soovitakse põhjenduses muuta õiguspäraseks nende andmete edasine töötlemine, et toetada suurandmete analüüsimist. Määruse ettepaneku kohaselt on sellise töötlemise ainus tingimus kohustus teha andmekaitsealane mõjuhinna juhul, kui töötlemise tulemusena võib tekkida suur oht füüsiliste isikute õigustele ja vabadustele. Sellest tingimusest ei piisa. Samuti on see vastuolus artiklis 6 esitatud kohustusega, et sellist töötlemist võib teha üksnes kasutajate nõusolekul ja juhul, kui andmeid ei ole võimalik anonüümida, teisisõnu ilma kordumatute tunnusteta. Sageli ei saa kasutajad keelduda sellest, et elektroonilise side teenuste osutajad koguvad nende asukohaandmeid, juhul kui selline kogumine on tehnilises mõttes vajalik kasutajale teabevahetuse edastamiseks või kui selline töötlemine on vajalik soovitud (näiteks navigeerimis-) teenuse osutamiseks. Oma varasemates arvamustes on töörihm leidnud, et nutiseadmete asukohaandmed on tundliku iseloomuga isikuandmed ja et selliste andmete analüüsimisest saadav kasu ei ületa kasutajate õigust oma teabevahetuse metaandmete konfidentsiaalsuse kaitseks, samuti ei ole see kasu ülimuslik nende üldiste isikuandmete kaitse üldmäärusest tulenevate andmekaitsega seotud õiguste suhtes. Seetõttu tuleks selles põhjenduses minimaalselt täpsustada, et teenuseosutajad peavad asukoha- või teiste metaandmete edasisel töötlemisel järgima isikuandmete kaitse üldmääruse artiklis 25 sätestatud kohustusi. See tähendab, et võtta tuleb vähemalt järgmised meetmed:

- i) ajutiste pseudonüümide kasutamine;
- ii) pseudonüüme ja algseid tuvastamist võimaldavaid andmeid sisaldava pöördotsingutabeli kustutamine;
- iii) andmete koondamine sellisel määral, et üksikuid kasutajaid ei saa nende marsruutide alusel enam tuvastada, ja
- iv) nende võõrväärtuste kustutamine, mis eeltoodust hoolimata tuvastamist võimaldaksid (kõiki neid meetmeid tuleb kohaldada ühel ajal).

Viimaks peab e-privatsuse määrus kohustama asukoha- ja muude metaandmete töötlemises osalevaid isikuid avalikustama enda kasutatavad anonüümimise ja edasise koondamise meetmed, ilma et see piiraks seadusega kaitstud saladuse hoidmise kohustust. See võimaldaks nii järelevalveasutustel kui ka laiemal avalikkusel hõlpsasti kontrollida, kas valitud meetod on piisav.

TÄPSUSTUSED SEOSSES MITTETELLITUD TEADAANNETEGA

43. Töörihm teeb ettepaneku täpsustada mittetellitud teadaannetega seoses järgmisi aspekte:

- a. **Nõusolekuta otseturundamise keelu sõnastus.** Määruse ettepaneku artikli 16 lõikes 1 on praegu märgitud, et elektroonilise side teenuseid võidakse kasutada otseturundusteadaannete saatmiseks (nõusoleku olemasolul), kuid selles ei ole sõnaselget keeldu saata (suunata või näidata)

otseturundusteadandeid ilma nõusolekuta. See on vastuolus teistes sätetes oleva lähenemisega, kus on esmalt sõnastatud keeld ja sellele järgnevad teatavad konkreetsed erandid. Praegune sõnastus viitab leebemale lähenemisele (mis ei ole arvatavasti taotluslik). Töörühm soovib kasutada e-privaatsuse direktiivi artikli 13 lõike 1 sõnastust veidi muudetud kujul: „Füüsilistel või juriidilistel isikutel on elektroonilise side teenuseid, sealhulgas häälkõnesid, automatiseeritud numbrivalimis- ja sidesüsteeme, sealhulgas poolautomaatseid süsteeme, mis ühendavad kõne saaja reaalse inimesega, fakse, elektronposti või muid elektroonilise side teenuseid lubatud lõppkasutajatele suunatud otseturustuseks kasutada ainult nende lõppkasutajate puhul, kes on selleks andnud eelneva nõusoleku.“

- b. **Turundusteateid ja olemasolevatele kontaktidele tehtavaid kõnesid käsitlevate sätete kohaldamisala.** Artikli 16 lõikes 2 on sätestatud, et kui isik saab oma kliendi elektronposti elektroonilised kontaktandmed, võib ta neid kasutada oma toodete ja teenuste edasiseks otseturunduseks juhul, kui klientidele antakse teabe kogumise ajal ja igas sõnumis selge, tasuta ja lihtne võimalus sellest keelduda. See piirdub praegu äriliste kontaktidega, mis on saadud „toote või teenuse müügi kontekstis“ ja oma sarnaste toodete või teenuste otseturunduseks. Arvestades, et otseturundussätteid kohaldatakse samamoodi mittetulunduslikule reklaamtegevusele (näiteks heategevusorganisatsioonide või erakondade reklaamtegevusele), tuleks seda sätet muuta nii, et see kohalduks samaväärselt mittetulundusorganisatsioonidele, kes võtavad ühendust neid varem toetanud isikutega, et tutvustada oma sarnaseid eesmärgi või ideaale, ja samasugune õigus keelduda peaks kehtima ka otseturunduskõnede puhul. Samuti tuleks „olemasolevate klientide kontaktidele“ kehtestada ajaline piirang nende kasutamiseks elektroonilises teabevahetuses kaubanduslikul, heategevuslikul või poliitilisel eesmärgil ning see ajaline piirang peaks kehtima ka otseturunduskõnede puhul. Kui liikmesriigid on otsustanud otseturunduslikest häälkõnedenest keeldumise süsteemi kasuks, on „olemasoleva kliendikontakti“ olemasolu kõnede mittesoovijate registri suhtes ülimuslik. Sellises olukorras ei ole lõppkasutajatel tulemuslikult võimalik takistada häirivate kõnede saamist äriühingutelt või organisatsioonidelt, kellega neil on olnud kontakt, aga kellega nad ei soovi enam tegemist teha. Seetõttu peaks määrus üldjuhul täpsustama, kui kaua see „olemasoleva kliendi“ erand kehtib, näiteks üks või kaks aastat, arvestades asjaomaste lõppkasutajate õiguspäraseid ootusi.
- c. **Otseturunduse eeskirjade kohaldamine juriidilistele isikutele.** Määruse ettepaneku artikli 16 lõikes 5 on sätestatud, et liikmesriigid tagavad, et juriidilisest isikust lõppkasutajate õigustatud huvi seoses soovimatute teadaannetega on piisavalt kaitstud. Kehtiva e-privaatsuse direktiivi artikli 13 lõikes 5 on kirjeldatud nende abonentide õiguslikke huve, kes ei ole füüsilised isikud. Ei ole selge, milline on selle sõnastuse muutmise mõju. Põhjendustes tuleks täpsustada, et see muudatus ei tähenda, et soovitakse pakkuda vähem kaitset. Sellega seondub ka asjaolu, et keeld teha otseturundust ilma nõusolekuta on seotud „füüsilisest isikust lõppkasutajatega, kes on andnud selleks oma nõusoleku“ (rõhuasetus lisatud). Tuleks täpsustada, et see hõlmab ka füüsilisi isikuid, kes *töötavad* juriidiliste

isikute *heaks*. Teisest küljest ei oleks nõusolekut vaja selleks, et võtta juriidiliste isikutega ühendust üldiste kontaktandmete vahendusel, mille nad on selleks otstarbeks avaldanud (näiteks „info@äriühing.eu“).

- d. **Otseturunduse eeskirjade kohaldamine (poliitilise) esindusõigusega isikutele.** Praegusel kujul võib artikkel 16 takistada rahvaesindajatele mõnede selliste teadaannete saatmist, milles on kirjeldatud äriprobleeme või -huve. Tuleks täpsustada, et määrus selliste teadaannete saatmist ei takista.

SELGITUSED PÕHIÕIGUSI KÄSITLEVATE ÕIGUSAKTIDE KOHALDAMISE KOHTA

44. **Harta ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni kohaldamine liikmesriikide andmete säilitamist käsitlevatele seadustele** vajab täpsustamist. Põhjenduses 26 on sätestatud, et kõik liikmesriikide avaliku huvi kaitsmiseks võetavad meetmed, näiteks seaduslik infopüük, peavad olema kooskõlas hartaga (ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga). See on hea, sest see on kooskõlas kohtuotsuses Tele2/Watson toodud mõttekäiguga, et kõik liikmesriikide kehtestatud erandid ELi seadustes sätestatud andmetöötlusega seotud kaitsemeetmetele peavad olema kooskõlas hartaga (ja liikmesriigi õigustes sisalduvate rikkumiste peale võib seega esitada hagi Euroopa Liidu Kohtule). Siiski on määruse ettepaneku artiklis 11 pelgalt märgitud, et määruse ettepaneku artiklite 5–8 ulatuse piirangu puhul peab austama põhiõiguste ja -vabaduste olemust ning see meede peab olema vajalik ja proportsionaalne. Siia tuleks lisada ka sõnaselge viide hartale ning Euroopa inimõiguste ja põhivabaduste konventsioonile.

45. **Side konfidentsiaalsust kaitseb ka Euroopa inimõiguste ja põhivabaduste konventsiooni artikkel 8.** Seletuskirja punktis 1.1 ja põhjenduses 1 selgitatakse, et määruse ettepanekuga rakendatakse harta artiklit 7. Seda korratakse põhjenduses 19. Side konfidentsiaalsuse põhiõigust ei kaitse aga mitte üksnes see säte, vaid ka Euroopa inimõiguste ja põhivabaduste konventsiooni artikkel 8. Sõnaselge viite lisamine mõnesse määruse ettepaneku artiklisse kinnitaks veelgi, et (lõpliku) määruse hindamisel tuleb arvesse võtta ka Euroopa Inimõiguste Kohtu asjakohast praktikat. See viide on muuseas olemas juba põhjendustes 20 (seoses lõppseadmetega) ja 26 (seoses seadusliku infopüügiga) ning seda toetavad veelgi seletuskirja punktis 2.1 esitatud kaalutlused (seoses harta ning Euroopa inimõiguste ja põhivabaduste konventsiooni vahelise seosega juriidiliste isikute kontekstis), kuid seda ei ole üheski asjakohases artiklis, näiteks artikli 11 lõikes 1.

MUUD TÄPSUSTUSED

46. Tuleks täpsustada, et **isikuandmete kaitse üldmäärusest tulenevad kohustused, näiteks need, mis on seotud isikuandmete rikkumise puhuks ettenähtud tegevuskorraga ja andmekaitsealaste mõjuhinnangutega, jäävad kehtima**, kui isikud töötlevad isikuandmeid elektroonilise side andmete kontekstis. Kuna põhjenduses 5 on mainitud, et määruse ettepanek on isikuandmete kaitse üldmääruse suhtes eriseadus ja et elektroonilise side andmete töötlemist tuleks lubada ainult määruse ettepaneku alusel, võib seada kahtluse alla, kas teatavad isikuandmete kaitse

üldmäärusest tulenevad kohustused kehtivad ka määruse ettepaneku kontekstis. Eelkõige tuleb see kõne alla olukorras, kus määruse ettepanekut on võimalik tõlgendada nii, et selles kehtestatakse teatav kohustus, samas kui selle küsimusega tegeleb ka isikuandmete kaitse üldmäärus. Mõned tüüpilised näited on järgmised:

- (i) määruse ettepanekus on kehtestatud kohustus teavitada „tuvastatud“ turvariskidest (artikkel 17) (vt ka märkus 35), kuid isikuandmete kaitse üldmääruses on sätestatud kord isikuandmetega seotud rikkumisest teavitamiseks (artiklid 33 ja 34);
- (ii) määruse ettepanekus on mainitud, et andmekaitsealase mõjuhinnangu tegemine ja järelevalveasutusega konsulteerimine kooskõlas isikuandmete kaitse üldmäärusega on teatavate asjaolude esinemise korral kohustuslik (põhjendused 17 ja 19 ning artikli 6 lõike 3 punkt b), samas kui isikuandmete kaitse üldmääruses on juba sätestatud, millal tuleb andmekaitsealane mõjuhinnang teha ja millal on konsulteerimine vajalik (artiklid 35 ja 36);
- (iii) ei ole välja öeldud, et isegi kui isik vastab kõigile määruse ettepaneku artiklis 5 sätestatud andmete töötlemise keelu erandi kohaldamiseks vajalikele tingimustele, peab ta isikuandmete töötlemisega seoses siiski järgima kõiki asjakohaseid isikuandmete kaitse üldmäärusest tulenevaid kohustusi ja igasugune muu töötlemine on isikuandmete kaitse üldmääruse kohaselt keelatud. Tuleks täpsustada, et sellest tulenevalt ei kohaldata isikuandmete kaitse üldmääruse artikli 6 lõikes 4 sätestatud vastavustesti;
- (iv) e-privatsuse määruse ettepanekus ei ole sätestatud samasugust sertifitseerimismehhanismi, nagu on isikuandmete kaitse üldmääruse artiklites 42 ja 43. Kuna isikuandmete kaitse üldmääruse artikli 42 kohaldamisala piirdub rangelt võttes andmekaitse sertifitseerimise mehhanismide ning isikuandmete kaitse üldmääruse järgimist tõendavate andmekaitsepitserite ja -märgiste kasutuselevõtuga, tuleks kaaluda võimalust kehtestada sellega võrreldav säte, mis võimaldaks sertifitseerida töötlemistoiminguid, standardeid, tooteid või teenuseid selle tõendamiseks, et need vastavad e-privatsuse määrusele.

Tagamaks, et sellist ebaselgust ei kasutata argumendina määruse ettepanekus sätestatud kaitse taseme langetamiseks, tuleks väljendada selgelt, et kõigil neil juhtudel peavad vastutavad töötlejad järgima ka isikuandmete kaitse üldmäärust.

47. Samuti tuleks täpsustada, et **nõusoleku tagasivõtmist puudutav nõue kehtib ka lõppseadmetega seotud sekkumise kontekstis**. Määruse ettepaneku artikli 8 lõike 1 punktis b on sätestatud võimalus lõppkasutajate lõppseadmetega seotud sekkumiseks nõusoleku olemasolu korral. Artikli 9 lõikes 3 on ette nähtud, et lõppkasutajatele antakse võimalus oma nõusolek igal ajal tagasi võtta, kuid see kehtib üksnes metaandmete ja sisu analüüsiga seotud nõusoleku puhul. Tuleks täpsustada, et see kohustus laieneb ka lõppseadmetega seotud sekkumisele.

48. Eeltooduga seoses tuleks täpsustada, et **meeldetuletus nõusoleku tagasivõtmise võimaluse kohta kehtib ka brauseri seadete kaudu antava nõusoleku puhul**. Artikli 9 lõikes 3 on nõutud, et lõppkasutajatele tuleb regulaarselt iga kuue kuu tagant meelde tuletada, et neil on võimalus oma nõusolek igal ajal tagasi võtta. Ehkki töörühm usub, et brauserite ja muu tarkvara, sealhulgas operatsioonisüsteemide, rakenduste ja asjade internetiga ühendatud seadmete tarkvaraliideste üldised seaded

(st sellised, mis ei põhine konkreetsetel üksikasjalikel kontrollimeetmetel) ei saa olla nõusoleku andmiseks kehtiv vahend, kuna üldistest seadetest ei piisa konkreetse nõusoleku andmiseks konkreetsetel juhtudel (vt märkus 24), peaksid vaikeseaded olema kasutajasõbralikud (vt märkus 19). *Kui* see jääb määruse ettepanekusse sisse, peavad seaded olema piisavalt üksikasjalikud, et kontrollida kogu isikuandmete töötlemist, millega kasutaja nõustub, ja hõlmama seadmete igat funktsiooni, mis võivad kaasa tuua isikuandmete töötlemise. Samuti tuleb lõppkasutajale vähemalt perioodiliselt (iga kuue kuu tagant) meelde tuletada võimalust neid seadeid muuta.

49. On kiiduväärt, et määruse ettepaneku kohaselt peab juba turule lastud tarkvara andma lõppkasutajale teada privaatsusseadete võimalustest (artikkel 10). **Siiski ei ole selge, kuidas on seda nõuet võimalik tulemuslikult kohaldada varasemast ajast pärit toodetele** ja muudele toodetele, mida enam ei toetata. Samuti tuleks täpsemalt selgitada, kuidas kohaldatakse seda nõuet avatud lähtekoodiga tarkvarale, mida arendatakse avatult ja detsentraliseeritult.
50. Tuleks täpsustada, et **määruse ettepaneku artiklis 10 sätestatud võimalus blokeerida (kolmanda isiku) küpsised on ülimuslik artikli 8 lõike 1 punktis d sätestatud erandi suhtes seoses veebis külastajate arvu mõõtmisega**. Teisisõnu peab kasutajatel isegi juhul, kui veebisait kasutab artikli 8 lõike 1 punktis d nimetatud veebis külastajate arvu mõõtmiseks analüüsivahendeid, ikkagi olema õigus oma brauseris need jälgimistehnoloogiad blokeerida.
51. **(Pool-)automatiseeritud numbrivalimis- ja sidesüsteemide määratlus vajab täpsustamist**. Selle termini määratluses määruse ettepaneku artikli 4 lõike 3 punktis h viidatakse lause teises pooles terminile endale („sealhulgas automatiseeritud numbrivalimis- ja sidesüsteemid, mis ühendavad kõne vastuvõtja reaalse inimesega“). Soovitame kustutada määratlusest see viimane lauseosa ja muuta artikli 4 lõike 3 punktis g toodud määratlust nii, et see hõlmaks ka kõnesid, mis on tehtud poolautomatiseeritud sidesüsteemide abil, näiteks automaatvalimissüsteemidega, mis ühendavad kõne vastuvõtja reaalse inimesega.
52. **„Teenuse tellimuse osaks olev teave“ vajab täpsustamist**. Põhjenduses 14 on märgitud, et elektroonilise side metaandmed „võivad sisaldada teenuse tellimuse osaks olevat teavet, kui sellist teavet töödeldakse elektroonilise side sisu edastamise, levitamise või vahetamise otstarbel“. Ei ole selge, mida selle sõnastusega öelda tahetakse.
53. Täpsustada tuleks **järjepidevuse ja koostöö mehhanismide kohaldatavust**. Põhjenduses 38 on märgitud, et määruse ettepanek tugineb isikuandmete kaitse üldmääruse järjepidevuse mehhanismile. Peale selle on artikli 18 lõikes 1 sätestatud, et isikuandmete kaitse üldmääruse VI ja VII peatükki kohaldatakse *mutatis mutandis*. Artiklis 19 on lisaks märgitud, et isikuandmete kaitse üldmääruse artikliga 70 kehtestatud ülesandeid täidab Euroopa Andmekaitsekoogu. Ehkki nende sätete kohaldamine on suhteliselt selge, ei saa välistada, et isikuandmete kaitse üldmääruses sätestatud järjepidevuse ja koostöö mehhanismi põhimõistetega seoses tekib tõlgendusküsimusi. Näiteks kohaldatakse „piiriülese isikuandmete töötlemise“ korral juhtiva järelevalveasutuse mehhanismi (isikuandmete kaitse üldmääruse artikli 56

lõige 1): ei ole selge, kuidas kohaldada seda määruse ettepaneku alusel lõppseadmetega seotud sekkumisele või sisu või metaandmete analüüsile. Seetõttu soovitame täpsustada mõnes põhjenduses nende põhimõistete kohaldamist ning rõhutada, et määruse ettepaneku kontekstis lahendatakse kõik lahendamata küsimused seoses nende isikuandmete kaitse üldmääruse peatükkidega kooskõlas nende peatükkide sätete eesmärgiga. Peale selle soovitame täpsustada, et artiklit 70 kohaldatakse määruse ettepaneku kontekstis Euroopa Andmekaitsekoostöö üldmääruse *mutatis mutandis* (see on praegu põhjendusest puudu).

* * *