



17/LT

WP 247

Nuomonė 01/2017 dėl siūlomo E. privatumo reglamento (2002/58/EB)

priimta 2017 m. balandžio 4 d.

Ši darbo grupė sudaryta pagal Direktyvos 95/46/EB 29 straipsnį. Ji yra nepriklausomas Europos patariamasis organas duomenų apsaugos ir privatumo klausimais. Jos uždaviniai aprašyti Direktyvos 95/46/EB 30 straipsnyje ir Direktyvos 2002/58/EB 15 straipsnyje.

Sekretoriato paslaugas teikia Europos Komisijos Teisingumo ir vartotojų reikalų generalinio direktorato C direktoratas (Pagrindinės teisės ir teisinė valstybė) (Directorate C (Fundamental Rights and rule of law) of the European Commission, Directorate General Justice and Consumers, Office No MO-59 05/035, B-1049 Brussels, Belgija) .

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

ASMENŲ APSAUGOS TVARKANT ASMENS DUOMENIS DARBO GRUPĖ,

įkurta 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB,

atsižvelgdama į minėtos direktyvos 29 ir 30 straipsnius,

atsižvelgdama į savo Darbo tvarkos taisykles,

PRIĖMĖ ŠIĄ NUOMONĘ:

SANTRAUKA

Darbo grupė palankiai vertina 2017 m. sausio 10 d. Europos Komisijos pasiūlymą dėl E. privatumo reglamento. Darbo grupė palankiai vertina tai, kad kaip norminis teisės aktas buvo **pasirinktas reglamentas**. Taip užtikrinama, kad taisyklės būtų vienodos visoje ES, o priežiūros institucijoms ir panašioms organizacijoms suteikiama daugiau aiškumo. Be to, padedama užtikrinti atitiktį Bendrajam duomenų apsaugos reglamentui (toliau – BDAR). Tokią atitiktį papildomai patvirtina sprendimas **tą pačią instituciją, atsakingą už stebėseną, kad būtų laikomasi BDAR**, paskirti atsakinga už e. privatumo taisyklių vykdymo užtikrinimą.

Kartu teigiamai vertintina tai, kad nuspręsta (išlaikyti) **papildomą teisės aktą**. Konfidencialių ryšių ir galinių įrenginių apsauga pasižymi konkrečiomis ypatybėmis, kurios BDAR nereglamentuotos. Todėl šio pobūdžio paslaugoms reikia papildomų nuostatų siekiant užtikrinti tinkamą pagrindinės teisės į ryšių privatumą ir konfidencialumą, įskaitant galinių įrenginių konfidencialumą, apsaugą. Šiuo klausimu darbo grupė aktyviai palaiko siūlomame reglamente pasirinktą **principinį požiūrį** taikyti **plačius draudimus ir siauras išimtis** ir **tikslingai taikyti sutikimo sąvoką**.

Darbo grupė palankiai vertina siūlomo reglamento taikymo srities išplėtimą siekiant **įtraukti viršstintkinių paslaugų (angl. *Over-The-Top*) teikėjus**; šios paslaugos funkcinio požiūriu prilygsta labiau tradicinėms ryšio priemonėms ir todėl turi tokią pačią galimybę paveikti žmonių privatumą ir teisę į ryšių slaptumą ES. Teigiama ir tai, kad siūlomas reglamentas aiškiai apima **turinį ir susijusius metaduomenis**, be to, jame pripažįstama, kad **metaduomenys gali atskleisti labai slaptus duomenis**.

Tačiau darbo grupė taip pat pažymi 4 aspektus, kurie jai kelia **didelį susirūpinimą**. Kalbant apie **galinių įrenginių buvimo vietos nustatymą, sąlygas, kuriomis leidžiama turinio ir metaduomenų analizę, numatytuosius galinių įrenginių ir programinės įrangos nuostačius, taip pat sekimo sienas** siūlomame reglamente BDAR numatytas apsaugos lygis būtų sumažintas. Šioje nuomonėje darbo grupė pateikia konkrečius siūlymus užtikrinti, kad E. privatumo reglamentu būtų užtikrintas tas pats arba didesnis apsaugos lygis, atitinkantis slaptą ryšių duomenų (turinio ir metaduomenų) pobūdį.

Kalbant apie **WiFi sekimą**, atsižvelgiant į duomenų rinkimo aplinkybes ir tikslus, gali būti, kad tokiam sekimui pagal BDAR reikalingas sutikimas arba jis galėtų vykti tik jeigu surinkti asmens duomenys yra anoniminami. Pastaruoju atveju būtina įvykdyti šias keturias sąlygas: duomenų rinkimo iš galinių įrenginių tikslas turi būti tik statistiniai skaičiavimai, sekimas laiko ir erdvės atžvilgiu turi būti tik toks, kiek tai yra būtina šiam tikslui pasiekti, iš karto po to duomenys turi būti ištrinti arba anoniminti, ir turi būti veiksminga galimybė atsisakyti. Europos Komisijos prašoma skatinti patvirtinti techninį mobiliųjų įrenginių standartą, kad būtų automatiškai nurodomas prieštaravimas dėl tokio sekimo.

Kalbant apie **turinio ir metaduomenų analizę**, atspirties taškas turėtų būti tai, kad ryšių duomenis draudžiama tvarkyti be visų galutinių paslaugų gavėjų (siuntėjų ir gavėjų) sutikimo. Kad paslaugų teikėjai galėtų teikti naudotojo aiškiai prašomas paslaugas, pavyzdžiui, paieškos ir indeksavimo funkcijos paslaugas arba teksto pavertimo kalba paslaugas,

nacionaliniu lygmeniu turi būti numatyta turinio ir metaduomenų tvarkymo išimtinai paties naudotojo asmeniniais tikslais išimtis.

Kalbant apie **sutikimą dėl sekimo**, darbo grupė ragina aiškiai uždrausti sekimo sienas, t. y. „sutik arba išėik“ tipo pasirinkimus, kai vartotojai verčiami sutikti su sekimu, jei nori gauti paslaugą.

Galiausiai darbo grupė rekomenduoja, kad galiniai įrenginiai ir programinė įranga **pagal numatytuosius nuostacius turėtų privatumo apsaugos nuostacius**, taip pat kad naudotojai turėtų aiškias galimybes patvirtinti arba pakeisti šiuos numatytuosius nuostacius diegimo metu. Naudojimo metu nuostaciai turi būti nesunkiai prieinami. Naudotojams turi būti sudarytos galimybės nurodyti konkretų sutikimą per savo naršyklės nuostacius. Privatumo pageidavimai turėtų apimti ne tik trečiųjų šalių įsikišimą ar slapukus. Darbo grupė primygtinai rekomenduoja nustatyti, kad būtų privaloma laikytis funkcijos „Nesekti“ standarto.

Darbo grupė taip pat nustatė kitus rūpimus klausimus, pavyzdžiui, susijusius su taikymo sritimi, galinių įrenginių apsauga ir tiesiogine rinkodara. Galiausiai darbo grupė nustatė klausimus, kuriuos reikėtų patikslinti, kad būtų geriau apsaugoti galutiniai paslaugų gavėjai ir visiems dalyvaujantiems suinteresuotiesiems subjektams būtų užtikrintas didesnis teisinis tikrumas.

TURINYS

1. ĮVADAS	6
2. TEIGIAMAI SIŪLOMO REGLAMENTO ASPEKTAI	6
<i>Derinimas visoje ES, baudų vienodinimas ir išimtinis duomenų apsaugos institucijų atliekamas vykdymo užtikrinimas.....</i>	<i>6</i>
<i>Taikymo srities išplėtimas, palyginti su E. privatumo direktyva.....</i>	<i>8</i>
<i>Tikslinis sutikimo sąvokos taikymas.....</i>	<i>10</i>
3. DIDELĮ SUSIRŪPINIMĄ KELIANTYS ASPEKTAI.....	10
<i>Pagal siūlomą reglamentą BDAR numatyta apsauga silpninama.</i>	<i>10</i>
4. KITI SUSIRŪPINIMĄ KELIANTYS KLAUSIMAI	16
<i>Reikėtų išplėsti teritorinę ir dalykinę taikymo sritį.....</i>	<i>16</i>
<i>Reikėtų stiprinti galinių įrenginių apsaugą</i>	<i>17</i>
<i>Tiesioginė rinkodara.....</i>	<i>21</i>
<i>Tvarkaraštis</i>	<i>23</i>
<i>Kiti susirūpinimą keliantys aspektai</i>	<i>23</i>
5. SIŪLYMAS PATIKSLINTI SIEKiant UŽTIKRINTI TEISINĮ TIKRUMĄ	26
<i>Taikymo srities patikslinimai.....</i>	<i>26</i>
<i>Paaiškinimai dėl sutikimo sąvokos ir taikymo</i>	<i>29</i>
<i>Patikslinimai dėl buvimo vietos ir kitų metaduomenų</i>	<i>30</i>
<i>Patikslinimai dėl neužsakytų pranešimų.....</i>	<i>31</i>
<i>Patikslinimai dėl pagrindinių teisių srities dokumentų taikymo</i>	<i>33</i>
<i>Kiti paaiškinimai.....</i>	<i>33</i>

1. ĮVADAS

1. 29 straipsnio darbo grupė (toliau – darbo grupė arba 29 straipsnio darbo grupė) palankiai vertina siūlomą Europos Komisijos (toliau – EK) E. privatumo reglamentą (toliau – siūlomas reglamentas arba E. privatumo reglamentas)¹, kuriuo siekiama pakeisti E. privatumo direktyvą².
2. Daug siūlomo reglamento aspektų yra teigiami ir Europos Komisija žengė svarbų žingsnį, pateikdama pasiūlymą dėl reglamento. Tačiau siūlomą reglamentą dar galima tobulinti. Taip būtų ne tik geriau apsaugoti galutiniai paslaugų gavėjai, bet ir visiems dalyvaujantiems suinteresuotiesiems subjektams būtų užtikrintas didesnis teisinis tikrumas.
3. Taigi darbo grupei kyla keli rūpimi klausimai ir ji norėtų pateikti keletą rekomendacijų dėl paaiškinimų, į kurias reikėtų atsižvelgti Europos Parlamentui ir ES Tarybai diskutuojant dėl siūlomo reglamento. Šioje nuomonėje pirmiausia bus apžvelgti teigiami siūlomo reglamento aspektai, o tada pažymėti susirūpinimą keliantys ir tikslintini klausimai.

2. TEIGIAMSI SIŪLOMO REGLAMENTO ASPEKTAI

DERINIMAS VISOJE ES, BAUDŲ VIENODINIMAS IR IŠIMTINIS DUOMENŲ APSAUGOS INSTITUCIJŲ ATLIEKAMAS VYKDYMO UŽTIKRINIMAS

4. Darbo grupė palankiai vertina tai, kad **kaip norminis teisės aktas buvo pasirinktas reglamentas**. Taip užtikrinama, kad taisyklės būtų vienodos visoje ES (su tam tikromis išimtimis, kurios aptariamos toliau). Taip suteikiamas aiškumas priežiūros institucijoms ir panašioms organizacijoms. Be to, atsižvelgiant į svarbų Bendrojo duomenų apsaugos reglamento (BDAR)³ vaidmenį siūlomame reglamente, tai padeda užtikrinti abiejų teisės aktų suderinamumą. Kartu teigiamai vertintina tai, kad **nuspręsta (išlaikyti) papildomą teisės aktą**. Konfidencialių ryšių ir galinių įrenginių apsauga pasižymi konkrečiomis ypatybėmis, kurios BDAR nereglamentuotos. Todėl, siekiant užtikrinti tinkamą šios pagrindinės teisės apsaugą, reikalingos papildomos nuostatos dėl šių paslaugų. Šiomis aplinkybėmis darbo grupė taip pat **pritaria siūlomame reglamente pasirinktam principiniam plačių draudimų ir siaurų**

¹ Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių), 2017/0003 (COD), url: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241.

² 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių) (OL L 201, 2002 7 31, p. 37–47, url: <http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=celex:32002L0058>).

³ 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) OL L 119/1, 2016 5 4, p. 1–88, url: <http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32016R0679>.

išimčių požiūriui ir mano, kad reikėtų vengti nustatyti neribotas išimtis pagal BDAR 6 straipsnį ir visų pirma pagal jo 6 straipsnio f punktą (teisėto intereso pagrindas).

5. Jei **tų pačių taisyklių vykdymą užtikrins ta pati institucija, atsakinga už stebėseną, kaip laikomasi BDAR**, bus toliau didinamas abiejų teisės aktų tarpusavio suderinamumas. Atsižvelgiant į asmens duomenų apsaugos ir ryšių bei galinių įrenginių konfidencialumo apsaugos tarpusavio ryšį, būtų naudinga, jei nuostatų vykdymą pagal siūlomą reglamentą būtų patikėta užtikrinti tai pačiai priežiūros institucijai, kuri užtikrina BDAR vykdymą (siūlomo reglamento 38 konstatuojamoji dalis ir 18 straipsnis). Be to, Europos Sąjungos Teisingumo Teismo (ESTT) jurisprudencijoje⁴ patvirtinta, jog labai svarbu, kad priežiūros institucija būtų nepriklausoma, kaip nurodyta Chartijos 7 straipsnyje. Tačiau praktiškai duomenų apsaugos institucijoms tektų daug papildomo darbo, bet nebūtų garantijos, kad tikslas bus pasiektas, jei nebūtų gautas papildomas biudžetas. Todėl duomenų apsaugos institucijos palankiai vertina siūlomo reglamento 38 konstatuojamąją dalį, kurioje pabrėžiama, kad kiekviena priežiūros institucija turėtų būti aprūpinta papildomais finansiniais ir žmogiškaisiais ištekliais, patalpomis ir infrastruktūra, kurie būtini naujajame reglamente jai numatytoms užduotims veiksmingai atlikti. Palankiai vertintina ir tai, kad 18 straipsnio 2 dalyje numatytas siūlomo reglamento priežiūros institucijų ir siūlomos Direktyvos, kuria nustatomas Europos elektroninių ryšių kodeksas (toliau –EERK)⁵, nacionalinių reguliavimo institucijų bendradarbiavimo teisinis pagrindas.
6. Atsižvelgiant į glaudų siūlomo reglamento ir BDAR tarpusavio ryšį, taip pat reikėtų palankiai vertinti tai, **kad siūlomame reglamente numatytos baudos būtų suderintos su BDAR**. Į siūlomo reglamento taikymo sritį patenkanti veikla yra gana konfidenciali, susijusi, be kita ko, su konfidencialių ryšių ir galinių įrenginių trikdymu. Baudų dydis turėtų atitikti šias konfidencialumo aplinkybes. Šios aplinkybės taip pat yra priežastis, dėl kurios derinimas visoje ES yra svarbus, kad visame regione būtų numatytas tas pats aukštas apsaugos lygis. Siūlomo reglamento 23 straipsnyje numatytos veiksmingos baudos už reglamento pažeidimus (panašaus dydžio baudos nustatytos už BDAR taisyklių pažeidimus, išskyrus kai kuriuos aspektus (žr. 38 pastabą).
7. Taip pat reikėtų palankiai vertinti tai, kad iš šio teisės akto **būtų išbrauktos konkrečios pranešimo apie duomenų pažeidimus taisyklės**, kad nebūtų nereikalingo dubliavimosi su BDAR duomenų pažeidimo reikalavimais.
8. **Palankiai vertintina ir tai, kad dabar daugiau dėmesio skiriama vienodo apsaugos lygio užtikrinimui visiems galutiniams paslaugų gavėjams**, nes

⁴ Žr., pvz., 2015 m. spalio 6 d. ETT sprendimo *Safe Harbour*, C-362/14, 41 punktą ir 2016 m. gruodžio 21 d. ETT sprendimo *Tele2 / Watson*, C-203/15 ir C-698/15, 123 punktą.

⁵ Pasiūlymas dėl Europos Parlamento ir Tarybos direktyvos, kuria nustatomas Europos elektroninių ryšių kodeksas (nauja redakcija), 2016/0288 (COD), 2016 10 12, url: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN.

siūlomame reglamente atsisakyta skirstymo į „abonentus“ ir kitus elektroninių ryšių paslaugų naudotojus.

TAIKYMO SRITIES IŠPLĖTIMAS, PALYGINTI SU E. PRIVATUMO DIREKTYVA

9. Darbo grupė palankiai vertina **siūlomo reglamento taikymo srities išplėtimą siekiant įtraukti virštinklinių paslaugų (angl. *Over-The-Top*) teikėjus**, – šios paslaugos funkcinio požiūriu prilygsta labiau tradicinėms ryšio priemonėms ir todėl vienodai gali paveikti ES piliečių privatumą ir teisę į ryšių slaptumą. Darbo grupė ypač palankiai vertina tai, kad visos virštinklinių paslaugų kategorijos (OTT0, OTT1 ir kai kurios OTT2)⁶ dabar patenka į reglamento taikymo sritį, nes jis apima ne tik tradicines ryšio priemones (OTT0), bet ir funkcinio požiūriu lygiavertes paslaugas (OTT1), kaip nurodyta siūlomo reglamento 8 straipsnio 1 dalies c punkte. Teigiama ir tai, kad, be EERK pateiktų apibrėžčių, įtraukiamos kai kurios OTT2 kategorijos, kai jomis užtikrinamas papildomas asmenų tarpusavio ir interaktyvus ryšys, neatsiejamas nuo atitinkamos paslaugos, pvz., žaidimuose, pasimatymų programėlėse ar apžvalgų interneto svetainėse (siūlomo reglamento 4 straipsnio 2 dalis). Be to, būtų naudinga **paaikškinti, kad apsauga taip pat taikoma įrenginių tarpusavio sąveikai**. 12 konstatuojamojoje dalyje paaikškinta, kad tarpusavio ryšį palaikantys įrenginiai patenka į siūlomu reglamentu suteikiamos apsaugos taikymo sritį. Tai pageidautina, nes tokie ryšiai paprastai apima privatumo teisių saugomą informaciją. Tačiau taikytinumą būtų galima patikslinti (žr. 40h pastabą).
10. Teigiama ir tai, kad **siūlomame reglamente aiškiai reglamentuotas turinys ir susiję metaduomenys**. 14 konstatuojamojoje dalyje paaikšinama, kad 4 straipsnio 3 dalies a punkte pateikta sąvoka „elektroninių ryšių duomenys“ apibrėžtis turėtų būti pakankamai plati, kad apimtų *visą* turinį ir susijusius metaduomenis, neatsižvelgiant į, pavyzdžiui, signalų perdavimo būdą. Tačiau darbo grupė kaip vieną iš susirūpinimų keliančių klausimų 39 pastaboje pažymi, kad esama sąvoka „elektroninių ryšių duomenys“ vis dar diskutuotina. Atsižvelgdama į šį taikymo srities išplėtimą, darbo grupė laikosi nuomonės, jog **pripažinimas, kad metaduomenys gali atskleisti labai slaptus duomenis** (žr. aiškinamojo memorandumo 2.2 punktą; 2 konstatuojamąją dalį), yra labai svarbus papildymas. Darbo grupė palankiai vertina tai, kad taip Europos Komisija atsižvelgia į ETT motyvus, kuriuos jis nurodė sprendimuose *Digital Rights Ireland* ir *Tele2 / Watson*. 29 straipsnio darbo grupė taip pat palankiai vertina **pripažinimą, kad turinio analizė yra didelį pavojų keliantis duomenų tvarkymas**. 19 konstatuojamojoje dalyje ir 6 straipsnio 3 dalies b punkte daroma logiška teisinė prielaida, kad pagal BDAR 35 straipsnį turinio skenavimas yra didelį pavojų keliantis duomenų tvarkymas ir, neatsižvelgiant į tai, ar yra likęs didelis pavojus, tam visada būtina iš anksto pasikonsultuoti su (pagrindine) duomenų apsaugos institucija. Tuo pat metu darbo grupė yra susirūpinusi sąvokos

⁶ Papildomai šios sąvokos paaikškintos BEREC, *Report on OTT Services*, BoR (16) 35, 2016 m. sausio 29 d., p. 15 ir 16, url: http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services. Taip pat reiktų atkreipti dėmesį į ataskaitos pastabą, kad šios kategorijos yra diskusijose dėl peržiūros vartotinos sąvokos, bet tai nėra teisinės sąvokos.

„metaduomenys“ taikymo sritimi ir tuo, kad metaduomenų analizei netaikomas tas pats privalomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą (žr. 33 ir 46 pastabas).

11. Taip pat būtų sveikintina ir toliau **pripažinti anoniminimo svarbą**. E. privatumo direktyvoje anoniminimo priemonės jau buvo numatytos siekiant užtikrinti suderinamumą (pvz., E. privatumo direktyvos 6 straipsnio 1 dalis, kurioje nurodyta, kad srauto duomenis reikia ištrinti arba pakeisti taip, kad taptų anoniminiais, kai šie duomenys nebėra reikalingi pranešimui perduoti). Siūlomo reglamento 6 straipsnio 2 dalies c punkte ir 6 straipsnio 3 dalies b punkte metaduomenų ir turinio tvarkymo draudimo išimtis leidžiama esant sutikimui, jeigu atitinkamo tikslo ar tikslų „nebūtų galima pasiekti tvarkant anonimine paverstą informaciją“. Reikalaujant tokių privatumo apsaugos priemonių, o ne tik prašant naudotojų sutikimo, šie naudotojai apsaugomi nuo neleistino tvarkymo. Tačiau darbo grupė taip pat yra labai susirūpinusi tuo, kad tokios anoniminimo technikos nereikėtų taikyti norint susekti naudotojų buvimo vietą per jų mobiliuosius įrenginius (žr. 17 pastabą). Be to, net jei būtų taikomos anoniminimo priemonės, paslaugų teikėjai visada turėtų atlikti poveikio duomenų apsaugai vertinimą (toliau – PDAV) (žr. 33 ir 46 pastabas) ir darbo grupė ragina nustatyti papildomą įpareigojimą paviesti, kaip duomenys yra anoniminami ir apibendrinami (žr. 42b pastabą).
12. Kitas teigiamas aspektas yra **plati galinių įrenginių apsaugos formuluotė**. 20 konstatuojamojoje dalyje ir 8 straipsnyje apibrėžiama, kad technologijos, naudojamos prieigai prie galinių įrenginių, nėra reikšmingos: bet kokiam galinių įrenginių trikdymui, įskaitant jos duomenų tvarkymo galimybių naudojimą, reikalingas galutinio paslaugų gavėjo sutikimas (taikant tam tikras išimtis). Dabar EK jau yra patvirtinusi, kad ši nuostata taikoma „įrenginių identifikavimui“. Be to, darbo grupė palankiai vertina tai, kad, jei trečioji šalis nesilaiko asmens **naršyklės nuostačiuose nurodytų pasirinkčių, tuo galima remtis** imantis vykdymo užtikrinimo priemonių tos trečiosios šalies atžvilgiu, kaip aprašyta 22 konstatuojamojoje dalyje. Tai padeda tais atvejais, kai trečioji šalis (pvz., reklamos tinklas) nesilaiko šių nuostatių. Tačiau tai turėtų būti įtvirtinta ir atitinkamoje siūlomo reglamento nuostatoje.
13. Galiausiai palankiai vertintina tai, kad **į siūlomo reglamento taikymo sritį ir toliau būtų įtraukti juridiniai asmenys** (žr. aiškinamojo memorandumo 2.2 punktą, 3, 33 ir 42 konstatuojamąsias dalis, 1, 15 straipsnius ir 16 straipsnio 5 dalį). Taip jau yra pagal E. privatumo direktyvą, tačiau kadangi duomenų apsaugos institucijoms bus pavesta užtikrinti naujų taisyklių įgyvendinimą, naudinga tai konkrečiai pabrėžti. Taip duomenų apsaugos institucijos gali imtis veiksmų tais atvejais, kai juridiniai asmenys nukenčia nuo pažeidimo, pvz., kai įmonės gauna brukalą arba kai jų ryšiai slapta stebimi. Tačiau darbo grupė taip pat pažymi, jog jai kelia susirūpinimą tai, kad sutikimo taikymas juridiniams asmenims nėra aiškus (žr. 41a pastabą) ir neaišku, ką reiškia juridinių asmenų „teisėtas interesas“ tiesioginės rinkodaros atveju (žr. 43c pastabą).

14. Darbo grupė palankiai vertina ir kitus patobulinimus, susijusius su sutikimo sąvokos taikymu ir aiškinimu. Pirmą, būtų pravartu **paaikškinti, kad interneto prieiga ir (mobilioji) telefonija yra būtinosios paslaugos ir kad šių paslaugų teikėjai negali „priversti“ savo klientų sutikti su bet koku duomenų tvarkymu, kuris nėra reikalingas pačiai būtinajai paslaugai teikti.** 18 konstatuojamojoje dalyje visų pirma pažymėta, kad pagrindinės prieigos prie plačiajuosčio interneto ir balso ryšio paslaugos turi būti laikomos būtinosiomis paslaugomis, o tai, atsižvelgiant į žmonių priklausomybę nuo prieigos prie šių paslaugų, reiškia, kad sutikimas, kad jų ryšio duomenys būtų tvarkomi tokiais papildomais tikslais (pvz., kad duomenys būtų tvarkomi reklamos arba rinkodaros tikslais) negali galioti. Tuo pat metu darbu grupei kelia susirūpinimą tai, kad šis paaikškinimas yra pernelyg ribotas. Kai kurių virštinklinių paslaugų teikėjų paslaugos taip pat gali būti laikomos būtinosiomis, ir E. privatumo reglamente taip pat reikėtų konkrečiai uždrausti „suteik arba išėm“ pobūdžio pasirinkimus kitomis aplinkybėmis (žr. 20 pastabą).
15. Be to, teigiama tai, kad **sutikimo įtraukti fizinių asmenų asmens duomenis į abonentų knygas reikalavimas yra suderintas.** Pagal siūlomo reglamento 15 straipsnį tvarkyti duomenis viešosiose abonentų knygose leidžiama tik fiziniams asmeniui sutikus, o jei tai juridinis asmuo, turi būti suteikta galimybė nesutikti dėl tokio tvarkymo. Tai išsamiau reglamentuota 31 konstatuojamojoje dalyje, kurioje pažymėta, kad šis sutikimas turi būti konkretus, t. y. kokių konkrečių kategorijų asmens duomenys turi būti įtraukti į abonentų knygą. Tačiau darbo grupė reiškia susirūpinimą, jog siūlomame reglamente galėtų būti aiškiau reglamentuota, kad paieškai ir atgalinei paieškai reikės konkrečiau, atskiro sutikimo (žr. 37 pastabą).
16. **Nauja tikslinė išimtis, taikoma neinvaziniam galinių įrenginių trikdymui,** taip pat būtų sveikintina. 29 straipsnio darbo grupė mano, jog siūlomame reglamente būtų naudinga paaikškinti, kad draudimas netaikomas duomenų srauto matavimui (pagal siaurą išimtį, kad tokį matavimą atlieka informacinės visuomenės paslaugų teikėjas, galutiniam paslaugų gavėjui paprašius, žr. siūlomo reglamento 8 straipsnio 1 dalies d punktą). Papildomai žr. 21 konstatuojamąją dalį. Tačiau darbo grupė siūlo vartoti technologijų požiūriu neutralią apibrėžtį ir paaikškinti šios išimties taikytinumą (žr. 25 pastabą).

3. DIDELĮ SUSIRŪPINIMĄ KELIANTYS ASPEKTAI

PAGAL SIŪLOMĄ REGLAMENTĄ BDAR NUMATYTA APSAUGA SILPNINAMA.

Kaip minėta, siūlomame reglamente yra keli svarbūs patobulinimai. Tačiau esama ir tam tikrų aspektų, dėl kurių kyla didesnis ar mažesnis susirūpinimas. Šiame skirsnyje darbo grupė aptaria keturis klausimus, kurie jai kelia **didelį susirūpinimą**. Tai yra nuostatos, kuriomis **silpninamas pagal BDAR suteikiamos apsaugos lygis**.

17. **Reglamente numatyti įpareigojimai susekti galinių įrenginių buvimo vietą turėtų atitikti BDAR reikalavimus.** Siūlomo reglamento 8 straipsnio 2 dalies b punkte reikalaujama tik rodyti pranešimą ir įgyvendinti saugumo priemonės, kad būtų renkama galinių įrenginių siunčiama informacija. 8 straipsnio 2 dalies b punkte papildomai pažymima, kad už šios informacijos rinkimą atsakingas asmuo turi nurodyti visas priemones, kurių gali imtis galutiniai paslaugų gavėjai, kad sustabdytų informacijos rinkimą arba kuo labiau sumažintų to rinkimo mastą. Taip 8 straipsnio 2 dalies b punkte sudaromas įspūdis, kad organizacijos gali rinkti galinių įrenginių siunčiamą informaciją siekdamos susekti fizinį asmenų judėjimą (pvz., *WiFi* sekimas arba *Bluetooth* sekimas) be atitinkamo asmens sutikimo. Šiuos duomenis renkanti šalis tikriausiai galėtų įvykdyti šį reikalavimą pateikdama pranešimą naudotojams, kad jie galėtų išjungti savo įrenginius, kai nenori būti sekami. Toks požiūris prieštarautų pagrindiniam Europos Komisijos telekomunikacijų politikos tikslui už nedidelę kainą visiems europiečiams teikti greitą interneto ryšį, taikant griežtas privatumo apsaugos priemones tarp valstybių.

Be to, siūlomame reglamente nenustatomi jokie aiškūs apribojimai, susiję su duomenų rinkimo apimtimi ar paskesne duomenų tvarkymo veikla. Šiomis aplinkybėmis reikėtų pažymėti, kad šie MAC adresai yra asmens duomenys, net ir po to, kai imtasi saugumo priemonių. Nenustatant papildomų reikalavimų ar apribojimų, šių asmens duomenų apsaugos lygis pagal siūlomą reglamentą yra gerokai mažesnis nei pagal BDAR, pagal kurį toks sekimas turėtų būti sąžiningas, teisėtas ir skaidrus. 25 konstatuojamojoje dalyje netikslingai pažymima, kad kai kurios *WiFi* sekimo funkcijos nekelia didelio pavojaus privatumui, o kitos, pvz., asmenų sekimas laikui bėgant – kelia. Nors darbo grupė vertina pripažinimą, kad toks sekimas kelia didelį pavojų privatumui, nėra prasmės iš anksto spręsti, kad kai kurios kitos funkcijos tokio pavojaus nekelia, papildomai neįvertinus aplinkybių ir duomenų tvarkymo proporcingumo. Tokį vertinimą reikėtų atlikti atsižvelgiant į toliau nurodytas sąlygas, susijusias su neanonimintu *WiFi* sekimu.

Atsižvelgiant į duomenų rinkimo aplinkybes ir tikslus, tikėtina, kad sekimui pagal BDAR atlikti būtinas sutikimas arba jis galėtų vykti tik jeigu surinkti asmens duomenys yra anoniminami. Pageidautina, kad šie duomenys būtų anoniminami iš karto po jų surinkimo. Jei duomenų neįmanoma iš karto anoniminti atsižvelgiant į jų rinkimo tikslus, duomenys gali būti tvarkomi tam tikrą laiką ir neanonimiškai, jeigu yra įvykdomos toliau nurodytos sąlygos: i) duomenų rinkimo tikslas yra tik statistiniai skaičiavimai (žr. toliau pateiktus pavyzdžius); ii) duomenų sekimas laiko ir erdvės atžvilgiu yra tik toks, kiek tai yra griežtai būtina šiam tikslui; iii) iš karto po to duomenys ištrinami arba anoniminami ir iv) turi būti veiksminga galimybė atsisakyti. Žinoma, visomis aplinkybėmis duomenų valdytojai turi laikytis reikalavimo teikti tinkamą informaciją.

Darbo grupei kelia susirūpinimą tai, kad galimas siūlymas asmeniškai atsisakyti duomenų rinkimo, kurį atlieka šiuos duomenis renkanti organizacija, sukeltų nepriimtina naštą piliečiams, nes ir privačiojo, ir viešojo sektoriaus organizacijos vis dažniau diegia tokias sekimo technologijas. Todėl darbo grupė ragina Europos teisės aktų leideją skatinti kurti įrenginių techninius standartus, kad įrenginiai automatiškai

praneštų apie nesutikimą dėl tokio sekimo, ir kad būtų galima užtikrinti tokio pranešimo reikalavimo laikymąsi.

Pavyzdžiui, tikėtina, kad sutikimo pagal BDAR reikės, jei duomenų valdytojas renka ir saugo netiesiogiai identifikuojamus (*WiFi* arba *Bluetooth*) įrenginių MAC adresus ir apskaičiuoja naudotojo buvimo vietą, kad susektų jo buvimo vietą laikui bėgant, pavyzdžiui, įvairiose parduotuvėse. Taip visų pirma yra tuo atveju, kai toks sekimas vykdomas viešose vietose, kur naudotojai gali pagrįstai tikėtis, kad jie nebus identifikuojami ar sekami, kai yra renkami praeivių MAC adresai. Tokį sutikimą galima gauti, pavyzdžiui, naudojant programėlę, kuria naudotojams siūloma leisti sekti jų buvimo vietą konkrečiose vietovėse mainais už komercinius pasiūlymus, siūlant registracijos taškus konkrečiose vietose arba naudojant sutikimo modulį *WiFi* viešojo belaidžio interneto zonose.

Tik ribotomis aplinkybėmis duomenų valdytojams gali būti leidžiama tvarkyti galinių įrenginių siunčiamą informaciją siekiant sekti jų fizinį judėjimą be atitinkamo asmens sutikimo. Pavyzdžiui, taip gali būti skaičiuojant klientus konkrečioje vietoje arba renkant siunčiamus duomenis abiejose saugumo patikros posto pusėse siekiant rodyti laukimo laiką. Tačiau abiem atvejais duomenis reikėtų ištrinti ir anoniminti iš karto po to, kai gali būti pasiektas statistinis tikslas. Tai reiškia, kad lankytojų įrenginių MAC adresai konkrečioje vietoje, pavyzdžiui, parduotuvėje, turi būti anoniminti iš karto po surinkimo, nuolat nesaugant MAC adresų, ir taip, kad nebūtų įmanoma techniškai iš naujo identifikuoti duomenų. Skaičiuojant laukimo laiką, MAC adresus reikėtų ištrinti arba anoniminti iš karto po to, kai jie tampa nebesvarbūs laukimo laikui apskaičiuoti (pvz., todėl, kad lankytojas jau yra kitoje saugumo patikros posto pusėje arba jau išėjo iš eilės).

Be to, duomenų valdytojui reikėtų įvykdyti duomenų kiekio mažinimo reikalavimus (pvz., sekimas negali vykti visą parą be poilsio dienų, kai jo tikslas susijęs tik su parduotuvės darbo valandomis ir (arba) imčių sudarymu tam tikrais intervalais). Duomenų valdytojais taip pat turi imtis kitų švelninimo priemonių siekdami užtikrinti, kad nebūtų daromas poveikis naudotojų privatumo teisėms arba kad šis poveikis būtų labai nedidelis, pavyzdžiui, siekiant apsaugoti šalia duomenų rinkimo centro gyvenančių asmenų privatumą.

Tai, kad siūlomo reglamento 8 straipsnio 2 dalyje pasirinktas tik pranešimo reikalavimas, dar labiau stebina, atsižvelgiant į 20 konstatuojamosios dalies išvadą, kad informacija, susijusi su galutinių paslaugų gavėjų įrenginiu, taip pat gali būti renkama nuotoliniu būdu siekiant identifikuoti ir sekti, ir kad toks duomenų tvarkymas, kaip nurodyta siūlomame reglamente, gali labai apriboti šių galutinių paslaugų gavėjų privatumą. Be to, šis įpareigojimas nėra platesnis už BDAR 13 ir 14 straipsniuose jau numatytą informavimo įpareigojimą. Privatumą dėl sekimo dar labiau riboja tai, kad su renkamais duomenimis gali susipažinti kiti asmenys, pvz., teisėsaugos institucijos gali nustatyti galutinių paslaugų gavėjų tapatybę remdamiesi saugomais MAC adresais, kuriuos transliuoja jų mobilieji įrenginiai.

18. Reikia išsamiau išdėstyti sąlygas, kuriomis leidžiama analizuoti turinį ir metaduomenis

Siūlomo reglamento 6 straipsnyje metaduomenims ir turiniui suteikiami skirtingi apsaugos lygiai. 29 straipsnio darbo grupė nepritaria šiam skirtumui: abiejų kategorijų duomenys yra itin slapti. Todėl metaduomenims ir turiniui reikėtų suteikti tą patį aukštą apsaugos lygį. Taigi atspirties taškas turėtų būti tai, kad metaduomenis ir turinį būtų draudžiama tvarkyti be visų galutinių paslaugų gavėjų (t. y. siuntėjo ir gavėjo) sutikimo.

Vis dėlto, atsižvelgiant į aplinkybes, tam tikrus duomenis gali būti leidžiama tvarkyti be sutikimo, jei tai yra griežtai būtina tokiais tikslais:

- Paslaugų teikėjai gali tvarkyti elektroninių ryšių duomenis siūlomo reglamento 6 straipsnio 1 dalies a ir b punktuose, 2 dalies a ir b punktuose nurodytais tikslais⁷.
- Reikėtų paaiškinti, kad kai kurios brukalo aptikimo ir (arba) filtravimo bei botneto mažinimo technikos taip pat gali būti laikomos griežtai būtinomis siekiant nustatyti arba nutraukti piktnaudžiavimą elektroninių ryšių paslaugomis (6 straipsnio 2 dalies b punktas). Kalbant apie brukalo filtravimą, brukalą gaunantiems galutiniams paslaugų gavėjams, jei tai techniškai įmanoma, turėtų būti siūloma išsamiai nurodytų atsisakymo galimybių.
- Reikėtų paaiškinti, kad elektroninių ryšių duomenų analizei klientų aptarnavimo tikslais taip pat gali būti taikoma išimtis, kai „tai būtina sąskaitai pateikti“ (žr. 6 straipsnio 2 dalies b punktą). Atitinkami metaduomenys gali būti laikomi iki laikotarpio, per kurį pagal nacionalinę teisę galima teisėtai ginčyti sąskaitą arba reikalauti mokėjimo. Atitinkami duomenys (pvz., URL) gali būti saugomi tik galutinio paslaugų gavėjo prašymu ir tik tokį laikotarpį, kuris yra griežtai būtinas ginčui dėl sąskaitos išspręsti (tai reiškia, kad 7 straipsnio 3 dalį reikėtų iš dalies pakeisti).
- Turi būti įmanoma tvarkyti elektroninių ryšių duomenis siekiant teikti galutinio paslaugų gavėjo aiškiai prašomas paslaugas, pavyzdžiui, paieškos arba raktinių žodžių indeksavimo funkciją, virtualiųjų padėjų, teksto pavertimo kalba sistemų ir vertimo paslaugas. Tam reikia nustatyti tokių duomenų analizės išimtį išimtinai asmeniniam (namų ūkio) naudojimui, taip pat individualiam, su darbu susijusiam naudojimui⁸. Todėl tai būtų įmanoma be visų galutinių paslaugų gavėjų sutikimo, tačiau tik paslaugos prašančiam galutiniam paslaugų gavėjui sutikus. Toks konkretus sutikimas taip pat neleistų paslaugų teikėjui naudoti šių duomenų kitais tikslais.

⁷ Kalbant apie būtinybę įvykdyti privalomuosius paslaugų kokybės reikalavimus, kaip nurodyta siūlomo reglamento 6 straipsnio 2 dalies a punkte, paslaugų teikėjai turėtų atsižvelgti į Reglamento (ES) 15/2120 (EERK), ypač 3 straipsnyje ir 10 ir 13–15 konstatuojamosiose dalyse nurodytas sąlygas. Pagal šią nuostatą paslaugų teikėjų gali būti reikalaujama tvarkyti ryšių duomenis siekiant nustatyti ir filtruoti kenkimo ir sekimo programinę įrangą ir jiems gali būti leidžiama suspausti duomenis.

⁸ Nors siūlomo reglamento 13 konstatuojamojoje dalyje bendrovių tinklai akivaizdžiai nepatenka į reglamento taikymo sritį, ši nauja asmeninio naudojimo išimtis taip pat turėtų būti siejama su darbuotojų naudojamomis debesijos paslaugomis su darbu susijusiais tikslais, pvz., atliekant paiešką jų e. pašte.

Tai reiškia, kad norint atlikti turinio ir (arba) metaduomenų analizę visais kitais tikslais, pvz., analizės, profiliavimo, vartotojų elgesiu grindžiamos reklamos ar kitais tikslais, kuriais paslaugų teikėjas siekia komercinės naudos, reikalingas visų galutinių paslaugų gavėjų, kurių duomenys būtų tvarkomi, sutikimas. Kalbant apie tokias situacijas, siūlomame reglamente reikėtų paaiškinti, kad vien e. laiško išsiuntimas ar kitoks asmeninis pranešimas naudojant kitą paslaugą galutiniam paslaugų gavėjui, kuris asmeniškai sutiko, kad jo turinys ir metaduomenys būtų tvarkomi (pvz., registruodamasis dėl pašto paslaugos), nelaikomas galiojančiu siuntėjo sutikimu.

Galiausiai reikėtų paaiškinti, kad kitų asmenų nei galutiniai paslaugų gavėjai duomenų tvarkymas (pvz., trečiojo asmens atvaizdas ar aprašymas, kuriuo keičiasi du asmenys) taip pat turi atitikti visas atitinkamas BDAR nuostatas.

19. Galiniai įrenginiai ir programinė įranga turi pagal numatytuosius nuostačius neleisti ir uždrausti neteisėtą jos trikdymą ir teikti informaciją apie galimybes.

Nors siūlomame reglamente programinės įrangos, kuri naudojama elektroniniams ryšiams, tiekėjai įpareigojami numatyti „galimybę“ neleisti galinių įrenginių tam tikros formos trikdymo, o diegimo metu programinės įrangos tiekėjai įpareigojami reikalauti, kad galutinis paslaugų gavėjas duotų su nuostačiu susijusį sutikimą (10 straipsnio 1 ir 2 dalys), toks pasirinkimas neprilygsta *standartizuotajai privatumo apsaugai*. Be to, „galimybė“ neleisti tam tikro trikdymo numatyta jau dabar ir iki šiol neleistino sekimo problema dar nėra pakankamai išspręsta. Būtent todėl rengiant BDAR buvo priimtas sąmoningas politinis sprendimas nustatyti duomenų apsaugos ir integruotosios apsaugos bei standartizuotosios privatumo apsaugos principus (BDAR 25 straipsnis). Siūlomame reglamente šių principų nesilaikoma kalbant apie ryšių ir įrenginių duomenis. Radijo įrangos direktyvoje 2014/53/ES⁹ (nurodyta 10 konstatuojamojoje dalyje) numatytas tik labai ribotas saugumo įpareigojimas, reikalaujant, kad į radijo įrangą būtų įdiegtos „naudotojo asmens duomenų ir privatumo apsaugai užtikrinti skirtos apsaugos priemonės“ (3 straipsnio 3 dalies e punktas). Tai negali pakeisti konkrečių numatytųjų privatumo apsaugos nuostačių pagal siūlomą reglamentą. Šiuo klausimu taip pat pažymėtina, kad 2016 m. gruodžio mėn. paskelbtoje Eurobarometro apklausoje dėl e. privatumo pažymima, jog „beveik septyni iš dešimties respondentų (69 proc.) visiškai sutinka, kad pagal numatytuosius jų naršyklės nuostačius reikėtų nutraukti dalijimąsi jų informacija“¹⁰. Darbo grupei taip pat susirūpinimą kelia naršyklės nuostačiai ir sąvokos „trečiosios šalys“ apibrėžtis. Žr. 24 pastabą. Be to, reikėtų turėti omenyje, kad ši nuostata susijusi ne tik su kompiuteriuose naudojamomis naršyklėmis, bet ir kitų rūšių programine įranga, kuri leidžia palaikyti ryšį (įskaitant operacines sistemas, programėles ir programinės įrangos sąsajas įrenginiams, prijungtiems prie daiktų interneto). Apibendrinant pažymėtina, kad galiniai įrenginiai ir programinė įranga turi *standartizuotai* turėti privatumo apsaugos nuostačius ir diegimo metu naudotojai turėtų būti nukreipiami į konfigūracijos meniu, jei norima nukrypti nuo šių numatytųjų nuostačių. Šie konfigūracijos meniu turėtų būti visada nesunkiai prieinami naudojimo metu. Darbo

⁹ Radijo įrangos direktyva 2014/53/ES.

¹⁰ Žr. *Flash Eurobarometer 443*, E. privatumo ataskaita (paskelbta 2016 m. gruodžio mėn.), p. 5.

grupė ragina Europos teisės aktų leidėją šiuo tikslu patikslinti 10 straipsnio taikymo sritį.

20. **E. privatumo reglamente reikėtų aiškiai uždrausti sekimo sienas**, t. y. kai prieiga prie interneto svetainės ar paslaugos neleidžiama, jei asmenys nesutinka būti sekami kitose interneto svetainėse ar teikiant kitas paslaugas. Kaip jau pažymėta ankstesnėse darbo grupės nuomonėse dėl E. privatumo direktyvos¹¹, tokie „sutik arba išėik“ pobūdžio metodai retai būna teisėti¹². Kai naudojant galinių įrenginių tvarkymo arba saugojimo pajėgumus arba renkant informaciją iš galutinių paslaugų gavėjų galinių įrenginių sudaromos galimybės ilgą laiką arba teikiant kelias paslaugas (pvz., skirtingose interneto svetainėse ar naudojant skirtingas programėles) sekti naudotojo veiklą, tokia duomenų tvarkymo veikla gali smarkiai riboti šių paslaugų gavėjų privatumą. Kadangi internetas yra labai svarbus suteikiant galimybę naudotis saviraiškos laisve, įskaitant teisę gauti informaciją, asmens galimybė gauti internete esantį turinį neturėtų priklausyti nuo sutikimo dėl veiklos sekimo įvairiuose įrenginiuose ir interneto svetainėse ar programėlėse. Todėl būsimame E. privatumo reglamente reikėtų nurodyti, kad prieiga prie turinio, pvz., interneto svetainėse ir programėlėse, neturėtų priklausyti nuo sutikimo dėl tokios invazinės duomenų tvarkymo veiklos, neatsižvelgiant į taikomą sekimo technologiją, kaip antai slapukus, įrenginių identifikavimą, unikaliųjų identifikatorių įdiegimą ar kitus stebėjimo būdus. Šio draudimo būtinybė pažymėta neseniai atliktoje Eurobarometro apklausoje dėl e. privatumo, kurioje nurodyta, kad „beveik du trečdaliai respondentų teigia esant nepriimtina, kad jų veikla internete yra stebima mainais už neribotą prieigą prie tam tikros interneto svetainės (64 proc.)“.

21. Apibendrinant pažymėtina, kad kalbant apie pirmiau nurodytus keturis aspektus, **turėtų būti įvykdytas siūlomame reglamente duotas pažadas užtikrinti vienodą ar didesnę apsaugos lygį nei BDAR**. 5 konstatuojamojoje dalyje užtikrintai pažymima, kad siūlomu reglamentu nesumažinamas BDAR numatytas apsaugos lygis. Tačiau, atsižvelgiant į tokį siūlomą reglamentą, koks jis yra dabar, tai neatitinka tikrovės, visų pirma kalbant apie įrenginių sekimą (17 pastaba), standartizuotosios privatumo apsaugos principo nebuvimą (19 pastaba) ir sutikimą (18 pastaba). Tai visų pirma yra svarbu, kaip pažymėta toje pat konstatuojamojoje dalyje, kad siūlomas reglamentas bus „BDAR *lex specialis*, kuriame patikslinamos ir papildomos BDAR nuostatos dėl asmens duomenimis laikomų elektroninių ryšių duomenų“. Darbo grupė siūlo E. privatumo reglamento tekste patikslinti bent tokius dalykus:

i) kad E. privatumo reglamente numatytiems draudimams turėtų būti teikiama pirmenybė prieš leidimus pagal BDAR (pvz., E. privatumo reglamento 5 straipsnyje numatytas trikdymo draudimas būtų viršesnis už elektroninių ryšių paslaugų teikėjų teises toliau tvarkyti asmens duomenis pagal BDAR 5 straipsnio 1 dalies b punktą ir 6 straipsnio 4 dalį);

ii) kai duomenis leidžiama tvarkyti esant bet kuriai draudimų išimčiai (įskaitant sutikimą) pagal E. privatumo reglamentą, šis duomenų tvarkymas,

¹¹ Žr., pvz., WP 240 (E. privatumo apžvalga), p. 16; WP 208 (sutikimo išimtis), p. 5.

¹² Ši pozicija neturi poveikio BDAR 7 straipsnio 4 daliai, pagal kurią kitose situacijose, kai tai yra tinkama, taip pat gali būti draudžiami „sutik arba išėik“ pobūdžio pasirinkimai.

jei jis susijęs su asmens duomenimis, vis vien turi atitikti atitinkamas BDAR nuostatas;

iii) kai duomenis leidžiama tvarkyti pagal bet kurią E. privatumo reglamente numatytą draudimų išimtį, bet koks kitas duomenų tvarkymas pagal BDAR draudžiamas, įskaitant duomenų tvarkymą kitais tikslais remiantis BDAR 6 straipsnio 4 dalimi. Taip nebūtų užkirstas kelias duomenų valdytojams prašyti papildomo sutikimo naujoms duomenų tvarkymo operacijoms. Be to, teisės aktų leidėjui nebūtų draudžiama E. privatumo reglamente numatyti papildomų, ribotų ir konkrečių išimčių, pavyzdžiui, leisti tvarkyti duomenis mokslo ar statistikos tikslais pagal BDAR 89 straipsnį arba apsaugoti asmenų „gyvybinius interesus“ pagal BDAR 6 straipsniod punktą.

Be to, E. privatumo reglamentą reikėtų aiškinti taip, kad juo būtų suteikiama tokia pati arba prirėkus aukštesnio lygio apsauga nei pagal BDAR.

4. KITI SUSIRŪPINIMĄ KELIANTYS KLAUSIMAI

Be pirmiau minėtų aspektų, 29 straipsnio darbo grupei kelia susirūpinimą toliau nurodyti aspektai.

REIKĖTŲ IŠPLĖSTI TERITORINĘ IR DALYKINĘ TAIKymo SRITĮ

22. Sąvoka „metaduomenys“ yra pernelyg siaurai apibrėžta. Dabar 4 straipsnio c punkte jie apibrėžiami kaip „elektroninių ryšių tinkle tvarkomi duomenys elektroninių ryšių turiniui perduoti, platinti ar juo keistis (pabraukta dokumento autoriaus). Vartojant žodį „tinklas“ išreiškiama nuostata, kad metaduomenimis būtų laikomi tik tie duomenys, kurie gaunami teikiant paslaugas „žemesniame“ tinklo lygyje. Tai galėtų reikšti, kad teikiant virštinklinę paslaugą gauti duomenys nebūtų laikomi metaduomenimis. Tai būtų nepageidautina, be to, tikriausiai, to ir neketinta daryti, atsižvelgiant į ketinimą išplėsti siūlomo reglamento taikymo sritį, įtraukiant virštinklinių paslaugų teikėjus. Siekiant spręsti šį klausimą, reikėtų iš dalies pakeisti elektroninių ryšių metaduomenų sąvoką, kad būtų įtraukti visi duomenys, tvarkomi siekiant perduoti, platinti elektroninių ryšių turinį arba juo keistis.

23. Be to, nerimą kelia tai, kad **teritorinė siūlomo reglamento taikymo sritis organizacijų, neturinčių padalinio ES, atžvilgiu apima tik elektroninių ryšių paslaugų teikėjus**. Pagal siūlomą reglamentą elektroninių ryšių paslaugų teikėjas, kuris nėra įsisteigęs ES, turi raštu paskirti atstovą Sąjungoje (3 straipsnio 2 dalis). 9 konstatuojamojoje dalyje taip pat paminėta, kad reglamentas būtų taikomas elektroninių ryšių paslaugų teikėjų atliekamam duomenų tvarkymui, neatsižvelgiant į duomenų tvarkymo vietą. Darbo grupė palankiai vertina šį paaiškinimą. Tačiau, kadangi nuostatos tekste nurodyti tik elektroninių ryšių paslaugų teikėjai, neaišku, kiek ši teritorinė taikymo sritis taikoma kitoms šalims (pvz., šalims, kurios trikdė arba renka galutinių paslaugų gavėjų galinių įrenginių perduodamą informaciją (žr. siūlomo reglamento 3 straipsnio 1 dalies c punktą ir 8 straipsnį). Todėl darbo grupė siūlo iš dalies pakeisti 3 straipsnio 2 ir 5 dalis siekiant įtraukti viešai prieinamų abonentų knygų paslaugų teikėjus, programinės įrangos, kuri reikalinga elektroniniams ryšiams, tiekėjus, ir asmenis, siunčiančius tiesioginės rinkodaros

komercinius pranešimus arba renkančius (kitą) informaciją, susijusią su galutinių paslaugų gavėjų galiniais įrenginiais arba saugomą šiuose įrenginiuose, jei jų veikla yra nukreipta į ES esančius naudotojus (žr. siūlomo reglamento 8 konstatuojamąją dalį)¹³.

REIKĖTŲ STIPRINTI GALINIŲ ĮRENGINIŲ APSAUGĄ

Kitas susirūpinimą keliantis aspektas siūlomame reglamente yra nepakankama galinių įrenginių apsauga.

24. Pirmą, **siūlomame reglamente neteisingai nurodoma, kad galiojantis sutikimas gali būti duotas per nespecialiuosius naršyklės nuostačius**. Darbo grupė pripažįsta, kad galutiniai paslaugų gavėjai šiuo metu yra pernelyg apkrauti prašymais duoti sutikimą (22 konstatuojamoji dalis). Naršyklės (ir panašios programinės įrangos) nuostačiai atlieka tam tikrą vaidmenį sprendžiant šią problemą. Tačiau, kadangi bendrieji naršyklės nuostačiai neskirti taikyti sekimo technologijos taikomajai programėlei vienu atskiru atveju, jie nėra tinkami sutikimui duoti pagal BDAR 7 straipsnį ir 32 konstatuojamąją dalį (nes sutikimas nėra pakankamai pagrįstas informacija ir nėra pakankamai konkretus).

Galutinis paslaugų gavėjas turi galėti duoti atskirą sutikimą dėl sekimo per interneto svetainę arba programėlę skirtingais tikslais (pvz., dalijimosi informacija socialinėje žiniasklaidoje arba reklamos tikslais). Duomenų valdytojas, atsakingas už kelias interneto svetaines arba programėles, gali taip pat prašyti sutikimo dėl visų kitų programėlių svetainių, kurias jis kontroliuoja, jei šis prašymas dėl sutikimo pateikiamas atskirai.

Be to, duomenų valdytojas turi įvykdyti visus kitus įpareigojimus, susijusius su sutikimu, įskaitant įpareigojimą teikti tinkamą informaciją naudotojams. Kalbant ir apie naršykles, ir apie duomenų valdytojus, tai reiškia, kad jei jie siūlytų tik vieną galimybę „sutikti su visais slapukais“, sutikimas negaliojotų, nes taip naudotojai negalėtų pateikti reikalaujamo išsamaus sutikimo. Tačiau naršyklėse turėtų būti galimybė leisti naudotojams informuotai ir sąmoningai nuspręsti sutikti su visais slapukais ir taip užkirsti kelią visiems būsimiems konkretiems prašymams dėl sutikimo, pateikiamiems jų lankomose interneto svetainėse.

Darbo grupė primygtinai rekomenduoja E. privatumo reglamente nustatyti, kad naršyklėse būtų privaloma įdiegti techninius mechanizmus, kaip antai funkcijos „Nesekti“ (angl. *Do Not Track*) standartą, siekiant užtikrinti, kad naudotojams būtų suteikta reali pasirinkimo galimybė ir galimybė kontroliuoti jų įrenginių trikdymą¹⁴.

¹³ Žr. BDAR 3 straipsnio 2 dalį. „Šis reglamentas taikomas asmens duomenų tvarkymui, kai Sąjungoje esančių duomenų subjektų asmens duomenis tvarko Sąjungoje neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas ir duomenų tvarkymo veikla yra susijusi su: a) prekių arba paslaugų siūlymu tokiems duomenų subjektams Sąjungoje, nepaisant to, ar už šias prekes arba paslaugas duomenų subjektui reikia mokėti; arba b) elgesio, kai jie veikia Sąjungoje, stebėseną.“ Ši pareiga taip pat galėtų apimti išimtis, kaip nurodyta BDAR 27 straipsnio 2 dalyje.

¹⁴ Žr. URL: <https://www.w3.org/TR/tracking-compliance/>. 7 punkte paaiškintas išimties modelis ir skirtumas tarp išimčių, taikomų visai interneto svetainei, ir išimčių, taikomų visam žiniatinklui. 6 punkte pateikiama kompiuterio skaitoma informacija, kurią duomenų valdytojai gali teikti, kiek tai susiję su informavimo reikalavimu siekiant gauti sutikimą.

Dar svarbiau yra tai, kad E. privatumo reglamentu reikėtų užtikrinti, kad visi duomenų valdytojai pasirinkimą ir dėl informacijos saugojimo įrenginyje, ir dėl funkcijos „Nesekti“ signalo iš naršyklės pripažintų teisiškai privaloma sutikimo arba atsisakymo išraiška. Tai neturi poveikio kitoms darbo grupės rekomendacijoms dėl atitikties funkcijos „Nesekti“ standartui, be kita ko, tikslo ribojimo principui, kai standartas bus baigtas rengti (tai numatoma padaryti 2017 m. pabaigoje).

Numanomos „sutikimo“ rūšys, pvz., spustelėjimas ant interneto svetainės arba naršymas tinklalapyje, negali būti svarbesni už sprendimus dėl saugojimo ir funkcijos „Nesekti“ signalo. Šį standartą naudinga naudoti todėl, kad jis taikomas ne tik slapukų sekimo technologijai, bet ir kitų rūšių sekimui, pvz., įrenginių identifikavimui.

Nustačius, kad šio standarto teisiškai privaloma laikytis, būtų išspręsta ir kita problema, esamame 10 straipsnyje vartojant sąvoką „trečiosios šalys“. Interneto svetainėje arba programėlėje paprastai yra daug elementų ir iš pačios interneto svetainės, ir išorinių elementų. Išorinis kodas taip pat gali veikti lankantis interneto svetainėje, o iš jos informacija pateikiama trečiosios šalies serveriui. Sekimo slapuką gali pateikti pirmoji šalis, kai naudotojas apsilanko, pvz., socialinių tinklų svetainėje. Ši socialinių tinklų svetainė taip pat galėtų būti trečioji šalis, kai šis naudotojas lankosi kitoje interneto svetainėje, kurioje vyksta sąveika su ta socialinių tinklų svetaine. Visais šiais atvejais, neatsižvelgiant į tai, ar jie susiję su informacijos „prieiga“, ar „saugojimu“ galutinio paslaugų gavėjo įrenginyje, tai yra įrenginio trikdymas, kuriam yra reikalingas sutikimas (nebent taikoma viena iš išimčių). Pagal funkcijos „Nesekti“ standartą vartojamos sąvokos „visos interneto svetainės“ ir „viso interneto“. Todėl, siekiant pagerinti visų suinteresuotųjų subjektų teisinį tikrumą, E. privatumo reglamente pateikta nuoroda į „trečiąsias šalis“ turėtų būti performuluota ir apimti visus subjektus, su kuriais sąveikauja įrenginys (nes jie išsaugo informaciją įrenginyje arba gauna ją).

Kad funkcijos „Nesekti“ standartas taptų suderinamas su aukštu pagal Chartiją suteikiamos pranešimų konfidencialumo ir duomenų apsaugos lygiu, E. privatumo reglamente reikėtų nurodyti, kad prašymus dėl sekimo visame internete, priešingai nei prašymus dėl sekimo visoje interneto svetainėje, reikia pateikti atskirai ir naudotojai turėtų galėti laisvai priimti arba atmesti šiuos prašymus. Be to, siekiant apsaugoti naudotojus nuo dažnų prašymų duoti sutikimą, E. privatumo reglamente reikėtų užtikrinti, kad atsisakymas sutikti dėl konkrečios organizacijos vykdomo sekimo visame internete (taikant funkcijos „Nesekti“ standartą arba per atskirą juodąjį sąrašą) šiai organizacijai bent 6 ateinančius mėnesius neleidžiama pateikti prašymų duoti sutikimą. Ši taisyklė nedraudžia šiai organizacijai, tiesiogiai apsilankius naudotojui (t. y. kaip pirmajai šaliai) prašyti sutikimo savo pačios interneto svetainėje (t. y. prašyti sutikimo, susijusio su visa interneto svetaine). Praktiškai tai reiškia, kad, pavyzdžiui, vaizdo transliavimo svetainė, kurioje įdiegti sekimo slapukai, gali prašyti sutikimo, kai šis naudotojas lankosi vaizdo transliavimo svetainėje, tačiau gali nebeprašyti šio sutikimo 6 mėnesius nuo tos dienos, kai šis naudotojas atsisakė sutikti ir lankosi kitose interneto svetainėse, kuriose pateikiami vaizdai, gauti iš transliavimo interneto svetainės.

25. Be to, **išimtis, taikoma „interneto svetainės lankomumui apskaičiuoti“, suformuluota netiksliai.** Siūlomo reglamento 8 straipsnio 1 dalies d punkte numatyta

išimtis, taikoma interneto svetainės lankomumo apskaičiavimui. Pirmasis susirūpinimą keliantis aspektas yra tas, kad ši sąvoka yra neapibrėžta ir gali būti painiojama su naudotojo profiliavimu. Pateikiant apibrėžtį reikėtų paaiškinti, kad ši išimtis negali būti taikoma jokiais profiliavimo tikslais. Išimtis turėtų būti taikoma tik naudojimo analizei, kuri yra būtina siekiant išanalizuoti naudotojo prašomos paslaugos teikimo rezultatus, bet ne naudotojo analizei (t. y. interneto svetainės, programėlės arba įrenginio nustatomos tapatybės naudotojų elgsenos analizei). Todėl išimties negalima taikyti tais atvejais, kai duomenis galima susieti su nustatomos tapatybės naudotojų duomenimis, kuriuos tvarko paslaugų teikėjas ar kiti duomenų valdytojai. Be to, jos aprašymas rodo, kad ši išimtis susijusi su labai konkrečia technologija. Todėl sąvoką „svetainės lankomumo apskaičiavimas“ reikėtų apibrėžti iš naujo, technologškai neutraliu būdu, kad ji apimtų panašią analitiniam naudojimui skirtą informaciją, gautą iš programėlių, nešiojamųjų įrenginių ir daiktų interneto prietaisų.

Darbo grupė siūlo semtis įkvėpimo iš Nyderlanduose galiojančios išimties, taikomos, jei tai griežtai būtina, siekiant gauti informaciją apie suteiktos informacinės visuomenės paslaugos techninę kokybę arba veiksmingumą ir neturi jokio poveikio arba turi nedidelį poveikį atitinkamo abonento arba galutinio paslaugos gavėjo arba naudotojo privatumui (žr. Nyderlandų telekomunikacijų įstatymo 11 straipsnio 7a dalies 3 punkto b papunktį). Šia išimtimi atsižvelgiama į tai, kad dauguma taikant interneto arba programėlių analizę surinktų duomenų vis vien yra asmens duomenys. Tai reiškia, kad šių duomenų tvarkymui taip pat taikomas BDAR. Tai, pavyzdžiui, reiškia, kad naudojimo analizę taip pat galėtų atlikti išorinė organizacija, tačiau tik jeigu:

- i) ši organizacija veikia kaip duomenų tvarkytoja;
- ii) sudaromas susitarimas dėl BDAR atitinkančio duomenų tvarkymo;
- iii) taikoma analizės technologija neleidžia pakartotinio identifikavimo, įskaitant, be kita ko, naudotojų IP adresų anoniminimą;
- iv) konkretus slapukas (-ai) ar kiti analizei naudojami duomenys gali būti naudojami tik šiai konkrečiai interneto svetainei, programėlei ar nešiojamajam įrenginiui ir negali būti susiejami su kitais identifikuojamais duomenimis;
- v) naudotojai turi teisę atsisakyti (taip pat žr. šios nuomonės 17 ir 50 pastabas).

Net jei sutikimo nebūtų reikalaujama, jei šios sąlygos būtų įvykdytos, duomenų valdytojai vis vien privalo teikti naudotojams tinkamą informaciją, pvz., funkcijos „Nesekti“ standarto sekimo būsenos laukeliuose¹⁵.

26. E. privatumo reglamente **reikėtų užtikrinti siauras ir tiksliai suformuluotas išimtis dėl sutikimo reikalavimų**. Sutikimo dėl įrenginių trikdymo reikalavimo išimties formuluotė 8 straipsnio 1 dalies c punkte beveik atitinka esamą E. privatumo direktyvos 5 straipsnio 3 dalies formuluotę; „būtiniais atvejais teikti informacinės visuomenės paslaugas, kurių aiškiai paprašo abonentas ar naudotojas“, tačiau svarbiausias žodis „griežtai“ praleistas, nepateikiant jokio paaiškinimo. Tai kelia susirūpinimą dėl dviejų priežasčių. Pirma, priežiūros institucijos ir organizacijos jau

¹⁵ Žr. Tracking Preference Expression (DNT), 2016 m. kovo 7 d. redaktoriaus projektas.

plačiai diskutavo dėl E. privatumo direktyvos nuostatos taikymo srities, o išbraukus žodį „griežtai“ teisinio tikrumo būtų dar mažiau. Tai kelia susirūpinimą ir todėl, kad darbo grupė jau yra pateikusi rekomendaciją dėl sąvokos „griežtai“ siauro aiškinimo šiomis aplinkybėmis. Darbo grupė savo nuomonėje dėl slapukams taikomos reikalavimo gauti sutikimą išimties (WP 194) pateikė tokį paaiškinimą:

„Slapukas yra griežtai būtinas siekiant suteikti konkrečią funkciją naudotojui (arba abonentui): jei slapukai išjungiami, funkcija nebus prieinama ir naudotojas arba abonentas jos aiškiai prašė kaip informacinės visuomenės paslaugos.“¹⁶

Be to, darbo grupė paaiškina, kad:

„trečiosios šalies“ slapukai paprastai naudojami atvejais, kurie nėra būtini naudotojui, besilankančiam interneto svetainėje, nes tokie slapukai paprastai susiję su paslauga, kuri nėra ta paslauga, kurios naudotojas „aiškiai paprašė“¹⁷.

Darbo grupė pridūrė, kad socialinių papildinių, skirtų ne platformos ar interneto svetainės naudotojams, naudojimas taip pat nebūtų laikomas griežtai būtinu.

Be to, nors siūlomo reglamento 6 straipsnio 1 dalies b punkte elektroninių ryšių duomenis leidžiama tvarkyti „jei tai būtina“ saugumo sumetimais, BDAR 49 konstatuojamojoje dalyje reikalaujama, kad tai būtų griežtai būtina. Galbūt žodis „griežtai“ praleistas sąmoningai, nes siūlomo reglamento 21 konstatuojamojoje dalyje minima, kad sutikimo dėl trikdymo neturėtų būti reikalaujama, jei tai yra „griežtai“ būtina. Vis dėlto siūlomame reglamente numatyta galimybė papildomai paaiškinti, kad būtinumo kriterijus taikant šį reglamentą turėtų būti aiškinamas siaurai visų išimčių atžvilgiu. Todėl darbo grupė siūlo, kiek tai susiję su visomis siūlomo reglamento 6 straipsnio ir 8 straipsnio 1 dalies išimtimis, prieš žodį „būtina“ įrašyti žodį „griežtai“.

Kita vertus, E. privatumo reglamente reikėtų aiškiai leisti trikdyti įrenginius siekiant įdiegti saugumo naujinius. Saugumo atnaujinimų siuntimas internetu yra pageidaujamas būdas diegti saugumo naujinius daugelyje galutinių paslaugų gavėjų įrenginių. Naujinių diegimas laikomas galinių įrenginių trikdymu. Yra teisėtas interesas užtikrinti, kad šių įrenginių saugumas būtų atnaujinamas. Saugumo pataisų teikėjas paprastai turėtų galėti įdiegti griežtai būtinus saugumo naujinius, negavęs galutinio paslaugų gavėjo sutikimo. Tačiau neaišku, ar šiam trikdymui gali būti taikoma trikdymo draudimo išimtis, susijusi su informacine visuomene (8 straipsnio 1 dalies c punktas). Reikėtų paaiškinti, kad, taikant šią išimtį, saugumo naujinius diegti leidžiama, tačiau tik jei i) saugumo naujiniai yra tinkamai sudėti į paketus ir niekaip nekeičia įrenginių programinės įrangos funkcijų (įskaitant sąveiką su kita programine įranga ar naudotojo pasirinktus nuostačius), ii) galutiniam paslaugų gavėjui iš anksto pranešama kiekvieną kartą, kai yra diegiamas naujinys, ir iii) galutinis paslaugų gavėjas gali išjungti automatinį šių naujinių diegimą.

¹⁶ 29 straipsnio darbo grupė, WP 294, Nuomonė 04/2012 dėl slapukams taikomos reikalavimo gauti sutikimą išimties, priimta 2012 m. birželio 7 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_lt.pdf.

¹⁷ Ten pat.

TIESIOGINĖ RINKODARA

Kiti susirūpinimą keliantys klausimai susiję su nepakankama apsauga nuo tiesioginės rinkodaros.

27. Pirma, susirūpinimą kelia tai, kad **tiesioginės rinkodaros taikymo sritis yra pernelyg ribota**. Siūlomo reglamento 4 straipsnio 3 dalies f punkte tiesioginės rinkodaros pranešimai apibrėžiami kaip „bet kokios formos raštiška ar žodinė reklama, siunčiama vienam ar keliems nustatytos arba nustatomos tapatybės galutiniams elektroninių ryšių paslaugų gavėjams“. Žodžio „siunčiama“ vartojimas reiškia technologinių ryšių priemonių naudojimą, kuris neišvengiamai apima pranešimo perdavimą, o reklama internete (per socialinės žiniasklaidos platformas arba interneto svetainėse) paprastai neapima reklamos „siuntimo“ siaurąja prasme. Tai taip pat matyti iš šioje apibrėžtyje pateiktų pavyzdžių (SMS, e. paštas) ir 33 konstatuojamojoje dalyje. Visa tai yra gana tradicinės rinkodaros komunikacijos formos, bet skambinimo sistemų – gana tradicinių – naudojimas vis tiek veikiausiai nepatenka į siūlomo reglamento taikymo sritį. Straipsnį ir konstatuojamąją dalį reikėtų iš dalies pakeisti siekiant įtraukti visą reklamą, *išsiųstą, nukreiptą arba pateiktą* vienam ar keliems nustatytos arba nustatomos tapatybės galutinių paslaugų gavėjams. Be to, reikėtų užtikrinti ir tai, kad elgsena grindžiama reklama (pagrįsta galutinių paslaugų gavėjų profiliais) taip pat būtų laikoma tiesioginės rinkodaros pranešimais, siunčiamais „vienam ar keliems nustatytos arba nustatomos tapatybės galutiniams elektroninių ryšių paslaugų gavėjams“ (nes tokia reklama yra skirta konkrečioms nustatomos tapatybės naudotojams).

Be to, pagal siūlomą „tiesioginės rinkodaros pranešimų“ taikymo sritį 16 straipsnio 1 dalyje numatyta apsauga apimtų pranešimus, kuriuose pateikta reklaminė medžiaga, ir asmenys nebūtų saugomi nuo kitų pranešimų, siunčiamų, nukreipiamų arba pateikiamų rinkodaros tikslais (pvz., siunčiant pranešimus potencialių vartotojų ratui nustatyti, kai prašoma sutikimo, propaguojant politines pažiūras ar balsavimo pasirinkimus, remiant labdaros arba kitas ne pelno organizacijas, vykdančias bendrą organizacijos prekės ženklo kūrimą). Be to, kaip tiesioginės rinkodaros būdas vis dar naudojami fakso aparatai, nors apibrėžtyje jie nepaminėti. Todėl į 4 straipsnio 3 dalies f punktą reikėtų įtraukti visų formų reklamą, agitaciją arba pardavimų skatinimą, taip pat ir kiek tai sietina su ne pelno organizacijomis, ir, be e. pašto ir SMS, reikėtų aiškiai įtraukti fakso aparatus (taip pat žr. siūlymą paaiškinti 43 pastabos a punkte). Galiausiai 32 konstatuojamojoje dalyje nurodyta, kad tiesioginė rinkodara apima politinių partijų pranešimus, siunčiamus savo partijai reklamuoti. Šią nuostatą reikėtų atnaujinti, įtraukiant politikus ir rinkimų kandidatus, reklamuojančius savo kandidatūrą.

28. Antra, **sutikimo dėl tiesioginės rinkodaros atšaukimas nėra nemokamas, be to, jį lengviau duoti nei atšaukti**. Galimybę atšaukti sutikimą pagal siūlomą reglamentą reikėtų paaiškinti siekiant užtikrinti nuoseklumą ir gerinti gavėjų apsaugą. Siūlomo reglamento 16 straipsnio 6 dalyje šiuo metu numatyta, kad tiesioginės rinkodaros gavėjams būtina pateikti „reikiamą informaciją, kad gavėjai galėtų pasinaudoti savo

teise lengvai atšaukti savo sutikimą gauti papildomų rinkodaros pranešimų“. Tai patvirtinta ir 34 konstatuojamojoje dalyje. Tačiau iš BDAR 70 konstatuojamosios dalies darytina išvada, kad duomenų subjektai pagal BDAR turėtų ne tik teisę nesunkiai prieštarauti dėl duomenų tvarkymo tiesioginės rinkodaros tikslais, bet ir daryti tai „nemokamai“. Ši sąvoka taip pat vartojama siūlomo reglamento 16 straipsnio 2 dalyje, tačiau tik dėl tiesioginės rinkodaros atsisakymo pagal kontaktinius duomenis, gautus pardavimo metu.

BDAR 7 straipsnio 3 dalyje numatyta, kad atšaukti sutikimą turi būti lygiai taip pat lengva, kaip ir jį duoti, ir kad asmenys turėtų galėti bet kada atšaukti savo sutikimą. Be to, darbo grupė išvadoje 04/2010 dėl FEDMA (WP 174) dėl Europos tiesioginės rinkodaros asociacijų federacijos (FEDMA) jau pripažino, kad svarbu, jog būtų siūlomas „paprastas, veiksmingas, nemokamas, tiesioginis ir nesunkiai prieinamas būdas atsisakyti gauti“ elektroninius komercinius pranešimus¹⁸. Šį sutikimo atšaukimo standartą reikėtų įtraukti į siūlomame reglamente pateiktas tiesioginės rinkodaros taisykles. Tas pats pasakytina apie BDAR 7 straipsnio 3 dalį, kad bet kada atšaukti sutikimą turėtų būti taip pat lengva, kaip ir jį duoti.

29. Atsižvelgiant į tai, **reikėtų patikslinti, kaip atšaukti sutikimą gauti tiesioginės rinkodaros skambučius arba kaip jų atsisakyti.** Pagal siūlomo reglamento 16 straipsnio 4 dalį valstybės narės gali pasirinkti balso ir balso rinkodaros skambučių atsisakymo tvarką. E. privatumo reglamente reikėtų nurodyti sutikimo gauti tiesioginės rinkodaros skambučius atšaukimo ir tokių skambučių atsisakymo tvarką. 36 konstatuojamojoje dalyje nurodyta, kad valstybės narės turėtų galėti nustatyti naujas ir (arba) toliau taikyti esamas nacionalines atsisakymo sistemas. Taigi pagal šią nuostatą valstybės narės netgi galėtų sudaryti tokias sąlygas, kai naudotojui reikėtų atsisakyti pavienių ryšių paslaugų teikėjų paslaugų. Šitaip naudotojai neapsaugomi nuo neužsakytų pranešimų¹⁹ ir neužtikrinamas BDAR atitinkantis mechanizmas, kad būtų galima nesunkiai ir bet kada atšaukti sutikimą. Todėl reglamente reikėtų nurodyti, kad kiekviena valstybė narė *privalo* sukurti nacionalinį registrą „Neskambinti“ (angl. *Do Not Call*). Be to, reglamente reikėtų nurodyti, kad neautomatizuotų skambučių gavėjams turėtų būti suteiktos dvi galimybės atšaukti sutikimą: dėl būsimų šios bendrovės ar organizacijos skambučių ir dėl galimybės šių skambučių metu užregistruoti nacionaliniame registre „Neskambinti“.

30. Kitas susirūpinimą keliantis klausimas yra tas, kad **nėra aiškiai draudžiama naudoti suklastotą tapatybę siunčiant tiesioginės rinkodaros pranešimus.** 34 konstatuojamojoje dalyje pažymėta, kad „būtina uždrausti slėpti tapatybę ir naudoti suklastotą tapatybę, suklastotus atgalinius adresus arba numerius“. Tačiau 16

18 29 straipsnio darbo grupė, WP 174, Nuomonė 04/2010 dėl Europos tiesioginės rinkodaros asociacijų federacijos (FEDMA) Europos elgesio kodekso dėl asmens duomenų naudojimo tiesioginei rinkodarai, 2010 m. liepos 13 d., url: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp174_lt.pdf.

¹⁹ Pavyzdžiui, Jungtinėje Karalystėje telekomunikacijų operatorius BT užregistravo 31 mln. erzinančių skambučių per savaitę. Žr. <http://www.bbc.com/news/business-38635921>.

straipsnio 4 dalyje nurodyta tik tai, kad galutiniams paslaugų gavėjams turi būti pranešama apie „juridinio arba fizinio asmens, kurio vardu perduodamas pranešimas, tapatybę“. Ši pareiga informuoti gavėjus apie tapatybę turėtų būti papildyta aiškiu draudimu tiesioginės rinkodaros tikslais naudoti paslėptus arba suklastotus kontaktinius adresus.

31. Šis aspektas susijęs su kita problema: **reikalavimas naudoti prefiksą tiesioginės rinkodaros skambučiams pateikiamas kaip reikalavimo suteikti galimybę nustatyti ryšio liniją alternatyva**. Pagal 16 straipsnio 3 dalį tiesioginės rinkodaros skambučiai leidžiami, jei skambintojas arba i) nurodo linijos, kuria su juo galima susisiekti, identifikacinius duomenis (16 straipsnio 3 dalies a punktas), arba ii) nurodo specialų kodą arba prefiksą, rodantį, kad skambutis yra rinkodaros skambutis (16 straipsnio 3 dalies b punktas). Nors darbo grupė palankiai vertina 16 straipsnio 3 dalies b punkte nustatytą įpareigojimą naudoti prefiksą, ji mano, kad šiuo reikalavimu neišsprendžiamas tas pats klausimas, kuris sprendžiamas 16 straipsnio 3 dalies a punkte nustatant įpareigojimą suteikti galimybę nustatyti ryšio liniją. Nors prefikso reikalavimu siekiama leisti gavėjui iš anksto nustatyti, kad tai yra rinkodaros skambutis (ir įdiegti šių skambučių blokavimo priemones), reikalavimu suteikti galimybę nustatyti ryšio liniją siekiama suteikti gavėjams (ir priežiūros institucijoms) priemones identifikuoti rinkodaros iniciatorių ir susisiekti su juo. Tai visų pirma svarbu kalbant apie automatizuotus skambučius, kai tarp rinkodaros teikėjo galimybių siųsti erzinančius skambučius ir gavėjo galimybių išvengti šių skambučių yra didelis disbalansas. Taigi reikalavimai turėtų būti ne alternatyvūs, o papildyti vienas kitą.

TVARKARAŠTIS

32. 29 straipsnio darbo grupė palankiai vertina tai, kad Europos Komisija pripažino, jog būtina, kad siūlomas reglamentas įsigaliotų kartu su BDAR 2018 m. gegužės mėn., siekiant išvengti abiejų teisės aktų nesuderinamumų. Tačiau vis dar kelia nerimą tai, kad tai yra plataus užmojo grafikas, o tam taip pat reikia baigti rengti EERK projektą. Todėl 29 straipsnio darbo grupė prašo visų teisėkūros procese dalyvaujančių suinteresuotųjų subjektų išsipareigoti dėl 2018 m. gegužės mėn. termino.

KITI SUSIRŪPINIMĄ KELIANTYS ASPEKTAI

Šiame skyriuje aptariami įvairūs papildomi susirūpinimą keliantys klausimai.

33. Pirma, 29 straipsnio darbo grupei susirūpinimą kelia **siūlymas, kad yra priimtinos netikslinės duomenų saugojimo priemonės**. Aiškinamajame memorandume pažymima, kad pagal siūlomą reglamentą valstybės narės gali nevaržomai toliau taikyti arba kurti nacionalines duomenų saugojimo sistemas, kuriose, *inter alia*, numatytos tikslinės duomenų saugojimo priemonės (1.3 punktas). Po Sprendimo *Tele2 / Watson*²⁰ tapo aišku, kad duomenų saugojimo sistemos, kurias taikant

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

numatytas tik tikslinis duomenų saugojimas, pagal Chartiją draudžiamos (ir net tokiu atveju joms taikomos svarbios sąlygos, pvz., priežiūra) ir kad bendro pobūdžio prieiga prie metaduomenų turi būti laikoma pažeidžiančia 7 straipsnio esmę taip pat kaip ir bendro pobūdžio prieiga prie elektroninio pranešimo turinio (žr. ESTT sprendimą *Schrems* ir 94 konstatuojamąją dalį). Taigi šio sakinio formuluotė rodo tam tikrą valstybių narių diskreciją, susijusią su duomenų saugojimo priemonėmis, kurios nėra. Kalbant apie tai, siūlomame reglamente **metaduomenims nesuteikiamas pakankamas apsaugos lygis**. Kaip pažymėta 10 pastaboje, 29 straipsnio darbo grupė palankiai vertina pripažinimą, kad metaduomenys gali atskleisti labai slaptus duomenis. Tačiau siūlomame reglamente metaduomenims nesuteikiama apsauga, kurią turėtų lemti toks pripažinimas. Atsižvelgiant į metaduomenų slaptumą, visų pirma prieš atliekant analizę pagal 6 straipsnio 2 dalies c punktą, reikėtų atlikti poveikio duomenų apsaugai vertinimą (PDAV) (taip pat žr. 46 pastabą).

34. Antra, **siūlomame reglamente būtų nepageidautinai išplėstos galimybės saugoti duomenis**. Siūlomo reglamento 11 straipsnyje aprašant tikslus, dėl kurių valstybės narės gali riboti reglamento 5–8 straipsniuose numatytus įpareigojimus, nurodomi BDAR 23 straipsnio 1 dalies a–e punktai. BDAR tokių apribojimų, susijusių su specialiosiomis duomenų kategorijomis, atsižvelgiant į didelę riziką duomenų subjektams, nenumatyta. Nors E. privatumo direktyvos 15 straipsnyje panašus apribojimas šiuo metu leidžiamas, tikslai yra labiau apriboti. Pagal naująją siūlomą reglamentą nauji apribojimai bus galimi siekiant „baudžiamųjų sankcijų vykdymo, įskaitant apsaugą nuo grėsmių visuomenės saugumui ir jų prevenciją, tikslais“ (BDAR 23 straipsnio 1 dalies d punktas) ir atsižvelgiant į „kitus Sąjungos ar valstybės narės svarbius tikslus, susijusius su bendrais viešaisiais interesais, visų pirma svarbiu ekonominiu ar finansiniu Sąjungos ar valstybės narės interesu, įskaitant pinigų, biudžeto bei mokesčių klausimus, visuomenės sveikatą ir socialinę apsaugą“ (BDAR 23 straipsnio 1 dalies e punktas). Šie tikslai ne tik yra nauji, palyginti su E. privatumo direktyva, bet ir 23 straipsnio 1 dalies d punkte nurodytas tikslas bei visas 23 straipsnio 1 dalies e punkto tikslas suformuluoti labai plačiai. Todėl siūloma išbraukti nuorodą į BDAR 23 straipsnio 1 dalies a–e punktus ir vietoj to paminėti tik tuos tikslus, kurie dabar minimi E. privatumo direktyvos 15 straipsnyje.

35. **Pareigos informuoti naudotojus apie pavojų saugumui taikymo sritis yra labai siaura**. Darbo grupė palankiai vertina tai, kad paslaugų teikėjai privalo pranešti naudotojams apie pavojų saugumui ir priemones šiam pavojui šalinti, pvz., šifravimą (17 straipsnis ir 37 konstatuojamoji dalis). Tačiau nuostatos pavadinimas yra „Informacija apie nustatytą pavojų saugumui“. Tai, kad pavadinime kalbama apie nustatytą pavojų, leidžia manyti, kad ši nuostata susijusi tik su (galimais) saugumo pažeidimais, nors pačios nuostatos tekstas ir konstatuojamoji dalis labiau rodo bendrą galutinių paslaugų gavėjų švietimą. Pavyzdžiui, jei paslaugų teikėjas nustato, kad naudotojo įrenginys yra užkrėstas kenkimo programine įranga ir tapo botneto dalimi, atrodo, kad šioje nuostatoje nustatomas tiesioginis įpareigojimas paslaugų teikėjui pranešti naudotojui apie su tuo susijusias grėsmes. Tačiau šios nuostatos taikymo sritį būtų galima patikslinti ir įtraukti ne vien šį atvejį. Ši nuostata turėtų apimti bent nustatytas visų galutiniam paslaugų gavėjui užsisakant abonementą pateiktų įrenginių, pvz., maršruto parinktuvų ir mobiliųjų įrenginių, keliamą pavojų saugumui,

į ją turėtų būti įtrauktas švietimas apie grėsmes, kylančias pakeitus nuostacius, kurie pagal integruotosios privatumo apsaugos principą yra sureguliuoti siekiant apsaugoti privatumą.

Darbo grupė rekomenduoja šią taikymo sritį išplėsti ir apimti programinės įrangos, kuri reikalinga elektroniniams ryšiams, tiekėjus (žr. 8 konstatuojamąją dalį) ir galbūt įtraukti naują – labai svarbių ryšių apsaugos technologijų tiekėjų, kurie nėra paslaugų teikėjai (pvz., šifravimo technologijos tiekėjų), – kategoriją. Jei taikymo sritis būtų šitaip išplėsta, reikėtų atkreipti dėmesį, kad šis įpareigojimas nesutampa su kitose priemonėse, pvz., TIS direktyvoje²¹ ir kitose teisės aktuose, susijusiuose su sertifikatu teikėjais, nustatytais įpareigojimais pranešti apie saugumo pažeidimus. Kadangi pastarosios technologijų tiekėjų kategorijos atstovai paprastai neturi tiesioginio ryšio su galutiniais paslaugų gavėjais, taip pat reikėtų paaiškinti, kaip jie gali įvykdyti informavimo įpareigojimą pagal šią nuostatą.

36. Darbo grupė palankiai vertina 2 ir 13 straipsnių nuostatas, kurios bus taikomos su numeriu siejamoms asmenų tarpusavio ryšio paslaugoms. Tačiau nėra iš karto aišku, kodėl **panašaus lygio privatumo apsaugos nebūtų galima suteikti funkcinio požiūriu lygiavertėms virštinklinėms skambinimo paslaugoms**.
37. Darbo grupei taip pat kelia nerimą tai, kad **trūksta aiškumo dėl išsamaus sutikimo dėl atgalinės paieškos abonentų knygoje**. Siūlomo reglamento 15 straipsnio 2 dalyje reikalaujama, kad paslaugų teikėjai gautų galutinių paslaugų gavėjų sutikimą prieš aktyvindami su duomenimis susijusias paieškos funkcijas (taip pat žr. 31 konstatuojamąją dalį). Darbo grupė palankiai vertina tai, kad yra suderintas sutikimo dėl įtraukimo į abonentų knygas reikalavimas, tačiau apgailestauja, kad sutikimas nėra pakankamai išsamus dėl įvairių paieškos rūšių. Pagal esamą E. privatumo direktyvą valstybėms narėms leidžiama reikalauti atskiro sutikimo dėl atgalinės paieškos pagal 12 straipsnio 3 dalį. Šiame straipsnyje nurodyta, jog „valstybės narės gali reikalauti, kad tais atvejais, kai viešuoju abonentų sąrašu siekiama daugiau nei tik suteikti galimybę ieškoti asmens kontaktinių duomenų pagal jo vardą ir pavardę ir, jei reikia, kai kuriuos kitus minimalius identifikatorius, būtų prašoma papildomo abonentų sutikimo“. Pagal šią nuostatą daugelyje valstybių narių dėl atgalinės paieškos funkcijų reikalaujama atskiro sutikimo, atsižvelgiant į skirtingus identifikavimo galimybių lygius ir todėl abiejų funkcijų trikdymo galimybes.
38. Vertinant formaliu, **baudų už visus reglamento pažeidimus dydis nėra suderintas**. Siūlomame reglamente valstybės narės turi nustatyti taisykles dėl baudų už siūlomo reglamento 23 straipsnio 4 ir 6 dalių bei 24 straipsnio pažeidimus. Būtų nuosekliau, jei to būtų reikalaujama ir pačiame E. privatumo reglamente.
39. Galiausiai **siūlomas reglamentas grindžiamas sąvokų apibrėžtimis, kurios gali tapti „judančiais taikiniais“**. Kalbant apie įvairias esmines siūlomo reglamento

²¹ 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti, OL L 194, 2016 7 19, p. 1–30, url: http://eur-lex.europa.eu/legal-content/LT/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

sąvokas, jame nurodomas kitas teisės aktas, kuris šiuo metu dar rengiamas: siūlomas EERK (pvz., žr. 4 straipsnio 1 dalies b punktą). Du svarbūs šio aspekto pavyzdžiai yra sąvokos „galutinis paslaugų gavėjas“ apibrėžtis, kuri dabar apima fizinius ir juridinius asmenis, ir sąvokų „elektroninių ryšių paslauga“ bei „asmenų tarpusavio ryšio paslauga“ apibrėžtys, kurios yra pateiktos siūlomo reglamento 4 straipsnio 1 dalies b punkte, o pastaroji sąvoka detalizuota 4 straipsnio 2 dalyje siekiant įtraukti paslaugų rūšis, kurioms konkrečiai netaikomas EERK²². Ši nuomonė grindžiama esamomis sąvokų apibrėžtimis, tačiau labai tikėtina, kad siūlomas EERK ir (arba) svarbiausios jo sąvokos keisis. Tai turėtų tiesioginį poveikį ir E. privatumo reglamentui. Būtų geriausia, jei visos EERK pateiktos sąvokos būtų savarankiškai apibrėžtos E. privatumo reglamente, arba kad siūlomame reglamente būtų bent jau pateikti paaiškinimai, jeigu kai kurių sąvokų apibrėžtys nukryptų nuo EERK pateiktų sąvokų apibrėžčių (pvz., kaip minėta, sąvoka „šalutinės paslaugos“ būtų įtraukta į sąvokos „asmenų tarpusavio ryšio paslauga“ apibrėžtį). Tačiau jei tai neįmanoma, darbo grupė norėtų pasiūlyti visoms teisėkūros procese dalyvaujančioms šalims užtikrinti, kad ir dėl siūlomo reglamento, ir dėl EERK būtų diskutuojama ir balsuojama vienu metu, kad suinteresuotieji subjektai galėtų teisingai įvertinti naujųjų dokumentų taikymo sritį ir poveikį.

5. SIŪLYMAS PATIKSLINTI SIEKiant UŽTIKRINTI TEISINĮ TIKRUMĄ

Be pirmiau aptarto aspekto, darbo grupė taip pat nori pabrėžti kai kurias siūlomo reglamento nuostatas, kurias būtų gerai patikslinti. Šie patikslinimai laikomi būtinais siekiant padidinti visų suinteresuotųjų subjektų teisinį tikrumą, kad E. privatumo reglamentas visoje ES bus suprantamas ir taikomas vienodai.

TAIKYMO SRITIES PATIKSLINIMAI

40. Kalbant apie siūlomo reglamento taikymo sritį, 29 straipsnio darbo grupė siūlo tokius patikslinimus:

- a. **Sąvoka „galutinis paslaugų gavėjas“ turėtų apimti visus pavienius naudotojus.** EERK 2 straipsnio 14 punkte „galutinis paslaugų gavėjas“ apibrėžiamas kaip naudotojas, neteikiantis viešųjų ryšių tinklų ar viešųjų elektroninių ryšių paslaugų. Reikėtų paaiškinti, kad asmenims, prisijungiantiems prie tinklų, pvz., prie tankių tinklų su savo *WiFi* maršruto parinktuvais, siūlomo reglamento apsauga taikoma.
- b. **Reikėtų paaiškinti, kad teritorinė taikymo sritis apima visus galutinius paslaugų gavėjus Sąjungoje.** 3 straipsnio 1 dalies a punkte numatyta, kad siūlomas reglamentas taikomas elektroninių ryšių paslaugų teikimui

²² Pvz., siūlomo reglamento 4 straipsnio 2 dalyje nurodyta, kad asmenų tarpusavio ryšio paslauga „apima paslaugas, kurias teikiant asmenų tarpusavio ir interaktyvus ryšys gali būti užmegztas tik kaip nesvarbi šalutinė funkcija, kuri iš esmės susijusi su kita paslauga“, o EERK 2 straipsnio 5 dalyje šios paslaugos specialiai neįtrauktos į šią apibrėžtį. (EERK 2 straipsnio 4 dalyje „asmenų tarpusavio ryšio paslaugos“ priskirtos platesnei „elektroninių ryšių paslaugos“ kategorijai).

galutiniams paslaugų gavėjams „Sajungoje“, o 3 straipsnio 1 dalies c punkte numatyta, kad jis taikomas „Sajungoje esančių“ galutinių paslaugų gavėjų galinių įrenginių apsaugai (pabraukta šio dokumento autoriaus). Ši frazė įvairiose kalbinėse versijose skiriasi. Vertime į vokiečių kalbą šio skirtumo nedaroma, o kituose vertimuose, pvz., į prancūzų, ispanų ir nyderlandų kalbas, šis skirtumas daromas. Iš 9 konstatuojamosios dalies aišku, kad teritorinė taikymo sritis turėjo būti plati, neatsižvelgiant į tai, ar paslaugos teikiamos ne iš Sajungos ir ar duomenys tvarkomi Sajungoje. Todėl siūloma išbraukti 3 straipsnio 1 dalies c punkto žodį „esančių“ siekiant pabrėžti šią plačią taikymo sritį.

- c. **Atrodo, kad siūlomu reglamentu siekiama apsaugoti tik *perduodamus konfidencialius pranešimus, o ne tada, kai jie saugomi*.** Pagal esamą požiūrį siūlomame reglamente daugiausia dėmesio skiriama pranešimų perdavimo apsaugai. Pvz., žr. 15 konstatuojamąją dalį, kurioje nurodyta, kad ryšių duomenų perėmimo draudimas turėtų būti taikomas tada, kai duomenys perduodami, t. y. iki kol numatytasis adresatas gaus pranešimo turinį. Šios apsaugos taikymo sritis grindžiama ryšių sąvoka, kuri jau yra pasenusi. Dauguma ryšių duomenų saugo paslaugų teikėjai, net ir po to, kai juos gauna. Reikėtų užtikrinti, kad būtų ir toliau saugomas šių duomenų konfidencialumas. Be to, tų pačių debesijos kompiuterija grindžiamų paslaugų abonentų (pvz., e. pašto teikėjų) tarpusavio ryšiai dažnai būna tik labai menkai susiję su perdavimu: siunčiant e. laišką, tai daugiausia atspindi paslaugų teikėjo duomenų bazėje, o pranešimai nėra faktiškai siunčiami iš vienos šalies kitai. Argumentas, kad šiam aspektui jau būtų taikomas BDAR, nėra įtikinamas: bendras siūlomo reglamento tikslas yra apsaugoti visus konfidencialius ryšius, neatsižvelgiant į technines šių ryšių priemones. Galbūt tai tik redakcinė klaida, nes 5 straipsnyje numatytas draudimas siejamas su „saugojimu“ ir „tvarkymu“.
- d. **Į taikymo sritį reikėtų įtraukti visas viešąsias belaidžio interneto zonas.** Kadangi viešąsias belaidžio interneto zonas įprasta naudoti, logiška, kad neturėtų kilti abejonių dėl to, ar yra saugomas tokiose zonose perduodamų pranešimų konfidencialumas. Tačiau reglamente tai nepaaiškinama, nes jo taikymo sritis apima tik tinklus, kuriais naudojasi „neapibrėžta galutinių paslaugų gavėjų grupė“ (13 konstatuojamoji dalis). Reikėtų apibrėžti sąvokas „neapibrėžta galutinių paslaugų gavėjų grupė“ ir „uždara galutinių paslaugų gavėjų grupė“. Visų pirma reikėtų paaiškinti, kad saugūs belaidžiai tinklai (t. y. apsaugoti slaptažodžiu) taip pat patenka į taikymo sritį, jei slaptažodis suteikiamas teoriškai neapibrėžtai naudotojų grupei, kurių tapatybės negalima nustatyti iš anksto (pvz., kavinės lankytojams, oro uoste esantiems keleiviams). Pagrindinis principas šiomis aplinkybėmis, kaip nurodyta ankstesnėje 29 straipsnio darbo grupės nuomonėje dėl E. privatumo direktyvos peržiūros, yra tai, kad „e. privatumo teisės aktas galėtų būti netaikomas tik toms paslaugoms, kurios teikiamos esanti oficialiems ar darbo santykiams tik su darbu susijusiais ar oficialiais tikslais, arba techniniams ne viešųjų organizacijų ar viešųjų organizacijų tarpusavio ryšiams siekiant kontroliuoti darbo ar verslo procesus, taip pat naudoti paslaugas išimtinai vidaus tikslais“ (p. 8).

- e. **Siūlomas reglamentas turėtų būti taikomas duomenims, surinktiems teikiant skaitmeninio transliavimo paslaugas.** Atsižvelgiant į slaptą žiūrėjimo elgsenos pobūdį, nes atskleidžiami žiūrovų asmeniniai interesai ir savybės, E. privatumo reglamente reikėtų patikslinti (galbūt konstatuojamojoje dalyje), kad jei į sąvokos „elektroninių ryšių paslauga“ apibrėžtį neįtraukiamos paslaugos, kuriomis teikiamas elektroninių ryšių tinklais perduodamas turinys, tai nereiškia, kad paslaugų teikėjai, siūlantys ir elektroninių ryšių paslaugas, ir turinio paslaugas, nepatenka į E. privatumo reglamento nuostatų taikymo sritį, kuri siejama su elektroninių ryšių paslaugų teikėjais. Tai labai svarbu, nes pagal siūlomą EERK (2 straipsnio 4 dalis) paslaugų, kuriomis teikiamas elektroninių ryšių tinklais perduodamas turinys, teikimas neįtrauktas į „elektroninių ryšių paslaugos“ apibrėžtį.
- f. **Paprastai ryšių duomenys yra asmens duomenys.** 4 konstatuojamojoje dalyje pažymėta, kad ryšių duomenys gali apimti asmens duomenis. Tačiau dauguma ryšių duomenų yra asmens duomenys²³ ir daugiausia tai yra gana asmeninio ir slapto pobūdžio duomenys, todėl reikėtų padaryti pakeitimą, siekiant nurodyti, kad paprastai tai yra asmens duomenys.
- g. **Konfidencialūs ryšiai apima platformų vidaus pranešimus.** 1 konstatuojamojoje dalyje paaiškinta, kad konfidencialumo principas taikomas „esamiems ir būsimiems komunikacijos būdams“. Šioje konstatuojamojoje dalyje toliau pateikiamas tokių būdų sąrašas, įskaitant „asmeninių žinučių siuntimą socialinėje žiniasklaidoje“. Tikriausiai taip siekiama įtraukti privačius socialinio tinklo (pvz., *Facebook*, *Twitter*) naudotojų tarpusavio pranešimus arba laiko skalėje skelbiamus pranešimus, kurie yra prieinami baigtiniam asmenų skaičiui, tačiau formuluotė nėra pakankamai aiški.
- h. **Kaip E. privatumo reglamentas taikomas įrenginių tarpusavio sąveikai.** Kaip nurodyta 9 punkte, darbo grupė palankiai vertina tai, kad apsauga išplėsta įtraukiant įrenginių tarpusavio sąveiką. Tačiau tai paminėta tik 12 konstatuojamojoje dalyje, o ne atitinkamame straipsnyje. Tokia apsauga pageidautina, nes tokie ryšiai paprastai apima privatumo teisių saugomą informaciją. Tačiau nereikėtų įtraukti siauros vien įrenginių tarpusavio ryšių kategorijos, jei šie ryšiai neturi poveikio nei privatumui, nei ryšių konfidencialumui, pvz., atvejų, kai šie ryšiai atsiranda vykdant perdavimo protokolą tarp tinklo elementų (pvz., serverių, perjungiklių) siekiant pranešti apie veikimo būseną.
- Kalbant apie E. privatumo reglamento taikymą, reikėtų patikslinti konkretų klausimą, susijusį su išmaniosiomis transporto sistemomis. Numatoma, kad transporto priemonės radijo ryšiu nuolat perduos duomenis, kurie apims unikalųjį identifikatorių. Jei E. privatumo reglamente nebus numatyta papildomos apsaugos, susijusios su ryšių duomenimis, taip būtų sudarytos sąlygos nuolat sekti vairuotojų vairavimo įpročius, maršrutus ir važiavimo

²³ Žr., pvz., 2003 m. lapkričio 6 d. ESTT sprendimo, C-101/01, 24 punktą (dėl telefono numerio), 2016 m. spalio 19 d. ESTT sprendimo *Breyer* (C-582/14) 49 punktą (dėl dinaminių IP adresų) ir 2014 m. balandžio 8 d. ESTT sprendimo *Digital Rights Ireland* (C-239/12 ir C-594/12) 26–27 punktus (dėl metaduomenų slaptumo).

greitį. Vis dėlto EERK 2 straipsnio 1 dalyje pateikiama nauja išplėsta ryšių tinklų apibrėžtis. Ji apima perdavimo sistemas, neturinčias centralizuotą administravimo pajėgumų ir leidžiančias perduoti signalus radijo ryšiu. E. privatumo reglamento 14 konstatuojamojoje dalyje patikslinta, kad tokie duomenys yra elektroninių ryšių duomenys. Pagal siūlomo reglamento 5 straipsnį bet koks šių ryšių perėmimas, stebėjimas arba saugojimas yra draudžiamas, nebent taikoma viena iš išimčių. Vis dėlto šiuos duomenis svarbu tvarkyti, leidžiant tokiems objektams kaip autonominiai automobiliai ir įrenginiai įspėti viena kitą apie kitų automobilių buvimą ar kitas grėsmes. Tada kyla klausimas, kokia išimtis būtų taikoma tokiu atveju. Galutinių paslaugų gavėjų sutikimas nėra tinkama išimtis, nes gali tapti būtina visada turėti galimybę tvarkyti šiuos duomenis. Todėl paslaugų teikėjai turi galėti remtis konkrečia išimtimi, leidžiant tokiems objektams kaip autonominiai automobiliai ir įrenginiai įspėti vieni kitus apie šalia esantį kitą tokį automobilį arba įrenginį ar kitas grėsmes.

PAAIŠKINIMAI DĖL SUTIKIMO SĄVOKOS IR TAIKymo

41. Dėl sutikimo sąvokos ir sutikimo taikymo esamame siūlomame reglamente 29 straipsnio darbo grupė siūlo tokius patikslinimus:

- a. **Kaip sutikimo sąvoka turėtų būti taikoma juridinių asmenų atžvilgiu?** 3 konstatuojamojoje dalyje pažymėta, jog reglamente reikėtų užtikrinti, kad BDAR nuostatos taip pat būtų taikomos galutiniams paslaugų gavėjams, kurie yra juridiniai asmenys. Pagal šią konstatuojamąją dalį tai apima sutikimo apibrėžtį pagal BDAR (taip pat žr. 18 konstatuojamąją dalį). Kaip pažymėta 13 pastaboje, darbo grupė palankiai vertina tai, kad juridiniai asmenys yra aiškiai įtraukti į reglamento taikymo sritį. Vis dėlto neaišku, kaip šis principas būtų taikomas praktiškai. Pagal BDAR pateiktą sutikimo apibrėžtį jis turi būti „pagrįstas informacija“, o duomenų subjekto valia turėtų būti išreikšta „pareiškimu arba vienareikšmiais veiksmais“ (BDAR 4 straipsnio 11 punktas). Reikėtų paaiškinti, kada juridinis asmuo faktiškai galėtų būti laikomas „informuotu“ ir kada yra išreikšta juridinio asmens valia.
- b. Šiomis aplinkybėmis pažymėtina, kad darbdavys daugeliu atvejų negali duoti sutikimo savo darbuotojų vardu, nes kai darbdavys reikalauja sutikimo iš darbuotojo, ir, atsižvelgiant į nelygią galių pusiausvyrą, gali kilti reali arba potenciali reikšminga žala, kurią lemtų nesutikimas, toks sutikimas negalioja, nes jis nėra duotas laisvai²⁴. Kalbant apie **bendroves, išduodančias įrenginius ar įrangą asmenims, siūlomame reglamente nėra (tinkamos) išimties** dėl trikdymo draudimo. Vienas pavyzdys – kai darbdavys nori atnaujinti bendrovės išduotą telefoną. Kitas pavyzdys – kai darbdavys siūlo darbuotojams nuomotis automobilius ir dėl administracinių priežasčių leidžia trečiajam asmeniui rinkti buvimo vietos duomenis naudojant automobilio

²⁴ Žr. Nuomonę 15/2011 dėl sutikimo sąvokos apibrėžties (WP 187), Nuomonę 8/2011 dėl asmens duomenų tvarkymo darbo santykiuose (WP 48) ir naują nuomonę dėl Duomenų tvarkymo darbe (priimta kartu su šia nuomone).

viduje esantį prietaisą. Abiem atvejais darbdavys yra suinteresuotas trikdyti šiuos įrenginius.

Trikdymo negalima laikyti būtinu informacinės visuomenės paslaugai teikti (8 straipsnio 1 dalies c punktas) arba interneto svetainės lankomumui apskaičiuoti (8 straipsnio 1 dalies d punktas). Šią problemą būtų galima išspręsti sukuriant naują išimtį, siekiant įtraukti atvejus, kai: i) darbdavys pateikia tam tikrą įrangą esant darbo santykiams; ii) darbuotojas yra šios įrangos naudotojas ir iii) trikdymas yra griežtai būtinas, kad darbuotojas galėtų naudotis įranga (tai reiškia, kad renkant duomenis taikomi proporcingumo ir subsidiarumo principai). Darbdavys gali trikdyti galutinių paslaugų gavėjų įrangą tik jeigu įvykdomos šios sąlygos.

- c. **Kontrolės gerinimas siekiant nutraukti automatinį skambučių persiuntimą.** 14 straipsnyje numatytos svarbios kontrolės priemonės, kad galutiniai paslaugų gavėjai nutrauktų automatinį trečiosios šalies atliekamą skambučių persiuntimą. Šią apsaugą būtų galima papildomai gerinti, reikalaujant galutinių paslaugų gavėjų sutikimo pradėti trečiosios šalies atliekamą skambučių persiuntimą.

PATIKSLINIMAI DĖL BUVIMO VIETOS IR KITŲ METADUOMENŲ

42. Darbo grupė siūlo patikslinti toliau nurodytus aspektus, susijusius su buvimo vietos duomenimis ir kitais duomenimis:

- a. **17 konstatuojamojoje dalyje reikėtų patikslinti frazės „kitais būdais nei teikiant elektroninių ryšių paslaugas gauti vietos nustatymo duomenys neturėtų būti laikomi metaduomenimis“** reikšmę. Neaišku, ar tai susiję su vietos nustatymo duomenimis, renkama, pavyzdžiui, naudojant programėles, kurios naudoja išmaniųjų įrenginių GPS funkcijos duomenis ir (arba) sukuria vietos nustatymo duomenis pagal šalia esančius *WiFi* maršruto parinktuvus, ir (arba) su vietos nustatymo duomenimis, renkama, naudojant transporto priemonėse įrengtus pagalbinus navigacijos įrenginius ir (arba) kitais būdais gaunant vietos nustatymo duomenis. Dėl aiškumo stokos atsiranda teisinis netikrumas, susijęs su prievolės taikymo sritimi. Bet kuriuo atveju fizinio asmens galinio įrenginio vietos nustatymo duomenys yra asmens duomenys ir todėl šių duomenų tvarkymui taikomi BDAR nustatyti įpareigojimai.
- b. Reikėtų patikslinti, kad **tvarkant daugumą vietos nustatymo duomenų ir kitų metaduomenų unikalaus identifikatoriaus nereikalaujama**. 17 konstatuojamojoje dalyje kaip komercinio elektroninių ryšių naudojimo pavyzdys minimi elektroninių ryšių paslaugų teikėjų naudojami spalviniai žemėlapiai. Tačiau siekiant sukurti pagrindinį spalvinį žemėlapi, jokie unikalūs identifikatoriai nebūtini ir pakanka statistinių skaičiavimų. Kitas minėtoje konstatuojamojoje dalyje pateiktas pavyzdys – infrastruktūros naudojimas ir apkrova taip pat gali būti apskaičiuojami pagal tam tikrus matavimo taškus, pavyzdžiui, renkant bendrus statistinius eismo kontrolės bokštų naudojimo duomenis siekiant parodyti apkrovą tam tikroje vietoje tam tikru laiku, ir tokiu atveju nereikia žinoti dar ir prisijungusių asmenų tapatybės.

Be to, konstatuojamojoje dalyje pateikiamas pavyzdys, kai parodoma, kaip tam tikru laikotarpiu tam tikromis kryptimis vyksta eismas, ir kai būtinas unikalus identifikatorius asmenų buvimo vietoms tam tikrais laiko intervalais susieti. Atrodo, kad šiuo pavyzdžiu konstatuojamojoje dalyje įteisinamas tolesnis šių duomenų tvarkymas siekiant sudaryti palankesnes sąlygas atlikti didelių duomenų kiekių analizę. Vienintelė siūlomame reglamente numatyta sąlyga, susijusio su šio pobūdžio duomenų tvarkymu, yra pareiga atlikti poveikio duomenų apsaugai vertinimą, jeigu tikėtina, kad dėl duomenų tvarkymo *kils didelis pavojus fizinių asmenų teisėms ir laisvėms*. Šios sąlygos nepakanka. Ji taip pat prieštarauja 6 straipsnyje nustatytam įpareigojimui, kad šio pobūdžio duomenų tvarkymas gali būti atliekamas tik gavus naudotojų sutikimą ir tik jeigu duomenų neįmanoma anoniminti, t. y. nenaudojami jokie unikalūs identifikatoriai. Dažnai naudotojai negali atsisakyti, kad elektroninių ryšių paslaugų teikėjai rinktų jų geografinės buvimo vietos duomenis, jei toks duomenų rinkimas yra techniškai būtinas siekiant perduoti pranešimą naudotojui arba jei toks duomenų tvarkymas yra būtinas siekiant suteikti prašomą (pvz., navigacijos) paslaugą. Ankstesnėse nuomonėse darbo grupė padarė išvadą, kad tokie vietos nustatymo duomenys iš išmaniųjų įrenginių yra slapti asmens duomenys ir kad nauda, gaunama analizuojant šiuos duomenis, nėra svarbesnė už naudotojų teises į jų ryšių metaduomenų konfidencialumo apsaugą ir už bendrąsias teises į duomenų apsaugą pagal BDAR. Todėl šioje konstatuojamojoje dalyje reikėtų nurodyti bent tai, kad paslaugų teikėjai privalo laikytis BDAR 25 straipsnyje nustatytų pareigų, jeigu vietos nustatymo ar kiti metaduomenys tvarkomi toliau. Tam reikėtų imtis bent tokių priemonių:

- i) naudoti laikinus pseudonimus;
- ii) ištrinti visas šių pseudonimų ir pradinių identifikacinių duomenų atgalinės paieškos atitikties lenteles;
- iii) apibendrinti duomenis tiek, kad pavieniai naudotojai nebegalėtų būti identifikuojami pagal konkrečius jų maršrutus, ir
- iv) ištrinti reikšmes, kuriomis remiantis dar būtų galimas identifikavimas (visas šias priemones reikia taikyti kartu).

Galiausiai E. privatumo reglamente šalis, dalyvaujančias tvarkant vietos nustatymo ir kitus metaduomenis, reikia įpareigoti viešinti jų taikomus anoniminimo ir tolesnio apibendrinimo metodus, nepažeidžiant įstatymais saugomo slaptumo reikalavimų. Taip ir priežiūros institucijos, ir plačioji visuomenė galėtų lengvai patikrinti, ar pasirinktas metodas yra tinkamas.

PATIKSLINIMAI DĖL NEUŽSAKYTŲ PRANEŠIMŲ

43. Darbo grupė siūlo patikslinti toliau nurodytus aspektus, susijusius su neužsakytais pranešimais:

- a. **Tiesioginės rinkodaros be sutikimo draudimo formuluotė.** Dabar siūlomo reglamento 16 straipsnio 1 dalyje pažymima, kad elektroninių ryšių paslaugos „gali“ būti naudojamos siekiant siųsti tiesioginės rinkodaros informaciją (esant sutikimui), tačiau nėra nustatyta aiškaus draudimo dėl

tiesioginės rinkodaros informacijos siuntimo (nukreipimo arba pateikimo) be sutikimo. Tai neatitinka kitose nuostatose įtvirtinto požiūrio, kai pirmiausia suformuluojamas draudimas, o po to nustatomos tam tikros, konkrečios išimtys. Pagal esamą formuluotę laikomasi lankstesnio požiūrio (kuris tikriausiai nėra sąmoningai pasirinktas). Darbo grupė siūlo šiek tiek pakeisti esamos E. privatumo direktyvos 13 straipsnio 1 dalies formuluotę: „Naudoti elektroninių ryšių paslaugas, įskaitant neautomatizuotus skambučius ir skambučius, kuriems naudojamos automatizuotos skambinimo ir ryšių sistemos, įskaitant pusiau automatines sistemas, kuriomis asmuo, kuriam skambinama, sujungiamas su kitu asmeniu, faksimilinius aparatus (faksus), elektroninį paštą, ar kitaip naudoti elektroninių ryšių paslaugas tiesioginės rinkodaros galutiniams paslaugų gavėjams tikslais fiziniais arba juridiniams asmenims gali būti leidžiama tik gavus išankstinį galutinių paslaugų gavėjų sutikimą.“

- b. **Nuostatų dėl rinkodaros pranešimų ir skambinimo esamiems kontaktams taikymo sritis.** 16 straipsnio 2 dalyje numatyta, kad jeigu asmuo gauna e. pašto kontaktinius duomenis iš esamo kliento, jis gali naudoti šiuos duomenis tolesnei tiesioginei savo prekių ir paslaugų rinkodarai, jei renkant duomenis kiekviename pranešime suteikiama galimybė laisvai ir nesunkiai pareikšti prieštaravimą. Šiuo metu tai taikoma tik komerciniams kontaktiniams duomenims, gautiems „parduodant produktą ar teikiant paslaugą“ ir tolesnei komercinei savo panašių prekių ar paslaugų rinkodarai. Kadangi nuostatos dėl tiesioginės rinkodaros vienodai taikomos nekomercinei (pvz., labdaros organizacijų ar politinių partijų) reklaminei veiklai, šią nuostatą reikėtų iš dalies pakeisti, kad ji būtų vienodai taikoma nekomercinėms organizacijoms, kad šios galėtų susisiekti su buvusiais rėmėjais, reklamuodamos panašius savo pačių tikslus ar idealus, ir ta pati teisė prieštarauti turėtų būti taikoma tiesioginės rinkodaros skambučiams. Be to, reikėtų nustatyti „esamų klientų kontaktinių duomenų“ galiojimo terminą siunčiant elektroninius pranešimus komerciniais, labdaros ar politikos tikslais, ir šis terminas taip pat turėtų būti taikomas tiesioginės rinkodaros skambučiams. Jeigu valstybės narės nusprendžia taikyti prieštaravimų dėl neautomatizuotų rinkodaros skambučių sistemą, santykio, susijusio su „esamo kliento kontaktiniais duomenimis“, buvimas yra svarbesnis už registraciją registre „Neskambinti“. Tokiomis aplinkybėmis galutiniai paslaugų gavėjai neturi veiksmingos galimybės užkirsti kelio erzinantiems skambučiams iš įmonių ar organizacijų, su kuriomis jie tam tikru metu bendravo, tačiau nebenori daugiau palaikyti ryšio. Todėl praktiniu požiūriu reglamente reikėtų nustatyti, kad ši „esamo kliento“ išimtis galioja, pavyzdžiui, vienus arba dvejus metus, atsižvelgiant į teisėtus atitinkamų galutinių paslaugų gavėjų lūkesčius.
- c. **Tiesioginės rinkodaros taisyklių taikymas juridiniams asmenims.** Siūlomo reglamento 16 straipsnio 5 dalyje numatyta, kad valstybės narės užtikrina, kad teisėti juridinio asmens statusą turinčių galutinių paslaugų gavėjų interesai, susiję su neužsakytais pranešimais, būtų pakankamai apsaugoti. Esamos E. privatumo direktyvos 13 straipsnio 5 dalyje aprašyti teisėti abonentų, kurie nėra fiziniai asmenys, interesai. Neaišku, koks būtų

tokio formuluotės pakeitimo poveikis. Konstatuojamosiose dalyse reikėtų paaiškinti, kad šis pakeitimas neatspindi ketinimo užtikrinti žemesnį apsaugos lygį. Kalbant apie tai, tiesioginės rinkodaros be sutikimo draudimas susijęs su sutikimą davusiais fizinio asmens statusą turinčiais galutiniais paslaugų gavėjais (pabraukta dokumento autoriaus). Reikėtų patikslinti, kad tai apima fizinius asmenis, *dirbančius* juridiniams asmenims. Tačiau sutikimo nereikėtų siekiant kreiptis į juridinius asmenis naudojant bendrus kontaktinius duomenis, kuriuos jie šiuo tikslu paviešino (pvz., info@jmonėspavadinimas.eu).

- d. **Tiesioginės rinkodaros taisyklių taikymas subjektams, veikiantiems kaip (politiniai) atstovai:** Pagal esamą 16 straipsnį gali būti neleidžiama siųsti išrinktiems atstovams tam tikrų pranešimų, kuriuose aptariami komerciniai klausimai arba interesai. Reikėtų patikslinti, kad reglamente tokie pranešimai nedraudžiami.

PATIKSLINIMAI DĖL PAGRINDINIŲ TEISIŲ SRITIES DOKUMENTŲ TAIKymo

44. **Chartijos ir EŽTK taikymą nacionaliniams duomenų saugojimo srities teisės aktams** reikėtų papildomai tikslinti. 26 konstatuojamojoje dalyje nurodyta, kad visos valstybių narių priemonės, kurias jos taiko siekdamas apsaugoti viešąjį interesą, pvz., teisėtos perėmimo priemonės, turi atitikti Chartiją (ne tik EŽTK). Tai pageidautina, nes atitinka Sprendime *Tele2 / Watson* pateiktus motyvus, kad visoms nacionalinėms ES teisėje numatytų duomenų apsaugos priemonių išimtims taikoma Chartija (ir todėl pažeidimai per nacionalinės teisės aktus gali būti perduodami nagrinėti Europos Sąjungos Teisingumo Teismui). Vis dėlto siūlomo reglamento 11 straipsnyje pažymima tik tai, kad ribojant siūlomo reglamento 5–8 straipsnių taikymo sritį, būtina paisyti pagrindinių teisių ir laisvių esmės ir tai turi būti būtina ir proporcinga priemonė. Čia taip pat reikėtų įtraukti aiškią nuorodą į Chartiją ir EŽTK.

45. **Kad pranešimų konfidencialumas taip pat būtų saugomas pagal EŽTK 8 straipsnį.** Aiškinamojo memorandumo 1.1 punkte ir 1 konstatuojamojoje dalyje paaiškinta, kad siūlomu reglamentu įgyvendinamas Chartijos 7 straipsnis. Tai pakartota 19 konstatuojamojoje dalyje. Vis dėlto pagrindinė teisė į konfidencialius ryšius saugoma ne tik šioje nuostatoje, bet ir pagal EŽTK 8 straipsnį. Pateikus aiškią nuorodą siūlomo reglamento straipsnyje būtų papildomai patvirtinta, kad vertinant (galutinį) reglamentą taip pat reikės atsižvelgti į visą aktualią Europos Žmogaus Teisių Teismo jurisprudenciją. Be to, ši nuoroda jau įtraukta į 20 konstatuojamąją dalį (susijusią su galiniais įrenginiais) ir 26 konstatuojamąją dalį (susijusią su teisėtu perėmimu) ir papildomai patvirtinta aiškinamojo memorandumo 2.1 punkto motyvuose (dėl Chartijos ir EŽTK santykio juridinių asmenų atžvilgiu), tačiau jos nėra nė viename iš atitinkamų straipsnių, pvz., 11 straipsnio 1 dalyje.

KITI PAAIŠKINIMAI

46. Reikėtų paaiškinti, kad **BDAR nustatyti įpareigojimai, pvz., susiję su pranešimo apie duomenų pažeidimą tvarka ir PDAV, ir toliau taikomi**, kai šalys tvarko

asmens duomenis tvarkydamos elektroninių ryšių duomenis. Kadangi 5 konstatuojamojoje dalyje paminėta, kad siūlomas reglamentas yra *lex specialis* BDAR atžvilgiu ir kad tvarkyti elektroninių ryšių duomenis turėtų būti leidžiama tik pagal siūlomą reglamentą, būtų galima kelti klausimą, ar tam tikri BDAR nustatyti įpareigojimai galioja ir taikant siūlomą reglamentą. Tai visų pirma pasakytina apie tuos atvejus, kai siūlomą reglamentą būtų galima aiškinti siekiant nustatyti tam tikrą įpareigojimą, nors tai yra nustatyta ir BDAR. Orientaciniai pavyzdžiai:

- (i) siūlomame reglamente įpareigojama pranešti apie „nustatytą“ pavojų saugumui (17 straipsnis) (taip pat žr. 35 pastabą), tačiau BDAR nustatyta pranešimo apie duomenų pažeidimą tvarka (33 ir 34 straipsniai);
- (ii) siūlomame reglamente paminėta, kad atlikti PDAV ir konsultuotis su priežiūros institucija pagal BDAR tam tikromis aplinkybėmis yra privaloma (17 ir 19 konstatuojamosios dalys ir 6 straipsnio 3 dalies b punktas), o BDAR jau nustatyta, kada reikia atlikti PDAV ir kada reikia konsultuotis (35 ir 36 straipsniai), ir
- (iii) nenurodyta, kad, jeigu laikomasi būtinų duomenų tvarkymo draudimo išimties sąlygų pagal siūlomo reglamento 5 straipsnį, vis vien reikia laikytis atitinkamų įpareigojimų pagal BDAR, kai tai susiję su asmens duomenų tvarkymu ir bet koks kitas duomenų tvarkymas pagal BDAR nėra leidžiamas. Reikėtų paaiškinti, kad dėl to BDAR 6 straipsnio 4 dalyje nustatytas suderinamumo testas netaikomas.
- (iv) Siūlomame E. privatumo reglamente nenumatyti panašūs sertifikavimo mechanizmai kaip BDAR 42 ir 43 straipsniuose. Kadangi, vertinant iš esmės, BDAR 42 straipsnio taikymo sritis nėra apribota duomenų apsaugos sertifikavimo mechanizmų ir duomenų apsaugos žymų nustatymu siekiant įrodyti, kad laikomasi BDAR, reikėtų apsvarstyti, ar nereikėtų įtraukti panašios nuostatos, kad duomenų tvarkymo operacijas, standartus, prekes ar paslaugas būtų galima sertifikuoti dėl jų atitikties E. privatumo reglamentui.

Siekiant užtikrinti, kad šia aiškumo stoka nebūtų naudojama kaip argumentu siekiant sumažinti apsaugos lygį pagal siūlomą reglamentą, reikėtų aiškiai nurodyti, kad visais šiais atvejais duomenų valdytojai taip pat privalo laikytis BDAR.

47. Be to, reikėtų paaiškinti, kad **reikalavimas dėl sutikimo atšaukimo taip pat taikomas, kai yra trikdomi galiniai įrenginiai**. Siūlomo reglamento 8 straipsnio 1 dalies b punkte numatyta galutinių paslaugų gavėjų galinių įrenginių trikdymo galimybė esant sutikimui. 9 straipsnio 3 dalyje reikalaujama, kad galutiniams paslaugų gavėjams būtų suteikta galimybė bet kada atšaukti sutikimą, tačiau tai taikoma tik sutikimui dėl metaduomenų ir turinio analizės. Reikėtų paaiškinti, kad šis įpareigojimas taikomas taip pat ir galinių įrenginių trikdymui.

48. Kalbant apie tai derėtų patikslinti, kad **reikalavimas priminti apie galimybę atšaukti sutikimą taip pat taikomas sutikimui, duotam per naršyklės nuostacius**. 9 straipsnio 3 dalyje reikalaujama, kad galutiniams paslaugų gavėjams periodiškai, kas 6 mėnesius būtų primenama apie galimybę bet kada atšaukti sutikimą. Nors darbo grupė mano, kad bendrieji naršyklių ir kitos programinės įrangos, įskaitant operacines sistemas, programėles ir programinės įrangos sąsajas su daiktų internetu sujungtuose įrenginiuose, nuostaciai (t. y. nuostaciai netaikant konkrečios ir išsamios kontrolės) negali būti pagrįsta priemonė duoti sutikimą, nes bendrieji nuostaciai nėra tinkami

konkrečiam sutikimui duoti dėl konkretaus atvejo (žr. 24 pastabą), o numatytieji nuostatai turi būti kuo patogesni naudotojui (žr. 19 pastabą). Jei siūlomame reglamente ši nuostata liktų, nuostatai turi būti pakankamai išsamūs, kad būtų galima valdyti visą duomenų tvarkymą, dėl kurio naudotojas duoda sutikimą, ir apimti kiekvieną įrenginių funkciją, dėl kurios gali būti tvarkomi duomenys. Be to, galutiniam paslaugų gavėjui turėtų būti bent jau periodiškai (kas 6 mėn.) primenama apie galimybę pasikeisti šiuos nuostatus.

49. Palankiai vertintina tai, kad siūlomame reglamente reikalaujama, kad rinkoje jau esančioje programinėje įrangoje galutiniam paslaugų gavėjui būtų pranešama apie galimybę nustatyti privatumo nuostatus (10 straipsnis). **Tačiau neaišku, kaip tai būtų galima veiksmingai taikyti seniai rinkoje esantiems produktams** ir kitiems neapribojamiems produktams. Be to, papildomai reikėtų paaiškinti, kaip šis įpareigojimas bus taikomas viešųjų šaltinių programinei įrangai, kuri kuriama atvirai ir decentralizuotai.
50. Reikėtų patikslinti, kad **siūlomai galimybei blokuoti (trečiųjų šalių) slapukus pagal siūlomo reglamento 10 straipsnį teikiama pirmenybė išimties, taikomos interneto svetainės lankomumui apskaičiuoti** pagal 8 straipsnio 1 dalies d punktą, **atžvilgiu**. Arba, kitaip tariant, nors pagal 8 straipsnio 1 dalies d punktą interneto svetainėje gali būti naudojama interneto svetainės lankomumui apskaičiuoti skirta analizė, naudotojai vis vien turėtų teisę blokuoti šias sekimo technologijas savo naršyklėje.
51. Reikėtų **patikslinti (pusiau) automatizuotų skambinimo ir ryšių sistemų sąvokos apibrėžtį**. Šios sąvokos apibrėžtyje siūlomo reglamento 4 straipsnio 3 dalies h punkto antroje sakinio dalyje pateikiama nuoroda į pačią sąvoką („įskaitant skambučius, kuriems naudojamos automatizuotos skambinimo ir ryšių sistemos, sujungiančios asmenį, kuriam skambinama, su kitu asmeniu“). Šį paskutinį sakinį siūloma išbraukti iš šios apibrėžties ir pakeisti 4 straipsnio 3 dalies g punkte pateiktą apibrėžtį, kad ji apimtų skambučius naudojant pusiau automatizuotas ryšių sistemas, pvz., automatinis numerio rinktuvas, kuriuos naudojant asmuo, kuriam skambinama, sujungiamas su kitu asmeniu.
52. Reikėtų **paaiškinti „paslaugos užsakymo sąlygose numatytą“ informaciją**. 14 konstatuojamojoje dalyje paminėta, kad elektroninių ryšių metaduomenys „gali apimti paslaugos užsakymo sąlygose numatytą informaciją, jei tokia informacija tvarkoma elektroninių ryšių turinio perdavimo, platinimo arba keitimosi juo tikslais“. Neaišku, ką reiškia ši formuluotė.
53. Reikėtų patikslinti **derėjimo užtikrinimo ir bendradarbiavimo mechanizmų taikytinumą**. 38 konstatuojamojoje dalyje pažymėta, kad siūlomas reglamentas grindžiamas BDAR derėjimo užtikrinimo mechanizmu. Be to, 18 straipsnio 1 dalyje numatyta, kad BDAR VI ir VII skyriai taikomi *mutatis mutandis*. 19 straipsnyje taip pat pažymėta, kad Europos duomenų apsaugos valdyba (EDAV) įgyvendina BDAR 70 straipsnyje nurodytas užduotis. Nors šių nuostatų taikymas gana aiškus, negalima atmesti, kad kils aiškinimo klausimų, susijusių su svarbiausiomis derėjimo užtikrinimo ir bendradarbiavimo mechanizmų sąvokomis pagal BDAR. Pavyzdžiui,

pagrindinės institucijos mechanizmas taikomas tais atvejais, kai yra „tarpvalstybinis duomenų tvarkymas“ (BDAR 56 straipsnio 1 dalis): neaišku, kaip tai taikoma galinių įrenginių trikdymo arba turinio arba metaduomenų analizės atveju pagal siūlomą reglamentą. Todėl patartina patikslinti šių svarbiausių sąvokų taikymą konstatuojamojoje dalyje ir pabrėžti, kad į visus likusius klausimus, susijusius su šių BDAR skyrių taikytinumu taikant siūlomą reglamentą, bus atsakyta aiškinant šių skyrių nuostatas, atsižvelgiant į jų tikslą. Be to, patartina patikslinti, kad 70 straipsnis taikant siūlomą reglamentą *mutatis mutandis* taikomas EDAV (dabar konstatuojamojoje dalyje to nenurodyta).

* * *