Suunised

Suunised 2/2023 e-privaatsuse direktiivi artikli 5 lõike 3 tehnilise kohaldamisala kohta

Versioon 2.0

Vastu võetud 7. oktoobril 2024

Versioonid

Versioon 1.0	14. november 2023	Suuniste vastuvõtmine avalikuks konsulteerimiseks
Versioon 2.0	7. oktoober 2024	Suuniste vastuvõtmine pärast avalikku konsulteerimist

Kommenteeritud kokkuvõte

Suunistes käsitleb Euroopa Andmekaitsenõukogu (EAKN) e-privaatsuse direktiivi artikli 5 lõike 3 kohaldatavust eri tehniliste lahenduste suhtes. Suunistega täiendatakse artikli 29 töörühma arvamust 9/2014 e-privaatsuse direktiivi kohaldamise kohta seadmetuvastuse suhtes ning nende eesmärk on anda selge ülevaade e-privaatsuse direktiivi artikli 5 lõikega 3 hõlmatud tehnilistest toimingutest.

See, et on ilmunud uued jälgimismeetodid nii olemasolevate jälgimisvahendite asendamiseks (nt küpsised, sest mõni brauserimüüja lõpetas võõrküpsiste toetamise) kui ka uute ärimudelite loomiseks, on muutunud oluliseks andmekaitseprobleemiks. Kuigi e-privaatsuse direktiivi artikli 5 lõike 3 kohaldatavus on mõne jälgimistehnoloogia, näiteks küpsiste korral hästi välja kujunenud ja seda rakendatakse, on vaja lahendada ebaselgused seoses sätte kohaldamisega kujunemisjärgus jälgimisvahendite suhtes.

Suunistes tuvastatakse kolm e-privaatsuse direktiivi artikli 5 lõike 3 kohaldatavuse põhielementi (punkt 2.1), nimelt „teave“, „abonendi või kasutaja lõppseade“ ning „juurdepääsu saamine teabele, selle salvestamine ja juurdepääs salvestatud teabele“. Lisaks on suunistes iga elemendi üksikasjalik analüüs (punktid 2.2–2.6).

Punktis 3 on seda analüüsi kohaldatud mitteammendavale loetelule kasutusjuhtudest, mis esindavad üldkasutatavaid tehnikaid, nimelt:

- URL- ja pikseljälitus
- Kohalik töötlemine
- Ainult IP-põhine jälgimine
- Ajutine ja vahendatud esemevõrgu (IoT) aruandlus
- Kordumatu tunnus

Sisukord

Euroopa Andmekaitsenõukogu,

võttes arvesse Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määruse (EL) 2016/679 (füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta; edaspidi „isikuandmete kaitse üldmäärus“) artikli 70 lõike 1 punkti e,

võttes arvesse Euroopa Majanduspiirkonna (EMP) lepingut, eelkõige selle XI lisa ja protokolli nr 37, mida on muudetud EMP ühiskomitee 6. juuli 2018. aasta otsusega nr 154/2018[1],

võttes arvesse Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, muudetud direktiiviga 2009/136/EÜ (edaspidi „e-privaatsuse direktiiv“), artikli 15 lõiget 3,

võttes arvesse töökorra artiklit 12 ja artiklit 22,

ON VASTU VÕTNUD JÄRGMISED SUUNISED:

1 SISSEJUHATUS

1. e-privaatsuse direktiivi artikli 5 lõike 3 punkti kohaselt on *„teabe salvestamine abonendi või kasutaja lõppseadmesse ja juurdepääsu saamine sinna juba salvestatud teabele“* lubatud ainult nõusoleku või samas artiklis sätestatud erieesmärkide alusel. Nagu on meelde tuletatud e-privaatsuse direktiivi põhjenduses 24[2], on selle sätte eesmärk kaitsta kasutajate lõppseadmeid, sest need moodustavad osa kasutajate eraelust. Artikli sõnastusest tuleneb, et e-privaatsuse direktiivi artikli 5 lõiget 3 kohaldatakse peale küpsiste ka „sarnaste tehnoloogiate“ suhtes. Samas puudub praegu e-privaatsuse direktiivi artikli 5 lõikega 3 hõlmatud tehniliste toimingute täielik loetelu.

2. Artikli 29 töörühma arvamuses 9/2014 e-privaatsuse direktiivi kohaldamise kohta seadmetuvastuse suhtes (edaspidi „artikli 29 töörühma arvamus 9/2014“) on juba selgitatud, et seadmetuvastus kuulub e-privaatsuse direktiivi artikli 5 lõike 3 tehnilisse kohaldamisalasse[3], kuid tehnoloogiate arengu tõttu on vaja täiendavaid suuniseid praegu täheldatud jälgimismeetodite kohta. Tehnikamaastik on viimase aastakümne jooksul arenenud – operatsioonisüsteemidesse manustatud identifikaatoreid kasutatakse üha rohkem ja luuakse uusi vahendeid, mis võimaldavad salvestada teavet lõppseadmetesse.

3. Ebaselgus seoses e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamisalaga on tekitanud ajendi rakendada alternatiivseid lahendusi internetikasutajate jälgimiseks ja suundumuse vältida e-privaatsuse direktiivi artikli 5 lõikes 3 sätestatud õiguslikke kohustusi. Kõik sellised olukorrad on problemaatilised ja nõuavad täiendavat analüüsi, et täiendada EAKN varasemaid suuniseid.

[1] Kõiki selle dokumendi viiteid liikmesriikidele tuleb mõista kui viiteid EMP liikmesriikidele.

[2] „Elektrooniliste sidevõrkude kasutajate lõppseadmed ja sellistes seadmetes säilitatav teave moodustavad osa kasutajate eraelust, mida tuleb kaitsta inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni kohaselt. Niinimetatud nuuskurvara, veebilutikad, varjatud identifikaatorid ja muud sellised vahendid võimaldavad kasutaja teadmata siseneda kasutaja lõppseadmesse, et pääseda juurde teabele, salvestada varjatud teavet või jälitada kasutaja tegevust, ning võimaldab tõsiselt sekkuda kõnealuste kasutajate eraellu. Selliste vahendite kasutamine peaks olema lubatud ainult õiguspärastel eesmärkidel ja asjaomaste kasutajate teadmisel.“

[3] Artikli 29 töörühma arvamus 9/2014, lk 11.

4. Käesolevate suuniste eesmärk on tehniliselt analüüsida e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamisala, nimelt selgitada, mida hõlmab väljend „*teabe salvestamine abonendi või kasutaja lõppseadmesse ja juurdepääsu saamine sinna juba salvestatud teabele*“. Suunistes ei käsitleta asjaolusid, mille korral töötlemistoiming võib kuuluda erandi alla e-privaatsuse direktiivis sätestatud nõusoleku kohustusest[4], sest neid asjaolusid tuleks analüüsida iga kord eraldi, arvestades ülevõtmist (ülevõtmisi) asjaomase liikmesriigi õigusesse ja riiklike pädevate asutuste antud suuniseid.

5. Konkreetsete kasutusjuhtude mitteammendavat loetelu analüüsitakse suuniste viimases osas.

2 ANALÜÜS

2.1 e-privaatsuse direktiivi artikli 5 lõike 3 kohaldatavuse põhielemendid

6. e-privaatsuse direktiivi artikli 5 lõiget 3 kohaldatakse, kui:

   a. **KRITEERIUM A:** tehtavad toimingud on seotud mõistega „*teave*“. Tuleb märkida, et kasutav termin on mitte „isikuandmed“, vaid „teave“.

   b. **KRITEERIUM B:** tehtavad toimingud hõlmavad abonendi või kasutaja „*lõppseadet*“ (B.1), mistõttu on vaja hinnata mõistet „*üldkasutatav sidevõrk*“ (B.2).

   c. **KRITEERIUM C:** tehtavad toimingud on „*salvestamine*“ (C.1) või „*juurdepääsu saamine*“ (C.2). Kumbagi mõistet saab uurida sõltumatult, nagu on meelde tuletatud artikli 29 töörühma arvamuses 9/2014: *„Väljendi „salvestamine või juurdepääsu saamine“ kasutamine viitab, et salvestamine ja juurdepääs ei pea toimuma sama teabevahetuse raames ning neid ei pea tegema sama isik.“*[5]

   Loetavuse huvides nimetatakse kasutaja lõppseadmesse salvestatud teabele juurdepääsu saavat üksust edaspidi „juurdepääsu saavaks üksuseks“.

2.2 Mõiste „teave“ – kriteerium A

7. Nagu on väljendatud seoses KRITEERIUMIGA A, kirjeldatakse siin punktis üksikasjalikult, mida hõlmab mõiste „teave“. Mõiste „teave“, mis hõlmab laiemat kategooriat kui üksnes isikuandmete mõiste, on seotud e-privaatsuse direktiivi kohaldamisalaga.

8. e-privaatsuse direktiivi artikli 5 lõike 3 eesmärk on kaitsta kasutajate eraelu, nagu on märgitud direktiivi põhjenduses 24: „*Elektrooniliste sidevõrkude kasutajate lõppseadmed ja sellistes seadmetes säilitatav teave moodustavad osa kasutajate eraelust, mida tuleb kaitsta inimõiguste ja põhivabaduste kaitse Euroopa konventsiooni kohaselt*.“ Seda kaitseb ka Euroopa Liidu põhiõiguste harta artikkel 7.

9. e-privaatsuse direktiivi artikli 5 lõike 3 ja põhjenduse 24 sõnastus hõlmab selge sõnaga stsenaariume, mis tungivad eraellu isegi ilma isikuandmeid kaasamata, näiteks viiruste salvestamine kasutaja lõppseadmesse. See näitab, et mõiste „teave“ määratlus ei tohiks piirduda omadusega olla seotud tuvastatud või tuvastatava füüsilise isikuga.

[4] Nagu on sätestatud e-privaatsuse direktiivi artikli 5 lõikes 3: „*See ei takista andmete tehnilist salvestamist ega juurdepääsu, mille ainus eesmärk on edastada sidet elektroonilises sidevõrgus või mis on teenuseosutajale hädavajalik sellise infoühiskonna teenuse osutamiseks, mida abonent või kasutaja on sõnaselgelt taotlenud.*“

[5] Artikli 29 töörühma arvamus 9/2014, lk 8.

10. Seda on kinnitanud ka Euroopa Liidu Kohus: „*See kaitse laieneb kogu lõppseadmetesse salvestatud teabele, olenemata sellest, kas tegemist on isikuandmetega või mitte, ja selle eesmärk on nähtuvalt samast põhjendusest kaitsta kasutajaid varjatud identifikaatorite ja muude analoogsete vahendite eest, mis võimaldavad kasutaja teadmata siseneda tema lõppseadmesse.*“[6]

11. Seda, kas e-privaatsuse direktiivi artikli 5 lõike 3 kohaldatavuse hindamisel tuleks arvestada selle teabe päritolu ja põhjusi, miks see on salvestatud lõppseadmesse, on varasemalt selgitatud, näiteks artikli 29 töörühma arvamuses 9/2014: „*Väär on tõlgendada seda nii, nagu ei peaks kolmas isik sellele teabele juurdepääsuks luba küsima üksnes seepärast, et tema ei salvestanud seda teavet. Nõusoleku küsimise nõue kehtib ka juurdepääsul kirjutuskaitstud väärtusele (nt võrguliidese MAC-aadressi päring operatsioonisüsteemi rakendusliidese kaudu).*“[7]

12. Kokkuvõttes hõlmab teabe mõiste nii isikustamata andmeid kui ka isikuandmeid, olenemata sellest, kuidas neid andmeid säilitati ja kes seda tegi, st kas seda tegi väline üksus (sh muud üksused peale selle, kellel on juurdepääs), kasutaja, tootja või toimus see muul viisil.

2.3 Mõiste „abonendi või kasutaja lõppseadmed“ – kriteerium B.1

13. See peatükk keskendub direktiivis 2008/63/EÜ toodud määratlusele, millele viidatakse direktiivi (EL) 2018/1972 artiklis 2 ja mille järgi on „lõppseade“ „*seade, mis on otseselt või kaudselt ühendatud üldkasutatava telekommunikatsioonivõrgu lõpp-punktiga, et saata, töödelda või võtta vastu teavet; nii otsese kui ka kaudse ühenduse korral võib ühenduse luua kaabli või optilise kaabli abil või elektromagnetiliselt; ühendus on kaudne siis, kui lõppseadme ja üldkasutatava võrgu ühenduse lõpp-punkti vahele paigaldatakse seadmed*“[8].

14. e-privaatsuse direktiivi põhjendus 24 annab selge ettekujutuse lõppseadmete rollist direktiivi artikli 5 lõikega 3 pakutava kaitse tagamisel. Peale selle, et e-privaatsuse direktiiviga kaitstakse kasutajate privaatsust seoses nende teabe konfidentsiaalsusega, kaitseb direktiiv seda ka kasutaja lõppseadme tervikluse tagamisega. Sellest arusaamast juhindutakse lõppseadme mõiste tõlgendamisel käesolevates suunistes.

15. e-privaatsuse direktiivi artiklis 3 on sätestatud, et direktiivi kohaldamiseks peab isikuandmete töötlemine toimuma seoses üldkasutatavate elektrooniliste sideteenuste osutamisega üldkasutatavates sidevõrkudes. See tähendab, et seade peaks olema seoses sellise teenusega kasutatav ja selleks, et seda saaks kvalifitseerida lõppseadmeks, peaks see olema ühendatud või ühendatav[9] üldkasutatava sidevõrgu liidesega. EAKN märgib, et 2009. aastal[10] e-privaatsuse direktiivi artikli 5 lõike 3 teksti tehtud muudatustega laiendati lõppseadmete kaitset, kustutades väljendi „elektrooniliste sidevõrkude kasutamine“, mille kaudu toimub teabe salvestamine abonendi või kasutaja lõppseadmesse ja juurdepääsu saamine sinna juba salvestatud teabele. Seega, kui seadmel on võrguliides, mis muudab selle ühenduskõlblikuks (isegi kui sellist ühendust veel ei ole), kohaldatakse

[6] Euroopa Kohtu 1. oktoobri 2019. aasta otsus, Planet 49, kohtuasi C-673/17, ECLI:EU:C:2019:801, punkt 70.
[7] Artikli 29 töörühma arvamus 9/2014, lk 8.
[8] Komisjoni 20. juuni 2008. aasta direktiiv 2008/63/EÜ konkurentsi kohta telekommunikatsioonivõrgu lõppseadmete turgudel (kodifitseeritud versioon), artikli 1 punkt 1.
[9] See tähendab, et võrguga ühendamiseks on olemas tehnilised võimalused, isegi kui seda ühendust veel ei ole.
[10] Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiv 2009/136/EÜ, millega muudetakse direktiivi 2002/22/EÜ universaalteenuse ning kasutajate õiguste kohta elektrooniliste sidevõrkude ja -teenuste puhul, direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris, ning määrust (EÜ) nr 2006/2004 tarbijakaitseseaduse jõustamise eest vastutavate siseriiklike asutuste vahelise koostöö kohta (EMPs kohaldatav tekst), ELT L 337, 18.12.2009, artikli 2 lõige 5 ja põhjendus 65.

e-privaatsuse direktiivi artikli 5 lõiget 3 iga üksuse suhtes, mis salvestaks teavet lõppseadmesse ja saaks sinna juba salvestatud teabele juurdepääsu, olenemata lõppseadmele juurdepääsu vahendist ja sellest, kas seade on võrguga ühendatud või ühendamata.

16. Seadmeid, mis on osa üldkasutatavast elektroonilise side võrgust, ei käsitata e-privaatsuse direktiivi artikli 5 lõike 3 kohaselt lõppseadmetena[11].

17. Lõppseade võib koosneda mis tahes arvust üksikutest riistvaraosadest, mis kokku moodustavad lõppseadme. See võib, kuid ei pruugi olla füüsiliselt suletud seade, mis mahutab kogu kuva-, töötlemis-, salvestus- ja välisseadmete riistvara (nt nutitelefonid, sülearvutid, võrguühendusega salvestusseadmed, võrgustatud autod või võrgustatud telerid, nutiprillid).

18. e-privaatsuse direktiivis tunnistatakse, et kasutaja lõppseadmesse salvestatud teabe konfidentsiaalsuse ja kasutaja lõppseadme tervikluse kaitse ei piirdu füüsiliste isikute eraelu kaitsega, vaid on seotud ka õigusega vabale kirjavahetusele või juriidiliste isikute õigustatud huvidega[12]. Sellisena kaitstakse e-privaatsuse direktiivi artikli 5 lõike 3 alusel lõppseadet, mis võimaldab sellist kirjavahetust ja juriidiliste isikute õigustatud huvide teostamist.

19. Kasutaja või abonent võib lõppseadmeid omada, rentida või saada neid muul viisil. Mitu kasutajat või abonenti võivad jagada sama lõppseadet.

20. See kaitse on e-privaatsuse direktiiviga tagatud kasutaja või abonendiga seotud lõppseadmele ning see ei sõltu sellest, kas kasutaja on juurdepääsuvahendi seadistanud (näiteks kui ta algatas elektroonilise side) või isegi sellest, kas kasutaja on nimetatud juurdepääsuvahendist teadlik.

2.4 Mõiste „üldkasutatav sidevõrk“ – kriteerium B.2

21. Et e-privaatsuse direktiiviga reguleeritud olukord on seotud *„üldkasutatavate elektrooniliste sideteenuste osutamisega ühenduse üldkasutatavates sidevõrkudes“*[13] ning lõppseadme määratluses on konkreetselt nimetatud mõistet *„üldkasutatav sidevõrk“*, on oluline seda mõistet selgitada, et selgitada konteksti, milles kohaldatakse e-privaatsuse direktiivi artikli 5 lõiget 3.

22. Elektroonilise side võrgu mõistet ei ole e-privaatsuse direktiivis määratletud. Sellele mõistele viidati algselt direktiivis 2002/21/EÜ (elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv))[14], mis hiljem asendati direktiivi 2018/1972 (Euroopa elektroonilise side seadustik) artikli 2 punktiga 1. See on nüüd sõnastatud nii:

> *„elektroonilise side võrk“ – ülekandesüsteemid, mis võivad, aga ei pruugi põhineda püsitaristul või kesksel juhtimisel, ja vajaduse korral lülitus- ja marsruutimisseadmed ning muud vahendid, sealhulgas võrguelemendid, mis ei ole aktiivsed, mis võimaldavad edastada signaale kaabli kaudu, raadio teel, optiliselt või muude elektromagnetiliste vahendite abil, kasutades sealhulgas satelliitvõrke, püsivõrke (ahel- ja pakettkommutatsioonivõrgud, k.a internet) ja mobiilsidevõrke, elektrikaabelsüsteeme, kui neid kasutatakse signaalide edastamiseks, raadio- ja*

[11] Võrgu piiride tuvastamine eri kontekstides: vt BERECi suunised ühiste lähenemisviiside kohta võrgu lõpp-punkti tuvastamiseks eri võrgutopoloogiates (BoR (20) 46).

[12] Nagu on meelde tuletatud Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiivi (EL) 2018/1972 (millega kehtestatakse Euroopa elektroonilise side seadustik) artikli 2 punktis 13, võib kasutaja olla füüsiline või juriidiline isik.

[13] e-privaatsuse direktiivi artikkel 3.

[14] Euroopa Parlamendi ja nõukogu 7. märtsi 2002. aasta direktiiv 2002/21/EÜ elektrooniliste sidevõrkude ja -teenuste ühise reguleeriva raamistiku kohta (raamdirektiiv)

teleringhäälinguvõrke ja kaabeltelevisioonivõrke, olenemata sellest, millist teavet nende kaudu edastatakse.[15]

23. See määratlus on neutraalne ülekandetehnoloogiate suhtes. Määratluse kohaselt on elektroonilise side võrk mis tahes võrgusüsteem, mis võimaldab edastada elektroonilisi signaale oma sõlmede vahel, olenemata kasutatavatest seadmetest ja protokollidest.

24. Direktiivi (EL) 2018/1972 kohane elektroonilise side võrgu mõiste ei sõltu taristu avalik-õiguslikust või eraõiguslikust laadist ega võrgu kasutuselevõtu või haldamise viisist („*mis võivad, aga ei pruugi põhineda püsitaristul või kesksel juhtimisel*“[16].) Järelikult on elektroonilise side võrgu määratlus direktiivi (EL) 2018/1972 artikli 2 tähenduses piisavalt lai, et hõlmata mis tahes liiki taristut. See hõlmab võrke, mida haldab või ei halda operaator, võrke, mida haldab operaatorite rühm ühiselt, või isegi ajutisi võrke, kus lõppseade võib dünaamiliselt liituda teiste lõppseadmete võrguga või sealt lahkuda, kasutades lühimaa ülekandeprotokolle.

25. See võrgu määratlus ei piira mis tahes ajal võrgus olevate lõppseadmete arvu. Mõne võrguskeemi aluseks on sõlmed, mis edastavad teavet ajutisel viisil hetkel ühendatud sõlmedele[17] ja mingil hetkel võivad suhelda ainult kaks partnerit. Sellised juhtumid kuuluksid e-privaatsuse direktiivi üldisesse kohaldamisalasse, kui võrguprotokoll võimaldab kaasata veel partnereid.

26. Sidevõrgu üldsusele kättesaadavust on vaja selleks, et seadet saaks pidada lõppseadmeks ja seega e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamiseks. Tuleb märkida, et asjaolu, et võrk tehakse kättesaadavaks piiratud hulgale üldsusele (nt tasulistele või tasuta abonentidele, vastavalt kõlblikkuskriteeriumitele), ei muuda sellist võrku privaatvõrguks[18].

2.5 Mõiste „juurdepääsu saamine“ – kriteerium C.1

27. Juurdepääsu saamise mõiste korrektseks piiritlemiseks on oluline arvestada e-privaatsuse direktiivi kohaldamisala, mis on sätestatud selle artiklis 1: „*põhiõiguste ja -vabaduste, eelkõige eraelu puutumatuse kaitse võrdväärse taseme tagamiseks isikuandmete töötlemise puhul elektroonilise side sektoris ja selliste andmete ning elektrooniliste sideseadmete ja -teenuste vaba liikumise tagamiseks ühenduses*“.

28. Lühidalt öeldes on e-privaatsuse direktiiv eraelu puutumatust säilitav õigusakt, mille eesmärk on kaitsta side konfidentsiaalsust ja seadmete terviklust. E-privaatsuse direktiivi põhjenduses 24 on selgitatud, et füüsiliste isikute korral moodustavad kasutaja lõppseadmed osa nende eraelust ning juurdepääs nendesse salvestatud teabele ilma nende teadmata võib tõsiselt sekkuda nende eraellu.

29. e-privaatsuse direktiiv kaitseb ka juriidilisi isikuid[19]. Sellest tulenevalt tuleb e-privaatsuse direktiivi artikli 5 lõikes 3 kasutatud mõistet „juurdepääsu saamine“ tõlgendada viisil, mis kaitseb neid õigusi rikkumise eest kolmandate isikute poolt.

[15] Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud) (EMPs kohaldatav tekst), artikli 2 punkt 1.

[16] Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/1972, millega kehtestatakse Euroopa elektroonilise side seadustik (uuesti sõnastatud) (EMPs kohaldatav tekst), artikli 2 punkt 1.

[17] Näiteks viivitustolerantse võrgusüsteemi kontekstis, kus rakendatakse „salvestamise ja edastamise tehnikaid“, nagu Briari avatud lähtekoodiga projekt.

[18] Üldkasutatavate sidevõrkude tuvastamise täiendav analüüs on BERECi suunistes avatud interneti määruse rakendamise kohta (BoR (20) 112).

[19] e-privaatsuse direktiivi põhjendus 26, vt punkt 17 eespool.

30. Teabe säilitamine või sellele juurdepääsu saamine võivad olla sõltumatud toimingud, mida teostavad sõltumatud üksused. e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamiseks ei pea toimuma korraga nii teabe salvestamine kui ka juurdepääs juba salvestatud teabele.

31. Nagu on märgitud artikli 29 töörühma arvamuses 9/2014: *„Väljendi „salvestamine või juurdepääsu saamine“ kasutamine viitab, et salvestamine ja juurdepääs ei pea toimuma sama teabevahetuse raames ning neid ei pea tegema sama isik. Ühe isiku salvestatud teave (sealhulgas kasutaja või seadme tootja salvestatud teave), millele saab hiljem juurdepääsu muu isik, kuulub seega artikli 5 lõike 3 kohaldamisalasse.“*[20] Sellest tulenevalt ei piirata juurdepääsu mõiste kohaldamiseks lõppseadmes oleva teabe päritolu.

32. Kui üksus astub samme, et saada juurdepääs lõppseadmesse salvestatud teabele, kohaldatakse e-privaatsuse direktiivi artikli 5 lõiget 3. Tavaliselt tähendab see, et juurdepääsu saav üksus saadab lõppseadmele ennetavalt konkreetsed juhised suunatud teabe saamiseks. See kehtib näiteks küpsiste kohta, mille korral juurdepääsu saav üksus annab lõppseadmele korralduse saata ennetavalt teavet iga järgmise hüperteksti edastusprotokolliga (HTTP) kutse kohta.

33. Nii on see ka siis, kui juurdepääsu saav üksus levitab salvestatud tarkvara kasutaja lõppseadmes ja saadab seejärel ennetavalt kutse võrgu kaudu rakendusliidese (API) lõpp-punktile. Muud näited on JavaScripti kood, mille korral juurdepääsu saav üksus annab kasutaja brauserile korralduse saata asünkroonseid päringuid koos suunatud teabega. Selline juurdepääs kuulub selgelt e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamisalasse, sest juurdepääsu saav üksus annab lõppseadmele selgesõnalise korralduse teabe saatmiseks.

34. Mõnel juhul ei pruugi üksus, kes annab lõppseadmele korralduse suunatud andmed tagasi saata, ja teavet saav üksus olla sama. See võib tuleneda kummagi üksuse vahelise ühismehhanismi loomisest ja/või kasutamisest. Kui seadmele antakse korraldus saata juba salvestatud teavet (näiteks protokolli või SDK[21] abil, mis tähendab, et lõppseade saadab teavet ennetavalt), on võimalik tungida lõppseadmesse, mistõttu toob selline juurdepääs kaasa e-privaatsuse direktiivi artikli 5 lõike 3 kohaldatavuse. Nagu on märgitud artikli 29 töörühma arvamuses 09/2014, võib see nii olla siis, kui veebileht annab lõppseadmele korralduse saata jälituspiksli lisamise kaudu teavet kolmandate isikute reklaamiteenustele[22]. Seda kasutusjuhtumit käsitletakse üksikasjalikult punktis 3.1.

2.6 Mõisted „teabe salvestamine“ ja „salvestatud teave“ – kriteerium C.2

35. Teabe salvestamine e-privaatsuse direktiivi artikli 5 lõike 3 tähenduses on teabe paigutamine füüsilisele elektroonilisele andmekandjale, mis on kasutaja või abonendi lõppseadme osa[23].

36. Tavaliselt ei salvestata teavet kasutaja või abonendi lõppseadmesse teise isiku otsese juurdepääsu kaudu seadme mälule, vaid pigem andes lõppseadmes olevale tarkvarale korralduse genereerida konkreetset teavet. Selliste korralduste alusel toimuv salvestamine loetakse vahetult algatatuks teise isiku poolt. See hõlmab nii väljakujunenud protokollide, näiteks brauseriküpsiste salvestamise kui ka kohandatud tarkvara kasutamist, olenemata sellest, kes lõi need protokollid või tarkvara või paigaldas lõppseadmesse.

[20] Artikli 29 töörühma arvamus 9/2014, lk 8.
[21] SDK (tarkvaraarenduskomplekt) on tarkvaraarenduse vahendite pakett, mis tehakse kättesaadavaks rakendustarkvara loomise hõlbustamiseks.
[22] Artikli 29 töörühma arvamus 9/2014, lk 9.
[23] Nagu on määratletud suuniste punktis 2.3.

37. e-privaatsuse direktiiv ei sea ülem- ega alampiiri ajale, mille jooksul peab teave säilima andmekandjal, et seda saaks lugeda salvestatuks, samuti puudub salvestatava teabe koguse ülem- ja alampiir.

38. Samuti ei sõltu salvestamise mõiste andmekandja liigist, millele teave salvestatakse. Tüüpilised näited on kõvakettaseadmed (HDD), pooljuhtkettaseadmed (SSD), programmeeritavad elekterkustutusega püsimälud (EEPROM) ja muutmälu (RAM), kuid vähem tüüpilised stsenaariumid, mis hõlmavad sellist andmekandjat nagu magnetlint või keskprotsessori (CPU) vahemälu, ei ole kohaldamisalast välja jäetud. Andmekandja võib olla ühendatud seesmiselt (nt SATA-ühenduse kaudu) või väliselt (nt USB-ühenduse kaudu).

39. „Salvestatud teave" tähendab teavet, mis on lõppseadmes juba olemas, olenemata selle teabe allikast või laadist. See hõlmab kõiki tulemusi, mis on saadud teabe salvestamisel e-privaatsuse direktiivi artikli 5 lõike 3 tähenduses, nagu eespool kirjeldatud (kas sama isiku poolt, kes hiljem saaks juurdepääsu, või muu kolmanda isiku poolt). Lisaks hõlmab see e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamisalast välja jäävate teabesalvestusprotsesside tulemusi, näiteks salvestamine lõppseadmesse kasutaja või abonendi enda või riistvaratootja poolt (nt võrguliidese kontrollerite MAC-aadressid), lõppseadmesse sisseehitatud andurid või lõppseadmes käivitatud protsessid ja programmid, mis võivad, kuid ei pruugi anda teavet, mis sõltub salvestatud teabest või tuleneb sellest.

3 KASUTUSJUHTUMID

40. Nagu on märgitud käesolevate suuniste sissejuhatuses[24], ei analüüsita suunistes e-privaatsuse direktiivi artikli 5 lõikes 3 sätestatud nõusoleku saamise kohustuse erandite kohaldamist. EAKN tuletab meelde, et alati, kui teavet salvestatakse või kui saadakse juurdepääs juba salvestatud teabele, tuleks hinnata, kas on vaja nõusolekut või kas saaks kohaldada e-privaatsuse direktiivi artikli 5 lõike 3 kohast erandit. Lugeja peaks seepärast kaalutlema erandeid oma kasutusjuhtumi korral koos tehnilise analüüsiga.

41. Ilma et see piiraks erikonteksti, milles saab kasutada tehnilisi kategooriaid, mida on vaja kontrollimisel, kas e-privaatsuse direktiivi artikli 5 lõiget 3 saab kohaldada, on võimalik mitteammendavalt tuvastada laialt kasutatavate identifikaatorite ja teabe üldkategooriad, mille suhtes võidakse kohaldada e-privaatsuse direktiivi artikli 5 lõiget 3.

42. Võrguside põhineb tavaliselt kihtmudelil, mis vajab identifikaatorite kasutamist, et võimaldada side nõuetekohast loomist ja toimumist. Nende identifikaatorite edastamine kaugosalejatele toimub tarkvara abil vastavalt kokkulepitud sideprotokollidele. Nagu eespool märgitud, ei välista asjaolu, et vastuvõttev üksus ei pruugi olla teabe saatmist korraldav üksus, e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamist. See võib olla seotud marsruutimise identifikaatoritega, näiteks lõppseadme MAC- või IP-aadressiga, kuid ka seansi identifikaatoritega (SSRC, Websocketi identifikaator) või autentimistokenitega.

43. Samamoodi võib rakendusprotokollis olla mitu mehhanismi kontekstiandmete esitamiseks (nt HTTP-päis, sh aksepteerimisväli või kasutajaagent), puhverdusmehhanism (nt ETag[25]) või muud funktsioonid (üks neist on küpsised või HSTS[26]). Taas võib nendele mehhanismidele tuginemine teabe kogumisel

[24] Vt punkt 4 eespool.
[25] HTTP ETag on identifikaator, mis võimaldab teha tingimuslikke päringuid puhverdatud kliendiandmete kehtivuse alusel.
[26] HTTP Strict Transport Security (HSTS) võimaldab serveritel määrata, mis ressursse alati taotleda HTTPS-ühenduste abil.

(näiteks seadmetuvastuse[27] või ressursiidentifikaatorite jälgimise kontekstis) viia e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamiseni.

44. Teisalt on olukordi, kus lõppseadmesse paigaldatud kohalikud rakendused kasutavad teatud teavet rangelt lõppseadmes, näiteks nutitelefoni süsteemi APId (juurdepääs kaamerale, mikrofonile, GPS-andurile, kiirenduskiibile, raadiokiibile, juurdepääs kohalikele failidele, kontaktiloendile, juurdepääs identifikaatoritele jne). See võib kehtida ka veebibrauserite kohta, mis töötlevad salvestatud või loodud teavet seadmes (nt küpsised, kohalik salvestusruum, WebSQL või isegi kasutajate endi esitatud teave). Sellise teabe kasutamine rakenduse poolt ei ole „juurdepääsu saamine juba salvestatud teabele“ e-privaatsuse direktiivi artikli 5 lõike 3 tähenduses seni, kuni teave ei välju seadmest, kuid kui sellele teabele või selle teabe tuletisele saadakse juurdepääs, kohaldatakse e-privaatsuse direktiivi artikli 5 lõiget 3.

45. Mõnedel juhtudel levitavad osalejad kahjurtarkvara elemente, näiteks krüptokaevetarkvara või üldisemalt pahavara, kasutades lõppseadmete töötlemissuutlikkust levitava osaleja huvides. Nimetatud pahavara levitamine kasutaja lõppseadmes oleks „salvestamine“ e-privaatsuse direktiivi artikli 5 lõike 3 tähenduses. Lisaks, kui tarkvara loob võrguühenduse, et saata teavet hilisemas etapis, oleks see „juurdepääsu saamine“ e-privaatsuse direktiivi artikli 5 lõike 3 tähenduses.

46. Allpool on konkreetne analüüs nende kategooriate kohta, mis pakuvad erihuvi kas nende laialdase kasutamise tõttu või seepärast, et nende kasutamise asjaolusid on vaja eraldi uurida.

3.1 URL- ja pikseljälitus

47. Jälituspiksel on hüperlink ressursile, tavaliselt kujutisfailile, mis on manustatud veebilehe või e-kirja sisusse. Tavaliselt puudub sellel pikselil eesmärk seoses taotletava sisuga; selle ainus eesmärk on automaatselt luua side kliendi ja piksli vastuvõtja vahel, mida muidu ei toimuks. See ei ole siiski süstemaatiline ja jälituspiksleid saab luua ka täiendava teabe lisamisega hüperlingiga laaditavatele kujutistele, mis on kasutajale kuvatava sisu seisukohast olulised. Side loomine edastab piksli kasutajale mitmesugust teavet, sõltuvalt konkreetsest kasutusjuhtumist.

48. E-kirja korral võib saatja lisada jälituspiksli, et tuvastada, millal loeb saaja e-kirja. Veebilehtede jälituspikslid võivad olla seotud üksusega, kes kogub palju selliseid päringuid ja suudab seega jälgida kasutajate käitumist. Sellised jälituspikslid võivad sisaldada lingi osana ka täiendavaid identifikaatoreid, metaandmeid või sisu. Need andmepunktid võib lisada veebilehe omanik, võib-olla seoses kasutaja tegevusega veebilehel, et koostada analüütilisi kasutusaruandeid. Need võivad olla ka dünaamiliselt genereeritud kliendipoolse rakendusloogika abil, mille on esitanud üksus.

49. Jälituslingid võivad toimida samamoodi, kuid identifikaator lisatakse veebilehe aadressile. Kui kasutaja külastab ühtset ressursilokaatorit (URL), laadib sihiks olev veebileht soovitud ressursi, kuid saab ka identifikaatori, mis ei ole ressursi tuvastamiseks asjakohane. Neid kasutatakse väga sageli e-kaubanduse veebilehtedel, et tuvastada sissetuleva liikluse allikas. Näiteks võivad sellised veebilehed pakkuda jälgitavaid linke partneritele kasutamiseks nende domeenis, et e-kaubanduse veebikoht teaks, kes nende partneritest vastutab müügi eest ja maksab komisjonitasu (partnerturundus).

50. Jälituslinke ja jälituspiksleid saab levitada mitmesuguste kanalite kaudu, näiteks e-kirjade, veebilehtede või jälituslinkide puhul isegi mis tahes tekstisõnumiteenuste kaudu. Selline jaotamine kasutaja lõppseadmesse on salvestamine vähemalt kliendipoolse tarkvara puhverdamise mehhanismi

[27] Nagu on märgitud sissejuhatuses, vt artikli 29 töörühma arvamus 9/2014 e-privaatsuse direktiivi kohaldamise kohta seadmetuvastuse suhtes

kaudu. Seega kohaldatakse e-privaatsuse direktiivi artikli 5 lõiget 3, isegi kui selline salvestamine ei ole püsiv.

51. Jälgimisandmete lisamine kasutajale saadetud URL-idele või kujutistele (pikslid) on korraldus lõppseadmele saata tagasi suunatud teave (määratud identifikaator). Dünaamiliste jälituspikslite korral on korralduseks rakendusloogika (tavaliselt JavaScript-koodi) levitamine. Sellest tulenevalt võib järeldada, et selliste jälgimismehhanismide kaudu esitatud identifikaatorite kogumine on „juurdepääsu saamine“ e-privaatsuse direktiivi artikli 5 lõike 3 tähenduses, mistõttu kohaldatakse seda ka selle etapi suhtes.

3.2 Kohalik töötlemine

52. Mõni tehnoloogia tugineb kohalikule töötlusele, mida juhendab kasutajate lõppseadmetes levitatav tarkvara, kus kohalikul töötlemisel saadud teave tehakse seejärel valitud osalejatele kättesaadavaks kliendipoolse rakendusliidese kaudu. See võib nii olla näiteks veebibrauseri pakutava rakendusliidese korral, kus kohapeal loodud tulemustele on võimalik saada kaugjuurdepääs.

53. Kui töödeldud teave tehakse millal tahes ja näiteks kliendipoolses koodis kättesaadavaks kolmandale isikule, näiteks saadetakse see võrgu kaudu serverisse tagasi, oleks selline toiming (mida korraldab kasutaja lõppseadmes levitatavat kliendipoolset koodi tootev üksus) „juurdepääsu saamine juba salvestatud teabele“. Asjaolu, et see teave luuakse kohalikult, ei välista e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamist.

3.3 Ainult IP-põhine jälgimine

54. Mõni teenusepakkuja arendab lahendusi, mis tuginevad ainult ühe komponendi, nimelt IP-aadressi kogumisele, et jälgida kasutaja navigeerimist[28], mõnel juhul ka mitme domeeni ulatuses. Sellega seoses võiks kohaldada e-privaatsuse direktiivi artikli 5 lõiget 3, kuigi IP kättesaadavaks tegemise korralduse on andnud muu üksus kui vastuvõtja.

55. IP-aadressidele juurdepääsu saamine tooks siiski kaasa e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamise üksnes siis, kui see teave pärineb abonendi või kasutaja lõppseadmest. Kuigi see ei ole süstemaatiliselt nii (näiteks kui CGNAT[29] on aktiveeritud), kuuluksid selle alla kasutaja ruuterist lähtuvad staatilised väljuvad IPv4-aadressid, samuti IPV6-aadressid, sest neid määratleb osaliselt host. Kui üksus ei suuda tagada, et IP-aadress ei pärine kasutaja või abonendi lõppseadmest, peab ta võtma kõik e-privaatsuse direktiivi artikli 5 lõike 3 kohased meetmed.

56. Kuigi siin suunistes ei analüüsita e-privaatsuse direktiivi artikli 5 lõikes 3 sätestatud nõusoleku saamise kohustuse erandite kohaldamist, on oluline taas meenutada, et selle artikli kohaldatavus ei tähenda süstemaatiliselt, et nõusolek on vaja saada. Seega tuletab EAKN meelde, et alati tuleks hinnata, kas nõusolekut on vaja või kas saaks kohaldada e-privaatsuse direktiivi artikli 5 lõike 3 kohast erandit[30].

[28] Lisaks ja olenemata IP-aadressi otstarbest ja funktsioonist aluseks oleva tehnilise side loomisel ja edastamisel või sellest, et see võib olla isikuandmed või mitte (e-privaatsuse analüüsis on see „teave“).
[29] Internetiteenuse pakkujad kasutavad piiratud IP-aadressiruumi maksimaalseks kasutamiseks operaatori tasemel NAT-i või CGNAT-i. See rühmitab mitu abonenti sama avaliku IP-aadressi alla.
[30] Artikli 29 töörühma arvamuses 9/2014 on näited, millal ei pruugi olla nõusolekut vaja.

3.4 Ajutine ja vahendatud IoT-aruandlus

57. Esemevõrgu (IoT) seadmed toodavad teavet pidevalt, näiteks seadmesse sisseehitatud andurite kaudu, mida võidakse, kuid ei pruugi, kohalikult eeltöödelda. Sageli tehakse teave kättesaadavaks kaugserverile, kuid see võidakse saada mitmeti.

58. Mõnel IoT-seadmel on otseühendus üldkasutatava sidevõrguga mobiilside SIM-kaardi kaudu. Teistel võib olla kaudne ühendus üldkasutatava sidevõrguga, näiteks WiFi kasutamise või teabe edastamise kaudu teisele seadmele kakspunktühenduse kaudu (näiteks Bluetoothi kaudu). Teine seade võib olla näiteks nutitelefon või spetsiaalne värav, mis võib teavet enne serverisse saatmist eeltöödelda või mitte.

59. Tootja võib anda IoT-seadmetele korralduse kogutud teavet alati voogedastada, kuid siiski puhverdada teave kõigepealt kohalikult, näiteks kuni ühendus on kättesaadav.

60. Igal juhul käsitatakse IoT-seadet, kui see on (otseselt või kaudselt) ühendatud üldkasutatava sidevõrguga, lõppseadmena. Asjaolu, et teavet voogedastatakse või puhverdatakse ajutise aruandluse jaoks, ei muuda selle teabe olemust. Mõlemal juhul kohaldataks e-privaatsuse direktiivi artikli 5 lõiget 3, sest kui IoT-seadmes oleva koodi abil antakse korraldus saata dünaamiliselt salvestatud andmed kaugserverisse, on see „juurdepääsu saamine“.

3.5 Kordumatu tunnus

61. Ettevõtted kasutavad sageli mõistet „kordumatud tunnused“ või „püsiidentifikaatorid“. Selliseid identifikaatoreid saab tuletada püsivatest isikuandmetest (ees- ja perekonnanimi, e-posti aadress, telefoninumber jt), mis on kasutaja seadmes räsitud, mida kogutakse ja jagatakse mitme vastutava töötleja vahel, et tuvastada isik üheselt eri andmekogumite kaudu (veebilehe või rakenduse kasutamisel kogutud andmete kasutamine, kliendisuhtehalduse (CRM) andmed, mis on seotud ostu või tellimusega internetis või mujal jne). Veebilehtedel kogutakse püsivaid isikuandmeid tavaliselt autentimise või uudiskirjade tellimise raames.

62. Nagu eespool märgitud, ei välista asjaolu, et kasutaja sisestab teavet, e-privaatsuse direktiivi artikli 5 lõike 3 kohaldamist seoses salvestamisega, sest see teave salvestatakse ajutiselt lõppseadmesse enne selle kogumist.

63. „Kordumatu tunnuse“ kogumisel veebikohtades või mobiilirakendustes annab koguv üksus brauserile korralduse see teave saata (kliendipoolse koodi levitamise kaudu). Seega toimub „juurdepääsu saamine“ ja kohaldatakse e-privaatsuse direktiivi artikli 5 lõiget 3.