

Ohjeet



Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan teknistä soveltamisalaa koskevat ohjeet 2/2023

Versio 2.0

Annettu 7. lokakuuta 2024

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Aiemmat versiot

Versio 1.0	14. marraskuuta 2023	Ohjeiden hyväksyminen julkista kuulemista varten
Versio 2.0	7. lokakuuta 2024	Ohjeiden hyväksyminen julkisen kuulemisen jälkeen

Tiivistelmä

Näissä ohjeissa Euroopan tietosuojaneuvosto käsittelee sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan sovellettavuutta erilaisiin teknisiin ratkaisuihin. Näillä ohjeilla laajennetaan 29 artiklan mukaisen työryhmän lausuntoa 9/2014 sähköisen viestinnän tietosuojadirektiivin soveltamisesta laitesormenjalkeen ja pyritään antamaan selkeä käsitys sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitetuista teknisistä toimista.

Uusista seurantamenetelmistä, jotka korvaavat nykyisiä seurantatyökaluja (esimerkiksi evästeet, koska jotkin selainvalmistajat eivät enää tue kolmannen osapuolen evästeitä) ja luovat uusia liiketoimintamalleja, on tullut kriittinen tietosuojaan liittyvä huolenaihe. Vaikka sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan sovellettavuus on vahvistettu ja pantu täytäntöön tiettyjen jäljitysteknologioiden, kuten evästeiden, osalta, on tarvetta käsitellä epäselvyyksiä, joita liittyy kyseisen säännöksen soveltamiseen uusien jäljitystyökalujen yhteydessä.

Ohjeissa yksilöidään kolme keskeistä tekijää sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisen kannalta (2.1 jakso): "tiedot", "tilaajan tai käyttäjän päätelaite" ja "tietojen käyttö" ja "tietojen tallentaminen sekä tallennetut tiedot". Lisäksi ohjeissa analysoidaan yksityiskohtaisesti kutakin tekijää (2.2–2.6 jakso).

3 jaksossa tätä analyysiä sovelletaan ei-tyhjentävään luetteloon käytön tapauksista, jotka edustavat seuraavia yleisiä tekniikoita:

- URL-osoitteet ja pikseliseuranta
- Paikallinen käsittely
- Ainoastaan IP-osoitteisiin perustuva seuranta
- Ajoittainen ja välitetty IoT-raportointi
- Yksilöllinen tunniste

Sisällysluettelo

1	Johdanto.....	5
2	Analyysi	6
2.1	Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisen keskeiset osatekijät.....	6
2.2	”Tiedon” käsite - kriteeri A.....	7
2.3	Käsite ”tilaajan tai käyttäjän päätelaite” – kriteeri B.1.....	7
2.4	”Yleisen viestintäverkon” käsite – kriteeri B.2	9
2.5	Käsite "tietojen käyttö" – kriteeri C.1.	10
2.6	Käsitteet "tietojen tallentaminen" ja "tallennetut tiedot" – kriteeri C.2.	11
3	Käyttötapaukset	12
3.1	URL-osoitteet ja pikseliseuranta	13
3.2	Paikallinen käsittely.....	14
3.3	Ainoastaan IP-osoitteisiin perustuva seuranta	14
3.4	Ajoittainen ja välitetty IoT-raportointi.....	15
3.5	Yksilöllinen tunniste	15

Euroopan tietosuojaneuvosto, joka

ottaa huomioon luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta 27 päivänä huhtikuuta 2016 annetun Euroopan parlamentin ja neuvoston asetuksen 2016/679/EU, jäljempänä 'yleinen tietosuoja-asetus', 70 artiklan 1 kohdan e alakohdan,

ottaa huomioon ETA-sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6. päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018¹,

ottaa huomioon henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 12 päivänä heinäkuuta 2002 annetun Euroopan parlamentin ja neuvoston direktiivin 2002/58/EY, sellaisena kuin se on muutettuna direktiivillä 2009/136/EY (jäljempänä 'sähköisen viestinnän tietosuojadirektiivi'), 15 artiklan 3 kohdan,

ottaa huomioon työjärjestyksensä 12 ja 22 artiklan,

JA ON ANTANUT SEURAAVAT OHJEET:

1 JOHDANTO

1. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaan viestintäverkkojen käyttö *tietojen tallentamiseksi tai tilaajan tai käyttäjän päätelaitteelle tallennettujen tietojen käyttämiseen sallitaan* vain suostumuksen tai tarpeellisuuden perusteella kyseisessä artiklassa säädettyjä erityisiä tarkoituksia varten. Kuten sähköisen viestinnän tietosuojadirektiivin² johdanto-osan 24 kappaleessa muistutetaan, kyseisen säännöksen tavoitteena on suojata käyttäjien päätelaitteita, koska ne ovat osa käyttäjien yksityiselämää. Kyseisen artiklan sanamuodosta seuraa, että sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa ei sovelleta yksinomaan evästeisiin vaan myös "samankaltaisiin teknologioihin". Tällä hetkellä ei kuitenkaan ole kattavaa luetteloa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitetuista teknisistä toimista.
2. 29 artiklan mukaisen tietosuojatyöryhmän (jäljempänä 'tietosuojatyöryhmä') lausunnossa 9/2014 (jäljempänä tietosuojatyöryhmän lausunto 9/2014) sähköisen viestinnän tietosuojadirektiivin soveltamista laitesormenjälkiin on jo selvennetty, ja laitesormenjäljet kuuluvat sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan tekniseen soveltamisalaan³. Koska teknologiat ovat kehittyneet, tarvitaan lisäohjeita nykyisiä tunnistettuja seurantatekniikoita varten. Tekninen ympäristö on kehittynyt viime vuosikymmenen aikana. Käyttöjärjestelmiin sulautettujen tunnistimien käyttö on

¹ Viittauksilla jäsenvaltioihin tarkoitetaan koko tässä asiakirjassa ETA:n jäsenvaltioita.

² "Sähköisten viestintäverkkojen käyttäjien päätelaitteet ja tällaisille laitteille tallennetut tiedot kuuluvat käyttäjien yksityiselämän alueeseen, mikä edellyttää ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn eurooppalaisen yleissopimuksen mukaista suojaa. Niin sanotut urkintatekniikat, jäljitteet, salatut tunnisteet ja muut vastaavat menetelmät mahdollistavat pääsyn käyttäjän päätelaitteelle tämän tietämättä tarkoituksena tiedon saanti, salatun tiedon tallentaminen tai käyttäjän toimien jäljittäminen, ja ne saattavat vakavasti loukata näiden käyttäjien yksityisyyttä. Tällaisten menetelmien käyttö olisi sallittava vain laillisiin tarkoituksiin ja siten, että kyseiset käyttäjät tietävät asiasta."

³ Tietosuojatyöryhmän lausunto 9/2014, s. 11.

lisääntynyt, ja lisäksi on luotu uusia työkaluja, jotka mahdollistavat tietojen tallentamisen päätelaitteisiin.

3. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisalaa koskeva tulkinnanvaraisuus on luonut kannustimia toteuttaa vaihtoehtoisia ratkaisuja internetin käyttäjien jäljittämiseksi ja johtanut pyrkimykseen kiertää sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädettyjä oikeudellisia velvoitteita. Kaikki tällaiset tilanteet herättävät huolta ja edellyttävät lisäanalyysia Euroopan tietosuojaneuvoston aiemman ohjeistuksen täydentämiseksi.
4. Näiden ohjeiden tarkoituksena on tehdä tekninen analyysi sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisalasta eli selvittää, mitä lauseeseen *"tallentaa tietoja tai käyttää tilaajan tai käyttäjän päätelaitteelle tallennettuja tietoja"* teknisesti sisältyy. Näissä ohjeissa ei käsitellä tilanteita, joissa käsittelytoimi voi kuulua sähköisen viestinnän tietosuojadirektiivissä säädettyjen suostumusvaatimusta koskevien poikkeusten soveltamisalaan,⁴ koska näitä tapauksia olisi analysoitava tapauskohtaisesti ottaen huomioon sen, miten jäsenvaltio on saattanut direktiivin osaksi kansallista lainsäädäntöään, ja kansallisten toimivaltaisten viranomaisten antamat ohjeet.
5. Näiden ohjeiden loppuosassa analysoidaan erityisiä käyttötapauksia koskevaa luetteloa, joka ei ole tyhjentävä.

2 ANALYYSI

2.1 Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisen keskeiset osatekijät

6. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa sovelletaan seuraavissa tapauksissa:
 - a. **KRITEERI A:** toteutetut toimet liittyvät *"tietoihin"*. On huomattava, että käytetty termi ei ole *"henkilötiedot"* vaan *"tiedot"*.
 - b. **KRITEERI B:** suoritettuihin toimintoihin liittyy tilaajan tai käyttäjän *"pätelaitte"* (B.1), mikä merkitsee tarvetta arvioida *"yleisen viestintäverkon"* käsitettä (B.2).
 - c. **KRITEERI C:** suoritetut toimet todellakin ovat *"tallentamista"* (C.1) tai *"tietojen käyttämistä"* (C.2). Näitä kahta käsitettä voidaan tutkia riippumattomasti, kuten tietosuojatyöryhmän lausunnossa 9/2014 muistutetaan: *"- - tallentaminen tai käyttäminen" käyttö merkitsee, että tallentamisen ja käyttämisen ei tarvitse tapahtua saman viestinnän aikana eikä saman toimijan toimesta"*⁵.

Luettavuuden vuoksi käyttäjän päätelaitteeseen tallennettuihin tietoihin käsiksi pääsevää yksikköä kutsutaan jäljempänä *"tietoihin pääseväksi yksiköksi"*.

⁴ Kuten sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa todetaan: *"Tämä ei estä teknistä tallentamista tai käyttöä, jonka ainoana tarkoituksena on toteuttaa viestinnän välittäminen sähköisissä viestintäverkoissa tai helpottaa sitä tai joka on ehdottoman välttämätöntä sellaisen tietoyhteiskunnan palvelun tarjoamiseksi, jota tilaaja tai käyttäjä on erityisesti pyytänyt."*

⁵ Tietosuojatyöryhmän lausunto 9/2014, s. 8.

2.2 ”Tiedon” käsite - kriteeri A

7. Kuten KRITEERISSÄ A todetaan, tässä jaksossa selvitetään seikkaperäisesti, mitä käsite ”tieto” kattaa. Termi tiedot, joka on henkilötietojen käsitettä laajempi luokka, liittyy sähköisen viestinnän tietosuojadirektiivin soveltamisalaan.
8. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan tavoitteena on suojella käyttäjien yksityisyyttä, kuten direktiivin johdanto-osan 24 kappaleessa todetaan: *”Sähköisten viestintäverkkojen käyttäjien päätelaitteet ja tällaisille laitteille tallennetut tiedot kuuluvat käyttäjien yksityiselämän alueeseen, mikä edellyttää ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn eurooppalaisen yleissopimuksen mukaista suojaa.”* Yksityiselämä suojellaan myös EU:n perusoikeuskirjan 7 artiklassa.
9. Itse asiassa 5 artiklan 3 kohdan ja sähköisen viestinnän tietosuojadirektiivin johdanto-osan 24 sanamuodot kattavat nimenomaan skenaariot, jotka tunkeutuvat tälle yksityiselle alueelle, vaikka niihin ei liittyisi henkilötietoja, esimerkiksi virusten tallentamisen käyttäjän päätelaitteeseen. Tämä osoittaa, että termin ”tieto” määritelmää ei pitäisi rajoittaa siihen, että se liittyy tunnistettuun tai tunnistettavaan luonnolliseen henkilöön.
10. Euroopan unionin tuomioistuimien on vahvistanut tämän seuraavasti: *”Tätä suojaa sovelletaan kaikkiin tällaiselle päätelaitteelle tallennettuihin tietoihin riippumatta siitä, onko kyse henkilötiedoista vai ei, ja sen tarkoituksena on tästä samasta johdanto-osan perustelukappaleesta ilmenevällä tavalla muun muassa suojata käyttäjiä vaaralta siitä, että salatut tunnisteet tai muut vastaavat menetelmät pääsevät näiden käyttäjien päätelaitteelle heidän tietämättään”*⁶.
11. Kysymyksiä siitä, olisiko näiden tietojen alkuperä ja syyt, joiden vuoksi ne on tallennettu päätelaitteisiin, otettava huomioon arvioitaessa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltuvuutta, on selvitetty aiemmin. Esimerkiksi tietosuojatyöryhmän lausunnossa 9/2014: *”Tätä ei voida tulkita siten, että kolmas osapuoli ei tarvitsisi suostumusta näiden tietojen käyttämiseen pelkästään koska ei ole itse tallentanut tietoja. Suostumusta koskevaa vaatimusta sovelletaan myös käsiteltäessä vain luettavissa olevaa arvoa (esimerkiksi pyydettyä verkkoliitännän MAC-osoitetta käyttöjärjestelmän sovellusliittymän kautta)”*⁷.
12. Yhteenvetona voidaan todeta, että tiedon käsite kattaa sekä muut kuin henkilötiedot että henkilötiedot riippumatta siitä, miten tiedot on tallennettu ja kuka ne on tallentanut, eli onko ne tallentanut ulkopuolinen taho (myös muu taho kuin se, joka voi päästä tietoihin), käyttäjä, valmistaja tai mikä tahansa muu yksityisyyteen tunkeutumisen skenaarioon liittyvä taho.

2.3 Käsite ”tilaajan tai käyttäjän päätelaite” – kriteeri B.1

13. Tämä jakso perustuu määritelmään, jota käytetään direktiivissä 2008/63/EY – ja johon viitataan direktiivin (EU) 2018/1972 2 artiklassa – jossa ”pätelaite” määritellään seuraavasti: *”suoraan tai välillisesti yleisen televerkon rajapintaan liitettyä tietojen lähettämiseen, käsittelyyn tai vastaanottamiseen tarkoitettua laitetta; molemmissa tapauksissa (suora tai välillinen) liitäntä voidaan tehdä johdoin, optisella kuidulla tai sähkömagneettisesti; yhteys on välillinen, jos on sijoitettu laite päätelaitteen ja verkon rajapinnan väliin”*⁸.

⁶ Unionin tuomioistuimen tuomio 1.10.2019, Planet 49, asiassa C-673/17, ECLI:EU:C:2019:801, 70 kohta.

⁷ Tietosuojatyöryhmän lausunto 9/2014, s. 8.

⁸ Komission direktiivi 2008/63/EY, annettu 20 päivänä kesäkuuta 2008, kilpailusta telepätelaitemarkkinoilla (kodifioitu toisinto), 1 artiklan 1 kohta.

14. Sähköisen viestinnän tietosuojadirektiivin johdanto-osan 24 kappaleessa annetaan selkeä käsitys päätelaitteiden roolista sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan tarjoaman suojan kannalta. Sähköisen viestinnän tietosuojadirektiivi suojaa käyttäjien yksityisyyttä paitsi heidän tietojensa luottamuksellisuuden osalta myös käyttäjän päätelaitteiden eheyden osalta. Tämä käsitys ohjaa päätelaitteen käsitteen tulkintaa näissä ohjeissa.
15. Sähköisen viestinnän tietosuojadirektiivin 3 artiklassa todetaan, että sähköisen viestinnän tietosuojadirektiiviä sovelletaan henkilötietojen käsittelyyn, joka liittyy yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa. Tämä tarkoittaa sitä, että laitteen olisi oltava käyttökelpoinen ollessaan yhteydessä tällaisen palvelun kanssa ja että laite olisi liitettävä tai kytkettävä yleisen viestintäverkon rajapintaan⁹, jotta se voidaan luokitella päätelaitteeksi. Tietosuojaneuvosto toteaa, että sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan tekstiin¹⁰ vuonna 2009 tehdyt muutokset laajensivat päätelaitteiden suojaa, kun poistettiin viittaus ”sähköisten viestintäverkkojen käyttöön” keinona tallentaa tietoja tai käyttää päätelaitteelle tallennettuja tietoja. Näin ollen niin kauan kuin laitteessa on verkkoliitäntä, joka mahdollistaa liitännän verkkoon (vaikka ei olisi käytössä), sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa sovelletaan kaikkiin yksiköihin, jotka tallentaisivat tietoja ja pääsisivät päätelaitteeseen jo tallennettuihin tietoihin katsomatta, miten päätelaitteeseen päästään ja onko laite kytketty verkkoon vai ei.
16. Laitteita, jotka ovat osa yleistä sähköistä viestintäverkkoa, ei katsottaisi päätelaitteiksi sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaan¹¹.
17. Päätelaite voi koostua useista yksittäisistä laitteista, jotka yhdessä muodostavat päätelaitteen. Tämä voi olla fyysisesti koteloitu laite, joka ylläpitää näyttö-, käsittely-, tallennus- ja oheislaitteita (kuten älypuhelimia, kannettavia tietokoneita, verkkoon kytkettyjä tallennuslaitteita, verkkoon liitettyjä autoja tai televisioita, älylaseja).
18. Sähköisen viestinnän tietosuojadirektiivissä tunnustetaan, että käyttäjän päätelaitteelle tallennettujen tietojen luottamuksellisuuden ja käyttäjän päätelaitteen eheyden suojaaminen ei rajoitu luonnollisten henkilöiden yksityiselämän suojeluun, vaan se koskee myös heidän kirjeenvaihtonsa tai oikeushenkilöiden oikeutettuja etujen kunnioittamista¹². Näin ollen päätelaite, joka mahdollistaa tämän kirjeenvaihdon ja oikeushenkilöiden oikeutetut edut, on suojattu sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan nojalla.
19. Käyttäjä tai tilaaja voi omistaa tai vuokrata päätelaitteen tai saada sen muulla tavoin käyttöönsä. Useilla käyttäjillä tai tilaajilla voi olla sama päätelaite.

⁹ Toisin sanoen on tekniset valmiudet liittyä verkkoon, vaikka yhteys ei olisi käytössä.

¹⁰ Euroopan parlamentin ja neuvoston direktiivi 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta (ETA:n kannalta merkityksellinen teksti), EUVL L 337, 18.12.2009, s. 11, 2 artiklan 5 kohta ja johdanto-osan 65 kappale.

¹¹ Verkon rajojen määrittämiseksi eri yhteyksissä viitataan BEREcin suuntaviivoihin yhteisistä lähestymistavoista verkon liityntäpisteen määrittämiseksi eri verkkotopologioissa (BoR (20) 46).

¹² Kuten eurooppalaisesta sähköisen viestinnän säännöstöstä 11 päivänä joulukuuta 2018 annetun Euroopan parlamentin ja neuvoston direktiivin (EU) 2018/1972 2 artiklan 13 kohdassa muistutetaan, käyttäjä voi olla luonnollinen henkilö tai oikeushenkilö.

20. Sähköisen viestinnän tietosuoja-direktiivi takaa tämän suojan käyttäjään tai tilaajaan liittyvälle päätelaitteelle, eikä se riipu siitä, onko käyttäjällä tarvittava käyttöoikeus (esimerkiksi onko hän käynnistänyt sähköisen viestinnän) tai edes siitä, tietääkö hän näistä käyttöoikeuksista.

2.4 ”Yleisen viestintäverkon” käsite – kriteeri B.2

21. Koska sähköisen viestinnän tietosuojadirektiivissä säännelty tilanne liittyy ”yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoamiseen yleisissä viestintäverkoissa yhteisössä”¹³ ja päätelaitteen määritelmässä mainitaan nimenomaan ”yleisen viestintäverkon” käsite, on ratkaisevan tärkeää selventää tätä käsitettä sen määrittämiseksi, missä yhteydessä sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa sovelletaan.
22. Sähköisen viestintäverkon käsitettä ei määritellä sähköisen viestinnän tietosuojadirektiivissä. Käsitteeseen viitattiin alun perin sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä annetussa direktiivissä 2002/21/EY (puitedirektiivi)¹⁴, joka korvattiin myöhemmin direktiivin 2018/1972 (eurooppalainen sähköisen viestinnän säännöstö) 2 artiklan 1 kohdalla. Se kuuluu nyt seuraavasti:

*”Tässä direktiivissä tarkoitetaan: sähköisellä viestintäverkolla” siirtojärjestelmiä riippumatta siitä, perustuvatko ne pysyvään infrastruktuuriin vai keskitettyyn hallintokapasiteettiin, sekä soveltuvin osin kytkentä- tai reitityslaitteistoa ja muita välineitä – myös verkkoelementtejä, jotka eivät ole aktiivisia – joilla voidaan siirtää signaaleja johtojen välityksellä, radioteitse, optisesti tai muulla sähkömagneettisella tavalla, mukaan luettuina satelliittiverkot, kiinteät (piiri- ja pakettikytkentäiset, mukaan luettuna internet) ja matkaviestintäverkot, sähkökaapelijärjestelmät siinä määrin kuin niitä käytetään signaalinsiirtoon, radio- ja televisiolähetyskäyttöön käytetyt verkot sekä kaapelitelevisioverkot riippumatta siitä, minkä tyyppistä informaatiota niissä siirretään”.*¹⁵

23. Tämä määritelmä on neutraali tiedonsiirtoteknologioiden osalta. Määritelmän mukaan sähköinen viestintäverkko on mikä tahansa verkkojärjestelmä, joka mahdollistaa sähköisten signaalien siirron sen yhtymäkohtien välillä riippumatta käytettävistä laitteista ja protokollista.
24. Direktiivin 2018/1972 mukainen sähköisen viestintäverkon käsite ei riipu infrastruktuurin julkisesta tai yksityisestä luonteesta eikä tavasta, jolla verkko otetaan käyttöön tai jolla sitä hallinnoidaan eli (*”perustuvatko ne pysyvään infrastruktuuriin vai keskitettyyn hallintokapasiteettiin”*¹⁶). Näin ollen direktiivin 2018/1972/EY 2 artiklan mukainen sähköisen viestintäverkon määritelmä on riittävän laaja kattamaan minkä tahansa infrastruktuurin. Siihen kuuluvat operaattorin hallinnoimat tai muut verkot, operaattoreiden ryhmän yhdessä hallinnoimat verkot tai jopa ad hoc-verkot, joissa päätelaite voi liittyä dynaamisesti muiden päätelaitteiden verkostoon tai poistua siitä lyhyen kantaman siirtoprotokollien avulla.

¹³ Sähköisen viestinnän tietosuojadirektiivin 3 artikla.

¹⁴ Euroopan parlamentin ja neuvoston direktiivi 2002/21/EY, annettu 7 päivänä maaliskuuta 2002, sähköisten viestintäverkkojen ja -palvelujen yhteisestä sääntelyjärjestelmästä (puitedirektiivi).

¹⁵ Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972, annettu 11 päivänä joulukuuta 2018, eurooppalaisesta sähköisen viestinnän säännöstöstä (uudelleenlaadittu), ETA:n kannalta merkityksellinen teksti, 2 artiklan 1 kohta.

¹⁶ Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/1972, annettu 11 päivänä joulukuuta 2018, eurooppalaisesta sähköisen viestinnän säännöstöstä (uudelleenlaadittu), ETA:n kannalta merkityksellinen teksti, 2 artiklan 1 kohta.

25. Tämä verkon määritelmä ei sisällä rajoituksia missään vaiheessa verkossa olevien päätelaitteiden määrälle. Jotkin verkkojärjestelmät perustuvat siihen, että yhtymäkohdat välittävät tietoa ad hoc -periaatteella parhaillaan yhteydessä oleville yhtymäkohdille¹⁷, ja jossakin vaiheessa voi olla vain kaksi keskenään kommunikoivaa vertaistahoa. Tällaiset tapaukset kuuluisivat sähköisen viestinnän tietosuojadirektiivin yleiseen soveltamisalaan, kunhan verkkoprotokolla mahdollistaa vertaisryhmien laajemman sisällyttämisen.
26. Viestintäverkon yleinen saatavuus on välttämätöntä, jotta laitetta voidaan pitää päätelaitteena ja sen voi katsoa kuuluvan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisalaan. On huomattava, että verkon antaminen vain rajatulle osalle yleisöä (esimerkiksi tilaajille riippumatta siitä, maksavatko he siitä vai eivät, jos kelpoisuusvaatimukset täyttyvät), ei tee verkosta yksityistä¹⁸.

2.5 Käsite "tietojen käyttö" – kriteeri C.1.

27. Jotta käsite "tietojen käyttö" voitaisiin määritellä asianmukaisesti, on tärkeää tarkastella sähköisen viestinnän tietosuojadirektiivin soveltamisalaa, josta mainitaan sen 1 artiklassa: *"- tarvitaan samantasoisien perusoikeuksien ja -vapauksien, erityisesti yksityisyyttä ja luottamuksellisuutta koskevan oikeuden, suojan varmistamiseksi henkilötietojen käsittelyssä sähköisen viestinnän alalla sekä tällaisten tietojen ja sähköisten viestintälaitteiden ja -palvelujen vapaan liikkuvuuden varmistamiseksi yhteisössä."*
28. Lyhyesti sanottuna sähköisen viestinnän tietosuojadirektiivi on yksityisyyttä suojaava oikeudellinen väline, jonka tarkoituksena on suojata viestinnän luottamuksellisuutta ja laitteiden eheyttä. Sähköisen viestinnän tietosuojadirektiivin johdanto-osan 24 kappaleessa selvennetään, että luonnollisten henkilöiden osalta käyttäjän päätelaite on osa heidän yksityisyyttään ja että siihen tallennettujen tietojen käyttäminen heidän tietämättään voi loukata vakavasti heidän yksityisyyttään.
29. Sähköisen viestinnän tietosuojadirektiivi suojaa myös oikeushenkilöitä¹⁹. Näin ollen sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaista "tietojen käyttämisen" käsitettä on tulkittava siten, että nämä oikeudet turvataan kolmansien osapuolten rikkomuksilta.
30. Tietojen tallentaminen ja käyttö voivat olla itsenäisiä toimintoja, ja niitä voivat suorittaa riippumattomat yksiköt. Sekä tietojen tallentamista että jo tallennettujen tietojen käyttöä ei edellytetä, jotta sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa voidaan soveltaa.
31. Kuten tietosuojatyöryhmän lausunnossa 9/2014 todetaan: *"Sanojen 'tallentaminen tai käyttäminen' käyttö merkitsee, että tallentamisen ja käyttämisen ei tarvitse tapahtua saman viestinnän aikana eikä saman toimijan toimesta. Yhden toimijan tallentama tieto (myös käyttäjän tai laitevalmistajan tallentama tieto), jota toinen toimija myöhemmin käyttää, kuuluu siis 5 artiklan 3 kohdan soveltamisalaan."*²⁰ Näin ollen päätelaitetta koskevien tietojen alkuperälle ei ole asetettu rajoituksia, jotta käytön käsitettä voitaisiin soveltaa.
32. Aina kun jokin yksikkö ryhtyy toimenpiteisiin käyttääkseen päätelaitteeseen tallennettuja tietoja, sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa. Tämä edellyttää yleensä sitä,

¹⁷ Esimerkiksi viivästystä sietävän verkkojärjestelmän yhteydessä, joka käyttää tallennus- ja välitystekniikoita (Briar in avoimen lähdekoodin hanke).

¹⁸ Lisätietoja julkisten viestintäverkkojen määrittämisestä on BERECin avoimen internetin sääntelyn toteuttamista koskevissa ohjeissa (BEREC Guidelines on the Implementation of the Open Internet Regulation, BoR (20) 112).

¹⁹ Sähköisen viestinnän tietosuojadirektiivin johdanto-osan 26 kappale, ks. kohta 17 edellä.

²⁰ Tietosuojatyöryhmän lausunto 9/2014, s. 8.

että tietoihin pääsevä yksikkö lähettää ennakoivasti erityisiä ohjeita päätelaitteelle saadakseen kohdennettuja tietoja. Näin on esimerkiksi evästeiden kohdalla, joissa tietoihin pääsevä yksikkö antaa päätelaitteelle ohjeet lähettää tietoja ennakoivasti kunkin myöhemmän Transfer Protocol (HTTP) - kutsun yhteydessä.

33. Näin on myös silloin, kun tietoihin pääsevä yksikkö jakaa käyttäjän päätelaitteeseen tallennetun ohjelmiston, joka sitten kutsuu ennakoivasti ohjelmointirajapintaa (API) verkon kautta. Lisäesimerkkejä ovat muun muassa JavaScript-koodi, jossa tietoihin pääsevä yksikkö ohjeistaa käyttäjän selainta lähettämään asynkronisia pyyntöjä kohdennettujen tietojen kanssa. Tällainen käyttö kuuluu selvästi sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisalaan, koska tietoihin pääsevä yksikkö nimenomaan ohjaa päätelaitteita lähettämään tiedot.
34. Joissakin tapauksissa yksikkö, joka ohjeistaa päätelaitteita lähettämään kohdennetun datan takaisin, ja tietoja vastaanottava taho ei välttämättä ole sama. Tämä voi johtua siitä, että nämä kaksi yksikköä tarjoavat ja/tai käyttävät yhteistä mekanismia. Laitteen ohjeistaminen lähettämään jo tallennetut tiedot (esimerkiksi käyttämällä protokollaa tai SDK:ta, joka²¹ edellyttää päätelaitteelta ennakoivaa tietojen lähettämistä) mahdollistaa tunkeutumisen päätelaitteisiin, joten tällainen käyttö johtaa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan sovellettavuuteen. Kuten tietosuojatyöryhmän lausunnossa 09/2014 todetaan, näin voi olla silloin, kun verkkosivustolla ohjeistetaan päätelaitetta lähettämään tietoja kolmannen osapuolen mainospalveluihin sisällyttämällä siihen kuvaviittauksia (pixel tag)²². Tätä käyttötapautta käsitellään tarkemmin 3.1 jaksossa.

2.6 Käsitteet "tietojen tallentaminen" ja "tallennetut tiedot" – kriteeri C.2.

35. Sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitetulla tietojen tallentamisella tarkoitetaan tietojen tallentamista fyysiselle sähköiselle tallennusvälineelle, joka on osa käyttäjän tai tilaajan päätelaitetta²³.
36. Tyypillisesti tietoja ei tallenneta käyttäjän tai tilaajan päätelaitteeseen siten, että toinen osapuoli pääsisi suoraan laitteen muistiin, vaan pikemminkin siten, että päätelaitteessa oleva ohjelmisto ohjataan tuottamaan erityistä tietoa. Tällaisen ohjeiden perusteella tapahtuvan tallentamisen katsotaan tapahtuvan suoraan toisen osapuolen aloitteesta. Tähän sisältyy vakiintuneiden protokollien, kuten selainevästeiden tallentaminen, sekä räätälöityjen ohjelmistojen käyttö riippumatta siitä, kuka on luonut tai asentanut protokollat tai ohjelmistot päätelaitteeseen.
37. Sähköisen viestinnän tietosuojadirektiivissä ei aseteta ylä- tai alarajaa sille, kuinka kauan tiedon on oltava tallennusvälineellä, jotta se voidaan katsoa tallennetuksi, eikä tallennettavan tiedon määrälle aseteta ylä- tai alarajaa.
38. Tallennuksen käsite vastaavasti ei riipu siitä, minkälaiselle välineelle tiedot tallennetaan. Tyypillisinä esimerkkeinä voisi mainita kiintolevyt (HDD), SSD-asetat, EEPROM:in ja hajasaantimuistin, mutta vähemmän tyypillisiä skenaarioita, joissa käytettyjä välineitä ovat esimerkiksi magneettinauha tai prosessori, ei jätetä soveltamisalan ulkopuolelle. Tallennusväline voidaan liittää sisäisesti (esim. SATA-liitännän kautta) tai ulkoisesti (esim. USB-liitännän kautta).

²¹SDK (ohjelmistokehityspaketti) on ohjelmistokehitystyökalujen kokonaisuus, joka on annettu saataville sovellusohjelmistojen luomisen helpottamiseksi.

²² Tietosuojatyöryhmän lausunto 9/2014, s. 9.

²³ Sellaisina kuin ne on määritelty 2.3 näiden ohjeiden jaksossa.

39. ”Tallennetuilla tiedoilla” tarkoitetaan päätelaitteessa jo olevia tietoja riippumatta kyseisten tietojen lähteestä tai luonteesta. Tähän sisältyy kaikki, mikä on tulosta sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitettusta tietojen tallentamisesta edellä kuvatulla tavalla (joko saman osapuolen toimesta, joka saisi myöhemmin pääsyn tietoihin, tai jonkin muun kolmannen osapuolen toimesta). Lisäksi se sisältää myös sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisalan ulkopuolelle jäävien tietojen tallennusprosessien tulokset, kuten käyttäjän tai tilaajan itsensä tai laitteiston valmistajan päätelaitteeseen tallentamat tiedot (kuten verkkosovittimen MAC-osoitteet), päätelaitteeseen integroidut anturit tai päätelaitteessa suoritettut prosessit ja ohjelmat, jotka voivat tai eivät voi tuottaa tallennetuista tiedoista riippuvaisia tai niistä johdettuja tietoja.

3 KÄYTTÖTAPAUKSET

40. Kuten edellä johdannossa todettiin²⁴, näissä ohjeissa ei analysoida sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädettyjen poikkeusten soveltamista velvollisuuteen saada suostumus. Tietosuojaneuvosto muistuttaa, että kaikissa tapauksissa, joissa tietoja säilytetään tai jo tallennettuja tietoja käytetään, olisi arvioitava, tarvitaanko suostumus vai voitaisiinko soveltaa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaista poikkeusta. Lukijan olisi sen vuoksi pohdittava poikkeuksia omalta kohdaltaan tämän teknisen analyysin kanssa.
41. Rajoittamatta sitä erityistä asiayhteyttä, jossa näitä teknisiä luokkia voidaan käyttää, mikä on tarpeen sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan sovellettavuuden määrittelemiseksi, on mahdollista määrittää ei-tyhjentävästi laajat tunnisteiden ja tietojen luokat, joita käytetään laajasti ja joihin voidaan soveltaa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa.
42. Verkkoviestintä perustuu yleensä kerrostettuun malliin, joka edellyttää tunnisteiden käyttöä, jotta viestintä voidaan luoda ja toteuttaa asianmukaisesti. Näiden tunnisteiden välittäminen etätoimijoille ohjataan ohjelmistolla sovittujen viestintäprotokollien mukaisesti. Kuten edellä todettiin, se, ettei vastaanottava yksikkö ehkä ole tietojen lähettämistä ohjeistava yksikkö, ei estä sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamista. Tämä voi koskea reititystunnuksia, kuten päätelaitteen MAC- tai IP-osoitetta, mutta myös istuntotunnuksia (SSRC, Websocket) tai tunnistevälineitä.
43. Samalla tavoin sovellusprotokollaan voi sisältyä useita mekanismeja kontekstietojen tarjoamiseksi (kuten HTTP-otsikko, mukaan lukien accept-kenttä tai käyttäjäagentti), välimuistiin tallentamismekanismi (kuten Etag)²⁵ tai muita toimintoja (esimerkiksi evästeet tai HSTS)²⁶. Jälleen kerran näiden mekanismien käyttäminen tietojen keräämiseen (esimerkiksi sormenjälkien²⁷ tai resurssitunnisteiden jäljittämisen yhteydessä) voi johtaa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamiseen.
44. Toisaalta joissakin tilanteissa päätelaitteeseen asennetut paikalliset sovellukset käyttävät joitakin tietoja ainoastaan päätelaitteen sisällä, mukaan lukien älypuhelimien järjestelmärajapinnat (pääsy

²⁴ Ks. edellä 4 kohta.

²⁵ HTTP ETag on tunnus, jonka avulla voidaan tehdä ehdollisia pyyntöjä välimuistiin tallennettujen asiakastietojen kelpoisuuden perusteella.

²⁶ HTTP Strict Transport Security (HSTS) avulla palvelimet voivat määrittää, mitä resursseja pyydetään aina HTTPS-yhteyksillä.

²⁷ Kuten johdannossa todettiin, ks. 29 artiklan mukaisen tietosuojatyöryhmän lausunto 9/2014 sähköisen viestinnän tietosuojadirektiivin soveltamisesta laitesormenjälkiin.

kameraan, mikrofoniin, GPS-anturiin, kiihdytinsiruun, radiosiruun, paikallisiin tiedostoihin, yhteystietoluetteloon, tunnisteisiin jne.). Näin voi olla myös sellaisten verkkoselainten kohdalla, jotka käsittelevät laitteen sisällä tallennettuja tai tuotettuja tietoja (kuten evästeet, paikallinen tallennus, WebSQL tai jopa käyttäjien itse toimittamat tiedot). Tällaisten tietojen käyttö sovelluksessa ei olisi sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitettua jo tallennettujen tietojen käyttämistä niin kauan kuin tiedot pysyvät laitteessa. Jos näihin tietoihin tai niiden mahdolliseen johtamiseen päästään käsiksi, sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa.

45. Joissakin tapauksissa toimijat levittävät myös haitallisia ohjelmistoja, esimerkiksi kryptolouhintaohjelmia tai yleisemmin haittaohjelmia, jotka hyödyntävät päätelaitteiden prosessointikykyä. Kyseisten haittaohjelmistojen levittäminen käyttäjän päätelaitteelle olisi sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitettua "tallentamista". Lisäksi, jos ohjelmisto muodostaa verkkoyhteyden tietojen lähettämiseksi myöhemmin, kyseessä on sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitettu "tietojen käyttämistä".
46. Jäljempänä esitetään erityinen analyysi joistakin näistä luokista, jotka ovat erityisen kiinnostavia joko niiden laajamittaisen käytön vuoksi tai siksi, että niiden käyttöolosuhteista on aiheellista tehdä erityistutkimus.

3.1 URL-osoitteet ja pikseliseuranta

47. Seurantapikseli on hyperlinkki resurssiin, yleensä kuvatiedostoon, joka sisältyy johonkin sisällön, kuten verkkosivuston tai sähköpostin, osaan. Tällä pikselillä ei yleensä ole mitään tehtävää, joka liittyisi pyydettyyn sisältöön itsessään. Sen ainoana tarkoituksena on luoda automaattisesti viestintäyhteys asiakkaan pikselin isännän välille, mitä ei muutoin olisi tapahtunut. Tämä ei kuitenkaan ole systemaattista, ja seurantapikseleitä voidaan luoda myös lisäämällä tietoja hyperlinkkien latauskuviin, joilla on merkitystä käyttäjälle näytettävän sisällön kannalta. Tiedonsiirron aloittaminen välittää pikselin isännälle erilaisia tietoja käyttötapauksesta riippuen.
48. Jos kyseessä on sähköpostiviesti, lähettäjä voi sisällyttää siihen seurantapikselin havaitakseen, milloin vastaanottaja lukee viestin. Verkkosivustojen seurantapikselit voivat linkittyä tahoon, joka kerää useita tällaisia pyyntöjä ja pystyy siten seuraamaan käyttäjien käyttäytymistä. Tällaiset seurantapikselit voivat sisältää myös muita tunnisteita, metatietoja tai sisältöä osana linkkiä. Verkkosivuston haltija voi lisätä näitä datapisteitä, jotka voivat liittyä käyttäjän toimintaan kyseisellä verkkosivustolla analyttisten käyttöraporttien tuottamiseksi. Ne voidaan myös luoda dynaamisesti yksikön toimittaman asiakaspuolen sovelluslogiikan avulla.
49. Seurantalinkit voivat toimia samalla tavalla, mutta tunniste liitetään verkkosivuston osoitteeseen. Kun käyttäjä käy URL-osoitteessa (Uniform Resource Locator), kohteena oleva verkkosivusto lataa pyydetyn resurssin, mutta kerää myös tunnisteiden, jolla ei ole resurssin tunnistamisen kannalta merkitystä. Verkkokauppasivustot käyttävät niitä hyvin yleisesti saapuvan liikenteen alkuperän tunnistamiseksi. Tällaiset verkkosivustot voivat esimerkiksi tarjota yhteistyökumppaneille jäljitettäviä linkkejä käytettäväksi verkkotunnuksillaan, jotta verkkokauppasivusto tietää yhteistyökumppanin, joka vastaa myynnistä ja maksaa välityspalkkion. Tämä tunnetaan nimellä affiliate-markkinointi tai kumppanuusmarkkinointi.
50. Sekä seurantalinkkejä että seurantapikseleitä voidaan jakaa monenlaisten kanavien kautta, esimerkiksi sähköpostin, verkkosivustojen tai, jos kyseessä ovat seurantalinkit, minkä tahansa tekstiviestijärjestelmän kautta. Tällainen jakelu käyttäjän päätelaitteelle on tallennusta ainakin

asiakaspuolen ohjelmiston välimuistimekanismin kautta. Näin ollen tällöin sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa, vaikka tallennus ei olisikaan pysyvää.

51. Seurantatietojen lisääminen käyttäjälle lähetettyihin URL-osoitteisiin tai kuviin (pikseleihin) on päätelaitteelle annettu ohje lähettää kohdennetut tiedot (määritetty tunniste) takaisin. Dynaamisesti rakennettujen seurantapikseleiden tapauksessa ohje on sovelluslogiikan (yleensä JavaScript-koodin) levittäminen. Näin ollen voidaan katsoa, että tällaisten seurantamekanismien kautta tapahtuva tunnisteiden kerääminen on sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa tarkoitettua "tietojen käyttämistä", joten sitä sovelletaan myös tähän.

3.2 Paikallinen käsittely

52. Jotkin tekniikat perustuvat käyttäjien päätelaitteisiin levitettävien ohjelmistojen ohjaamaan paikalliseen käsittelyyn, jossa paikallisen käsittelyn tuottamat tiedot asetetaan valittujen toimijoiden saataville asiakaspuolen ohjelmointirajapinnan kautta. Näin voi olla esimerkiksi verkkoselaimen tarjoaman ohjelmointirajapinnan tapauksessa, jossa paikallisesti tuotettuja tuloksia voidaan käyttää etänä.
53. Jos esimerkiksi asiakaspuolen koodissa käsitelty tieto annetaan jossakin vaiheessa kolmannen osapuolen käyttöön, esimerkiksi lähetetään verkon kautta takaisin palvelimelle, tällainen toiminto (jonka on määrännyt käyttäjän päätelaitteeseen jaetun asiakaspuolen koodin tuottaja) olisi "jo tallennettujen tietojen käyttämistä". Se, että nämä tiedot tuotetaan paikallisesti, ei estä sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamista.

3.3 Ainoastaan IP-osoitteisiin perustuva seuranta

54. Jotkin palveluntarjoajat kehittävät ratkaisuja, jotka perustuvat vain yhden komponentin eli IP-osoitteen keräämiseen käyttäjän navigoinnin seuraamiseksi, joissakin tapauksissa useilla verkkotunnuksilla²⁸. Tässä yhteydessä voitaisiin soveltaa sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa, vaikka ohje IP-osoitteen saataville asettamisesta olisi tullut muulta kuin vastaanottavalta yksiköltä.
55. IP-osoitteiden käyttöoikeuden saaminen käynnistäisi kuitenkin sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamisen vain silloin, kun nämä tiedot ovat peräisin tilaajan tai käyttäjän päätelaitteesta. Vaikka asia ei ole systemaattisesti näin (esimerkiksi kun CGNAT²⁹ on aktivoitu), käyttäjän reitittimestä peräisin olevat staattiset IPv4-osoitteet kuuluisivat tähän tapaukseen samoin kuin IPV6-osoitteet, koska ne ovat osittain isännän määrittelemiä. Ellei yksikkö pysty varmistamaan, että IP-osoite ei ole peräisin käyttäjän tai tilaajan päätelaitteesta, sen on toteutettava kaikki sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaiset toimenpiteet.
56. Vaikka näissä ohjeissa ei analysoida sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdassa säädettyjen poikkeusten soveltamista suostumuksensaamisvelvoitteeseen, on tärkeää taas muistuttaa, että tämän artiklan soveltaminen ei systemaattisesti tarkoita, että suostumus on saatava. Tietosuojaneuvosto muistuttaa näin ollen, että kussakin tapauksessa olisi arvioitava, tarvitaanko

²⁸ Tämä ei riipu IP-osoitteen käytöstä ja tehtävästä taustalla olevan teknisen viestinnän luomiseen, siirtämiseen tai välittämiseen tai siitä, ovatko tiedot henkilötietoja vai eivät (sähköisen viestinnän tietosuoja-analyysin osalta kyse on tiedoista).

Internet-palveluntarjoajat käyttävät²⁹ NAT- tai CGNAT-tekniikkaa rajoitetun IP-osoiteavaruuden käytön maksimoimiseksi. Se ryhmittelee useita tilaajia saman julkisen IP-osoitteen alle.

suostumus vai voitaisiinko soveltaa poikkeusta sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan mukaan³⁰.

3.4 Ajoittainen ja välitetty IoT-raportointi

57. Laitteet esineiden internetissä (IoT, Internet of Things) tuottavat ajan mittaan jatkuvasti tietoa esimerkiksi laitteeseen upotettujen antureiden välityksellä, joita voidaan tai ei voida esikäsittellä paikallisesti. Usein tiedot ovat etäpalvelimen saatavilla, mutta keräämisen tavat voivat vaihdella.
58. Joillakin IoT-laitteilla on suora yhteys julkiseen viestintäverkkoon matkapuhelimen SIM-kortin avulla. Jotkin laitteet voivat olla epäsuorasti yhteydessä yleiseen viestintäverkkoon esimerkiksi käyttämällä WIFI:ä tai välittämällä tietoa toiseen laitteeseen kaksipisteyhteyden kautta (esimerkiksi Bluetoothin kautta). Toinen laite voi olla esimerkiksi älypuhelin tai erityinen yhdyskäytävä, joka voi tai ei voi esikäsittellä tietoja ennen niiden lähettämistä palvelimelle.
59. Valmistaja voi antaa IoT-laitteille ohjeet kerättyjen tietojen välittämisestä aina suoratoistona, mutta ne voivat silti ensin tallentaa tiedot paikalliseen välimuistiin esimerkiksi siihen asti, kunnes yhteys on käytettävissä.
60. Joka tapauksessa IoT-laite, joka on liitetty (suoraan tai epäsuorasti) yleiseen viestintäverkkoon, katsotaan itsessään päätelaitteeksi. Se, että tiedot lähetetään suoratoistona tai välimuistiin ajoittaista raportointia varten, ei muuta näiden tietojen luonnetta. Molemmissa tapauksissa sovellettaisiin sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa, koska IoT-laitteessa olevan koodin avulla dynaamisesti tallennetut tiedot lähetetään etäpalvelimelle ("tietojen käyttö").

3.5 Yksilöllinen tunniste

61. Yksi yritysten käyttämä yleinen työkalu tunnetaan yksilöllisten tunnisteiden (unique identifiers) tai pysyvien tunnisteiden (persistent identifiers) käsitteenä. Tällaiset tunnisteet voidaan johtaa käyttäjän laitteeseen tallennetuista pysyvistä henkilötiedoista (etu- ja sukunimi, sähköpostiosoite, puhelinnumero jne.), jotka kerätään ja jaetaan useiden rekisterinpitäjien kesken, jotta henkilö voidaan tunnistaa yksilöllisesti eri tietokokonaisuuksissa (verkkosivuston tai sovelluksen kautta kerätyt tiedot, asiakkuudenhallintatiedot, data ostoksista tai tilauksista verkossa tai muualla jne.). Verkkosivustoilla pysyvät henkilötiedot saadaan yleensä tunnistautumisen tai uutiskirjeiden tilaamisen yhteydessä.
62. Kuten edellä todetaan, se, että käyttäjä syöttää tietoja, ei estä sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohdan soveltamista tallentamisen osalta, koska nämä tiedot tallennetaan väliaikaisesti päätelaitteelle ennen keräämistä.
63. Verkkosivustoilla tai mobiilisovelluksissa tapahtuvan "yksilöllisen tunnisteen" keräämisen yhteydessä keräävä yksikkö ohjeistaa selainta (jakamalla asiakaspuolen koodia) lähettämään kyseiset tiedot. Näin ollen kyseessä on "tietojen käyttö", ja siihen sovelletaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 3 kohtaa.

³⁰ Tietosuojatyöryhmän lausunnossa 9/2014 esitetään joitakin esimerkkejä tapauksista, joissa suostumusta ei ehkä tarvita.