

Teletunnistietojen säilytysvelvollisuus – Euroopan unionin tuomioistuimen Tele2-tuomio

1. Johdanto

EU:n tuomioistuimen suuren jaoston tuomio 21. joulukuuta 2016 yhdistetyissä asioissa (C-203/15) Tele2 Sverige AB vastaan Post- och telestyrelsen ja (C-698/15) Secretary of State for the Home Department vastaan Tom Watson, Peter Brice ja Geoffrey Lewis on viimeisin ratkaisu sähköisen viestinnän tietosuoja ja EU:n perusoikeuskirjan 7 artiklan yksityisyyden suojaa ja 8 artiklan henkilötietojen käsittelyä koskevien ratkaisujen sarjassa. Aiemmin Digital Rights Ireland -tuomiossa (yhdistetyt asiat C-293/12 ja C-594/12) EU:n tuomioistuin piti yleistä teletunnistietojen säilytysvelvollisuutta koskevaa direktiiviä pätemättömänä, koska direktiivissä itsessään ei ollut säädetty kansallisten viranomaisten tietoihin pääsyn perusteista, tietojen käytön valvonnasta ja säilytyksestä unionin alueella. Schrems-tuomiossa (asia C-362/14) henkilötietojen luovutusta Yhdysvaltoihin koskeva komission safe harbour -päätös todettiin pätemättömäksi Yhdysvaltain viranomaisten yleisluonteisen tietoihin pääsyn mahdollistavan massavalvonnan takia. Digital Rights Ireland -tuomiossa ei käsitelty sitä, olisiko kaikkia teletunnistietoja koskeva määräaikainen yleinen tallennusvelvollisuus rikostutkinnan tarpeisiin perusoikeuskirjan 7 ja 8 artiklan vastaista. Nyt Tele2-tuomion myötä sähköisen viestinnän direktiivin 2002/58 EY 15 artiklan 1 kohtaa ei voi Euroopan perusoikeuskirjan 7, 8 ja 11 artiklan ja 52 artiklan 1 kohdan valossa tulkita niin, että se sallisi kaikkien tilaajien liikenne- ja paikkatietojen yleisen ja erotuksetta tapahtuvan säilyttämisen rikollisuuden torjumiseksi.

Tukholman kamarioikeus totesi asiaa koskevassa tuomiossaan 7.3.2017 (asia 7380-14), että yleinen kaikkia teletunnistietoja koskeva säilytysvelvollisuus jopa vakavien rikosten torjumiseksi oli suhteetonta EU:n perusoikeuksien kannalta. Kamarioikeus ei kuitenkaan arvioinut Ruotsin oikeudenkäymiskaaren (Rättegångsbalken 27 luku) salaisiin pakkokeinoihin perustuvia tunnistetietoihin kohdistuvia pääsyn edellytyksiä ja yhdenmukaisuutta EU-oikeuden kannalta. Kamarioikeus ei myöskään arvioinut kysymystä, täyttääkö tunnistetietojen käsittely teleyritysten laskutusta varten ja viestiliikenteen toteuttamiseksi EU-oikeuden vaatimukset.¹

Tele2-tuomio asettaa myös Suomen lainsäädännön kehittämislle vaikean kysymyksen siitä, miten teletunnistietojen käyttö vakavien rikosten torjuntaan

1. Kamarioikeuden tuomio saatavilla <http://www.kammarrattenistockholm.domstol.se/>.

voitaisiin toteuttaa ilman, että kaikkeen luottamukselliseen viestintään puututaan yleisen tallennuksen muodossa. Pitäisikö tunnistetietojen tallennuksesta rikostutkinnan tarpeisiin ja pääsystä tallennettuihin tietoihin tehdä eri päätökset? Pääsystä pakkokeinolain (806/2011) mukaisesti televalvontatietoihin päättää tuomioistuin poliisin vaatimuksen perusteella. Jos tuomioistuimen tai riippumattoman hallinnollisen viranomaisen pitäisi tehdä päätös myös tietojen tallentamisesta ja säilyttämisestä rikosten torjunnan tarpeisiin, johtaisi se kaksinkertaiseen päätöksentekomenettelyyn.

Suomessa teletunnistetietojen säilytysvelvollisuus rikostutkinnan tarpeisiin on määritelty tietoyhteiskuntakaaren (917/2014, TYK) 157 §:ssä. Säilytysvelvollisuus on luonteeltaan yleinen, ja se koskee porrastetusti eri tunnistetietoja kuudesta kahteentoista kuukautta viestintätapahtumasta. Pääsy rikostutkinnan tarpeisiin säilytettäviin tietoihin on määritelty tarkkarajaisesti pakkokeinolain 10 luvun 6 §:n 2 kohdan mukaisesti televalvontaan oikeuttavien rikosten selvittämiseksi ja syyteharkintaan saattamiseksi. Tele2-tuomiossa on esitelty Ruotsin ja Yhdistyneen kuningaskunnan lainsäädäntöä teletunnistetietoihin pääsystä. Molemmissa maissa tunnistetietoihin pääsyn kynnyks on rikoksen vakavuuden osalta matalampi ja edellytykset väljemmät kuin Suomen pakkokeinolaissa.

Yksityisyyden ja luottamuksellisen viestinnän suojaa voidaan arvioida tunnistetietojen käsittelyn, säilyttämisen sekä niihin kohdistuvan pääsyn kannalta. Käsittelen Tele2-ennakkopäätöksen tulkintaa ja merkitystä suomalaiselle lainsäädännölle. Arvioin nykyisiä tunnistetietojen käsittelyoikeuksia ja tallennusvelvollisuuksia ennakkopäätöksen pohjalta. Sähköisen viestinnän tietosuojaa koskevan direktiivin 2002/58/EY 15 artiklassa on määritelty mahdollisuudet säätää poikkeuksia sähköisen viestinnän luottamuksellisuudesta. Arvioin tunnistetietoihin pääsyä koskevia oikeuksia nykyisen kotimaisen lainsäädännön eri perusteiden sekä valmisteilla olevan tiedustelulainsäädännön kannalta. Koska EU:n komissio ehdottaa sähköisen viestinnän tietosuojaa koskevan direktiivin 2002/58/EY korvaamista sähköisen viestinnän tietosuojaa koskevalla asetuksella, muutoksella on merkitystä kotimaisen lainsäädännön muutostarpeiden arvioinnille.²

Rikostutkinnan pakkokeinolakiin perustuvien tunnistetietojen saannin lisäksi eri laeissa on säännöksiä oikeudesta saada tunnistetietoja muun muassa hätäpuhelujen paikantamiseen, tekijänoikeusloukkausten selvittämiseen sekä poliisin tehtävien suorittamiseen. Säilytysvelvollisella teleyrityksellä on mahdollisuus ja oikeus käsitellä teletunnistetietoja TYK 17 ja 18 luvun mukaisesti omia käyttötarkoituksia varten, muun muassa palvelujen kehittämistä, laskutusta

2. Komissio ehdottaa korkeatasoisen yksityisyydensuojan varmistavia sääntöjä kaikkeen sähköiseen viestintään ja päivittää EU:n toimielimiä koskevia tietosuojasääntöjä. 2017/0003 (COD) Bryssel 10. tammikuuta 2017.

ja markkinointia varten. Arvioin tunnistetietojen käsittelyn edellytyksiä ja tietoihin pääsyn toteuttamista eri lakien perusteella.

2. Tunnistetietojen säilytysvelvollisuus sekä viestinnän luottamuksellisuus ja yksityiselämän suoja

Direktiivin 2002/58/EY 15 artikla antaa mahdollisuuden poiketa sähköisen viestinnän luottamuksellisuudesta kansallisen turvallisuuden, puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisten viestintäjärjestelmien luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi. EU:n tuomioistuimen tunnistetietojen säilytysvelvollisuutta koskevat ratkaisut ovat koskeneet säilytysvelvollisuutta koskevan direktiivin 2006/24 pätevyyttä Digital Rights Ireland -tuomiossa sekä liikenne- ja paikkatietojen yleistä ja erotuksetta tapahtuvaa säilytysvelvollisuutta rikostutkinnan tarpeisiin Tele2-tuomiossa. EU:n tuomioistuimen mukaan perusoikeuskirjan 7 ja 8 artiklan turvaamiin oikeuksiin puuttuminen edellyttää rikoksilta riittävää vakavuutta. Kun direktiivissä 2006/24 itsessään ei asetettu edellytyksiä rikoksia koskevan kansallisen lainsäädännön ja viranomaisten toimivallan, säilytettävien tietojen ja henkilöiden vakavaan rikollisuuteen liittymisen osalta, direktiivi katsottiin pätemättömäksi. Tele2-tuomiossa todetaan kaikkia tilaajia koskevan liikenne- ja paikkatietojen säilytysvelvollisuuden ilman yhteyttä vakavaan rikollisuuteen olevan perusoikeuskirjan vastaista.

Tele2-tuomion jälkeen voidaan todeta, että kaikkea sähköistä viestintää koskeva tunnistetietojen tallentaminen ja säilyttäminen rikostutkinnan tarpeisiin on vastoin EU:n perusoikeuskirjan 7 ja 8 artiklan oikeuksia. Tele2-tuomiossa on mainittu perusoikeuskirjan 11 artiklan turvaama sananvapaus osana punnintaharkintaa, mutta tapauksessa ei kuitenkaan ollut kyse konkreettisista sananvapauteen perustuvista intresseistä.³ Julkisasiamiehen ratkaisuehdotuksessa on listattu ehtoja, joita jäsenvaltio voi asettaa sähköisten viestintäpalvelujen tarjoajille. Julkisasiamies arvioi, ettei ole pois suljettua, että kansallinen järjestelmä, joka sisältää kaikki kyseiset takeet, on silti katsottava demokraattisessa yhteiskunnassa suhteettomaksi säilyttämisvelvollisuudesta aiheutuvien vakavien

3. Muun muassa Google Spain SL -tapauksessa (asia C-131/12) EU:n tuomioistuin piti Googlen hakukoneeseen liittyviä intressejä taloudellisina eikä käyttäjien perusoikeuskirjan 11 artiklan sananvapauteen liittyvinä oikeuksina. *Riitta Ollila*: Henkilötietojen suoja EU:n perusoikeutena. Artikkeleita eurooppaoikeudesta. Defensor Legis 2014 s. 814–824.

riskien ja vakavien rikosten torjunnassa saatavan hyödyn välisen epäsuhtan vuoksi.⁴

EU:n tuomioistuimen mukaan säännösten on perustuttava objektiivisiin kriteereihin niiden olosuhteiden ja edellytysten määrittelemiseksi, joilla toimivaltaisille kansallisille viranomaisille on annettava oikeus saada tilaajien tai rekisteröityjen käyttäjien tietoja. Tältä osin oikeus voidaan lähtökohtaisesti myöntää rikollisuuden torjumisen tavoitteen yhteydessä vain sellaisten henkilöiden tietoihin, joiden epäillään suunnittelevan, tekvän tai tehneen vakavan rikoksen tai olevan jollakin tavalla mukana tällaisessa rikoksessa. Sellaisissa tilanteissa, joissa kansallisen turvallisuuden, maanpuolustuksen tai yleisen turvallisuuden elintärkeitä intressejä uhkaa terrorismi, oikeus saada muiden henkilöiden tietoja voidaan kuitenkin myöntää myös, jos olemassa on objektiivisia seikkoja, joiden perusteella voidaan katsoa, että näillä tiedoilla voidaan konkreettisesti tapauksessa tosiasiallisesti myötävaikuttaa tällaisen toiminnan torjumiseen.

Tele2-tuomion mukaan kansallisessa lainsäädännössä pitäisi mainita, missä olosuhteissa ja millä edellytyksillä tietojen säilyttämistoimenpide voidaan toteuttaa ennaltaehkäisevästi, jotta taataan toimenpiteen rajoittuminen täysin välttämättömään. Säilyttämisen on oltava sellaisten objektiivisten perusteiden mukaista, joilla luodaan yhteys säilytettävien tietojen ja asetetun tavoitteen välille. Edellytysten on oltava sellaisia, että niillä rajoitetaan toimenpiteen laajuutta ja asianomaista yleisöä. Rajoitus voisi perustua välilliseen yhteyteen vakavaan rikollisuuteen tai maantieteelliseen alueeseen, jos siihen liittyy kohonnut riski vakavien rikosten valmisteluun tai toteuttamiseen.⁵

Yleinen kaikkia teletunnistetietoja koskeva tallennusvelvollisuus rikostutkinnan tarpeita varten näyttää EU:n tuomioistuimen asettamien reunaehtojen perusteella mahdottomalta. Kun rikostutkinnan tarpeisiin kohdistuva yleinen vuoden säilytysvelvollisuus on Suomessa tähän saakka alkanut viestintätapahtumasta, vakavaan rikollisuuteen ja niihin perustuviin yhteyksiin pohjautuva tunnistettietojen tallennus voitaisiin tehdä vasta näiden edellytysten toteamisen jälkeen tuomioistuimen tai hallintoviranomaisen päätöksellä. Tämä voitaisiin toteuttaa joko tallennusvelvollisuutta ja tietoihin pääsyä koskevilla erillisillä päätöksillä tai vain tietoihin pääsyä koskevalla päätöksellä, jolloin pääsyn yhteydessä arvioitaisiin mahdollisuus saada teleoperaattorin hallussa olevia aikaisempia tunnistetietoja. Viestintähistoriaan perustuvien tietojen hyödyntäminen riippuisi siitä, kuinka paljon teleoperaattori on tallentanut tunnistetietoja laskutusta tai muuta omaa käyttöä varten.

4. Yhdistetyt asiat C-203/15 ja C-698/15, julkisasiamiehen ratkaisuehdotus, Henrik Saugmandsgaard Øe 19.7. 2016, kohdat 262–263.

5. C-203/15 Tele2, kohdat 109–110.

3. Tunnistetietojen käsittely omaa käyttötarkoitusta varten

Teleyrityksen oikeudet käsitellä välitystietoja verkko- ja viestintäpalvelun käyttämiseksi, laskuttamiseksi, tietoturvan varmistamiseksi, teknisen vian havaitsemiseksi ja teknistä kehittämistä varten sekä väärinkäytöstilanteissa, joissa verkko-, viestintä- tai lisäarvopalvelun maksullista palvelua käytetään maksutta, on määriteltä TYK 17 luvussa. Teleyritys saa käsitellä välitystietoja vain sen verran kuin on tarpeellista. Välitystietojen käsittelyllä ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Tunnistetietojen käsittelyä koskevat edellytykset käsittelyn minimaalisuudesta ja välttämättömyydestä käyttötarkoitukseen nähden. TYK 139 §:n 3 momentti antaa mahdollisuuden käsitellä laskun määräytymistä koskevia tunnistetietoja vähintään kolme kuukautta ja enintään kolmen vuoden ajan vanhentumiseen saakka laskun eräpäivästä. Teleyritysten omaa käyttötarkoitusta varten tapahtuvan tunnistetietojen käsittelyn ja säilytyksen on sanottu kuuluvan liikesalaisuuden piiriin. Toisaalta viestintäviraston määräyksessä 53 *säilytysvelvollisuudella* tarkoitetaan tietoyhteiskuntakaaren 19 luvussa säädettyä velvollisuutta säilyttää tiettyjä tietoja viranomaistarpeita varten kauemmin kuin niitä muutoin säilytettäisiin.⁶ Säilytysvelvollisuuden piiriin kuuluvat tiedot on mainitusta syystä johtuen pystyttävä erottamaan säilytysvelvollisen yrityksen omaakin tarvetta varten käsittelemistä tiedoista.⁷

TYK 145 §:n mukaan viestinnän välittäjän on tallennettava yksityiskohtaiset tapahtumatiedot luottamuksellisuuden ja yksityisyyden suojan kannalta keskeisiä välitystietoja sisältävissä tietojärjestelmissä tapahtuvasta välitystietojen käsittelystä. Tapahtumatiedot on säilytettävä kaksi vuotta niiden tallentamisesta. Tapahtumatiedot tarkoittavat sellaisia käsittelyn lokitietoja, joissa välitystapahtumat voidaan kohdistaa tietyn viestinnän osapuolen viestintätapahtumaan.⁸ Näiden ohjeiden perusteella voidaan arvioida, että tunnistetietoja teleyrityksen omaa käyttöä varten säilytetään ainakin kaksi vuotta, jos lokitietojen tallentaminen edellyttää myös alkuperäisten tunnistetietojen olemassaolon todentamista. Lokitietoihin liittyviä tunnistetietoja voidaan tallentaa vain siltä osin kuin niihin on kohdistunut hakuja ja käsittelyä.⁹

6. Toisaalta internet-operaattorilla ei ole yleistä lakisääteistä velvollisuutta tallentaa omaa käyttöä koskevia tunnistetietoja. *Pekka Savola*: Tunnistamistietojen luovutusmääräykset ja telepakko-keinot. Lakimies 2003 s. 886–908, s. 889.

7. Viestintäviraston määräys 53 tunnistamistietojen tallentamisvelvollisuudesta. Julkaistu 16.02.2013.

8. HE 221/2013 vp tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta s. 154.

9. Tarkoitus on estää tunnistetietojen hakuun kohdistuvia väärinkäytöksiä ja toteuttaa hakuja toteuttaneiden henkilöiden oikeusturvaa. *Pekka Savola*: Internet-operaattori ja perusoikeudet.

Käsittelyä laskutusta varten koskeva TYK 139 §:n 4 momentti edellyttää, että viestinnän välittäjän on ilmoitettava tilaajalle tai käyttäjälle, millaisia välitystietoja käsitellään ja kuinka kauan niiden käsittely kestää. Oman matkapuhelinliittymäni välitystietoja koskevaan kyselyyn sain vastauksena, että puhelutietojen, viestien ja datatikkettien tallennusajat ovat enimmillään kolme vuotta eli kuluva vuosi ja kaksi edellistä vuotta. Teleyritysten omaa käyttötarkoitusta varten tapahtuva välitystietojen käsittely ja niiden tallentaminen kestää pitempään kuin TYK 157 §:n tunnistetietojen säilytysvelvollisuus rikostutkinnan tarpeisiin. Tämä antaisi mahdollisuuden kohdistaa rikosten torjuntaan ja selvittämiseen perustuvia pakkokeinoja teleyritysten omaa käyttötarkoitusta varten tapahtuvaan välitystietojen käsittelyyn ja tallentamiseen.

4. Perusteet tunnistetietoihin pääsyle

Direktiivin 2002/58/EY 15 artiklassa on lueteltu perusteet pääsyle teletunnistetietoihin. Siinä ei ole nimenomaisia säännöksiä tunnistetietojen käsittelystä siviilioikeudellisten vaatimusten yhteydessä, mutta sähköisen viestintäjärjestelmän luvattoman käytön torjunta ja tutkinta ovat perusteita rajoittaa viestinnän luotamuksellisuutta. Näiden perusteiden lisäksi immateriaalisten oikeuksien suojaamista koskevan direktiivin 2004/48 8 artikla velvoittaa jäsenvaltiot kansallisella lainsäädännöllä varmistamaan, että toimivaltaisilla oikeusviranomaisilla on oikeus saada tietoja tekijän- ja teollisoikeuksia loukkaavien jakeluverkkojen alkuperästä rikos- tai siviilioikeudelliseen menettelyyn. EU:n tuomioistuin on myös katsonut, ettei sähköisen viestinnän tietosuojadirektiivissä suljeta pois jäsenvaltioiden mahdollisuutta säätää velvollisuudesta paljastaa henkilötietoja siviiliprosessin yhteydessä.¹⁰ EU:n tuomioistuin on kuitenkin korostanut sitä, että direktiivejä on tulkittava tavalla, jolla voidaan varmistaa unionin oikeusjärjestyksessä suojattujen eri perusoikeuksien välinen tasapaino sekä yleisten oikeusperiaatteiden, kuten suhteellisuusperiaatteen, noudattaminen.¹¹

Suomessa tekijänoikeuslain (404/1961) 60 a §:ssä annetaan tekijälle tai hänen edustajalleen oikeus saada välittäjänä toimivalta palvelun tarjoajalta yhteystiedot sellaisesta teleliittymästä, josta tekijän oikeuksien suojan kannalta merkittävässä määrin saatetaan yleisön saataviin tekijänoikeudella suojattua aineistoa ilman tekijän suostumusta. IP-osoitteiden tunnistetietojen luovutusta koskevia vaatimuksia käsitellään markkinaoikeudessa. Silloin kun IP-osoitteen yhteystietojen

Oikeustiede–Jurisprudentia 2013 s. 163.

10. C-275/06 Promusicae, kohdat 54–55 ja C-461/10 Bonnier Audio, kohdat 54–55.

11. C-275/06 Promusicae, kohdat 68 ja 70 ja C-461/10 Bonnier Audio, kohdat 59–61.

luovutusta koskeva markkinaoikeuden päätös pannaan täytäntöön, täytäntöönpano ei kohdistu TYK 157 §:n perusteella rikostutinnan tarpeisiin säilytettäviin tunnistetietoihin. Tekijänoikeusrikoksen rangaistusasteikko vastaa TYK 157 §:n televalvontatietoihin pääsyn edellytyksiä, mutta tekijänoikeuslain 60 a §:n yhteystietojen luovutuksessa kyse ei ole rikostutunnasta.¹²

TYK 321 §:n perusteella hätäilmoituksia vastaanottavalla viranomaisella on oikeus saada hätäilmoituksen kohteena olevan henkilön käyttämän päätelaitteen ja liittymän sijainnin ilmaisevat yhteystiedot ja sijaintitiedot, jos henkilö on ilmeisessä hädässä tai välittömässä vaarassa. Tällainen tiedonsaantioikeus vastaa henkilötietolain (523/1999) 8 §:n 3 kohdan rekisteröidyn elintärkeää etua henkilötietojen käsittelyä. Vastaava rekisteröidyn elintärkeä etu mainitaan myös henkilötietodirektiivissä (95/46/EY) ja tulevan tietosuojalain (2016/679/EU) 6 artiklan 1 kohdan d alakohdassa perusteena henkilötietojen käsittelylle. Viranomaisten oikeudesta saada välitystietoja rikosten ennalta estämiseksi, paljastamiseksi tai selvittämiseksi säädetään poliisilaissa (872/2011), rajavartioloissa (578/2005), henkilötietojen käsittelystä rajavartiolaitoksessa annetussa laissa (579/2005), tullilaissa (1466/1994) ja pakkokeinolaissa. Näissä laeissa perusteet välitystietojen saannille on määritelty kussakin laissa erikseen.

Pakkokeinoja koskevan lainsäädännön voimassaolon aikana teleyrityksillä ei ole aina ollut laissa säänneltyä velvollisuutta tallentaa ja säilyttää tunnistetietoja viranomaisten käyttöön. Tässä mielessä pakkokeinot ovat aikaisemminkin kohdistuneet teleyrityksen hallussa oleviin tietoihin. Aikaisemman pakkokeinolain (450/1987) aikana siihen on lisätty telekuuntelua ja televalvontaa koskevia 5a luvun säännöksiä erityisesti lakimuutoksilla 402/1995 ja 646/2003. Tällöin laissa ei ollut tunnistetietojen säilytysvelvollisuutta, mutta pakkokeinolain 5a luvun 9 §:ssä (646/2003) määriteltiin teleyrityksen avustamisvelvollisuus telekuunteluun ja -valvontaan. Vastaava avustamisvelvollisuus on nykyisen pakkokeinolain (806/2011) 10 luvun 63 §:ssä. Tele2-tuomion jälkeen on arvioitava, pitäisikö tunnistetietojen säilytysvelvollisuus viranomaistarpeisiin poistaa ja korvata se tuomioistuimen päätökseen perustuvalla teleyrityksen avustamisvelvollisuudella.

Viranomaistarpeita varten säädetty säilytysvelvollisuus voidaan korvata rajaamalla säilytysvelvollisuus vain vakavia rikoksia koskeviin tietoihin tai kohdistamalla pääsy teleyritysten omaa käyttöä varten tallentamiin tietoihin tai muuten olemassa oleviin tietoihin. Suomen sähköisen viestinnän tietosuojalaissa (516/2004) ei alun perin ollut velvollisuutta säilyttää tunnistetietoja viranomaistarpeita varten, vaan sitä koskeva 14 a § (343/2008) lisättiin lakiin direktiivin 2006/24/EY vaatiman muutoksen takia. Sen jälkeen kun EU:n tuomioistuin oli katsonut Digital Rights Ireland -tuomiossa direktiivin 2006/24/EY pätemättömäksi, asiaa arvioitiin uudelleen perustuslakivaliokunnassa käsiteltävänä olleen

12. *Jussi Päivärinne*: IP-osoitteen juridinen luonne ja käyttäjän yhteystietojen selvittäminen tekijänoikeuslain 60a §:n perusteella. *Defensor Legis* 2013 s. 196–215, s. 215.

tietoyhteiskuntakaaren yhteydessä. Perustuslakivaliokunta arvioi, että avoimeksi jää, merkitseekö viranomaistarpeita varten säädetyn säilyttämisvelvollisuuden ulottuminen käytännössä kaikkien sähköisiä viestimiä käyttävien ihmisten tietoihin jo yksinään oikeasuhtaisuusvaatimuksen loukkausta. Perustuslakivaliokunta katsoi, että säilytysvelvollisuuden rajaaminen henkilöpiiriin ja viestinnän kohteiden osalta olisi asiallisesti ja teknisesti vaikea toteuttaa. Lisäksi tällainen sääntely saattaisi valiokunnan mielestä osoittautua muiden perusoikeuksien, kuten luottamuksellisen viestin salaisuuden suojan, kannalta ongelmalliseksi.¹³

EU:n tuomioistuimen Tele2-tuomiossa yleinen kaikkia viestintämuotoja koskeva tallennusvelvollisuus nähtiin suurempana uhkana yksityisyyden suojalle kuin mahdollisuus säädellä tarkkarajaisesti pääsyä tallennettuun tietoon. Tästä seuraavat kansallisen lainsäädännön kehittämisvaihtoehdot ovat, että säilytysvelvollisuus muotoillaan uudelleen tai säännellään pääsyä teleyrityksen hallussa oleviin omaa käyttöä varten käsittelemiін tietoihin. Kun päätöksen- teko vakavaa rikollisuutta koskevasta säilytysvelvollisuudesta olisi käytännössä mahdotonta tehdä heti viestintätapahtuman jälkeen, pääsyn pitäisi pohjautua teleyrityksen omaa käyttöä varten käsittelemiін tunnistetietoihin. Ennakoivaan rikostorjuntaan olisi mahdollista saada tietoja vakavien rikosten tekijöiden tai niihin osallistuvien henkilöiden tietojen seurantaan. Järjestäytyneestä tai piiloon jäävästä rikollisuudesta ei välttämättä saada tietoja heti rikosten tapahduttua. Tässä mielessä tunnistetietojen historiaan kohdistuva tutkinta voi olla tarpeen vakavien rikosten selvittämiseksi. Ennakoiva tarkkailu edellyttää profilointia mahdollisesta syyllistymisestä vakaviin rikoksiin.

Poliisilain 5 luvussa säännellään poliisin salaisten tiedonhankintakeinojen käyttöä. Salaisen tiedonhankintakeinon käytön yleisenä edellytyksenä on, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja. Poliisilain 5 luvun 8 §:n mukaan tele- tunnistetietoihin voidaan kohdistaa televalvontaa, jos henkilön lausumien, uh- kausten tai käyttäytymisen perusteella taikka muutoin voidaan olettaa hänen syyllistyvän lainkohdassa mainittuihin vakaviin rikoksiin. Salaiset tiedonhankin- takeinot kohdistuvat vakavien rikosten ennaltaehkäisyyn ja seurantaan, kun taas pakkokeinot kohdistuvat jo tapahtuneiden rikosten tutkintaan. Telekuuntelua ja televalvontaa koskevassa tuomioistuimen päätöksessä on mainittava luvan voimassaoloaika kellonajan tarkkuudella.¹⁴ Koska TYK 157 § rajaa säilytysvel- vollisuuden vuoteen viestintätapahtumasta, lupa voidaan myöntää taannehtivasti enintään vuoden takaisin tunniste- ja paikkatietoihin.¹⁵

13. PeVL 18/2014 vp.

14. Poliisilain 5 luvun 7 §:n 3 momentin 4 kohta ja 10 §:n 6 momentin 5 kohta sekä pakkokeinolain 10 luvun 5 §:n 3 momentti ja 9 §:n 3 momentin 5 kohta.

15. Muun muassa Jari Aarnion vuonna 2013 alkaneessa rikostutkinnassa tunnistetietoja oli käy- tettävissä vuodesta 2012 alkaen. Tieto on saatu MTV:n rikostoimittaja Jarkko Sipilältä.

5. Lainsäädännön muutostarpeita

Teletunnistetietoihin pääsyä koskevan lainsäädännön tarkastelun perusteella voidaan todeta, että pääsy kohdistuu pääsääntöisesti vakavien rikosten tutkintaan ja ennaltaehkäisyyn. Tämän lisäksi teleyhteystietoihin liittyviä henkilötietoja on mahdollista luovuttaa tekijänoikeusloukkausten torjumiseksi ja hätäkeskukseen tehtyjen ilmoitusten käsittelemiseksi. Tekijänoikeusloukkausten torjunta yhdistyy direktiivin 2002/58/EY 15 artiklassa mainittuun sähköisen viestintäjärjestelmän luvattoman käytön torjuntaan, mutta näiden varsinainen oikeutusperuste on muussa EU-lainsäädännössä. Tekijänoikeutta loukkaava tietojärjestelmien käyttö on oikeudetonta tekijänoikeuden haltijoita kohtaan, mutta ei välttämättä viestintäjärjestelmien luvatonta käyttöä.

Tele2-tuomiossa ja EU:n tuomioistuimen muussa sähköisen viestinnän tietosuoja koskevassa oikeuskäytännössä ei ole arvioitu teletunnistetietojen käsittelyä kansallisen turvallisuuden tai puolustuksen ja yleisen turvallisuuden tarpeisiin. Kansallinen turvallisuus sekä puolustus ja yleinen turvallisuus ovat direktiivin 2002/58/EY 15 artiklan mukaisia perusteita puuttua luottamukselliseen viestintään. Kansallista turvallisuutta koskevaa Euroopan unionista tehdyn sopimuksen (SEU) 4 artiklan 2 kohdan tarkoittamaa poikkeusta on arvioitu muussa oikeuskäytännössä, muun muassa Suomea koskevassa asiassa C-615/10 *Insinööri* *InsTiimi Oy* kansalliseen turvallisuuteen liittyvissä hankinnoissa. Poikkeusta on tulkittava suppeasti ja kansalliseen turvallisuuteen vetoavan jäsenvaltion on näytettävä toteen tarve turvautua kyseiseen perusteeseen.¹⁶ Kansallinen turvallisuus, puolustus ja yleinen turvallisuus tulevat arvioitavaksi sotilas- ja siviilitiedustelua koskevan lainsäädännön valmistelun yhteydessä.

Suomen perustuslain (731/1999) 10 §:n 4 momenttiin esitetään lisättäväksi luottamuksellisen viestin salaisuuden rajoittamista koskeva säännös tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Sotilastiedustelua koskevassa laissa voidaan sitten tavallisella lailla säätää viestiliikenteeseen puuttumisesta.¹⁷ Direktiivin 2002/58/EY 15 artikla koskee lainsäädännöllisiä toimenpiteitä, joilla puututaan luottamukselliseen viestintään kansallisen turvallisuuden, yleisen turvallisuuden ja puolustuksen tarkoituksessa. Rajoitusten on oltava välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä.

16. *Sonya Walkila*: Luottamuksellisen viestinnän suoja ja sen rajoitusedellytykset EU-oikeudessa. Liitemuistio julkaisussa Luottamuksellisen viestin salaisuus. Perustuslakisääntelyn tarkentaminen. Oikeusministeriön mietintöjä ja lausuntoja 41:2016 s. 68–76, s. 71, *Juha Raitio*: Euroopan unionin oikeus. Talentum Pro 2016 s. 696–698.

17. Luottamuksellisen viestin salaisuus 2016 s. 45.

EU:n komission ehdotuksessa 2017/0003 (COD) sähköisen viestinnän tietosuoja-asetukseksi on vastaava 11 artikla, jonka mukaan unionin tai jäsenvaltion lainsäädännössä voidaan lailla rajoittaa luottamuksellisuutta, jos rajoituksissa noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia ja se on demokraattisessa yhteiskunnassa välttämätön, asianmukainen ja oikeasuhteinen toimenpide tietosuoja-asetuksen vastaavien hyväksyttävien rajoitusperusteiden saavuttamiseksi. EU:n tietosuoja-asetuksen 23 artiklassa kansallinen turvallisuus, puolustus, yleinen turvallisuus, rikoksiin liittyvät toimenpiteet ja yleiseen julkiseen etuun liittyvät tärkeät tavoitteet ovat perusteita kansallisille lainsäädäntötoimenpiteille. Luottamukselliseen sähköiseen viestintään puuttumisesta pitää säätää kansallisella lailla, toimenpiteiden on oltava oikeasuhteisia ja rajoituksissa pitää noudattaa keskeisiltä osin perusoikeuksia ja -vapauksia. Direktiivin muuttumisen asetukseksi ei olennaisesti muuta EU-oikeudellista säädöstä. Asetuksen mainitsemia perusoikeuksia ja -vapauksia määrittelee EU:n tuomioistuimen oikeuskäytäntö niiden tulkinnan osalta.

EU:n komission ehdotuksen 2017/0003 (COD) 6 artiklassa säädellään sähköisen viestinnän tietojen sallittua käsittelyä. Metadatan käsittely laskutusta, yhteenliittämismaksujen laskentaa tai laittoman käytön havaitsemista varten on edelleen sallittua. Sen sijaan metadatan käsittely edellyttää loppukäyttäjän suostumusta tiettyä tarkoitusta tai palvelujen tarjontaa varten loppukäyttäjille. Metadatan säilyttäminen laskutusta varten voisi kestää niin kauan kuin lasku voidaan laillisesti riitauttaa tai maksu periä kansallisen lainsäädännön mukaisesti. Teleoperaattorin metadatan käsittelyyn omaa käyttötarkoitusta varten ja säilytystä laskutusta varten ei olisi tulossa olennaisia muutoksia nykytilanteeseen nähden. Toki loppukäyttäjän suostumus ja käsittelyn minimointi sisällön käsittelyyn ja palvelujen tarjoamisen tarkoituksiin korostuvat.

Liikenne- ja viestintäministeriö on 20.3.2017 asettanut työryhmän arvioimaan sähköisen viestinnän välittämiseen liittyvien tietojen säilytysvelvollisuutta.¹⁸ TYK 157 §:n kumoaminen ja talletustietoihin kohdistuvan eri lakeihin perustuvan tuomioistuimen päätöksen toteuttaminen pääsynä teleyrityksen omaa käyttöä varten käsittelemiin tietoihin olisi mahdollinen muutos. Riskinä tässä olisi, että teleyritysten omaa käyttöä varten tapahtuva tunnistetietojen käsittely voisi olla vaihtelevaa eri yrityksillä. Etuna olisi kuitenkin, että tunnistetietoihin pääsy kohdistuisi vain tuomioistuimen määräämiin lain edellytyksiä vastaaviin tietoihin. EU:n tuomioistuimen mukaan rikollisuuden torjumisen puitteissa tietojen saannin pitää rajoittua vain vakavan rikollisuuden torjun-

18. Ruotsissa hallitus on määrännyt tehtäväksi selvityksen siitä, mitä muutoksia Tele2-tuomio edellyttää lainsäädäntöön, jotta se vastaisi EU-oikeuden vaatimuksia suhteellisuudesta yksityiselämän suojan ja rikostutkinnan kesken. Datalagring och EU-rätten. Kommittédirektiv Dir. 2017:16 16.2.2017. Selvityksen tekee laamanni Sigurd Heuman, ordförande i Säkerhets- och integritetsskyddsmyndigheten 9.10.2017 mennessä.

taan, joten kansallisen lain on asetettava nämä edellytykset. Poliisilain 5 luvun salaisten tiedonhankintakeinojen käytön edellytykset liittyvät vakavien rikosten torjuntaan. Suomen lainsäädäntö täyttää pääpiirteittäin nämä edellytykset.

Poliisilain 4 luvun 3 §:n mukaan poliisilla on yksittäistapauksessa oikeus pyynnöstä saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot. Tähän ei tarvita tuomioistuimen lupaa, vaan pyynnön pitää perustua poliisin tehtävien hoitamiseen. Apulaisoikeusasiamies on poliisin tunnistamistietojen hankkimista koskevassa ratkaisussa 25.11.2013 dnro 4654/4/13 arvioinut, että poliisin toimintaa koskevan suhteellisuusperiaatteen vuoksi tunnistamistietoja ei pitäisi pyytää aivan vähäisiä rikoksia koskevilla epäilyissä, vaikka säännöksen soveltamisalaa ei ole rajattu asian vakavuuteen liittyvillä syillä. Koska asiasta on säädetty lailla, lain perustuslainmukaisuuden tutkiminen ei kuulunut oikeusasiamiehen toimivaltaan. Sananvapauslain (460/2003) 17 §:n mukainen verkkoviestin tunnistetietojen luovutus viestin sisällön rikosta vastaavan teon perusteella vastaa osittain samaa asiaa. Verkkoviestin tunnistamistietojen luovutuksessa on kyse anonyymien verkkoviestinnän suojaista sananvapauden käytön tilanteissa.

Teleosoitetta koskevilla tiedoilla kyse ei ole samassa määrin yksityiselämää koskevista tiedoista kuin Tele2-tuomion kaikkea viestiliikennettä koskevilla yhteys- ja paikkatiedoissa. Tunnistetietojen hyödyntäminen on lisääntynyt valvonta- ja hätätilanteissa sekä väärinkäytösten torjumiseksi.¹⁹ Bonnier Audio - ja Promusicae -tuomioissa on arvioitu IP-osoitteen tietojen luovuttamisedellytyksiä tilanteissa, joissa tekijänoikeutta väitetään loukatun. Pääsy tunnistetietoihin voi olla vakavien rikosten tutkinnassa laajempaa ja yksityiselämään kohdistuva puuttuminen merkittävämpää kuin yksittäisen IP-osoitteen tietojen luovuttaminen tekijänoikeusloukkausten selvittämisessä tai poliisin tehtävien suorittamisessa. Tele2-tuomio ei koske kaikkiin mahdollisiin tilanteisiin liittyvää tunnistetietojen käsittelyä ja tietoihin pääsyä, eikä eri perusteisiin liittyvä EU:n tuomioistuimen oikeuskäytäntö ole yhtenäistä. Tämä pitää ottaa huomioon myös kotimaisen lainsäädännön muutostarpeita arvioitaessa.

Riitta Ollila

19. Pekka Savola on tehnyt luovutus- ja pakkokeinosäännösten vertailua koskevan taulukon. *Savola LM 2013 s. 906.*