

Muistio
29.3.2023VN/25156/2023
Julkinen**Jatkoselvitys Unionin oikeuskäytännön aiheuttamista muutostarpeista Suomen kansalliseen lainsäädäntöön sähköisen viestinnän välitystietojen säilyttämisvelvollisuudesta ja viranomaiskäytöstä****1 Johdanto**

Sähköisestä viestinnästä kertyy liikenne- ja paikkatietoja (välitystietoja). Välitystietoja ovat esimerkiksi puhelinnumero, sähköpostiosoite sekä IP-osoite silloin, kun niitä käsitellään viestinnän välittämisen yhteydessä. Välitystiedot ovat tietoja, joita käsitellään viestintäverkoissa viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi ja jotka ovat yhdistettävissä viestinnän osapuoliin.

Välitystietojen säilytysvelvollisuutta koskeva kansallinen lainsäädäntö uudistettiin tietoyhteiskuntakaaren (917/2014) säätämisen yhteydessä. Tietoyhteiskuntakaaren nimi vaihtui vuonna 2018 laiksi sähköisen viestinnän palveluista. Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen. Säilytysvelvollisuutta koskeva kansallinen sääntely perustuu nykyään sähköisen viestinnän tietosuojadirektiivin¹ 15(1) artiklaan, jossa jäsenvaltioille annetaan mahdollisuus poiketa direktiivin tietyistä velvoitteista. Kysymystä säilytysvelvollisuuden säätämisen perusteista, rajoista ja säilytettävien tietojen käyttökohteista on vuosien varrella käsitelty useissa Euroopan unionin tuomioistuimen enakkoratkaisuissa.

Liikenne- ja viestintäministeriö on selvittänyt Suomen sääntelyn EU-oikeuden mukaisuutta keväällä 2017², kun unionin tuomioistuin oli antanut ratkaisunsa ns. Tele2 ja Watson -asiassa³. Tämän jälkeen unionin tuomioistuimen oikeuskäytäntöä ja sen vaikutuksia kansalliseen lainsäädäntöön on arvioitu keväällä 2021 laaditussa arviomuistiossa.⁴ Tällöin käsiteltiin erityisesti unionin tuomioistuimen ratkaisuja asioissa Ministerio Fiscal⁵, Privacy International ja La Quadrature du Net⁶ sekä Prokuratuur⁷.

Vuoden 2021 arviomuistiossa ei tunnistettu kansallisessa lainsäädännössä välittömiä muutostarpeita, mutta siinä tunnistettiin eräitä seikkoja, jotka tulee huomioida selvemmin, jos sääntelyä jatkossa muutetaan. Näitä olivat muun muassa jo vuonna 2017 esille nostettu säilytysvelvollisuuden soveltamiskäytäntöön liittyvä epäselvyys rikosten ennaltaehkäisemisessä ja tietojen säilyttäminen unionin alueella.⁸

¹ Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi).

² Liikenne- ja viestintäministeriö (2017): Selvitys sähköisen viestinnän välitystietojen säilytysvelvollisuudesta. Raportit ja selvitykset 9/2017; O 42/2017 vp.

³ Yhdistetyt asiat C-203/15 ja C-698/15 Tele2 Sverige AB vastaan Post- och telestyrelsen ja Secretary of State for the Home Department vastaan Tom Watson ym. (2016).

⁴ Arviomuistio Unionin tuomioistuimen oikeuskäytännön aiheuttamat muutostarpeet sähköisen viestinnän välitystietojen säilyttämisvelvollisuudelle ja viranomaiskäytölle VN/7266/2021.

⁵ Asia C-207/16 Ministerio Fiscal (2018).

⁶ Asia C-623/17 Privacy International vastaan Secretary of State for Foreign and Commonwealth Affairs ym. Yhdistetyt asiat C-511/18, C-512/18 ja C-520/18 La Quadrature du Net ym. vastaan Premier ministre ym.

⁷ Asia C-746/18 Rikosoikeudenkäynti Prokuratuur (2021).

⁸ Muina mahdollisesti huomioitavina asioina arviomuistiossa tunnistettiin arkaluontoisten tietojen käsittelyyn ja automaattiseen käsittelyyn liittyvien erityisten suojakeinojen tarve sekä saatavien tietojen rajaaminen tietopyynnöissä välttämättömään tietokategorioittain ja ajallisesti.

Arviomuistion lausuntokierroksella muun muassa oikeuskanslerinviraston lausunnossa nostettiin kuitenkin esiin tarve ryhtyä ripeästi toimenpiteisiin eräiden arviomuistiossa tunnistettujen mahdollisten muutostarpeiden osalta.⁹

Kevään 2021 jälkeen unionin tuomioistuimen ratkaisukäytäntö on kehittynyt edelleen. Vuonna 2022 unionin tuomioistuin antoi useamman sähköisen viestinnän tietosuojaa ja luottamuksellisuutta koskevan ratkaisun, joiden valossa Suomen kansallista lainsäädäntöä on jälleen syytä arvioida.

Tällä jatkoselvityksellä täydennetään aikaisempia arviomuistioita erittelemällä tätä unionin tuomioistuimen uutta oikeuskäytäntöä. Jatkoselvityksessä tarkastellaan, onko unionin tuomioistuin tehnyt uusia linjauksia tai selventänyt kansallisen lainsäädännön arviointia suhteessa aikaisempiin linjauksiinsa. Siten aikaisemmissa selvityksissä käsitellyt linjauksia Suomen kansallisen lainsäädännön unionin oikeuden mukaisuudesta ei käsitellä tässä jatkoselvityksessä laajemmin kuin mitä unionin tuomioistuimen tuore oikeuskäytäntö osoittaa tarpeelliseksi. Myöskään unionin tuomioistuimen linjauksia vuotta 2022 vanhemmasta oikeuskäytännöstä ei käsitellä tässä jatkoselvityksessä enempää kuin mikä on tarpeen uusien linjauksien tarkastelemiseksi.

Jatkoselvityksessä tarkastellaan erityisesti vuoden 2022 ratkaisuja SpaceNet ja Telekom Deutschland¹⁰ (jäljempänä SpaceNet), G. D. vastaan Commissioner of An Garda Síochána¹¹ (jäljempänä G. D.), VD ja SR¹² sekä Spetsializirana prokuratura¹³.

Jatkoselvityksen tarkastelussa on kyseisten ratkaisujen valossa kansallinen sääntely, joka koskee sähköisen viestinnän välitystietojen säilyttämistä viranomaiskäyttöön sekä viranomaisten oikeutta saada kyseisiä tietoja. Erityisesti tarkastelussa on siis laki sähköisen viestinnän palveluista, jossa säädetään velvollisuudesta säilyttää tiedot viranomaistarpeita varten.

Tietojen saantia säännellään kansallisesti pakkokeinolaissa (806/2011), poliisilaissa (872/2011) sekä sotilastiedustelulaissa (590/2019). Näitä lakeja tässä jatkoselvityksessä käsitellään vain pintapuolisesti siinä määrin kuin unionin tuomioistuimen oikeuskäytännön uusien linjausten mukaan on tarpeen. Lisäksi kyseisiä säädöksiä käsitellään lyhyesti tarkasteltaessa kansalliseen lakiin mahdollisesti tehtyjä muutoksia. Kokonaisuuden kannalta tulee huomioida myös kansallinen laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019), jossa ei kuitenkaan ole suoraan tässä jatkoselvityksessä käsitellyn oikeuskäytännön kannalta olennaista sääntelyä eikä sitä käsitellä tässä selvityksessä. Unionin tuomioistuimen tuore oikeuskäytäntö keskittyy erityisesti tietojen säilyttämiseen, joten vastaavasti tässä selvityksessä korostuu säilyttämistä koskeva sääntely.

Unionin tuomioistuin on lisäksi antanut ratkaisun asiassa M.I.C.M.¹⁴, joka koskee käyttäjien IP-osoitteiden säilyttämistä ja käsittelyä tekijänoikeusloukkausten selvittämiseksi. Jatkoselvityksessä ei käsitellä tekijänoikeusdirektiiviin liittyviä kysymyksiä koskien tekijänoikeuksien suojaamista ja asianmukaista tasapainottamista, sillä nämä eivät kuulu liikenne- ja viestintäministeriön toimialaan.¹⁵

⁹ Ks. tarkemmin Lausuntoyhteenveto: Arviomuistio Suomen data retention -sääntelyn unionin oikeuden mukaisuudesta VN/7266/2021.

¹⁰ Yhdistetyt asiat C-793/19 ja C-794/19 Saksan liittotasavalta vastaan SpaceNet AG ja Telekom Deutschland GmbH (2022).

¹¹ Asia C-140/20 G. D. vastaan Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources ja Attorney General (2022).

¹² Yhdistetyt asiat C-339/20 ja C-397/20 VD ja SR (2022).

¹³ Asia C-350/21 Spetsializirana prokuratura (2022).

¹⁴ Asia C-597/19 Mircom International Content Management & Consulting (M.I.C.M.) Limited vastaan Telenet BVBA ym. (2021).

¹⁵ Ks. VNOS 14 §, 18 § ja 21 §; ks. vastaavasti Lausuntoyhteenveto: Arviomuistio Suomen data retention -sääntelyn unionin oikeuden mukaisuudesta VN/7266/2021.

Selvityksessä ei myöskään käsitellä asioissa VD ja SR sekä G. D. käsiteltyä pätemättömyyttä koskevan tuomion vaikutusten ajallista rajoittamista.

Unionin tuomioistuin on myös antanut ratkaisun asiassa HYA¹⁶, joka koskee telekuuntelupäätösten perusteluvollisuutta. Unionin tuomioistuin ei pitänyt EU:n perusoikeuskirjan ja sähköisen viestinnän tietosuojadirektiivin vastaisena käytäntöä, jossa tuomioistuin myöntää telekuunteluluvan vakiomuotoisella päätöksellä silloin, kun luvan myöntämisen perusteet käyvät ilmi lupahakemuksesta.

Unionin tuomioistuimessa on yhä vireillä useita ennakkoratkaisupyynnöitä, jotka koskevat välitystietojen säilytysvelvollisuutta sekä viranomaisten oikeutettua pääsyä säilytettyihin tietoihin. Unionin tuomioistuimen ratkaisukäytäntöä on siis syytä seurata edelleen tarkasti ja tarpeen mukaan arvioida kansallista lainsäädäntöä myös tulevan oikeuskäytännön valossa. IP-osoitteiden säilyttämistä koskevien linjausten yhteydessä käsitellään lyhyesti vireillä olevista asioista julkisasiamiehen 27.10.2022 antamaa ratkaisuehdotusta asiassa C-470/21 La Quadrature du Net ym.¹⁷ (jäljempänä *QdN II-ratkaisuehdotus*).

Tämän jatkoselvityksen laatimisen aikaan unionin lainsäädäntömenettelyssä on yhä käsiteltävänä Euroopan komission vuonna 2017 antama ehdotus sähköisen viestinnän tietosuoja-asetukseksi¹⁸. Asetuksen on tarkoitus korvata nykyinen sähköisen viestinnän tietosuojadirektiivi, jonka 15 artiklan mukaisiin poikkeamismahdollisuuksiin välitystietojen säilytysvelvoitetta ja niiden viranomaiskäyttöä koskeva kansallinen lainsäädäntö perustuu. Voimaantullessaan asetuksella voi siis olla vaikutusta kansalliseen viestinnän välitystietojen käsittelyä ja säilyttämistä sekä viranomaiskäyttöä koskevaan sääntelyyn. Neuvottelut ovat kuitenkin edenneet hitaasti, eikä asetuksen voimaantulosta, saati lopullisesta sisällöstä, ole tämän jatkoselvityksen laatimisen aikaan tarkempaa tietoa. Kansallista sääntelyä voi mahdollisesti olla tarpeen tarkastella uudelleen asetuksen tultua voimaan.

Euroopan ihmisoikeustuomioistuimessa on käsitelty useita samoja kysymyksiä kuin unionin tuomioistuimessa¹⁹. Tässä jatkoselvityksessä keskitytään kuitenkin vain unionin tuomioistuimen ratkaisuihin, koska EU:n perusoikeussuoja voi vain parantaa eikä heikentää suojan tasoa suhteessa ihmisoikeussopimukseen. Mahdollisessa säädösvalmistelussa on kuitenkin otettava asianmukaisesti huomioon Suomen kansainväliset ihmisoikeusvelvoitteet.

2 Unionin tuomioistuimen vuoden 2022 ratkaisukäytäntö

Sähköisen viestinnän välitystietojen säilyttämistä ja viranomaiskäyttöä koskevissa vuoden 2022 ratkaisuissa unionin tuomioistuin on täsmentänyt tulkintaansa aikaisemmasta ratkaisukäytännöstään. Unionin tuomioistuimen oikeuskäytännön kumulatiivisen luonteen vuoksi myös tässä jatkoselvityksessä viitataan vanhimpaan oikeuskäytäntöön, jossa tulkinta on esitetty.

Sähköisen viestinnän tietosuojadirektiivin 15(1) artiklan nojalla jäsenvaltiot voivat poiketa kyseisen direktiivin vaatimuksista välitystietojen käsittelylle. Artiklassa on asetettu yleiset edellytykset sekä sallitut perusteet direktiivin mukaisesta käsittelystä poikkeamiselle. Rajoitusten tulee olla välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden (valtion turvallisuus) sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan

¹⁶ Asia C-349/21 HYA ym. (2023).

¹⁷ Julkisasiamiehen ratkaisuehdotus C-470/21 La Quadrature du Net ym. (2022).

¹⁸ Komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiiviksi 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus) COM(2017) 10 final.

¹⁹ Ks. esim. [Ekimdzhev and Others v. Bulgaria](#), 2022, § 394–421.

varmistamiseksi. Unionin tuomioistuimen tulkintaa näistä yleisistä edellytyksistä on käsitelty yksityiskohtaisesti vuoden 2021 arviomuistiossa.²⁰

2.1 Yleiset reunaehdot

Unionin tuomioistuin on todennut, että sähköisen viestinnän tietosuojadirektiivi on perussäädös henkilötietojen säilyttämisessä ja niiden käsittelystä sähköisen viestinnän alalla

Unionin tuomioistuin vahvisti ratkaisussaan VD ja SR laajemmin sähköisen viestinnän tietosuojadirektiivin ja sitä koskevan unionin tuomioistuimen oikeuskäytännön suhdetta muuhun lainsäädäntöön toteamalla, että kyseinen direktiivi on perussäädös silloin, kun on kyse henkilötietojen säilyttämisestä ja yleisemmin niiden käsittelystä sähköisen viestinnän alalla. Siten unionin tuomioistuimen sähköisen viestinnän tietosuojadirektiivistä tekemä tulkinta koskee myös tilanteita, joissa muut kuin lainvalvontaviranomaiset voivat pyytää sähköisten viestintäpalvelujen tarjoajien hallussa olevia tietoliikennetietoja.²¹ (VD ja SR kohta 79) Vaikka toisaalla lainsäädännössä säädettäisiinkin viranomaisten toimivaltuuksista saada sähköisten viestintäpalvelujen hallussa olevia tietoja, tulisi näiden tietojen käsittelyn laillisuutta viestintäpalvelujen tarjoajien kannalta arvioida sähköisen viestinnän tietosuojadirektiivissä säädettyjen edellytysten ja unionin tuomioistuimen kyseisestä direktiivistä tekemän tulkinnan valossa. (VD ja SR kohta 82)

> Sähköisen viestinnän tietosuojadirektiivi ja unionin tuomioistuimen sitä koskeva oikeuskäytäntö tulee ottaa huomioon myös silloin, kun muualla lainsäädännössä säädetään sähköisten viestintäpalvelujen tarjoajien hallussa olevien tietoliikennetietojen käsittelystä.

Tuomioistuimen tai riippumattoman hallintoelimen ennakkovalvonta

Tietojen saannin edellytyksenä on tuomioistuimen tai riippumattoman hallintoviranomaisen suorittama ennakkovalvonta. Riippumattomalla hallinnollisella elimellä on oltava asema, jossa se voi suorittaa tehtävänsä objektiivisesti ja puolueettomasti. Riippumattomuuden vaatimus siis edellyttää, että kyseinen viranomaislainen on ulkopuolinen siihen viranomaiseen nähden, joka pyytää kyseisten tietojen saantia. (Prokuratuur kohdat 53 ja 54) Poliisimies, jolla on toimivalta valvoa etukäteen poliisin tutkintayksiköiltä peräisin olevia tietopyyntöjä, ja joka ei ole näihin kyseisiin yksiköihin nähden ulkopuolinen, ei täytä riippumattomuuden ja puolueettomuuden vaatimuksia huolimatta siitä, että häntä avustaa tässä tehtävässä poliisin yksikkö, jolla on tietty itsenäisyys tehtävänsä hoitamisessa. (G. D. kohta 111)

Sääntelyssä on oltava selkeät ja täsmälliset säännöt, joissa ilmaistaan, missä olosuhteissa ja millä edellytyksillä sähköisten viestintäpalvelujen tarjoajien on annettava toimivaltaisille kansallisille viranomaisille oikeus saada tietoja (Tele2 kohta 117). Näiden on perustuttava objektiivisille kriteereille niiden olosuhteiden ja edellytysten määrittelemiseksi, joilla toimivaltaisille kansallisille viranomaisille on annettava oikeus saada kyseessä olevia tietoja (Privacy International kohta 78). Tilanne, jossa tietojen saantia koskevien pyyntöjen käsittelystä vastuussa oleva virkamies on yksin toimivaltainen arvioimaan rekisteröityjä koskevia epäilyjä ja tutkimaan heitä koskevien tietojen saamisen välttämättömyys, ei vastaa vaatimusta objektiivisille kriteereille siten kuin sitä on aikaisemmassa oikeuskäytännössä tulkittu. (G. D. kohta 113)

²⁰ Vuoden 2021 arviomuistio s. 4-9.

²¹ VD ja SR –ratkaisu koskidirektiivin 2003/6 ja asetuksen N:o 596/2014 mukaisesti rahoitusalan toimivaltaisia viranomaisia. Ratkaisussa unionin tuomioistuin katsoi, että kansallinen säännöstö, jolla sähköisten viestintäpalvelujen tarjoajat velvoitetaan säilyttämään ennaltaehkäisevästi markkinoiden väärinkäyttöön liittyvien rikosten, ml. sisäpiirikaupat, torjumiseksi kaikkien sähköisiä viestintävälineitä käyttävien tietoliikennetiedot yleisesti ja erotuksetta ylittää täysin välttämättömät rajat eikä se ole unionin oikeuden mukainen. (VD ja SR kohdat 92-95.)

> Unionin tuomioistuin on täsmentänyt tulkintojansa siitä, millainen järjestely täyttää riippumattoman hallinnollisen elimen vaatimuksen ja millaiset objektiiviset kriteerit päätöksenteolle on asetettava.

2.2 Unionin tuomioistuimen sallituksi arvioimat tietojen säilyttämisen toimenpiteet vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien uhkien ehkäisemiseksi

Unionin tuomioistuin on vahvistanut erityisesti QdN-ratkaisussa²² esitettyä sallittujen säilyttämistoimien jaottelua. G. D. ja SpaceNet -ratkaisuissa tuomioistuin toistaa, että tuomioistuin on QdN-ratkaisun 168 kohdassa täsmentänyt, että direktiivin 2002/58 15 artiklan 1 kohta, luettuna perusoikeuskirjan 7, 8 ja 11 artiklan sekä 52 artiklan 1 kohdan valossa, ei ole esteenä lainsäädännöllisille toimenpiteille, joissa säädetään ***vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi***²³

– liikenne- ja paikkatietojen **kohdennetusta säilyttämisestä**, joka on objektiivisten ja syrjimättömien seikkojen perusteella rajattu rekisteröityjen muodostamien ryhmien mukaan tai maantieteellisen kriteerin avulla ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa

– liittymän lähteelle annettujen **IP-osoitteiden yleisestä ja erotuksetta tapahtuvasta säilyttämisestä** ajanjaksoksi, joka on rajattu täysin välttämättömään

– sähköisten viestintävälineiden **käyttäjien henkilöllisyyttä koskevien tietojen** yleisestä ja erotuksetta tapahtuvasta **säilyttämisestä**, ja

– siitä, että sähköisten viestintäpalvelujen tarjoajat **määrätään** toimivaltaisen viranomaisen päätöksellä, johon kohdistuu tehokas tuomioistuinvalvonta, **varmistamaan nopeasti (quick freeze)** kyseisten palveluntarjoajien käytössä olevien **liikenne- ja paikkatietojen säilyttäminen** tietyn ajan,

jos näillä toimenpiteillä varmistetaan selvin ja täsmällisin säännöin, että kyseessä olevien tietojen säilyttämisen ehtona on, että näihin toimenpiteisiin liittyviä aineellisia ja menettelyllisiä edellytyksiä noudatetaan, ja että rekisteröidyillä on tehokkaat takeet väärinkäytön vaaroja vastaan. (G. D. kohta 67 ja SpaceNet kohta 75)

Unionin tuomioistuin on täsmentänyt kyseisten liikenne- ja paikkatietojen säilyttämistä koskevien toimenpiteiden moninaisuudesta, että näitä eri toimenpiteitä voidaan kansallisen lainsäätäjän valinnan mukaan ja täysin välttämättömän rajoja noudattaen soveltaa yhdessä. Siten unionin oikeus ei ole esteenä näiden toimenpiteiden yhdistämiselle. (G. D. kohta 92) Unionin tuomioistuin on kuitenkin muistuttanut, että se, että on mahdollisesti vaikea määrittää tarkasti niitä tilanteita ja edellytyksiä, joiden toteutuessa kohdennettu säilyttäminen voidaan toteuttaa, ei voi oikeuttaa jäsenvaltioita muuttamaan poikkeusta säännöksi siten, että ne säätävät liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä. (G. D. kohta 84)

Liikenne- ja paikkatietojen kohdennettu säilyttäminen

Tuomioistuimen mukaan unionin oikeus ei ole esteenä kansalliselle lainsäädännölle, jossa säädetään vakavan rikollisuuden torjumiseksi liikenne- ja paikkatietojen [ennakoivasta] kohdennetusta säilyttämisestä, joka on objektiivisten ja syrjimättömien seikkojen perusteella rajattu asianomaisten

²² QdN-ratkaisua on käsitelty tarkemmin vuoden 2021 arviomuistiossa.

²³ QdN-ratkaisun 168 kohdassa unionin tuomioistuin on lisäksi katsonut unionin oikeuden mukaiseksi myös tietyt säilyttämistoimet kansallisen turvallisuuden takaamiseksi, mutta G.D. ja SpaceNet -ratkaisuissa käsitellään vain toimenpiteitä vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien uhkien ehkäisemiseksi.

henkilöiden ryhmien mukaan tai maantieteellisen kriteerin avulla ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa. Säilyttämistoimenpiteiden on oltava luonteeltaan poikkeuksellisia. Unionin tuomioistuin on tarkentanut kohdennetun säilyttämisen kriteerejä viimeaikaisessa oikeuskäytännössään.

Ensinnäkin tuomioistuin toteaa, että direktiivin 2002/58 mukaan käyttöön otetuissa kansallisissa järjestelmissä ei aseteta kohdennettua säilyttämistä koskevan määräyksen antamisen edellytykseksi sitä, että vakavan rikoksen mahdollinen tapahtumapaikka tai tällaiseen tekoon osallistumiseen epäillyt henkilöt ovat ennalta tiedossa. (G. D. kohta 75)

Henkilöryhmään perustuvan kohdentamiskriteerin osalta tuomioistuin on selventänyt, että jäsenmailla on mahdollisuus toteuttaa säilyttämistoimenpiteitä, jotka kohdistuvat henkilöihin, jotka on tunnistettu – kansallisessa oikeudessa määriteltujen objektiivisten ja syrjimättömien seikkojen perusteella – henkilöiksi, jotka aiheuttavat uhan asianomaisen jäsenvaltion yleiselle turvallisuudelle tai kansalliselle turvallisuudelle. (ks. Tele2 kohta 110 ja QdN kohta 149) Säilyttämistoimenpide voidaan siis kohdistaa henkilöihin, jotka tällaisen tunnistamisen perusteella ovat parhaillaan tutkinnan tai muiden valvontatoimenpiteiden kohteena. Kyse voi olla myös henkilöistä, joilla on kansallisessa rikosrekisterissä merkintä vakavista rikoksista, mikä voi merkitä suurta rikosten uusimisvaaraa. (G. D. kohta 78) Tällainen kohdentaminen ei ole syyttömyysolettaman vastaista. (Spetsializirana prokuratura kohta 46)

Lisäksi tuomioistuin on selventänyt, että toimivaltaiset kansalliset viranomaiset voivat toteuttaa säilyttämistoimenpiteen perustuen maantieteelliseen kriteeriin, kuten rikollisuuden keskimääräiseen määrään jollakin maantieteellisellä alueella, ilman että niillä välttämättä olisi konkreettisia indisoita vakavan rikoksen valmistelusta tai tekemisestä asianomaisilla alueilla. (G. D. kohta 80)

Koska tällaiseen kriteeriin perustuva kohdennettu säilyttämistoimenpide voi kohteena olevien vakavien rikosten ja kunkin jäsenvaltion oman tilanteen mukaan koskea sekä paikkoja, joille on ominaista vakavien rikosten suuri määrä, että paikkoja, jotka ovat erityisen alttiita tällaisten rikosten tekemiselle, se ei ole lähtökohtaisesti myöskään omiaan johtamaan syrjintään, koska vakavan rikollisuuden keskimääräistä esiintymistä koskevalla kriteerillä ei sellaisenaan ole mitään yhteyttä mahdollisesti syrjiviin tekijöihin. (G. D. kohta 80)

Maantieteellisiä alueita voidaan ja tarvittaessa täytyy mukauttaa niiden valinnan perusteena olleiden olosuhteiden kehityksen mukaan, mikä mahdollistaa muun muassa reagoimisen vakavan rikollisuuden torjunnan kehitykseen. (G. D. kohta 82) Mukauttaminen on myös tarpeen sen varmistamiseksi, että säilyttämistoimenpiteiden kesto ei ylitä sitä, mikä on täysin välttämätöntä. (G. D. kohta 82; myös QdN kohta 151)

Unionin tuomioistuin vaikuttaa vahvistavan, että henkilöön liittyvien ja maantieteellisten kriteerien lisäksi myös muut erottavat kriteerit liikenne- ja paikkatietojen kohdennetun säilyttämisen toteuttamiseksi ovat mahdollisia. Unionin tuomioistuimen mukaan muita objektiivisia ja syrjimättömiä kriteerejä voidaan ottaa huomioon sen varmistamiseksi, että kohdennetun säilyttämistoimenpiteen ulottuvuus rajoittuu täysin välttämättömään. Lisäksi vakavien rikosten ja henkilöiden, joiden tiedot säilytetään, välillä tulee olla ainakin välillinen yhteys. Tällaisten kriteerien yksilöiminen kuuluu kuitenkin direktiivin 2002/58 15 artiklan 1 kohdan mukaisesti jäsenmaille eikä unionin tuomioistuimelle. (G. D. kohta 83)

IP-osoitteiden yleinen ja erotuksetta tapahtuva säilyttäminen

Unionin tuomioistuin on käsitellyt ratkaisukäytännössään myös IP-osoitteiden säilyttämistä. Unionin tuomioistuin on katsonut, että liittymän lähteelle annettujen IP-osoitteiden yleinen ja erotukseton säilyttäminen ei lähtökohtaisesti ole vastoin unionin oikeutta, kunhan tiukasti noudatetaan QdN-ratkaisun mukaisesti aineellisia ja menettelyllisiä edellytyksiä. (G. D. kohta 74) IP-osoitteiden

säilyttämisestä ja niihin pääsyn saamisen edellytyksistä on odotettavissa lisää unionin tuomioistuimen oikeuskäytäntöä, sillä kysymystä käsitellään tuomioistuimessa yhä vireillä olevassa asiassa C-470/21 QdN II. Julkisasiamies on antanut ratkaisuehdotuksensa 27.10.2022. Julkisasiamies käsittelee ratkaisuehdotuksessaan IP-osoitteiden yleistä ja erotuksetta tapahtuvaa säilyttämistä. Tuomioistuimen oikeuskäytäntö voisi julkisasiamiehen mukaan johtaa siihen, että kansalliset viranomaiset eivät voisi yksilöidä muun kuin vakavan verkkorikollisuuden tekijöitä. Tämä johtaisi siihen, että yksinomaan verkossa tehdyt rikokset jäisivät systemaattisesti ratkaisematta. (QdN II ratkaisuehdotus kohta 80) Erityisesti mielenkiintoista on, että julkisasiamies ehdottaa ratkaisuehdotuksensa kohdassa 82, että unionin tuomioistuin tarkastelisi tietyiltä osin uudelleen IP-osoitteiden säilyttämistä koskeviin kansallisiin toimenpiteisiin liittyvää oikeuskäytäntöään.

Tietojen säilyttämisen nopea varmistaminen (quick freeze)

Unionin tuomioistuin on käsitellyt myös tietojen säilyttämisen nopeaa varmistamista (ns. quick freeze) yhtenä mahdollisena säilyttämistoimenpiteenä, jolla voidaan toteuttaa kohdennettua ja rajoitettua säilyttämistä. Unionin tuomioistuin on täsmentänyt nopean varmistamisen säilyttämistoimenpiteen ulottuvuutta uudessa oikeuskäytännössään.

Nopean säilyttämisen osalta unionin tuomioistuin toteaa samoin kuin kohdennetun säilyttämisen osalta, että säilyttämisen nopeasta varmistamisesta annettu määräys ei rajoitu koskemaan vain ennen tällaisen määräyksen antamista tunnistettuja epäiltyjä. (G. D. kohta 75) Nopea tietojen turvaaminen voi koskea esimerkiksi sellaisten henkilöiden liikenne- ja paikkatietoja, joiden kanssa uhri on ollut yhteydessä ennen yleistä turvallisuutta koskevan uhan ilmenemistä tai ennen vakavan rikoksen tekemistä. (G. D. kohta 89)

Samoin nopea säilyttämistoimenpide voidaan kohdistaa myös koskemaan tiettyä maantieteellistä aluetta. Kyseeseen voi tulla esimerkiksi rikoksen teko- tai valmistelupaikka [tai kansalliseen turvallisuuteen kohdistuvan loukkauksen tapahtuma- tai valmistelupaikka]. Lisäksi säilyttäminen voidaan määrätä sellaisiin liikenne- ja paikkatietoihin, jotka liittyvät tiettyyn paikkaan, jossa henkilö, joka on mahdollisesti joutunut vakavan rikoksen uhriksi, on kadonnut. Sekä säilyttämistoimenpiteen että tietojen saamisen tulee olla QdN-ratkaisun 164-167 kohdassa esitetyn välttämättömyysvaatimuksen edellytysten mukainen. (G. D. kohta 90)

Toimivaltaiset viranomaiset voivat määrätä nopeasta säilyttämistoimenpiteestä heti tutkinnan ensimmäisessä vaiheessa eli siitä hetkestä lähtien, jolloin kyseiset viranomaiset voivat kansallisen oikeuden asian kannalta merkityksellisten säännösten mukaan aloittaa tutkinnan. (G. D. kohta 91)

Unionin tuomioistuin vaikuttaa siis selventävän, että säilyttämismääräys voi kohdistua myös ajallisesti taaksepäin eli määräys ei kohdistu ainoastaan määräyksenantohetken jälkeen syntyviin liikenne- ja paikkatietoihin.

Täysin välttämättömään rajattu ajanjakso

Unionin tuomioistuin käsitteli SpaceNet-ratkaisussaan myös säilyttämistoimenpiteen ajallisen rajaamisen vaikutusta. Tuomioistuin ensinnäkin toteaa, että säilyttämisaika on merkityksellinen tekijä muiden joukossa sen määrittämiseksi, onko unionin oikeus esteenä tällaiselle toimenpiteelle. Sähköisen viestinnän tietosuojadirektiivin 15 artiklan toisen virkkeen mukaisesti säilyttämisen keston edellytetään olevan ”rajoitettu”. (SpaceNet kohta 85)

Unionin tuomioistuimen aikaisemman oikeuskäytännön mukaan puuttumisen vakavuus johtuu siitä vaarasta, että säilytetyt tiedot – niiden määrä ja moninaisuus huomioon ottaen – mahdollistavat yhdessä tarkasteltuina hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä ja että niiden avulla voidaan erityisesti laatia asianomaisen henkilön tai

asianomaisten henkilöiden profiili, joka on yksityisyyden suoja koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö.

Liikenne- ja paikkatietojen säilyttäminen on joka tapauksessa vakavaa riippumatta säilyttämisaikajaksosta ja säilytettyjen tietojen määrästä tai laadusta, kun kyseisen tietojen joukon perusteella voidaan tehdä hyvin täsmällisiä päätelmiä kyseessä olevan henkilön tai olevien henkilöiden yksityiselämästä. (SpaceNet kohta 88; vastaavasti tietojen saannin ajallisesta rajaamisesta ks. Prokuratuur kohta 39)

Jopa rajoitetun liikenne- ja paikkatietojen määrän säilyttäminen tai tietojen säilyttäminen lyhyen aikaa saattaa antaa täsmällisiä tietoja henkilön yksityiselämästä. (SpaceNet kohta 89; vastaavasti oikeudesta saada rajoitettu määrä tietoja tai lyhyeltä ajalta ks. Prokuratuur kohta 40)

Tuomioistuin vahvisti tämän ajanjakson rajaamista koskevan tulkintansa Spetsializirana prokuratura -ratkaisussa. (kohta 52)

Tuomioistuin ei kuitenkaan näytä antavan selvää vastausta siihen, mikä on katsottava täysin välttämättömään rajatuksi ajanjaksoksi. Edes lyhyellä säilytysajalla, kuten neljään tai kymmeneen viikkoon rajatulla säilyttämisellä, ei voida kuitenkaan estää sitä, että puuttuminen olisi vakavaa.

> Tiivistetysti tuomioistuimen uudet linjaukset koskien QdN-ratkaisun tuomiolauselman mukaisia sallittuja säilyttämistoimenpiteitä, kun kyse on vakavan rikollisuuden ja yleiseen turvallisuuteen kohdistuvien uhkien torjumisesta:

- Kohdennetun säilyttämisen edellytyksenä ei ole, että tapahtumapaikka tai epäilty henkilöt ovat ennen säilyttämismääräyksen antamista tiedossa;
- Samoin quick freeze -määräys voi koskea myös muita kuin ennen määräyksen antamista tunnistettuja epäiltyjä;
- Henkilöryhmiin perustuva säilyttämistoimi voidaan – kansallisen oikeuden mukaisten objektiivisten ja syrjimättömien seikkojen perusteella – kohdentaa esim. tutkinnan tai valvontatoimenpiteiden alaisiin henkilöihin tai joilla on rikosrekisterissä merkintä suurta rikosten uusimisvaaraa merkitsevistä vakavasta rikoksesta;
- Maantieteelliseen kriteeriin perustuvan säilyttämistoimenpiteen edellytyksenä ei ole, että kriteerillä välttämättä olisi konkreettisia indisoita vakavan rikoksen valmistelusta tai tekemisestä asianomaisilla alueilla;
- Jäsenvaltiot voivat asettaa myös muita erottavia kriteereitä henkilöön liittyvien ja maantieteellisten kriteerien lisäksi, kunhan säilyttämistoimenpiteen ulottuvuus rajoittuu täysin välttämättömään ja kunhan vakavien rikosten ja henkilöiden, joiden tiedot säilytetään, välillä on ainakin välillinen yhteys;
- Quick freeze -määräys voidaan ulottaa myös ajallisesti taaksepäin eli se ei rajoitu vain määräyksenantohetken jälkeen syntyviin tietoihin;
- Quick freeze -määräys voidaan antaa etenkin sellaisten henkilöiden välitystietojen säilyttämiseen, keiden kanssa uhri on ollut yhteydessä ennen uhan ilmenemistä tai rikoksen tekemistä;
- Quick freeze -määräys voidaan asettaa myös maantieteellisen kriteerin perusteella;
- Oikeuskäytännössä käsiteltyjä sallittuja säilyttämistoimenpiteitä voidaan välttämättömän rajoissa soveltaa yhdessä;
- Jopa rajoitetun liikenne- ja paikkatietojen määrän säilyttäminen tai tietojen säilyttäminen lyhyen aikaa saattaa antaa täsmällisiä tietoja henkilön yksityiselämästä.

> Unionin tuomioistuin vaikuttaa siis pääosin täsmentäneen ja selittäneen aikaisemman oikeuskäytäntönsä mukaisesti sallittuja säilyttämistoimenpiteitä.

> Säilyttämisen ajallisen rajaamisen osalta unionin tuomioistuin ei anna selvää vastausta, mikä on katsottava täysin välttämättömään rajatuksi ajanjaksoksi. Lyhytkään säilytysaika ei poissulje sitä, että puuttuminen ei voisi olla vakavaa.

2.3 Säilyttämisperusteet ja tietojen saanti

QdN-ratkaisussaan unionin tuomioistuin on vahvistanut yleisen edun mukaisten tavoitteiden (rikollisuuden torjunta, yleiseen turvallisuuteen kohdistuvien uhkien torjunta ja kansallinen turvallisuus) välille suhteellisuusperiaatteen mukaisen hierarkian. Tavoitteen tärkeyden on oltava oikeassa suhteessa toimenpiteestä aiheutuvan puuttumisen vakavuuteen nähden. (G. D. kohta 56) Erityisen vakavaakaan rikollisuutta ei voida rinnastaa kansallista turvallisuutta koskevaan uhkaan. (G. D. kohta 63) Liikenne- ja paikkatietojen laillinen säilyttäminen kansallisen turvallisuuden varmistamiseksi ei vaikuta niiden vakavan rikollisuuden ehkäisemiseksi tapahtuvan säilyttämisen laillisuuteen. (G. D. kohta 64)

Unionin tuomioistuin on oikeuskäytännössään korostanut, että liikenne- ja paikkatietojen säilyttäminen ja kyseisten tietojen saanti merkitsevät erillisiä puuttumisia perusoikeuskirjassa taattuihin perusoikeuksiin, mikä edellyttää perusoikeuskirjan 52 artiklan 1 kohdan nojalla erillistä oikeuttamisperustetta. Tästä johtuu, että kansallinen lainsäädäntö, jolla taataan niiden edellytysten täysimääräinen noudattaminen, jotka johtuvat sähköisen viestinnän tietosuojadirektiivin tulkintaa koskevasta oikeuskäytännöstä tietojen saannin alalla, ei voi luonteensa vuoksi rajoittaa tai edes korjata näiden tietojen yleisestä säilyttämisestä johtuvaa vakavaa puuttumista yksilön oikeuksiin. (G. D. kohta 47) Tämä koskee myös kansallisessa lainsäädännössä asetettuja takeita, joilla säilytetyt tiedot pyritään suojaamaan tietojen väärinkäyttöä ja lainvastaista saantia koskevilta vaaroilta. (SpaceNet kohta 91)

Samoin tuomioistuin katsoi, että tietosuojaviranomaisen tai parlamentaarisen elimen suorittama säilyttämiseen kohdistuva valvonta, vaikkakin vähentää luvattoman pääsyn riskiä, ei se poista itse säilyttämisestä aiheutuvaa riskiä yksilön perusoikeuksiin. (Spetsializirana prokuratura kohta 59)

Tietojen määrää ja niistä johdettavia konkreettisia tietoja henkilön yksityiselämästä voidaan arvioida vasta mainittuihin tietoihin tutustumisen jälkeen. Tuomioistuin tai toimivaltainen riippumaton viranomais myöntää luvan saada tietoja väistämättä ennen kuin liikenne- ja paikkatietoihin ja niistä saataviin yksityiselämää koskeviin tietoihin voidaan tutustua. Näin ollen tietojen säilyttämisen kuin myös tietojen saannin muodostaman puuttumisen vakavuuden arvioinnissa on välttämättömästi otettava huomioon se kyseessä olevien henkilöiden yksityiselämälle aiheutuva riski, joka yleisesti liittyy säilytettyjen tietojen luokkaan, ilman että on lisäksi tiedettävä, ovatko kyseisistä tiedoista saatavat yksityiselämään liittyvät tiedot konkreettisesti arkaluontoisia. (Prokuratuur kohta 40; SpaceNet kohta 89)

Tuomioistuimen oikeuskäytännön mukaan oikeus saada säilytysvelvollisuuden perusteella säilytetyt tiedot voidaan lähtökohtaisesti perustella ainoastaan sillä yleisen edun mukaisella tavoitteella, jonka tähden kyseisille palveluntarjoajille on asetettu tämä säilyttämisvelvollisuus. Tästä voidaan poiketa vain silloin, jos tietojen saannin tarkoitus on merkitykseltään suurempi kuin säilyttämisen perustana ollut tavoite. (QdN kohta 165-166) Säilytettyjen tietojen saaminen päinvastaisessa tilanteessa olisi vastoin yleistä etua koskevien tavoitteiden hierarkiaa. (G. D. kohta 99)

Liikenne- ja paikkatietoja ei voida säilyttää yleisesti ja erotuksetta vakavan rikollisuuden torjumiseksi. Näiden tietojen saantia ei siis myöskään voida perustella samassa tarkoituksessa. Jos tietoja on poikkeuksellisesti säilytetty yleisesti ja erotuksettomasti kansallisen turvallisuuden suojaamiseksi, ei näitä tietoja voida saada rikosoikeudellisen menettelyn yhteydessä, sillä kielto säilyttää tietoja yleisesti ja erotuksetta vakavan rikollisuuden torjumiseksi menettäisi silloin kokonaan tehokkaan vaikutuksena. (G. D. 100)

Unionin tuomioistuin on muistuttanut, että se on edellyttänyt kansallisten viranomaisten jokaisessa tapauksessa varmistavan, että niin saatavat tiedot kuin tiedonsaannin ajanjakso on rajattu tarkasti välttämättömään ja että pääsyn lisäksi säädetään aineellisista ja menettelyllisistä säännöksistä, jotka koskevat saatujen tietojen käyttöä (Spetsializirana prokuratura kohdat 64 ja 67).

Säilytettävien tietojen saataville asettamisessa ja näiden tietojen käytössä rikostutkinnassa on kyse kahdesta erillisestä henkilötietojen käsittelystä. Näistä jälkimmäinen kuuluu rikosasioiden tietosuojadirektiivin soveltamisalaan. Jäsenvaltiot voivat säätää rekisteröidyn informoinnista rikosasioiden tietosuojadirektiivin 13 artiklan mukaisesti. Unionin tuomioistuin kuitenkin toteaa, että kyseinen lainkohta ei mahdollista tietojensaantioikeuden rajaamista kokonaan pois. (Spetsializirana prokuratura kohdat 68–71). Oikeudesta tehokkaihin oikeussuojakeinoihin on säädettävä rikosasioiden tietosuojadirektiivin 54 artiklan mukaisesti. Tarkemman sääntelyn antaminen kuuluu kansallisen prosessiautonomian piiriin, kunhan vastaavuus- ja tehokkuusperiaatteita noudatetaan. Unionin tuomioistuin kuitenkin katsoo, että riittävää ei ole, mikäli oikeussuojakeinona on ainoastaan se, että tuomioistuin myöntää pääsyn säilytettäviin tietoihin yksinomaan toimivaltaisten viranomaisten hakemuksen perusteella ilman, että asianosaisia henkilöitä on kuultu ja ilman että tuomioistuimen on mahdollista ottaa huomioon näiden henkilöiden mahdollista vastustusta. (Spetsializirana prokuratura kohdat 72–75)

Näin ollen unionin oikeus on esteenä sellaiselle kansalliselle lainsäädännölle, jossa rekisteröidyille ei turvata tietojensaantioikeutta unionin lainsäädännön mukaisesti ja ilman että rekisteröidyillä on valitusmahdollisuus lainvastaista pääsyä vastaan (Spetsializirana prokuratura kohta 76).

> Unionin tuomioistuimen uudet linjaukset:

- Erityisen vakavaakaan rikollisuutta ei voida rinnastaa kansallista turvallisuutta koskevaan uhkaan
- Tietojen saannille asetetut rajoitukset eivät voi rajoittaa tai korjata tietojen yleisestä säilyttämisestä johtuvaa vakavaa puuttumista yksilön oikeuksiin
- Oikeutettu säilyttämisperuste yhtä tarkoitusta varten ei vaikuta toisen (alemman) tasoisen säilyttämisperusteen laillisuuteen
- Tietoon pääsyä ei voida oikeuttaa yleisen edun tavoitteiden hierarkian mukaisella alemmalla perusteella kuin mihin tietojen säilyttäminen perustuu
- Unionin oikeus on esteenä sellaiselle kansalliselle lainsäädännölle, jossa rekisteröidyille ei turvata tietojensaantioikeutta unionin lainsäädännön mukaisesti ja ilman että rekisteröidyillä on valitustie lainvastaista pääsyä vastaan.

3 Suomen lainsäädännön EU-oikeuden mukaisuuden arviointi

3.1 Kansalliseen lainsäädäntöön tehdyt muutokset

Laki sähköisen viestinnän palveluista (917/2014)

Viestinnän välitystietojen säilyttämisvelvollisuudesta säädetään sähköisen viestinnän palveluista annetun lain 157 §:ssä. Kyseiseen pykälään ei ole tehty muutoksia vuoden 2021 arviomistion laatimisen jälkeen.²⁴

Pakkokeinolaki (806/2011), poliisilaki (872/2011), laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019) ja sotilastiedustelulaki (590/2019)

²⁴ Ks. 2021 arviomistio s. 17: Vuonna 2017 tehdyn arvioinnin jälkeen pykälään on tehty vain teknisluonteisia muutoksia. (HE 61/2018 vp; HE 98/2020 vp).

Säilytysvelvollisuuden alaisten tietojen luovuttaminen on sidottu SVPL 157 §:n viittauksella pakkokeinolain 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi.

Momentin 6 kohtaa on muutettu vuonna 2021 siten, että siihen on lisätty televalvonnan perusterikokseksi terrorismirikoksiin liittyvä julkinen kehottaminen (HE 89/2021 vp).²⁵ Terrorismirikoksia kokonaisuudessaan voi pitää vakavina rikoksina, joten muutos on linjassa viestinnän välitystietoja koskevan oikeuskäytännön kanssa.

Säilytysvelvollisuuden alaisten välitystietojen käyttötarkoituksista kansallisen turvallisuuden tarkoituksiin säädetään poliisilain 5 a luvun 53 §:ssä ja sotilastiedustelulain 103 §:ssä. Kumpaankaan pykälään ei ole tehty muutoksia vuoden 2021 arviomuistion laatimisen jälkeen.

Lisäksi kokonaisuuteen liittyy myös laki tietoliikennetiedustelusta siviilitiedustelussa, jossa säädetään tietoliikennetiedustelun käyttämisestä poliisilain 5 a luvussa tarkoitetussa siviilitiedustelussa. Siviilitiedustelulakia ei käsitellä tässä jatkoselvityksessä, sillä säilytysvelvollisuuden perusteella säilytettyjen tietojen saantia koskeva peruste sisältyy poliisilain 5 a lukuun.

Pakkokeinolain ja poliisilain osalta on huomioitava, että kyseisiin lakeihin on tulossa muutoksia (HE 217/2022 vp ja HE 275/2022 vp). Eduskunta on hyväksynyt pakkokeinolakia koskevan hallituksen esityksen mietinnön LaVM 30/2022 vp mukaisena ja poliisilain HaVM 42/2022 vp mukaisena.

Telekuuntelu- ja televalvontalupaa ei enää jatkossa haeta ja määrätä teleosoite- tai telepäätelaittekohtaisesti, vaan telepakkokeinoja voidaan kohdistaa mihin tahansa tietyn epäillyn käytössä olevaan osoitteeseen tai laitteeseen. Epäillyn käyttämien teleosoitteiden ja -päätelaitteiden yksilöintitietojen selvittäminen jää esityksen mukaan pidättämiseen oikeutetun virkamiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen virkavastuulla selvittäväksi asiaksi. Tuomioistuin päättää edelleen henkilöstä, jonka viestintään telekuuntelun tai televalvonnan on tarkoitus kohdistua. Käytännössä kuitenkin toimenpiteen laajuus ja kohdistuminen henkilön hallussa olevaan tai muuten hänen käyttämäkseen oletettuun laitteeseen tai osoitteeseen jää riippumaan pidättämiseen oikeutetun virkamiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen päätöksestä.

Unionin tuomioistuin on ratkaisuisaan linjannut, että tietojen saannin edellytyksenä on tuomioistuimen tai riippumattoman hallintoviranomaisten suorittama ennakkovalvonta. Kyseisen tuomioistuimen tai elimen ratkaisu annetaan perustellusta pyynnöstä, jonka nämä viranomaiset esittävät rikoksen estämisen, selvittämisen tai syyteharkintamenettelyssä. (TS kohta 120) Toimivaltainen kansallisten viranomaisten on varmistettava jokaisessa yksittäistapauksessa, että sekä kyseessä olevien tietojen luokka tai luokat että ajanjakso, jolta kyseisten tietojen saantia pyydetään, ovat asian olosuhteet huomioon ottaen rajattu kyseessä olevan tutkinnan kannalta täysin välttämättömään (Prokuratuur kohta 38). Lisäksi unionin tuomioistuin on katsonut, että tilanne, jossa tietojen saantia koskevien pyyntöjen käsittelystä vastuussa oleva virkamies on yksin toimivaltainen arvioimaan rekisteröityjä koskevia epäilyjä ja tutkimaan heitä koskevien tietojen saamisen välttämättömyys, ei vastaa vaatimusta objektiivisille kriteereille siten kuin sitä on aikaisemmassa oikeuskäytännössä tulkittu. (G. D. kohta 113)

Pakkokeinolain ja poliisilain muutoksen jälkeenkin tuomioistuin tekee päätöksen henkilöstä, johon telepakkokeino kohdistuu. Kyse ei siis liene G. D. –ratkaisun mukaisesta tilanteesta, jossa tietojen saantia koskevien pyyntöjen käsittely olisi keskitetty poliisin virkamiehelle, vaikka muutos lisää poliisin päätösvaltaa. Toisaalta perustuslakivaliokunta arvioi ehdotuksen merkittävän perustuslakivaliokunnan käsityksen mukaan huomattavaa ja periaatteellisesti merkittävää muutosta perustuslain 10 §:ssä turvatun luottamuksellisen viestin salaisuuden suojan rajoittamista koskevaan lainsäädäntöön (PeVL

²⁵ Ks. vastaavasti arviomuistio 2021 s. 21 ja HE 30/2018 vp.; HE 135/2020 vp.

99/2022 vp, 5 kohta). Unionin tuomioistuin on edellyttänyt, että viranomaisten on varmistettava yksittäistapauksessa, että pyydettävät tiedot on sekä tietojen luokkien että ajanjakson suhteen rajattu välttämättömään. Televalvontaa koskevan vaatimuksen sisällölle asetetuissa edellytyksissä (pakkokeinolain 10 luvun 9 §; poliisilain 5 luvun 10 §) ei erikseen vaadita rajaamaan saatavia tietoja, mutta aikaisemmin vaatimuksessa on tullut esittää toimenpiteen kohteena oleva teleosoite tai telepäätelaitte sekä mahdolliset televalvonnan rajoitukset ja ehdot. Muutos vaikuttaa siis heikentäneen laista johtuvaa velvoitetta rajata pyydettävät tiedot teleosoitteen ja telepäätelaitteen mukaan vaatimuksessa, joka esitetään tuomioistuimelle.²⁶ Hallintovaliokunta on kuitenkin korostanut, että sääntelyn mukaan pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystään kuuluvan poliisimiehen on tehtävä toimenpiteen kohteena olevista teleosoitteista tai -päätelaitteista erillinen päätös, jossa on nimenomaisesti perusteltava syyt niiden valitsemiselle (HaVM 42/2022 vp). Pakkokeinojen käyttöön lisäksi sisältyy yleisinä vaatimuksina suhteellisuusperiaatteen ja vähimmän haitan periaatteen noudattaminen.

Kansalliseen lainsäädäntöön on siis pääasiassa tehty sellaisia muutoksia, joiden unionin oikeuden mukaisuutta ei ole tässä yhteydessä tarvetta arvioida tarkemmin. Lainsäädäntöä muutettaessa tulee kuitenkin arvioida lähemmin unionin tuomioistuimen asettamaa edellytystä, jonka mukaan toimivaltaisten kansallisten viranomaisten on varmistettava jokaisessa yksittäistapauksessa, että sekä kyseessä olevien tietojen luokka tai luokat että ajanjakso, jolta kyseisten tietojen saantia pyydetään, on asian olosuhteet huomioon ottaen rajattu kyseessä olevan tutkinnan kannalta täysin välttämättömään.

Alla käsitellään seuraavaksi tuomioistuimen vuoden 2022 oikeuskäytännössä esittämiä uusia linjauksia ja arvioidaan niiden vaikutusta kansalliseen lainsäädäntöön.

3.2 Unionin tuomioistuimen linjaukset

Yleiset reunaehdot

Unionin tuomioistuimen mukaan sähköisen viestinnän tietosuojadirektiivi on perussäädös henkilötietojen säilyttämisessä ja niiden käsittelystä sähköisen viestinnän alalla

Viestinnän välitystietojen säilyttämisvelvollisuudesta säädetään SVPL:n 157 §:ssä. Säilytysvelvollisuutta koskeva kansallinen sääntely perustuu sähköisen viestinnän tietosuojadirektiivin 15(1) artiklaan, jossa jäsenvaltioille annetaan mahdollisuus poiketa direktiivin velvoitteista. On selvää, että SVPL 157 §:ää tarkastellaan sähköisen viestinnän tietosuojadirektiivin ja sitä koskevan unionin tuomioistuimen oikeuskäytännön valossa. Tässä jatkoselvityksessä tarkastelu rajoittuu SVPL 157 §:n mukaiseen tietojen säilyttämiseen.

Jatkossa kansallista lakia muutettaessa tai uusien lainsäädäntöehdotusten valmistelun yhteydessä on syytä kiinnittää huomiota siihen, että säädettäessä viranomaisten toimivaltuuksista saada sähköisen viestinnän välitystietoja tulee myös tarkastella kyseisestä lainsäädännöstä viestintäpalveluiden tarjoajille mahdollisesti johtuvia velvoitteita säilyttää tai käsitellä viestinnän välitystietoja. Lainsäädännössä tulee tarpeen mukaan nimetä selkeästi myös tietojen säilyttämisperuste. Säilyttämisperusteiden laajentamiseen muussa lainsäädännössä tulisi suhtautua hyvin varovaisesti. *Riippumatonta hallintoviranomaista koskevat vaatimukset*

Suomessa SVPL 157 §:n mukaisten viestinnän välitystietojen saannista päättää PKL:n 10:9:n mukaisesti tuomioistuin. Tältä osin unionin tuomioistuimen hallintoviranomaisen riippumattomuutta koskevilla linjauksilla ei ole vaikutusta kansalliseen lainsäädäntöön.

²⁶ Ks. vastaavasti vuoden 2021 arviomuistio s. 19, jossa johtopäätöksenä oli, että välitöntä muutostarvetta ei tältä osin ole, mutta kysymys saatavien tietojen rajaamisesta tietopyynnössä välttämättömään tietokategorioittain ja ajallisesti tulee huomioida selvemmin, jos sääntelyä muutetaan.

Unionin tuomioistuimen sallituksi arvioimat tietojen säilyttämisen toimenpiteet vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien uhkien ehkäisemiseksi

Vuoden 2017 selvityksessä on eritelty Suomen välitystietojen säilyttämistä. Selvityksen johtopäätöksenä on, että kansallinen lainsäädäntö sisältää rajoituksia säilytysvelvollisuuteen, pääasiassa seuraavasti²⁷:

- o Säilytysvelvollisuus on rajattu tiettyihin teleyrityksiin sisäministeriön päätöksellä, mikä rajaa maantieteellistä kattavuutta;
- o Säilytysvelvollisuus on rajattu tiettyihin palveluihin ja niiden sisällä tiettyihin tietoluokkiin;
- o Säilytyksen kesto on rajattu kansallisessa lainsäädännössä palveluluokittain 6, 9 ja 12 kk säilytysaikoihin, PeV edellyttämällä tavalla;
- o Säilytetyt tiedot saavien viranomaisten henkilöpiiriä on rajattu;
- o Laissa edellytetään, että ne henkilöt, jotka edellä mainituissa viranomaisissa saavat tutkia televalvonnalla saatuja tietoja, määrätään erikseen.

2017 esitetyt pääasialliset rajoitukset säilyttämismääräyksiin	Käsittely SpaceNet-ratkaisussa	FI rajoitusten arviointi SpaceNet-ratkaisun valossa
Säilytysvelvolliset yritykset rajattu tiettyihin teleyrityksiin SM:n päätöksellä	SpaceNet kohdan 83 mukaan DE lainsäädännössä säädetty säilyttäminen ”koskee lähes kaikkia väestöön kuuluvia henkilöitä”	FI säilytysvelvolliset yritykset kattaa 87 % laajakaistaliittymistä ja 99 % matkapuhelinliittymistä (ks. s. 16)
Säilytysvelvollisuus on rajattu tiettyihin palveluihin ja tiettyihin tietoluokkiin	DE lainsäädännössä lähes vastaavat (tarkempi erittely ks. liite 1)	FI säilytettävien tietojen laajuus vaikuttaa vastaavan olennaisin osin SpaceNet-ratkaisussa käsiteltyä tietojen säilyttämisen laajuutta (ks. alla tarkemmin)
Säilytyksen kesto on rajattu palveluluokittain 6, 9 ja 12 kk säilytysaikoihin	DE tietojen säilytys on rajattu 4 vk paikkatietojen ja 10 vk muiden tietojen osalta	Lyhytkään säilytysaika ei estä puuttumisen vakavuutta
Säilytetyt tiedot saavien viranomaisten henkilöpiiriä on rajattu	Vastaava kirjaus sisältyy DE lainsäädäntöön; EUT ei kuitenkaan arvioinut tätä erikseen (SpaceNet kohta 91)	EUT:n mukaan säilyttämisestä johtuvaa loukkausta ei voida rajoittaa tai korjata pääsyä koskevien rajoitusten noudattamisella
Laissa edellytetään, että tietoja tutkivat henkilöt määrätään erikseen		

Unionin tuomioistuin täydentää tuoreissa ratkaisuissaan aikaisempaa oikeuskäytäntöään QdN-ratkaisun tuomiolauselman mukaisista sallituista säilyttämistoimenpiteistä. Kohdennetun säilyttämisen ja tietojen säilyttämisen nopean varmistamisen osalta tuomioistuin vaikuttaa lähinnä täsmentävän ja selittävän aikaisempaa tulkintaansa. Erityisesti tuomioistuin vahvistaa sen, että sallittuja säilyttämistoimenpiteitä voidaan välttämättömän rajoissa yhdistellä.

Kohdennetun säilyttämisen osalta tuomioistuin selventää myös, että jäsenvaltiot voivat asettaa myös muita erottavia kriteereitä henkilöön liittyvien ja maantieteellisten kriteerien lisäksi, kunhan säilyttämistoimenpiteen ulottuvuus rajoittuu täysin välttämättömään ja kunhan vakavien rikosten ja henkilöiden, joiden tiedot säilytetään, välillä on ainakin välillinen yhteys. Suomessa säilytysvelvollisuus on rajattu tiettyihin palveluihin. Lisäksi säilytettävät tiedot on rajattu tietoluokittain välttämättömään.²⁸

²⁷ Ks. vuoden 2017 selvitys s. 22.

²⁸ LiVM 10/2014 vp.

Kansalliseen lainsäädäntöön ei kohdistu suoraa muutospainetta siltä osin kuin tuomioistuin on oikeuskäytännössään täsmentänyt ja selittänyt sallittujen säilyttämistoimenpiteiden ulottuvuutta.

Säilyttämisen ajallisen rajaamisen osalta unionin tuomioistuin ei anna selvää vastausta, mikä on katsottava täysin välttämättömään rajatuksi ajanjaksoksi. Lyhytkään säilytysaika ei poissulje sitä, että puuttuminen ei voisi olla vakavaa.

Suomessa säilytysaikojen pituus ja niiden porrastus perustuu Digital Rights Ireland -tuomion jälkeen suoritettuun välttämättömyysarviointiin.²⁹ Kansallisen lain mukaiset säilytysajat (6, 9 tai 12 kk) ovat Suomessa huomattavasti pidemmät kuin SpaceNet-ratkaisussa arvioidut saksalaisen lainsäädännön mukaiset neljä ja kymmenen viikkoa.

Suomessa olevaa säilytysvelvollisuutta ei ole pidetty yleisenä ja erotuksettomana vaan rajattuna³⁰. Unionin tuomioistuimen linjausten perusteella ei kuitenkaan voida sulkea pois sitä vaihtoehtoa, että unionin tuomioistuimen arvioinnissa suomalaista säilyttämismuutoksia päädyttäisiin pitämään yleisenä ja erotuksettomana (tarkemmin alla).

Säilyttämisperusteet ja tietojen saanti

Unionin tuomioistuin on käsitellyt tietojen säilyttämisperusteiden välistä hierarkiaa ja tietojen saantia, sekä näiden välistä yhteyttä seuraavasti:

- Erityisen vakavaakaan rikollisuutta ei voida rinnastaa kansallista turvallisuutta koskevaan uhkaan;
- Tietojen saannille asetetut rajoitukset eivät voi rajoittaa tai korjata tietojen yleisestä säilyttämisestä johtuvaa vakavaa puuttumista yksilön oikeuksiin;
- Oikeutettu säilyttämisperuste yhtä tarkoitusta varten ei vaikuta toisen (alemman) tasoisen säilyttämisperusteiden laillisuuteen;
- Tietoon pääsyä ei voida oikeuttaa yleisen edun tavoitteiden hierarkian mukaisella alemmalla perusteella kuin mihin tietojen säilyttäminen perustuu;
- Unionin oikeus on esteenä sellaiselle kansalliselle lainsäädännölle, jossa rekisteröidyille ei turvata tietojensaantioikeutta unionin lainsäädännön mukaisesti ja ilman että rekisteröidyillä on valitustie lainvastaista pääsyä vastaan.

Suomessa tietoja säilytetään vakavien, pakkokeinolain 10 luvun 6 §:n 2 momentin mukaisten rikosten torjuntaa varten. Säilytysvelvollisuuden laajuutta ei ole kohdennettu eri tavoin vakavan rikollisuuden, yleisen turvallisuuden tai kansallisen turvallisuutta koskevien tavoitteiden perusteella. Poliisilaki ja sotilastiedustelulaki ovat laajentaneet käyttötarkoitusta kansalliseen turvallisuuteen. Siten hierarkiassa alemman tasoisen perusteiden (vakava rikollisuus) mukaisesti säilytettyjen tietojen käyttö korkeamman tasoisen perusteiden tarkoituksessa on suhteellisuusperiaatteen mukaisesti mahdollista. Tältä osin välitöntä muutostarvetta ei siis ole, vaikka täysin ongelmattomana ei voida pitää sitä, että kaikkia säilytysperusteita ei ole mainittu säilyttämismuutoksen yhteydessä.

Jatkovalmistelussa on lisäksi syytä tarkastella, tulisiko säilyttämistä koskevaa sääntelyä eriyttää eri tasoisten säilyttämisperusteiden osalta.

Unionin tuomioistuin on tarkentanut, että tietojen säilyttämisen (kuin myös saannin) vakavuuden arvioinnissa ei ole merkitystä sillä, ovatko tiedot konkreettisesti arkaluontoisia ja että tietojen saantia

²⁹ LiVM 10/2014 vp

³⁰ Ks. vuoden 2017 selvitys, s. 22.

koskevien sääntöjen täysimääräinen noudattaminen ei voi rajoittaa tai edes korjata tietojen yleisestä säilyttämisestä johtuvaa vakavaa puuttumista yksilön oikeuksiin.

Suomessa säilyttämisvelvollisuuden hyväksyttävyyttä ei ole ensisijassa perusteltu tietojen ei-arkaluontoisuudella.³¹ Tältä osin muutostarvetta ei ole.

Sen sijaan vuoden 2017 selvityksessä säilyttämisvelvollisuuden rajoituksiksi on tunnistettu seikkoja, jotka koskevat pääasiassa tietojen saantia koskevien sääntöjen noudattamista ja joilla pyritään suojaamaan tietoja väärinkäytön vaaroilta.³² Sähköisen viestinnän palveluista annettu laki kuitenkin sääntelee tietojen säilyttämisvelvollisuutta. Jatkossa on syytä kiinnittää huomiota siihen, että pääsyä koskevalla suojaomilla ei voi perustella säilyttämisen oikeasuhtaisuutta.

3.3 Suomen ja Saksan lainsäädännön vertailu

Suomen ja Saksan kansallisia viestinnän välitystietojen säilyttämistä koskevia lainsäädäntöjä voidaan pitää varsin samankaltaisina. Molemmissa järjestelmissä säilyttäminen on rajattu tiettyihin palveluihin, ja kunkin palvelun osalta on määritelty yksityiskohtaisesti säilytettävät tietokategoriat. Lisäksi molemmissa lainsäädännöissä on myös suojatakeita väärinkäytöksiä vastaan. Saksan kansallinen lainsäädäntö ja tietojen säilyttämisen laajuus, siten kuin unionin tuomioistuin on sitä eritellyt SpaceNet-ratkaisussaan, antaa konkreettisen vertailukohdan myös Suomen kansallisen lainsäädännön arvioinnille.

Säilytettyjen tietojen laajuuden osalta unionin tuomioistuin katsoi, että muutamista säilyttämisvelvollisuuden rajoituksista huolimatta Saksan kansallinen lainsäädäntö pääasiallisesti vastaa QdN-ratkaisuun johtanutta tilannetta. (SpaceNet kohta 78) Unionin tuomioistuin katsoi, että Saksan kansallisen lainsäädännön mukainen viestinnän välitystietojen säilyttäminen koskee lähes kaikkia väestöön kuuluvia henkilöitä, vaikka he eivät ole edes välillisesti tilanteessa, joka voisi johtaa rikosoikeudellisen menettelyn vireillepanoon. Samoin tuomioistuin katsoi, että Saksan lainsäädännössä säädetään liikenne- ja paikkatiedoista *olennaisen osan*, jonka **laajuus vastaa olennaisilta osin** QdN-ratkaisuun johtanutta säilytettyjen tietojen laajuutta, *perustetta edellyttämätöntä sekä yleistä ja henkilöllisesti, ajallisesti ja maantieteellisesti erottelematonta säilyttämistä*. (SpaceNet kohta 83)

SpaceNet-ratkaisussa unionin tuomioistuin arvioi Saksan kansallista viestinnän välitystietojen säilyttämistä koskevaa lainsäädäntöä varsin yksityiskohtaisesti. Ratkaisu tarjoaa konkreettisen esimerkin siitä, miten säilytettävien tietojen laajuutta voidaan arvioida. Suomen ja Saksan lainsäädäntöjen vertailu mahdollistaa sen arvioinnin, vastaako Suomen kansallinen lainsäädäntö *olennaisilta osin* QdN-ratkaisussa käsiteltyä tietojen säilyttämisen laajuutta. SpaceNet-ratkaisussa unionin tuomioistuin katsoi, ettei Saksan kansallisen lain kaltaista tietojen säilyttämisvelvollisuutta voida pitää kohdennettuna tietojen säilyttämisenä. (SpaceNet kohdat 83-84) Seuraavaksi on siis syytä tarkastella yksityiskohtaisemmin Suomen ja Saksan kansallisista järjestelmistä johtuvaa tietojen säilyttämisen laajuutta.

Merkittävin ero Suomen ja Saksan välitystietojen säilyttämistä koskevissa lainsäädännöissä on säilytysajan kesto. Saksassa säilytysaika on rajattu paikkatietojen osalta 4 viikkoon ja muiden tietojen osalta 10 viikkoon. Suomessa säilytysaika on SVPL 157 §:n 4 momentissa porrastettu palvelutyypeittäin. Matkaviestinverkon puhelin- ja tekstiviestipalveluiden osalta tiedot tulee säilyttää 12 kuukautta, internetyhteyspalveluiden tiedot 9 kuukautta ja internetpuhelinpalvelun tiedot 6 kuukautta.

Suomen ja Saksan lainsäädännöissä on joitain eroavaisuuksia siitä, mitä tietoja palveluntarjoajien tulee kunkin palvelutyyppin osalta säilyttää. Säilytysvelvoitteen alaiset palvelut on määritelty SVPL 157 §:n 2

³¹ Vastaavasti arviomuistio 2021 s. 18.

³² Ks. 2017 selvitys s. 22.

momentissa. Säilytysvelvollisuus koskee säilytysvelvollisen yrityksen tarjoamaan internetpuhelinpalveluun, internetyhteyspalveluun ja puhelinpalveluun liittyviä tietoja. Palveluluokat ovat Suomessa ja Saksassa samat, sillä erotuksella, että Suomessa ei säilytetä kiinteän puhelinverkon palveluiden tietoja. (SpaceNet kohta 14)

Suomessa säilytettävät tietoluokat on määritelty SVPL 157 §:n 3 momentissa. Säilytysvelvollisuuden piiriin kuuluvien tietojen teknisiä yksityiskohtia on määritelty Viestintäviraston (nyk. Liikenne- ja viestintävirasto) määräyksessä 53 B/2014 M. Saksan kansallista viestinnän välitystietojen säilyttämistä koskevaa lainsäädäntöä on vertailtu Suomen sähköisen viestinnän palveluista annetun lain mukaisiin säädöksiin yksityiskohtaisesti liitteessä 1 (*Vertailutaulukko sähköisen viestinnän välitystietojen säilyttämistoimenpiteiden laajuudesta Suomen ja Saksan kansallisessa lainsäädännössä*). Säilytettävien tietojen luokat vastaavat pääasiassa toisiaan ja niissä on vain pieniä eroja. Saksassa tulee säilyttää pre-paid-liittymän aktivoinnista syntyvät tiedot ja internetyhteyspalvelun mobiilikäytön yhteyden alkaessa käytetyt lähetyssovellusten tunnuksien. SVPL:ssä internetyhteyspalvelun osalta tulee säilyttää myös laitteen tunnus mutta ei paikkatietoja.

Säilyttämisvelvollisuus ei koske viestinnän sisältöä, tietoja vierailuista internetsivuista ja tietoja sähköpostipalveluista Suomessa eikä Saksassa (SVPL 157 §:n 5 mom.; SpaceNet kohta 15 ja Telekommunikationsgesetz 113 b §:n 5 kohta). Lisäksi säilytettävien tietojen ulkopuolelle voidaan Saksassa hakemuksesta rajata tiettyjen sosiaalialan tai kirkon auttavat puhelinpalvelut. Vastaavaa rajoitusta ei Suomessa ole.

Saksassa säilytysvelvollisia ovat operaattorit, jotka tarjoavat loppukäyttäjille yleisesti saatavilla olevia telepalveluita. (SpaceNet kohta 13; Telekommunikationsgesetz 113 a §:n 1 momentti) Suomessa sisäministeriö määrittelee säilytysvelvolliset yritykset päätöksellään. (SVPL 157 § 1 mom.) Säilytysvelvollisia yrityksiä Suomessa ovat 27.2.2015 annetun päätöksen mukaan DNA Oyj, Elisa Oyj, Telia Finland Oyj ja Ålands Telekommunikation Ab. Säilytysvelvollisten yritysten piiriin voidaan periaatteessa katsoa siis olevan Suomessa suppeampi.

Nimetyt yritykset on määritelty säilytysvelvollisiksi merkittävän yhteenlasketun markkinaosuuden ja maantieteellisen kattavuuden perusteella. Tästä seuraavien rajausten merkittävyyttä vähentää se, että nimettyjen teleyritysten markkinaosuus kattaa suurimman osan Suomen matkaviestinpalveluista ja kiinteistä internetyhteyspalveluista.³³ Kolmen suurimman teleyrityksen DNA:n, Elisan ja Telia Finlandin yhteenlaskettu markkinaosuus on 87 % kiinteän verkon laajakaistaliittymistä³⁴ ja yli 99 % matkaviestinverkon liittymistä³⁵. Siten säilytysvelvollisten yritysten erillinen nimeäminen ei käytännössä kavenna juurikaan säilytettävien tietojen laajuutta.

Suomen ja Saksan kansallisia lainsäädäntöjä koskien säilytettäviä tietoja voidaan pitää varsin samankaltaisina. Suurimmat erot liittyvät säilytysaikoihin, jotka Saksassa ovat huomattavasti lyhyempiä kuin Suomessa. Säilytysvelvollisuutta koskevat palveluluokat ovat Suomessa ja Saksassa lähes samat, sillä erotuksella, että Suomessa ei enää säilytetä kiinteän lankapuhelinverkon puhelinpalveluun liittyviä tietoja. Kullekin palvelulle määritellyt säilytettävät tietoluokat ovat varsin samankaltaisia, pienin erotuksin.

Suomen kansallinen välitystietojen säilyttämistä koskeva lainsäädäntö vastaa keskeisiltä osin SpaceNet-ratkaisussa käsiteltyä tietojen säilyttämisen laajuutta, jonka unionin tuomioistuin on katsonut koskevan lähes kaikkia väestöön kuuluvia henkilöitä ilman edes välillistä yhteyttä tilanteeseen, joka

³³ Ks. vastaavasti vuoden 2017 selvitys s. 6 ja 22.

³⁴ DNA, Elisa ja Telia Finland Kiinteän verkon laajakaistaliittymien markkinaosuudet kesäkuu 2022 = 87 % (Finnet 9; muut 4 %) (<https://tieto.traficom.fi/fi/tilastot/kiinteän-verkon-laajakaistaliittymät>, päivitetty 19.10.2022)

³⁵ DNA, Elisa, Telia Finland Matkaviestinverkon liittymien markkinaosuudet kesäkuu 2022 = yli 99 % (muut alle 1 %) (<https://tieto.traficom.fi/fi/tilastot/matkaviestinverkon-liittymät>, päivitetty 19.10.2022)

voisi johtaa rikosoikeudellisen menettelyn vireillepanoon ja jossa säädetään liikenne- ja paikkatiedoista olennaisen osan sellaisesta säilyttämisestä, joka on perustetta edellyttämätöntä, yleistä ja henkilöllisesti, ajallisesti ja maantieteellisesti erottelematonta. (SpaceNet kohta 83) Unionin tuomioistuimen mukaan tällaista lainsäädäntöä ei voida pitää kohdennettuna tietojen säilyttämisenä. (SpaceNet kohta 84)

Kun otetaan huomioon SpaceNet-ratkaisussa esitetty arviointi sekä yllä käsitelty Suomen ja Saksan kansallisten järjestelmien samankaltaisuus, ei voida sulkea pois sitä vaihtoehtoa, että suomalaista säilyttämisvelvollisuutta pidettäisiin yleisenä ja erotuksettomana.

4 Johtopäätökset

Yllä käsitellysti unionin tuomioistuimen ratkaisukäytäntö sähköisen viestinnän välitystietojen säilyttämistä ja viranomaiskäyttöä koskien on kehittynyt vuoden 2022 ratkaisuiden perusteella. Eräiltä osin unionin tuomioistuin vaikuttaa, erityisesti G. D. –ratkaisussaan, selkeyttävän ratkaisukäytäntöään ja selittävän sen soveltamista. Selkeytyksiä ovat muun muassa: 1) sallittuja säilyttämistoimenpiteitä voidaan välttämättömän rajoissa soveltaa yhdessä; 2) myös muut erottavat kriteerit ovat kansallisen lainsäätäjän harkinnan mukaan mahdollisia maantieteellisten ja henkilöryhmään perustuvien kriteerien lisäksi, kunhan säilyttämistoimenpiteen ulottuvuus rajoittuu täysin välttämättömään ja kunhan vakavien rikosten ja henkilöiden, joiden tiedot säilytetään, välillä on ainakin välillinen yhteys; ja 3) kohdennetun säilyttämisen ja quick freeze -määräyksen kohdistuvien tietojen piiriä on selvennetty ja tällaisen säilyttämismääräyksen antamisen ajankohtaa on selvennetty. Toisaalta säilyttämisen ajalliseen rajaamiseen tuomioistuin ei anna selvää vastausta. Tuomioistuin muistuttaa, että säilyttäminen itsessään on vakava puuttuminen perusoikeuksiin ja sitä ei muuta toiseksi edes melko lyhytkin säilyttämisanjakso, kuten neljä tai kymmenen viikkoa.

SpaceNet-ratkaisussa käsiteltyä Saksan kansallista lainsäädäntöä voidaan pitää samankaltaisena Suomen kansallisen järjestelmän kanssa. SpaceNet-ratkaisu tarjoaa Suomelle konkreettisen vertailukohdan tarkastella kansallista lainsäädäntöämme ja verrata sitä unionin tuomioistuimen oikeuskäytäntöön, sillä ratkaisussa tuomioistuin soveltaa aikaisempaa ratkaisukäytäntöään arvioidessaan Saksan kansallista lainsäädäntöä. Yllä ja jatkoselvityksen liitteenä olevassa vertailutaulukossa on eritelty yksityiskohtaisesti Suomen ja Saksan tietojen säilyttämistä koskevaa keskeistä lainsäädäntöä.

Johtopäätöksenä on, että Suomen kansallinen välitystietojen säilyttämisvelvollisuus vaikuttaa vastaavan *olennaisin osin* Saksan kansallisen järjestelmän mukaista tietojen säilyttämisen laajuutta. Näin Suomen kansallista lainsäädäntöä on mahdollista pitää liikenne- ja paikkatietojen säilyttämisenä, joka koskee lähes kaikkia väestöön kuuluvia henkilöitä, vaikka he eivät ole edes välillisesti tilanteessa, joka voisi johtaa rikosoikeudellisen menettelyn vireillepanoon ja jossa säädetään samoin liikenne- ja paikkatiedoista olennaisen osan, jonka laajuus vastaa olennaisilta osin QdN-ratkaisuun johtaneissa asioissa säilytettyjen tietojen laajuutta, sellaisesta säilyttämisestä, joka on perustetta edellyttämätöntä, yleistä ja henkilöllisesti, ajallisesti ja maantieteellisesti erottelematonta. Sekä Suomen että Saksan kansallisessa järjestelmässä on säilyttämisen kohdentamisen perusteina käytetty pääasiassa vastaavia kohdentamisperusteita. Unionin tuomioistuin toteaa kuitenkin suoraan, että SpaceNet-ratkaisussa käsitellyn kaltaista tietojen säilyttämisvelvollisuutta ei voida pitää kohdennettuna tietojen säilyttämisenä.

Siten kansallista lainsäädäntöä on tarpeen päivittää, jotta varmistetaan sekä käyttäjien yksityisyyden suojan kunnioittaminen ja että puuttuminen siihen rajoitetaan välttämättömään siten kuin unionin tuomioistuimen oikeuskäytännössä puuttumisen laajuutta on käsitelty. Samalla on tärkeää varmistaa, että viranomaisilla on tehokkaat ja oikeasuhteiset toimivaltuudet tiedon saantiin rikollisuuden torjumiseksi, yleisen turvallisuuden takaamiseksi sekä kansallisen turvallisuuden varmistamiseksi.

Unionin tuomioistuimen ratkaisukäytännön seurauksena myös muut jäsenmaat ovat tarkastelleet tai tarkastelevat kansallista välitystietojen säilyttämistä koskevaa lainsäädäntöään. Esimerkiksi Irlanti ja Belgia ovat jo uudistaneet lainsäädäntöään ja ottaneet käyttöön säilyttämistoimenpiteitä noudattaen unionin tuomioistuimen oikeuskäytännössä käsittelemiä sallittujen säilyttämistoimien laajuutta. SpaceNet-ratkaisun jälkeen myös Saksassa on tehty arviointia ja valmisteltu muutoksia kansalliseen lainsäädäntöön. Vaikutuksista kansalliseen lainsäädäntöön ovat lisäksi ilmoittaneet ainakin Viro ja Tanska. Lisäksi Bulgaria tarkastelee Spetsializirana prokuratura -ratkaisun seurauksena muutostarpeita kansalliseen lainsäädäntöön. Osassa jäsenmaista, kuten Portugalissa ja Alankomaissa, ei ole voimassa olevaa lainsäädäntöä välitystietojen säilyttämismääräyksen voimaantulusta. Osa jäsenmaista kannattaa EU-tason ratkaisua asiaan.

Arviomuistion 2021 lausuntokierroksella lausunnonantajia pyydettiin lausumaan mielipiteensä siitä, tulisiko sähköisen viestinnän välitystietojen säilyttämismääräyksen voimaantulusta antaa uusi EU-tason lainsäädäntöehdotus. Suurin osa ilmaisee vastauksissaan, että heillä ei ole asiassa kantaa tai he eivät halua lausua asiasta. Viisi lausunnonantajaa vastusti EU-tason lainsäädäntöehdotusta ja vain yksi kannatti sitä.³⁶

Unionin tason yhtenäinen ratkaisu lähivuosina vaikuttaa epätodennäköiseltä. Arvioinnissa ja jatkovalmistelussa tulee kuitenkin ottaa huomioon EU:n lainsäädäntömenettelyssä yhä valmistelussa oleva sähköisen viestinnän tietosuoja-asetusehdotus. Asetusehdotuksella on tarkoitus kumota nykyinen sähköisen viestinnän tietosuojadirektiivi. Asetusehdotuksessa tulisi säätää viestinnän välitystietojen sallituista käsittelytoimista sekä siitä perusteesta, jolla kansallisesti voitaisiin poiketa asetusehdotuksen velvoitteista tietyissä hyväksytyissä tarkoituksissa, kuten rikollisuuden torjunnan, yleisen turvallisuuden ja kansallisen turvallisuuden takaamisen tarkoituksissa. Lisäksi unionin tuomioistuimessa on edelleen vireillä useita ennakkoratkaisupyynnöitä, joilla oletettavasti oikeustila tulee muuttumaan vielä lähivuosina.

Unionin tuomioistuin on oikeuskäytännössään käsitellyt eräitä säilyttämistoimenpiteitä, jotka eivät olisi unionin oikeuden vastaista, kuten tietojen säilyttämisen kohdentaminen maantieteellisen tai henkilöpiiriin liittyvän kriteerin avulla. Vuoden 2017 selvityksen yhteydessä esitettyjen asiantuntija-arvioiden mukaan säilytysvelvollisuuden rajaaminen tiettyyn henkilöpiiriin tai maantieteelliseen alueeseen on hyvin haasteellista toteuttaa asiallisesti ja teknisesti.³⁷ Tulevia kansallisia ratkaisuja arvioitaessa on myös kiinnitettävä huomiota siihen, että säilytysvelvollisuuden kohdentamisessa tulee huomioida muut perusoikeuksiin liittyvät näkökohdat.

Vuoden 2021 arviomuistiossa on tunnistettu eräitä seikkoja, jotka tulee huomioida selvemmin, jos sääntelyä jatkossa muutetaan. Nämä ovat jo vuonna 2017 esille nostettu säilytysvelvollisuuden soveltamiskäytäntöön liittyvä epäselvyys rikosten ennaltaehkäisemisessä ja tietojen säilyttäminen unionin alueella, arkaluontoisten tietojen käsittelyyn ja automaattiseen käsittelyyn liittyvien erityisten suojakeinojen tarve sekä saatavien tietojen rajaaminen tietopyynnöissä välttämättömään tietokategorioittain ja ajallisesti.

Lisäksi on aiheellista kiinnittää huomiota myös vuoden 2021 arviomuistion lausuntokierroksella saaduissa lausunnoissa esiin nostettuihin kehityskohteisiin. Erityisesti oikeuskanslerinviraston lausunnoissa kehoitettiin ryhtymään toimiin, että lakiin sisällytettäisiin velvoite säilyttää tietoja unionin alueella sekä sääntelyä asianmukaisista teknisistä ja organisatorisista toiminnoista, joilla taataan tietojen koskemattomuuden ja turvallisuuden erityisen korkea suojan ja turvan taso.

³⁶ Ks. Lausuntoyhteenveto: Arviomuistio Suomen data retention -sääntelyn unionin oikeuden mukaisuudesta VN/7266/2021 s. 3.

³⁷ Ks. Raportit ja selvitykset 9/2017 s. 21.

Liitteet

Liite 1: Vertailutaulukko sähköisen viestinnän välitystietojen säilyttämistoimenpiteiden laajuudesta Suomen ja Saksan kansallisessa lainsäädännössä