LUONNOS

Sähköisen viestinnän välitystietojen säilytysvelvollisuus

Arviomuistio kansallisen lainsäädännön täsmentämisen vaihtoehdoista

Liikenne- ja viestintäministeriö, Helsinki XX

LIIKENNE- JA VIESTINTÄMINISTERIÖ
KOMMUNIKATIONSMINISTERIET

Sisältö

Tiivistelmä

Yksityiselämän, henkilötietojen suoja sekä viestinnän luottamuksellisuus on taattu EU:n perusoikeuskirjassa ja perustuslaissa. Sähköisen viestinnän palveluista annetun lain (917/2014) 157 §:ssä on säädetty nimetyille teleyrityksille velvollisuus säilyttää sähköisen viestinnän välitystietoja viranomaistarpeisiin. Välitystietojen säilyttämisen ja käytön viranomaistarpeisiin on arvioitu olevan merkittävä rajoitus niin viestinnän luottamuksellisuuteen kuin yksityiselämän ja henkilötietojen suojaan. Rajoitukset perusoikeuksiin ovat mahdollisia ainoastaan siltä osin kuin ne perustuvat jonkin yleiseen etuun liittyvän tavoitteen varmistamiseen, ne rajoitetaan välttämättömään ja niissä kunnioitetaan perusoikeuksien keskeistä sisältöä. Sähköisen viestinnän välitystietojen säilyttäminen on arvioitu välttämättömäksi esitutkinta- ja tiedusteluviranomaisille muun muassa rikosten selvittämiseksi ja kansallisen turvallisuuden varmistamiseksi.

Sähköisen viestinnän välitystiedoilla tarkoitetaan teleoperaattorille tallentuvia tietoja viestinnän välittämisestä, eli esimerkiksi kännykkäpuheluiden osalta tietoja kuten puhelinnumero, liittymän tilaajan nimi sekä viestinnän aika ja paikka. Teleoperaattoreilla on tarve käsitellä viestinnän välitystietoja esimerkiksi palvelun toteuttamiseksi ja siitä laskuttamiseksi. Tietojen käsittely on sallittua vain siinä laajuudessa kuin laissa on säädetty.

EU:n tuomioistuin on edellisten vuosien aikana antanut useita ennakkoratkaisuja, joissa se on arvioinut välitystietojen säilyttämistä ja käyttöä edelleen rikollisuuden torjuntaan sekä yleisen ja kansallisen turvallisuuden varmistamiseksi. Unionin tuomioistuimen oikeuskäytännön aiheuttamaa muutostarvetta kansalliseen lainsäädäntöön on arvioitu liikenne- ja viestintäministeriössä vuosina 2017, 2021 ja 2023. Arviointien ja erityisesti oikeuskanslerilta saadun lausunnon johdosta on päädytty tarpeeseen täsmentää kansallista lainsäädäntöä unionin tuomioistuimen linjausten mukaisesti.

Unionin tuomioistuimen oikeuskäytännön mukaan välitystietojen säilytysvelvollisuuden tulee perustua objektiivisiin ja syrjimättömiin kriteereihin. Tuomioistuin on linjannut, että välitystietojen säilyttämisestä on mahdollista säätää vakavan rikollisuuden torjumiseksi sekä yleisen ja kansallisen turvallisuuden suojaamiseksi. Tuomioistuin on asettanut säilyttämiselle tiukempia reunaehtoja silloin, kun välitystietoja säilytetään vakavan rikollisuuden torjuntaan ja yleisen turvallisuuden suojaamiseen, ja pitänyt pääsääntöisesti yleistä ja erotuksetonta säilytysvelvollisuutta näitä tarkoituksia varten unionin oikeuden vastaisena. Kansallisen turvallisuuden takaamiseksi unionin tuomioistuin on pitänyt mahdollisena säilyttää välitystietoja yleisesti ja erotuksetta tilanteissa, joissa asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi.

Unionin tuomioistuin on käsitellyt eräitä säilyttämistoimenpiteitä, jotka täyttäisivät perusoikeuskirjasta johtuvat perusoikeuden rajoitusedellytykset. Tuomioistuin on muun muassa arvioinut, ettei unionin oikeus ole esteenä lainsäädännöllisille toimenpiteille, joissa säädetään kansallisen turvallisuuden suojaamiseksi, rikollisuuden torjumiseksi ja yleisen turvallisuuden suojaamiseksi sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä. Vastaavasti se on sallinut välitystietojen kohdennetun säilyttämisen, liittymän lähteelle annettujen IP-osoitteiden yleisen ja erotuksettoman säilyttämisen sekä niin kutsutut quick freeze -määräykset, siltä osin kuin ne ovat välttämättömiä kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi. Tuomioistuin on lisäksi edellyttänyt, että jäsenvaltioiden on varmistettava riittävät ja tehokkaat aineelliset ja menettelylliset takeet väärinkäytön vaaroja vastaan.

Osa EU-jäsenmaista, esimerkiksi Tanska, Irlanti ja Belgia, on muuttanut kansallista lainsäädäntöään tuomioistuimen oikeuskäytännössä arvioimien säilyttämistoimenpiteiden mukaiseksi. Myös Ruotsissa on laadittu ehdotus vastaavaksi sääntelyksi. Osassa jäsenmaista, kuten Alankomaissa ja Portugalissa, ei ole voimassa olevaa sääntelyä välitystietojen säilyttämisvelvollisuudesta. Vertailun perusteella voidaan todeta, että jäsenvaltiot ovat ottaneet käyttöön erityyppisiä velvoitteita. Jäsenvaltioiden näkemykset säilytyksen kohdentamisesta ja välttämättömyydestä näyttävät eroavan toisistaan. Tämä voi osin selittyä poliittisella tahdolla tai lainmuutosprosessin hitaudella, osin jäsenvaltiokohtaisilla erityispiirteillä, joita vasten esimerkiksi toimenpiteen välttämättömyyttä kansallisesti arvioidaan.

Sähköisen viestinnän palveluista annetun lain 157 §:n mukaan sisäministeriö nimeää päätöksellään teleyritykset (säilytysvelvollinen yritys), joilla on velvollisuus säilyttää tarjoamaansa matkaviestinverkon puhelinpalveluun tai tekstiviestipalveluun, internetpuhelinpalveluun sekä internetyhteyspalveluun liittyvät laissa täsmennetyt tiedot. Tietojen säilytysajat on porrastettu kuuden, yhdeksän ja 12 kuukauden pituisiksi jaksoiksi palvelutyypeittäin. Kyseisen pykälän mukaan säilytettäviä tietoja saa käyttää ainoastaan pakkokeinolain (806/2011) 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi. Välitystietojen käyttötarkoituksia on lisäksi laajennettu vuonna 2019 säädetyillä siviili- ja sotilastiedustelulaeilla myös kansallisen turvallisuuden tarkoituksiin.

Arviomuistiossa käsitellään sähköisen viestinnän tietosuojadirektiivin (ePrivacy-direkiivin) sallimaa kansallista liikkumavaraa säätää välitystietojen säilyttämisesta ja käytöstä rikollisuuden torjumiseksi sekä yleisen ja kansallisen turvallisuuden varmistamiseksi. Arviomuistiossa nostetaan esiin eri vaihtoehtoja välitystietojen säilyttämiselle ja niiden myöhemmälle käytölle sen varmistamiseksi, että kansallinen sääntely täyttää sekä EU:n perusoikeuskirjan, siten kuin unionin tuomioistuin on niitä tulkinnut, että perustulain mukaiset reunaehdot. Yksi vaihtoehto varmistaa, että kansallinen lainsää-

däntö on unionin oikeuden mukaista, olisi tarvittaessa täsmentää ja muokata kansallista sääntelyä perustuslain ja unionin oikeuden mukaiseksi, huomioiden erityisesti unionin tuomioistuimen oikeuskäytäntö koskien sähköisen viestinnän tietosuojadirektiivin tulkintaa EU:n perusoikeuskirjan valossa. Toinen mahdollisuus saattaa Suomen lainsäädäntö unionin oikeuden mukaiseksi on kumota säilytysvelvollisuutta koskeva sääntely kokonaisuudessaan. Vaikka säilytysvelvollisuuden kumoaminen parantaisi yksityiselämän ja henkilötietojen suojaa sekä turvaisi luottamuksellista viestintää, säilytysvelvollisuuden kumoamista ei kuitenkaan voida pitää realistisena vaihtoehtona, sillä se voisi vaarantaa toimivaltaisten viranomaisten mahdollisuuksia saada välttämättömiä tietoja esimerkiksi rikollisuuden selvittämiseen sekä yleisen ja kansallisen turvallisuuden varmistamiseen. Mikäli välitystietoja ei säilytettäisi erikseen viranomaistarpeita varten, viranomaisten mahdollisuus saada välitystietoja riippuisi siitä, miten ja kuinka kauan teleyritykset säilyttävät välitystietoja omia tarkoituksiaan varten.

Arviomuistiossa on selvitetty lisäksi eräitä kysymyksiä ja vaihtoehtoja, jotka eivät suoraan seuraa unionin tuomioistuimen oikeuskäytännöstä, mutta jotka voisivat parantaa toimivaltaisten viranomaisten mahdollisuuksia torjua rikollisuutta. Tältä osin arviomuistiossa käsitellään mahdollisuutta ulottaa säilytysvelvollisuus myös internetin päällä tarjottavien eli over-the-top- viestintäpalveluiden tietoihin ja IP-osoitteiden säilytysvelvollisuuden laajentamiseen.

Unionin tuomioistuimen oikeuskäytäntö kehittyy edelleen, sillä tuomioistuimessa on edelleen virellä ennakkoratkaisupyyntöjä, joilla saattaa olla vaikutusta kansalliseen valmisteluun. Välitystietojen säilyttämiseen ja saatavuuteen liittyvät ongelmat ovat osin jaettuja koko unionin tasolla, ja niiden ratkaiseminen saattaa edellyttää unionin tasoisia toimia. Siten unionin tason keskustelua tietojen säilyttämisvelvollisuudesta tulee seurata jatkossa tarkasti myös kansallista sääntelyä arvioitaessa.

1. Johdanto

Velvollisuudesta säilyttää sähköisen viestinnän välitystietoja viranomaistarpeita varten säädetään sähköisen viestinnän palveluista annetun lain (SVPL, 917/2014) 157 §:ssä. Pykälässä säädetty välitystietojen säilytysvelvollisuus perustuu sähköisen viestinnän tietosuojadirektiiviin[1]. Direktiivin 15(1) artiklan nojalla jäsenvaltioiden on mahdollista rajoittaa eräiden direktiivin mukaisten oikeuksien ja velvollisuuksien soveltamista.

SVPL 157 §:n säilytysvelvollisuus on poikkeus sähköisen viestinnän tietosuojadirektiivin pääsääntöön. Direktiivin lähtökohtana on, että viestinnän välitystiedot (ns. liikenne- ja paikkatiedot) on poistettava tai tehtävä nimettömiksi, kun niitä ei enää tarvita viestinnän välittämiseen. Tämän taustalla on perusoikeuksien suojaaminen. Viestinnän luottamuksellisuus, yksityiselämän suoja, henkilötietojen suoja ja sananvapaus ovat perusoikeuksia, jotka koskettavat myös viestin sisällön lisäksi viestinnän välitystietoja.

Poikkeuksen tekeminen direktiivin lähtökohtaan on kuitenkin katsottu kansallisesti välttämättömäksi esitutkinta- ja turvallisuusviranomaisille esimerkiksi useiden rikosten selvittämiseksi, syyteharkintaan saattamiseksi ja kansallisen turvallisuuden turvaamiseksi. Tietojen säilyttämiselle on siis hyväksyttävä yleisen edun mukainen tavoite, joka palautuu viime kädessä valtion velvollisuuteen turvata oikeus elämään. Hyväksyttävän tavoitteen ohella tulee varmistaa, että rajoitukset perusoikeuksiin tehdään tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Arviointia tulee tehdä sekä EU:n perusoikeuskirjan että perustuslain näkökulmasta.

Näiden oikeuksien, erityisesti yksityiselämän ja henkilötietojen suojan tasapainottaminen yleisen edun mukaisen tavoitteen, eli rikollisuuden torjunnan ja yleisen turvallisuuden varmistamisen tavoitteen kanssa, on osoittautunut vaikeaksi. Kysymystä säilytysvelvollisuuden säätämisen perusteista, rajoista ja säilytettävien tietojen käyttötarkoituksista on vuosien varrella käsitelty useissa unionin tuomioistuimen ennakkoratkaisuissa. Säilytysvelvollisuutta koskeva kansallinen lainsäädäntö uudistettiin sähköisen viestinnän palveluista annetun lain[2] säätämisen yhteydessä.

Sen jälkeen säilytysvelvollisuutta koskevaa kansallisen lainsäädännön EU-oikeuden mukaisuutta on arvioitu kolmesti. Ensimmäinen selvitys[3] tehtiin vuonna 2017 unionin

[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, jäljempänä myös ePrivacy-direktiivi).
[2] Alun perin tietoyhteiskuntakaarena tunnetun lain nimi muutettiin lailla 68/2018 nykyiseen muotoonsa.
[3] Liikenne- ja viestintäministeriö, Selvitys sähköisen viestinnän välitystietojen säilytysvelvollisuudesta, 22.6.2017, Raportit ja selvitykset 9/2017, jatkossa LVM 9/2017. Tieto-

tuomioistuimen annettua joulukuussa 2016 ratkaisunsa ns. Tele2 ja Watson ym. -asiassa[4]. Keväällä 2021 liikenne- ja viestintäministeriössä laadittiin arviomuistio unionin tuomioistuimen kehittyneen oikeuskäytännön valossa. Silloin tarkasteltiin erityisesti Ministerio Fiscal-[5], Privacy International-[6], La Quadrature du Net-[7] ja Prokuratuur-tapauksissa[8] annettujen ennakkoratkaisuiden aiheuttamia muutostarpeita sähköisen viestinnän välitystietojen säilyttämisvelvollisuudelle ja viranomaiskäytölle.[9] Kummassakaan selvityksessä ei nähty välitöntä lainsäädännön muutostarvetta. Niissä kuitenkin tunnistettiin eräitä seikkoja, joita jatkossa olisi syytä arvioida tarkemmin. Vuoden 2017 selvityksessä nostettiin esiin säilytysvelvollisuuden soveltamiskäytäntöön liittyvä epäselvyys, jonka mukaan esitutkintaviranomaiset saavat säilytysvelvollisuuden nojalla säilytettyjä tietoja muun lainsäädännön nojalla myös rikosten estämisen tarkoituksiin. Vuoden 2021 selvityksessä puolestaan todettiin, että tietojen arkaluonteisuudesta, tietojen automaattisesta käsittelystä ja tietopyyntöjen rajaamisesta ei ole nimenomaisia säännöksiä laissa, mutta näihin liittyvät vaatimukset on mahdollista huomioida muun sääntelyn nojalla.

Kolmas selvitys laadittiin maaliskuussa 2023 jatkoselvitykseksi vuoden 2021 arviomuistiolle.[10] Kyseisessä selvityksessä arvioitiin erityisesti unionin tuomioistuimen vuonna 2022 antamia ratkaisuja tapauksissa SpaceNet ja Telekom Deutschland[11]; G. D. vastaan Commissioner of An Garda Síochána[12]; VD ja SR[13] sekä Spetsializirana

---

yhteiskuntakaaren säätämisen yhteydessä eduskunta edellytti laajapohjaisen työryhmän perustamista, ja jonka tehtävänä oli laatia kattava selvitys viranomaisten tarpeista, tietojen säilyttämisestä sekä säilyttämisen yksityisyyden suojaan liittyvistä kysymyksistä. Työn pohjalta tuli tehdä arvio kyseisen sääntelyn mahdollisista muutostarpeista. EV 106/2014 vp.

[4] 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., 21.12.2016, ECLI:EU:C:2016:970, jatkossa Tele2.

[5] Asia C-207/16, Ministerio Fiscal, 2.10.2018, ECLI:EU:C:2018:788.

[6] Asia C-623/17, Privacy International vastaan Secretary of State for Foreign and Commonwealth Affairs ym., 6.10.2020, ECLI:EU:C:2020:790, jatkossa Privacy International.

[7] Yhdistetyt asiat C-511/18, C-512/18 ja C-520/18 La Quadrature du Net ym. vastaan Premier ministre ym., 6.10.2020, ECLI:EU:C:2020:791, jatkossa QdN.

[8] Asia C-746/18 Rikosoikeudenkäynti Prokuratuur, 2.3.2021, ECLI:EU:C:2021:152.

[9] Liikenne- ja viestintäministeriö, Unionin tuomioistuimen oikeuskäytännön aiheuttamat muutostarpeet sähköisen viestinnän välitystietojen säilyttämisvelvollisuudelle ja viranomaiskäytölle, Arviomuistio, 24.3.2021, VN/7266/2021.

[10] Liikenne- ja viestintäministeriö, Jatkoselvitys Unionin oikeuskäytännön aiheuttamista muutostarpeista Suomen kansalliseen lainsäädäntöön sähköisen viestinnän välitystietojen säilyttämisvelvollisuudesta ja viranomaiskäytöstä, 29.3.2023. VN/25156/2023

[11] Yhdistetyt asiat C-793/19 ja C-794/19, Saksan liittotasavalta vastaan SpaceNet AG ja Telekom Deutschland GmbH, 20.9.2022, ECLI:EU:C:2022:702, jatkossa SpaceNet.

[12] Asia C-140/20, G. D. vastaan Commissioner of An Garda Síochána, Minister for Communications, Energy and Natural Resources ja Attorney General, 5.4.2022, ECLI:EU:C:2022:258, jatkossa G. D..

[13] Yhdistetyt asiat C-339/20 ja C-397/20 VD ja SR, 20.9.2022, ECLI:EU:C:2022:703.

prokuratura (Bulgaria)[14]. Selvityksen johtopäätöksenä on, että Suomen lainsäädännön mukainen säilyttämisvelvollisuus vastaa keskeisiltä osin SpaceNet-ratkaisussa käsiteltyä tiedon säilyttämisen laajuutta. Unionin tuomioistuin katsoi kyseisen säilyttämisen liian laajaksi, joten se ei täyttänyt sähköisen viestinnän tietosuojadirektiivin ja perusoikeuskirjan edellytyksiä.[15]

Unionin tuomioistuimen oikeuskäytäntö kehittyy edelleen. Jatkoselvityksen laatimisen jälkeen unionin tuomioistuin on antanut ratkaisunsa asiassa A. G. ja Lietuvos Respublikos generalinė prokuratūra.[16] Unionin tuomioistuimessa on myös vireillä ennakkoratkaisupyyntöjä, joilla saattaa olla vaikutusta Suomen kansalliseen välitystietojen säilyttämisvelvollisuutta käsittelevään lainsäädäntöön.[17]

Hankkeella on myös yhteys eräisiin muihin käynnissä oleviin lainsäädäntöhankkeisiin. Ensinnäkin sähköisen viestinnän tietosuojadirektiivin korvaavan asetusehdotuksen (COM/2017/010, ns. ePrivacy-asetusehdotus) neuvottelut ovat olleet käynnissä EU:n lainsäädäntömenettelyssä vuodesta 2017 alkaen. Tällä asetusehdotuksella olisi tarkoitus päivittää sähköisen viestinnän tietojen käsittelyn sääntöjä koko EU:n laajuisesti. Neuvotteluissa on ollut esillä tarve mahdollistaa myös jatkossa viestinnän tietojen käsittely kansallisella lainsäädännöllä ePrivacy-direktiivin 15 artiklan kaltaisella sääntelyllä. Vastikään hyväksytyn ns. E-evidence-sääntelyn asetuksen ((EU) 2023/1543) edellyttämää täydentävää lainsäädäntöä ja direktiivin ((EU) 2023/1544) edellyttävää täytäntöönpanoa koskevaa lainsäädäntöä valmistelevan työryhmän (OM099:00/2023) työ on käynnistynyt syksyllä 2023. Lisäksi sisäministeriössä on meneillään lainsäädäntöhanke poliisin tiedonvaihtoa koskevan sääntelyn muuttamiseksi (SM046:00/2023). Hankkeen tehtävänä on arvioida poliisilain 4 ja 7 luvun ja poliisin henkilötietolain 3 ja 4 luvun kansallista tiedonvaihtoa koskevien säännösten muutostarpeet suhteessa voimassa olevaan yleislainsäädäntöön ja poliisin nykyisen toimintaympäristön vaatimuksiin ja valmistella arvion pohjalta ehdotukset tarvittaviksi lainsäädäntömuutoksiksi.

Arviomuistiossa keskitytään rikollisuuden torjunnan, yleisen turvallisuuden ja kansallisen turvallisuuden turvaamisen tavoitteen vuoksi säädettyyn säilytysvelvollisuuteen sähköisen viestinnän tietosuojadirektiivin näkökulmasta. Siinä ei siten käsitellä esi-

[14] Asia C-350/21, Spetsializirana prokuratura (Bulgaria), 17.11.2022, ECLI:EU:C:2022:896.
[15] Vuoden 2023 jatkoselvitys, s. 17-18 ja sen liite 1.
[16] Asia C-162/22 A. G. ja Lietuvos Respublikos generalinė prokuratūra, 7.9.2023, ECLI:EU:C:2023:631, jatkossa A. G..
[17] Esim. asia C-470/21, jossa on kyse IP-osoitteiden säilyttämisen ja saannin edellytyksistä, sekä asia C-241/22, jossa on kyse viranomaisten oikeudesta saada muita kuin säilytysvelvollisuuden nojalla säilytettyjä tietoja.

merkiksi tekijänoikeusdirektiiviin liittyviä kysymyksiä tai sellaisia unionin tuomioistuimen ratkaisuissa käsiteltyjä kysymyksiä, jotka eivät välittömästi liity säilytysvelvollisuuteen[18].

Liikenne- ja viestintäministeriö on 26.10.2023 asettanut sähköisen viestinnän säilytysvelvollisuutta koskevan lainsäädännön täsmentämistä tukevan työryhmän. Työryhmässä on liikenne- ja viestintäministeriön lisäksi edustajat oikeusministeriöstä, sisäministeriöstä ja puolustusministeriössä. Työryhmän tehtävänä on kerätä tietopohja tulevan lainsäädännön muutoksen tueksi. Erityisesti työryhmän tehtävänä on selvittää unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön sekä Suomen perustuslain asettamat reunaehdot ja keinot yhteensovittaa nämä viranomaisten oikeutettujen tietotarpeiden kanssa.

Tässä arviomuistiossa arvioidaan alustavasti eri vaihtoehtoja, miten välitystietojen säilyttämistä ja viranomaisten pääsyä kyseisiin tietoihin koskeva kansallinen lainsäädäntö voitaisiin järjestää, jotta lainsäädäntö olisi Suomen perustuslain ja EU:n perusoikeuskirjan, siten kuin unionin tuomioistuin on sitä tulkinnut, mukainen. Tarkoituksena on varmistaa, että säilytysvelvollisuus ja tietoihin pääsy rajoittuu yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojan kannalta välttämättömään, turvaten kuitenkin samalla toimivaltaisille viranomaisille oikeasuhtaisen pääsyn tietoihin. Lisäksi asiassa tulee tarkastella yleisestä tietosuoja-asetuksesta[19] mahdollisesti seuraavia rajoituksia ja edellytyksiä tietojen käsittelylle. Arviomuistiossa tarkasteltuja vaihtoehtoja säilyttämisvelvollisuuden järjestämiseksi selvitettäisiin tarkemmin valmistelemalla luonnos hallituksen esitykseksi.

Arviomuistion laatimisen aikana on kuultu säilytysvelvollisia yrityksiä, tietoja hyödyntäviä viranomaisia, Liikenne- ja viestintävirasto Traficomia sekä valtiovarainministeriötä. Lisäksi arviomuistioluonnoksesta järjestettiin lausuntokierros *X.X.-X.X.2024*.

[18] Siten esimerkiksi tuomion vaikutusten ajallisten vaikutusten rajaamista ei tarkastella arviomuistiossa.
[19] Luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta annettu Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 (yleinen tietosuoja-asetus, jäljempänä myös TSA).

2. Nykytila

2.1 Säilytysvelvollisten yritysten velvollisuus säilyttää sähköisen viestinnän välitystietoja

Kansallinen säilytysvelvollisuutta koskeva lainsäädäntö uudistettiin, kun säädettiin laki sähköisen viestinnän palveluista (jäljempänä myös SVPL). Laki säädettiin perustuslakivaliokunnan myötävaikutuksella.[20] Lain 136 §:n 3 momentin mukaan muu kuin viestinnän osapuoli saa käsitellä muuta kuin yleisesti vastaanotettavaksi tarkoitettua viestintää ja sen välitystietoja ilman viestinnän osapuolen suostumusta vain, jos laissa niin säädetään. Tällainen säännös on SVPL 157 §:ssä. Mainitun pykälän mukaan sisäministeriö nimeää päätöksellään[21] teleyritykset (säilytysvelvollinen yritys), joilla on velvollisuus säilyttää tarjoamaansa matkaviestinverkon puhelinpalveluun tai tekstiviestipalveluun (jatkossa matkaviestinverkon palvelut), internetpuhelinpalveluun sekä internetyhteyspalveluun liittyvät tiedot.

SVPL 157 §:n 3 momentissa säädetään tarkemmin niistä tiedoista, jotka tulee säilyttää. Säilytettävät tiedot määritellään palvelutyypeittäin.[22] Kaikkien palvelutyyppien osalta tulee säilyttää tieto, jonka avulla voidaan yksilöidä viestintäpalvelun käyttäjä; tilaajan ja rekisteröidyn käyttäjän nimi ja osoite; liittymän tunniste sekä viestintätapahtumien tai viestintäpalvelun käytön ajankohta ja kesto. Matkaviestinverkon palveluiden sekä internetpuhelinpalvelun osalta tulee myös yksilöidä viestintätyyppi, viestinnän vastaanottaja ja viestintätapahtumat. Matkaviestinverkon palveluiden osalta säilytysvelvollisen yrityksen tulee myös säilyttää tieto viestintään käytetyn laitteen sijainnista. Säilytettäviin tietoihin sisältyy internetyhteyspalvelun osalta liittymän asennusosoite sekä matkaviestinverkon palveluiden osalta tieto viestintään käytetyn laitteen sijainnista viestinnän alkaessa. Pykälän 5 momentin mukaan säilytysvelvollisuus ei koske viestin sisältöä eikä verkkosivustojen selaamisesta kertyviä välitystietoja.

Tietojen säilytysvelvollisuuden kesto on viestintätapahtuman ajankohdasta alkaen matkaviestinverkon palveluiden osalta 12 kuukautta, internetpuhelinpalvelun osalta 9 kuukautta ja internetyhteyspalvelun osalta 6 kuukautta (SVPL 157.3 §).

---

[20] PeVL 18/2014 vp, s. 4–9.
[21] Sisäministeriön päätös SM1523258, 27.02.2015. SMDno-2014-3051.
[22] Liikenne- ja viestintävirasto voi SVPL 157 §:n 8 momentin nojalla antaa tarkentavia määräyksiä säilytettävistä tiedoista. Säilytettävistä tiedoista on määrätty 17.12.2014 annetulla Viestintäviraston määräyksellä 53 B/2014 M.

Säilytysvelvollisuutta on rajoitettu pääosin palvelutyyppien, näille eriteltyjen säilytettävien tietoluokkien ja säilytyksen ajallisen keston perusteella.[23] Periaatteessa säilytysvelvollisten yritysten määrääminen erikseen kohdentaa säilytysvelvollisuutta. Kuitenkin säilytysvelvollisten yritysten maantieteellisen kattavuuden ja huomattavan markkinaosuuden vuoksi on riski siitä, että unionin tuomioistuimen oikeuskäytännön valossa kyse ei olisi niin olennaisesta kohdentamisesta, että se täyttäisi unionioikeuden vaatimukset.[24]

Työryhmän saaman selvityksen mukaan säilytysvelvollisilla yrityksillä on tällä hetkellä toisistaan eroavia käytäntöjä siitä, miten tiedot käytännössä säilytetään. Tiedot säilytetään kunkin teleoperaattorin omissa järjestelmissä. Yritysten velvollisuudesta varmistaa tietojen korkea suojan ja turvan taso käsitellään tarkemmin myöhemmin jaksossa 5.5. Kullakin teleoperaattorilla on sopimus KRP:n kanssa tietopyyntöihin vastaamisesta, ja kaikilla säilytysvelvollisilla teleoperaattoreilla on rajapinnat pyyntöjen vastaanottamiseksi sähköisessä muodossa sekä rajapintoja vastausten toimittamiseksi määrämuotoisena esitutkintaviranomaisten omiin järjestelmiin. Esitutkinta- ja tiedusteluviranomaisilla ei siten ole suoraa pääsyä teleoperaattorien hallussa olevaan dataan, vaan tiedot toimitetaan erillisen järjestelmän kautta.

2.2 Sähköisen viestinnän välitystietojen saanti viranomaistarpeisiin

2.2.1 SVPL 157 §:n perusteella säilytettävien tietojen saanti rikosten selvittämiseksi

SVPL 157 §:ssä säädetään edellä kuvatulla tavalla tietojen säilytysvelvollisuudesta. Tämän lisäksi pykälässä säädetään niistä tarkoituksista, joita varten viranomaiset voi-

[23] Vastaavasti LVM 9/2017, s. 22.
[24] Säilytysvelvollisia yrityksiä Suomessa ovat 27.2.2015 annetun päätöksen mukaan DNA Oyj, Elisa Oyj, Telia Finland Oyj ja Ålands Telekommunikation Ab. Sisäministeriön päätöksen perusteluiden mukaan nimetyt yritykset on valittu merkittävän yhteenlasketun markkinaosuuden sekä maantieteellisen kattavuuden perusteella. Unionin tuomioistuimen tuoreen oikeuskäytännön merkitystä kansallisen lainsäädännön kannalta on arvioitu yksityiskohtaisemmin vuoden 2023 jatkoselvityksessä. Nykytilan arvioinnista ks. tarkemmin tämän arviomuistion 6.2 jakso.

vat käyttää tietoja. Mainitun pykälän mukaan säilytettäviä tietoja saa käyttää ainoastaan pakkokeinolain (806/2011) 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi.[25]

Tietojensaantioikeudesta säädetään puolestaan muualla laissa. SVPL 322 §:n mukaan viranomaisten oikeudesta saada välitystietoja rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi säädetään poliisilaissa, rikostorjunnasta Rajavartiolaitoksessa annetussa laissa (108/2018), henkilötietojen käsittelystä Rajavartiolaitoksessa annetussa laissa (639/2019), rikostorjunnasta Tullissa annetussa laissa (623/2015), henkilötietojen käsittelystä Tullissa annetussa laissa (650/2019) ja pakkokeinolaissa. Pykälän 2 momentin mukaan viranomaistarkoituksia varten SVPL 157 §:n perusteella säilytettäviä tietoja voivat saada säilytysvelvollisilta yrityksiltä ainoastaan ne viranomaiset, joilla on lain perusteella oikeus saada tiedot.[26]

SVPL 157 §:n mukaisen säilytysvelvollisuuden alaan kuuluvien sähköisen viestinnän välitystietojen saanti tapahtuu esitutkinnassa, siviilitiedustelussa sekä sotilastiedustelussa (takautuvan) televalvonnan avulla. Kaikki esitutkintalain (805/2011) mukaiset esitutkintaviranomaiset eli poliisi[27], Tulli, Rajavartiolaitos ja puolustusvoimat voivat tietyissä tilanteissa saada esitutkinnassa tutkittavana olevien rikosten selvittämiseksi ja syyteharkintaan saattamiseksi SVPL 157 §:n perusteella säilytettäviä tietoja, sillä kunkin esitutkintaviranomaisen vastuulla on ainakin joidenkin sellaisten rikosten esitutkinta, jotka täyttävät PKL 10:6.2:n edellytykset. Lisäksi viranomaiskohtaisissa laeissa säädetään salaisten tiedonhankintakeinojen käytöstä rikosten rikoksen estämiseen, paljastamiseen tai vaaran torjumiseen.

Rikoksen selvittämiseen käytettävistä salaisista pakkokeinoista säädetään kattavasti pakkokeinolain 10 luvussa. Rikoksen estämiseen, paljastamiseen ja vaaran torjumiseen käytettävistä salaisista tiedonhankintakeinoista säädetään pakkokeinolain kanssa mahdollisimman yhteneväisesti poliisilain 5 luvussa. Koska salaisten pakkokeinojen käytöstä säädetään yhdenmukaisesti eri esitutkintaviranomaisia koskevissa laeissa, seuraavaksi kuvataan vain pakkokeinolain ja poliisilain sääntelyä.

---

[25] Ks. kuitenkin 2.2.2 jakso tiedustelutoiminnan lisäämisestä tarkoituksiin, joita varten tietoja voi saada. Lisäksi on syytä ottaa huomioon, että teleyritykset säilyttävät viestinnän välitystietoja jonkin aikaan myös omia tarkoituksiansa varten (esimerkiksi edellisen kuukauden tiedot liittymän käytön laskutusta varten). SVPL 157 § säädetyt rajaukset eivät sovellu silloin, kun poliisi pyytää teleyrityksen omia tarpeita varten säilyttämiään tietoja esimerkiksi poliisilain 4:3.1 ja 4:3.2 nojalla.

[26] Tämän on oikeuskäytännössä katsottu estävän tietojen luovuttamisen tekijänoikeuslain 60 a §:n nojalla (KKO:2017:85). Tekijänoikeusdirektiiviin liittyvien kysymysten osalta ks. asia C-597/19 Mircom International Content Management & Consulting (M.I.C.M.) Limited vastaan Telenet BVBA ym. (17.6.2021, ECLI:EU:C:2021:492).

[27] Lukuun ottamatta suojelupoliisia.

Pakkokeinolain 1 luvussa säädetään pakkokeinojen käyttöä koskevista yleisistä rajoitusperiaatteista. Esimerkiksi suhteellisuusperiaatteen mukaan pakkokeinoja saadaan käyttää vain, jos pakkokeinon käyttöä voidaan pitää puolustettavana ottaen huomioon tutkittavana olevan rikoksen törkeys, rikoksen selvittämisen tärkeys sekä rikoksesta epäillylle tai muille pakkokeinon käytöstä aiheutuva oikeuksien loukkaaminen ja muut asiaan vaikuttavat seikat. Vähimmän haitan periaatteen mukaan pakkokeinon käytöllä ei kenenkään oikeuksiin saa puuttua enempää kuin on välttämätöntä käytön tarkoituksen saavuttamiseksi, ja pakkokeinon käytöllä ei saa aiheuttaa kenellekään tarpeettomasti vahinkoa tai haittaa. Lisäksi hienotunteisuusperiaatteen mukaan pakkokeinoja käytettäessä on vältettävä aiheettoman huomion herättämistä ja toimittava muutenkin hienotunteisesti.

Lisäksi on tarpeen ottaa huomioon, että pakkokeinon käytön sitominen tietyn vakavuustason rikokseen liittyy edellä mainittuun pakkokeinolain 1 luvun 2 §:ssä ilmaistuun suhteellisuusperiaatteeseen, jonka keskeisenä sisältönä on oikeasuhtaisuus käytettävän pakkokeinon ja selvitettävänä olevan rikoksen vakavuuden välillä. Suhteellisuusperiaate on otettava huomioon paitsi pakkokeinoa konkreettisessa tilanteessa käytettäessä, myös jo arvioitaessa tarvetta lainsäädännöllä mahdollistaa pakkokeinon käyttö tietyn rikoksen selvittämisessä. Vaikka rikoksen rangaistusasteikko sellaisenaan mahdollistaisi pakkokeinon käytön tietyssä tapauksessa, erityisesti rikoksen lievempien ilmenemismuotojen osalta tilanne on konkreettisessa soveltamistilanteessa vielä lisäksi arvioitava suhteellisuusperiaatteen valossa.[28]

Poliisilain 1 luvussa säädetään niin ikään suhteellisuusperiaatteesta sekä vähimmän haitan periaatteesta.

Edelleen pakkokeinolain 10 luvun 2 §:ssä säädetään salaisten pakkokeinojen käytön edellytyksistä. Kaikkien salaisten pakkokeinojen käytön yleisenä perusedellytyksenä on, että niillä voidaan olettaa saatavan rikoksen selvittämiseksi tarvittavia tietoja (PKL 10:2.1). Sääntely on kolmiportainen ottaen huomioon viimeksi mainittu tuloksellisuusodotus, mutta osassa keinoja käytön edellytyksenä on lisäksi erittäin tärkeä merkitys rikoksen selvittämiselle ja muutaman keinon osalta edellytetään jo mainittujen lisäksi myös välttämättömyyttä.[29] Tämä ei kuitenkaan ole vaatimus kaikissa tilanteissa. Esimerkiksi jäljempänä selostettavan televalvonnan (PKL 10:6) osalta sen käytön edellytyksenä ei pakkokeinolain (PKL10:2.2) mukaan ole, että sen käyttämiselle olisi erittäin tärkeä merkitys rikoksen selvittämiseksi tai että keinon käytön tulee olla välttämätöntä rikoksen selvittämiseksi.

[28] HE 217/2022 vp, s. 9.
[29] Esitutkinta ja pakkokeinot (Fredman, Kanerva, Tolvanen, Viitanen, 2020) s. 1068-1069.

Salaisten tiedonhankintakeinojen käytön edellytyksistä säädetään vastaavasti poliisilain 5:2:ssa.

PKL 10:6.1:n ja poliisilain 5:8.1:n mukaan televalvonnalla hankittavat tiedot koskevat joko televalvonnan kohteena olevaan teleosoitteeseen tai telepäätelaitteeseen lähetettyyn tai vastaanotettuun viestiin liittyviä viestinnän välittäjän hallussa olevia välitystietoja taikka teleosoitteen tai telepäätelaitteen sijaintitietoa.[30] Televalvontaa koskevaa sääntelyä on uudistettu lokakuussa 2023 voimaan tulleella muutoksella.[31] Lailla on muutettu televalvonnalla hankittavien tietojen määritelmää, mutta tällä ei ole tarkoitus muuttaa televalvonnan käyttöalaa.[32] Edellä mainituissa televalvontaa koskevissa lainkohdissa ei nimenomaisesti säädetä pääsystä juuri SVPL 157 §:n perusteella säilytettäviin tietoihin.

Televalvonnan käytöstä esitutkinnassa päättää tuomioistuin pidättämiseen oikeutetun virkamiehen vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu virkamies saa päättää televalvonnasta ja sijaintitietojen hankkimisesta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään vuorokauden aikana. Jos tuomioistuin ei tällaisessa tilanteessa anna lupaa televalvontaan, kiireellisessä tilanteessa saatu tieto on heti hävitettävä. (PKL 10 luku 9 § ja 58 §)

Vastaavasti myös poliisilain 5 luvun 10 §:n mukaan tuomioistuin päättää 8 §:n 2 ja 5 momentissa sekä 9 §:n 1 ja 4–6 kohdassa tarkoitetusta televalvonnasta sekä televalvonnasta 3 §:ssä tarkoitetuissa tapauksissa pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Samoin kiireellisissä asioissa pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies saa päättää televalvonnasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen.

[30] Rikostorjunnasta Tullissa annetun lain 3 luvun 4 §:n 1 momentissa sekä rikostorjunnasta Rajavartiolaitoksessa annetun lain 16 §:ssä säädetään myös televalvonnasta. Lainkohdat vastaavat pitkälti esimerkiksi edellä mainitussa poliisilain lainkohdassa aiemmin käytettyä ilmaisua. Sen sijaan laissa sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa (255/2014) ei säädetä oikeudesta televalvontaan.
[31] Pakkokeinolain osalta HE 217/2022 vp ja EV 305/2022 vp, poliisilain osalta HE 275/2022 vp ja EV 316/2022 vp sekä Rajavartiolaitoksen rikostorjuntalain salaisia tiedonhankintakeinoja koskevaan 3 lukuun on tehty osin samanlaiset muutokset HE 7/2023 vp ja EV 9/2023 vp. Käynnissä on myös vastaava muutostyö Tullin osalta lakiin rikostorjunnasta Tullissa.
[32] Poliisilain 5 luvun 8 §:n 1 momentin osalta ks. HE 275/2022 vp, s. 35. PKL 10 luvun 6 §:n 1 momentin osalta ks. HE 217/2022 vp, s. 123.

Pakkokeinolain 10 luvun 9 §:n 3 momentin ja poliisilain 5 luvun 10 §:n 5 momentin mukaan televalvonnasta voidaan päättää myös takautuvasti.[33] Säännöksen mukaan televalvontaa koskeva lupa tai päätös voi koskea myös luvan antamista tai päätöksen tekemistä edeltävää määrättyä aikaa, joka voi olla kuukautta pidempi. Takautuvaa lupaa tai päätöstä televalvonnasta ei ole rajoitettu ajalliselta ulottuvuudeltaan laissa. Takaraja tulee kuitenkin siitä, miltä ajalta säilytysvelvollisella yrityksellä on tallennettuja kyseisiä tietoja.

Pakkokeinolain 10 luvun 9 §:ssä ja poliisilain 5 luvun 10 §:ssä säädetään televalvontaa koskevan vaatimuksen ja päätöksen sisällöstä. Siinä ei erikseen vaadita rajaamaan niitä viestinnän välitystietoja, joihin tietopyyntö kohdistuu, mutta vaatimuksessa on esitettävä mahdolliset televalvonnan rajoitukset. Pakkokeinolakiin ja poliisilakiin lokakuussa 2023 voimaan tulleen muutoksen myötä vaatimuksessa ja tuomioistuimen päätöksessä ei enää eritellä toimenpiteen kohteena olevan teleosoitetta ja telepäätelaitetta, vaan jatkossa lupa myönnettäisiin henkilösidonnaisesti. Epäillyn ollessa tuntematon kohdistetaan lupa yhä teleosoite- ja telepäätelaitekohtaisesti. Vaikka muutoksen jälkeen tuomioistuimen päätöksessä ei yksilöidä valvonnan kohteena olevia telepäätelaitteita tai teleosoitteita, tulee televalvonnasta päättävän pidättämiseen oikeutetun virkamiehen kuitenkin tehdä perusteltu päätös televalvonnan kohdentamisesta tiettyihin telepäätelaitteisiin tai teleosoitteisiin. (PKL 10:9.5; poliisilaki 5:10)

Pakkokeinolain 10 luvun 50 §:n mukaan salaisten pakkokeinojen käytössä noudatetaan, mitä lain 8 luvun 23–26 §:ssä säädetään tietojärjestelmän haltijan tietojenantovelvollisuudesta ja datan säilyttämismääräyksestä. Pakkokeinolain 8 luvun 24 §:n mukaan pidättämiseen oikeutettu virkamies voi antaa datan säilyttämismääräyksen, jolla määrätään dataa hallussaan tai määräysvallassaan pitävä säilyttämään se muuttumattomana. Määräyksestä on pyynnöstä annettava kirjallinen todistus, jossa yksilöidään määräyksen kohteena oleva data. Se voi koskea myös dataa, jonka voidaan olettaa tulevan laitteeseen tai tietojärjestelmään määräyksen antamista seuraavan kuukauden aikana. Säilyttämismääräys annetaan kolmeksi kuukaudeksi kerrallaan, mutta se voidaan uusia ja se tulee kumota niin pian kuin se ei enää ole tarpeen. (PKL 8:25 §)

Nykykäytännössä on havaittu tulkintaerimielisyys säilytysvelvollisuuden alaisten tietojen käytössä rikosten ennaltaehkäisemisen osalta.[34] Sähköisen viestinnän palveluista annetun lain 157 §:n mukaan säilytettäviä tietoja saa käyttää *ainoastaan* pakkokeino-

[33] Lokakuussa voimaan tulleilla pakkokeinolain ja poliisilain kyseisiin lainkohtiin tehdyillä muutoksilla täsmennettiin lain sanamuotoa siten, ettei lupaa voida myöntää tulemaan voimaan myöhempänä ajankohtana. HE 275/2022 vp, s. 25 ja HE 217/2022 vp, s. 122 ja 125.
[34] Ks. myös LVM 9/2017, s. 24 ja siihen jätetyt eriävät mielipiteet.

lain 10 luvun 6 §:n 2 momentissa tarkoitettujen *rikosten selvittämiseksi* ja *syyteharkintaan asettamiseksi*. Tämän lisäksi tietoja kuitenkin käytetään myös rikosten ennalta ehkäisemisen tarkoitusta varten muun lainsäädännön, kuten poliisilain perusteella.

Tulkitaerimielisyyden on esitetty juontuvan SVPL 157 §:n ja 322 §:n keskinäisestä viittaussuhteesta. SVPL 157 §:n säätämisen yhteydessä tietojen käyttötarkoituksista, joiden mainitsemista lain tasolla perustuslakivaliokunta on aiemmin edellyttänyt, on jätetty pois maininta tietojen käytöstä rikosten tutkimiseksi. Asiaa ei kuitenkaan ole valmisteluasiakirjoissa avattu. Voimassa olevan lain sanamuodon mukaan tietojen käyttö on siis rajattu ainoastaan tiettyjen rikosten selvittämiseksi ja syyteharkintaan asettamiseksi. Vuoden 2017 selvityksessä kävi ilmi, että tietoyhteiskuntakaaren (nyk. laki sähköisen viestinnän palveluista) 157 §:ää on käytännössä tulkittu koskevan myös rikosten estämistä. Tämä perustuu SVPL 322 §:n 1 momentin sanamuotoon, jossa mainitaan myös rikosten estäminen. Työryhmässä esitetyn selvityksen perusteella säilytysvelvollisuuden alaisia tietoja hyödynnetään rikosten ennaltaehkäisemisessä muun lainsäädännön, kuten poliisilain perusteella.[35]

Tältä osin on huomattava, että ePrivacy-direktiivin 15 artikla sanamuodon mukaan sallisi tietojen käytön kansallista lainsäädäntöä laajemminkin, sillä sen mukaan sallittua olisivat rajoitukset, jotka ovat välttämättömiä, asianmukaisia ja oikeasuhtaisia rikosten torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi. Direktiivin ohella asiaa olisi arvioitava myös perustuslain näkökulmasta. Perustuslain 10 §:n 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana.

2.2.2 SVPL 157 §:n perusteella säilytettävien tietojen saanti kansallisen turvallisuuden suojaamiseksi ja maanpuolustuksen turvaamiseen

SVPL 157 §:n perusteella säilytettävien välitystietojen käyttötarkoitus on vuonna 2019 säädetyillä siviili- ja sotilastiedustelulaeilla laajennettu kansallisen turvallisuuden tarkoituksiin. Säilytettävien tietojen käyttämisestä kansallisen turvallisuuden perusteella

[35] LVM 9/2017, s. 16. SVPL:n 157 §:n ja 322 §:n keskinäisen suhteen tulkintaepäselvyydestä ks. sisäministeriön eriävä mielipide (SMDno-2017-1066), jonka se jätti kyseiseen selvitykseen.

säädetään poliisilain 5 a luvussa ja sotilastiedustelusta annetussa laissa (SotTiedL, 590/2019).[36]

Edellytyksistä tietojen saannille on säädetty pitkälti samoin kuin pakkokeinolaissa. Tuomioistuin päättää televalvonnasta sotilastiedustelussa tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen sotilaslakimiehen tai muun virkamiehen vaatimuksesta ja siviilitiedustelussa suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos televalvontaa koskeva asia ei siedä viivytystä, em. vaatimuksen esittävä virkamies saa päättää televalvonnasta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Siviilitiedustelussa tästä kuitenkin päättää suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta. Jos tuomioistuin ei tällaisessa tilanteessa anna lupaa televalvontaan, kiireellisessä tilanteessa saatu tieto on heti hävitettävä.[37] Lupa tai päätös voidaan antaa myös takautuvasti koskien luvan antamista tai päätöksen tekemistä edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.[38] Takautuvaa lupaa tai päätöstä televalvonnasta ei ole rajoitettu ajalliselta ulottuvuudeltaan laissa.

Tiedustelulaeissa on säädetty nimenomaisesti välttämättömyysedellytyksestä. Poliisilain 5 a luvun 4 §:n 1 momentin mukaan tiedustelumenetelmän[39] käytön yleisenä edellytyksenä siviilitiedustelussa on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Sotilastiedustelusta annetun lain 12 §:n 1 momentin mukaan televalvonnan käyttämisen sotilastiedustelussa tulee täyttää tiedustelumenetelmän käytön yleisenä edellytyksenä oleva välttämättömyyden kriteeri.[40] Tämän lisäksi lupa muun kuin valtiollisen toimijan hallussa olevaan tai hänen muuten käyttämän teleosoitteen tai telepäätelaitteen televalvontaan voidaan kuitenkin myöntää vain, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi tiedustelutehtävän kannalta (37.3 §).

SVPL 157 §:n perusteella säilytettäviä tietoja saa käyttää poliisilain 5 a luvun 53 §:n mukaan siviilitiedustelussa, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Sotilastiedustelussa taas

[36] Tässä yhteydessä huomioon otettavaa on, että tietoliikennetiedustelu jää SVPL 157 §:n rajoitusten ulkopuolelle, sillä tietoliikennetiedustelussa ei aseteta teleyrityksiin kohdistuvaa tallennusvaatimusta (ks. QdN kohdat 101–103).
[37] Poliisilaki 5 a luku 7 § ja 46 §; SotTiedL 38 ja 87 §.
[38] Poliisilaki 5 a luku 7 §; SotTiedL 38 §.
[39] Kuten televalvonta, tukiasematietojen ja teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen (Poliisilaki 5 a:2.1).
[40] Tämä koskee tiedustelumenetelmän käyttöä muuhun kuin valtiolliseen toimijaan.

näitä tietoja voidaan käyttää sotilastiedustelusta annetun lain 103 §:n mukaan tietojen hankkimiseksi sotilastiedustelun kohteena olevasta lain 4 §:ssä tarkoitetusta toiminnasta.

Tiedustelutoimintaan kohdistuu erikseen säädetty hallinnonalan sisäinen valvonta (poliisilaki 5 a luvun 59 §; SotTiedL 105 § ja 106 §). Tiedustelun asianmukaisuutta valvoo uusi viranomainen, tiedusteluvalvontavaltuutettu, ja tiedusteluun kohdistuu myös parlamentaarinen valvonta (laki tiedustelutoiminnan valvonnasta). Tiedusteluvalvontavaltuutetulle on tehtävä ilmoitus tiedustelumenetelmien käytöstä (poliisilaki 5 a:61; SotTiedL 108 §).

Sähköisen viestinnän tietosuojadirektiivissä kansallinen turvallisuus (valtion turvallisuus) ja puolustus ovat niin ikään mainittu 15 artiklan 1 kohdassa. Tältäkin osin on otettava huomioon myös perustuslaki. Perustuslain 10 §:n 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

2.2.3 Tietojen saanti teleyrityksen omia tarkoituksia varten säilyttämistä tiedoista

Poliisilla on oikeus saada välitystietoja rikosten ennalta estämiseksi, paljastamiseksi, selvittämiseksi, vaaran torjumiseksi sekä eräissä poliisitutkinnoissa, kuten kuolemansyyn selvittämisessä, kadonneen henkilön etsinnässä tai liiketoimintakiellon määräämistä tai pidentämistä koskevassa tutkinnassa.[41] Televalvonta tai tiedonsaantipyyntö voi siten kohdistua myös muihin kuin säilytysvelvollisuuden nojalla säilytettyihin tietoihin eli tietoihin, joita viestinnän välittäjä käsittelee jonkin toisen perusteen nojalla.

Esitutkintaviranomaisilla voi olla tarve tunnistaa käyttäjä ennen televalvonnan käyttämistä. Tällaisia tunnistamispyyntöjä tehdään poliisilain 4:3.1 ja 4:3.2 nojalla (ks. myös jakso 5.1.3).[42] Poliisilain 4:3.1 mukaan poliisilla on päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada rikoksen estämiseksi tai selvittämiseksi tarvittavia tietoja yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä. Poliisilla on sama oikeus saada 6 luvussa tarkoitetussa poliisitutkinnassa tarvittavia tietoja, jos tärkeä yleinen tai yksityinen etu sitä vaatii. Poliisilain 4:3.2 mukaan poliisilla on yksittäistapauksessa

[41] Ks. vastaavasti LVM 9/2017, s. 15.
[42] Vastaavasti laki sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa 44 ja 93 §, laki henkilötietojen käsittelystä Rajavartiolaitoksessa 20 §, laki sotilastiedustelusta 104 § ja laki rikostorjunnasta Tullissa 14 §.

oikeus pyynnöstä saada teleyritykseltä ja yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi. Poliisilla on vastaava oikeus saada postitoimintaa harjoittavalta yhteisöltä jakeluosoitetietoja.

Kyseinen pykälä vastaa pakkokeinolain 10:25 §:n mukaista teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimista. Yksilöintiin tarvittavat tiedot hankittaisiin nimenomaan sen takia, että niiden perusteella voitaisiin hankkia tuomioistuimelta lupa televalvontaan tai telekuunteluun.[43]

Poliisilain 4.3:1 ja 4.3.2 mukaiset pyynnöt kohdistuvat teleyrityksen asiakastietoihin tai sen omia tarkoituksia varten säilyttämiin tietoihin. Käyttäjän tunnistamiseksi tarvittavat tiedot ovat usein välttämättömiä telepakkokeinojen kohdistamiseksi tiettyyn henkilöön. Tietopyyntöä ei voida kohdistaa säilytysvelvollisuuden alaisiin tietoihin, ellei tutkittavana oleva rikos täytä televalvonnan edellytyksiä. Säilytysvelvollisuuden alaisiin tietoihin tehtäviä hakuja rajoittaa sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentti, jossa viitataan pakkokeinolain 10 luvun 6 §:n 2 momentissa tarkoitettuihin rikoksiin. Tilanteessa, jossa tietopyyntöä ei voida kohdistaa säilytysvelvollisuuden alaisiin tietoihin, pyyntö kohdistetaan tietoihin, joita teleyritys käsittelee jonkin toisen perusteen nojalla.

Unionin tuomioistuin ei ole asettanut erityisiä rajoituksia käyttäjän henkilöllisyyttä koskevien tietojen säilyttämiseen. Niitä voi käyttää rikosten torjuntaa, tutkintaa, selvittämistä ja syyteharkintaa sekä yleisen turvallisuuden takaamista varten. (QdN 157–159 kohta.) Unionin tuomioistuimessa on kuitenkin vireillä ennakkoratkaisupyyntö asiassa C-241/22 DX, jossa käsiteltävänä on kysymys siitä viranomaisten oikeudesta saada liikenne- ja paikkatietoja muun perusteen kuin tietojen säilytysvelvollisuuden nojalla teleyrityksen käsittelemiin tietoihin. Oikeustila saattaa vielä tältä osin siis kehittyä.

2.3 Säilytettävien tietojen suojaaminen

Sähköisen viestinnän tietosuojadirektiivin 4 artiklan 1 kohdassa sekä 4 artiklan 1 a kohdassa edellytetään, että palveluntarjoajat toteuttavat asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa säilytettyjen tietojen tehokas suoja väärinkäytön vaaraa vastaan sekä näiden tietojen kaikenlaista laitonta saantia vastaan. Unionin tuomioistuin on tulkinnut näitä vaatimuksia.[44] Kun otetaan huomioon

[43] HE 224/2020 vp; HE 266/2004 vp.
[44] On kuitenkin huomattava, että kansallisessa lainsäädännössä asetetuilla takeilla, joilla säilytettyjä tietoja pyritään suojaamaan väärinkäytöltä ja lainvastaiselta saannilta,

säilytettyjen tietojen määrä, niiden arkaluonteisuus sekä niiden lainvastaista saantia koskeva vaara, sähköisten viestintäpalvelujen tarjoajien on mainittujen tietojen täyden koskemattomuuden ja luottamuksellisuuden takaamiseksi varmistettava erityisen korkea suojan ja turvan taso turvautumalla asianmukaisiin teknisiin ja organisatorisiin toimiin. Kansallisessa säännöstössä on erityisesti säädettävä tietojen säilyttämisestä unionin alueella ja tietojen lopullisesta hävittämisestä, kun niiden säilyttämisaika päättyy.[45]

Lisäksi sähköisen viestinnän tietosuojadirektiivin 4 artiklan mukaan näillä toimenpiteillä on vähintään varmistettava, että henkilötietoja pääsee käsittelemään vain siihen luvan saanut henkilöstö oikeudellisesti perustelluissa tapauksissa, suojattava tallennetut tai siirretyt henkilötiedot tahattomalta tai laittomalta tuhoamiselta, tahattomalta kadottamiselta tai muuttamiselta taikka luvattomalta tai laittomalta säilyttämiseltä, käsittelyltä, käytöltä tai luovuttamiselta, ja varmistettava henkilötietojen käsittelyä koskevan turvapolitiikan toteuttaminen.

Kyseinen 4 artikla on toimeenpantu kansallisesti sähköisen viestinnän palveluista annetun lain 247 §:llä, jonka mukaan viestinnän välittäjän on huolehdittava palvelujensa, viestien, välitystietojen ja sijaintitietojen tietoturvasta.[46] Toimenpiteet, joilla huolehditaan tietoturvasta, on suhteutettava uhan vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Säilytysvelvollinen yritys päättää tietojen säilyttämisen teknisestä toteuttamisesta. Tiedot on säilytettävä kustannustehokkaasti. Lisäksi on otettava huomioon säilytysvelvollisen yrityksen liiketoiminnan tarpeet ja järjestelmien tekniset ominaispiirteet sekä maksuvelvollisen viranomaisen tarpeet.[47]

Sähköisen viestinnän palveluista annetun lain 158 §:n 3 momentin mukaan säilytysvelvollisen yrityksen on nimettävä henkilöt, joilla on oikeus käsitellä säilytettäviä tietoja tai tehtävät, joissa niitä saa käsitellä. Säilytysvelvollisen yrityksen on huolehdittava, että tilaajan saatavilla on tietoa tietojen säilyttämisestä ja sen tarkoituksesta. Säilytysvelvollisuuden teknisen toteutuksen ja tietoturvallisuuden vaatimusta on tarkennettu

ei voida rajoittaa tai korjata säilyttämisestä johtuvaa vakavaa puuttumista käyttäjän perusoikeuksiin. SpaceNet kohta 91; G. D. kohta 47.
[45] Tele2 kohta 122. Ks. analogisesti kumotun direktiivin 2006/24 osalta tuomio asiassa Digital Rights Ireland, kohta 66–68.
[46] HE 221/2013 vp, s. 189.
[47] Sähköisen viestinnän palveluista annettu laki 158 § 1 mom.

sähköisen viestinnän palveluista annetun lain 158 §:n 6 momentin nojalla annetussa viestintäviraston määräyksessä.[48]

SVPL:ssä ei ole nimenomaisesti säädetty SVPL 157 §:n nojalla säilytettyjen tietojen erityisen korkeasta suojan ja turvan tasosta eikä tietojen poistamisesta. Siinä ei myöskään nimenomaisesti säädetä vaatimusta säilyttää tietoja unionin alueella. Työryhmän saaman selvityksen mukaan tällä hetkellä kaikkien säilytysvelvollisten yritysten tietokannat sijaitsevat Suomessa. SVPL 158 §:n 2 momentin mukaista säilytysvelvollisuuden piiriin kuuluvien tietojen käsittelyä varten perustetun järjestelmän käyttöä koskevassa sopimuksessa edellytetään, että säilytysvelvollisen yrityksen tulee varmistaa, mikäli tietosisältöä tallennetaan ulkomailla sijaitseviin järjestelmiin, että itse tietosisältö on vain suomalaisten turvallisuusmääräysten mukaisesti tarkastettujen henkilöiden käytettävissä. Vuoden 2021 arviomuistion laatimisen yhteydessä saatujen tietojen mukaan tietojen suojan ja turvan taso olisi erityisen korkea ja tiedot poistettaisiin säilytysajan päätyttyä. Kyseiset vaatimukset eivät kuitenkaan nimenomaisesti käy nykyisellään ilmi laista.

[48] Määräys teleyritysten tietojen säilytysvelvollisuudesta viranomaistarpeita varten, 53 B/2014 M 17.12.2014. Sen mukaan säilytysvelvollisen yrityksen on suojattava säilytysvelvollisuuden piiriin kuuluvat tiedot oikeudettomalta käsittelyltä sekä säilytyksen aikana että niitä viranomaiselle siirrettäessä. Säilytysvelvollisen yrityksen on tarkistettava asianmukaisesti viranomaiselta tulevan, säilytysvelvollisuuden piiriin kuuluviin tietoihin kohdistuvan tietopyynnön laillisen perusteen olemassaolo. Säilytysvelvollisen yrityksen on tallennettava viranomaiselta tulevan, säilytysvelvollisuuden piiriin kuuluviin tietoihin kohdistuvan tietopyynnön toteuttamisesta 2 vuodeksi tiedot siitä, mitä tietoja on haettu ja mitkä tiedot on luovutettu, tietojen hakemisen ajankohta, tietojen hakija sekä tietojen hakemisen laillinen peruste.

3. EU-oikeuden ja valtiosääntöiset reunaehdot

3.1 Perus- ja ihmisoikeuksista seuraavien vaatimusten huomioiminen

Sähköisen viestinnän välitystietojen säilytyksessä on kyse perus- ja ihmisoikeuksien rajoituksesta. Viestinnän luottamuksellisuus, yksityiselämän suoja, henkilötietojen suoja ja sananvapaus ovat perusoikeuksia, jotka koskettavat myös viestin sisällön lisäksi viestinnän välitystietoja. Näiden tietojen säilyttämiseen liittyviä velvoitteita on arvioitu unionin tuomioistuimen oikeuskäytännössä erityisesti perusoikeuskirjan 7, 8 ja 11 artikloiden sekä 52 artiklan valossa. Siten unionin oikeudesta seuraa rajoituksia siihen, miten tietojen säilytysvelvollisuudesta tai niiden käytöstä voidaan kansallisesti säätää. Samoin myös Euroopan ihmisoikeussopimuksen 8 artiklasta seuraa rajoituksia sille, miten asiasta voidaan säätää. Euroopan ihmisoikeustuomioistuin on oikeuskäynnössään arvioinut tästä artiklasta seuraavia rajoituksia suhteessa teleyrityksiin kohdistuvaan säilytysvelvollisuuteen. Lisäksi kansallisesti asiaa on arvioitu perustuslakivaliokunnan lausuntokäytännössä.

Tässä arviomuistiossa esitellään eri vaihtoehtoja, miten välitystietojen säilyttämistä ja viranomaisten pääsyä kyseisiin tietoihin koskeva kansallinen lainsäädäntö voitaisiin järjestää, jotta lainsäädäntö olisi Suomen perustuslain ja EU:n perusoikeuskirjan, siten kuin unionin tuomioistuin sitä oikeuskäytännössään on tulkinnut, mukainen, rajoittuu yksityiselämän, henkilötietojen ja viestinnän luottamuksellisuuden suojan kannalta välttämättömään ja samalla turvaa viranomaisille oikeutetun ja oikeasuhtaisen pääsyn tietoihin tehokkaan rikostorjunnan varmistamiseksi. Tarkasteluun vaikuttaa siis vahvasti unionin tuomioistuimen oikeuskäytäntö, josta seuraa rajoituksia kansalliselle lainsäädännölle.

Keskeiset reunaehdot sähköisen viestinnän välitystietojen säilyttämisestä tulevat unionin tuomioistuimen oikeuskäytännöstä. Ne muodostavat myös keskeiset perusoikeudelliset reunaehdot, sillä unionin tuomioistuin on tulkinnut sähköisen viestinnän tietojen käsittelyä EU:n perusoikeuskirjan 7 (yksityis- ja perhe-elämän kunnioittaminen), 8 (henkilötietojen suoja), 11 (sananvapaus ja tiedonvälityksen vapaus) ja 52(1) (oikeuksien ja periaatteiden ulottuvuus ja tulkinta) artiklan valossa. Tämän lisäksi tulee kuitenkin arvioida, tuleeko muista perusoikeuskirjan määräyksistä, Suomen perustuslaista, Euroopan ihmisoikeussopimuksesta tai kansalais- ja poliittisten oikeuksien sopimuksesta (jäljempänä KP-sopimus) muita perus- ja ihmisoikeudellisia reunaehtoja.

3.2 Perusoikeuskirjan, ihmisoikeusvelvoitteiden ja perustuslain reunaehdot

3.2.1 Perusoikeuskirja

Perusoikeuskirjan määräysten osalta on otettava huomioon niiden soveltamisala. Perusoikeuskirjan 51(1) artiklan mukaan perusoikeuskirjan määräykset koskevat unionin toimielimiä, elimiä ja laitoksia toissijaisuusperiaatteen mukaisesti sekä jäsenvaltioita ainoastaan silloin, kun viimeksi mainitut soveltavat unionin oikeutta. Tämän vuoksi ne kunnioittavat tämän perusoikeuskirjan mukaisia oikeuksia, noudattavat sen sisältämiä periaatteita ja edistävät niiden soveltamista kukin toimivaltansa mukaisesti ja unionille perussopimuksissa annetun toimivallan rajoja noudattaen.

Unionin tuomioistuin on tulkinnut EU-oikeuden soveltamisalaa säilytysvelvollisuuden kontekstissa erityisesti QdN-ratkaisussaan. Unionin tuomioistuimen mukaan kansallinen säännöstö, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on säilytettävä liikenne- ja paikkatiedot kansallisen turvallisuuden suojaamiseksi ja rikollisuuden torjumiseksi, kuuluu direktiivin 2002/58 soveltamisalaan. (QdN kohdat 100-104 ja Lietuvos Respublikos generalinė prokuratūra kohta 28)

Perusoikeuskirjan 7, 8 ja 11 artikla

Kun arvioidaan säilytysvelvollisuutta EU:n perusoikeuskirjan kannalta, asiassa ovat relevantteja erityisesti yksityiselämän suojaa (7 artikla) ja henkilötietojen suojaa (8 artikla) koskevat määräykset. Lisäksi unionin tuomioistuin on kiinnittänyt huomiota säilytysvelvollisuuden vaikutuksiin suhteessa perusoikeuskirjan 11 artiklassa taattuun sananvapauteen. Perusoikeuskirjan 52(1) artiklan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Unionin tuomioistuin on ratkaisukäytännössään arvioinut säilytysvelvollisuutta suhteessa perusoikeuskirjaan. Näissä ratkaisuissaan unionin tuomioistuin on arvioinut eräät säilyttämistoimenpiteet unionin oikeuden mukaisiksi. Siten unionin tuomioistuimen oikeuskäytäntö tarjoaa ohjeistusta siihen, millaiset ratkaisut ovat sähköisen viestinnän tietosuojadirektiivin ja perusoikeuskirjan valossa mahdollisia.

Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan.

Unionin tuomioistuin on arvioinut yksityselämän suojaan puuttumista merkitsevää sääntelyä perusoikeuskirjan valossa ja katsonut muun muassa, että merkitystä ei ole sillä, ovatko kyseiset yksityiselämään liittyvät tiedot arkaluonteisia vai eivät tai onko asianomaisille mahdollisesti aiheutunut haittaa tästä puuttumisesta (Digital Rights Ireland, kohta 33, ks. vastaavasti tuomio Österreichischer Rundfunk ym., C-465/00, C-138/01 ja C-139/01, EU:C:2003:294, 75 kohta). Unionin tuomioistuin on myös katsonut, että velvollisuus säilyttää tietyn ajan tietoja henkilön yksityiselämästä ja hänen viestinnästään merkitsee sellaisenaan puuttumista perusoikeuskirjan 7 artiklassa taattuihin oikeuksiin. Lisäksi toimivaltaisten kansallisten viranomaisten oikeus saada tietoja merkitsee myös puuttumista tähän perusoikeuteen (Digital Rights Ireland, kohdat 34-35).

Perusoikeuskirjan 8 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan. Tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty.

Henkilötietojen suoja liittyy kiinteästi perusoikeuskirjan 7 artiklassa vahvistettuun yksityiselämän suojaan. (Volker und Markus Schecke ja Eifert, C-92/09 ja C-93/09, EU:C:2010:662, 47 kohta) Unionin tuomioistuin on katsonut, että liikenne- ja paikkatietojen säilyttäminen kuuluu perusoikeuskirjan 8 artiklan soveltamisalaan, sillä se merkitsee kyseisessä artiklassa tarkoitettua henkilötietojen käsittelyä. Säilyttämisen on siten täytettävä kyseisestä artiklasta johtuvat tietojen suojan vaatimukset. (Digital Rights Ireland kohta 29)

Perusoikeuskirjan 11 artiklan mukaan jokaisella on oikeus sananvapauteen. Tämä oikeus sisältää mielipiteenvapauden sekä vapauden vastaanottaa ja levittää tietoja tai ajatuksia viranomaisten siihen puuttumatta ja alueellisista rajoista riippumatta.

Unionin tuomioistuin on kiinnittänyt ratkaisuissaan huomiota myös liikenne- ja paikkatietojen säilytysvelvollisuuden vaikutuksista perusoikeuskirjan 11 artiklassa taatun sananvapauden harjoittamiseen. (ks. esim. Digital Rights kohdat 25 ja 70; Tele2 kohdat 92 ja 101) Unionin tuomioistuimen mukaan myös sananvapaus tulee ottaa huomioon direktiivin 2002/58 15 artiklan 1 kohtaa tulkittaessa, kun otetaan huomioon sen erityinen merkitys demokraattisissa yhteiskunnissa. Perusoikeuskirjan 11 artiklassa taattu perusoikeus on eräs demokraattiseen ja moniarvoiseen yhteiskuntaan liittyvä olennainen perusta ja kuuluu arvoihin, joille unioni Euroopan unionista tehdyn sopimuksen (SEU) 2 artiklan mukaisesti perustuu. (Tele2 kohta 93 ja siinä viitattu oikeuskäytäntö)

Liikenne- ja paikkatietojen säilyttäminen viranomaisten käyttöä varten on unionin tuomioistuimen mukaan omiaan vaikuttamaan ennalta ehkäisevästi siihen, miten sähköisten viestintävälineiden käyttäjät käyttävät perusoikeuskirjan 11 artiklassa taattua sananvapauttaan. (Digital Rights kohta 28, Tele 2 kohta 101) Nämä vaikutukset ovat sitä vakavampia, mitä enemmän tietoja säilytetään ja mitä moninaisempia ne ovat. (QdN kohta 118) Samoin kuin yksityiselämän suojaa ja tietosuojaa koskevat perusoikeudet, myöskään sananvapaus ei ole ehdoton, vaan se on suhteutettava siihen tehtävään, joka niillä on yhteiskunnassa. (QdN kohta 120 oikeuskäytäntöviittauksineen).

Perusoikeuskirjan muut määräykset

Perusoikeuskirjan 16 artiklassa säädetään elinkeinovapauden periaatteesta. Elinkeinovapaus tunnustetaan unionin oikeuden sekä kansallisten lainsäädäntöjen ja käytäntöjen mukaisesti.

Perusoikeuskirjan 17 artiklassa säädetään omistusoikeudesta. Jokaisella on oikeus nauttia laillisesti hankkimastaan omaisuudesta sekä käyttää, luovuttaa ja testamentata sitä. Keneltäkään ei saa riistää hänen omaisuuttaan muutoin kuin yleisen edun sitä vaatiessa laissa säädetyissä tapauksissa ja laissa säädettyjen ehtojen mukaisesti ja siten, että hänelle suoritetaan kohtuullisessa ajassa oikeudenmukainen korvaus omaisuuden menetyksestä. Omaisuuden käyttöä voidaan säännellä lailla siinä määrin kuin se on yleisen edun mukaan välttämätöntä.

Perusoikeuskirjan 21 artiklassa säädetään syrjintäkiellosta. Artiklan 1 kohdan mukaan kielletään kaikenlainen syrjintä, joka perustuu sukupuoleen, rotuun, ihonväriin tai etniseen taikka yhteiskunnalliseen alkuperään, geneettisiin ominaisuuksiin, kieleen, uskontoon tai vakaumukseen, poliittisiin tai muihin mielipiteisiin, kansalliseen vähemmistöön kuulumiseen, varallisuuteen, syntyperään, vammaisuuteen, ikään tai sukupuoliseen suuntautumiseen tai muuhun sellaiseen seikkaan.

Perusoikeuskirjan 47 artiklassa säädetään oikeudesta tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen. Artiklan 1 kohdan mukaan jokaisella, jonka unionin oikeudessa taattuja oikeuksia ja vapauksia on loukattu, on oltava tässä artiklassa määrättyjen edellytysten mukaisesti käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa.

Perusoikeuskirjan 48 artiklan 1 kohdan mukaan jokaista syytettyä on pidettävä syyttömänä, kunnes hänen syyllisyytensä on laillisesti näytetty toteen.

Unionin tuomioistuimen oikeuskäytännössä käsittelemien ratkaisuiden voidaan katsoa täyttävän myös nämä perusoikeuskirjan määräykset. Unionin tuomioistuin ei ole erikseen nostanut elinkeinovapautta tai omaisuudensuojaa ongelmalliseksi seikaksi säily-

tysvelvollisuutta koskevassa oikeuskäytännössään. Myöhemmin jaksossa 6.3.3.2 käsiteltävän säilytysvelvollisuuden henkilöllisen kohdentamisen osalta unionin tuomioistuin ei ole pitänyt tällaista henkilöpiirin perusteella määriteltävää kriteeriä itsessään syrjivänä, joskin tuomioistuin edellyttää, että tällaisen toimenpiteen kohteiksi valikoitumisen pitää perustua kansallisessa oikeudessa määriteltyihin objektiivisiin ja syrjimättömiin seikkoihin. (G.D. kohdat 75–78) Maantieteellistä kohdentaminen ei unionin tuomioistuimen mukaan lähtökohtaisesti ole omiaan johtamaan syrjintään. (G.D. kohta 80) Unionin tuomioistuin on nimenomaisesti todennut, ettei kohdennettu säilyttäminen ole syyttömyysolettaman vastaista (Spetsializirana prokuratura (Bulgaria) kohta 46). Kohdennettu säilyttäminen ei myöskään ole vastoin uhrien yhdenvertaisen kohtelun vaatimusta (Spetsializirana prokuratura (Bulgaria) kohta 44). Oikeussuojakeinoihin liittyvät perusoikeuskirjan vaatimukset ovat merkityksellisiä (HYA e.a. kohta 43 ja 44). Perusoikeuskirjan ja direktiivin 15(1) artiklan vaatimukset ovat osin päällekkäisiä. Perusoikeuskirjan vaatimukset ulevat katetuksi unionin tuomioistuimen oikeuskäytännössään konkretisoimien direktiivin 15(1) artiklan yleisten välttämättömyyden, asianmukaisuuden ja oikeasuhtaisuuden edellytysten kautta.

3.2.2 Euroopan ihmisoikeussopimus ja KP-sopimus

Euroopan ihmisoikeussopimuksen 8 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

Kuten EU:n perusoikeuskirjan osalta, myös ihmisoikeussopimuksen näkökulmasta viranomaisen ei tarvitse tosiasiassa käsitellä tietoja, jotta kyse olisi yksityiselämään puuttumisesta, vaan puuttumiseksi on katsottava jo se, että viranomainen kerää ja tallentaa niitä myöhempää käyttöä varten (S. and Marper v. the United Kingdom, 4.12.2008, kohta 85). Pelkkä sellaisen lainsäädännön olemassaolo, joka mahdollistaa viestintäyhteyksien salaisen tarkkailun, puuttuu viestinnän osapuolten ja myös potentiaalisten osapuolten ihmisoikeussopimuksen 8 artiklassa taattuihin oikeuksiin (Klass v. Saksa 6.9.1978 sekä Liberty ja muut v. Yhdistynyt Kuningaskunta 1.10.2008).

Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö koskee pitkälti viranomaisten toimintaa. Ihmisoikeustuomioistuin on kuitenkin katsonut, että artikla soveltuu teleyrityksiin kohdistuvaan säilytysvelvollisuuteen. Tuomioistuin on katsonut, että yleiseen säilytysvelvollisuuteen sovelletaan vastaavia suojakeinoja, joita ihmisoikeustuomiois-

tuin on asettanut salaisille valvontatoimenpiteille ja tietoliikennetiedustelulle (Ekimdzhiev and Others v. Bulgaria, 2022, §§ 291 ja 394–395). Suojakeinot voidaan tiivistää seuraavasti:

- säilyttämistä koskevan sääntelyn on oltava julkisesti saatavilla
- laissa on säädettävä, miten säilytettävä tieto suojataan
- laissa on määriteltävä perusteet, joiden nojalla tietoja voidaan säilyttää ja pääsy tietoihin antaa
- laissa on määriteltävä menettely sille, miten tietoihin saadaan antaa pääsy ml. suojatoimenpiteet
    - tietojen saanti vaatii tuomioistuimen antaman luvan (kiireellisissä tapauksissa jälkikäteisen)
    - tietojensaantia koskevassa hakemuksessa on määriteltävä, mitä tarkoitusta varten tietoja haetaan ja miksi pyydetty tieto on välttämätöntä
    - tuomioistuimelle on toimitettava kaikki sen harkinnan kannalta merkitykselliset tiedot
    - tuomioistuimen on perusteltava ratkaisunsa
- laissa on määriteltävä ajanjakso, jonka viranomaiset saavat säilyttää ja käyttää dataa
- laissa on määriteltävä menettely sille, miten saatua tietoa säilytetään, tarkastellaan, käytetään, välitetään eteenpäin ja tuhotaan
- laissa on määriteltävä menettelyt ja toimintatavat riippumattoman viranomaisen suorittamaan valvontaan ml. korjaavat toimivaltuudet
- laissa on säädettävä tehokkaasta ilmoitusmenettelystä kohteelle
- laissa on säädettävä tehokkaista oikeussuojakeinoista

(Ekimdzhiev and Others v. Bulgaria, 2022, §§ 291 ja 396–418).

Kyseiset vaatimukset ovat käytännössä pitkälti yhteneviä unionin tuomioistuimen asettamien vaatimusten kanssa. Toisaalta ihmisoikeustuomioistuin ei ole tiedusteluratkaisuissaan ehdottomasti torjunut massavalvontaa, vaan tuonut esille kansallisen harkintamarginaalin (Centrum för Rättvisa v. Ruotsi (19.6.2018), § 112)[49]. Ihmisoikeustuomioistuimen vaatimukset nousevatkin käytännössä merkityksselliseksi erikseen ja erityisesti silloin, kun kansallinen sääntely ei ole EU-oikeuden soveltamisalassa.

[49] Perustuslakivaliokunnan mielestä EIT:n linjaus massavalvonnan kuulumista kansallisen harkintamarginaalin piiriin korostava käytäntö ei muodosta EUT:n oikeuskäytäntökin huomioon ottaen perustetta arvioida massavalvonnan sallittavuutta toisin (PeVL 36/2018 vp s. 12).

Edellä todetusti teleoperaattoreihin kohdistuva säilytysvelvollisuus on kuitenkin EU-oikeuden soveltamisalassa.

Euroopan ihmisoikeussopimus suojaa myös omaisuutta ja elinkeinovapautta (1. pöytäkirjan 1 artikla), syrjimättömyyttä (14 artikla), oikeutta tehokkaaseen oikeussuojakeinoon (13 artikla) sekä syyttömyysolettamaa (6(2) artikla). Näitä ei kuitenkaan ole arvioitu erikseen säilyttämisvelvollisuutta koskevassa ihmisoikeustuomioistuimen oikeuskäytännössä.

KP-sopimuksen 17 artiklan mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. Jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan. YK:n ihmisoikeusneuvostossa on hyväksytty useita raportteja yksityiselämän suojasta digitalisaation aikakaudella.[50] Niissä todetaan, että säilytysvelvollisuudella puututaan yksityiselämän suojaan. Toimenpiteen välttämättömyyteen ja suhteellisuuteen on kiinnitetty tässäkin yhteydessä huomiota samoin kuin oikeussuojakeinoihin.[51] Tässäkin yhteydessä on nostettu esille systemaattisen tarkkailun mahdollinen uhka sananvapaudelle, kokoontumisvapaudelle, osallistumiselle ja demokratialle.[52] KP-sopimuksen vaatimukset vaikuttavat olevan sisällöltään yhteneväisiä ihmisoikeussopimuksen ja perusoikeuskirjan kautta.

3.2.3 Perustuslaki

Nykyinen voimassa oleva välitystietojen säilyttämisvelvollisuutta koskeva lainsäädäntö on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 18/2014 vp). Perustuslakivaliokunta piti unionin tuomioistuimen silloin vastikään antaneen Tele2-ratkaisun huomioita pohjana kansallisen säilytysvelvollisuutta koskevan säätelyn valtiosääntöisessä tarkastelussa. Vaikka unionin tuomioistuimen tuomio ei suoranaisesti koskenut Suomen kansallista täytäntöönpanolainsäädäntöä, tuli kansallisen sääntelyn perustuslakivaliokunnan mukaan täyttää tuomiossa mainitut edellytykset. Perustuslakivaliokunta piti tällöin selvänä, että myös kansallista sääntelyä on syytä arvioida paitsi kansallisten perusoikeussäännösten myös unionin tuomioistuimen tuomiossa käsiteltyjen EU:n perusoikeuskirjan yksityiselämän suojaa ja henkilötietojen suojaa koskevien määräysten valossa. (PeVL 18/2014 vp, s. 4-5)

[50] A/HRC/27/37 (2014), A/HRC/39/29 (2018), A/HRC/48/31 (2021) ja A/HRC/51/17 (2022).
[51] Ks. esim. A/HRC/27/37, 20, 24–27 ja 37–41 kappale. Myöhemmissä raporteissa tuodaan esille samoja huomioita.
[52] A/HRC/51/17, 43 kappale.

Perustuslain 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Valittavina olevien toimenpiteiden arviointiin vaikuttaa perustuslaissa turvattu luottamuksellisen viestin salaisuuden suoja. Tämän oikeuden rajoittamista asiassa puoltavat vakavien rikosten selvittämisintressiin ja rikosoikeudellisen järjestelmän uskottavuuteen liittyvät hyväksyttävät ja yhteiskunnallisesti painavat perusteet. Perustuslakivaliokunta on painottanut, että yksityiselämän ja henkilötietojen suoja tulee suhteuttaa toisiin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin intresseihin (PeVL 35/2018 vp, s. 4, PeVL 14/2018 vp, s. 6 ja PeVL 5/1999 vp, s. 2) tai esimerkiksi vakavien rikosten selvittämisintressiin ja rikosoikeudellisen järjestelmän uskottavuuteen liittyviin hyväksyttäviin ja yhteiskunnallisesti painaviin perusteisiin (PeVL 32/2013 vp, s. 7).

Perustuslakivaliokunnan valtiosääntöisiin tehtäviin ei lähtökohtaisesti kuulu EU-oikeuden kansallisen täytäntöönpanosääntelyn arviointi EU:n aineellisen lainsäädännön kannalta (ks. esim. PeVL 14/2018 vp, s. 7). Perustuslakivaliokunnan mukaan perustuslain 10 §:n 4 momentin rajoissa säädettävien valtuuksien, esimerkiksi siviili- ja sotilastiedustelua koskevissa hallituksen esityksissä tiedusteluviranomaisille ehdotettavien toimivaltuuksien, on oltava sopusoinnussa myös Suomen kansainvälisten ihmisoikeusvelvoitteiden, erityisesti Euroopan ihmisoikeussopimuksen, ja EU-oikeuden kanssa. Valiokunta korosti tarvetta seurata EIT:n ja EUT:n käytäntöä tiedustelutoiminnan alalla. Valiokunta katsoi, että tämän oikeuskäytännön mukaisesti on arvioitava ehdotettuja uusia rajoitusperusteita kansallista lainsäädäntöä valmisteltaessa ja säädettäessä samoin kuin sovellettaessa niitä viranomaisissa ja tuomioistuimissa (PeVM 4/2018 vp, s. 9).

Perustuslakivaliokunnan mukaan on sinänsä selvää, että Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan unionin lainsäädäntö on ensisijaista suhteessa kansallisiin säännöksiin oikeuskäytännössä määriteltyjen edellytysten mukaisesti (ks. PeVL 20/2017 vp, s. 6 ja PeVL 51/2014 vp, s. 2/II), eikä suomalaisessa lainsäädännössä ole syytä pyrkiä EU-oikeuden kanssa ristiriidassa oleviin ratkaisuihin (esim. PeVL 19/2021 vp, kappale 14 ja siinä mainittu lausuntokäytäntö), vaikka valiokunnan valtiosääntöisiin tehtäviin ei lähtökohtaisesti kuulukaan kansallisen täytäntöönpanosääntelyn arviointi EU:n aineellisen lainsäädännön kannalta (esim. PeVL 32/2021 vp, kappale 3). (PeVL 81/2022 vp, kappale 8)

Perustuslakivaliokunta on arvioinut EU-oikeudellisia lainsäädäntöhankkeita perus- ja ihmisoikeuksien kannalta kiinnittämällä huomiota myös merkitykselliseen tuomioistuinkäytäntöön (ks. myös. PeVL 28/2016 vp, s. 5—6, PeVL 20/2016 vp, s. 4—5). Valiokunta on katsonut myös EU-oikeuteen perustuvan yksityiselämän ja henkilötietojen suojan kannalta merkityksellisen kansallisen sääntelyn valmistelussa olevan syytä kiinnittää huomiota erityisesti EU-tuomioistuimen asioissa Digital Rights Ireland (C-293/12 ja C-594/12), Schrems (C-362/14) ja Tele2 Sverige ja Watson (C-698/15 ja C-203/15) antamiin ratkaisuihin (PeVL 13/2017 vp, s. 4—5, PeVL 9/2017 vp, s. 5).

Perustuslakivaliokunta on arvioinut laajasti kansallisen tietoyhteiskuntakaariehdotuksen (nyk. laki sähköisen viestinnän palveluista) sääntelyä teleyritysten velvollisuudesta säilyttää tietoja viranomaistarpeita varten EU-tuomioistuimen asiassa Digital Rights Ireland antaman tuomion valossa. Valiokunta piti selvänä, että myös kansallista sääntelyä oli tuolloisessa sääntelyasetelmassa syytä arvioida paitsi kansallisten perusoikeussäännösten myös unionin tuomioistuimen tuomiossa käsiteltyjen EU:n perusoikeuskirjan yksityiselämän suojaa ja henkilötietojen suojaa koskevien määräysten valossa (PeVL 18/2014 vp, s. 4/II—7/II). Valiokunta on katsonut myös, että lainsäätäjän toimivaltaan ei voi kuulua yksityiselämän suojan kannalta keskeisten arkaluonteisten tietojen käsittelystä säätäminen vastoin EU:n oikeuteen kuuluvan yleisen tietosuoja-asetuksen sääntelyä (PeVL 15/2018 vp, s. 45). Valiokunta on arvioinut myös EU-oikeuden eri tulkintavaihtoehtojen tuottaman epävarmuuden valtiosääntöistä merkitystä (PeVL 15/2018 vp, s. 53). (PeVL 36/2018 vp, s. 6 ja 7)

Perustuslakivaliokunta on arvioidessaan hallituksen esityksiä, joiden tarkoitus on EU:n oikeuden täytäntöönpano, kiinnittänyt huomiota siihen, että vaikka perustuslakivaliokunnan valtiosääntöisiin tehtäviin ei lähtökohtaisesti kuulu kansallisen täytäntöönpanosääntelyn arviointi EU:n aineellisen lainsäädännön kannalta (ks. esim. PeVL 10/2022 vp, kappale 13, PeVL 13/2019 vp, s. 2, PeVL 31/2017 vp, s. 4) siltä osin kuin Euroopan unionin lainsäädäntö edellyttää kansallista sääntelyä tai mahdollistaa sen, tätä kansallista liikkumavaraa käytettäessä otetaan huomioon perus- ja ihmisoikeuksista seuraavat vaatimukset (ks. esim. PeVL 1/2018 vp, PeVL 25/2005 vp). Valiokunta on näissä yhteyksissä painottanut, että hallituksen esityksessä on erityisesti perusoikeuksien kannalta merkityksellisen sääntelyn osalta syytä tehdä selkoa kansallisen liikkumavaran alasta (ks. esim. PeVL 1/2018 vp, s. 3, PeVL 26/2017 vp, s. 42). Valiokunta on arvioinut myös jo ehdotuksia EU-sääntelyksi kiinnittäen huomiota kansallisen liikkumavaran alaan erityisesti perusoikeusherkissä kysymyksissä (ks. esim. PeVL 37/2021 vp, kappale 25 ja PeVL 39/2021 vp, kappale 10 ja 11). (PeVL 11/2022 vp, 7 kohta.)

Henkilötietojen suoja ja luottamuksellisen viestin salaisuuden suoja

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Pykälän 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Pykälän 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Välitystietojen säilytysvelvollisuuden sääntely on merkityksellistä perustuslain 10 §:ssä turvattujen yksityiselämän, henkilötietojen suojan sekä luottamuksellisen viestin

salaisuuden suojan kannalta. Perustuslain 10 §:n arvioinnin osalta muodostuu erityisesti perustuslain 10 §:n 4 momentin muutokseen ja siihen liittyvä perustuslakivaliokunnan käytäntö, jossa on keskeisesti arvioitu luottamuksellisen viestin salaisuuden rajoittamisen edellytyksiä.

Perustuslain 10 §:ssä turvatun yksityiselämän suojan lähtökohta on yksilön oikeus elää omaa elämäänsä ilman viranomaisten ja ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista siihen. (PeVL 53/2005 vp, s. 2, PeVL 36/2002 vp, s. 5/II, PeVL 9/2004 vp, s. 5/II). Perustuslakivaliokunta on pitänyt valtiosääntöoikeudellisesti ongelmallisena ja oikeasuhtaisuusvaatimuksen vastaisena sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin. (PeVL 20/2016 vp, s. 5, PeVL 18/2014 vp, s. 6). Perustuslakivaltiokunta on katsonut, että perustuslain 10 §:n 4 momentin säännöksestä ja lisäksi yleisiin rajoitusedellytyksiin kuuluvasta välttämättömyysvaatimuksesta johtuu, että luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee olla kohdennettua ja rajattua (PeVL 35/2018 vp, s. 12) ja nostanut esille, että mainittu säännös ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa (PeVM 4/2018 vp, s. 8).

Viestin sisällön lisäksi perustuslain säännöksillä suojataan myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle. Perustuslakivaliokunta aikaisemmin vakiintuneesti katsoi, että viestin tunnistamistiedot jäävät luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (ks. esim. PeVL 33/2013 vp, s. 3/I, PeVL 6/2012 vp, s. 3—4, PeVL 29/2008 vp, s. 2/II ja PeVL 3/2008 vp, s. 2/I). Kuitenkin unionin tuomioistuimen Digital Rights Ireland –tuomion jälkeen perustuslakivaliokunta katsoi, että tuomio antaa perusteita arvioida tätä oppia uudelleen. Tämän seurauksena perustuslakivaliokunta totesi, että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen. (PeVL 18/2014 vp, s. 6/II)

Perusoikeusrajoituksen hyväksyttävyyttä arvioitaessa on merkitystä rajoitustoimien tarkoituksella. Mitkä tahansa viranomaistarpeet eivät kuitenkaan oikeuta asettamaan yrityksille tämän kaltaista säilytysvelvollisuutta. Tämä ei ole asianmukaista velvoitteen täsmällisyyden ja tarkkarajaisuuden vaatimuksen kannalta. (PeVL 3/2008 vp, s. 2/I) Säilytystietojen säilyttämisvelvoitetta puoltaa vakavan rikollisuuden torjuntaan liittyvä hyväksyttävä peruste. (PeVL 18/2014 vp, s. 7/I) Yllä käsitellysti säilytysvelvollisuus on unionin tuomioistuimen oikeuskäytännössä katsottu olevan mahdollista rikollisuuden ja yleiseen turvallisuuteen kohdistuvien uhkien torjumiseksi ja kansallisen turvallisuuden suojaamiseksi.

Nykyisen lain säätämisen yhteydessä perustuslakivaliokunta arvioi, että unionin tuomioistuimen Digital Rights Ireland -tuomion valossa näyttäisi olevan perusteltua pyrkiä rajaamaan säilyttämisvelvollisuutta sekä henkilöpiirin että viestinnän sisällön osalta. Lisäksi perustuslakivaliokunta katsoi, ettei tuomioista johdu suoranaista estettä sellaiselle sääntelylle, jossa oikeasuhtaisuuden vaatimukset toteutetaan muilla tavoin. (PeVL 18/2014 vp, s. 6–7)

Säädettäessä nykyisen sähköisen viestinnän palvelulain 19 lukua, perustuslakivaliokunta edellytti, että säilytettävät tiedot on yksilöitävä laissa, ja että liikenne- ja viestintävaliokunnan tuli täsmentää, mitkä ehdotetun säännöksen perusteella säilytettävät tiedot ovat välttämättömiä sääntelyn taustalla olevan tarkoituksen kannalta. Sellaisia tietoja, jotka eivät ole tarkoituksen kannalta välttämättömiä, ei voi vaatia säilytettäväksi. (PeVL 18/2014 vp, s. 7) Perustuslakivaliokunta on myös aikaisemmin pitänyt suhteellisuusperiaatteen kannalta tärkeänä, ettei palveluntarjoajaa velvoiteta erikseen tuottamaan tai hankkimaan tietoja, vaan ainoastaan säilyttämään tarjoajan saatavilla muutenkin olevat tiedot. (PevL 3/2003, s. 2/II, PeVL 3/2006 vp, s. 3/I, PeVL 35/2004 vp, s. 3/II) Säilyttämisvelvollisuuden vähimmäissisällön kannalta perustuslakivaliokunta on pitänyt aivan olennaisena, mihin tietoihin tai tietotyyppeihin velvollisuus ulottuu. Tällaisten, sääntelyn kannalta olennaisten seikkojen ja rajausten tulee käydä säännöksistä ilmi täsmällisesti. (PeVL 3/2006 vp, s. 3/II, PeVL 35/2004 vp, s. 3/II)

Perustuslakivaliokunta on kiinnittänyt huomiota perusoikeuden rajoituksen välttämättömyyttä arvioitaessa myös siihen, että tiettyjä rikoksia ei käytännössä pystytä selvittämään tai estämään ilman televalvontaa. (PeVL 32/2013 vp, s. 4[53]) Myös unionin tuomioistuin on erityisesti IP-osoitteiden säilyttämisvelvollisuuden oikeasuhtaisuutta arvioidessaan kiinnittänyt huomiota siihen, että ilman tietojen säilyttämisvelvollisuutta verkkorikosten paljastaminen voi osoittautua mahdottomaksi. (QdN kohta 154) Tältä osin on kuitenkin huomattava, että vaikka sähköisen viestinnän tietojen säilytysvelvollisuus voi olla välttämätöntä joidenkin rikosten selvittämiseksi, näin ei automaattisesti ole kaikkien rikosten osalta eikä kaikkien teleyritysten käsittelemien ja säilyttämien tietojen osalta.

Perustuslakivaliokunnan mukaan tunnistamistietojen säilyttämiseen liittyy aina riskejä yhtä hyvin luottamuksellisen viestin salaisuuden kuin henkilötietojen suojan kannalta. Riskit kasvavat, mitä kauemmin tietoja säilytetään (PeVL 3/2008 vp, s. 2/I; PeVL 3/2006 vp, s. 3/II). Perustuslakivaliokunta on lausuntokäytännössään peräänkuuluttanut tietojen säilytysajan porrastamisen arvioimista suhteutettuna siihen hyötyyn, joka tiedoilla voi olla hyväksyttävien tavoitteiden saavuttamisen kannalta. Valiokunnan mielestä arvio on tehtävä ennen kaikkea henkilötietojen käsittelyn pääasiallisen käyttötarkoituksen näkökulmasta. (PeVL 28/2016 vp, s. 7, ks. myös PeVL 9/2017 vp, s. 4) Mitä

[53] Kyseisessä lausunnossa valiokunta arvioi tunnistamistietojen hankkimista automaattiseen tietojenkäsittelyjärjestelmään kohdistuneiden rikosten tapauksissa.

pidemmäksi tietojen säilytysaika muodostuu, sitä olennaisempaa on huolehtia tietoturvasta, tietojen käytön valvonnasta ja rekisteröidyn oikeusturvasta. (PeVL 13/2017 vp ja PeVL 28/2016 vp, s. 7) Perustuslakivaliokunta on edellyttänyt unionin tuomioistuimen ratkaisukäytännön huomioimista myös säilytysaikojen arvioinnissa. (PeVL 13/2017 vp, s. 6, PeVL 9/2017 vp, s. 5) Säilytysajan osalta perustuslakivaliokunta on aiemmin pitänyt 12 kuukauden oikeasuhtaisuuden kannalta hyväksyttävänä ja riittävänä vastaamaan viranomaisten tarpeita (PeVL 3/2008 vp, s. 2/II), mutta unionin tuomioistuimen ratkaisun valossa piti arveluttavana, ettei säilyttämisaikaa oltu eritelty suhteessa siihen mahdolliseen hyötyyn, joka tiedoista voi vakavan rikollisuuden torjumisen tavoitteen kannalta olla. (PeVL 18/2014 vp, s. 7) Liikenne- ja viestintävaliokunta porrasti nykylainsäädännön mukaiset säilytysajat 6–12 kuukauteen perustuslakivaliokunnan edellyttämänä. (LiVM 10/2014 vp)

Kuten tämän arviomuistion unionin tuomioistuimen oikeuskäytäntöä erittelevässä jaksossa tarkemmin käsitellään, unionin tuomioistuin on täsmentänyt myöhemmässä oikeuskäytännössään niitä perusteita, joita perusoikeuskirja ja sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohdassa mainittu unionin oikeuden oikeasuhtaisuuden vaatimus edellyttää. Lisäksi unionin tuomioistuin on vahvistanut, että kansallinen lainsäätäjä voi asettaa myös muita erottavia kriteereitä liikenne- ja paikkatietojen kohdennetun säilyttämisen toteuttamiseksi, kunhan ne ovat objektiivisia ja syrjimättömiä, ja joilla varmistetaan, että kohdennetun säilyttämistoimenpiteen ulottuvuus rajoittuu täysin välttämättömään ja että vakavien rikosten ja henkilöiden, joiden tiedot säilytetään, välillä on ainakin välillinen yhteys. (G. D. kohta 83) Perustuslain vaatimukset sellaisina kuin perustuslakivaliokunta on niitä tulkinnut, ovat pitkälti yhtenevät EU-oikeudesta tulevien vaatimusten kanssa. Joitakin aste-eroja kuitenkin on esimerkiksi säilytysajan pituudessa, joissa EU-oikeuden vaatimukset vaikuttavat olevan hieman tiukempia. Vaikuttaisi siltä, että säätämällä välitystietojen säilyttämisvelvollisudesta unioninoikeuden vaatimukset täyttävällä tavalla täytetään lähtökohtaisesti samalla perustuslain sääntelylle asettamat edellytykset.[54]

Perustuslaki vaikuttaisi kuitenkin ainakin yhdessä suhteessa asettavan täsmällisempiä vaatimuksia kuin unionin oikeus. Perustuslain 10 §:n 4 momentissa säädetään kvalifioiduista lakivarauksista, jotka määrittävät tarkemmin sitä, millä perusteilla luottamuksellisen viestin salaisuutta voidaan rajoittaa. Perustuslain 10 §:n 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä

[54] Perustuslakivaliokunta on myös todennut, että säilyttämisvelvollisuutta koskevaa sääntelyä on syytä arvioida EU:n perusoikeuskirjan 7 ja 8 artiklan määräysten valossa, ja perustuslakivaliokunta on myös unionin tuomioistuimen oikeuskäytännön johdosta osin arvioinut uudestaan perustuslain 10 §:ää koskevaa käytäntöä (PeVL 18/2014 vp, s. 3 ja 4).

tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.[55]

Perustuslakivaliokunta painottanut, että yksityiselämän ja henkilötietojen suoja tulee suhteuttaa toisiin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin intresseihin (PeVL 35/2018 vp, s. 4, PeVL 14/2018 vp, s. 6 ja PeVL 5/1999 vp, s. 2) tai esimerkiksi vakavien rikosten selvittämisintressiin ja rikosoikeudellisen järjestelmän uskottavuuteen liittyviin hyväksyttäviin ja yhteiskunnallisesti painaviin perusteisiin (PeVL 32/2013 vp, s. 7). Perustuslain esitöiden mukaan yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten piiriin kuuluvat esimerkiksi huumausainerikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetosrikokset (HE 309/1993 vp, s. 54). Perustuslakivaliokunnan käytännössä edellä mainittuihin rikoksiin on rinnastettu mm. törkeä lapsen seksuaalinen hyväksikäyttö (PeVL 26/2014 vp, s. 4). Perustuslakivaliokunta on myös katsonut mahdolliseksi tehdä rajoituksia luottamuksellisen viestin salaisuuden suojaan henkilön henkeä tai terveyttä uhkaavan välittömän vaaran torjumiseksi tietyin reunaehdoin (PeVL 6/2018 vp).

Välttämättömiä rajoituksia viestin salaisuuteen voi säätää yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa. Perusoikeusrajoituksen hyväksyttävät perusteet on siis määritelty eri tavalla kuin unionioikeudessa. Perusteet vaikuttavat suppeammilta kuin sähköisen viestinnän tietosuojadirektiivissä. Lisäksi tietojen käyttötarkoitus rajautuu perustuslain sanamuodon mukaan rikosten tutkintaan, kun sähköisen viestinnän tietosuojadirektiivissä säädetään torjunnasta, tutkinnasta, selvittämisestä ja syyteharkinnan varmistamisesta. Lisäksi unionin tuomioistuin on torjunnan osalta viitannut myös rikosten ehkäisemiseen.[56]

[55] Perustuslain 10 §:n 4 momenttiin on sisällytetty erityisiä rajoituslausekkeita, joissa annetaan tavallisen lain säätäjälle valtuus perusoikeuden rajoittamiseen ja toisaalta asetetaan lainsäätäjän harkintavaltaa rajoittavia lisäkriteerejä. Perustuslain 10 §:n 4 momentin lakivarauksessa mainitaan osin samoja edellytyksiä kuin perusoikeuksien yleisissä rajoitusedellytyksissä. Näitä ovat lailla säätämisen vaatimus ja rajoituksen välttämättömyys. Perusoikeuksien yleisiä rajoitusedellytyksiä sovelletaan lakivarausta täydentävästi. Tällaisten kvalifioitujen lakivarausten tarkoituksena on määrittää tavallisen lain säätäjän rajoitusmahdollisuus mahdollisimman täsmällisesti ja tiukasti siten, ettei perustuslain tekstissä anneta avoimempaa perusoikeuden rajoitusvaltuutta kuin välttämättä on tarpeen (PeVM 25/1994 vp, s. 5). Toisaalta perustuslakivaliokunta on pitänyt selvänä, ettei tällaisesta rajoituslausekkeesta säädettäessä ole voitu ennakoida kaikkia, esimerkiksi tekniikan kehityksestä aiheutuvia, myöhempiä sääntelytarpeita. (ks. PeVM 4/2018 vp, s. 6, PeVL 36/2017 vp, s. 5, PeVL 30/2010 vp, s. 6/I)

[56] Ks. esim. QdN 140 kohta. Siten terminologisista eroista huolimatta sähköisen viestinnän tietosuojadirektiivin 15(1) artiklan perusteita voinee tulkinta pitkälti yhdenmukaisesti tietosuoja-asetuksen 2(2(d)) artiklan ja rikosasioiden tietosuojadirektiivin 1(1) artiklan kanssa (ensimmäistä ei sovelleta ja toista sovelletaan henkilötietojen käsittelyyn, jota toimivaltaiset viranomaiset suorittavat rikosten ennalta estämistä, tutkintaa, paljastamista tai rikoksiin liittyviä syytetoimia varten tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten) kanssa.

Perustuslakivaliokunta on lausuntokäytännössään katsonut, että käytännössä ei ole mahdollista vetää täsmällistä rajaa rikoksen tekohetken mukaan, ja monien rikosten luonteesta johtuen niiden selvittäminen ei ole mahdollista, mikäli rikoksen tekeminen ei ylipäätään paljastu, mikä puolestaan saattaa vaatia ennakollista varautumista rikoksen tapahtumiseen. (PeVL 2/1996 vp) Perustuslain 10 §:n 3 momentin rajoituslausekketta on jo ennen uuden perustuslain voimaantuloa (ks. esim. PeVL 2/1996 vp, PeVL 5/1999 vp) tulkittu varsin johdonmukaisesti siten, että rikoksen tutkintana pidetään sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei olisi vielä edennyt toteutuneen teon asteelle. Tältä osin tulkinta on vakiintunut eikä siitä ole epäselvyyttä. Näillä perustein valiokunta torjui ehdotuksen tutkinnassa-sanan korvaamisen torjunnassa-sanalla. Se katsoi, että rikosten torjunnan käsite muuttaisi siten rajoituslausekkeen painopisteen rikosten selvittämisestä niiden ennalta estämiseen. Perustuslakivaliokunnan mukaan ehdotettu rikosten torjunnan käsite saattaa myöhemmässä tulkintakäytännössä johtaa myös luottamuksellisen viestin salaisuuden rajoitusmahdollisuuksien laajentumiseen nykysääntelyyn verrattuna, vaikka sitä hallituksen esityksen perustelujen mukaan ei oltu tarkoitettu. Myöskään tulkinta, jossa edellytetään rajoituksilta vähintään konkreettista ja yksilöityä rikosepäilyä, ei ole vastaavalla tavalla kiinnitettävissä rikoksen torjunnan kuin rikoksen tutkinnan käsitteeseen. (PeVM 4/2018 vp, s. 5 ja 6.) Valiokunta on pitänyt tärkeänä, että toimenpiteen valtiosääntöoikeudellisen sallittavuuden edellytyksenä oleva konkreettinen ja yksilöity rikosepäily tuodaan selvästi esille myös säännöksen sanamuodossa. (PeVL 5/1999 vp)

Vaikka siis sekä perustuslaissa että sähköisen viestinnän tietosuojadirektiivissä käytetään tutkinta-käsitettä, perustuslain käsitteen ei voida katsoa rajoittuvan vain samaan kuin direktiivin vastaava käsite, vaan se kattaa myös muita direktiivissä erikseen lueteltuja käyttötarkoituksia.[57]

Perustuslain 10.4§:n kvalifioitu lakivaraus sisältää myös erityisen rajoitusedellytyksen, joka mahdollistaa viestin salaisuuden välttämättömistä rajoituksista säätämisen tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Perustuslakivaliokunta arvioi kansallista turvallisuutta ja siihen kohdistuvaa vakavaa uhkaa perustuslain 10 §:n muutoksen yhteydessä. (PeVM 4/2018 vp)

Perustuslakivaliokunnan käsityksen mukaan kansallinen turvallisuus ja vakava uhka ovat sisällöltään varsin laaja-alaisia käsitteitä. Niiden soveltamisessa korostuu tarve ottaa huomioon ja noudattaa eurooppalaisessa oikeuskäytännössä tiedonhankintame-

[57] Toisaalta terminologisesti on syytä huomata, että unionin tuomioistuin säännönmukaisesti viittaa säilytysvelvollisuutta koskevassa oikeuskäytännössään säännönmukaisesti rikollisuuden torjuntaan yleisen edun mukaisena tavoitteena, jolla puuttuminen viestinnän luottamuksellisuuteen voidaan oikeuttaa.

netelmiä määrittelevälle lainsäädännölle asetettavia perusvaatimuksia. Tällaisia vaatimuksia ovat muun muassa viranomaisten toimivaltuuksien käyttöön kohdistuva tuomioistuimen ennakollinen hyväksyminen, riippumaton valvonta, oikeusturvan toteuttaminen tuomioistuimessa ja tietosuojan perusteiden noudattaminen. Perustuslakivaliokunta korostaa erityisesti vahvoja oikeusturvatakeita sekä laaja-alaista ja tehokasta tiedusteluvaltuuksien käytön valvontaa ja riittäviä soveltamisrajoituksia myös, koska kyse on poikkeuksellisesta rajoitusperusteesta, jossa irrottauduttaisiin rikosperusteisesta toiminnasta ja joka niin ollen tulisi sovellettavaksi myös tilanteissa, joissa ei tiedonhankintavaiheessa eikä välttämättä muutoinkaan voitaisi kohdistaa konkreettista ja yksilöityä rikosepäilyä. (PeVM 4/2018 vp, s. 8) Tämä on merkityksellistä siitäkin syystä, että perustuslain uusi 10 §:n 4 momentti ei vastaisuudessa koskisi ainoastaan tiedusteluvaltuuksia, vaan kaikkia tulevaisuudessa mahdollisesti ehdotettavia uusia luottamuksellisen viestinnän rajoitusvaltuuksia. (PeVM 4/2018 vp, s. 8)

Lisäksi perustuslakivaliokunta on painottanut, että perustuslain 10 §:n 4 momentin rajoissa säädettävien valtuuksien on oltava sopusoinnussa myös Suomen kansainvälisten ihmisoikeusvelvoitteiden, erityisesti Euroopan ihmisoikeussopimuksen, ja EU-oikeuden kanssa. Valiokunta on korostanut myös, että perustuslaissa turvattu perusoikeussuojan taso voi olla korkeampi kuin suojan vähimmäistason asettavista ihmisoikeusvelvoitteista johtuu. (PeVM 4/2018 vp, PeVL 59/2017 vp, PeVL 43/2016 vp, PeVL 24/2016 vp, PeVL 59/2014 vp)

Kansallista turvallisuutta ei ole lain tasolla yksiselitteisesti määritelty (ks. PuVM 6/2022 vp — HE 222/2022 vp). Puolustusvaliokunnan mietinnössä on katsottu, että kansallinen turvallisuus on monisyinen käsite, jonka ytimessä on kansakunnan turvallisuus ja olemassaolo. Yhtä lailla puolustusvaliokunta on todennut, että mahdollisimman laaja kansallisen turvallisuuden määritelmä on valiokunnan mielestä välttämätön edellytys sille, että lainsäädännön suomia valtuuksia voidaan täysimääräisesti hyödyntää esimerkiksi kriittisen infrastruktuurin tehokkaassa suojaamisessa. Toisaalta kansallisen turvallisuuden käsitettä on käsitelty varsin laajasti Euroopan ihmisoikeustuomioistuimen ratkaisukäytännössä, jonka mukaan ainakin sotilaallinen maanpuolustus, terrorismintorjunta ja laittoman tiedustelutoiminnan torjunta kuuluvat käsitteen piiriin (mm. Weber & Saravia v. Saksa, 29.6.2006; Klass ja muut v. Saksa). Kansalliseen turvallisuuteen saattaa kuitenkin kohdistua monenlaisia uhkia, joita on vaikea ennakoida tai määritellä etukäteen. Tästä seuraa, että käsitteen selventäminen on ensisijaisesti jätettävä kansallisen käytännön varaan (Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010).

Unionin tuomioistuin on puolestaan katsonut, että kansallisen turvallisuuden säilyttäminen vastaa ensisijaisen tärkeää intressiä suojella valtion keskeisiä tehtäviä ja yhteiskunnan perustavanlaatuisia etuja, ja siihen kuuluu sellaisten terrorismin kaltaisten toimien torjuminen ja niistä rankaiseminen, jotka ovat omiaan horjuttamaan vakavasti tietyn maan perustavanlaatuisia perustuslaillisia, poliittisia, taloudellisia tai yhteiskunnallisia rakenteita ja erityisesti uhkaamaan suoraan yhteiskuntaa, väestöä tai valtiota

sellaisenaan. Kansalliseen turvallisuuteen kohdistuva uhka eroaa luonteeltaan, vakavuudeltaan ja uhan muodostavien erityisten olosuhteiden vuoksi siitä yleisestä ja pysyvästä vaarasta, jonka muodostavat jännitteiden tai häiriöiden, jopa vakavien, ilmeneminen, tai vakavat rikokset. (G. D. kohdat 61 ja 62)

Perustuslaista johtuu tarve yhtäältä tulkita kansallisen turvallisuuden käsitettä suppeasti sekä toisaalta asettaa uhan vakavuusaste korkealle. Rajoitusperusteeseen vetoavalla on myös velvollisuus esittää riittävät perustelut sille, että jokin toiminta voi muodostua vakavaksi uhaksi kansalliselle turvallisuudelle. Välttämättömyysvaatimuksen täyttymiseksi ei perustuslakivaliokunnan mielestä riitä, että tiedon hankkimisen luottamuksellisista viesteistä voidaan yleisesti katsoa edistävän kansallista turvallisuutta. Sen sijaan on osoitettava, että tiedon hankkiminen kussakin yksittäistapauksessa ja siihen liittyvät yksilökohtaiset perusoikeuksien rajoitukset ovat tehokkaita ja välttämättömiä keinoja hankkia tietoja kyseisessä tilanteessa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. (PeVM 4/2018 vp, s. 8-9)

Kansallisen turvallisuuden käsitesisältöä on arvioitu siviili- ja sotilastiedustelusta säätämisen yhteydessä. Perustuslain 10 §:ää muutettiin tuolloin niin, että sen 4 momentti sallii säätää lailla välttämättömistä rajoituksista viestin salaisuuteen tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan perustuslain säännöksessä kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä taikka kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Ilmaisu ”kansallinen turvallisuus” tarkoittaa sitä, ettei säännöksessä tarkoitettu uhkaava toiminta kohdistuisi ensisijaisesti kehenkään yksilönä vaan yleisemmin yhteiskuntaan ja sen ihmisyhteisöön (HE 198/2017 vp, s. 36).

Perustuslakivaliokunnan mukaan poliisilain siviilitiedustelua koskevan 5 a luvun luottamuksellisen viestinnän suojaan puuttuvissa toimivaltuuksissa on kyse tiedon hankkimisesta perustuslain 10 §:n 4 momentissa tarkoitetusta sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Kyse on perustuslakivaliokunnan mukaan poikkeuksellisesta rajoitusperusteesta, jossa irrottauduttaisiin rikosperusteisesta toiminnasta ja joka näin ollen tulisi sovellettavaksi myös tilanteissa, joissa ei tiedonhankintavaiheessa eikä välttämättä muutoinkaan voitaisi kohdistaa konkreettista ja yksilöityä rikosepäilyä (PeVL 98/2022 vp, s. 4, PeVM 4/2018 vp, s. 8).

Perustuslakivaliokunnan mielestä kansallisen turvallisuuden suojaamiseen voi sinänsä sisältyä erittäin painavia perusteita rajoittaa henkilötietojen suojan ja yksityiselämän suojan perusoikeuksia. Tässä yhteydessä perustuslakivaliokunta on viitannut siihen, että kansallisella turvallisuudella voidaan myös EU-oikeudessa perustella toimenpiteitä, joilla puututaan perusoikeuksiin vakavammin kuin toimenpiteillä, joita perusteltaisiin jollain muulla tavoitteella (ks. myös esim. tuomio 6.10.2020, La Quadrature du Net ym., C-511/18, C-512/18 ja C520/18, 136 kohta). (PeVL 48/2022 vp, s. 4)

Syrjintäkielto

Perustuslakivaliokunta on tiedustelulakien yhteydessä nostanut esille myös syrjintäkiellon merkityksen. Ottaen huomioon, että tiedustelutoiminnan salaisiin tiedonhankintakeinoihin saattaa liittyä merkittäviä profiloinnin riskejä, on sääntelyssä perustuslakivaliokunnan mielestä varmistuttava myös siitä, ettei se johda perustuslain 6 §:ssä tarkoitettuun kiellettyyn syrjintään (PeVL 35/2018 vp, s. 5).

Perustuslakivaliokunta on myös tiedustelulakien yhteydessä käsitellyt toiminnan kohdistamista henkilöryhmään. Perustuslakivaliokunta katsoi, että laissa on syytä täsmällisemmin määritellä, mitä siinä henkilöryhmällä tarkoitetaan ja mitä edellytyksiä useamman henkilön pitämiselle henkilöryhmänä asetetaan. Esityksen perusteluissa mainitut edellytykset muistuttavat rikoslain 6 luvun 5 §:n 2 momentissa tarkoitettuja järjestäytyneelle rikollisryhmälle asetettuja edellytyksiä. Poliisilain 5 a lukuun on tarkkarajaisuuden ja täsmällisyyden turvaamiseksi perusteltua sisällyttää vastaavan kaltainen henkilöryhmän määritelmä. (PeVL 35/2018 vp, s. 18.)

Syrjintäkieltoa säilytysvelvollisuuden osalta on käsitelty nimenomaisesti EU-oikeudessa. Tätä oikeuskäytäntöä on käsitelty tarkemmin yllä jaksossa 3.2.1.

Sananvapaus

Perustuslain 12 §:ssä turvattu sananvapaus sisältää oikeuden ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Perustuslain sananvapaussäännöksen keskeisenä tarkoituksena on sen esitöiden mukaan taata kansanvaltaisen yhteiskunnan edellytyksenä oleva vapaa mielipiteenmuodostus, avoin julkinen keskustelu, joukkotiedotuksen vapaa kehitys ja moniarvoisuus sekä mahdollisuus vallankäytön julkiseen kritiikkiin (HE 309/1993 vp, s. 56/II). Ydinajatukseltaan sananvapautta on perinteisesti pidetty ennen muuta poliittisena perusoikeutena (PeVL 19/1998 vp, s. 5/I). Julkistamisella tarkoitetaan kaikenlaista viestien julkaisemista, levittämistä ja välittämistä. Säännöksestä ilmeneviä sananvapauden ulottuvuuksia ei tulekaan tulkita liian kapeasti (ks. esim. PeVL 52/2010 vp, s. 2).

Sananvapautta säilytysvelvollisuuden osalta on käsitelty EU-oikeudessa. Tätä oikeuskäytäntöä on käsitelty tarkemmin yllä jaksossa 3.2.1.

Oikeus elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen

Perustuslain 7 §:n mukaan jokaisella on oikeus elämään sekä henkilökohtaiseen vapauteen, koskemattomuuteen ja turvallisuuteen. Oikeudella henkilökohtaiseen turvallisuuteen korostetaan julkisen vallan positiivisia toimintavelvoitteita ihmisten suojaamiseksi rikoksilta ja muilta heihin kohdistuvilta oikeudenvastaisilta teoilta. Sillä edelly-

tetään toimia myös rikosten uhrien oikeuksien turvaamiseksi ja aseman parantamiseksi. (PeVL 44/1998 vp, s. 2-3) Vaikka tietojen säilytysvelvollisuudella puututaan perusoikeuksiin, voidaan arvioinnissa ottaa huomioon myös sääntelyn taustalla oleva hyväksyttävänä pidettävä yleisen edun mukainen tavoite, joka palautuu viime kädessä valtion velvollisuuteen turvata oikeus elämään.

Omaisuudensuoja

Perustuslain 15 §:n mukaan jokaisen omaisuus on turvattu. Omaisuudensuoja sisältää paitsi omistajalle lähtökohtaisesti kuuluvan vallan hallita, käyttää ja hyödyntää omaisuuttaan haluamallaan tavalla myös vallan määrätä siitä. (PeVL 41/2006 vp, s. 2) Jos omistusoikeuteen kuuluvia oikeuksia vähennetään tai rajoitetaan, puututaan samalla omaisuudensuojaan, vaikka omistusoikeuden kohteena oleva esine sinänsä säilyisikin koskemattomana haltijallaan. (HE 309/1993 vp, s. 62) Kumottuun sähköisen viestinnän tietosuojalakiin ehdotettua sopimuspakkoa säilytysvelvollisuudesta perustuslakivaliokunta piti jossain määrin ongelmallisena perustuslain 15 §:n turvaamaan omaisuudensuojaan liittyvän sopimusvapauden ja perustuslain 21 §:n 2 momentin mukaisen hyvän hallinnon takeiden kannalta. Tällaisten velvollisuuksien perusteista tulee perustuslain 80 §:n 1 momentin nojalla säätää lailla. (PeVL 3/2008 vp, s. 3/I)

Omistajan oikeuksia voidaan rajoittaa lailla esimerkiksi omaisuuden käyttöön kohdistuvin erilaisin kielloin, rajoituksin ja velvoittein, kunhan sääntely täyttää perusoikeutta rajoittavalta lailta vaaditut yleiset edellytykset. Lisäksi perustuslakivaliokunnan käytännössä on katsottu, että laissa asetettavien velvollisuuksien koskiessa pörssiyhtiöitä tai muita varallisuusmassaltaan huomattavia oikeushenkilöitä lainsäätäjän liikkumavara on omaisuudensuojan näkökulmasta lähtökohtaisesti suurempi kuin silloin, kun sääntelyn vaikutukset muodostuisivat hyvin välittömiksi oikeushenkilön taustalla olevien luonnollisten henkilöiden asemalle. Valiokunta on niin ikään katsonut, että mitä etäämpänä oikeushenkilö on yksilöistä ja mitä vähäisempiä ja välillisempiä ovat ehdotettujen toimenpiteiden vaikutukset yksilöiden konkreettisiin taloudellisiin etuihin, sitä epätodennäköisemmin oikeushenkilöön kohdistuvat toimenpiteet voivat olla ristiriidassa perustuslaissa turvatun omaisuudensuojan kanssa. (PeVL 9/2008 vp, s. 4)

Perustuslain 15 §:n 1 momentin yleislausekkeesta ei johdu vaatimusta korvata omistajalle mitä tahansa käyttörajoitusta eikä täyden korvauksen vaatimusta korvauksia myönnettäessä. Omaisuuden käyttörajoituksen korvaaminen on yksi kokonaisarviointiin vaikuttava osatekijä, joka otetaan huomioon selvitettäessä, onko käyttöoikeuden rajoitus omaisuuden perustuslainsuojan kannalta sallittu (PeVL 10/2014 vp, s. 5). Perustuslaista ei toisaalta seuraa estettäkään siinä edellytettyä paremmalle korvaussäätelylle.

Välitystietojen säilytysvelvollisuus saattaa siis rajoittaa teleyritysten omaisuudensuojaa. Rajoituksena tätä tulee arvioida perustulain näkökulmasta perusoikeuksien yleisten rajoitusedellytysten valossa. Unionioikeudessa omaisuudensuojan rajoitusten arviointi on ollut yllä todetusti suppeaa.

Liikkumisvapaus

Perustuslain 9 §:n 1 momentin mukaan Suomen kansalaisella ja maassa laillisesti oleskelevalla ulkomaalaisella on vapaus liikkua maassa ja valita asuinpaikkansa. Maantieteellisesti kohdennetulla säilyttämisvelvollisuudella voi olla yhteys liikkumisvapauden käyttämiseen. Perustuslakivaliokunnan käytännössä teleosoitteen ja telepäätelaitteen sijaintitietoa koskevan sääntelyn ja tukiasematietojen saamisen yhteys liikkumisvapauteen on tunnistettu, mutta sitä ei ole pidemmälti problematisoitu.[58] Oikeuskirjallisuudessa on kuitenkin kiinnitetty huomiota myös liikkumisvapauteen.[59]

Oikeusturva

Perustuslakivaliokunta on tiedustelulakien yhteydessä nostanut esille myös oikeusturvan merkityksen. Sääntelyn arvioinnissa on huolehdittava siitä, että asianosaisilla on oikeus ihmisoikeussopimuksen 13 artiklassa tarkoitettuihin tehokkaisiin oikeussuojakeinoihin, joiden merkitys on perustuslain 21 §:n oikeudenmukaisen oikeudenkäynnin takeiden tavoin korostunut. (PeVL 35/2018 vp, s. 5)

Oikeusturvaa säilytysvelvollisuuden osalta on käsitelty EU-oikeudessa. Tätä oikeuskäytäntöä on käsitelty tarkemmin yllä jaksossa 3.2.1.

Lainsäädäntövallan delegointi

Perustuslain 80 §:n 2 momentin mukaan myös muu viranomainen voidaan lailla valtuuttaa antamaan oikeussääntöjä määrätyistä asioista, jos siihen on sääntelyn kohteeseen liittyviä erityisiä syitä eikä sääntelyn asiallinen merkitys edellytä, että asiasta säädetään lailla tai asetuksella. Välitystietojen säilytysvelvollisuuden on aikaisemmin katsottu liittyvän hyvin teknillisessä ympäristössä toimivaan toimialaa, mistä johtuen erityiset syyt oikeussääntöjen antamiseen näyttävät täyttyvän. Laista tulee täsmällisesti käydä ilmi, mistä asioista säädetään asetuksella ja mistä viranomaisen määräyksillä. (PeVL 3/2008 vp, s. 3/II)

[58] PeVL 36/2002 vp, s. 5/II, PeVL 9/2004, s. 5–6 ja PeVL 11/2005 vp, s. 5/II.
[59] Niklas Vainio, Viestinnän yksityisyyden suojan turvallisuusperusteinen rajoittaminen perustuslakivaliokunnan käytännössä. Lakimies 6/2017 s. 813–837, 825–826 ja 830.

Lisäksi perustuslakivaliokunta on katsonut, että toimivaltaperusteiden täsmällinen ja ennakoitava määrittely merkitsee vaatimusta laintasoisesta sääntelystä, sen täsmällisyydestä ja tarkkarajaisuudesta. Sääntelyn oikeusvaikutusten tulee olla ennakoitavissa. Henkilön tulee, tarvittaessa oikeudellista apua käyttäen, kyetä ennakoimaan laista hänelle johtuvat seuraukset. Esimerkiksi julkistamattomat sisäiset viranomaismääräykset eivät täytä ennakoitavuusvaatimusta. (PeVL 35/2018 vp, s. 7)

Perustuslain 80 § asettaa edellytykset lainsäädäntövallan delegoinnille. Näitä edellytyksiä tulee arvioida ja ne tulee ottaa huomioon, kun sääntelyratkaisua ja tarvetta alemmanasteiselle sääntelylle arvioidaan.

3.3 Sähköisen viestinnän tietosuojadirektiivin reunaehdot

Sähköisen viestinnän välitystietojen säilyttämistä koskeva sääntely kuuluu EU-oikeuden soveltamisalaan. Kansallinen liikkumavara säätää välitystietojen säilyttämisvelvollisuudesta perustuu sähköisen viestinnän tietosuojadirektiivin 15 artiklaan. Sen mukaan jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan kyseisessä direktiivissä säädettyjen oikeuksien ja velvollisuuksien soveltamisalaa, jos tällaiset rajoitukset ovat 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 varmistamiseksi. Tätä varten jäsenvaltiot voivat muun muassa hyväksyä lainsäädännöllisiä toimenpiteitä, joissa säädetään tietojen säilyttämisestä sellaiseksi rajoitetuksi ajaksi, joka on perusteltua tässä kohdassa säädetyistä syistä.

Sallittujen perusteiden luettelo on tyhjentävä. Tietojen saannin on vastattava tosiasiallisesti ja täysin jotakin näistä tavoitteista, ja säännöksen tavoitteella on lisäksi oltava yhteys sen perusoikeuksiin puuttumisen vakavuuteen, jota tämä tietojen saanti merkitsee. (Tele2 kohta 90 ja 115) Merkitystä ei ole sillä, ovatko kyseessä olevat yksityiselämään liittyvät tiedot arkaluonteisia tai onko asianomaisille mahdollisesti aiheutunut haittaa tästä puuttumisesta. (Ministerio Fiscal kohta 51; Privacy International kohta 70; QdN kohta 115) Merkitystä ei ole myöskään sillä, käytetäänkö säilytettyjä tietoja myöhemmin. (QdN kohta 116)

Unionin tuomioistuin on antanut useita ratkaisuja tietosuojadirektiivin 15 artiklan tulkinnasta luettuna yhdessä perusoikeuskirjan kanssa. Tämän perusteella tuomioistuin on määritellyt sallittuja säilytysvelvollisuuksia perustuen puuttumisen vakavuuden arviointiin (ks. Tele2 kohta 115). Taustalla on ajatus siitä, että välitystietojen säilyttämisessä

kyse on suppeasti tulkittavasta poikkeuksesta pääsääntöön. (Tele2 kohta 89) Säilyttämisestä ei saa muodostua pääsääntöä, sillä muutoin tehtäisiin viimeksi mainitun säännöksen sisältö laajalti tyhjäksi (Tele2 kohta 89) ja koska säilytysvelvollisuus vaikuttaa ehkäisevästi perusoikeuksien käyttöön (G. D. kohta 65).

Unionin tuomioistuimen mukaan unionin oikeus ei ole esteenä lainsäädännöllisille toimenpiteille, joissa

– sallitaan kansallisen turvallisuuden takaamiseksi se, että **sähköisten viestintäpalvelujen tarjoajat määrätään säilyttämään liikenne- ja paikkatiedot yleisesti ja erotuksetta tilanteissa, joissa asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka**, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi, ja joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa päätökseen, jolla tällainen määräys annetaan, tehokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on jokin näistä tilanteista ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan; mainittu määräys voidaan antaa ainoastaan ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa, jos kyseinen uhka on edelleen olemassa;

– säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi **liikenne- ja paikkatietojen kohdennetusta säilyttämisestä**, joka on objektiivisten ja syrjimättömien seikkojen perusteella **rajattu asianomaisten henkilöiden ryhmien mukaan tai maantieteellisen kriteerin avulla** ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa;

– säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi **liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksettomasta säilyttämisestä** ajanjaksoksi, joka on rajoitettu täysin välttämättömään;

– säädetään kansallisen turvallisuuden suojaamiseksi, rikollisuuden torjumiseksi ja yleisen turvallisuuden suojaamiseksi **sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä**; ja

– sallitaan vakavan rikollisuuden torjumiseksi ja varsinkin kansallisen turvallisuuden takaamiseksi se, että **sähköisten viestintäpalvelujen tarjoajat määrätään toimivaltaisen viranomaisen päätöksellä**, johon kohdistuu tehokas tuomioistuinvalvonta, **varmistamaan nopeasti** 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 asianomaisilla henkilöillä on tehokkaat takeet väärinkäytön vaaroja vastaan. (QdN tuomiolauselma)

Unionin tuomioistuimen esittämä jako perustuu siihen, että tavoitteen tärkeyden on oltava oikeassa suhteessa toimenpiteestä aiheutuvan puuttumisen vakavuuteen nähden. (G. D. kohta 56) Tuomioistuimen oikeuskäytännön mukaan oikeus saada säilytysvelvollisuuden perusteella säilytettyjä tietoja 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) Esimerkiksi vakavan rikollisuuden torjumiseksi säilytettäviä tietoja voi käyttää myös kansallisen turvallisuuden tavoitteen vuoksi. (QdN kohta 166) Säilytettyjen tietojen saaminen päinvastaisessa tilanteessa olisi vastoin yleistä etua koskevien tavoitteiden hierarkiaa. (G. D. kohta 99)

QdN-ratkaisussaan unionin tuomioistuin on siis vahvistanut yleisen edun mukaisten tavoitteiden (rikollisuuden torjunta, yleiseen turvallisuuteen kohdistuvien uhkien torjunta ja kansallinen turvallisuus) välille suhteellisuusperiaatteen mukaisen hierarkian. Erityisesti kansallisen turvallisuuden takaamista koskeva tavoite on tärkeämpi kuin nämä muut sähköisen viestinnän tietosuojadirektiivin 15 artiklassa tarkoitetut muut tavoitteet. Kansallisen turvallisuuden takaamista koskevalla tavoitteella voidaan näin ollen oikeuttaa toimenpiteitä, joilla puututaan perusoikeuksiin vakavammin kuin toimenpiteillä, jotka voitaisiin oikeuttaa näillä muilla tavoitteilla. (QdN kohdat 135–136) 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) Vastaavasti taas vakavan rikollisuuden torjunta ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen ovat yleisen edun mukaisten tavoitteiden hierarkiassa tärkeämpiä kuin rikosten torjuminen yleensä ja yleiseen turvallisuuteen kohdistuvien muiden kuin vakavien uhkien ehkäiseminen. (A. G. kohta 38) Vain sellaiset puuttumiset mainittuihin perusoikeuksiin, jotka eivät ole vakavia, voidaan oikeuttaa rikosten torjuntaa, tutkintaa, selvittämistä ja syyteharkintaa yleisesti koskevalla tavoitteella. (G. D. kohta 59)

Unionin tuomioistuin on katsonut, että direktiivin 15 artiklan soveltamisalaan kuuluu paitsi lainsäädännöllinen toimenpide, jossa sähköisten viestintäpalvelujen tarjoajat velvoitetaan säilyttämään liikenne- ja paikkatiedot, myös lainsäädännöllinen toimenpide, jossa ne velvoitetaan antamaan toimivaltaisille kansallisille viranomaisille oikeus saada näitä tietoja. (Tele2 kohta 76; Privacy International kohta 39) Yllä esitetty yleisen edun mukaisten tavoitteiden hierarkiasta soveltuu soveltuvin osin sellaisten liikenne- ja paikkatietojen myöhempään käyttöön, joita sähköisten viestintäpalvelujen tarjoajat ovat säilyttäneet vakavan rikollisuuden torjumiseksi toteutetun toimenpiteen

perusteella. Tällaisia tietoja ei nimittäin voida sen jälkeen, kun niitä on säilytetty ja annettu toimivaltaisten viranomaisten käyttöön vakavan rikollisuuden torjumiseksi, välittää muille viranomaisille eikä käyttää korruptiota muistuttavien virkavirheiden torjumisen kaltaisten sellaisten tavoitteiden saavuttamiseksi, jotka ovat yleisen edun mukaisten tavoitteiden hierarkiassa alempana kuin vakavan rikollisuuden torjunta ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen. (A. G. kohta 41) Saatujen tietojen käyttö kuuluu rikosasioiden tietosuojadirektiivin 2016/680 soveltamisalaan. (Spetsializirana prokuratura (Bulgaria) kohta 68)

Kun säilytysvelvollisuudesta säädetään, on yleisten edun mukaisten tavoitteiden lisäksi otettava huomioon 15(1) artiklan yleiset edellytykset ***välttämättömyydestä, asianmukaisuudesta ja oikeasuhtaisuudesta***[60]. Niiden on unionin tuomioistuimen oikeuskäytännössä katsottu sisältävän seuraava ehdot ja takeet:

1. **Yleisen edun mukainen tavoite on tasapainotettava kyseessä olevien oikeuksien kanssa**. Yksityiselämän kunnioittamista koskevan perusoikeuden suoja edellyttää, että poikkeukset henkilötietojen suojaan ja sitä koskevat **rajoitukset toteutetaan täysin välttämättömän rajoissa**.

    1.1. Rajoittaminen on arvioitava mittaamalla tällaiseen rajoittamiseen sisältyvän puuttumisen vakavuus ja tarkastamalla, että kyseisen rajoituksen yleisen edun mukaisen tavoitteen tärkeys on oikeassa suhteessa tähän vakavuuteen. (QdN 130 ja 131 kohta)

    1.2. Yleisen edun mukaisten tavoitteiden välillä vallitsee niiden tärkeyteen perustuva hierarkia. (G. D. kohta 56)

2. Kun säädetään **säilyttämisvelvollisuudesta**, kansallisessa säännöstössä on säädettävä selvistä ja täsmällisistä toimenpiteen laajuutta ja soveltamista koskevista säännöistä.

    2.1. Kyseisen säännöstön on oltava kansallisen oikeuden mukaan laillisesti sitova. (Tele2 kohta 117)

    2.2. Säännöstössä on asetettava vähimmäisvaatimukset, jotta henkilöillä joiden henkilötiedoista on kyse, on riittävät takeet, joiden avulla heidän henkilötietojaan voidaan tehokkaasti suojata väärinkäytön vaaroilta. (Tele2 kohta 109)

[60] Lisäksi on otettava huomioon perusoikeuksien yleiset rajoitusedellytykset, joita on käsitelty edellä, vaikka tässä esitetyt vaatimukset ovat osittain sisäkkäisiä niiden kanssa.

2.2.1. Säännöstössä on erityisesti mainittava, missä olosuhteissa ja millä edellytyksin tällaisten tietojen käsittelyä koskeva toimenpide voidaan toteuttaa. (Tele2 kohta 109)

2.2.2. Tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti, etenkin, kun on olemassa huomattava näiden tietojen lainvastaista saantia koskeva vaara. Nämä näkökohdat pätevät erityisesti silloin, kun on suojattava kyseistä henkilötietojen erityisryhmää eli arkaluonteisia tietoja. (QdN kohta 132)

2.3. Tietojen säilyttämisen on aina oltava sellaisten objektiivisten perusteiden mukaista, joilla luodaan yhteys säilytettävien tietojen ja asetetun tavoitteen välille. (Tele2 kohta 110)

2.3.1. Erityisesti vakavan rikollisuuden torjunnan osalta tietojen, joiden säilyttämisestä säädetään, on oltava omiaan edistämään vakavien rikosten torjuntaa tai selvittämistä tai syyteharkintaa. (G. D. kohta 55)

2.4. Aineellisten edellytysten on erityisesti oltava käytännössä sellaisia, että niissä rajataan tehokkaasti toimenpiteen laajuus ja tätä kautta asianomainen yleisö. (Tele2 kohta 110)

2.4.1. Asianosaisen yleisön toiminnan on voitava olla edes epäsuorasti tai kaukaisesti yhteydessä asetettuun tavoitteeseen. (Tele2 kohta 105, QdN kohta 137)

2.4.2. Aineelliset edellytykset voivat vaihdella vakavan rikollisuuden ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa koskevien toimenpiteiden mukaan. (Tele2 kohta 110)

2.5. Kohdennettu säilytysvelvollisuus ei saa olla syrjivä. (QdN kohta 150)

2.5.1. Nämä näkökohdat pätevät erityisesti silloin, kun on suojattava kyseistä henkilötietojen erityisryhmää eli arkaluonteisia tietoja. (QdN kohta 132)

3. Kun säädetään **viranomaisen oikeudesta saada välitystietoja**, on myös säädettävä aineellisista ja menettelyllisistä kyseistä käyttöä koskevista edellytyksistä.

3.1. Kyseisen säännöstön on oltava kansallisen oikeuden mukaan sitova. (Tele2 kohta 117)

3.2. Säännöstössä ei voida tyytyä vaatimaan, että viranomaisten oikeus saada tietoja vastaa kyseisen säännöstön tarkoitusta, vaan kansallisessa säännöstössä on säädettävä myös aineellisista ja menettelyllisistä edellytyksistä, joilla toimivaltaiset kansalliset viranomaiset voivat saada säilytettyjä tietoja. (Tele2 kohta 118, Privacy International kohta 77)

3.2.1. 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)

3.2.2. Näiden on perustuttava objektiivisille kriteereille niiden olosuhteiden ja edellytysten määrittelemiseksi, joilla toimivaltaisille kansallisille viranomaisille on annettava oikeus saada kyseessä olevia tietoja (PI kohta 78). Oikeus saada välitystietoja voidaan lähtökohtaisesti myöntää rikollisuuden torjumisen tavoitteen yhteydessä vain sellaisten henkilöiden tietoihin, joiden epäillään suunnittelevan, tekevän tai tehneen vakavan rikoksen tai olevan jollakin tavalla mukana tällaisessa rikoksessa. Erityisissä tilanteissa, kuten niissä, 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 konkreettisessa tapauksessa tosiasiallisesti myötävaikuttaa tällaisen toiminnan torjumiseen. (Tele2 kohta 119)

3.2.3. Tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti, etenkin, kun on olemassa huomattava näiden tietojen lainvastaista saantia koskeva vaara. (Privacy International kohta 68)

3.2.4. Silloin kun taustalla on (sallittu) yleinen ja erotukseton säilyttäminen, hyödyntämistä (muun muassa jäljittäminen) koskevien takeiden ja edellytysten on oltava tiukkoja. (QdN kohta 156)

3.3. Tietojen saannin edellytyksenä on tuomioistuimen tai riippumattoman hallintoviranomaisten suorittama ennakkovalvonta.[61] (Tele2 kohta 120)

[61] Kiireellisissä tapauksissa jälkikäteinen valvonta on sallittu.

3.3.1. Kyseisen tuomioistuimen tai elimen ratkaisu annetaan perustellusta pyynnöstä, jonka viranomaiset esittävät rikoksen estämis-, selvittämis- tai syyteharkintamenettelyssä. (Tele2 kohta 120)

3.3.2. Etukäteisvalvonta edellyttää muun muassa sitä, että sen suorittamisesta vastaavalla tuomioistuimella tai riippumattomalla hallintoelimellä on kaikki valtuudet ja kaikki takeet, jotka ovat välttämättömiä sen varmistamiseksi, että kyseessä olevat eri legitiimit intressit ja oikeudet sovitetaan yhteen. Tarkemmin ottaen rikostutkinnan osalta tällainen valvonta edellyttää sitä, että kyseinen tuomioistuin tai elin pystyy turvaamaan oikeudenmukaisen tasapainon yhtäältä rikollisuuden torjumiseksi tehtävän tutkinnan tarpeisiin liittyvien legitiimien intressien ja toisaalta henkilöiden, joita tietojensaanti koskee, yksityiselämän kunnioittamista ja henkilötietojen suojelua koskevien perusoikeuksien välillä. (Prokuratuur kohta 52)

3.3.3. Siinä tapauksessa, että kyseisen valvonnan suorittaa tuomioistuimen sijaan riippumaton hallinnollinen elin, kyseisellä elimellä on oltava asema, jossa se voi suorittaa tehtävänsä objektiivisesti ja puolueettomasti, ja sen on tätä varten oltava suojattu kaikelta ulkopuoliselta vaikuttamiselta. Niinpä riippumattomuutta koskeva vaatimus, joka etukäteisvalvonnasta vastaavan viranomaisen on täytettävä, edellyttää sitä, että kyseinen viranomainen on ulkopuolinen siihen viranomaiseen nähden, joka pyytää kyseisten tietojen saantia, jotta ensiksi mainittu voi suorittaa valvonnan objektiivisesti ja puolueettomasti suojattuna kaikelta ulkopuoliselta vaikuttamiselta. Erityisesti rikosasioissa riippumattomuuden vaatimus tarkoittaa, että tästä etukäteisvalvonnasta vastaava viranomainen ei yhtäältä osallistu kyseisen rikostutkinnan suorittamiseen ja toisaalta on neutraalissa asemassa rikosprosessin asianosaisiin nähden. (Prokuratuur kohdat 53 ja 54)[62]

[62] Unionin tuomioistuin on katsonut muun muassa, että tutkintaa johtavaa syyttäjäviranomaista, joka tarvittaessa ajaa syytettä, ei voida pitää ulkopuolisena kyseessä oleviin legitiimeihin intresseihin nähden, koska tämän tehtävänä ei nimittäin ole ratkaista asiaa täysin riippumattomasti vaan saattaa se tarvittaessa toimivaltaisen tuomioistuimen käsiteltäväksi syytettä ajavana asianosaisena oikeudenkäynnissä. Näin ollen tällainen syyttäjäviranomainen ei voi suorittaa säilytettyjen tietojen saantia koskevien pyyntöjen ennakkovalvontaa (Prokuratuur 55 ja 57 kohta). Unionin oikeus on myös esteenä kansalliselle lainsäädännölle, jonka nojalla poliisin vakavien rikosten tutkinnan ja syytetoimien yhteydessä esittämien, sähköisten viestintäpalvelujen tarjoajien säilyttämien tietojen saantia koskevien pyyntöjen keskitetty käsittely kuuluu poliisivirkamiehelle, jota avustaa poliisin sisäinen yksikkö, jolla on tietty itsenäisyys tehtäväänsä suorittaessaan, ja jonka päätökset voivat myöhemmin olla tuomioistuinvalvonnan kohteena. (G.D. 114 kohta)

3.3.4. Kansallisen sääntelyn on täytettävä perusoikeuskirjan 47 artiklan vaatimukset eli tuomioistuimen tai riippumattoman viranomaisen päätös on esimerkiksi perusteltava. (HYA e.a. kohta 43, 44 ja 46)

3.4. Tietojen saannin on tapahduttava täysin välttämättömän rajoissa (Tele2 kohta 116) suhteessa säilytyksen tarkoitukseen, mikä on varmistettava kansallisessa lainsäädännössä selvin ja täsmällisin säännöksin. (Spetsializirana prokuratura (Bulgaria) kohta 65) Toimivaltaisten 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)

3.5. On myös tärkeää, että toimivaltaiset kansalliset viranomaiset, joille on annettu oikeus saada säilytettyjä tietoja, tiedottavat tästä asianomaisille henkilöille sovellettavien kansallisten menettelyjen mukaisesti heti, kun tämä tiedoksianto ei vaaranna kyseisten viranomaisten suorittamia tutkimuksia. (Tele2 kohta 121)

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

3.5.2. Säilytettävien tietojen käyttö rikostutkinnassa kuuluu rikosasioiden tietosuojadirektiivin[63] soveltamisalaan, jonka 13 artiklan mukaisesti jäsenvaltiot voivat säätää rekisteröidyn informoinnista. Unionin tuomioistuin kuitenkin toteaa, että kyseinen lainkohta ei mahdollista tietojensaantioikeuden rajaamista kokonaan pois. (Spetsializirana prokuratura (Bulgaria) kohdat 68–71)

3.5.3. Oikeudesta tehokkaisiin 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 ainoas-

[63] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta.

taan 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 (Bulgaria) kohdat 72–75)

3.6. Oikeus saada tietoja voidaan myöntää ainoastaan, jos palveluntarjoajat ovat säilyttäneet kyseisiä tietoja tavalla, joka on yhteensopiva sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohdan kanssa. (Prokuratuur kohta 29)

4. Säilytettävän tiedon asiamukainen **suojaaminen** ja säilytyksen rajoittaminen

4.1. Sähköisten viestintäpalvelujen tarjoajien on mainittujen tietojen täyden koskemattomuuden ja luottamuksellisuuden takaamiseksi varmistettava erityisen korkea suojan ja turvan taso turvautumalla asianmukaisiin teknisiin ja organisatorisiin toimiin. (Tele2 kohta 122)

4.2. Kansallisessa säännöstössä on erityisesti säädettävä tietojen säilyttämisestä unionin alueella ja tietojen lopullisesta hävittämisestä, kun niiden säilyttämisaika päättyy. (Tele2 kohta 122)

4.3. Tietojen saannille asetetut rajoitukset eivät voi rajoittaa tai korjata tietojen yleisestä säilyttämisestä johtuvaa vakavaa puuttumista yksilön oikeuksiin. (G. D. kohta 47)

4.3.1. Tämä koskee myös kansallisessa lainsäädännössä asetettuja takeita, joilla säilytettyjä tietoja pyritään suojaamaan tietojen väärinkäyttöä ja lainvastaista saantia koskevilta vaaroilta. (SpaceNet kohta 91)

4.3.2. Tietosuojaviranomaisen tai parlamentaarisen elimen suorittama säilyttämiseen kohdistuva valvonta, vaikkakin vähentää luvattoman pääsyn riskiä, ei poista itse säilyttämisestä aiheutuvaa riskiä yksilön perusoikeuksiin. (Spetsializirana prokuratura (Bulgaria) kohta 59)

5. Jäsenvaltioiden on taattava, että riippumaton viranomainen valvoo unionin oikeudessa taatun suojan tason noudattamista luonnollisten henkilöiden henkilötietojen käsittelyssä. (Tele2 kohta 123)

6. 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. (VD ja SR kohdat 79 ja 82)

3.4 Yleisen tietosuoja-asetuksen reunaehdot

Sähköisen viestinnän tietosuojadirektiivin täsmentää ja täydentää EU:n yleistä tietosuoja-asetusta.[64] Henkilötietojen käsittelyyn sovelletaan yleistä tietosuoja-asetusta siltä osin kuin sähköisen viestinnän tietosuojadirektiivi ei sisällä asetusta täsmentävää erityissääntelyä. Oikeuskirjallisuudessa on todettu, että henkilötietoina pidettävien välitystietojen käsittelyn on oltava sähköisen viestinnän tietosuojadirektiivin mukaista, jotta se olisi myös tietosuoja-asetuksen mukaista.[65]

Kaikki yritykset, joille säilytysvelvollisuus voitaisiin asettaa, eivät välttämättä kuulu sähköisen viestinnän tietosuojadirektiivin soveltamisalaan, vaan niiden käsittelyyn sovellettaisiin yleistä tietosuoja-asetusta. Tällaisia yrityksiä voivat olla esimerkiksi tietyt hosting-palvelut. Yleisen tietosuoja-asetuksen soveltamisalalla henkilötietojen käsittelyyn sovelletaan suoraan asetuksen säännöksiä. Asetus jättää kuitenkin eräissä asioissa lainsäätäjälle liikkumavaraa antaa asetusta täydentävää ja täsmentävää sääntelyä. Liikkumavaraa sisältävät säännökset eivät joitakin poikkeuksia lukuun ottamatta velvoita jäsenvaltioita säätämään tietosuoja-asetusta täydentävää lainsäädäntöä, vaan asia on yleensä jätetty kansallisen lainsäätäjän harkintaan. Koska asetus on suoraan sovellettava ja yksityiskohtainen säädös, kansallisen liikkumavaran käyttöön on suhtauduttava pidättyvästi.

Perustuslakivaliokunnan mukaan tietosuoja-asetuksen yksityiskohtainen sääntely, jota tulkitaan ja sovelletaan EU:n perusoikeuskirjassa turvattujen oikeuksien mukaisesti, muodostaa yleensä riittävän säännöspohjan myös perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta. Henkilötietojen suoja tulee turvata ensisijaisesti EU:n yleisen tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla. Kansallisen erityislainsäädännön säätämiseen tulee siten suhtautua pidättyvästi ja rajata sellainen vain välttämättömään tietosuoja-asetuksen salliman kansallisen liikkumavaran puitteissa. (ks. PeVL 14/2018 vp, s. 4–5 ja PeVL 52/2022 vp, 4 kohta) Perustuslakivaliokunnan mukaan on kuitenkin selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksenkin edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä suurempi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn osalta. (ks. PeVL 14/2018 vp, s. 5) Perustuslakivaliokunnan mielestä arkaluonteisten tietojen käsittelyä koskevaa sääntelyä on sanotun johdosta, tietosuoja-asetuksen mahdollistamissa puitteissa,

[64] Direktiivin 1(2) artikla, ks. EU:n tietosuojaneuvoston lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta.
[65] Marko Priiki, Sähköisen viestinnän välitystietojen ja henkilötietojen käsittelyperusteiden suhteesta – kansallinen lainsäädäntö suoraan sovellettavan tietosuoja-asetuksen aikana. Oikeustiede - Jurisprudentia LVI:2023 s. 213–303, 261.

edelleen syytä arvioida myös aiemman sääntelyn lakitasoisuutta koskevan käytännön pohjalta. (ks. PeVL 14/2018 vp, s. 6) Arkaluonteisten tietojen käsittelyn on oltava välttämätöntä ja sääntelyn täsmällistä ja tarkkarajaista. (ks. PeVL 52/2022 vp, 7 kohta)

Tietosuoja-asetuksen soveltamisalalla sääntelyliikkumavaraa sisältyy ennen muuta tilanteisiin, joissa henkilötietojen käsittely perustuu yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan c tai e alakohtiin, eli käsittely perustuu rekisterinpitäjän lakisääteisen velvoitteen noudattamiseen tai on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Jäsenvaltioilla on tällöin 6 artiklan 2 ja 3 kohdassa tarkoitettua sääntelyliikkumavaraa antaa asetusta täydentävää sääntelyä edellyttäen, että se on yleisen edun tavoitteen mukaista sekä oikeasuhteista sillä tavoiteltuun oikeutettuun päämäärään nähden. Tietosuoja-asetusta täsmentävä sääntely voi koskea muun muassa käsiteltäviä henkilötietoja ja niiden käyttötarkoituksia, henkilötietojen säilyttämistä ja poistamista sekä tietojen luovuttamisesta. Tietosuoja-asetuksen 6 artiklan ohella sääntelyliikkumavaraa liittyy myös asetuksen 10 artiklaan, jossa säädetään rikoksiin, rikostuomioihin ja niihin liittyviin turvaamistoimiin liittyvien tietojen käsittelystä ja käsittelyä koskevista reunaehdoista. Tietosuoja-asetuksen 10 artiklan mukaan kyseisten henkilötietojen käsittely on sallittua ainoastaan asetuksen 6 artiklan 1 kohdan perusteella viranomaisen valvonnassa tai silloin, kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa säädetään asianmukaisista suojatoimista rekisteröidyn oikeuksien ja vapauksien suojelemiseksi. Kattavaa rikosrekisteriä pidetään vain julkisen viranomaisen valvonnassa.

Tietosuoja-asetuksen 23 artikla mahdollistaa lisäksi, että unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan tietyin reunaehdoin lainsäädäntötoimenpiteellä rajoittaa niiden velvollisuuksien ja oikeuksien soveltamisalaa, joista säädetään 12–22 artiklassa ja 34 artiklassa sekä 5 artiklassa, siltä osin kuin sen säännökset vastaavat 12–22 artiklassa säädettyjä oikeuksia ja velvollisuuksia, jos kyseisessä rajoituksessa noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia ja rajoitus on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide. Rajoituksista säätäminen ovat mahdollista ainoastaan asetuksessa määriteltyjen tavoitteiden (kuten kansallinen turvallisuus, puolustus, yleinen turvallisuus tai rikostorjunta) turvaamiseksi. Tietosuoja-asetuksen 23 artikla edellyttää lisäksi, että jäsenvaltion lainsäädännössä säädetään tarpeellisista erityisistä säännöksistä koskien muun muassa käsiteltäviä henkilötietoja, niiden käyttötarkoituksia, rajoitusten soveltamisalaa, säilytysaikoja sekä suojatoimia, joilla estetään väärinkäyttö tai lainvastainen pääsy tietoihin.

Hosting-palveluiden osalta säilytysvelvollisuudesta ja tietosuoja-asetuksen 12–22, 34 tai 5 artiklassa säädettyjen oikeuksien ja velvollisuuksien rajoittamisesta voitaisiin säätää asetuksen 6 ja 23 artiklan nojalla, mikäli asetuksessa säädetyt reunaehdot täyttyvät. Kansallisen liikkumavaran reunaehdot vaikuttavat vastaavanlaisilta kuin sähköisen viestinnän tietosuojadirektiivin nojalla. Vastaavasti kuin sähköisen viestinnän tietosuojadirektiivin 15 artiklassa, tietosuoja-asetuksen 23 artiklan mahdollistamat

rajoitukset ovat mahdollisia vain tiettyjen ennalta määriteltyjen tavoitteiden takaamiseksi ja vain siltä osin kuin ne ovat välttämättömiä ja oikeasuhteisia, edellyttäen, että niissä noudatetaan keskeisiltä osin perusoikeuksia ja -vapauksia. Unionin tuomioistuin on katsonut, että sen sähköisen viestinnän tietosuojadirektiivistä esittämiä toteamuksia ja arviointeja sovelletaan soveltuvin osin tietosuoja-asetuksen 2016/679 23 artiklaan. (QdN kohta 211–212) Tämä perustuu siihen, että unionin tuomioistuimen käytäntö ankkuroituu perusoikeuskirjaan. (QdN kohta 210)

4. Kansainvälinen vertailu

Välitystietojen säilyttämisvelvollisuutta ei ole harmonisoitu EU-tasolla sen jälkeen, kun unionin tuomioistuin kumosi vuonna 2006 annetun direktiivin[66] sillä perusteella, ettei se ollut suhteellisuusperiaatteen mukainen vaan sillä puututtiin liikaa Euroopan unionin perusoikeuskirjassa turvattuihin yksityiselämän suojaan ja henkilötietojen suojaan.[67]

Unionin tuomioistuimen oikeuskäytännön seurauksena useat jäsenmaat ovat muuttaneet kansallista lainsäädäntöä. Esimerkiksi Belgia, Irlanti ja Tanska ovat säätäneet kansallisissa lainsäädännöissään mahdollisuudesta toteuttaa säilytystoimenpiteitä, joita unionin tuomioistuin on ratkaisuissaan käsitellyt. Lisäksi Ruotsissa on valmistunut kesällä 2023 selvitys välitystietojen säilyttämisvelvollisuudesta. Ruotsin selvitys sisältää ehdotuksia kansallisen lainsäädännön uudistamiseksi unionin tuomioistuimen ratkaisuiden perusteella. Lisäksi on huomattava, että kaikissa EU-jäsenmaissa, kuten Portugalissa ja Alankomaissa, ei ole voimassa olevaa lainsäädäntöä välitystietojen säilyttämisvelvollisuudesta.

Edellisten vuosien aikana keskusteluun on noussut mahdollisuus ja tarve harmonisoida jälleen säilytysvelvollisuutta EU-tasolla. Komission tiedonannossa järjestäytyneen rikollisuuden torjunnan strategiaksi 2021-2025 (COM(2021) 170 final) mukaan komissio aikoo analysoida ja hahmotella mahdollisia tietojen säilyttämisen toimintamalleja arvioituaan EU-tuomioistuimen oikeuskäytäntöä ja konsultoituaan jäsenvaltioita asiassa. Toistaiseksi ei ole tiedossa, millaisia toimenpiteitä komission hahmottelemat ratkaisut voisivat sisältää ja voisivatko ne tarkoittaa uutta EU-tasoista sääntelyä säilytysvelvollisuuksien harmonisoimiseksi. EU-tason keskustelut aiheesta ovat siirtyneet alkuvuonna 2023 perustettuun korkean tason ryhmään, jonka tehtävänä on tarkastella lainvalvontaviranomaisten kohtaamia haasteita pääsyssä digitaalisiin ja sähköisiin tietoihin (ns. *High-Level Group on Access to Data for Effective Law Enforcement*). Kyseisen ryhmän tehtävänä on tunnistaa viranomaisten kohtaamat haasteet ja kehittää ehdotuksia näiden haasteiden ratkaisemiseksi. Suomi osallistuu korkean tason ryhmään, ja työryhmässä käydyissä keskusteluissa tarve EU-tason sääntelylle säilytysvelvollisuuden harmonisoimiseksi on ollut vahvasti esillä. Ryhmän johtopäätökset kootaan loppuraportiksi, joka valmistuu aikaisintaan kesällä 2024.

---

[66] Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta.
[67] Yhdistetyt asiat C-293/12 ja C-594/12 Digital Rights Ireland, 8.4.2014, ECLI:EU:C:2014:238.

Seuraavaksi käsitellään Ruotsin ehdotusta sekä Belgian, Irlannin ja Tanskan kansallista sääntelyä, jolla unionin tuomioistuimen ratkaisukäytännössään erittelemiä säilytystoimenpiteitä on otettu käyttöön. Lisäksi alla kuvataan muiden Pohjoismaiden ja Saksan kansallisen lainsäädännön ja sen mahdollisen tarkastelun tilanne.

Vertailun perusteella voidaan todeta, että jäsenvaltiot ovat ottaneet käyttöön erityyppisiä velvoitteita. Jäsenvaltioiden näkemykset säilytyksen kohdentamisesta ja välttämättömyydestä näyttävät eroavan toisistaan. Tämä voi osin selittyä poliittisella tahdolla tai lainmuutosprosessin hitaudella, osin jäsenvaltiokohtaisilla erityispiirteillä, joita vasten esimerkiksi toimenpiteen välttämättömyyttä kansallisesti arvioidaan.

Ruotsi

Ruotsin kansalliseen lainsäädäntöön on tehty muutoksia Tele2-tuomion jälkeen. Unionin tuomioistuimen mukaan liikenne- ja paikkatietojen yleinen ja erotukseton säilyttäminen ennakoivasti sallittuja perusteita varten on kielletty (TS kohta 112). Ratkaisussa unionin tuomioistuin katsoi, että Ruotsin silloisen lainsäädännön mukainen säilyttämisvelvollisuus oli yleistä ja erotuksetonta, sillä se kattoi kaikkien perinteisten teleoperaattoreiden tarjoamat puhelin-, viestintä- ja laajakaistapalvelut, ja siten siis unionin oikeuden vastaista. Ratkaisun jälkeen uusi lainsäädäntö astui voimaan lokakuussa 2019. Tällöin lainsäädäntöä muutettiin siten, että esimerkiksi säilytysvelvollisuutta rajattiin tuomioistuimen ratkaisun perusteella ja säilytysaikoja eriytettiin. Säilytysvelvollisuudesta on säädetty laissa sähköisestä viestinnästä (*Lagen (2022:482) om elektronisk kommunikation*).

Tele2-tuomion jälkeistä unionin oikeuskäytäntöä ja sen vaikutuksia on arvioitu toukokuussa 2023 valmistuneessa selvityksessä *Datalagring och åtkomst till elektronisk information (SOU 2023:22)*[68]. Selvityksessä ehdotetaan uutta lainsäädäntöä tietojen säilytysvelvollisuudeksi kansallisen turvallisuuden turvaamiseksi sekä ns. kohdennettua säilyttämistä vakavan rikollisuuden torjumiseksi.

Kansallisen turvallisuuden takaamiseksi ehdotus sisältäisi mahdollisuuden määrätä yleinen ja erotukseton tietojen säilyttämisvelvollisuus. Suojelupoliisi (*Säkerhetspolisen, Säpo*) voisi vahvistaa kansalliseen turvallisuuteen kohdistuvan uhan ja tällaisen uhan ollessa päällä päättää yleisestä ja erotuksettomasta tietojen säilyttämisvelvollisuudesta. Kansalliseen turvallisuuteen perustuva säilyttämisvelvollisuus olisi nykyistä lainsäädäntöä laajempi sekä säilytettävien tietojen että säilytysaikojen osalta. Säily-

[68] Statens offentliga utredgningar 2023:22, saatavilla https://www.riksdagen.se/sv/dokument-och-lagar/dokument/statens-offentliga-utredningar/sou-2023-22-_hbb322

tysmääräyksen kesto olisi rajoitettu uhan olemassa oloon, mutta se olisi rajoitettu korkeintaan vuoteen. Säilytysaika olisi kaksi vuotta, pääsääntöisesti alkaen viestinnän ajankohdasta.

Säpon päätöksiä valvomaan perustettaisiin turvallisuus- ja tietosuojaviranomaiseen (*Säkerhets- och integritetsskyddsnämnden, SIN*) uusi erillinen elin (*Datalagringsdelegationen*). Pääsy kansallisen turvallisuuden perusteella säilytettäviin tietoihin rajattaisiin koskemaan sellaisen rikollisuuden torjumista, johon liittyy vakava uhka Ruotsin turvallisuudelle. Päätös kansalliseen turvallisuuteen perustuvasta säilyttämisvelvollisuudesta on salassapidettävä (*omfattas av sekretess*) ja palveluntarjoajia koskee vaitiolovelvollisuus.

Vakavan rikollisuuden torjumiseksi ehdotettaisiin uutta sääntelyä, johon kuuluisi maantieteellisesti kohdennettu ja ns. laajennettu säilyttäminen. Maantieteellisesti kohdennettu säilyttäminen toteutettaisiin alueella, jossa objektiivisten kriteerien perusteella todetaan olevan korkeampi todennäköisyys vakavaan rikollisuuteen kuin muilla alueilla. Maantieteellinen kohdentaminen perustuisi virallisiin tilastoihin ilmoitetuista rikoksista. Säilytyskohteen alueellisia yksiköitä olisivat kunnat. Ruotsin posti- ja televiranomainen *Post- och telestryrelsen* määräisi vuosittain ne kunnat, joiden alueella säilytysvelvollisuus on voimassa.

Selvityksessä on arvioitu vuosien 2020–2022 mukaisten tilastojen mahdollista säilyttämisvelvollisuuden laajuutta. Selvityksessä ehdotettavan laskutavan mukaan maantieteellisesti kohdennettu säilytysvelvollisuus kattaisi 132 kuntaa maan 290 kunnasta, mikä kattaisi noin 7,3 miljoonan asukkaan tiedot koko maan noin 10,4 miljoonasta asukkaasta.[69] Vakavan rikollisuuden todennäköisyys tarkasteltavalla alueella laskettaisiin tietyssä kunnassa ilmoitettujen rikosten lukumäärän aritmeettisena keskiarvona kolmen edeltävän vuoden ajalta, jolta tilastot ovat saatavissa. Kuntien vaihtelevat asukasmäärät otettaisiin huomioon siten, että rikosten lukumäärä suhteutettaisiin tuhanteen asukkaaseen.[70]

Laajennettu säilyttäminen täydentäisi maantieteellisesti kohdennettua säilyttämistä. Tämä koskisi rajattua maantieteellistä aluetta, jolla on tapahtunut vakava rikos tai jossa todennäköisesti tapahtuu vakavaa rikollisuutta sekä suojeltavia paikkoja. Lisäksi se voitaisiin kohdistaa henkilöön, joka on tuomittu vakavasta rikoksesta tai joka on ollut salaisten pakkokeinojen kohteena, sekä laitteeseen tai tilaajatietoon, jota on käytetty tai jota voidaan kohtuudella olettaa käytettävän vakavaan rikokseen.

[69] SOU 2023:22 s. 261. Selvityksen mukaan siinä ehdotetut raja-arvot eivät olisi ongelmallisia suhteellisuusperiaatteen näkökulmasta, sillä säilytysvelvollisuus kattaisi alle puolet maan pinta-alasta, ks. s. 260.
[70] SOU 2023:22 s. 259-260.

Laajennetusta tietojen säilyttämisestä päättäisi poliisi, Säpo tai tulliviranomainen. Soveltamisen valvonnasta vastaisi SIN. Maantieteellisesti kohdennettu säilyttäminen kattaisi vähemmän tietoja kuin nyt voimassa oleva säilytysvelvollisuus. Myös laajennettua säilyttämistä koskevat päätökset olisivat luottamuksellisia ja palveluntarjoajia koskee vaitiolovelvollisuus.

Vakavan rikollisuuden torjumiseen tarkoitettujen kohdennettujen säilytysvelvollisuuksien mukainen tietojen säilytysaika olisi yksi vuosi, pääsääntöisesti laskien viestintäajankohdasta. Säilytysaikaa pidennettäisiin nykyisistä käytännöistä. Pidempää säilytysaikaa on perusteltu sillä, että vaikka nykyisiä säilytysaikoja valmisteltaessa tunnistettiin, että suurin osa tietopyynnöistä kohdistuu alle viiden kuukauden ikäisiin tietoihin, niin kokonaiskuvan muodostamiseksi tietoja tarvitaan pidemmältä ajalta. Taustalla vaikuttaa esimerkiksi vakavan rikollisuuden määrän lisääntyminen sekä viestinnän siirtyminen perinteisistä viestintäkanavista internetiin. Näitä rikoksia voi olla vaikea havaita, tutkinta on monimutkaista ja niihin osallistuu monia toimijoita. Rikosten kansainvälinen ulottuvuus lisää myös tarvetta pidemmälle tutkinta-ajalle. Joissakin tapauksissa voi kestää pitkään, ennen kuin lainvalvontaviranomaiset saavat pääsyn tietoihin.[71]

Lisäksi selvitykseen sisältyy ehdotus säilytysvelvollisuuden ulottamisesta yleisten numeroista riippumattomien henkilöiden välisten viestintäpalveluiden tarjoajiin (ns. Over-the-Top –palvelut, OTT-palvelut). Säilytysvelvollisuus koskisi viestintää, joka jossain määrin tapahtuu Ruotsissa. Tämä tarkoittaisi esimerkiksi viestintää, joka lähetetään tai vastaanotetaan Ruotsissa sijaitsevan IP-osoitteen kautta. Säilytysvelvollisuus vastaisi kestoltaan ja laajuudeltaan muille säilytysvelvollisille ehdotettuja toimenpiteitä.

Tanska

Tanskan välitystietojen säilyttämisvelvollisuutta sääntelevää kansallista lainsäädäntöä on muutettu QdN-ratkaisun jälkeen. Uudistuksella muutettiin Tanskan oikeudenkäymiskaarta (*Lov om rettens pleje tai retsplejeloven*) ja televiestintälakia (*Teleloven*). Uudistettu lainsäädäntö tuli voimaan 30.3.2022. Uusi lainsäädäntö mahdollistaa 1) yleisen ja erotuksettoman säilyttämisen kansallisen turvallisuuden tarpeisiin; 2) maantieteellisten ja henkilöpiirin perusteella kohdennetun säilyttämisen vakavan rikollisuuden torjumiseksi; sekä 3) yleisen ja erotuksettoman IP-osoitteiden säilyttämisen. Tietoja säilytetään vuoden ajan.

Yleinen ja erotukseton säilyttäminen on mahdollista, mikäli riittävän konkreettiset seikat osoittavat, että on olemassa vakava uhka Tanskan kansalliselle turvallisuudelle ja se osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi (vastaa-

[71] SOU 2023:22 s. 310-311.

vasti ks. QdN tuomio kohta 137). Uhan olemassa olon vahvistaa oikeusministeri perustuen turvallisuus- ja tiedusteluviranomaisten tietoihin, viranomaisjulkaisuihin sekä tietoihin tietyistä rikoksista, kuten vakoilu ja terrorismi. Tietojen tallentamisen velvoite on korkeintaan yksi vuosi, ja tietoja tulee säilyttää vuoden ajan viestintäajankohdasta. Säilyttämisvelvollisuus tuli sovellettavaksi ensimmäistä kertaa samaan aikaan, kun uudistettu laki tuli voimaan vuonna 2022.

Tanskan poliisi (*Rigspolitiet*) voi määrätä teleyritykset säilyttämään tietyn henkilön tai tiettyyn viestintävälineeseen liittyvät viestinnän välitystiedot. Tietyn henkilön tietojen säilytysmääräyksen edellytyksenä on, että toimenpiteen kohde on tuomittu vakavasta rikoksesta eli rikoksesta, joista on mahdollista tuomita yli 3 vuotta vankeutta, tai muista laissa erikseen nimetyistä vakavista rikoksista. Henkilöön kohdistuvan säilytysmääräyksen kesto on porrastettu kolmeen, viiteen tai kymmeneen vuoteen ja se riippuu tuomioon johtaneelle rikokselle säädetystä maksimirangaistuksesta. Säilytysaika on yksi vuosi. Säilytysvelvollisuus alkaa, kun henkilö vapautetaan vankilasta tai ehdollisen rangaistuksen tultua lainvoimaiseksi. Toimenpiteen kohdetta ei tiedoteta asiasta.

Säilytysmääräys voidaan myös kohdistaa laitteeseen, johon liittyviä tietoja on hankittu televalvonnalla (*teleoplysning*) tai henkilöön, jolla on ollut hallussaan tällainen laite. Myös sellaisen laitteen, johon on oltu yhteydessä telekuuntelun kohteena olleesta laitteesta, tiedot voidaan säilyttää. Tällöin edellytyksenä ei ole, että henkilöä olisi syytetty tai tuomittu rikoksesta. Tietoja tallennetaan vuoden ajan telekuuntelun päättymisestä, ja säilytysaika on vuosi tallennushetkestä.

Lisäksi Tanskan poliisi voi määrätä teleyritykset säilyttämään viestinnän välitystietoja tietyillä maantieteellisillä alueilla, joilla on yhteys vakavaan rikollisuuteen. Kiinteiden puhelinlinjojen ja palveluntarjoajien omien internetpuhelinpalveluiden tietoja ei tallenneta. Rikollisuutta tarkastellaan tietyn neliökilometrin perusteella jaoteltujen alueiden perusteella. Alueella katsotaan olevan yhteys vakavaan rikollisuuteen, mikäli alueella on kansalliseen keskiarvoon verrattuna 1,5 kertainen määrä rikosilmoituksia vakavista rikoksista tai alueen asukkaista on tuomittu vakavasta rikoksesta. Kansallinen keskiarvo lasketaan kolmen edellisen vuoden perusteella. Määräys voidaan kohdistaa myös sensitiivistä infrastruktuuria ympäröivään alueeseen tai erityisen turvallisuuskriittiseen alueeseen. Tällaisia alueita ovat esimerkiksi lentokentät, rautatie- ja metroasemat, ja vankilat, tai suurlähetystöjen, armeijan tai kuninkaallisten ja pääministerin asutusten alueet. Säädöksessä ei ole määritelty tallennusajan rajoitusta. Tiedot tulee säilyttää vuoden ajan viestintäajankohdasta.

Teleyritykset voidaan määrätä konkreettisissa tapauksissa säilyttämään tiettyjen viestintälaitteiden, henkilöiden ja maantieteellisten alueiden tiedot, mikäli on syytä uskoa, että niillä on yhteys vakavaan rikollisuuteen. Määräys täydentää yllä esiteltyä säilytysmääräystä, sillä tämä säilyttämisperuste edellyttää jonkin ”tietyn syyn” (*bestemte grunde*), jonka perusteella voidaan olettaa, että tiedot ovat välttämättömiä tutkinnalle. Kynnys on kuitenkin alempi kuin telekuuntelussa, sillä poliisi ei saa tällä määräyksellä

suoraan pääsyä tietoihin. Säilytysmääräys voidaan antaa, mikäli poliisilla on syytä uskoa, että sillä on yhteys vakavan rikollisuuden suunnitteluun. Säilyttämismääräyksen antaa tuomioistuin. Tallennusajan tulee olla mahdollisimman lyhyt eikä se saa ylittää kuutta kuukautta. Määräys voidaan kuitenkin uusia aina kuudeksi kuukaudeksi kerrallaan. Tiedot säilytetään vuoden ajan. Määräyksessä tulee nimetä kohdehenkilö, viestintäväline tai maantieteellinen alue. Toimenpiteen kohteilla on käytettävissään telekuuntelua vastaavat oikeussuojakeinot.

Teleyritysten tulee säilyttää yleisesti ja erotuksetta tiedot internetyhteyden käyttäjistä. Säilytysvelvollisuus ei koske tietoja viestinnästä, vaan kyse on käyttäjän henkilöllisyyttä koskevista tiedoista. Säilytysaika on yksi vuosi.

Norja

Norjan säilytysvelvollisuutta koskeva laki (*Datalagrinsloven*) annettiin vuonna 2011, mutta *Digital Rights Ireland* –ratkaisun antamisen seurauksena kyseinen laki ei tullut koskaan voimaan. Norjassa ei siis ole sovellettu säilyttämisvelvollisuutta koskevaa lainsäädäntöä, mutta kyseistä säädöstä ei myöskään ole kumottu.

Vuonna 2022 Norjassa tuli voimaan laki IP-osoitteiden säilyttämisestä (*Lov om lagring av IP-adresser mv*). Laissa säädetään velvollisuudesta rekisteröidä ja tallentaa IP-osoitteita sekä menettelystä, jolla poliisi voi saada pääsyn näihin tietoihin. Lisäksi siinä säädetään velvoitteesta poistaa tiedot säilytysajan päätyttyä. Säilytysaika on 12 kuukautta viestintätapahtuman päättymisestä. Säilytysvelvollisuus koskee tietoja, joka on tarpeen tilaajan tunnistamiseksi joko a) julkisen IP-osoitteen ja viestintäajankohdan tai b) usean käyttäjän jakaessa saman julkisen IP-osoitteen, myös lähdeportin ja viestintäajankohdan perusteella. Säilytysvelvollisuus koskee lähtevää viestintää, kohdetietoja ei säilytetä. Palveluntarjoajalla on siis velvollisuus ylläpitää rekisteriä henkilöistä, joille tietty IP-osoite (kiinteä tai dynaaminen) on osoitettu tiettynä aikana. Säilytysvelvollisia ovat julkisesti saatavilla olevien sähköisten viestintäpalveluiden tarjoajat sekä käytettyjen viestintäverkkojen tarjoajat. Säilytysvelvollisuuteen ei ole tehty rajoituksia esimerkiksi palveluntarjoajan markkinaosuuden tai koon perusteella.

Islanti

Islannin laissa sähköisistä viestintäpalveluista säädetään, että teleyritysten tulee rikosten selvittämisen ja yleisen turvallisuuden perusteella säilyttää tiedot käyttäjien sähköisen viestinnän välitystiedoista kuuden kuukauden ajan. Säilytysvelvollisuus koskee vähintään tietoja, jotka ovat tarpeen sen selvittämiseksi, mikä yrityksen asiakkaista on tietyn puhelinnumeron, IP-osoitteen tai käyttäjänimen käyttäjä. Lisäksi tulee säilyttää tiedot käyttäjän yhteyksistä, niiden päivämäärät, kehen on oltu yhteydessä ja siirretyn datan määrä.

Saksa

Vuoden 2023 jatkoselvityksessä analysoitiin erityisesti Saksan kansallista tietojen säilytysvelvollisuutta koskevaa lainsäädäntöä siten kuin unionin tuomioistuin oli sitä käsitellyt SpaceNet-ratkaisussaan.[72] Säilytysvelvollisuudesta on säädetty televiestintälaissa (*Telekommunikationsgesetz*). Sittemmin Saksan liittovaltion hallintotuomioistuin (*Bundesverwaltungsgericht*) on vahvistanut SpaceNet-ratkaisussa käsitellyn lainsäädännön unionin oikeuden vastaiseksi.[73] Säilytysvelvollisuutta koskevaa lainsäädäntöä ei ole sovellettu vuonna 2017 annetun kieltomääräyksen jälkeen. Toistaiseksi Saksassa ei ole tehty päätöstä siitä, miten lainsäädäntöä tulisi muuttaa. Poliittisessa keskustelussa on ollut esillä quick freeze -määräyksen ottaminen käyttöön sekä IP-osoitteiden laaja tallentaminen lapsiin kohdistuvien seksuaaliväkivaltarikosten ja lapsipornorikosten selvittämiseksi.

Irlanti[74]

Irlanti on muuttanut kansallista lainsäädäntöään G. D. -ratkaisun (C-140/20) jälkeen. Uudistuksella muutettiin viestintälakia (*Communications (Retention of Data) (Amendment) Act*). Uudessa laissa sallitaan yleinen ja erotukseton säilyttäminen kansallisen turvallisuuden tarpeisiin, edellyttäen tuomioistuimen ennakkovalvontaa. Lisäksi siinä säädetään säilyttämis- ja esittämismääräyksistä, jotka edellyttävät tuomioistuimen ennakkovalvontaa. Tietojen saanti vakavan rikollisuuden ja kansallisen turvallisuuden perusteella edellyttää tuomioistuimen hyväksynnän.

Käyttäjätietoja koskee yleinen ja erotukseton säilytysvelvollisuus. Kyseisten tietojen saanti ei edellytä tuomioistuimen ennakkovalvontaa, eikä niiden käyttöä ole rajattu vain vakavaan rikollisuuteen. IP-osoitteita koskee myös yleinen ja erotukseton säilytysvelvollisuus, mutta näiden saanti edellyttää tuomioistuimen ennakkovalvonta ja se on mahdollista vain vakavan rikollisuuden tapauksissa.

Lisäksi Irlannin lainsäädäntö sisältää mahdollisuuden antaa liikenne- ja paikkatietojen säilytysmääräys sekä kansallisen turvallisuuden että vakavan rikollisuuden tapauksissa. Vakavan rikollisuuden perusteella annettavaa säilytysmääräystä ei voida kohdistaa kansallisen turvallisuuden perusteella säilytettyihin tietoihin. Määräyksiä on

[72] Liikenne- ja viestintäministeriö, Jatkoselvitys Unionin oikeuskäytännön aiheuttamista muutostarpeista Suomen kansalliseen lainsäädäntöön sähköisen viestinnän välitystietojen säilyttämisvelvollisuudesta ja viranomaiskäytöstä, 29.3.2023. VN/25156/2023, jakso 3.3.
[73] BVerwG 6 C 6.22 – 14.8.2023 annettu tuomio. ks. https://www.bverwg.de/de/pm/2023/66
[74] Kuvaus perustuu neuvoston työryhmässä (COPEN DR) 30.11.2022 pidettyyn esitykseen ja siis esityshetken tilanteeseen. Irlannin kansallista sääntely uudistettiin nopeasti G. D. –ratkaisun antamisen jälkeen. Vuonna 2022 pidetyssä esityksessä kuitenkin tunnistettiin mahdollinen tarve lainsäädännön tarkemmalle tarkastelulle jatkossa.

mahdollista kohdentaa maantieteellisen, henkilöperusteisen tai muun kriteerin perusteella. Esittämismääräyksellä velvoitetaan palveluntarjoaja välittämään tiettyjä tietoja toimivaltaisille viranomaisille vakavan rikollisuuden tai kansallisen turvallisuuden perusteella.

Lisäksi Irlannin lainsäädännössä on erillistä sääntelyä koskien pääsyä sijaintitietoihin tietyissä tilanteissa (vakava uhka elämälle tai henkilökohtaiseen turvallisuuteen, kadonneet ihmiset).

Belgia[75]

Belgian uusi kansallinen lainsäädäntö (*Loi du 20 juillet 2022 relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités*) on tullut voimaan heinäkuussa 2022. Laissa on 24 kuukauden siirtymäaika, jotta teleyritykset voivat toteuttaa ja selvittää tarvittavat tekniset ja operatiiviset toimet velvoitteiden noudattamiseksi. Lainsäädäntö velvoittaa yleiseen ja erotuksettomaan tietojen säilyttämiseen koskien 1) tietoja käyttäjän, päätelaitteen tai viestintäpalvelun (ml. IP-osoite) tunnistamiseksi, mutta ei viestintätietoja; 2) vakavien, todellisten ja ajankohtaisten kansalliseen turvallisuuteen kohdistuvien uhkien tapauksissa. Yleinen säilyttäminen on mahdollista, kun uhkataso on arvioitu joko neliportaisen asteikon toiseksi korkeimmaksi tai korkeimmaksi kansallisten turvallisuusviranomaisten mukaan.

Kohdennettu säilyttäminen perustuu maantieteelliseen kriteeriin. Tiedot säilytetään, jos käyttäjä on viestinnän aikana jollain hetkellä kyseisellä alueella. Myös henkilöperusteisesti tietoja säilytetään silloin, kun havaitaan viestintäyhteyden väärinkäyttö.

Maantieteellinen kriteeri koskee kahdenlaisia alueita. Yhtäältä strategisia paikkoja, jotka ovat haavoittuvia vakavan rikollisuuden tai kansalliseen turvallisuuden kohdistuvan uhan vuoksi, ja toisaalta alueita, joilla esiintyy merkittävä määrä vakavaa rikollisuutta perustuen tilastotietoon. Vakavan rikollisuuden esiintymistä arvioidaan absoluuttisesti tilastojen perusteella (määritelty rikostyypeittäin: 3–4 kpl / 1 000 asukasta / kolmen vuoden keskiarvolla). Säilytysaika määräytyy rikosten esiintyvyyden perusteella 6–12 kuukauden välillä.

Uudistettu lainsäädäntö on kansallisen perustuslakituomioistuimen käsittelyssä. Useammassa sääntelyä koskevassa valituksessa on haastettu se, onko uudet säilyttämissäännöt perustuslain ja EU:n perusoikeuskirjan mukaisia. Valitusten mukaan uudessa

[75] Kuvaus perustuu neuvoston työryhmässä (COPEN DR) 30.11.2022 pidettyyn esitykseen ja siis esityshetken tilanteeseen.

lainsäädännössä on kyse järjestelmällisestä tietojen säilyttämisestä eikä siinä tehdä erottelua säilyttämisen suhteen.

5. Tietojen säilyttämisen arvioinnin yleiset kysymykset

5.1 Säilyttämismääräyksen antamiseen toimivaltainen viranomainen

Unionin tuomioistuin on oikeuskäytännössään sallinut sellaiset lainsäädännölliset toimenpiteet, joissa säädetään IP-osoitteiden ja henkilöllisyyttä koskevien tietojen ennakoivasta säilyttämisestä rikollisuuden torjumiseksi ja yleisen turvallisuuden takaamiseksi. Nämä kyseiset säilytystoimenpiteet voidaan siis järjestää siten, että yleinen ja erotukseton säilytysvelvollisuus seuraa suoraan lainsäädännöstä ilman erillistä päätöstä tai määräystä. Sen sijaan unionin tuomioistuimen muut säilyttämistoimenpiteet edellyttävät pääasiassa jonkinlaista päätöstä tai ratkaisua siitä, että laissa asetetut kriteerit täyttyvät, ja jolla säilytysvelvollisuus realisoituu.

Unionin tuomioistuin on kansallisen turvallisuuden takaamiseksi tapahtuvan ennakoivan säilyttämisen ja tietojen nopean varmistamisen osalta arvioinut, että unionin lainsäädäntö ei ole esteenä lainsäädännölliselle toimenpiteelle, jonka mukaan toimivaltaiset viranomaiset voivat määrätä palveluntarjoajat säilyttämään määräyksen mukaisesti käyttäjien liikenne- ja paikkatiedot. (QdN kohdat 137 ja 163) Tuomioistuimen tai riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, tulee voida kohdistaa tällaiseen määräykseen tehokasta valvonta. (QdN kohdat 139 ja 163) Toisin kuin tietojen saantia koskevaan pyyntöön, tietojen säilyttämismääräyksen edellytyksenä ei ole tuomioistuimen *ennakko*valvonta.

Kohdennetun säilyttämisen osalta tuomioistuin ei ole yhtä selkeästi nimennyt tahoa, jonka päätöksellä säilyttämisvelvollisuus voisi realisoitua. Henkilöperusteisen säilyttämisen osalta unionin tuomioistuimen mukaan kohteeksi *voidaan valikoida* henkilöt, joiden tiedot voivat paljastaa ainakin välillisen yhteyden vakaviin rikoksiin, myötävaikuttaa vakavan rikollisuuden torjumiseen tai ehkäistä yleistä turvallisuutta koskevan vakavan uhan taikka kansallista turvallisuutta koskevan uhan. (Tele2 kohta 111 ja QdN kohta 148) Kohteeksi valitut henkilöt voivat olla henkilöitä, jotka *on etukäteen tunnistettu* sovellettavien kansallisten menettelyjen yhteydessä objektiivisten ja syrjimättömien seikkojen perusteella henkilöiksi, jotka aiheuttavat uhan yleiselle turvallisuudelle tai kansalliselle turvallisuudelle. Tämä voi tarkoittaa siis säilyttämistoimenpidettä, joka kohdistuu henkilöihin, jotka tällaisen tunnistamisen perusteella ovat parhaillaan tutkinnan tai muiden valvontatoimenpiteiden kohteena tai joilla on kansallisessa rikosrekisterissä merkintä vakavista rikoksista, mikä voi merkitä suurta rikosten uusimisvaaraa. (G. D. kohdat 77-78)

Unionin tuomioistuimen käsittelemät vaihtoehdot mahdollisiksi säilytystoimenpiteiksi olisivat pitkälti Suomessa uudenlaista sääntelyä. Viranomaisen antamaan määräykseen perustuva säilytysvelvollisuus ei vaikuta suoraan istuvan suomalaiseen pakkokeinojärjestelmään. Esimerkiksi henkilösidonnainen säilytysmääräys saattaisi luoda uuden toimenpideluokan ns. ennakollisena pakkokeinona, jolla viranomaiset voisivat osoittaa henkilöitä mahdollisen tulevan telepakkokeinon kohteeksi. Varsinainen pakkokeino, eli kyseisten tietojen saanti televalvonnalla, toteutettaisiin vasta myöhemmin tuomioistuimen lupaan perustuen. Henkilöperusteisella säilyttämismääräyksellä kuitenkin rajattaisiin henkilöiden piiriä, mihin kyseistä pakkokeinoa voitaisiin myöhemmin käyttää.

Nykyisin pakkokeinolain 8 luvun 24 §:n mukainen datan säilyttämismääräys on lähinnä unionin tuomioistuimen käsittelemiä säilytystoimenpiteitä. Pakkokeinolain datan säilyttämismääräys ei arvion mukaan ole itsessään kovin käyttökelpoinen välitystietojen säilytysvelvollisuuden kannalta, sillä kyseinen määräys on sidottu tarpeeseen varmistaa data muuttumattomana ennen laite-etsinnän toimittamista. Sen käytön edellytyksenä on siis 1) aikomus toimittaa laite-etsintä sekä 2) riski siitä, että data, jolla voi olla merkitystä tutkittavana olevan rikoksen selvittämiselle, häviää tai sitä muutetaan. Pakkokeinolain 10:50 §:n mukaan salaisten pakkokeinojen käytössä noudatetaan, mitä 8 luvun 23-26 §:ssä säädetään tietojärjestelmän haltijan tietojenantovelvollisuudesta ja datan säilyttämismääräyksestä. Tietoja hyödyntävien viranomaisten mukaan tarve tämän soveltamiseen teletietoihin on ollut vähäistä, sillä kyseiset tiedot ovat muutoin olleet tallessa.

Maantieteellisen kriteerin perusteella kohdennettu säilyttäminen on unionin tuomioistuimen ratkaisuissa sidottu selvästi toimivaltaisen kansallisen viranomaisen arvioon siitä, että yhdellä tai useammalla maantieteellisellä alueella vallitsee tilanne, johon liittyy vakavien rikosten valmistelun tai toteuttamisen korkea riski. Tämän arvion tulee perustua objektiivisiin ja syrjimättömiin kriteereihin. (QdN kohta 150 ja siinä viitattu oikeuskäytäntö) Toisin kuin kansallisen turvallisuuden mukaiseen yleiseen säilyttämisen määräykseen tai tietojen nopean varmistamisen määräykseen, tällaiseen toimivaltaisten viranomaisten arvioon ei unionin tuomioistuin vaikuta edellyttävän kohdistettavan tehokasta tuomioistuinvalvontaa. (ks. esim. QdN-ratkaisun tuomiolauselma)

Unionin tuomioistuimen mukaan direktiivin 2002/58 soveltamisalaan kuuluu myös kansallinen säännöstö, jonka mukaan valtion viranomainen voi velvoittaa sähköisen viestintäpalveluiden tarjoajat antamaan toimivaltaisille viranomaisille pääsy näihin tietoihin. (Privacy International kohta 39) Unionin tuomioistuin on oikeuskäytännössään korostanut, että liikenne- ja paikkatietojen säilyttäminen merkitsee sinänsä yhtäältä poikkeusta direktiivin 2002/58 5 artiklan 1 kohdassa säädetystä kiellosta, jonka mukaan muut henkilöt kuin käyttäjät eivät saa tallentaa näitä tietoja, ja toisaalta puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin. Sillä ei ole merkitystä, ovatko ky-

seessä olevat yksityiselämään liittyvät tiedot arkaluonteisia, onko asianomaisille mahdollisesti aiheutunut haittaa tästä puuttumisesta tai käytetäänkö säilytettyjä tietoja myöhemmin. Oikeus saada näitä tietoja merkitsee myöhemmästä kätöstä riippumatta säilyttämisestä erillistä puuttumista kyseisiin perusoikeuksiin. (QdN kohdat 115-116 ja siinä viitattu oikeuskäytäntö)

Unionin tuomioistuin on siis katsonut, 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 säilytettyjä tietoja pyritään suojaamaan tietojen väärinkäyttöä ja lainvastaista saantia koskevilta vaaroilta. (SpaceNet kohta 91)

Estettä ei kuitenkaan ole sille, että kansallisesti säädettäisiin säilyttämismääräyksen antamisen edellytyksistä unionin tuomioistuimen oikeuskäytäntöä tiukemmin. Ennakollinen tuomioistuinvalvonta parantaisi sekä viestintäpalveluiden käyttäjien että säilyttämismääräyksen toimeenpanosta vastaavien yritysten oikeusturvaa. Toisaalta tuomioistuimen ennakkovalvonnan lisääminen tietojen säilyttämisvaiheeseen tietojen saannin lisäksi lisäisi hallinnollista taakkaa ja todennäköisesti kuormittaisi tuomioistuimia. Tunnistamismääräyksen antamiseen toimivaltaista viranomaista asetettaessa tulisi siis pyrkiä tasapainoon viranomaisten toiminnan tarkoituksenmukaisen järjestämisen ja säilyttämisvelvollisuuden toimeenpanosta vastaavien ja sen kohteena olevien kannalta.

SVPL 157 §:n mukaisesti sisäministeriö nimeää erikseen päätöksellään säilytysvelvolliset yritykset. Lain esitöiden mukaan yhteiskunnan varojen käytön kannalta on perusteltua, että sisäasiainministeriö, jonka hallinnonalaa tietojen tallentaminen palvelee ja jonka budjetista tallentaminen kustannetaan, voi määritellä ne teleyritykset, joille on rikoksen estämisen ja selvittämisen tarpeiden valossa tarkoituksenmukaista kustantaa tietojen tallentamisen edellyttämät laitteet ja ohjelmistot.[76]

Lähes kaikki unionin tuomioistuimen oikeuskäytännössä käsittelemät säilyttämistoimenpiteet edellyttävät muutoksia säilytysvelvollisten yritysten järjestelmiin ja käytäntöihin. Näin on erityisesti maantieteelliseen kriteeriin perustuvan maantieteellisen säilyttämisen kohdalla, sillä tietoja ei nykyisten käytäntöjen mukaan voida eritellä säilytettäväksi tietyiltä alueilta.

[76] HE 221/2014 vp, s. 155.

SVPL 299 §:n mukaan teleyrityksellä on oikeus saada valtion varoista korvaus yksinomaan viranomaisen avustamiseksi hankittujen järjestelmien, laitteistojen ja ohjelmistojen investoinneista ja ylläpidosta aiheutuneista välittömistä kustannuksista. Kustannusten korvaamisesta päättää tarvittaessa Liikenne- ja viestintävirasto.

SVPL 158 §:n mukaan sisäministeriöllä on oikeus hankkia ulkopuoliselta palveluntarjoajalta järjestelmä, johon säilytysvelvollisuuden piiriin kuuluvat tiedot voidaan siirtää. Tällä hetkellä tällaista järjestelmää ei kuitenkaan ole käytössä, vaan tietopyyntöjen ja niihin vastausten toimittaminen on järjestetty SALPA-järjestelmän kautta.

Ottaen huomioon potentiaalisten säilytysvelvollisten yritysten laaja ja monipuolinen joukko, tulisi tarvetta erilliseen nimeämispäätökseen tarkastella myös niissä säilyttämistoimenpiteissä, joihin ei unionin tuomioistuimen oikeuskäytännöstä tai muualta seuraa erillistä velvoitetta alistaa säilyttämistä viranomaisen harkintaan. Tällaisia säilyttämistoimenpiteitä ovat erityisesti IP-osoitteiden ja henkilöllisyyttä koskevien tietojen säilyttämisvelvollisuus. Vaihtoehtoisesti säilytysvelvollisten yritysten piiriä voitaisiin täsmentää lain tasolla.[77] Tällöinkin kuitenkin riskinä on, että säilytysvelvollisten yritysten piiri laajenisi nykyisestään merkittävästi, jolloin säilyttämisvelvollisuuden järjestämiseksi tarpeellisten järjestelmien, laitteistojen ja ohjelmistojen investoinneista ja ylläpidosta johtuvat, valtion varoista korvattavat kulut saattavat nousta kohtuuttomasti.

Muutoksenhausta 157 §:n nojalla annettuun päätökseen on säädetty SVPL 342 §:ssä. Sen mukaan säilytysvelvollinen yritys voi 157 §:ssä tarkoitettuun tietojen säilytysvelvollisuutta koskevaan päätökseen vaatia oikaisua sisäministeriöltä. Oikaisuvaatimusmenettelystä säädetään hallintolain 7 a luvussa (581/2010). Mikäli toimivalta antaa säilyttämismääräys annettaisiin muillekin toimijoille kuin sisäministeriölle, tulisi myös muutoksenhakua tarkastella yksityiskohtaisemmin. Tämä tulisi tehdä jatkovalmistelun yhteydessä.

5.2 Säilytysvelvolliset yritykset

Sähköisen viestinnän palveluista annetun lain 157 §:n mukaan säilytysvelvollisuus koskee sisäministeriön päätöksellä erikseen nimeämiä teleyrityksiä. Säilytysvelvollisia yrityksiä Suomessa ovat 27.2.2015 annetun päätöksen mukaan DNA Oyj, Elisa Oyj, Telia Finland Oyj ja Ålands Telekommunikation Ab. Sisäministeriön päätöksen perusteluiden mukaan nimetyt yritykset on valittu merkittävän yhteenlasketun markkinaosuuden sekä maantieteellisen kattavuuden perusteella.

[77] Ks. mahdollisten säilytysvelvollisten yritysten käsittelystä jakso 5.2.

Sähköisen viestinnän palveluista annetussa laissa ei ole teleyrityksen määritelmää tarkemmin asetettu erillisiä vaatimuksia siihen, mikä yritys voidaan määrätä säilytysvelvolliseksi yritykseksi.[78] Säilytysvelvollisuus ei kuitenkaan koske merkitykseltään vähäistä teletoimintaa. Sähköisen viestinnän palveluista annetun lain 3 §:n 27-kohdan mukaan teleyrityksellä tarkoitetaan sitä, joka tarjoaa verkkopalvelua tai viestintäpalvelua ennalta rajaamattomalle käyttäjäpiirille eli harjoittaa yleistä teletoimintaa.

Teleyrityksen määritelmä on laaja, ja se kattaa monenlaisia palveluntarjoajia. Teleyrityksiä ovat perinteisten teleoperaattorien lisäksi esimerkiksi numeroista riippumattomien henkilöiden välisten viestintäpalveluiden tarjoajat, kuten verkon päällä tarjottavien ns. Over-the-top –viestintäpalveluiden tarjoajat (ns. OTT-viestintäpalveluiden tarjoajat). Teletoiminnan sääntely on teknologianeutraalia. Se koskee kohdeviestintää kuten puhelin-, tekstiviesti-, laajakaista- ja sähköpostipalveluita ja joukkoviestintää kuten kaapelitelevisio-, IPTV-, antennitelevisio- ja radiopalveluita.

Nykyisen lain ratkaisua, jonka mukaan säilytysvelvollisia yrityksiä ovat sisäministeriön erikseen päätöksellään nimeämät teleyritykset, on perusteltu mm. sillä, että välitystietojen tallentamisvelvollisuuden edellyttämät laitteet ja ohjelmistot korvataan teleyrityksille valtion varoista SVPL 299 §:n mukaisesti. Esitöiden perusteella sisäministeriön arvioinnissa voidaan painottaa esimerkiksi erilaisia rikostutkinnallisia tekijöitä ja kustannushyötysuhteita. Lain valmistelun yhteydessä tämän arvioitiin tarkoittavan, että ensisijaisesti suuret ja käyttäjien suosimat palveluntarjoajat säilyttäisivät tietoja, mutta myös sellaiset pienemmät toimijat, jotka ovat useimmiten kriittisiä rikostutkinnan kannalta.[79]

Arviomuistion laatimisen yhteydessä tietoja hyödyntävät viranomaiset ovat tuoneet esiin tarpeen velvoittaa laajemmin teleyrityksiä tietojen säilyttämiseen. Nykyinen lainsäädäntö ei kuitenkaan aseta nimenomaisia rajoitteita sille, millainen yritys säilytysvelvolliseksi yritykseksi voidaan nimetä eikä siten juurikaan rajoita mahdollisten säilytysvelvollisten yritysten piiriä.

Liikenne- ja viestintävirasto Traficom ylläpitää teletoimintarekisteriä yleisen teletoiminnan harjoittamisesta ilmoituksen tehneistä yrityksistä. Teletoimintarekisterissä on tällä

[78] Säilytysvelvollisen yrityksen määritelmää on muutettu vuonna 2020, jolloin pykälän 1 momentista on poistettu viittaus säilytysvelvollisten yritysten yhteydestä teletoimintailmoitukseen. Samalla pykälään lisättiin täsmennys, ettei säilytysvelvollisuus koske merkitykseltään vähäistä teletoimintaa. Kyseisillä muutoksilla ei ollut tarkoitus muuttaa silloista nykytilaa, vaan muutokset tehtiin silloisen nykytilan säilyttämiseksi. HE 98/2020 vp, s. 248.

[79] HE 221/2013 vp, s. 155-156.

hetkellä noin 350 ilmoituksen tehnyttä teleyritystä.[80] Ilmoituksen tehneet yritykset ovat toiminnaltaan ja kooltaan varsin erilaisia. Jotta säilytysvelvollisuus kohdistuu sellaisiin toimijoihin, joiden tiedot ovat välttämättömiä säilytysvelvollisuuden tavoitteiden turvaamiseksi, olisi jatkossakin syytä rajata niiden yritysten piiriä, joille velvoite asetetaan. Tämä voitaisiin jatkossakin tehdä sisäministeriön tai muun toimivaltaisen viranomaisen päätöksellä.[81]

Yllä jaksossa 5.1 käsitellysti tietojen säilyttämisen toteutusvaihtoehdot edellyttävät unionin tuomioistuimen oikeuskäytännön mukaan pääsääntöisesti viranomaisen määräyksen ennen säilyttämisen alkamista. Poikkeuksena tästä on IP-liittymän lähteelle annettujen IP-osoitteiden yleinen ja erotukseton säilyttäminen sekä sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen säilyttäminen. Niiltä osin kuin teleyritykseen kohdistettaisiin säilyttämismääräys, olisi säilytysvelvollinen yritys osoitettava määräyksessä. Täten säilytysvelvollisten yritysten piiri tulisi arvioitavaksi ja rajattavaksi viimeistään määräyksen antohetkellä.

5.3 Säilytysajan rajaaminen välttämättömään

Unionin tuomioistuin on oikeuskäytännössään käsitellyt sekä säilyttämistoimenpiteen että tietopyynnön rajaamista ajallisesti välttämättömään. Sähköisen viestinnän tietosuojadirektiivin 15 artiklan toisen virkkeen mukaan jäsenvaltioiden hyväksymät lainsäädännölliset toimenpiteet tietojen säilyttämiseksi tulee olla rajoitettu ajaksi, joka on perusteltua kyseisessä artiklassa listattujen syiden eli yleisen edun mukaisten tavoitteiden syistä. Säilytysaika on siis merkityksellinen tekijä muiden joukossa sen määrittämiseksi, onko unionin oikeus esteenä tällaiselle toimenpiteelle. (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 suojaa koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö. Jopa rajoitetun liikenne- ja paikkatietojen mää-

[80] Huom. Ilmoitusvelvollisuus ei koske toimijaa, joka tarjoaa **ainoastaan** henkilöiden välistä numeroista riippumatonta viestintäpalvelua. Numeroista riippumattomia henkilöiden välisiä viestintäpalveluja ovat esimerkiksi internetin kautta käytettävät pikaviestinpalvelut sekä sähköpostipalvelut. Siten esimerkiksi keskeiset OTT-viestintäpalvelut eivät sisälly teletoimintarekisteriin.
[81] Ylempänä jaksossa 5.2 on käsitelty tarkemmin säilyttämismääräyksen antamiseen toimivaltaisen viranomaisen käsitettä.

rän säilyttäminen tai tietojen säilyttäminen lyhyen aikaa saattaa antaa täsmällisiä tietoja henkilön yksityiselämästä. (SpaceNet kohdat 87-89; Spetsializirana prokuratura (Bulgaria) kohta 52)

Digital Rights Ireland -ratkaisussa unionin tuomioistuin katsoi, että kumotussa direktiivissä säädettiin tietojen säilytysajasta (6-24 kuukautta) tekemättä tietojen hyödyllisyyteen perustuvaa erottelua eri tietoluokkien välillä. Lisäksi säilyttämisen keston määrittäminen ei perustunut objektiivisiin perusteisiin sen takaamiseksi, että säilyttäminen rajoittuu täysin välttämättömään. (Digital Rights Ireland kohdat 63–64) Unionin tuomioistuin ei kuitenkaan ole antanut 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.[82] Myös kansallisesti perustuslakivaliokunta on katsonut, että viestinnän välitystietojen säilyttämiseen liittyy aina riskejä luottamuksellisen viestin salaisuuden sekä henkilötietojen suojan kannalta, ja nämä riskit kasvavat, mitä kauemmin tietoja säilytetään. (PeVL 3/2008 vp, s. 2; PeVL 3/2006 vp, s. 3/II)

Sähköisen viestinnän palveluista annetun lain 157 §:n 4 momentissa asetetut säilytysajat perustuvat Digital Rights Ireland -ratkaisun jälkeen suoritettuun välttämättömyysarviointiin.[83] Perustuslakivaliokunta on aikaisemmin pitänyt 12 kuukauden säilytysaikaa oikeasuhtaisuuden kanalta hyväksyttävänä ja riittävänä vastaamaan viranomaisten tarpeita. (PeVL 3/2008 vp, s. 2/II) Digital Rights Ireland -ratkaisun jälkeen perustuslakivaliokunta kuitenkin edellytti, että tietojen säilytysaikoja on arvioitava tavoitteen toteutumisen kannalta ja säilytysajat tulisi tämän mukaisesti porrastaa joko 12 kuukaudeksi tai tätä lyhyemmäksi ajaksi. (PeVL 18/2014 vp, s. 7) Sähköisen viestinnän palveluista annetussa laissa säilytysajat on porrastettu säilytettävien palvelutyyppien kategorioiden mukaan siten, että matkaviestinverkon puhelin- ja tekstiviestipalveluihin liittyvät tiedot tulee säilyttää 12 kuukautta, internetyhteyspalvelun tarjoamiseen liittyvät tiedot yhdeksän kuukautta ja internetpuhelinpalvelun tarjoamiseen liittyvät tiedot kuusi kuukautta.

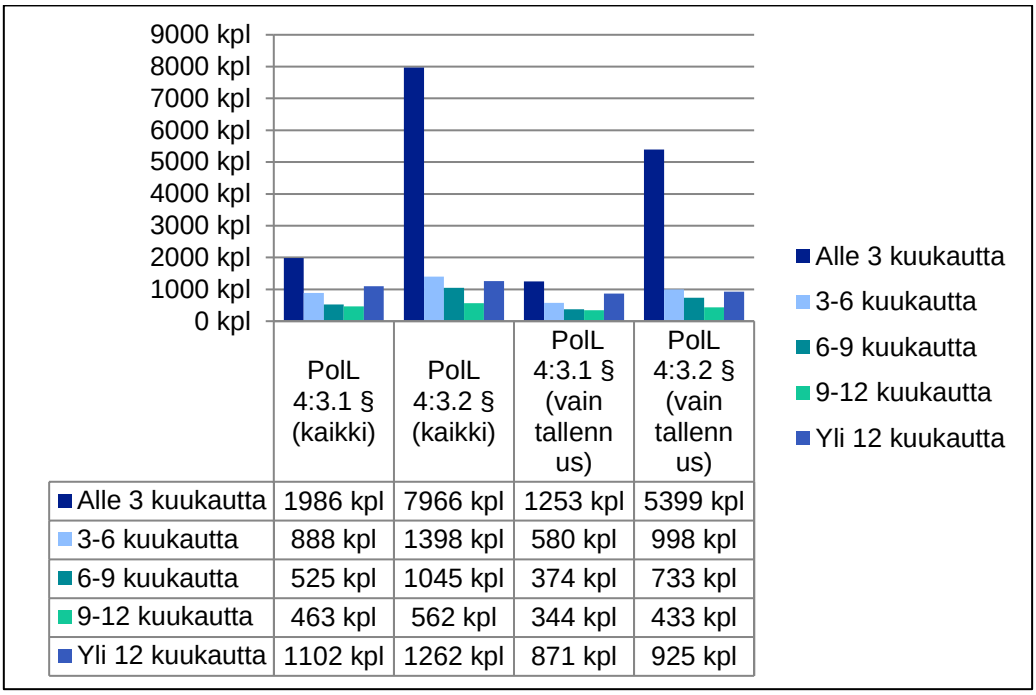
Perustuslakivaliokunta on lausuntokäytännössään peräänkuuluttanut tietojen säilytysajan porrastamisen arvioimista suhteutettuna siihen hyötyyn, joka tiedoilla voi olla hyväksyttävien tavoitteiden saavuttamisen kannalta. Valiokunnan mielestä arvio on tehtävä ennen kaikkea henkilötietojen käsittelyn pääasiallisen käyttötarkoituksen näkökulmasta. (PeVL 28/2016 vp, s. 7, ks. myös PeVL 9/2017 vp, s. 4) Mitä pidemmäksi

[82] Ks. vastaavasti jatkoselvitys 2023 VN/25156/2023 s. 8. SpaceNet-ratkaisussa unionin tuomioistuin arvioi Saksan kansallista lainsäädäntöä, jossa säilytysajat oli asetettu varsin lyhyiksi. Paikkatietoja tuli säilyttää 4 viikkoa ja muita tietoja 10 viikkoa. Näin lyhyeen rajattu säilytysaika ei itsessään riittänyt vaikuttamaan siihen, etteikö kyseisten tietojen yleinen ja erotukseton säilyttäminen voisi olla vakava puuttuminen käyttäjien perusoikeuksiin.
[83] LiVM 10/2014 vp.

tietojen säilytysaika muodostuu, sitä olennaisempaa on huolehtia tietoturvasta, tietojen käytön valvonnasta ja rekisteröidyn oikeusturvasta. (PeVL 13/2017 vp ja PeVL 28/2016 vp, s. 7) Perustuslakivaliokunta on edellyttänyt unionin tuomioistuimen ratkaisukäytännön huomioimista myös säilytysaikojen arvioinnissa. (PeVL 13/2017 vp, s. 6, PeVL 9/2017 vp, s. 5)

Sähköisen viestinnän palveluista annetun lain 157 §:n mukaan tietojen säilyttämisaika alkaa viestintätapahtuman ajankohdasta. Omaa tarvetta varten tapahtuva tietojen käsittelyaika riippuu kyseisestä tiedosta ja teleyrityksillä on toisistaan poikkeavia käytäntöjä siitä, kuinka pitkään tällaisia tietoja säilytetään. Esimerkiksi internetliittymille annettujen IP-osoitteiden säilytysajat vaihtelevat operaattoreiden kesken muutamasta viikosta muutamaan kuukauteen. Kaikkia palvelun toteuttamiseen liittyviä tietoja ei palveluntarjoajalla ole tarvetta säilyttää ja käsitellä lainkaan palvelun toteuttamisen jälkeen. Ilman erillistä säilytysvelvollisuutta merkittävää osaa tiedoista ei säilytettäisi, esimerkiksi vastaamattomiin puheluihin liittyviä tietoja ei olisi tarpeen säilyttää.

Työryhmän saaman selvityksen mukaan telepakkokeinoihin liittyviä tiedonsaantipyyntöjä tehdään eniten alle kolme kuukautta vanhaan tietoon. Tiedonsaantipyynnöt vähenevät, mitä pidemmältä ajalta niitä haetaan. Tiedonsaantipyyntöjen vähenemistä saattaa myös selittää tieto siitä, että SVPL 157 §:n mukainen säilytysaika saattaa päättyä jo lyhyimmillään kuuden kuukauden jälkeen, jolloin tarvittavaa tietoa ei enää säilytysvelvollisuuden nojalla ole käytettävissä. Merkittävin ero on kuitenkin alle kolmen kuukauden ja kolmesta kuuteen kuukauteen säilytettyihin tietoihin kohdistuvissa tietopyynnöissä, jolloin ensimmäisen kohdalla tietopyyntöjä tehdään noin nelinkertaisesti verrattuna jälkimmäiseen. Vuosittain tehdään myös tiedonsaantipyyntöjä tietoihin, jotka ovat syntyneet yli 12 kuukautta sitten. Tarve voi siis kohdistua myös tietoihin pidemmältä aikaväliltä kuin mitä SVPL 157 §:ssä säädetty säilytysvelvollisuus kattaa.



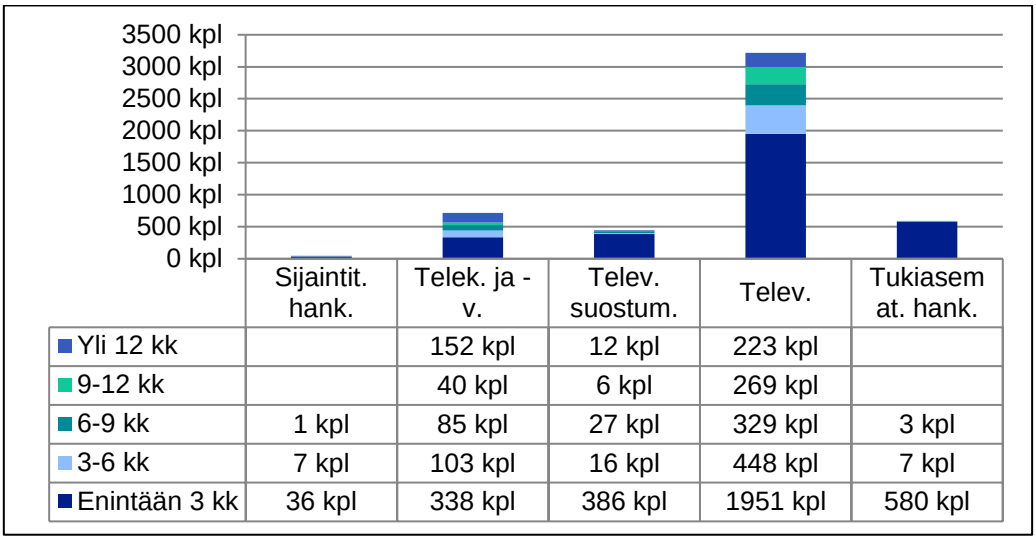
	PolL 4:3.1 § (kaikki)	PolL 4:3.2 § (kaikki)	PolL 4:3.1 § (vain tallennus)	PolL 4:3.2 § (vain tallennus)
Alle 3 kuukautta	1986 kpl	7966 kpl	1253 kpl	5399 kpl
3-6 kuukautta	888 kpl	1398 kpl	580 kpl	998 kpl
6-9 kuukautta	525 kpl	1045 kpl	374 kpl	733 kpl
9-12 kuukautta	463 kpl	562 kpl	344 kpl	433 kpl
Yli 12 kuukautta	1102 kpl	1262 kpl	871 kpl	925 kpl

Taulukko 1: Kaikki tiedonsaanti- sekä tiedon tallentamisvelvollisuuden alaiset pyynnöt[84]

Kaiken kaikkiaan rikoksen tutkimiseksi tehtyjä tiedonsaantipyyntöjä oli 4 964 vuonna 2022 (4 785 kappaletta edellisenä vuonna 2021). Tiedon tallennusvelvollisuuden alaiseen tietoon on ollut mahdollisuus päästä käsiksi 2 551 tapauksessa, sillä 871 pyyntöä on kohdistunut sellaiseen tietoon, jota ei ole enää saatavilla. Liittymän omistajan tai käyttäjän tunnistamiseksi tehtyjä tiedonsaantipyyntöjä oli 12 233 kappaletta vuonna 2022.Tilaston perusteella 62 % tiedonsaantipyynnöistä on toteutettu liittymän omistajan tai käyttäjän selvittämiseksi televalvontarikoksissa.[85]

[84] Lähde: Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2022. POL-2022-159162. 09.03.2023, s. 22. Saatavilla: https://intermin.fi/documents/1410869/4113506/poliisin-salaiset-tiedonhankinta-keinot-ja-valvonta-2022.pdf/23e1ea9a-1a56-c134-6549-ba01bde33bf4/poliisin-salaiset-tiedonhankintakeinot-ja-valvonta-2022.pdf?t=1696321151971

[85] Poliisihallituksen kertomus, s. 21.



	Sijaintit. hank.	Telek. ja -v.	Telev. suostum.	Telev.	Tukiasem at. hank.
Yli 12 kk		152 kpl	12 kpl	223 kpl	
9-12 kk		40 kpl	6 kpl	269 kpl	
6-9 kk	1 kpl	85 kpl	27 kpl	329 kpl	3 kpl
3-6 kk	7 kpl	103 kpl	16 kpl	448 kpl	7 kpl
Enintään 3 kk	36 kpl	338 kpl	386 kpl	1951 kpl	580 kpl

Taulukko 2: Takautuvat telepakkokeinot, tiedon tallennusvelvollisuus, haetun tiedon ikä (PKL)[86]

Edellä käsiteltyjen tilastojen valossa tietopyyntöjä tehdään selvästi eniten enintään kolmen kuukauden ikäisiin tietoihin. Tietopyyntöjen määrä pääsääntöisesti laskee, mitä vanhemmista tiedoista on kyse. Säilytysajalla on suora yhteys siihen, miten pitkältä ajalta tiedot ovat saatavissa, ja siis miten pitkältä ajalta viranomaisilla on käytettävissä tietoja takautuvasti.

Unionin tuomioistuimen oikeuskäytännön mukaan myös erittäin lyhytkin säilytysaika, kuten neljä tai kymmenen viikkoa, saattaa tarkoittaa vakavaa puuttumista käyttäjän perusoikeuksiin, sillä näiden tietojen yhdistelmän perusteella voidaan tehdä hyvin täsmällisiä johtopäätöksiä niiden henkilöiden yksityiselämästä, joiden tietoja on säilytetty. (SpaceNet kohdat 88–90) Useiden tietojen osalta ensimmäisen ja toisen ryhmän eli alle kolmen kuukauden ja kolmesta kuuteen kuukauden ikäisten tietojen välillä tietopyynnöt moninkertaistuvat. Muiden ryhmien välillä ei ole yhtä merkittävää eroa. Tilastojen perusteella vaikuttaisi siltä, että ehdottoman välttämättömänä säilytysaikana voidaan perustellusti pitää ainakin kolmea kuukautta. Tämä olisi pidempi säilytysaika kuin SpaceNet-ratkaisussa, mutta tätä säilytysaikaa voi perustella välttämättömyyden näkökulmasta juuri Suomen tilastotietojen valossa.

Toisaalta tietopyyntöjen määrää ensimmäisen kolmen kuukauden ajalta selittää osin se, että suurin osa rikoksista tulee poliisin selvitettäväksi varsin pian. Koska rikoksista ilmoitetaan hyvin nopeasti, on luonnollista, että alle kolmen kuukauden ikäisten tietojen tietopyynnöt korostuvat. Tietopyyntöjen määrä on yllä viitatuissa tilastoissa jaoteltu kolmen kuukauden pituisiin jaksoihin. Siten niistä ei käy ilmi, miten tietopyyntöjen määrät jakautuisivat esimerkiksi viikkotasolla tarkasteltuna.

[86] Poliisihallituksen kertomus, s. 20.

Vanhemman tiedon merkitys korostuu, mitä vakavammista ja vaikeammin selvitettävistä rikoksista on kyse. Viranomainen saattaa tulla tietoiseksi rikoksesta vasta varsin myöhään tapahtuneeseen verrattuna. Esimerkiksi vainajan löytyessä ja henkirikosta tutkittaessa on välttämätöntä saada tiedot pidemmältä ajalta kuin kolmelta kuukaudelta. Niin sanotusti pimeänä tutkittavaksi tulleen henkirikoksen, eli kun rikoksesta epäilty henkilö ei ole tiedossa, selvittäminen voi olla käytännössä mahdotonta, mikäli televalvontaa ei voida hyödyntää. Tällaisissa tilanteissa tarve pidemmälle säilytysajalle korostuu. Mitä pidemmältä ajalta tiedot ovat saatavissa, sitä paremmin pystytään turvaamaan poliisin kyky torjua ja tutkia rikoksia.

On selvää, että viranomaisilla on tarve saada tietoja eri tilanteissa eri ajalta, ja tarve voi kohdistua myös yli 12 kuukauden takaisiin tietoihin. Törkeimpien rikosten, erityisesti henkirikokset, vakavat väkivaltarikokset, törkeät huumausainerikokset, osalta myös vanhemmilla tiedoilla on keskeinen merkitys. On myös huomattava, että piilorikollisuuden, esimerkiksi huumausainerikosten, osalta tietopyynnön ajallinen kohdistuminen riippuu keskeisesti siitä, milloin poliisi on tullut tietoiseksi rikoksesta ja voi käynnistää tiedonhankinnan. Rikosten selvittämiseksi kokonaiskuvan muodostaminen saattaa edellyttää tietojen saantia myös pidemmältä ajalta. Takautuvilla televalvontatiedoilla on usein keskeinen merkitys eri osatekoihin osallisten henkilöiden osallisuuden ja keskinäisten yhteyksien selvittämisen kannalta.

Vakavien rikosten pitkien tutkinta-aikojen vuoksi pidempää säilytysaikaa voidaan pitää tarpeellisena. Samassa kokonaisuudessa henkilöitä voisi jäädä tuomitsematta, jos näyttöä ei olisi liian lyhyen säilytysajan vuoksi saatavilla. Myös rikossarjojen osalta tekojen vakavuus saattaa selvitä vasta myöhemmin, jolloin tutkinnan alkuvaiheessa televalvontakynnys ei välttämättä ole ylittynyt, mutta ylittyisi myöhemmin. Rajat ylittävissä tutkinnoissa myös korostuu tarve pitkille säilytysajoille. Lyhyt säilytysaika saattaa johtaa myös muiden, mahdollisesti yksityiselämän suojaan vakavammin puuttuvien pakkokeinojen käyttökynnyksen alenemiseen, jos rikostutkinnan kannalta tarpeellisia tietoja jouduttaisiin hankkia vaihtoehtoisin menetelmin siksi, että tietopyyntö kohdistuisi tietoihin, joita ei ole enää saatavilla.[87]

Nykyisen lain säätämisen yhteydessä perustuslakivaliokunta piti Digital Rights Ireland -ratkaisun valossa arveluttavana, että säilytysaikaa ei säännöksessä ole lainkaan eritelty suhteessa siihen mahdolliseen hyötyyn, joka tiedoista voi vakavan rikollisuuden torjumisen tavoitteen kannalta olla. Perustuslakivaliokunta ei kuitenkaan yksiselitteisesti edellyttänyt säilytysaikojen porrastamista kansallisessa laissa, vaan olennaista oli säilytysaikojen arviointi tavoitteen toteutumisen kannalta. (PeVL 18/2014 vp, s. 7)

[87] Näitä toimenpiteitä ei kuitenkaan ole mielekästä verrata keskenään, sillä ennakollinen ja tiettyyn rikosepäilyyn kiinnittymätön tietojen säilyttäminen on luonteeltaan varsin erilainen kuin tiettyyn rikostutkinaan liittyvä pakkokeinojen käyttö. Näistä ensimmäinen kohdistuu laajaan joukkoon ihmisiä, joita ei ole syytä epäillä rikoksesta. Myös toimenpiteiden oikeussuojakeinot eroavat toisistaan.

Unionin tuomioistuimen uudemmassa oikeuskäytännössä ei ole sittemmin käsitelty Digital Rights Ireland -ratkaisua yksityiskohtaisemmin mahdollista säilytysaikojen porrastamista. Jatkovalmistelussa tulisi arvioida tarkemmin kunkin säilytystoimenpiteen osalta välttämätön säilytysaika, joka voi vaihdella säilytystoimenpiteiden kesken.

Säilytysaikoja voitaisiin porrastaa myös sen perusteella, onko kyse sijaintitiedoista vai välitystiedoista.[88] Sijaintitiedot kertovat viestinnän luottamuksellisuuden suojan piiriin kuuluvien tietojen lisäksi myös henkilön toiminnasta fyysisessä maailmassa, sillä sijaintitietojen perusteella voidaan tehdä päätelmiä henkilön elämästä esimerkiksi usein vierailtujen sijaintien perusteella.

SPVL 157 §:n mukaan säilytettäviin tietoihin sisältyy myös käyttäjän sijainnin ilmaisevia tietoja. SVPL:ssä on myös erillistä sääntelyä sijaintitietojen käsittelystä (20 luku). SVPL 157 §:ssä ei ole tehty erottelua välitys- ja sijaintitietojen välillä, vaan tietoihin viitataan SVPL 157 §:n nojalla säilytettävinä tietoina. Se, pidetäänkö sijainnin ilmaisevaa tietoa laissa välitystietona vai sijaintitietona ratkeaa tiedon käyttötarkoituksen perusteella. Jos sijainnin ilmaisevaa tietoa käytetään viestinnän toteuttamisessa, kysymyksessä on välitystieto. Tällöin liittymän tai päätelaitteen sijainnin ilmaiseva tieto on välttämätön viestinnän toteuttamiseksi. (HE 221/2013 vp, s. 88)

Tietojen säilyttämistoimenpide voidaan tuomioistuimen mukaan toteuttaa ”ajanjaksoksi, joka on rajoitettu täysin välttämättömään”. Kansallista turvallisuutta vaarantavan uhan torjumiseksi annettu yleinen ja erotukseton säilyttämismääräys sekä tietojen kohdennettu säilyttämismääräyksen osalta kyseistä ajanjaksoa voidaan jatkaa. (QdN tuomiolauselma) Palveluntarjoajien hallussa olevien tietojen säilyttämisen nopea varmistaminen ei ole nimenomaisesti sidottu samanlaiseen aikamääreeseen. Myöskään käyttäjien henkilöllisyyttä koskevien tietojen yleistä ja erotuksetta tapahtuvaa säilyttämistä unionin tuomioistuin ei ole edellyttänyt rajattavan vastaavasti välttämättömään. (QdN tuomiolauselma)

Pakkokeinolain mukainen datan säilyttämismääräys voidaan antaa korkeintaan kolmeksi kuukaudeksi kerrallaan. Määräys voidaan kuitenkin uudistaa rikoksen tutkinnan sitä edellyttäessä, ja se on kumottava niin pian kuin se ei enää ole tarpeen. (Pakkokeinolaki 8:25 §)

Esimerkiksi Belgiassa tietojen säilytysaika on porrastettu kuuden ja 12 kuukauden välille, riippuen vakavan rikollisuuden esiintymisestä tietyllä alueella. Tanskan kansallisessa lainsäädännössä rikollisuuden torjumiseksi säilytettävien tietojen säilytysajaksi on asetettu yksi vuosi, ja vastaavaa säilytysaikaa on ehdotettu myös Ruotsin selvityk-

[88] Tällaiseen ratkaisuun on esimerkiksi päädytty Saksan säilytysvelvollisuutta koskevassa lainsäädännössä, jota käsiteltiin SpaceNet-ratkaisussa. Sijaintitietojen säilytysaika oli laissa rajattu vain neljään viikkoon ja muiden tietojen säilytysaika oli 10 viikkoa.

sessä. Vuoden säilytysaika on myös kansallisesti perustuslakivaliokunnan arvion mukaan oikeasuhtaisuuden kannalta hyväksyttävä enimmäissäilytysaika. (PeVL 18/2014 vp, s. 7/II) Säilytysvelvollisuuden ajallisen keston oikeasuhtaisuuden arvioinnissa voitaisiin ottaa huomioon myös se, kauanko viestintäpalveluntarjoajat säilyttävät tietoja omia tarkoituksiaan varten. Toisaalta työryhmän saamien tietojen mukaan näissä säilytysajoissa on eroavaisuuksia yritysten välillä, eikä niiden lainmukaisuutta ole toistaiseksi arvioitu.

5.4 Säilytettävien tietojen yksilöiminen

Nykyisin säilytettävät tietokategoriat on yksilöity SVPL 157 §:ssä. Säilytysvelvollisuuden perusteella säilytettävien tietojen teknisistä yksityiskohdista on määrätty Viestintäviraston (nyk. Liikenne- ja viestintävirasto Traficom) määräyksessä.[89] Säilytysvelvollisuus on ulotettu sellaisiin tietoihin, joita säilytysvelvolliset yritykset käsittelevät joka tapauksessa. Suhteellisuusperiaatteen kannalta perustuslakivaliokunta on pitänyt tärkeänä, ettei palvelun tarjoajaa velvoiteta erikseen tuottamaan tai hankkimaan tietoja, vaan ainoastaan säilyttämään tarjoajan saatavilla muutenkin olevat tiedot (PeVL 3/2008 vp, s. 2/II, PeVL 3/2006 vp, s. 3/I, PeVL 35/2004 vp, s. 3/II). Jatkossakin tulisi kiinnittää huomiota siihen, ettei säilytysvelvollisuudella luoda velvoitetta kerätä sellaisia tietoja, jotka eivät ole välttämättömiä palvelun toteuttamisen kannalta. SVPL 157 §:n 3 momentin mukaan säilytettävät tiedot tulee rajata vain siihen, mikä on palvelun tekninen toteutus huomioon ottaen välttämätöntä laissa määriteltyjen seikkojen yksilöimiseksi. Jatkossakin tulee ottaa huomioon perustuslain 80 §:n sääntely lainsäädäntövallan siirtämisestä.

Tietoja hyödyntävien viranomaisten näkökulmasta nykyiset SVPL 157 §:ssä säilytettäväksi määrätyt tietokategoriat ovat edelleen tarpeellisia. Ainoa selvityksen laatimisen aikana viranomaisten puolelta esiin tuotu tarve tarkastella säilytettävien tietokategorioiden laajentamista koskee IP-osoite- ja porttitietojen säilyttämistä.[90]

Nykyisen lain säätämisen yhteydessä perustuslakivaliokunta edellytti, että liikenne- ja viestintävaliokunnan oli täsmennettävä, mitkä ehdotetun säännöksen perusteella säilytettävät tiedot ovat välttämättömiä sääntelyn taustalla olevan tarkoituksen eli vakavien rikosten tutkimisen, selvittämisen ja syyteharkintaan asettamisen kannalta. Sellaisia tietoja, jotka eivät ole tämän tarkoituksen kannalta välttämättömiä, ei voi vaatia säilytettäviksi. (PeVL 18/2014 vp, s. 7) Säilyttämisvelvollisuuden vähimmäissisällön

[89] Viestintäviraston määräys teleyritysten tietojen säilytysvelvollisuudesta viranomaistarpeita varten. Viestintävirasto 53 B/2014 M.
[90] IP-osoitteisiin liittyvien tietojen säilyttämisen laajentamista käsitellään tarkemmin alempana jaksossa 7.3.

kannalta perustuslakivaliokunta on pitänyt aivan olennaisena, mihin tietoihin tai tietotyyppeihin velvollisuus ulottuu. Tällaisten, sääntelyn kannalta olennaisten seikkojen ja rajausten tulee käydä säännöksistä ilmi täsmällisesti. (PeVL 3/2006 vp, s. 3/II, PeVL 35/2004 vp, s. 3/II)

SVPL 157 §:ssä säilytettävät tietokategoriat on määritelty palvelukohtaisesti. Säilyttämisvelvollisuuden piiriin kuuluvia palveluita ovat matkaviestinverkon puhelinpalveluun tai tekstiviestipalveluun, internetpuhelinpalveluun tai internetyhteyspalveluun liittyvät yksilöidyt tiedot. Lain säätämisen yhteydessä liikenne- ja viestintävaliokunta arvioi perustuslakivaliokunnan edellyttämällä tavalla tietojen säilyttämisen välttämättömyyttä. Tällöin valiokunta rajoitti säilytysvelvollisuuden edellä SVPL 157 §:ssä lueteltuihin palveluihin, ja hallituksen esityksestä poiketen säilytysvelvollisuuden piiristä poistettiin tietyt palvelut[91], joiden tietoja ei sen hetkisen arvion perusteella voitu katsoa olevan välttämätöntä säilyttää vakavien rikosten selvittämistä ja syyteharkintaa asettamista varten. (LiVM 10/2014 vp, s. 24-25)

Työryhmän saaman selvityksen mukaan tietopyyntöjä tehdään matkaviestinverkon palveluiden tietoihin noin yhdeksänkertaisesti verrattuna internetpalveluihin liittyviin tietopyyntöihin. Esimerkiksi liittymän omistajan tai käyttäjän tunnistamiseksi tehtyjä tiedonsaantipyyntöjä oli 12 233 kappaletta vuonna 2022. Tilaston perusteella 62 % tiedonsaantipyynnöistä on toteutettu liittymän omistajan tai käyttäjän selvittämiseksi televalvontarikoksissa.[92] Vaikka viestintätavat ja –palvelut ovat muuttuneet, niin matkaviestinverkon palveluiden tiedot ovat edelleen viranomaisten tehtävien kannalta tarpeellisia.

Sinänsä perustuslakivaliokunnan tai unionin tuomioistuimen oikeuskäytännöstä ei seuraa velvoitetta määritellä säilytettäviä tietoja nykyisen kaltaisen järjestelmän mukaan, jossa säilytettävät tiedot on rajattu tiettyihin palveluihin liittyviin tietoihin, jos muutoin voidaan varmistaa, että säilytettävät tiedot voidaan yksilöidä ja ne on rajattu välttämättömään sääntelyn taustalla olevan tarkoituksen kannalta. Ottaen huomioon teleyritysten tarjoamien palveluiden monipuolisuus ja niissä käsiteltyjen tietojen kokonaismäärä, johtaisi palveluluokkien poistaminen käytännössä säilytysvelvollisuuden laajenemiseen. Tämä olisi myös erikoista ottaen huomioon vuonna 2014 tehty palveluluokkien rajoitus. Tällöin säilytysvelvollisuuden piiriin saattaisi tulla esimerkiksi sellaisia palveluita, kuten kiinteän puhelinverkon palvelut eli ns. lankapuhelimet, joita ei pidetty rikostorjunnan kannalta välttämättöminä vuonna 2014 ja joiden merkitys sittemmin on entisestään laskenut.

[91] Tietoja ei enää säilytetä viranomaistarpeita varten lainkaan säilytysvelvollisen yrityksen kiinteän verkon puhelinpalveluista (ns. lankapuhelin), sähköpostipalveluista, lisäpalveluista, EMS-palveluista ja multimediapalveluista.
[92] Poliisihallituksen kertomus, s. 21.

Jatkovalmistelun aikana tulisi arvioida yksityiskohtaisemmin tarve säätää jatkossakin nykyistä lainsäädäntöä vastaavasti säilytettävät tiedot palveluluokittain.[93] Vaihtoehtoisesti jatkovalmistelussa voitaisiin tarkastella mahdollisuutta määrittää säilyttämisvelvollisuuden palveluluokat erillisen säilyttämismääräyksen yhteydessä tai lakia alemmantasoisella sääntelyllä. Tällaisella ratkaisulla voitaisiin mahdollistaa nopeampi reagointi muuttuviin viestintätapoihin. Tämä ei kuitenkaan vaikuta ensisijaiselta ratkaisulta, sillä lain tasolla tulisi säätää säilytettävistä tiedoista riittävän tarkasti yllä mainitut rajoitukset huomioon ottaen.

5.5 Säilytysvelvollisten yritysten organisatoriset ja tekniset toimet tietojen suojaamiseksi

Tele2 ja Watson -ratkaisussa unionin tuomioistuin arvioi kriteerejä sähköisen viestinnän liikenne- ja paikkatietojen säilyttämiselle ja viranomaisten pääsylle liikenne- ja paikkatietoihin sähköisen viestinnän tietosuojadirektiivin ja Euroopan unionin perusoikeuskirjan näkökulmasta. Direktiivin 2002/58 4 artiklan 1 kohdassa sekä 4 artiklan 1 a kohdassa edellytetään, että palveluntarjoajat toteuttavat asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa säilytettyjen tietojen tehokas suoja väärinkäytön vaaraa vastaan sekä näiden tietojen kaikenlaista laitonta saantia vastaan. Unionin tuomioistuin on oikeuskäytännössään kiinnittänyt huomiota siihen, että direktiivin 2002/58 15 artiklan 1 alakohdassa ei sallita jäsenmaita poikkeamaan kyseisistä 4 artiklan alakohdista. Sen sijaan unionin tuomioistuin on kiinnittänyt huomiota siihen, että säilytettyjen tietojen määrä, niiden arkaluonteisuus sekä niiden lainvastaista saantia koskeva vaara huomioiden on sähköisten viestintäpalvelujen tarjoajien säilytettävien tietojen täyden koskemattomuuden ja luottamuksellisuuden takaamiseksi varmistettava erityisen korkea suojan ja turvan taso turvautumalla asianmukaisiin teknisiin ja organisatorisiin toimiin. Kansallisessa säännöstössä on erityisesti säädettävä tietojen säilyttämisestä unionin alueella ja tietojen lopullisesta hävittämisestä, kun niiden säilyttämisaika päättyy. (Tele2 kohta 122; analogisesti myös Digital Rights Ireland, kohdat 66–68)

Sähköisen viestinnän tietosuojadirektiivin 4 artiklan mukaan näillä toimenpiteillä on vähintään varmistettava, että henkilötietoja pääsee käsittelemään vain siihen luvan saanut henkilöstö oikeudellisesti perustelluissa tapauksissa, suojattava tallennetut tai siirretyt henkilötiedot tahattomalta tai laittomalta tuhoamiselta, tahattomalta kadottamiselta tai muuttamiselta taikka luvattomalta tai laittomalta säilyttämiseltä, käsittelyltä,

[93] Tarvetta palveluluokkien yksityiskohtaisempaan tarkasteluun ja päivittämiseen käsitellään yksityiskohtaisemmin jäljempänä OTT-viestintäpalveluihin ulotettavan säilytysvelvollisuuden arvioinnin yhteydessä.

käytöltä tai luovuttamiselta, ja varmistettava henkilötietojen käsittelyä koskevan turvapolitiikan toteuttaminen.

Kyseinen 4 artikla on toimeenpantu kansallisesti sähköisen viestinnän palveluista annetun lain 247 §:llä, jonka mukaan viestinnän välittäjän on huolehdittava palvelujensa, viestien, välitystietojen ja sijaintitietojen tietoturvasta.[94] Toimenpiteet, joilla huolehditaan tietoturvasta, on suhteutettava uhan vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin sekä käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Säilytysvelvollinen yritys päättää tietojen säilyttämisen teknisestä toteuttamisesta. Tiedot on säilytettävä kustannustehokkaasti. Lisäksi on otettava huomioon säilytysvelvollisen yrityksen liiketoiminnan tarpeet ja järjestelmien tekniset ominaispiirteet sekä maksuvelvollisen viranomaisen tarpeet.[95] Sähköisen viestinnän palveluista annetun lain 158 §:n 3 momentin mukaan säilytysvelvollisen yrityksen velvollisuuteen huolehtia tietoturvasta sovelletaan 247 §:ää, ja sen on nimettävä henkilöt, joilla on oikeus käsitellä säilytettäviä tietoja tai tehtävät, joissa niitä saa käsitellä. Säilytysvelvollisen yrityksen on huolehdittava, että tilaajan saatavilla on tietoa tietojen säilyttämisestä ja sen tarkoituksesta.

Säilytysvelvollisuuden teknisen toteutuksen ja tietoturvallisuuden vaatimusta on tarkennettu sähköisen viestinnän palveluista annetun lain 158 §:n 6 momentin nojalla annetussa viestintäviraston määräyksessä.[96] Sen mukaan säilytysvelvollisen yrityksen on suojattava säilytysvelvollisuuden piiriin kuuluvat tiedot oikeudettomalta käsittelyltä sekä säilytyksen aikana että niitä viranomaiselle siirrettäessä. Säilytysvelvollisen yrityksen on tarkistettava asianmukaisesti viranomaiselta tulevan, säilytysvelvollisuuden piiriin kuuluviin tietoihin kohdistuvan tietopyynnön laillisen perusteen olemassaolo. Säilytysvelvollisen yrityksen on tallennettava viranomaiselta tulevan, säilytysvelvollisuuden piiriin kuuluviin tietoihin kohdistuvan tietopyynnön toteuttamisesta 2 vuodeksi tiedot siitä, mitä tietoja on haettu ja mitkä tiedot on luovutettu, tietojen hakemisen ajankohta, tietojen hakija sekä tietojen hakemisen laillinen peruste.

Myös yleisen tietosuoja-asetuksen 32 artiklassa säädetään käsittelyn turvallisuudesta. Kyseisen artiklan mukaan rekisterinpitäjän ja käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet. Tällaisina toimenpiteinä mainitaan esimerkiksi henkilötietojen pseudonymisointi ja salaus, kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus sekä kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa.

[94] HE 221/2013 vp, s. 189.
[95] Sähköisen viestinnän palveluista annettu laki 158 § 1 mom.
[96] Määräys teleyritysten tietojen säilytysvelvollisuudesta viranomaistarpeita varten, 53 B/2014 M 17.12.2014.

Näin ollen voidaan pitää tarkoituksenmukaisena, että säilytysvelvollinen yritys jatkossakin päättää tietojen säilyttämisen teknisestä toteuttamisesta siten, että tietopyyntöihin voidaan vastata ilman tarpeetonta viivästystä. Sääntelyllä tulee varmistaa, että säilytysvelvollisilta yrityksiltä edellytetään jatkossakin riittäviä teknisiä ja organisatorisia toimia, jotta voidaan varmistaa tietojen säilytettävien tietojen korkea suojan ja turvan taso. Organisatoristen toimien vahvistamiseksi sääntelyä muutettaessa tulisi harkita, mikäli silloisen Viestintäviraston vuoden 2014 määräykseen sisältyvä velvoite tallentaa kahden vuoden ajan viranomaiselta tulevien tietopyyntöjen käsittelyyn liittyvät tiedot tulisi nostaa lain tasolle samaan yhteyteen, jossa säädetään säilytysvelvollisen yrityksen velvoitteesta nimetä henkilöt, jotka tietoja voivat käsitellä, tai tehtävät, joiden yhteydessä tietojen käsittely on sallittua. Teknisten velvoitteiden osalta nykytilaa voidaan pitää riittävänä, mutta valmistelussa tulisi harkita, mikäli lakiin on tarpeen ottaa nimenomainen velvoite varmistaa säilytysvelvollisuuden nojalla säilytettyjen tietojen tekninen turvaaminen. Velvoite organisatoristen ja teknisten toimien toteuttamiseksi tulisi jatkossakin seurata laintasoisesta sääntelystä. Tätä velvoitetta voitaisiin jatkossakin täydentää ja selkeyttää yksityiskohtaisemmin Liikenne- ja viestintäviraston määräyksellä.

Tele2-ratkaisussaan unionin tuomioistuin liitti korkean suojan ja turvan tason varmistaviin asianmukaisiin teknisiin ja organisatorisiin toimiin velvoitteen säätää nimenomaisesti tietojen säilyttämisestä EU:n alueella sekä tietojen poistamisesta. Sähköisen viestinnän palvelulain 158 §:ssä asetetaan edellytykset säilytysvelvollisuuden piiriin kuuluvien tietojen säilyttämisestä kustannustehokkaasti sekä säilytysvelvollisen yrityksen vaatimuksesta huolehtia tietoturvasta. Sähköisen viestinnän palvelulain 137 §:n 3 momenttiin sisältyy yleinen velvoite käsittelyn jälkeen hävittää tai tehdä välitystiedot sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään, jollei laissa toisin säädetä. Työryhmän saaman selvityksen mukaan säilytysvelvollisten yritysten tietokannat sijaitsevat Suomessa. Sähköisen viestinnän palveluista annetussa laissa ei kuitenkaan säädetä nimenomaisesti 157 §:n nojalla säilytettyjen tietojen poistamisesta eikä siinä aseteta nimenomaista edellytystä, että tiedot tulisi säilyttää Euroopan unionin alueella.

Jatkovalmistelussa tulisi kiinnittää huomiota siihen, että lain tasolla varmistettaisiin minimissään Tele2-ratkaisun edellytys, että tiedot tulisi säilyttää unionin alueella. Kirjauksella ei pyrittäisi muuttamaan nykytilaa eikä sillä odoteta olevan välittömiä muutoksia nykyisten säilytysvelvollisten yritysten käytäntöihin. Yllä käsiteltyjä säilytysmääräyksiä voitaisiin kuitenkin jatkossa kohdistaa mahdollisesti laajempaan joukkoon teleyrityksiä. Edellytys tietojen säilyttämisestä unionin alueella olisi selventävä kirjaus, jolla varmistettaisiin yksiselitteisesti lain tasolla, että säilytysvelvollisuuden nojalla säilytettyjä tietoja ei tule säilyttää kolmansissa maissa.

6. Tietojen säilyttämisvelvollisuuden toteutusvaihtoehtojen arviointi

6.1 Kansallisen säilytysvelvollisuuden kumoaminen

Sähköisen viestinnän tietosuojadirektiivi mahdollistaa säilytysvelvollisuuden asettamisen. Se ei kuitenkaan velvoita siihen. Yksi mahdollisuus saattaa Suomen lainsäädäntö EU-oikeuden mukaiseksi olisi siten kumota säilytysvelvollisuutta koskeva sääntely. Oikeuskirjallisuudessa on huomautettu, että säilytysvelvollisuus tuli Suomen lainsäädäntöön vasta (kumotun) säilytysvelvollisuutta koskeneen direktiivin täytäntöönpanon myötä.[97]

Tämä ratkaisu parantaisi yksityiselämän suojaa ja luottamuksellisen viestin salaisuuden suojaa. Tästä näkökulmasta kumoaminen olisi myös perustuslain 22 §:n mukaista. Unionin tuomioistuin on todennut sähköisen viestinnän tietosuojadirektiivin sanamuodon perusteella, että sähköisten viestintävälineiden käyttäjillä on oikeus odottaa lähtökohtaisesti, että heidän viestintänsä ja siihen liittyvät tiedot säilyvät nimettöminä eikä niitä voida tallentaa, jos he eivät ole antaneet siihen suostumustaan. (G. D. kohta 37) Yllä kuvatusti säilytysvelvollisuus on vakava puuttuminen sellaisiin perusoikeuksiin, jotka ovat demokraattiseen ja moniarvoiseen yhteiskuntaan liittyviä olennaisia perustoja.

Säilytysvelvollisuuden kumoaminen poistaisi myös puuttumisen teleyritysten omaisuudensuojaan.

Kumoaminen ei kuitenkaan vaikuta ensisijaiselta vaihtoehdolta. Vaikka kumoaminen parantaisi yksien perusoikeuksien toteutumista, se johtaisi toisten perusoikeuksien, erityisesti oikeuden elämään ja henkilökohtaiseen vapauteen ja koskemattomuuteen, sekä valtion keskeisten tehtävien suorittamisen heikentymiseen. Pakkokeinolakiperusteista telekuuntelua ja televalvontaa tehdään vuosittain noin 500 tapauksessa, pelkkää televalvontaa vajaassa 2 000 tapauksessa ja tukiasematietojen keräämistä noin 600 tapauksessa. Poliisilakiperusteisten telepakkokeinojen käyttö on edelleen pakkokeinolain mukaisiin vastaaviin keinoihin verrattuna vähäistä, mutta niiden käytössä tapahtui vuonna 2022 selkeää nousua. Poliisilakiperusteista televalvontaa on

[97] Riitta Ollila, Teletunnistetietojen säilytysvelvollisuus – Euroopan unionin tuomioistuimen Tele2-tuomio. Lakimies 3–4/2017 s. 494–504, 500.

ollut vuosittain vajaassa 200 tapauksessa sekä telekuuntelua ja valvontaa muutamassa kymmenessä.[98] Työryhmän saamien tietojen mukaan yli puolessa tapauksissa näin saaduilla tiedoilla on ratkaiseva tai tärkeä merkitys. Vain noin 10-20 % tapauksissa telepakkokeinoilla hankituilla tiedoilla ei ole ollut merkitystä. Valtaosassa tapauksista käytetyillä telepakkokeinoilla on arvioitu olleen jonkin asteista merkitystä rikoksen selvittämisessä.[99]

Toisaalta viranomaistarpeisiin säädetyn säilytysvelvollisuuden kumoaminen ei myöskään tarkoittaisi sitä, että näitä tietoja ei säilytettäisi lainkaan. Tällöin suuren määrän rikoksia selvittäminen riippuisi siitä, onko teleyrityksellä tiedot vielä tallella omia tarkoituksiaan varten. Työryhmän saaman selvityksen mukaan tietojen säilytysajoissa on operaattorikohtaisia eroa. Lisäksi osaa tietoja, kuten IP-osoitteita tai tietoja vastaamattomista puheluista, säilytetään vain lyhyen aikaa. Erot teleyritysten välillä niiden säilytyspolitiikassa on tunnistettu kumoamisen riskiksi myös oikeuskirjallisuudessa.[100] Tällöin tietojen saatavuus olisi sattumanvaraista ja saannin ennakoitavuus heikkoa. Mikäli viestinnän välitystietoja ei ole saatavilla, joutuvat viranomaiset turvautumaan muihin tiedonhankintakeinoihin tietotarpeen täyttämiseksi. Tällöin kyseeseen voi tulla toimenpiteet, joista johtuu vakavampi perusoikeusrajoitus, kuten telekuunteluun.

Unionin tuomioistuin onkin todennut, että sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohta ilmentää sitä, että perusoikeuskirjan 7, 8 ja 11 artiklassa vahvistetut oikeudet eivät ole ehdottomia vaan ne on suhteutettava siihen tehtävään, joka niillä on yhteiskunnassa. Siten on otettava huomioon myös perusoikeuskirjan 3, 4, 6 ja 7 artiklassa vahvistettujen oikeuksien tärkeys sekä kansallisen turvallisuuden suojelua ja vakavan rikollisuuden torjuntaa koskevien tavoitteiden tärkeys, millä myötävaikutetaan muiden henkilöiden oikeuksien ja vapauksien suojeluun. Siltä osin kuin on kyse erityisesti sellaisten rikosten tehokkaasta torjunnasta, joiden uhreja ovat etenkin alaikäiset ja muut haavoittuvaisessa asemassa olevat henkilöt, on otettava huomioon, että perusoikeuskirjan 7 artiklasta voi seurata viranomaisia koskevia toimintavelvollisuuksia sellaisten oikeudellisten toimenpiteiden toteuttamiseksi, joilla suojataan yksityis- ja perhe-elämää. Tällaiset velvollisuudet voivat perustua myös mainittuun 7 artiklaan kodin ja viestien suojaamisen osalta sekä 3 ja 4 artiklaan jokaisen ruumiillisen ja henkisen koskemattomuuden suojaamisen osalta sekä kidutuksen sekä epäinhimillisen tai halventavan kohtelun kiellon osalta. (G. D. kohta 49)

Unionin tuomioistuin on lisäksi todennut, että kun otetaan huomioon nämä erilaiset toimintavelvollisuudet, kyseessä olevat legitiimit intressit ja oikeudet on välttämättä

[98] Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2022, s. 4 ja 14-15.
[99] Poliisihallituksen kertomus, s. 13.
[100] Riitta Ollila, Teletunnistetietojen säilytysvelvollisuus – Euroopan unionin tuomioistuimen Tele2-tuomio. Lakimies 3–4/2017 s. 494–504, 503.

sovitettava yhteen. Euroopan ihmisoikeustuomioistuin on näet katsonut, että ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen 3 ja 8 artiklasta johtuvat toimintavelvollisuudet, joita vastaavat takeet sisältyvät perusoikeuskirjan 4 ja 7 artiklaan, edellyttävät muun muassa sellaisten aineellisten ja menettelyllisten säännösten antamista sekä sellaisten käytännön toimenpiteiden toteuttamista, joilla voidaan tehokkaasti torjua henkilöihin kohdistuvia rikoksia tehokkaalla tutkinnalla ja syytteeseenpanolla, ja tämä velvollisuus on sitäkin tärkeämpi, kun lapsen fyysinen ja henkinen hyvinvointi ovat uhattuina. Niiden toimenpiteiden osalta, jotka toimivaltaisten viranomaisten on toteutettava, on kuitenkin noudatettava täysimääräisesti lain määräämää järjestystä ja muita takeita, joilla voidaan rajoittaa rikostutkintavaltuuksien laajuutta, sekä muita vapauksia ja oikeuksia. Kyseisen tuomioistuimen mukaan on erityisesti luotava oikeudellinen kehys, jonka avulla voidaan sovittaa yhteen legitiimit intressit ja suojeltavat oikeudet. (G. D. kohta 50) Kun otetaan huomioon nämä erilaiset toimintavelvollisuudet, kyseessä olevat legitiimit intressit ja oikeudet on välttämättä sovitettava yhteen, ja on erityisesti luotava oikeudellinen kehys tätä yhteensovittamista varten. (SpaceNet kohta 65)

Säilytysvelvollisuus on aikaisemmin arvioitu välttämättömäksi. Myös perustuslakivaliokunta on aikanaan pitänyt sääntelyä perustuslain yleisten rajoitusedellytysten valossa mahdollisena. Säilytysvelvollisuutta koskevaa sääntelyä puoltaa perustuslakivaliokunnan mukaan vakavan rikollisuuden torjuntaan liittyvä hyväksyttävä peruste.[101]

Huomioon voidaan myös ottaa, että Suomi on ratifioinut 23.11.2001 tehdyn Euroopan neuvoston tietoverkkorikollisuutta koskevan yleissopimuksen (Euroopan sopimussarja – nro 185, ”Budapestin sopimus”). Lisäksi Suomi on myös allekirjoittanut, mutta ei vielä ratifioinut, Budapestin sopimuksen 2. lisäpöytäkirjan (CETS No. 224). Unionin tuomioistuin on huomauttanut (QdN kohta 162), että sopimuksen 14 artiklassa määrätään, että sopimuspuolet ryhtyvät yksittäistä rikostutkintaa tai rikosoikeudenkäyntiä varten jo tallennettujen liikennetietojen osalta tiettyihin säilyttämisen nopean varmistamisen kaltaisiin toimenpiteisiin. Kyseisen yleissopimuksen 16 artiklan 1 kappaleessa määrätään erityisesti, että sopimuspuolet ryhtyvät tarvittaviin lainsäädännöllisiin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet määrätä tai muutoin varmistaa nopeasti sellaisten liikennetietojen säilyttäminen, jotka on tallennettu tietojärjestelmän avulla, erityisesti silloin kun on syytä uskoa, että näiden tietojen häviäminen tai muuttaminen on erityisen todennäköistä. Kyseisen yleissopimuksen 20 artiklassa määrätään, että kukin sopimuspuoli ryhtyy tarvittaviin lainsäädännöllisiin ja muihin toimenpiteisiin antaakseen toimivaltaisille viranomaisilleen valtuudet: a) hankkia tai tallentaa kyseisen sopimuspuolen alueella teknisin keinoin, ja b) velvoittaa palveluntarjoaja sen olemassa olevan teknisen valmiuden puitteissa: i) hankkimaan tai tallentamaan kyseisen sopimuspuolen alueella teknisin keinoin; tai ii) toimimaan yhteistyössä toimivaltaisten viranomaisten kanssa ja avustamaan niitä, kun nämä hankkivat

[101] Ks. PeVL 18/2014 vp, s. 7.

tai tallentavat, reaaliajassa tietoja liikennetiedoista, jotka liittyvät yksilöityjen viestien siirtämiseen tietojärjestelmän avulla kyseisen sopimusvaltion alueella.

Lisäksi voidaan ottaa huomioon viime aikainen eurooppalainen kehitys varmistaa lainvalvontaviranomaisten riittävä tietojen saanti. Unionissa on esimerkiksi vastikään hyväksytty E-evidence-sääntely, jonka tavoitteena on parantaa sähköisten todisteiden turvaamista ja hankkimista yli rajojen. E-evidence-asetuksella ((EU) 2023/1543) ja e-evidence-direktiivillä ((EU) 2023/1544) säädetään sähköistä todistusaineistoa rikosasioissa koskevista eurooppalaisesta esittämismääräyksestä ja säilyttämismääräyksestä ja laillisten edustajien nimittämisestä sähköisen todistusaineiston keräämiseksi rikosasioissa. Asetuksessa säännellään, miten ja millä edellytyksillä jäsenvaltion lainvalvontaviranomainen voi suoraan velvoittaa Euroopan unionin alueella palveluita tarjoavan palveluntarjoajan toimittamaan tai säilyttämään tietyn palveluntarjoajan hallussa olevan sähköisessä muodossa olevan tiedon käytettäväksi todistusaineistona käynnissä olevassa rikosoikeudellisessa menettelyssä. Kysymys voisi olla esimerkiksi sähköpostia koskevista sisältö- tai lähetystiedoista. Asetuksella ei ole tarkoitettu vaikutettavan jäsenvaltioiden sisäisiin menettelyihin, joissa on kysymys lainvalvontaviranomaisen oikeuksista velvoittaa samassa jäsenvaltiossa toimivaa palveluntarjoajaa luovuttamaan tietoja. Mahdollisessa kansallisessa sääntelyssä ei kuitenkaan voida säätää asetuksen sääntelyn vastaisesti. Direktiivissä säännellään palveluntarjoajien laillisten edustajien nimittämistä todistusaineiston keräämisen helpottamiseksi rikosasioissa. Kyseisten säädösten edellyttämä kansallisen lainsäädännön valmistelu on aloitettu syksyllä 2023.

Edellä mainitut seikat puoltavat sitä, että säilytysvelvollisuudesta säädettäisiin jatkossakin, eikä kumoaminen vaikuta realistiselta vaihtoehdolta.

6.2 Nykyisen säilytysvelvollisuuden säilyttämisen riskit

Sähköisen viestinnän tietosuojadirektiivin jättämää kansallista liikkumavaraa on käsitelty yllä jaksossa 3. Nykyinen kansallinen säilytysvelvollisuutta koskeva lainsäädäntö on säädetty perustuslakivaliokunnan myötävaikutuksella Digital Rights Ireland -ratkaisun antamisen jälkeen. Tällöin perustuslakivaliokunta katsoi, että kyseisen tuomion valossa näyttäisi olevan perusteltua pyrkiä rajaamaan säilyttämisvelvollisuutta sekä henkilöpiirin että viestinnän osalta. Tämän katsottiin kuitenkin olevan sekä asiallisesti että teknisesti erittäin vaikea toteuttaa. Perustuslakivaliokunta katsoi, ettei tuomiosta johtunut suoranaista estettä sellaiselle sääntelylle, jossa oikeasuhtaisuuden vaatimukset toteutetaan muilla tavoin. Sääntelyllä on myös hyväksyttävä peruste. (PeVL 18/2014 vp, s. 6–7)

Nykyistä lainsäädäntöä on arvioitu yksityiskohtaisesti vuonna 2017[102]. Sittemmin unionin tuomioistuin on monilta osin kehittänyt edelleen ja täsmentänyt Digital Rights Ireland -ratkaisulla luomaansa viestinnän välitystietojen yleiseen ja erotuksettomaan säilytysvelvollisuuteen liittyvää tulkintakäytäntöään. Tämän jälkeen asiassa on laadittu arviomuistio vuonna 2021 sekä sitä täydentävä jatkoselvitys vuonna 2023.

Vuoden 2017 selvityksessä on eritelty Suomen välitystietojen säilyttämistä. Selvityksen johtopäätöksenä on, että kansallinen lainsäädäntö sisältää rajoituksia säilytysvelvollisuuteen, pääasiassa seuraavasti[103]:

- Säilytysvelvollisuus on rajattu tiettyihin teleyrityksiin sisäministeriön päätöksellä, mikä rajaa maantieteellistä kattavuutta;

- Säilytysvelvollisuus on rajattu tiettyihin palveluihin ja niiden sisällä tiettyihin tietoluokkiin;

- Säilytyksen kestoa on rajattu kansallisessa lainsäädännössä palveluluokittain 6, 9 ja 12 kk säilytysaikoihin;

- Säilytettyjä tietoja saavien viranomaisten henkilöpiiriä on rajattu;

- Laissa edellytetään, että ne henkilöt, jotka edellä mainituissa viranomaisissa saavat tutkia televalvonnalla saatuja tietoja, määrätään erikseen.

Suomessa olevaa säilytysvelvollisuutta ei ole valtioneuvoston piirissä tehdyissä arvioissa pidetty yleisenä ja erotuksettomana vaan rajattuna[104]. Unionin tuomioistuimen linjausten perusteella ei kuitenkaan voida sulkea pois sitä vaihtoehtoa, että unionin tuomioistuimen arvioinnissa suomalaista säilyttämisvelvollisuutta päädyttäisiin pitämään yleisenä ja erotuksettomana.[105] Myös oikeuskirjallisuudessa suomalaisen säilytysvelvollisuuden on katsottu olevan yleistä ja erotuksetonta.[106]

---

[102] Liikenne- ja viestintäministeriö, Selvitys sähköisen viestinnän välitystietojen säilytysvelvollisuudesta, 22.6.2017, Raportit ja selvitykset 9/2017 (LVM 9/2017).
[103] Ks. LVM 9/2017, s. 22.
[104] Ks. LVM 9/2017, s. 22.
[105] Ks. jatkoselvitys 2023, s. 19.
[106] Pekka Savola, Sähköisen viestinnän luottamuksellisuuden rajoitusten oikeasuhtaisuuden arvioimisesta.
Oikeus, tieto ja viesti – Viestintäoikeuden vuosikirja 2015 s. 50–89, 74; Riitta Ollila, Teletunnistetietojen säilytysvelvollisuus – Euroopan unionin tuomioistuimen Tele2-tuomio. Lakimies 3–4/2017 s. 494–504, 495. Toisaalta myös vastakkainen näkemys on esitetty joskin sekin on ajalta ennen SpaceNet-ratkaisua (ks. Mikael Lohse, Sähköisen viestinnän välitystietojen säilyttäminen ja käyttäminen. Defensor Legis 5/2017, s. 745–753, 750–752).

Vuoden 2017 selvityksessä tunnistettujen säilytysvelvollisuutta pääasiassa rajaavia tekijöitä on arvioitu yksityiskohtaisemmin vuoden 2023 jatkoselvityksessä. Tiivistetysti pääasialliset säilytysvelvollisuuden rajoitukset näyttäytyvät unionin tuomioistuimen uudemman oikeuskäytännön valossa seuraavasti:

2017 esitetyt pääasialliset rajoitukset säilyttämisvelvollisuuteen	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[107]	FI säilytettävien tietojen laajuus vaikuttaa vastaavan olennaisin osin SpaceNet-ratkaisussa käsiteltyä tietojen säilyttämisen laajuutta (ks. alla tarkemmin)
Säilytyksen kestoa 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
Säilytettyjä tietoja saavien viranomaisten henkilöpiiriä on rajattu Laissa edellytetään, että tietoja tutkivat henkilöt määrätään erikseen	Vastaava kirjaus sisältyy DE lainsäädäntöön; EUT ei kuitenkaan arvioinut tätä erikseen (SpaceNet kohta 91)	EUT:n mukaan säilyttämisestä johtuvaa perusoikeuksiin puuttumista ei voida rajoittaa tai korjata pääsyä koskevien rajoituksien noudattamisella

Yhtenä vaihtoehtona voidaan pitää nykytilan säilyttämistä. Kuten vuoden 2023 jatkoselvityksessä on arvioitu, nykyisen sääntelyn osalta ei kuitenkaan voida sulkea pois sitä vaihtoehtoa, että suomalaista säilyttämisvelvollisuutta pidettäisiin yleisenä ja erotuksettomana. Unionin tuomioistuin on korostanut, että kansallinen lainsäädäntö, jossa säädetään liikenne- ja paikkatietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä, kattaa lähes koko väestön sähköisen viestinnän ilman, että tehtäisiin mitään erottelua, rajoituksia tai poikkeuksia tavoitteen perusteella. Tällainen säännöstö koskee yleisellä tavalla kaikkia sähköisiä viestintäpalveluja käyttäviä henkilöitä, vaikka kyseiset henkilöt eivät ole edes välillisesti tilanteessa, joka voisi johtaa rikosoikeudelli-

[107] Ks. tarkemman erittelyn osalta vuoden 2023 jatkoselvityksen liite 1.

sen menettelyn vireillepanoon. (QdN kohta 143 ja siinä viitattu oikeuskäytäntö) Tarkastellessaan Saksan säilyttämisvelvollisuutta koskevaa lainsäädäntöä unionin tuomioistuin kiinnitti huomiota siihen, että lainsäädännössä säädetty säilyttämisvelvollisuus ulottuu *hyvin laajaan liikenne- ja paikkatietojen kokonaisuuteen*, joka vastaa olennaisin osin tietoja, jotka unionin tuomioistuin on katsonut unionin oikeuden vastaiseksi. Saksan kansallisessa lainsäädännössä säädetty liikenne- ja paikkatietojen säilyttäminen koskee lähes kaikkia väestöön kuuluvia henkilöitä, vaikka he eivät ole edes välillisesti tilanteessa, joka voisi johtaa rikosoikeudellisen menettelyn vireillepanoon. Siinä säädetään samoin liikenne- ja paikkatiedoista olennaisen osan sellaisesta säilyttämisestä, joka on perustetta edellyttämätöntä, yleistä ja henkilöllisesti, ajallisesti ja maantieteellisesti erottelematonta. (SpaceNet kohdat 81-83)

LVM:n arvion mukaan Suomen kansallinen välitystietojen säilyttämisvelvollisuus vaikuttaa vastaavan olennaisin osin sellaista tietojen säilyttämisen laajuutta, jonka unionin tuomioistuin on todennut unionin oikeuden vastaiseksi. Mikäli sähköisen viestinnän palveluista annetun lain 157 § riitautettaisiin ja tulevaisuudessa todettaisiin unionin oikeuden vastaiseksi, sitä ei voisi EU-oikeuden etusijan takia soveltaa. Kuten unionin tuomioistuin on muistuttanut esimerkiksi G. D. -ratkaisussaan, unionin oikeuden ensisijaisuuden periaatteella vahvistetaan unionin oikeuden etusija jäsenvaltioiden oikeuteen nähden. Kyseisen periaatteen mukaan on niin, että jos kansallinen tuomioistuin, jonka tehtävänä on toimivaltansa puitteissa soveltaa unionin oikeuden säännöksiä ja määräyksiä, ei voi tulkita kansallista säännöstöä unionin oikeuden vaatimusten mukaisesti, sillä on velvollisuus varmistaa kyseisten säännösten ja määräysten täysi vaikutus ja jättää tarvittaessa omasta aloitteestaan soveltamatta kaikkia unionin oikeuden kanssa ristiriidassa olevia, myös myöhemmin annettuja kansallisen lainsäädännön säännöksiä ilman, että sen olisi pyydettävä tai odotettava, että tällainen säännös ensin poistetaan lainsäädäntöteitse tai jollakin muulla perustuslain mukaisella keinolla. (G. D. kohta 118 ja siinä viitattu oikeuskäytäntö)

Lainsäädännön nykytilasta ja EU-oikeuden tulkinnan kehittymisestä voi seurata, että tuomioistuimet eivät myöntäisi takautuvaa televalvontaa säilytysvelvollisuuden nojalla säilytettyihin tietoihin, koska säilytysvelvollisuutta voidaan pitää EU-oikeuden vastaisena. Tällä voisi myös olla vaikutus nykykäytännön mukaan säilytettyihin tietoihin. Teleyritykset voisivat lopettaa tietojen säilyttämisen tai poistaa säilyttämänsä tiedot. Jo todistusaineeksi saatujen tietojen voitaisiin väittää olevan lainvastaisesti saatuja.

Sähköisen viestinnän tietosuojadirektiivin 15 artiklan vastaisen säilyttämisen kautta hankittujen todisteiden hyväksyttävyys kuuluu jäsenvaltioiden menettelyllistä itsemääräämisoikeutta koskevan periaatteen mukaisesti kansallisen oikeuden alaan, edellyttäen, että muun muassa vastaavuus- ja tehokkuusperiaatteita noudatetaan. (ks. esim. G. D. kohta 128) Suomessa on sääntelyä lainvastaisesti saatujen todisteiden hyödyntämisestä (ks. KKO:2023:14 sekä oikeudenkäymiskaaren 17 luvun 25 §).

Mikäli nykyinen kansallinen lainsäädäntö säilytetään muuttamattomana, kansalliseen lainsäädäntöön nykyisessä muodossa liittyy riski siitä, että se katsottaisiin unionin oikeuden vastaiseksi. Tällöin on olemassa riski siitä, että välitystietoja ei ole saatavissa takautuvan televalvonnan keinoin tai saatujen tietojen hyödynnettävyys todistusaineistona systemaattisesti kyseenalaistettaisiin, kunnes kansallista lainsäädäntöä muutettaisiin.

Havaittujen epäselvyyksien ennakollisella täsmentämisellä voitaisiin varmistaa, että viranomaisilla on oikeasuhtainen ja oikeutettu pääsy sähköisen viestinnän välitystietoihin perusoikeuksia kunnioittavalla tavalla myös tulevaisuudessa. Kansallista lainsäädäntöä olisi tarpeen täsmentää, jotta varmistetaan sen olevan Suomen perustuslain ja EU:n perusoikeuskirjan, siten kuin unionin tuomioistuin on sitä oikeuskäytännössään tulkinnut, mukainen, rajoittuvan yksityiselämän suojan kannalta välttämättömään ja samalla turvataan viranomaisille oikeutetun ja oikeasuhtaisen pääsyn tietoihin tehokkaan rikostorjunnan ja kansallisen turvallisuuden varmistamiseksi.

6.3 Säilytysvelvollisuuden täsmentäminen unionin tuomioistuimen oikeuskäytännön linjausten mukaisesti

6.3.1 Unionin tuomioistuimen oikeuskäytännöstä johtuvat säilytystoimenpiteet

Unionin tuomioistuin on edellä jaksossa 3 tarkasteltujen reunaehtojen lisäksi käsitellyt oikeuskäytännössään eräitä säilyttämistoimenpiteitä, jotka eivät tuomioistuimen mukaan olisi unionin oikeuden vastaisia. Unionin tuomioistuimen mukaan unionin oikeus ei ole esteenä lainsäädännöllisille toimenpiteille, joissa

– sallitaan kansallisen turvallisuuden takaamiseksi se, että **sähköisten viestintäpalvelujen tarjoajat määrätään säilyttämään liikenne- ja paikkatiedot yleisesti ja erotuksetta tilanteissa, joissa asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka**, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi, ja joko tuomioistuin tai riippumaton hallinnollinen elin, jonka ratkaisu on sitova, voi kohdistaa päätökseen, jolla tällainen määräys annetaan, tehokasta valvontaa, jolla pyritään tarkastamaan, että kyseessä on jokin näistä tilanteista ja että niitä edellytyksiä ja takeita, joista on säädettävä, noudatetaan; mainittu määräys voidaan antaa ainoastaan ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa, jos kyseinen uhka on edelleen olemassa;

– säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi **liikenne- ja paikkatietojen kohdennetusta säilyttämisestä**, joka on objektiivisten ja syrjimättömien seikkojen perusteella **rajattu asianomaisten henkilöiden ryhmien mukaan tai maantieteellisen kriteerin avulla** ajanjaksoksi, joka on rajoitettu täysin välttämättömään mutta jota voidaan jatkaa;

– säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi **liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksettomasta säilyttämisestä** ajanjaksoksi, joka on rajoitettu täysin välttämättömään;

– säädetään kansallisen turvallisuuden suojaamiseksi, rikollisuuden torjumiseksi ja yleisen turvallisuuden suojaamiseksi **sähköisten viestintävälineiden käyttäjien henkilöllisyyttä koskevien tietojen yleisestä ja erotuksetta tapahtuvasta säilyttämisestä**; ja

– sallitaan vakavan rikollisuuden torjumiseksi ja varsinkin kansallisen turvallisuuden takaamiseksi se, että **sähköisten viestintäpalvelujen tarjoajat määrätään toimivaltaisen viranomaisen päätöksellä**, johon kohdistuu tehokas tuomioistuinvalvonta, **varmistamaan nopeasti** 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 asianomaisilla henkilöillä on tehokkaat takeet väärinkäytön vaaroja vastaan. (QdN tuomiolauselma)

Sittemmin unionin tuomioistuin on täsmentänyt tulkintaansa aikaisemmasta ratkaisukäytännöstään ja erityisesti rikollisuuden torjunnan tavoitteen näkökulmasta (ks. 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)

Näissä säilyttämisperusteissa unionin tuomioistuin on arvioinut mahdollisia säilyttämistoimenpiteitä suhteutettuna perusoikeuksiin puuttumisen vakavuuteen. (Tele2

kohta 115) Säilyttämistoimenpiteiden tulee pääsääntöisesti olla luonteeltaan poikkeuksellisia. (G. D. kohta 75 ja 40 sekä siinä viitattu oikeuskäytäntö)

Unionin tuomioistuimen ratkaisuissa jätetään kuitenkin kansallisen lainsäätäjän harkintavaltaan monia seikkoja. Seuraavaksi käsitellään yksityiskohtaisemmin eri seikkoja, joita säilyttämistoimenpiteiden toteuttamiseksi tulisi kansallisessa lainsäädännössä ottaa huomioon ja ratkaista. Tämän arviomuistion tarkoituksena on arvioida erilaisia vaihtoehtoja, miten kansallinen säilytysvelvollisuutta koskeva lainsäädäntö voitaisiin tulevaisuudessa järjestää. Kaikkiin säilytystoimenpiteisiin liittyviin kysymyksiin ei ole ollut mahdolilista saada arviomuistion laatimisen aikana vastauksia. Arviointia täydennetään jatkovalmistelun aikana.

6.3.2 Säilytysperusteiden eriyttäminen ja yleisen edun mukaisten tavoitteiden hierarkia

Sähköisen viestinnän palveluista annetun lain 157 §:n mukaan kyseisestä pykälästä seuraavan säilytysvelvollisuuden perusteella säilytettyjä tietoja saa käyttää ainoastaan pakkokeinolain 10 luvun 6 §:n 2 momentissa määriteltyjen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi. Sittemmin käyttöä on laajennettu tiedustelulaeilla myös siviili- ja sotilastiedustelun tarkoituksiin. SVPL 157 §:ssä ei kuitenkaan ole nimenomaisesti mainittu säilyttämisperustetta, eikä tietojen käyttöä ole jaoteltu näiden säilyttämisperusteiden mukaisesti. Sähköisen viestinnän palveluista annetun lain 322 §:n mukaan viranomaisten oikeudesta saada välitystietoja rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi säädetään poliisilaissa, rikostorjunnasta Rajavartiolaitoksessa annetussa laissa, henkilötietojen käsittelystä Rajavartiolaitoksessa annetussa laissa, rikostorjunnasta Tullissa annetussa laissa, henkilötietojen käsittelystä Tullissa annetussa laissa ja pakkokeinolaissa. Saman lain 157 §:n perusteella säilytettäviä tietoja voivat saada säilytysvelvollisilta yrityksiltä ainoastaan ne viranomaiset, joilla on lain perusteella oikeus saada tiedot.[108]

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) Lii-

[108] Ks. tarkemmin SVPL 322 §:n muutostarpeiden arvioinnista jäljempänä jakso 7.5.

kenne- 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. (G. D. kohta 47) Sekä tietojen säilyttämisvelvollisuutta että tietojen saantia tulee siis tarkastella erillisinä kokonaisuuksina.

Tuomioistuimen oikeuskäytännön mukaan oikeus saada säilytysvelvollisuuden perusteella säilytettyjä tietoja 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) Sitä vastoin säilytettyjen tietojen saaminen päinvastaisessa tilanteessa olisi vastoin yleistä etua koskevien tavoitteiden hierarkiaa. (G. D. kohta 99)

Unionin tuomioistuin on tunnistanut yleisen edun tavoitteiden mukaisessa hierarkiassa seuraavan jaottelun:

1) rikollisuuden torjunta yleensä ja yleisen turvallisuuden suojaaminen;

2) vakavan rikollisuuden torjunta ja yleistä turvallisuutta koskevan vakavan uhan torjuminen;

3) kansallisen turvallisuuden takaaminen.

Nykyisin Suomen kansallisessa lainsäädännössä ei tehdä vastaavaa erottelua säilytysperusteiden välillä. Säilytysperuste ei käy nimenomaisesti ilmi SVPL 157 §:ssä, vaan siinä viitataan tietojen käyttöön. Lisäksi SVPL 157 §:ssä viitataan pakkokeinolain televalvonnan perusterikoksiin. Kyseinen lista ei kuitenkaan ole identtinen niiden rikosten kanssa, joihin televalvontaa voidaan käyttää rikoksen estämiseen, paljastamiseen tai vaaran torjumiseen muun lainsäädännön nojalla.

Näin ollen käyttötarkoituksia ei ole eritelty tiettyihin säilytysperusteisiin nähden. Kansallista lainsäädäntöä voisi olla tarpeen tältä osin täsmentää. Säilytysvelvollisuutta koskevasta sääntelystä tulisi käydä selvästi ilmi, mihin yleisen edun tavoitteeseen säilytysvelvollisuus perustuu. Muutos kohdistuisi sähköisen viestinnän palveluista annetun lain 157 §:ään. Säilytysvelvollisuuden alaisten tietojen käyttötarkoitus voitaisiin täydentää vastaamaan käytäntöä tietojen käytöstä myös rikosten ennalta estämiseen. Tarkkaa sanamuotoa on kuitenkin arvioitava vielä PL 10.4 §:n ja sähköisen viestinnän tietosuojadirektiivin 15(1) artiklan termejä vasten.

Lisäksi on huomattava, että poliisilla on oikeus saada viestinnän välitystietoja eräissä poliisitutkinnoissa ja eräissä muissa poliisitehtävissä. Poliisitutkinnalla tarkoitetaan muuta poliisin toimitettavaksi laissa säädettyä tutkintaa kuin rikoksen johdosta toimitettavaa esitutkintaa. Sähköisen viestinnän palvelulain 157 §:ssä ei ole erikseen säädetty säilyttämisvelvollisuudesta näihin poliisitehtäviin. Vastaavia käyttötarkoituksia ei ole mainittu sähköisen viestinnän tietosuojadirektiivin 15(1) artiklassa, mutta ne voisi mahdollisesti kiinnittää joko yleiseen turvallisuuteen[109] tai rikosten torjuntaan, tutkintaan ja selvittämiseen. Perustuslain 10 §:n 4 momentin käyttötarkoituksista voitaisiin puolestaan kiinnittyä yksilön turvallisuutta vaarantavien rikosten tutkintaan. Tämän säilytysvelvollisuuden tulisi olla välttämätöntä.

Unionin tuomioistuin ei ole oikeuskäytännössään käsitellyt erikseen yllä kuvattujen poliisitutkintojen kaltaisten tilanteiden asettumista sähköisen viestinnän luottamuksellisuutta koskevaan oikeuskäytännön kehykseen. Säilytysperusteen ja käyttötarkoituksen symmetriaa tulee arvioida yleisen edun mukaisten tavoitteiden hierarkian valossa. Tietojen säilyttämistä ja saantia poliisitutkintoihin on käsitelty tarkemmin jäljempänä jaksossa 7.6.

Käytännössä sama tieto saattaisi kuitenkin tulla säilytettäväksi usealla eri perusteella. Näin olisi esimerkiksi sellaisissa tilanteissa, joissa tietyn alueen tai tietyn käyttäjän viestintään liittyviä tietoja voitaisiin vaatia säilytettäväksi sekä kansallisen turvallisuuden suojaamiseksi että vakavan rikollisuuden torjumiseksi. Tietojen eriytetty säilyttäminen eri käyttötarkoituksia varten voisi aiheuttaa merkittäviä lisäkustannuksia ja moninkertaista säilyttämistä, jos tietojen säilyttäminen tulisi teknisesti toteuttaa siten, että eri säilytysperusteen tiedot säilytettäisiin erillään toisistaan. Työryhmän saaman selvityksen perusteella vaikuttaa kuitenkin siltä, että eri perusteilla säilytettävät tiedot voitaisiin tallentaa yhteen järjestelmään, jolloin vältyttäisiin samalle yritykselle aiheutuvista kustannuksista, joka johtuisi saman tiedon tallentamisesta moneen kertaan. Sääntelyssä tulisi pyrkiä siihen, että sama tietotyyppi säilytettäisiin vain kertaalleen.

Työryhmän saamien tietojen mukaan teknisesti olisi mahdollista tiedon tallentamisen yhteydessä määritellä sille tietyt arvot, millä perusteella kyseistä tietoa säilytetään, jolloin tietoon pääsyn yhteydessä voidaan varmistua siitä, ettei pääsyä myönnetä sellaiseen tietoon, jonka säilyttämisperuste ei ole unionin tuomioistuimen edellyttämällä tavalla symmetrinen tiedon käyttötarkoituksen kanssa. Tällaisten arvojen asettamisesta aiheutuu kuitenkin etenkin käytännön käyttöönoton yhteydessä kustannuksia. Tällä

[109] Tällöin tosin mentäisiin perinteisestä turvallisuuskäsityksestä (suoja väkivallalta) kohti laajaa turvallisuuskäsitystä (myös muun muassa muun muassa köyhyyteen, terveyteen, ympäristöön ja henkilökohtaiseen koskemattomuuteen liittyvät uhat). Tällainen laajentuminen olisi kuitenkin hyväksytty perustuslakivaliokunnan käytännössä. (Niklas Vainio, Viestinnän yksityisyyden suojan turvallisuusperusteinen rajoittaminen perustuslakivaliokunnan käytännössä. Lakimies 6/2017 s. 813–837, 815–817.)

hetkellä teleyritysten järjestelmissä olevien viestintätietojen luokittelu eri säilytysperusteisiin edellyttäisi manuaalista työtä, mikä olisi ilmeisen aikaa vievää ja vaivalloista, ja tästä aiheutuisi yrityksille merkittäviä henkilöstökustannuksia. Ottaen huomioon säilytetyn tiedon määrä, tästä voisi mahdollisesti seurata, että ennen sääntelyn voimaantuloa syntyneille tiedoille ei ole mahdollista määrittää erillistä säilytysperustetta. Siten sääntelyssä tulisi varmistaa tarpeellinen siirtymäaika, jotta säilyttämisperusteiden eriyttäminen voitaisiin toteuttaa automaattisesti tiedon syntymisen ja tallentamisen hetkellä.

Nykykäytännön mukaan kukin säilytysvelvollinen yritys vastaa itse tietojen säilyttämisestä. Tietojen saantipyynnöt toimitetaan yrityksille Salpa-järjestelmän avulla. Säilyttämisperusteiden eriyttäminen johtaisi siihen, että palveluntarjoajien tulisi jatkossa tarkistaa tietopyyntöihin vastattaessa käyttöperusteen lisäksi sen sopivuus suhteessa säilytysperusteeseen. Jatkovalmistelussa on vielä arvioitava säilytysperusteiden eriyttämisen perusoikeusvaikutuksia.

6.3.3 Säilytysvelvollisuuden asettaminen rikollisuuden torjumiseksi ja yleisen turvallisuuden takaamiseksi

6.3.3.1 Kohdennettu säilyttäminen maantieteellisen kriteerin perusteella

Unionin tuomioistuin on oikeuskäytännössään edellyttänyt, että toimenpiteen kohteet ovat objektiivisten ja syrjimättömien seikkojen perusteella rajattu. Maantieteellinen säilyttämiskriteeri voi koskea erityisesti sellaisia paikkoja, joilla on yhteys vakavan rikollisuuden esiintymiseen tai erityinen alttius tällaisiin rikoksiin. Maantieteellisesti kohdennettu säilyttämistoimenpide voidaan toteuttaa joko tilastotiedon valossa (paikat, joilla tehdään lukuisia vakavia rikoksia) tai tiettyyn paikkaan liittyvän uhkan perusteella (paikat, jotka ovat erityisen alttiita vakavien rikosten tekemiselle, kuten paikat ja infrastruktuurit, joissa käy säännöllisesti hyvin suuri määrä henkilöitä taikka strategiset paikat). Strategisia paikkoja voivat olla esimerkiksi lentoasemia, rautatieasemia, merisatamia tai tietullialueita. (G. D. kohta 79 oikeuskäytäntöviittauksineen) Säilyttäminen voi perustua maantieteelliseen kriteeriin, kuten rikollisuuden keskimääräiseen määrään jollakin maantieteellisellä alueella, ilman että niillä välttämättä olisi konkreettisia indisioita vakavan rikoksen valmistelusta tai tekemisestä asianomaisilla alueilla. (G. D. kohta 80)

Unionin tuomioistuimen oikeuskäytännöstä on tunnistettavissa kaksi erillistä vakavan rikollisuuden uhkaan liittyvää maantieteellisen kriteerin mahdollisuutta: rikollisuuden määrä tai esiintyminen tilastojen valossa sekä kriittisen infrastruktuurin tai muutoin

korkeariskiset alueet ja paikat. Tuomioistuimen oikeuskäytäntö jättää kuitenkin huomattavasti liikkumavaraa siihen, miten nämä alueet määritellään.

Maantieteellisen säilyttämistoimenpiteen kriteeristössä voidaan ottaa huomioon esimerkiksi yleiseen turvallisuuteen kohdistuvien uhkien todennäköisyys tai vakavien rikosten määrä suhteessa asukaslukuun tietyllä maantieteellisellä alueella.

Maantieteellisen alueen yksiköitä voi olla esimerkiksi kunnat, kuten Ruotsin selvityksessä on ehdotettu. Isompana tarkasteltavana yksikkönä voisi olla myös maakunnat. Tanskan ja Belgian malleissa maa on jaettu tietyn neliökilometrimäärän kokoisiin alueisiin. Alustavien arvioiden mukaan Suomessa kunta- tai maakuntaperusteinen alueiden tarkastelu olisi neliökilometriin perustuvaa rajaa käyttökelpoisempi ainakin tietoja tarvitsevien viranomaisten näkökulmasta.

Strategisina ja rikoksille alttiina paikkoina tulisi arvioida kansallisen turvallisuuden ja maanpuolustuksen kannalta keskeisten kohteiden sijaintia sekä yhteiskunnan kannalta elintärkeiden toimintojen sijaintia ja näihin liittyvää uhkaa. Tällaisia alueita voisivat olla esimerkiksi kunnat, joissa sijaitsevat isoimmat rajanylityspaikat tai kriittistä infrastruktuuria. Kriittisen infrastruktuurin alueiden määrittelyssä voitaisiin huomioida esimerkiksi CER-direktiivi[110], huoltovarmuuskeskuksen tiedot tai valtioneuvoston asetus kriittisistä sähkönkäyttöpaikoista (981/2022). Muita alueita voisivat olla esimerkiksi suuret juna-asemat, vankilat, lentokentät tai poliisiasemat.

Esimerkiksi CER-direktiivin mukaan kriittisellä infrastruktuurilla tarkoitetaan hyödykettä, tilaa, laitteistoa, verkostoa tai järjestelmää tai osaa hyödykkeestä, tilasta, laitteistosta, verkostosta tai järjestelmästä, joka on välttämätön sellaisen palvelun, joka on olennainen välttämättömien yhteiskunnan toimintojen, taloudellisen toiminnan, kansanterveyden, yleisen turvallisuuden tai ympäristön ylläpitämiseksi, tarjoamiseksi.[111] Sähkönkäyttöpaikka-asetuksen 2 §:ssä on määritelty kriittiset sähkönkäyttöpaikat, joita ovat esimerkiksi yhdyskuntien vesihuoltopalveluiden keskeiset kohteet, joilla on erityistä terveydensuojelullista tai ympäristönsuojelullista merkitystä, häiriöttömän sähköntoimituksen jatkumisen tai palauttamisen kannalta välttämättömät kantaverkonhaltijan, sähkönjakeluverkonhaltijoiden ja sähköntuottajien valvomot, sähköasemat, merkittävät sähkövarastot ja sähköntuotantolaitokset sekä näiden käyttämät viestintäverkoai kaasun siirtoverkon keskeiset kohteet.

Rikollisuuden määrään perustuva säilyttämiskriteeri olisi mahdollista asettaa joko suhteelliseen rajaan perustuen (keskimääräistä korkeampi rikollisuus tietyllä alueella joh-

[110] Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2557, annettu 14 päivänä joulukuuta 2022, kriittisten toimijoiden häiriönsietokyvystä ja direktiivin 2008/114/EY kumoamisesta. CER sanoista *Critical Entities Resilience*.
[111] CER-direktiivin 2 artiklan 4 ja 5 alakohdat.

taisi alueelliseen kohdennettuun säilyttämismääräykseen) tai kiinteään rajaan perustuen (kaikki tietyn raja-arvon ylittävät alueet tulisivat säilytysvelvollisuuden piiriin. Esimerkiksi Tanskan kansallinen lainsäädäntö perustuu tällaiseen suhteelliseen rajaan, kun taas Belgian mallissa rikollisuuden esiintyvyyttä tarkastellaan kiinteän raja-arvon perusteella.

Kiinteä raja saattaa johtaa siihen, että merkittävä rikollisuuden lasku voisi tarkoittaa suurten alueiden tippumista säilytysvelvollisuuden ulkopuolelle, mutta toisaalta kiinteällä rajalla voidaan käytännössä mahdollistaa lähes koko Suomen kattava säilytysvelvollisuus. Tämä riippuisi pitkälti siitä, mille tasolle säilytysvelvollisuuden laukaiseva kynnys asettuisi. Käytännössä lähes koko maan kattava säilyttämisvelvollisuus olisi kuitenkin nykytilaan verrattuna kestävämpi, sillä säilyttämisperuste olisi asetettu EUT:n oikeuskäytännön mukaisesti objektiivisen kriteerin eli vakavan rikollisuuden määrän perusteella. Tällainen laajamittainen säilyttäminen voisi olla jossain määrin rikosten uhrien yhdenvertaisen kohtelun kannalta kannatettavaa, kun taas suhteelliseen rajaan perustuva säilyttäminen saattaisi asettaa ihmiset eriarvoiseen asemaan. Tältä osin EUT on kuitenkin todennut, että kohdennettu (eli rajatumpi) säilyttäminen ei ole vastoin uhrien yhdenvertaisen kohtelun vaatimusta (Spetsializirana prokuratura (Bulgaria) 44 kohta).

Mikäli taas alueilla esiintyviä rikosmääriä tarkasteltaisiin suhteessa muilla alueilla tapahtuvaan rikollisuuden määrään ja vain tämän perusteella keskimääräistä useammin vakavan rikollisuuden kohteeksi joutuvien alueiden tiedot säilytettäisiin, tarkoittaisi tämä käytännössä sitä, että välttämättä olisi aina joitain alueita, joilta tietoja ei ole säilytysvelvollisuuden nojalla saatavilla.

Rikollisuuden määrään perustuva maantieteellinen kriteeri edellyttäisi tilastotietojen saantia. Rikollisuuden määrää arvioitaessa voitaisiin ottaa huomioon esimerkiksi televalvontatiedoissa esiintyvät alueet. Myös tilastokeskuksen mahdollista roolia tulisi selvittää.

Nykyisen SVPL 157 §:n mukaisesti sisäministeriö voisi olla toimivaltainen viranomainen tällaisen säilyttämismääräyksen antamiseen. Maantieteelliseen kriteeriin perustuva säilyttämismääräys palvelisi potentiaalisesti laajasti esitutkinta- ja tiedusteluviranomaisia. Tällainen säilyttäminen edellyttäisi oletettavasti myös merkittäviä järjestelmäkustannuksia säilytysvelvollisissa yrityksissä. Tällaisten kustannusten korvaaminen puoltaisi sitä, että myös jatkossa sisäministeriö voisi antaa säilyttämismääräyksen.

Maantieteellisen kriteerin perusteella toimitettava säilytystoimenpide voitaisiin osoittaa tiettyihin alueella sijaitseviin tukiasemiin. Työryhmän saamien tietojen mukaan tukiasemaverkko kuitenkin jatkuvasti elää. Maantieteellinen kohdentaminen vaatii siten operaattoreilta jatkuvaa (manuaalista) työtä. Tämä lisää virheiden mahdollisuutta sekä aiheuttaa kustannuksia. Koska teleyritys tekisi kohdentamisen tukiasematietojen perusteella, teleyrityksen näkökulmasta ei ole ratkaisevaa merkitystä, määriteltäisiinkö

säilytyskohde maantieteellisesti esimerkiksi postinumeron tai kuntien rajojen perusteella. Teleyritys joutuu nämä alueet joka tapauksessa määrittelemään tukiasemiensa kautta. Yksi tarkasteltava vaihtoehto olisikin, voitaisiinko tiettyä maantieteellistä aluetta vastaavat tukiasemat määrittää tietyin määräajoin tai jos tukiasemissa on tapahtunut olennaisia muutoksia.

Jatkovalmistelussa tulisi selvittää tarkemmin sitä, määritettäisiinkö alueellinen säilytysvelvollisuus tietyllä alueella sijaitsevien vai sitä palvelevien tukiasemien kautta. Jälkimmäinen vaihtoehto tarkoittaisi käytännössä sitä, että määräyksessä asetettaisiin kriteerit, joilla tukiaseman katsottaisiin palvelevan säilytysvelvollisuuden piiriin kuuluvaa aluetta. Tällaisen määrittelyn tarkkuus vaikuttaa kuitenkin epävarmalta.[112] Sama tukiasema voi palvella useaa aluetta ja siten sekä säilytysvelvollisuuden piiriin kuuluvaa että sen ulkopuolelle rajautuvaa aluetta. Tämä saattaa johtaa käytännön ongelmaan, kun määritellään sitä, missä tilanteissa tietty henkilö olisi viestintätapahtuman aikana säilytysvelvollisuuden piiriin kuuluvalla alueella. Tällainen tilanne saattaisi johtaa siihen, että teleyritykselle tallentuisi tietoja myös säilytysvelvollisuuden ulkopuolisilta alueilta. Säilytysvelvollisten yritysten oikeusturvan vuoksi olisi kannatettavaa, että maantieteellinen kriteeri olisi riittävän yksiselitteinen ja tarkkarajainen, jotta tällaisilta tilanteilta vältyttäisiin. Tästä syystä säilytysmääräyksen kohdistaminen tietyllä maantieteellisellä alueella sijaitseviin tukiasemiin vaikuttaisi alustavan arvion mukaan perustellulta ratkaisulta.

Mikäli säilytysvelvollisuus haluttaisiin kohdentaa esimerkiksi tietyn kriittisen infrastruktuurin alueella tapahtuvaan viestintään, tulisi jatkovalmistelussa selvittää myös sitä, miten laaja alue tällöin tulisi säilyttämisvelvollisuuden kohteeksi. Yksi vaihtoehto voisi olla määrittää säilyttämisvelvollisuus sellaisiin kuntiin, joissa kriittistä infrasturktuuria sijaitsee.

Jatkovalmistelussa ratkaistava kysymys on myös se, millä perusteella tietyn henkilön viestinnän katsotaan tapahtuneen säilytysvelvollisuuden piiriin kuuluvalla alueella. Keskeinen kriteeri tulisi olla se, onko henkilö ollut viestinnän aikana jollakin hetkellä kyseisellä alueella.[113] Säilytysvelvollisuus koskisi jatkossakin viestinnän välittämiseen liittyviä tietoja, joten muusta syystä säilytysvelvolliselle yritykselle syntyvät tai tallentuvat sijainnin ilmaisevat tiedot eivät tulisi tallennettavaksi. Säilytysvelvollisuuden rajaaminen alueellisesti saattaisi johtaa siihen, että tietyissä tilanteissa tietyn viestintätapahtuman tiedot saattaisivat olla puutteellisia, mikäli henkilö siirtyisi viestintätapahtuman aikana säilytysvelvollisuuden piiriin kuuluvan alueen ulkopuolelle. Säilytysvelvollisuuden seuraaminen henkilön mukana säilytysvelvollisuuden piiriin kuuluvan alueen

[112] Tukiasemien tarkka kuuluvuusalue voi olla haastavaa määrittää laskennallisesti, eikä rajoja voi vetää viivoittimella, koska radioverkkojen olosuhteet vaihtelevat. Viallinen tai tehonsäästömoodissa oleva tukiasema/solu voi muuttaa sitä, mitkä tukiasemat tai solut palvelevat tietty aluetta. Myös rankat sääolosuhteet saattavat vaikuttaa asiaan.
[113] Vastaavasti esim. Belgian kansallisessa sääntelyssä.

ulkopuolelle olisi kuitenkin säilytysvelvollisen yrityksen kannalta haastavaa tai mahdotonta käytännössä toteuttaa, sillä tämä edellyttäisi säilytystoimenpiteen ulottamista myös sellaisille alueille, joita ei olisi määrätty säilytysalueeksi ja joilta siis lähtökohtaisesti tietoja ei tulisi säilyttää. Tämä olisi myös ongelmallista säilytysperusteen oikeutuksen kannalta: tällainen viestintätapahtuman seuraaminen johtaisi siihen, että säilytysvelvollisuus laajenisi käytännössä myös sellaisille alueille, jotka eivät ole täyttäneet säilytysvelvollisuudelle asetettua objektiivista kriteeriä.

Erillinen kysymys on laajemmin se, miten voidaan katsoa viestinnän tapahtuvan tietyllä alueella. Sääntelyn hyväksyttävyyden kannalta säilytysvelvolliselle yritykselle asetettava velvoite käsitellä käyttäjien tietoja ainoastaan käyttäjän sijainnin selvittämiseksi vaikuttaa ongelmalliselta. Perustuslakivaliokunta on aikaisemmin pitänyt suhteellisuusperiaatteen kannalta tärkeänä, ettei palveluntarjoajaa velvoiteta erikseen tuottamaan tai hankkimaan tietoja, vaan ainoastaan säilyttämään tarjoajan saatavilla muutenkin olevat tiedot. (PevL 3/2003, s. 2/II, PeVL 3/2006 vp, s. 3/I, PeVL 35/2004 vp, s. 3/II) Nykyisten säilytysvelvollisuuteen kuuluvien palveluluokkien kannalta tämä vaikuttaa ongelmalliselta erityisesti internetpuhelinpalveluiden tallentamisen kannalta.[114] Jatkovalmistelussa tulee selvittää vielä yksityiskohtaisemmin, miten maantieteellinen säilytyskriteeri käytännössä vaikuttaisi säilytettäviin tietoihin ja johtaisiko se käytännössä vain tiettyjen palveluluokkien tietojen, kuten matkaviestinverkon viesti- ja puhelinpalveluihin liittyvien tietojen tallentamiseen.

Kohdennetun säilyttämisen kriteerit tulisi määritellä lainsäädännössä, joten kriteerit, joihin maantieteellisesti kohdistettu säilyttämismääräys voidaan kohdistaa, olisivat julkisia. Toimenpiteen tehokkuuden kannalta kyseenalaista olisi kuitenkin sellaisen tiedon julkistaminen, josta kävisi laajalle yleisölle ilmi, että kaikki liikenne- ja paikkatiedot tietyllä alueella säilytetään tietyn aikaa. Tällöin henkilöt, joihin liittyviä liikenne- ja paikkatietoja viranomaiset myöhemmin voisivat tarvita, voisivat välttää kyseisillä alueilla liikkumista. Tämä voisi merkittävästi vähentää toimenpiteellä potentiaalisesti saavutettavaa hyötyä. Tästä syystä jatkovalmistelussa tulisi vielä tarkastella yksityiskohtaisemmin tarvetta asettaa tiedot tietyn säilytystoimenpiteen toteuttamisesta tietyllä maantieteellisellä alueella salassa pidettäviksi. Erityisesti tulee selvittää, kattavatko julkisuuslain nykyiset salassapitoperusteet nämä tiedot vai pitäisikö säätää uusi peruste.

Maantieteellisiä alueita voidaan ja tarvittaessa täytyy mukauttaa niiden valinnan perusteena olleiden olosuhteiden kehityksen mukaan, mikä mahdollistaa muun muassa

[114] IP-osoitteiden säilyttämisvelvollisuuden osalta ei ole ilmennyt tarvetta kohdentaa säilyttämistä maantieteellisesti. IP-osoitteiden säilyttämisvelvollisuutta käsitellään jäljempänä tarkemmin. Selvityksen laatimisen yhteydessä on myös esitetty kysymys esimerkiksi maantieteellisen säilytyskriteerin soveltamisesta satelliittipuhelinpalveluiden tietoihin. Nämä puhelinpalvelut eivät kuitenkaan ole SVPL 157 §:n mukaan säilytettäviä palveluluokkia, eikä selvityksen laatimisen aikana ole myöskään esitetty tarvetta laajentaa säilytysvelvollisuutta kattamaan tällaisia palveluita.

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) Säilytysvelvollisuuden piiriin kuuluvia alueita on siis syytä tarkastella säännöllisesti, jotta varmistetaan toimenpiteen tehokkuus ja välttämättömyys. Tarkasteluvälin tulisi olla riittävän pitkä, jotta sekä säilytysvelvollisille yrityksille että säilytysmääräyksen antavalle viranomaiselle alueiden määrittelystä aiheutuva hallinnollinen taakka ei muodostu kohtuuttomaksi. Tämä on myös yritysten oikeusvarmuuden sekä viranomaisten toiminnan kannalta olennaista. Toisaalta liian pitkä tarkasteluväli saattaa johtaa siihen, että viranomaiset eivät voi riittävän tehokkaasti tai nopeasti reagoida tietyllä alueella mahdollisesti tapahtuviin rikollisuuden tai sen riskin muutoksiin. Maantieteelliseen kriteeriin perustuvan säilyttämisen etuna on tietty pysyvyys. Tästä syystä tarkasteluvälin ei tulisi olla 12 kuukautta lyhyempi aika. Vuosittaiseen tarkasteluväliin on päädytty myös Tanskan kansallisessa lainsäädännössä sekä Ruotsin säilytysvelvollisuuden uudistamista koskevassa esityksessä.

6.3.3.2 Kohdennettu säilyttäminen henkilöpiirin perusteella

Unionin tuomioistuin on oikeuskäytännössään edellyttänyt, että toimenpiteen kohteet ovat objektiivisten ja syrjimättömien seikkojen perusteella rajattu. Kohteeksi valikoidut henkilöt voivat muun muassa olla henkilöitä, jotka on etukäteen tunnistettu sovellettavien kansallisten menettelyjen yhteydessä objektiivisten ja syrjimättömien seikkojen perusteella henkilöiksi, jotka aiheuttavat uhan asianomaisen jäsenvaltion yleiselle turvallisuudelle tai kansalliselle turvallisuudelle. (QdN kohta 149) Säilyttämistoimenpide voidaan unionin tuomioistuimen mukaan 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 (Bulgaria) kohta 46)

Henkilöperusteinen ennakollinen tietojen säilyttäminen olisi kansallisessa lainsäädännössä uudentyyppinen toimenpide. Toimenpiteellä rajattaisiin ennakollisesti sellaiset henkilöt, joihin voitaisiin myöhemmin kohdistaa televalvontaa. Kyse olisi tietynlaisesta telepakkokeinon käyttöä edeltävästä ja valmistelevasta menetelmästä. Toisaalta toimenpiteellä rajattaisiin tosiasiallisesti henkilöitä tulevan televalvonnan ulkopuolelle, sillä vaikka myöhemmin ilmenisi oikeutettu peruste saada tietyn henkilön viestinnän tietoja, niitä ei välttämättä ole enää tallennettuna viranomaisten käyttöä varten.

Työryhmän saaman selvityksen mukaan esimerkiksi sellaisia henkilöitä, joihin on edellisinä vuosina kohdistettu telepakkokeinoja ja joiden viestinnän tietoihin kohdistetaan lähivuosien aikana tietopyyntöjä, on vain muutamia vuosittain. Siten esimerkiksi

säilyttämistoimenpiteen kohdistaminen aikaisempien rikosepäilyjen perusteella ei vaikuta tehokkaalta tavalta varmistaa tietojen säilyttämistä. Lisäksi ongelmallisena voidaan pitää tilannetta, jossa aikaisemman tuomion perusteella automaattisesti rajoitettaisiin henkilön oikeutta yksityiselämän suojaan.[115]

Unionin tuomioistuin ei ole kuitenkaan oikeuskäytännössään rajannut henkilöperusteista kohdentamista sellaisiin henkilöihin, joihin on aikaisemmin kohdistettu telepakkokeinoja, vaan unionin tuomioistuimen mukaan tämä kriteeri voi kattaa laajemmankin joukon, esimerkiksi koskien henkilöitä, joilla on aikaisempaa taustaa vakavista rikoksista. Henkilöperusteinen kohdentaminen on unionin tuomioistuimen mukaan mahdollista myös henkilöihin, jotka ovat tutkinnan tai muiden valvontatoimenpiteiden kohteina. Jälkimmäisen osalta toimenpide saattaisi olla päällekkäinen myöhemmin käsiteltävän tietojen nopean säilyttämisen varmistamisen kanssa.

Säilytysvelvolliset yritykset toivat selvityksen aikana esiin, että säilytysvelvollisuuden kohdentaminen tiettyyn henkilöön olisi teknisesti helppoa, mikäli määräys annettaisiin esimerkiksi liittymän numeron perusteella. Teleoperaattorien näkökulmasta liittymän ostaneen henkilön henkilöllisyyden selvittäminen tai se, mitä liittymiä henkilöllä on käytössä, kuuluvat viranomaisten tehtäviin eikä teleoperaattorille. Toisaalta taas tietoja tarvitsevien viranomaisten näkökulmasta on haastavaa, miten tietyn henkilön käyttämät numerot sidottaisiin näihin henkilöihin, sillä henkilön kautta ei ole helppo saada liittymän tosiasiallista käyttäjää selville.

Vakavan ja järjestäytyneen rikollisuuden toimijat käyttävät yleisesti rekisteröimättömiä teleliittymiä ja laiteita. Siten on epävarmaa, kohdistuisiko säilytysvelvollisuus toiminnallisesti oikein, vaikka viranomainen pystyisi laatimaan ja ylläpitämään luetteloa säilytysvelvollisuuden piirissä olevista henkilöistä.

Henkilöperusteinen säilyttämiskriteeri tulisi määritellä myös siten, että se olisi käytännössä toteutettavissa. Teknisesti henkilöperusteinen säilyttäminen olisi helppo toteuttaa liittymän numeron tai IMEI-koodin perusteella. Toisaalta IMEI-koodin perusteella kohdistettuna säilytysvelvollisella yrityksellä ei olisi näkymää siihen, mikäli puhelin vaihtaisi omistajaa. Sen sijaan esimerkiksi rekisteröimättömiä prepaid-liittymiä hyödyntävien henkilöiden tunnistaminen olisi mahdotonta, sillä teleoperaattoreilla ei välttämättä ole tietoa siitä, kuka liittymän on ostanut ja kuka sitä käyttää. Säilyttämisvelvoitteen toteuttamisesta aiheutuisi nykytilaan verrattuna säilytysvelvollisille yrityksille kustannuksia, sillä säilytysvelvoitteen kohteita tulisi säännöllisesti päivittää. Automatisoituna toteutettuna päivittämisestä ei aiheutuisi vastaavia kustannuksia. Tällöin tulisi

[115] Esimerkiksi oikeusasiamies Jääskeläinen on rikostiedustelulainsäädäntöä koskevan lausuntonsa yhteydessä suhtautunut hyvin varauksellisesti ajatukseen, että vankeusrangaistukseen tuomittu henkilö menettäisi automaattisesti osan perustuslaissa taatusta henkilötietojen suojasta. EOAK/2827/2023, s.7.

erityisesti kiinnittää kuitenkin huomiota käsittelyn suojatoimiin ja muihin edellytyksiin, joita arkaluontoisten tietojen käsittelystä säädettäessä tulee huomioida.

Henkilöön liittyvän säilyttämiskriteerin muotoilu siten, että se olisi samaan aikaan sekä tiedon tarpeen täyttävä että toteuttamiskelpoinen, on varsin haastavaa. Lisäksi rikostaustan perusteella ja uhka-arvion perusteella laadittava säilytystoimenpiteen kohteiden lista johtaisi käytännössä siihen, että teleyrityksille muodostuisi mahdollisesti kattaviakin tietokantoja valtion turvallisuusviranomaisten rekisteröimistä henkilöistä. Hieman samankaltaista valtion turvallisuusviranomaisten henkilörekisterien sisältämien tietojen laajamittaista käsittelyä muissa henkilörekistereissä on - huomattavasti vähäriskisemmissä konteksteissa - pyritty torjumaan henkilötietojen käsittelystä poliisitoimessa annetun lain 54 §:n 2 momentin sääntelyllä. Tällaisten henkilölistojen käsittely edellyttäisi säilytysvelvollisilta yrityksiltä erityisiä toimenpiteitä kyseisten tietojen luottamuksellisuuden ja turvallisuuden varmistamiseksi. Kuten yllä jaksossa 4.2 on todettu, henkilöllisen kohdentamisen mahdollistavien henkilötietojen luovuttamisesta ja niiden käsittelystä teleyrityksissä tulisi säätää erikseen, ottaen huomioon tällaisesta käsittelystä rekisteröidyille aiheutuva riski ja yleisen tietosuoja-asetuksen 10 artikla.

Sähköisen viestinnän tietosuojadirektiivissä ei säädetä, millä edellytyksin viranomaiset voivat toimittaa teleyrityksille sellaisia henkilötietoja, joiden avulla teleyritykset voisivat kohdentaa säilyttämistä henkilöllisin perustein. Direktiivissä ei myöskään säädetä teleyrityksille erillistä käsittelyperustetta valikoida kyseisen listan perusteella välitystiedot ja säilyttää ne. Viranomaisten tietojenluovutuksen osalta kyseinen sääntely kuuluisi todennäköisesti nk. rikosasioiden tietosuojadirektiivin (EU) 2016/680 soveltamisalaan, sillä tietojen luovutuksen tarkoitus liittyy rikosten ennalta estämiseen, tutkimiseen tai paljastamiseen[116]. Sen sijaan teleyritysten osalta tällaisten henkilötietojen käsittely kuuluisi todennäköisesti sekä sähköisen viestinnän tietosuojadirektiivin että yleisen tietosuoja-asetuksen soveltamisalaan (lakisääteinen velvoite).[117]

Perustuslakivaliokunnan mukaan tietosuoja-asetuksen yksityiskohtainen sääntely, jota tulkitaan ja sovelletaan EU:n perusoikeuskirjassa turvattujen oikeuksien mukaisesti, muodostaa yleensä riittävän säännöspohjan myös perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta. Henkilötietojen suoja tulee turvata ensisijaisesti EU:n yleisen tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla.

---

[116] Liikkumavara ei siten tulisi sähköisen viestinnän tietosuojadirektiivin 15(1) artiklasta, koska kyseisten henkilötietojen luovuttamisessa ei suoraan ole kyse viestinnän luottamuksellisuuden rajoittamisesta.

[117] Vrt. EU:n tietosuojaneuvoston lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta, 31 ja 34 kohta. Rinnakkaisen soveltamisen kannalle on päädytty myös oikeuskirjallisuudessa, ks. Marko Priiki, Sähköisen viestinnän välitystietojen ja henkilötietojen käsittelyperusteiden suhteesta – kansallinen lainsäädäntö suoraan sovellettavan tietosuoja-asetuksen aikana. Oikeustiede - Jurisprudentia LVI:2023 s. 213–303, 256–257.

Kansallisen erityislainsäädännön säätämiseen tulee siten suhtautua pidättyvästi ja rajata sellainen vain välttämättömään tietosuoja-asetuksen salliman kansallisen liikkumavaran puitteissa (ks. PeVL 14/2018 vp, s. 4–5 ja PeVL 52/2022 vp, 4 kohta). Perustuslakivaliokunnan mukaan on kuitenkin selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksenkin edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä suurempi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn osalta (ks. PeVL 14/2018 vp, s. 5). Arkaluonteisten tietojen käsittelyn on oltava välttämätöntä ja sääntelyn täsmällistä ja tarkkarajaista (ks. PeVL 52/2022 vp, 7 kohta).

Rikostuomioihin ja rikoksiin liittyvät henkilötiedot voidaan myös lukea valtiosääntöisesti arkaluonteisiksi. (PeVL 15/2018 vp, s. 38) Siispä annettaessa sääntelyä, jolla sallittaisiin tai jopa edellytettäisiin tällaisten tietojen käsittelyä, tulee kiinnittää huomiota myös niiden edellyttämiin erityisiin suojakeinoihin.

Tässä tapauksessa kyse olisi sekä laajuudeltaan ja lajiltaan sellaisesta henkilötietojen käsittelystä, josta muodostuu erityisiä riskejä rekisteröidyn oikeuksille. Henkilöllisen kohdentamisen mahdollistavien henkilötietojen luovuttamisesta ja niiden käsittelystä teleyrityksissä tulisi säätää erikseen – ottaen huomioon myös yleisen tietosuoja-asetuksen 10 artikla.[118]

Henkilöperusteinen säilyttäminen parantaisi sivullisten yksityiselämän suojaa, sillä toimenpiteen kohteiden joukko olisi tarkkaan rajattu. Henkilöperusteisesti kohdennettuun säilyttämiseen liittyy erityisesti toimenpiteen ennakollinen ulottuvuus. Tiettyjen henkilöiden osoittaminen toimenpiteen kohteeksi esimerkiksi aikaisemman rikostaustan vuoksi on ei ole ongelmatonta syyttömyysolettaman näkökulmasta. Toimenpiteen hyväksyttävyyttä heikentää myös arviot siitä, että aikaisemman rikostaustan perusteella muodostettavaa henkilöiden piiriä ei voida pitää tehokkaana toimenpiteenä rikollisuuden torjunnan kannalta.

[118] Kyseisessä artiklassa säädetään rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelystä. Rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittely 6 artiklan 1 kohdan perusteella suoritetaan vain viranomaisen valvonnassa tai silloin, kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa säädetään asianmukaisista suojatoimista rekisteröidyn oikeuksien ja vapauksien suojelemiseksi. Kattavaa rikosrekisteriä pidetään vain julkisen viranomaisen valvonnassa.

6.3.3.3 Kohdennettu säilyttäminen muiden objektiivisten ja syrjimättömien kriteereiden perusteella

Unionin tuomioistuimen mukaan henkilöön liittyvien ja maantieteellisten kriteerien lisäksi myös muut erottavat kriteerit liikenne- ja paikkatietojen kohdennetun säilyttämisen toteuttamiseksi ovat mahdollisia. 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) Kuitenkaan 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).

Eräs tällainen kohdentamiskriteeri, joka ei suoraan liity ylläoleviin maantieteellisiin tai henkilöperusteisiin kriteereihin, voisi olla suuret ja kävijämäärältään merkittävät tapahtumat, joihin arvioidaan kohdistuvan kasvanut riski rikollisuudelle. Tällainen tapahtuma ei suoraan vastaa unionin tuomioistuimen oikeuskäytännössä eriteltyjä toimenpiteitä. Lainsäädännössä voitaisiin kuitenkin asettaa objektiiviset ja syrjimättömät kriteerit, joiden perusteella kyseeseen voisi tulla tapahtumat, joissa käy paljon ihmisiä ja jotka ovat erityisen alttiita vakavien rikosten tekemiselle. (vrt. QdN kohta 150)

Tapahtuman kestoksi annettava kohdennettu säilyttämismääräys olisi myös ajallisesti toteutettavissa siten, että sen kesto rajoittuu välttämättömään, sillä tiettyyn tapahtumaan liittyvä riski lienee usein ajallisesti tarkkaan määriteltävissä. Rikollisen toiminnan suunnittelu saattaa kuitenkin alkaa ennen tällaista hetkeä tai rikollinen toiminta voidaan suunnitella etäältä. Maantieteellisen kriteerin tavoin toimitettava säilytystoimenpide voitaisiin osoittaa tiettyihin tapahtuma-alueella sijaitseviin tukiasemiin.

Muut kohdentamisvaihtoehdot on syytä pitää mielessä. Niitä ei kuitenkaan voi pitää ensisijaisena vaihtoehtona, sillä niiden hyväksyttävyyteen unioninoikeuden näkökulmasta liittyy riskejä. Niitä voisi harkita täydentävänä keinona esimerkiksi tilanteessa, jossa maantieteellinen kohdentaminen rajautuisi melko pieneen osaan Suomea.

6.3.3.4 Quick freeze –säilyttämismääräys

Yhtenä mahdollisena kohdennettuna ja rajattuna säilyttämisperusteena unionin tuomioistuin on käsitellyt tietojen säilyttämisen nopeaa varmistamista (ns. quick freeze). Quick freeze -säilyttämismääräys on tuomioistuimen mukaan mahdollista toteuttaa vakavan rikollisuuden torjumiseksi ja kansallisen turvallisuuden takaamiseksi. Määräyk-

sen voisi antaa toimivaltainen viranomainen, jonka päätökseen kohdistuu tehokas tuomioistuinvalvonta. (QdN tuomiolauselma) Säilyttämismääräys kattaisi palveluntarjoajien käytössä olevat liikenne- ja paikkatiedot (QdN kohta 163), eli sellaiset tiedot, jotka ovat syntyneet ennen määräyksen antamista ja joita teleyritys käsittelee jonkin muun perusteen nojalla, sekä tiedot, jotka syntyvät määräyksen antamisen jälkeen.

Unionin tuomioistuin on edellyttänyt, että toimenpiteen välttämättömyyden varmistamiseksi säilyttämisvelvollisuuden on koskettava ainoastaan liikenne- ja paikkatietoja, joilla voidaan myötävaikuttaa vakavan rikoksen tai kansalliseen turvallisuuteen kohdistuvan loukkauksen selittämiseen. Säilyttämisen kesto on rajoitettava täysin välttämättömään, mutta sitä voidaan kuitenkin jatkaa, kun olosuhteet ja toimenpiteellä tavoiteltu päämäärä sen oikeuttavat. (QdN kohta 164)

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) Se voi myös kattaa rikoksen uhrin sosiaalista tai ammatillista lähipiiriä koskevat tiedot. (QdN kohta 165)

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)

Toisin kuin tietojen kohdennettu säilyttämismääräys maantieteellisen tai henkilöpiirin perusteella, quick freeze -määräys vaikuttaa unionin tuomioistuimen oikeuskäytännön mukaan edellyttävän tiettyä konkreettista rikosepäilyä tai kansallista turvallisuutta uhkaavan tilanteen selvittämistä. Säilyttäminen kohdistuisi vain määräyksenantohetkellä teleoperaattorin hallussa oleviin tietoihin ja sen jälkeen syntyviin tietoihin. Oikeuskäytännön perusteella vaikuttaa siltä, että quick freeze -määräystä ei olisi mahdollista antaa ennakollisesti tietyille alueille tai tiettyihin henkilöihin liittyen. Tällaisissa tilanteissa tulisi tarkasteltavaksi yllä esitelty kohdennettu säilyttämismääräys.

Kansallinen lainsäädäntö ei suoraan tunnista quick freeze -määräyksen kaltaista sääntelyä, mutta pakkokeinolaissa on säädetty datan säilyttämismääräyksestä, jolla viestinnän välittäjä voidaan velvoittaa säilyttämään viestinnän tiedot muuttumattomana. Datan säilyttämismääräyksen edellytyksenä on aie laite-etsinnän toimittamisesta ja vaara, että ennen sen toimittamista data, jolla voi olla merkitystä tutkittavana olevan rikoksen selvittämiselle häviää tai sitä muutetaan. (PKL 8:24 § 1 mom. ensimmäinen lause) Datan säilyttämismääräyksen edellytykset on siis sidottu laite-etsinnän toimittamisen edellytyksiin.[119] Quick freeze -määräys, siten kuin unionin tuomioistuin on sitä tulkintakäytännössään käsitellyt, ei edellyttäisi nimenomaista vaaraa siitä, että tiedot häviäisivät tai niitä muutettaisiin.

Quick freeze -säilyttämismääräys olisi kohdistettavissa sekä tietyn henkilön että tietyn maantieteellisen alueen perusteella. Unionin tuomioistuin on nimenomaisesti todennut, että tämä määräys voidaan kohdistaa esimerkiksi tietyn rikoksen tekopaikkoihin sekä rikoksesta epäillyn lisäksi myös uhrin ja hänen lähipiirinsä tietoihin. Tällaisella määräyksellä varmistettaisiin, että viranomaisilla olisi käytettävissä tiettyyn rikokseen tai kansallista turvallisuutta uhkaavaan tilanteeseen liittyviä liikenne- ja paikkatietoja. Maantieteelliseen alueeseen kohdistettu quick freeze –määräys voisi tarkoittaa esimerkiksi tietyn tolppaluvan alueella tapahtuneen viestinnän tietojen määräämistä säilytettäväksi.

Quick freeze -määräys tietyn henkilön tietojen säilyttämiseksi olisi viestinnän luottamuksellisuuden suojan kannalta vähemmän ongelmallinen, sillä toimenpiteellä puututtaisiin vain sellaisten henkilöiden tietoihin, joilla voidaan nähdä olevan yhteys vakavan rikoksen selvittämiseen tai kansallisen turvallisuuden varmistamiseen. Maantieteelliseen alueeseen, kuten rikoksen tekopaikkaan, kohdistettava quick freeze -määräys kohdistuisi todennäköisesti myös sellaisten alueella liikkuneiden henkilöiden tietoihin, jotka eivät suoraan liity selvitettävänä olevaan rikokseen. Säilyttäminen olisi kuitenkin nykyistä käytäntöä kohdennetumpaa.

Ainoana säilyttämistoimenpiteenä quick freeze –määräys ei vaikuta vastaavan riittävän tehokkaasti viranomaisten tiedonsaantitarpeisiin. Tällöin takautuva tiedonsaanti saattaisi olla sattumanvaraista ja riippuisi pitkälti palveluntarjoajien omista tarpeista, jolloin myös ennakoitavuus olisi heikkoa. Sen sijaan se voisi olla käyttökelpoisempi toimenpide yhdessä muiden säilyttämistoimenpiteiden kanssa ja niitä tukevana toimenpiteenä. Kyse voisi olla esimerkiksi maantieteellistä säilyttämistä tukevasta toimenpiteestä tilanteissa, joissa tietyllä alueella rikollisuuden määrä vähenisi niin, että

[119] PKL 10:50 on viittaus samaan datan säilyttämismääräykseen, jota voidaan käyttää telepakkokeinopuolella esimerkiksi silloin, kun säilytysvelvollisuuden alaisia tietoja olisi säilytysajan rajoituksen vuoksi poistumassa ja kyseisiä tietoja saatettaisiin vielä tarvita. Tällä pystytään varmistamaan tiedot, jotka muuten olisivat vaarassa hävitä. Poliisilaista vastaava viittaus puuttuu.

maantieteellinen säilytyskynnys ei ylittyisi. Samoin sillä voitaisiin pidentää säilytysaikoja tilanteissa, joissa laista seuraava säilytysaika olisi loppumassa, mutta televalvonnan kynnys ei vielä olisi ylittynyt.

6.3.3.5 IP-osoitteiden säilyttäminen

Unionin tuomioistuin on QdN-ratkaisussaan katsonut, että unionin oikeus ei ole esteenä kansalliselle lainsäädännölle, jossa säädetään kansallisen turvallisuuden takaamiseksi, vakavan rikollisuuden torjumiseksi ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksettomasta säilyttämisestä ajanjaksoksi, joka on rajoitettu täysin välttämättömään. Edellytyksenä on, että 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 asianomaisilla henkilöillä on tehokkaat takeet väärinkäytön vaaroja vastaan. (QdN tuomiolauselma).

Unionin tuomioistuimen mukaan viestinnän lähteen IP-osoitteet eivät ole yhtä arkaluonteisia kuin muut liikennetiedot, mikäli säilytyksen kohteena ovat ainoastaan lähteen eivätkä viestinnän vastaanottajan IP-osoitteet, sillä nämä osoitteet eivät paljasta sellaisinaan mitään tietoa niistä kolmansista henkilöistä, jotka ovat olleet yhteydessä viestinnän alullepanijana olevaan henkilöön. Toisaalta IP-osoitteita voidaan käyttää internetin käyttäjän verkkotoiminnan kattavaan jäljittämiseen, mikä mahdollistaa käyttäjän yksityiskohtaisen profiilin selvittämisen. Siten IP-osoitteiden säilyttäminen ja analysointi merkitsee vakavaa puuttumista internetin käyttäjän perusoikeuksiin. (QdN kohdat 152-153)

Verkkorikoksen tapauksessa IP-osoite voi kuitenkin olla ainoa tutkintakeino, jolla voidaan yksilöidä henkilö, jolle tietty osoite oli annettu rikoksen tekohetkellä. Verkkorikosten paljastaminen voi osoittautua mahdottomaksi, mikäli kyseisiä tietoja ei ole direktiivin 2002/58 15 artiklan 1 kohtaan perustuvalla lainsäädännöllisellä toimenpiteellä säilytettävä pidemmäksi ajanjaksoksi. (QdN kohta 154) Liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksettomasta säilyttämisestä johtuva puuttuminen yksityiselämän suojaan ja henkilötietojen suojaan on kuitenkin vakavaa, joten ainoastaan vakavan rikollisuuden torjunta ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen sekä kansallisen turvallisuuden takaaminen voivat oikeuttaa kyseisen puuttumisen. (QdN kohta 156)

Säilyttämisen kesto ei saa ylittää sitä, mikä on täysin välttämätöntä tavoitellun päämäärän kannalta. Lopuksi on todettava, että tällaisessa toimenpiteessä on säädettävä *tiukoista* edellytyksistä ja takeista asianomaisten henkilöiden verkossa suorittaman viestinnän ja toteuttamien toimien osalta siltä osin kuin on kyse näiden tietojen hyödyntämisestä muun muassa jäljittämällä. (QdN kohta 156)

Unionin tuomioistuimessa on vireillä ennakkoratkaisupyyntö, jossa käsitellään IP-osoitetta vastaavaa henkilöllisyyttä koskevien tietojen säilyttämistä ja saantia, ja erityisesti unionin tuomioistuimen kyseisten tietojen saantia tekijänoikeuksien suojaamiseksi koskevan oikeuskäytännön (Promusicae, M.I.C.M. –ratkaisut) ja yksityiselämän suojaa koskevan oikeuskäytännön (erityisesti QdN-ratkaisu) arvioiminen (asia C-470/21, jäjempänä QdN II –ratkaisuehdotus). Julkisasiamiehen ratkaisuehdotus on annettu 28.9.2023.

Liittymän lähteelle annettujen IP-osoitteiden säilyttämisestä on vakava puuttuminen perusoikeuksiin (QdN 153 ja 156 kohta). Koska IP-osoitteiden saaminen voi kuitenkin olla ainoita tapoja selvittää verkossa tapahtuneita vakavia rikoksia, unionin tuomioistuin on suhtautunut sallivasti niiden yleiseen ja erotuksettomaan säilyttämiseen täysin välttämättömään rajatuksi ajanjaksoksi (QdN 154 kohta). IP-osoitteen ja sitä vastaavan henkilöllisyyden perusteella ei pelkästään ole mahdollista tehdä yhtä pitkällisiä päätelmiä henkilön yksityiselämästä kuin muiden välitystietojen osalta (QdN 157 kohta).

Tällä hetkellä sähköisen viestinnän palveluista annetun lain 157 §:n 5 momentissa on nimenomaisesti suljettu säilyttämisvelvollisuuden ulkopuolelle verkkosivustojen selaamisesta kertyvät välitystiedot. Perusoikeusrajoituksen oikeasuhtaisuuden ja unionin tuomioistuimen oikeuskäytännön valossa voidaan pitää kannatettavana nykytilan säilyttämistä.

Toimenpiteen välttämättömyyden sekä oikeuksien ja intressien yhteensovittamisen kannalta on erityisesti kiinnitettävä huomiota siihen, että verkkorikosten tapauksessa IP-osoite saattaa olla ainoa tutkintakeino, jolla voidaan yksilöidä henkilö, jolle kyseinen IP-osoite oli annettu tietyn rikoksen tekohetkellä. (QdN kohdat 153-154, ks. vastaavasti QdN II-ratkaisuehdotus 27.10.2022, kohta 65)[120]

Sen sijaan IP-osoitteita koskeviin tietoihin – vaikka niitä voi säilyttää yleisesti ja erotuksettomasti – pääsyyn on noudatettava tiukasti sellaisia aineellisia ja menettelyllisiä edellytyksiä, joita kyseisten tietojen käyttöön on sovellettava (QdN 155 kohta). Siten kyseiset tietopyynnöt jo unionioikeuden tulkintavaikutuksen takia eivät voi kohdistua

[120] Unionin tuomioistuin kiinnitti erityisesti huomiota siihen, että IP-osoite saattaa olla ainoa tutkintakeino lapsipornografian hankkimisen, levittämisen, välittämisen tai verkkoon lähettämisen tapauksissa. (QdN kohta 155) Julkisasiamies Szpunar on asian C-470/21 ratkaisuehdotuksissa ehdottanut tulkintaa, jonka mukaan sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohta mahdollistaisi IP-osoitetta vastaavien henkilöllisyyttä koskevien tietojen säilyttämisen ja saannin vain, kun on kyse sellaista rikosta koskevasta rikosoikeudellisesta menettelystä, jonka tekijää ei voitaisi tunnistaa ilman näitä tietoja. Julkisasiamies korostaa, että se koskisi ainoastaan rikoksia, jotka on tehty yksinomaan internetissä, eikä sillä kyseenalaistettaisi oikeuskäytäntöratkaisuja, jotka koskevat laajempien tietojen säilyttämistä ja saantia, joilla pyritään muihin tavoitteisiin. (QdN II –ratkaisuehdotus 28.9.2023 kohta 89)

säilytysvelvollisuuden nojalla säilytettäviin tietoihin, koska saantimenettely ilman tuomioistuinvalvontaa ei täytä unionioikeuden vaatimuksia.[121] Oikeuskirjallisuudessa on myös kysytty, täyttäisikö tällainen pääsy ihmisoikeussopimuksen vaatimukset[122] (ihmisoikeussopimuksen vaatimukset lailla säätämisestä ja ennakoitavuudesta[123]) tai perusoikeuksien rajoitusedellytykset.[124] Unionin tuomioistuimessa on kuitenkin yhä vireillä ennakkoratkaisupyyntö asiassa C-470/21, jossa käsitellään erityisesti IP-osoitteiden säilyttämistoimenpiteitä ja unionin tuomioistuimen oikeuskäytännössä asetettuja edellytyksiä tietojen tallentamiselle ja säilyttämiselle. Ottaen huomioon osittain epäselvä ja kehittyvä oikeustila, tulisi asiaa arvioida yksityiskohtaisemmin vasta asian C-470/21 ratkaisun valossa.

Nykyisen sääntelyn mukaan internetyhteyspalvelussa säilytysvelvollisuus koskee tilaajan ja rekisteröidyn käyttäjän nimeä ja osoitetta, liittymän tunnistetta ja asennusosoitetta sekä tietoa, jonka avulla voidaan yksilöidä viestintäpalvelun käyttäjä, viestintään käytetty laite sekä palvelun käytön ajankohta ja kesto. Säilytettävät tiedot tulee rajata vain siihen, mikä on palvelun tekninen toteutus huomioon ottaen välttämätöntä tässä tarkoitettujen seikkojen yksilöimiseksi.

Yleisenä lähtökohtana on, että IP-osoite on välitystieto silloin, kun sitä joko nykyhetkessä käsitellään tai sitä on aiemmin käsitelty viestinnän välittämiseen. IP-osoitteen välitystietoluonteeseen vaikuttaa se, mistä kyseinen IP-osoite on kerätty tai saatu.

Sähköisen viestinnän palveluista annetun lain 3 §:n 40 kohdan mukaan välitystiedolla tarkoitetaan muun ohella oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi. Kun IP-osoitetta käsitellään viestinnän välittämiseksi ja tieto on yhdistettävissä luonnolliseen tai oikeushenkilöön, on sitä pidettävä välitystietona.[125]

Liittymän IP-osoitteen tallentamisen kohdalla tiedon luonne voisi erota myös sen mukaan, onko kyse staattisesta vai dynaamisesta IP-osoitteesta. Tietoja verkosta kerättäessä tällä erottelulla ei ole merkitystä, mutta staattisen osoitteen kohdalla osoite voidaan saada myös asiakasrekisteristä ilman, että kyse olisi välitystiedosta (tällöin voisi olla kyse kuitenkin henkilötiedoista), joskaan näitä staattisia osoitteita ei yleensä ole

[121] Tietojen saantia omia tarkoituksia varten säilytettäviin tietoihin käsitellään tosin vielä vireillä olevassa asiassa C-241/22 DX.
[122] Pekka Savola, Sähköisen viestinnän luottamuksellisuuden rajoitusten oikeasuhtaisuuden arvioimisesta. Oikeus, tieto ja viesti – Viestintäoikeuden vuosikirja 2015 s. 50–89, 65–69 ja 83.
[123] Benedik v. Slovenia, 62357/14, § 127 ja 131–133.
[124] Pekka Savola, Tunnistamistietojen luovuttamismääräykset ja telepakkokeinot. Lakimies 5/2013 s. 886–908, 903–904 ja 907.
[125] Ks. KKO:2022:23, k. 26, Sittemmin kyseisessä kohdassa käytetty termi *tunnistamistieto* on korvattu termillä välitystieto (pakkokeinolaki 10:6 § (452/2023)).

kuluttajien käytössä. Dynaamisen IP-osoitteen määrittäminen teleyrityksen DHCP-palvelimen avulla katsotaan välitystietojen käsittelyksi, koska se tapahtuu viestinnän välittämisen mahdollistamiseksi[126]; vastaavasti tällaisen IP-osoitteen tallentaminen sekä myöhempi tarkastelu katsotaan välitystietojen käsittelyksi. Myös staattisen osoitteen käsittelyä on pidettävä välitystietojen käsittelynä, kun tieto osoitteesta kerätään verkkoelementeistä, jossa sitä on käsitelty viestinnän välittämiseen.

Joissain tilanteissa IP-osoite saattaa myös rinnastua asiakastietoihin.[127] Arvioitaessa sitä, onko jokin tieto välitystieto vai jotain muuta tietoa, ei ole merkitystä sillä, onko kyseinen tieto henkilötieto. Välitystiedot ovat usein henkilötietoja. Myös unionin tuomioistuimen oikeuskäytännössä IP-osoite on katsottu sekä henkilö- että liikennetiedoksi (QdN kohta 152 kohta ja tuomio 17.6.2021, M.I.C.M., C-597/19, EU:C:2021:492, 113 kohta).

Unionin tuomioistuin on katsonut, että vaikka IP-osoitteet kuuluvat liikennetietoihin, ne luodaan ilman, että ne liittyvät tiettyyn viestintään, ja niiden ensisijaisena tarkoituksena on tunnistaa sähköisten viestintäpalvelujen tarjoajien välityksellä luonnollinen henkilö, joka omistaa päätelaitteen, jonka kautta viestintä internetin välityksellä tapahtuu. Sähköpostin ja internetin välityksellä tarjottavien puhelinpalvelujen osalta on siis todettava, että siltä osin kuin pelkästään viestinnän lähteen eikä viestinnän vastaanottajan IP-osoitteet säilytetään, nämä osoitteet eivät paljasta sellaisinaan mitään tietoa niistä kolmansista henkilöistä, jotka ovat olleet yhteydessä viestinnän alullepanijana olevaan henkilöön. Tähän ryhmään kuuluvat tiedot eivät ole siis yhtä arkaluonteisia kuin muut liikennetiedot. Koska IP-osoitteita voidaan kuitenkin käyttää muun muassa internetin käyttäjän selailupolun ja siten hänen verkkotoimintansa kattavaan jäljittämiseen, näiden tietojen perusteella voidaan selvittää internetin käyttäjän yksityiskohtainen profiili. Mainittujen IP-osoitteiden säilyttäminen ja analysointi, jota tällainen jäljittäminen edellyttää, merkitsee siten sellaista vakavaa puuttumista perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin internetin käyttäjän perusoikeuksiin, jolla voi olla tämän tuomion 118 kohdassa tarkoitetun kaltainen ennalta ehkäisevä vaikutus. (QdN kohta 152-153)

---

[126] SVPL 3 §:n 40 kohta; KKO 2022:23, k. 26.

[127] Esimerkiksi tietoverkkorikoksia koskevassa Euroopan Neuvoston yleissopimuksessa (Sops 60/2007; ns. Budapestin sopimus; ETS 185) asiakastiedolla tarkoitetaan palveluntarjoajan tarjoamien palveluiden tilaajia koskevia tietoja, jotka eivät ole liikennetietoja tai viestin sisältöä koskevia tietoja, ja joita palveluntarjoaja säilyttää tietojärjestelmään tallennettuina, ja joista ilmenee esimerkiksi käytetyn viestintäpalvelun tyyppi ja sen kesto, sekä tilaajan henkilöllisyys ja muut asiakastiedot. Tällöinkin kuitenkin edellytyksenä on, että kyseinen tieto ei ole liikennetieto. Budapestin sopimuksen tulkintasuosituksia antava komitea T-CY:n Cloud Evidence Groupin vuonna 2016 antaman näkemyksen mukaan IP-osoitetieto on katsottava tilaajatiedoksi silloin, kun tiedon tarkoituksena on yksilöidä tietty käyttäjä: (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e, s. 12 ja 37–38.)

SVPL 157 §:ään sisältyy nimenomainen kirjaus siitä, että säilytysvelvollisuus ei koske verkkosivustojen selaamisesta kertyviä välitystietoja. Aikaisemmin perustuslakivaliokunta on todennut tallentamismahdollisuuden ulottamista verkkosivujen selaamisesta kertyviin tietoihin merkitsevän periaatteellisesti merkittävää puuttumista yksityiselämän ja henkilötietojen suojaan. Koska teleyritykset joutuvat joissain palveluissa jakamaan samaa IP-osoitetta yhtäaikaisesti useammalle eri käyttäjälle, saattaa viranomaisen tietopyyntö tuottaa vastauksena useiden käyttäjien tietoja. Verkkoteknologiaan liittyvistä syistä sääntelylle (eli käyttäjän tunnistamiseksi tarvittavien välitystietojen tallentamiselle) voi olla olemassa vakavan rikollisuuden torjumisen näkökulmasta hyväksyttävä peruste. (PeVL 18/2014 vp, s. 8) Sähköisen viestinnän palveluista annetun lain 157 §:n 5 momentissa kuitenkin päädyttiin säätämään, että säilytysvelvollisuus ei koske verkkosivustojen selaamisesta kertyviä välitystietoja.

Internetyhteyden IP-osoitteen säilyttäminen itsessään ei johda päällekkäisten tietojen keräämiseen. Sääntelyä uudistettaessa tulee pohdittavaksi, jäsennetäänkö sääntely esimerkiksi niin, että liittymän IP-osoitteen säilyttämisestä säädettäisiin yleisesti nykyiseen tapaan. Tällöin ei näyttäisi tarpeelliselta toistaa liittymän IP-osoitteen säilyttämistä muilla mahdollisilla perusteilla, kuten kohdennetun säilytysvelvollisuuden tai kansallisen turvallisuuden takaamisen perusteella säilytettävien tietotyyppien kohdalla. Riippuen siitä mitä nämä muut tietotyypit tulisivat olemaan, voivat nekin periaatteessa tapauskohtaisesti sisältää liittymälle annetun IP-osoitteen. Tämän tyyppistä päällekkäisyyttä ei kuitenkaan lähtökohtaisesti ole syytä pitää ongelmallisena, kunhan aina on selvää, millä perusteella kyseistä tietoa on säilytetty ja mihin käyttötarkoituksiin sitä on vastaavasti mahdollista käyttää.

IP-osoitteiden säilytysvelvollisuutta pohtiessa tulee lisäksi huomioida, että julkinen IP-osoite voi olla myös jaettu useiden käyttäjien kesken, jos käytetään osoitteenmuunnosta (NAT) – tällöin on tärkeää, että tallennusvelvollisuus ulottuu myös tietoon osoitteenmuunnoksesta, jolloin voidaan käytettyjen porttien perusteella määrittää tarkempi käyttäjä. Nykyisin tämä on huomioitu Viestintäviraston määräyksessä 53B/2014 teleyritysten tietojen säilytysvelvollisuudesta viranomaistarpeita varten (6.1 §:n 3 kohta), ja asia tulisi jatkossakin joko huomioida lain tasolla tai määräyksenantovaltuudessa.

6.3.3.6 Henkilöllisyyttä koskevien tietojen säilyttäminen

Osana viestintään liittyvien tietojen säilytysvelvollisuutta unionin tuomioistuin on käsitellyt henkilöllisyyttä koskevien tietojen säilytysvelvollisuutta. Kynnys tällaisten tietojen säilyttämiseen on unionin tuomioistuimen mukaan matala. Henkilöllisyyttä koskevien tietojen säilyttäminen on mahdollista yleisesti rikollisuuden torjumiseksi, yleisen turvallisuuden ja kansallisen turvallisuuden suojaamiseksi. Säilytysvelvollisuus voi olla yleistä ja erotuksetonta, eli teleyritykset voidaan velvoittaa ennakollisesti säilyttämään kaikkien käyttäjiensä henkilöllisyyttä koskevat tiedot. Pelkästään näiden tietojen perusteella ei nimittäin voida selvittää suoritetun viestinnän päivämäärää, kellonaikaa,

kestoa ja vastaanottajia eikä myöskään paikkoja, joissa viestintä on tapahtunut. Näistä ei käy myöskään ilmi viestinnän määrä tiettyjen henkilöiden kanssa tiettynä ajanjaksona. Niistä ei siis saada käyttäjien osoitteiden kaltaisia yhteystietoja lukuun ottamatta mitään tietoa viestinnästä eikä käyttäjien yksityiselämästä. Henkilöllisyyttä koskevien tietojen säilyttäminen ei siis lähtökohtaisesti ole vakava puuttuminen käyttäjän perusoikeuksiin. (QdN kohta 157 ja Ministerio Fiscal kohdat 59-60)

Henkilöllisyyttä koskevat tiedot eroavat muista säilytysvelvollisuuden alaisista tiedoista, sillä palveluntarjoajilla on tarve käsitellä kyseisiä tietoja myös muuta tarkoitusta kuin viestin välittämistä varten. Silloin kun kyse on henkilöllisyyttä koskevien tietojen käsittelystä ja etenkin säilyttämisestä ja saannista pelkästään asianomaisen käyttäjän tunnistamista varten, ei kyseisillä tiedoilla voida sellaisinaan saada tietoa henkilön viestinnästä tai liikkumisesta tietyllä alueella. Tältä osin tiedot vastaisivat palveluntarjoajan tavanomaista asiakastietojen käsittelyä ja säilyttämistä. Unionin tuomioistuin ei myöskään ole edellyttänyt tällaisten tietojen säilyttämiselle asetettavan rajoitettua säilytysaikaa. (QdN kohta 159)

Tällaisten tietojen säilyttäminen ennakollisesti yleisesti ja erotuksetta vastaisi nykytilaa, sillä henkilöllisyyttä koskevat tiedot ovat osa SVPL 157 §:n mukaisesti säilytettäviä tietoja. Mikäli säilytysvelvollisuus ulotettaisiin myös muihin kuin nykyisiin neljään nimettyyn yritykseen, säilytysvelvollisuuden voidaan katsoa laajenevan. Tällöin tulisi myös arvioida yksityiskohtaisemmin tarvetta säätää säilytysvelvollisista yrityksistä yksityiskohtaisemmin, sillä kuten yllä on tarkemmin käsitelty, nykyinen SVPL 157 §:n mukainen potentiaalisten säilytysvelvollisten yritysten piiri on varsin laaja ja sisältää monenlaisia toimijoita, joiden ei voida katsoa olevan säilytysvelvollisuuden tavoitteiden kannalta välttämättömiä. Säilytysvelvollisten yritysten piiriä voitaisiin myös jatkossa rajoittaa nimittämällä säilytysvelvolliset yritykset sisäministeriön erillisellä päätöksellä. Tämä mahdollistaisi laintasoista määrittelyä joustavamman mahdollisuuden päivittää säilytysvelvollisuutta rikollisuuden torjumisen ja kansallisen turvallisuuden varmistamisen tavoitteiden edellyttämällä tavalla muuttuvat tilanteet huomioiden. Toisaalta säilytysvelvollisten yritysten piirin rajoittamisella voidaan arvioida olevan vaikutusta myös perusoikeuden rajoituksen laajuuteen. Jatkovalmistelun aikana tulee vielä arvioida tarkemmin, olisiko tästä siis säädettävä yksityiskohtaisemmin myös lain tasolla.

Toisaalta kyseessä on myös pitkälti tiedot, joita palveluntarjoajat käsittelisivät ja tallentaisivat joka tapauksessa muun toiminnan yhteydessä. Täten henkilöllisyyttä koskevien tietojen säilytysvelvollisuudella ei arvioida olevan tosiasiallista vaikutusta viestintäpalveluiden käyttäjien yksityiselämän suojaan verrattuna nykytilaan. Teleyritysten tarve käsitellä asiakkaan tietoja ei ole riippuvainen SVPL 157 §:n mukaisesta säilytysvelvollisuudesta. Tiedossa ei ole ongelmia henkilöllisyyttä koskevien tietojen saannissa, mikä johtuisi nimenomaisen sääntelyn puutteesta. Siten erillinen säännös asi-

asta ei vaikuta välttämättömältä. Henkilöllisyyttä koskevien tietojen säilyttämistä koskevan nimenomaisen sääntelyn puute saattaisi kuitenkin johtaa teleyrityskohtaisiin eroihin tietojen saatavuudessa.

Prepaid-liittymien rekisteröinti

Asiakastietojen säilyttämiseen liittyvänä seikkana on tuotu esiin tarve arvioida mahdollisuutta prepaid-liittymien tietojen rekisteröintivelvoitteen perustamiseksi. Vuoden 2022 lopussa Suomessa oli 700 000 aktiivista prepaid-liittymää. Yhteensä matkaviestinverkon liittymiä oli 9,27 miljoonaa. Suomessa prepaid-liittymien osuus muista puhelinliittymistä on varsin alhainen kansainvälisessä vertailussa.[128] Prepaid-liittymien määrä on laskenut vuodesta 2012, jolloin aktiivisia liittymiä oli 930 000, mutta viime vuosina niiden määrä on jälleen ollut nousussa.[129] Prepaid-liittymän ostaminen ei edellytä rekisteröimistä eikä niitä tarjoavilla palveluntarjoajilla ole laista johtuvaa velvoitetta tarkistaa ja rekisteröidä liittymää oston yhteydessä.

Tällä hetkellä osa prepaid-liittymistä edellyttää ostajan henkilöllisyyden luotettavaa varmistamista. Sähköisen tunnistautumisen ratkaisut saattaisivat helpottaa niiden käyttäjäryhmien, jotka hyötyvät keveästä ja helposta liittymien käyttöönotosta, eli erityisesti maassa lyhytaikaisesti oleskelevat henkilöt, henkilöllisyyden varmistamista liittymän oston yhteydessä. Digitaalisen henkilöllisyyden vahvistavat ratkaisut ovat parhaillaan kehitettävänä, mutta tällä hetkellä käytössä olevia vahvan sähköisen tunnistamisen välineitä ovat lähinnä suomalaisen pankin verkkopankkitunnukset, teleyritysten mobiilivarmenteet tai Digi- ja väestötietoviraston kansalaisvarmenne. Tällöin esimerkiksi maassa tilapäisesti oleskelevilla ei tyypillisesti ole käytössään vahvoja sähköisiä tunnistusvälineitä. Toisaalta fyysisesti liittymiä hankittaessa henkilöllisyystodistusten merkitys korostuu tunnistamiskeinona. Riskinä on, että liittymän omistajat ja haltijat eriytyvät, mikäli rajalliset tunnistautumisvaihtoehdot hankaloittavat prepid-liittymän ostamista tiettyjen käyttäjäryhmien osalta.

Osa teleoperaattoreista on mahdollistanut anonyyminä ostetun prepaid-liittymän rekisteröimisen jälkikäteen, minkä jälkeen prepaid-liittymään on mahdollista tehdä muutoksia ja se helpottaa asiakaspalvelussa asioimista. Rekisteröinnin yhteydessä asiakkaan henkilöllisyys varmistetaan. Asiakkaan tulee olla täysi-ikäinen. Rekisteröinti

[128] Globaalisti 72 % kaikista käytetyistä SIM-korteista oli ennakolta maksettuja vuonna 2021. GSMA: Access to Mobile Services and Proof of Identity 2021, saatavilla: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf
Vuonna 2020 Suomen lisäksi vain Ranskassa, Japanissa ja Etelä-Koreassa prepaid-liittymät muodostivat alle 10 % kaikista mobiililiittymistä. GSMA: Access to Mobile Services and Proof of Identity 2020, saatavilla: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf.

[129] Traficom: Viestintäpalveluiden tilastotaulukko. Saatavilla https://tieto.traficom.fi/fi/tilastot/matkaviestinverkon-liittymat, vierailtu 2.10.2023.

mahdollistaisi esimerkiksi numeron siirron, jolloin rekisteröintivelvoite voisi olla kuluttajillekin hyödyllinen vaihtoehto. Rekisteröityjä prepaid-liittymiä on tällä hetkellä kuitenkin vain vähän, joten käytettävissä oleva mahdollisuus rekisteröidä prepaid-liittymiä ei vaikuta olevan kuluttajille merkittävä etu.

Prepaid-liittymien etuna on pidetty rekisteröintivapaudesta johtuvaa hallinnollista ja menettelyllistä keveyttä. Lisäksi prepaid-liittymät ovat tietyille asiakasryhmille, esimerkiksi alaikäisille, toimiva liittymämuoto. Prepaid-liittymää on pidetty myös tarpeellisena ja toimivana turisteille, vaihto-opiskelijoille ja muille Suomessa lyhyen aikaa oleskeleville tai luottotietonsa menettäneille henkilöille. Rekisteröintivelvoitteesta aiheutuvat kielteiset vaikutukset kohdistuisivat erityisesti henkilöihin, joilla ei ole henkilöllisyyttä osoittavia asiakirjoja, kuten suurimpaan osaan turvapaikanhakijoista. Tämä vaikuttaisi suoraan heidän asiointi- ja yhteydenpitomahdollisuuksiinsa. Puhelinliittymää voidaan pitää välttämättömyyspalveluna, jolloin tulisi kiinnittää asianmukaisesti huomiota niiden yhdenvertaiseen saavutettavuuteen.

Toisaalta prepaid-liittymistä tapahtuva viestintä aiheuttaa tietoa tarvitseville viranomaisille katvealueita, sillä liittymän käyttäjän henkilöllisyys ei ole teleyrityksellä tiedossa.

Prepaid-liittymien rekisteröintiä on selvitetty edellisen kerran vuonna 2010. Tällöin liikenne- ja viestintävaliokunta totesi, että asiantuntijakuulemisissa on tuotu esille useita käytännön haasteita rekisteröinnin osalta. Tällöin pidettiin myös todennäköisenä, että asiasta olisi tulossa EU-tason ehdotuksia.[130]

Tällä hetkellä ei ole voimassa eikä lähiaikoina odotettavissa EU-tason ehdotusta prepaid-liittymien rekisteröimiskäytäntöjen harmonisoimiseksi. Valtaosassa jäsenmaista on voimassa prepaid-liittymien pakollinen rekisteröinti. Unionin tuomioistuin on kuitenkin selventänyt oikeuskäytännössään, ettei unionin oikeus ole esteenä sääntelylle, jonka tavoitteena on vakavan rikollisuuden torjunta ja jolla velvoitetaan prepaid-liittymien myyjät tarkistamaan ostajan henkilöllisyyden ja rekisteröimään nämä tiedot. Estettä ei myöskään ole sille, että myyjä velvoitettaisiin antamaan nämä tiedot toimivaltaisille viranomaisille. (G. D. kohta 72)

Prepaid-liittymien rekisteröiminen toisi uusia velvollisuuksia ja vastuita sekä alan toimijoille että niille tahoille, jotka näitä liittymiä myyvät. Prepaid-liittymiä myyviä tahoja ei ole tällä hetkellä lailla rajoitettu, ja niitä myyvät hyvin erilaiset toimijat, esimerkiksi kioskit ja huoltoasemat. Rekisteröintivelvoitteen seurauksena myyjille tulisi yksityiselämän suojan toteutumista ja henkilötietojen asianmukaista käsittelyä kuin myös tietoturvallisuutta koskevia velvoitteita. Rekisteröimisvelvoite edellyttäisi siis järjestelmämuutoksia sekä teleoperaattoreiden että edustajakanavienkin rajapintoihin.

[130] LiVM 21/2010 vp, s. 7.

Prepaid-liittymien rekisteröintivelvollisuudella saattaisi olla myös vaikutuksia kyseisiä liittymiä toiminnassaan tarvitsemiin tai välittämiin viranomaisiin. Saadun selvityksen perusteella vastaanottokeskusten tehtävänä on lähinnä ohjeistaa turvapaikanhakijoita liittymien hankinnassa. Tästä poikkeuksena ovat ilman huoltajaa maassa olevat lapset, sillä niissä puhelin ja liittymä tulevat yleisesti keskuksen puolesta ja hankkimana. Rekisteröintivelvoite saattaa siis lisätä erityisesti ilman huoltajaa maassa oleville lapsille tarkoitettujen vastaanottokeskusten hallinnollista taakkaa. Mikäli tunnistaminen edellyttäisi virallista henkilöllisyystodistusta, niin ainakin osa Kelan asiakkaista saattaisi tarvita taloudellista tukea henkilöllisyystodistuksen hankintaan, jos sellaista ei asiakkaalla jo olisi.

Prepaid-liittymien rekisteröintivapaus liittyy kansalaisten mahdollisuuteen käyttää viestintäpalveluita anonyymisti. Euroopan ihmisoikeustuomioistuin on tuonut esille, että anonymiteetillä (ainakin) verkkokeskusteluissa on myös arvonsa ja yhteys EIS 8 ja 10 artikloihin (Standard Verlagsgesellschaft mbH v. Itävalta (nro 3), nro 39378/15, §§ 74–78, 7.12.2021). Viestintäpalvelun ikärajan valvontaan liittyvän keskustelun yhteydessä eduskunta on kiinnittänyt huomiota siihen, että edellytys kaikkien verkon käyttäjien henkilöllisyyden tarkistamisesta ikärajojen valvomiseksi vaarantaisi muun muassa toisinajattelijoiden, ihmisoikeusaktivistien, väärinkäytösten paljastajien ja vainottujen vähemmistöjen aseman, joka monessa tapauksessa edellyttää turvallisuussyistä anonyymia verkon käyttöä. (SuVL 7/2023 vp, kohta 10) Rekisteröintivelvoite rajoittaisi saatavilla olevia liittymätyyppejä sekä kuluttajien mahdollisuuksia viestiä anonyymisti.

Toisaalta prepaid-liittymien rekisteröimisvelvollisuuden osalta on huomattava sekä oikeuden anonymiteettiin että toimenpiteen tehokkuuden kannalta, että prepaid-liittymät eivät ole ainoita viestintävälineitä, joilla voidaan viestiä anonyymisti. Myös ulkomailta ostetut prepaid-liittymät toimivat Suomessa, joten käyttäjillä olisi edelleen mahdollisuus hankkia rekisteröimättömiä prepaid-liittymiä muualta, vaikkakin suurimmassa osassa EU:n jäsenmaista on voimassa rekisteröintivelvoite. Aikaisemmin rekisteröintivelvoitteen on arvioitu lähinnä haittaavan suomalaisten toimijoiden toimintaa ja liittymätyyppiä tarvitsevien tahojen mahdollisuuksia viestintään estämättä kuitenkaan asiaan liittyvää rikollisuutta.[131]

Elokuusta 2022 alkaen Ruotsissa on kielletty anonyymien prepaid-liittymien myynti. Rekisteröintivelvoite koskee sekä matkapuhelin- että mobiililaajakaistaliittymiä.

Sähköisestä viestinnästä annetun lain (*Lagen (2022:482) om elektronisk kommunikation*) (luku 8, 24-25 § ja 31 sekä 33 §) mukaan sähköisten viestintäverkkojen ja muiden kuin numeroista riippumattomien viestintäpalveluiden tarjoajien tulee saattaa ri-

[131] Ks. vastaukset kirjallisiin kysymyksiin KK 33/2007 vp ja KK 353/2012 vp. Ks. myös LiVM 21/2010 vp, s. 7, jonka mukaan asiantuntijakuulemisissa on tuotu esille useita käytännön haasteita.

kolliseen toimintaan tai rikosepäilyyn liittyvästä vaatimuksesta saataville tietoja tilaussopimuksesta. Tällaisen vaatimuksen voi esittää esimerkiksi poliisi, Säpo, tulliviranominen (*Tullverket*) tai syyttäjäviranomainen (*Åklagarmyndigheten*).

Rekisteröintivelvoite koskee ennalta maksettuja, yleisesti saatavilla olevia numeroista riippuvia henkilöidenvälisten viestintäpalveluiden ja internetyhteyspalveluntarjoajia. Rekisteröitäviä tietoja ovat tilaajan nimi ja postiosoite, henkilötunnus tai muu identifioiva tunnus sekä numero tai muu palvelun identifioiva tunnus. Myös rekisteröintiaika tulee tallentaa. Tiedot tulee säilyttää rekisteröintihetkestä lähtien ja vuoden ajan palvelun päättymisestä. Tilaajan tietojen yhteydessä tulee varmistaa tilaajan henkilöllisyys voimassa olevalla henkilöllisyystodistuksella tai luotettavalla sähköisellä tunnistamisella. Mikäli tilaajalla ei ole kumpaakaan näistä, tulee henkilöllisyys todentaa muulla tavoin. Jos tilaaja on oikeushenkilö, sovelletaan aikaisempaa oikeushenkilön edustajaan. Myös henkilöllisyyden varmistaminen tulee kirjata.

Mikäli prepaid-palvelua käyttää ilman uutta rekisteröintiä joku muu kuin se, kenelle se on rekisteröity, tulee palvelun tarjoaminen keskeyttää. Tämä ei koske kuitenkaan liittymän satunnaista käyttöä tai jos toinen käyttäjä on tilaajan läheinen sukulainen. Palvelua ei tule keskeyttää myöskään, jos rekisteröity tilaaja on oikeushenkilö ja liittymää käytetään siihen liittyvässä toiminnassa, tai jos palvelun on hankittu lainvalvontaviranomaisen tai puolustusviranomaisen toimintaan.

Myös muissa Pohjoismaissa on säädetty prepaid-liittymien rekisteröintivelvoite. Saadun selvityksen mukaan tämä on johtanut prepaid-liittymien myynnin laskuun.

Jatkovalmistelun aikana tulisi vielä arvioida tarkemmin, miten tunnistamisen edellytykset voitaisiin asettaa. Erityisesti tulisi tarkastella, edellyttääkö tunnistaminen voimassa olevaa virallista kuvallista henkilöllisyystodistusta vai olisiko se toteutettavissa myös muulla tavoin. Tällaisia muita tapoja voisivat olla Ruotsin mallin mukainen vahva sähköinen tunnistaminen.

Tällä hetkellä ei ole saatavissa tarkempia tietoja siitä, miten merkittävässä määrin rekisteröimättömät prepaid-liittymät aiheuttavat haittaa lainvalvonta- ja tiedusteluviranomaisten tehtävien hoitamisessa. Viranomaisten kokemuksen mukaan prepaid-liittymän hankkineiden henkilöiden henkilöllisyyden selvittäminen on hankaloitunut joissain tapauksissa aiempaan verrattuna ja rekisteröinti toisi helpotusta tähän. Joissain tapauksissa tietoa liittymän ostajasta ei ole saatavissa suoraan myyjältä vaan se on hankittava ulkomailta maksutapahtumien keskittämisen vuoksi. Tällaisen tiedon saaminen voi olla hankalaa ja riippuu tietopyynnön kohdemaan kansallisesta lainsäädännöstä.

Suuressa osassa EU-jäsenmaista on voimassa prepaid-liittymien rekisteröintivelvoite. Tiedossa ei ole, että asiasta olisi valmisteilla yleiseurooppalaista ratkaisua. Jos Suomessakin otettaisiin käyttöön monissa jäsenmaissa oleva rekisteröintivelvoite, niin se voisi jossain määrin tuoda ratkaisun edellä kuvattuun viranomaisten haasteeseen. Rekisteröintivelvoite hankaloittaisi sitä, että suuria määriä kortteja hankittaisiin esimerkiksi bulvaanin toimesta. Toisaalta rekisteröintivelvoite ei estä bulvaanien käyttöä, jolloin rekisteröintivelvoite saattaisi hankaloittaa nykyisestään todellisen käyttäjän selvittämistä. Rekisteröity käyttäjä ei ole rikollisessa käytössä juurikaan se henkilö, joka liittymää tosiasiallisesti käyttää. Rekisteröimispakon jälkeen ostettujen liittymien käyttäjän selvittäminen saattaisi lisätä viranomaisen työtä liittymän käyttäjän tunnistamiseksi tilanteissa, joissa liittymä olisi rekisteröity eri henkilölle.

Viranomaiset toivat myös esiin, että suomalaisia prepaid-liittymiä on käytetty merkittävässä määrin petoksissa ja huijauksissa, jotka kohdistuvat Suomen kansalaisiin. Arvion mukaan rekisteröintipakko saattaisi myös auttaa estämään huijauspuheluita ja muita väärinkäytöksiä erityisesti nykyisessä tilanteessa, kun mahdollisuuksia soittajan numeron ja viestin lähettäjän tietojen väärentämiseksi on rajoitettu[132], ja jolloin riskinä on, että huijauksia tekevät toimijat siirtyisivät enenevissä määrin käyttämään rekisteröimättömiä prepaid-liittymiä.

Prepaid-liittymien rekisteröintivelvoitteen osalta tulisi myös arvioida riittävä siirtymäaika, jolloin liittymät tulisi rekisteröitäviksi. Esimerkiksi Ruotsissa päädyttiin ratkaisuun, jossa ennen rekisteröintivelvoitetta ostetut liittymät tuli aktivoida sähköisessä järjestelmässä tiettyyn päivämäärään mennessä. Osa teleoperaattoreista tarjoaa jo nyt mahdollisuuden rekisteröidä prepaid-liittymän ostamisen jälkeen. Jälkikäteisessä aktivoinnissa tosin korostuu yllä kuvatut rajoitukset erityisesti niiden käyttäjien osalta, joilla ei ole käytettävissään Suomessa yleisesti käytössä olevia vahvoja sähköisiä tunnistautumisen ratkaisut. Mikäli jälkikäteistä aktivointivelvoitetta ei asetettaisi, jäisi käyttäjille myös rekisteröimättömiä liittymiä käyttöön.

[132] Ks. https://www.traficom.fi/fi/ajankohtaista/traficomin-maarays-kampittaa-rikollisten-mahdollisuuksia-tekstiviestihuijauksiin ja https://www.traficom.fi/fi/ajankohtaista/maarayksen-velvoitteet-voimaan-jopa-200-000-huijauspuhelua-estetaan-paivassa.

6.3.4 Säilytysvelvollisuuden asettaminen kansallisen turvallisuuden takaamiseksi

6.3.4.1 Rikollisuuden torjumiseksi asetettujen säilytysvelvoitteiden kanssa vastaavat toimenpiteet

Unionin tuomioistuin on tuoreessa oikeuskäytännössään, erityisesti ratkaisuissa G. D. ja SpaceNet, keskittynyt täsmentämään niitä edellytyksiä, joita säilytystoimenpiteisiin liittyy silloin, kun säädetään velvoitteesta säilyttää viestinnän välitystietoja vakavan rikollisuuden torjumiseksi tai yleiseen turvallisuuteen kohdistuvien vakavien uhkien torjumiseksi. Kuitenkin kansallisen turvallisuuden nimissä perusoikeuksia voidaan rajoittaa enemmän kuin vakavan rikollisuuden torjumisen tavoitteen vuoksi. Unionin tuomioistuimen käsittelemät säilytystoimenpiteet voidaan oikeuttaa myös kansallisen turvallisuuden varmistamisen tavoitteen vuoksi. Tällöin siis yllä jaksossa 6.3.3 käsitellyt säilyttämistoimepiteet voivat tulla kyseeseen myös silloin, kun tavoitteena on torjua kansalliseen turvallisuuteen kohdistuvaa uhkaa.

Yleisen edun mukaisten tavoitteiden hierarkiaa koskevan oppinsa yhteydessä unionin tuomioistuin on myös nimenomaisesti todennut, että tilanteissa, joissa tietojen saannin tarkoitus on merkitykseltään suurempi kuin säilyttämisen perustana ollut tavoite, voidaan tietojen säilytysvelvollisuuden ja saannin perusteiden symmetriasta poiketa. (QdN kohta 165-166)

Siispä mikäli tietoja säilytetään vakavan rikollisuuden ja yleiseen turvallisuuteen kohdistuvien uhkien torjumisen tavoitteiden vuoksi, voidaan kansallisessa lainsäädännössä sallia tällaisten tietojen käyttö myös kansallisen turvallisuuden tavoitteen turvaamiseksi. Tällöin ei ole välttämätöntä asettaa erillistä kansallisen turvallisuuden takaamisen säilytysperustetta, vaan tietojen hyödyntäminen voitaisiin sallia myös varmistamalla vakavan rikollisuuden torjumiseksi säilytettyjen tietojen käyttö tätä tarkoitusta varten. Toisaalta joiltain osin tietty säilyttämisvelvollisuuden laukaiseva kriteeri saattaa olla päällekäinen sekä kansallisen turvallisuuden että vakavan rikollisuuden torjumisen tavoitteiden kannalta. Näin on erityisesti silloin, mikäli yllä jaksossa 6.3.2.1 käsitellysti päädyttäisiin asettamaan maantieteellinen säilyttämiskriteeri kriittisen infrastruktuurin perusteella.

Sääntelyn selkeyden ja siitä aiheutuvan hallinnollisen taakan minimoimiseksi yllä esitetysti olisi jatkovalmistelussa syytä varmistua siitä, ettei samoja tietoja säilytetä useaan kertaan. Edellä todettu huomioon ottaen on siis syytä arvioida sitä, miltä osin olisi tarkoituksenmukaista säätää tietojen säilytysperusteeksi myös kansallisen turvallisuuden varmistaminen, vai riittäisikö alemman tavoitteen eli vakavan rikollisuuden torjuminen säilytysperusteeksi.

Esimerkiksi mikäli lainsäädännössä asetettaisiin yleinen ja erotukseton velvoite säilyttää liittymän lähteelle annetut IP-osoitteet vakavan rikollisuuden torjumiseksi, olisi samat tiedot säilytettynä ja käytettävissä myös kansallisen turvallisuuden varmistamiseksi. Tällöin erillinen kansallisen turvallisuuden säilyttämisperuste ei toisi erityistä lisäarvoa.

Toisaalta edellä todetusti kansallista turvallisuutta voidaan pitää tärkeämpänä yleisen edun mukaisena tavoitteena verrattuna rikollisuuden torjuntaan. Tällöin säilyttämistoimenpiteiden laajuutta tai ajallista kestoa voisi olla mahdollista muuttaa säilytysperusteen mukaisesti. Kuitenkin myös näiden toimenpiteiden osalta tulisi varmistua siitä, että noudatetaan unionin tuomioistuimesta ja perustuslaista johtuvia reunaehtoja, kuten säilytysajan rajoittaminen välttämättömään.

6.3.4.2 Yleinen ja erotukseton säilyttäminen kansallisen turvallisuuden takaamiseksi

QdN-ratkaisussa unionin tuomioistuin toteaa, että sähköisen viestinnän direktiivin soveltamisalaan kuuluu kansallinen säännöstö, jonka mukaan sähköisten viestintäpalvelujen tarjoajien on säilytettävä liikenne- ja paikkatiedot kansallisen turvallisuuden suojaamiseksi. (QdN kohta 104) Kansallisen turvallisuuden takaamista koskeva tavoite on tärkeämpi kuin direktiivin 2002/58 15 artiklan 1 kohdassa tarkoitetut muut tavoitteet, ja etenkin rikollisuuden, jopa vakavan rikollisuuden, torjumista yleisesti ja yleisen turvallisuuden suojaamista koskevat tavoitteet. Näin ollen kansallisen turvallisuuden takaamista koskevalla tavoitteella voidaan näin ollen perustella toimenpiteitä, joilla puututaan perusoikeuksiin vakavammin kuin toimenpiteillä, jotka voitaisiin perustella näillä muilla tavoitteilla. (Privacy International kohta 75, QdN kohta 136) Kansallisen turvallisuuden nimissä perusoikeuksia voidaan rajoittaa enemmän kuin vakavan rikollisuuden torjumisen nimissä. Tästä johtuen kansallisen turvallisuuden varmistamiseksi on mahdollista säätää muihin unionin tuomioistuimen oikeuskäytännössään käsittelemiin säilytystoimenpiteisiin verrattuna laajemmasta perusoikeuksien puuttumisesta eli laajamittaisemmasta välitystietojen säilytysvelvollisuudesta.

Unionin tuomioistuimen mukaan on mahdollista säätää sellainen säilyttämistoimenpide, jonka mukaan toimivaltaiset viranomaiset voivat määrätä sähköisten viestintävälineiden tarjoajat säilyttämään kaikkien sähköisten viestintävälineiden käyttäjien liikenne- ja paikkatiedot rajoitetun ajanjakson ajan, kun on olemassa riittävän konkreettisia seikkoja, joiden perusteella voidaan katsoa, että asianomaisen jäsenvaltion kansalliseen turvallisuuteen kohdistuu kaltainen vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi. (QdN kohta 137) Määräys on rajattava ajallisesti täysin välttämättömään. Uhan jatkumisen vuoksi määräys voidaan uusia, mutta kulloisenkin määräyksen voimassaoloaika ei saa ylittää ennakoitavissa olevaa ajanjaksoa. (QdN kohta 138)

Kaikkien sähköisen viestintävälineiden käyttäjien tietojen säilyttäminen edellyttää rajoituksia ja tiukkoja takeita, joilla voidaan tehokkaasti suojata asianomaisten henkilöiden henkilötietoja väärinkäytön vaaroilta. (QdN kohta 138)

Perustuslakivaliokunnan käsityksen mukaan kansallinen turvallisuus ja vakava uhka ovat sisällöltään varsin laaja-alaisia käsitteitä. Niiden soveltamisessa korostuu tarve ottaa huomioon ja noudattaa eurooppalaisessa oikeuskäytännössä tiedonhankintamenetelmiä määrittelevälle lainsäädännölle asetettavia perusvaatimuksia. Tällaisia vaatimuksia ovat muun muassa viranomaisten toimivaltuuksien käyttöön kohdistuva tuomioistuimen ennakollinen hyväksyminen, riippumaton valvonta, oikeusturvan toteuttaminen tuomioistuimessa ja tietosuojan perusteiden noudattaminen. (PeVM 4/2018 vp, s. 8) Perustuslakivaliokunnan mukaan perustuslaista johtuu tarve tulkita kansallisen turvallisuuden käsitettä suppeasti sekä asettaa säännöksessä mainitun uhan vakavuusaste korkealle (PeVM 4/2018 vp, s. 8—9).

Rajoitusperusteen käyttö edellyttää riittäviä perusteluja sille, että jokin toiminta voi muodostua vakavaksi uhaksi kansalliselle turvallisuudelle. Perustuslakivaliokunnan mukaan on osoitettava, että tiedon hankkiminen kussakin yksittäistapauksessa ja siihen liittyvät yksilökohtaiset perusoikeuksien rajoitukset ovat tehokkaita ja välttämättömiä keinoja hankkia tietoja kyseisessä tilanteessa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta (PeVM 4/2018 vp, s. 8-9). Unionin tuomioistuimen mukaan yleinen ja erotukseton säilyttämismääräys kansallisen turvallisuuden varmistamiseksi edellyttää, että on olemassa riittävän konkreettisia seikkoja, joiden perusteella voidaan katsoa, että jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi. (QdN kohta 137)

Perustuslakivaliokunnan mielestä kansallisen turvallisuuden suojaamiseen voi sinänsä sisältyä erittäin painavia perusteita rajoittaa henkilötietojen suojan ja yksityiselämän suojan perusoikeuksia. Perustuslakivaliokunta on myös viitannut unionin tuomioistuimen oikeuskäytäntöön, jonka mukaan kansallisella turvallisuudella voidaan perustella toimenpiteitä, joilla puututaan perusoikeuksiin vakavammin kuin muihin tavoitteisiin pyrkivillä toimenpiteillä (PeVL 48/2022 vp, s. 4)

Täten siis kansallisen turvallisuuden varmistaminen voi perustuslain 10 §:n 4 momentin erityisten rajoitusedellytysten osalta oikeuttaa pidemmälle menevän rajoituksen luottamuksellisen viestinnän suojaan. Samalla kuitenkin sekä unionin tuomioistuin että perustuslakivaliokunta on edellyttänyt erityisiä suojakeinoja, kuten tuomioistuimen suorittamaa tai muuta riippumatonta valvontaa, oikeusturvan toteuttamista tuomioistuimessa sekä tietosuojan perusteiden noudattamista, jotta toimenpiteen kohteiden henkilötietoja voidaan suojata väärinkäytöksiltä.

Kansalliseen turvallisuuden uhkaa on haastava määritellä yksityiskohtaisesti. Unionin tuomioistuin on edellyttänyt, että yleinen ja erotukseton säilyttäminen kansallisen turvallisuuden suojaamiseksi on mahdollista tilanteissa, joissa on olemassa riittävän konkreettisia seikkoja, joiden perusteella kansalliseen turvallisuuteen kohdistuva uhka voidaan havaita. Tällaisen vakavan uhan tulee lisäksi osoittautua todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi.

Unionin tuomioistuin on täsmentänyt kansallisen turvallisuuden käsitettä toteamalla, että yksinomaan jäsenmailla säilyvä vastuu kansallisesta turvallisuudesta vastaa ensisijaisen tärkeää intressiä suojella valtion keskeisiä tehtäviä ja yhteiskunnan perustavanlaatuisia etuja, ja siihen kuuluu sellaisten etenkin terrorismin kaltaisten toimien torjuminen ja niistä rankaiseminen, jotka ovat omiaan horjuttamaan vakavasti tietyn maan perustavanlaatuisia perustuslaillisia, poliittisia, taloudellisia tai yhteiskunnallisia rakenteita ja erityisesti uhkaamaan suoraan yhteiskuntaa, väestöä tai valtiota sellaisenaan (QdN kohta 135).

Kansallisen turvallisuuden käsitettä on käsitelty varsin laajasti Euroopan ihmisoikeustuomioistuimen ratkaisukäytännössä, jonka mukaan ainakin sotilaallinen maanpuolustus, terrorismintorjunta ja laittoman tiedustelutoiminnan torjunta kuuluvat käsitteen piiriin (mm. Weber & Saravia v. Saksa, 29.6.2006; Klass ja muut v. Saksa). Kansalliseen turvallisuuteen saattaa kuitenkin kohdistua monenlaisia uhkia, joita on vaikea ennakoida tai määritellä etukäteen. Tästä seuraa, että käsitteen selventäminen on ensisijaisesti jätettävä kansallisen käytännön varaan (Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010).

Suomessa kansallisen turvallisuuden käsitesisältöä on selvennetty siviili- ja sotilastiedustelusta säätämisen yhteydessä. Perustuslain 10 §:ää muutettiin tuolloin niin, että sen 4 momentti sallii säätää lailla välttämättömistä rajoituksista viestin salaisuuteen tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan perustuslain säännöksessä kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä taikka kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Ilmaisu ”kansallinen turvallisuus” tarkoittaa sitä, ettei säännöksessä tarkoitettu uhkaava toiminta kohdistuisi ensisijaisesti kehenkään yksilönä vaan yleisemmin yhteiskuntaan ja sen ihmisyhteisöön (HE 198/2017 vp, s. 36).

Kansalliseen turvallisuuteen kohdistuvia vakavia uhkia konkretisoivat edelleen poliisilain 5 a luvussa (ns. siviilitiedustelulaki) ja sotilastiedustelulaissa säädetyt kansallisen turvallisuuden suojaamiseksi toteutettavan tiedustelun kohteet. Tiedustelun kohteiksi määritellään poliisilain 5 a luvun 3 §:n mukaan:

1) terrorismi;

2) ulkomainen tiedustelutoiminta;

3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö;

4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö;

5) kansanvaltaista yhteiskuntajärjestystä vakavasti uhkaava toiminta;

6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta;

7) vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille;

8) kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi;

9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta;

10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta vakavasti uhkaava toiminta;

11) kansanvaltaista yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus.

Sotilastiedustelulain 4 § sisältää pitkälti vastaavan kaltaisen luettelon toiminnoista, jotka voivat olla sotilastiedustelun kohteena. Sotilastiedustelun kohteena on lisäksi vieraan valtion toiminta tai muu sellainen toiminta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja.

Koska kansallisen turvallisuuden ja siihen kohdistuvien vakavien uhkien käsitettä on edellä kuvatulla tavalla EU-oikeuden ja Suomea sitovien kansainvälisten ihmisoikeusvelvoitteiden asettamissa puitteissa Suomessa täsmennetty poliisilain 5 a luvun 3 §:ssä ja sotilastiedustelulain 4 §:ssä, olisi luontevaa, että kyseisissä säännöksissä mainitut uhkat voisivat muodostaa perusteen säilyttämismääräyksen antamiselle. Lisäkriteeriksi olisi asetettava, että havaittu uhka on sillä tavalla yleinen ja vakava, että se tekee teletietojen yleisen säilyttämisen välttämättömäksi uhkalta suojautumiseksi.

Kuten edellä tässä selvityksessä on todettu, on unionin tuomioistuin edellyttänyt, että tuomioistuimen tai riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, tulee voida kohdistaa kansallisen turvallisuuden suojaamiseksi annettavaan teletietojen säilyttämismääräykseen tehokasta valvontaa. (QdN kohdat 139 ja 163) Toisin kuin tietojen saantia koskevaan pyyntöön, tietojen säilyttämismääräyksen edellytyksenä ei ole tuomioistuimen ennakkovalvonta. Tämä merkitsee, että säilyttämismääräyksen antajana voi olla viranomainen. Edellä selvityksen kansainvälisestä vertailusta ilmenee, että esimerkiksi Tanskassa määräyksen antaa oikeusministeri, kun taas Ruot-

sissa on esitetty tehtävän antamista turvallisuuspoliisille. Suomessa tarkoituksenmukaisin ratkaisu saattaisi olla se, että kansallisen turvallisuuden uhkan olemassaolon toteaa ja määräyksen antaa sisäministeriö. Sisäministeriöllä on jo nykyisin tähän vertautuvia, sähköisen viestinnän palveluista annetun lain perusteella annettuja tehtäviä, kuten lain 157 §:ään perustuva oikeus nimetä tallennusvelvolliset teleyritykset. Lain esitöissä on edellä todetusti pidetty perusteltuna, että tallentamisvelvollisten teleyritysten määrittely kuuluu sisäministeriölle, koska tallentaminen palvelee sisäministeriön hallinnonalaa ja tallentaminen kustannetaan sen budjetista. Samat näkökohdat soveltuvat sen tahon valintaan, joka päättäisi kansallisen turvallisuuden suojaamiseksi välttämättömän säilyttämisen määräämisestä.

Sisäministeriön päätöksen todellisen ja olemassa olevan tai ennakoitavissa olevan vakavan kansallisen turvallisuuden uhan käsillä olosta ja sen perusteella määrättävästä säilyttämisvelvollisuudesta tulisi perustua Suojelupoliisin tai Puolustusvoimien esitykseen ja uhka-arvioon. Edellä mainituilla tahoilla tulisi olla velvollisuus esittää uhka-arviossaan riittävät seikat sen tueksi, että jokin poliisilain 5 a luvun 3 §:ssä tai sotilastiedustelulain 4 §:ssä mainittu uhka on sillä tavalla konkreettinen, yleinen ja vakava, että se perustelee säilyttämismääräyksen antamisen välttämättömyyden.

Lain tasolla tulisi säätää säilyttämismääräyksen ajanjakson rajoittumisesta välttämättömään. Uhan olemassa olon jatkuessa määräyksen voimassaolon aikaa tulisi jatkaa. (QdN tuomiolauselma) Perusteet säilyttämismääräyksen ajanjaksosta tulisi käydä ilmi sisäministeriön päätöksestä ja perustua Suojelupoliisin ja Puolustusvoimien esitykseen ja uhka-arvioon. Koska säilyttämismääräyksen kesto olisi sidottava tällaisen uhkatilanteen kestoon, vaikuttaisi perustellulta sitoa tietojen säilyttämisaika myös säilyttämismääräyksen kestoon, mutta tietojen käyttötarve saattaa ilmetä vasta myöhemmin. Yllä kansainvälisen vertailun yhteydessä käsitellysti Tanskassa on säädetty ja Ruotsissa esitetään säädettäväksi säilytysmääräyksen ajallista rajaamista korkeintaan yhteen vuoteen. Tanskassa tiedot tulisi säilyttää vuoden ajan viestintäajankohdasta, kun taas Ruotsissa ehdotetaan tietojen säilyttämisajaksi kahta vuotta.

Sääntelyn hyväksyttävyyden kannalta on keskeistä huomata, että kansallisen turvallisuuden turvaamiseksi annettava yleinen ja erotukseton säilyttämismääräys ei olisi mahdollista rajoittamattomaksi ajanjaksoksi. Peruste säilyttämismääräykselle tulisi perustella tapauskohtaisesti uhka-arvion perusteella ja sen voimassaoloaika tulisi sitoa tällaisen uhan olemassa oloon. Mahdollisuus kansallisen turvallisuuden turvaamiseksi annettavaan säilyttämismääräykseen ei siis automaattisesti johtaisi kaikkien säilytysvelvollisiksi määrättävien käyttäjien viestintätietojen säilyttämiseen, vaan se edellyttäisi viranomaisen määräyksen antamista.

Sisäministeriölle voitaisiin säätää velvollisuus kuulla tiedusteluvalvontavaltuutettua Suojelupoliisin tai Puolustusvoimien esityksestä ja sen perusteena olevasta uhka-arviosta. Tiedustelutoiminnan valvonnasta annetun lain (121/2019) 7 §:n mukaan tiedus-

teluvalvontavaltuutetun tehtävänä on valvoa tiedustelutoiminnan lainmukaisuutta, valvoa perus- ja ihmisoikeuksien toteutumista tiedustelutoiminnassa ja edistää oikeusturvan toteutumista ja siihen liittyviä hyviä käytäntöjä tiedustelutoiminnassa. Lain 8 §:n mukaan tiedusteluvalvontavaltuutetulla on oikeus salassapitosäännösten estämättä saada viranomaisilta ja muilta julkista hallintotehtävää hoitavilta maksutta valvontatehtäviensä hoitamiseksi tarvitsemansa tiedot. Tiedusteluvalvontavaltuutetun tiedonsaantioikeus kattaa toisin sanoen myös ne Suojelupoliisin tai Puolustusvoimien säilyttämismääräyksen antamista koskevan esityksen tueksi esittämät seikat, jotka ovat salassa pidettäviä julkisuuslain (621/1999) 24 §:n 1 momentin esimerkiksi 9 tai 10 kohdan perusteella.

Koska unionin tuomioistuin on edellyttänyt, että tuomioistuimen tai riippumattoman hallinnollisen elimen, jonka ratkaisu on sitova, tulee voida kohdistaa kansallisen turvallisuuden suojaamiseksi annettavaan teletietojen säilyttämismääräykseen tehokasta valvonta, tulisi sisäministeriön päätöksestä voida valittaa riippumattomaan lainkäyttöelimeen. Sisäministeriön tekemän päätöksen muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019). Järjestelmältä edellytettävän tehokkuuden ja uhka-arvion sisältämien tietojen salassapidon varmistamiseksi olisi arvioitava, onko valitusoikeutettujen piiriä mahdollista rajata esimerkiksi siten, että oikeus valittaa sisäministeriön päätöksestä säädettäisiin esimerkiksi ainoastaan tiedusteluvalvontavaltuutetulle. Jo nykyinenkin sähköisen viestinnän palveluista annetun lain 345 §:n sisältämä sääntely on poikkeussääntelyä suhteessa oikeudenkäynnistä hallintoasioissa säädettyyn lakiin sisältyvään sääntelyyn.

Sisäministeriön määräykselle vaihtoehtoisena ratkaisuna voidaan pitää määräyksen antamisen osoittamista tuomioistuimen päätettäväksi. Vaikka unionin tuomioistuimen oikeuskäytäntö ei edellytä tuomioistuimen suorittamaa ennakkovalvontaa tällaisen säilyttämismääräyksen antamiseen, ei siitä myöskään johdu estettä määräyksen alistamiselle ennakkovalvonnalle. Toimenpiteen laajuus ja vakava puuttuminen laajan joukon perusoikeuksiin ilman suoraa tai epäsuoraa liityntää toimenpiteen tavoitteeseen saattaisi tukea tällaista ratkaisua. Jatkovalmistelussa tulee vielä arvioida tarkemmin, miten tuomioistuimen suorittama valvonta tulisi järjestää.

Perusoikeuksien rajoituksista tulee säätää lailla. Säilyttämisvelvoitteen toteuttaminen lailla annetun määräyksenantovaltuuden perusteella edellyttää tarkempaa arviointia myös PL 80 §:n näkökulmasta.

Kuten muissakin säilytysperusteissa olisi myös tässä tilanteessa otettava huomioon se, että tietojen saanti olisi edelleen tuomioistuinvalvonnan alaista ja mahdollista siten kuin televalvonnasta on muualla säädetty. Tällä perusteella säilytettävät tiedot eivät olisi sellaisinaan viranomaisten käytettävissä, vaan tiedot olisivat luovutettavissa televalvontaa koskevien edellytysten mukaisesti (sotilastiedustelulaki 4:38§ ja poliisilaki 5 a:7§).

6.3.5 Säilyttämisvelvollisuuden toteutusvaihtoehtojen alustava perusoikeusarviointi

Valittavina olevien toimenpiteiden arvioinnissa on syytä ottaa huomioon yhtäältä perusoikeuksina suojattu yksityiselämän suoja, luottamuksellisen viestin salaisuuden suoja ja henkilötietojen suoja, ja toisaalta näiden oikeuksien tietynasteista rajoittamista puoltavat vakavien rikosten selvittämisintressiin ja rikosoikeudellisen järjestelmän uskottavuuteen liittyvät yhteiskunnallisesti painavat perusteet. Viestinnän välitystietojen säilytysvelvollisuutta ja siihen liittyvää perusoikeuksien rajoitusta tarkoittavaa sääntelyä puoltaa vakavan rikollisuuden torjuntaan liittyvä hyväksyttävä peruste. (PeVL 18/2014 vp, s. 7)

Kaikkien alla olevien toimenpiteiden voidaan arvioida vaikuttavan käyttäjien yksityiselämän ja henkilötietojen suojaan. Viestinnän välitystietojen säilyttämisvelvollisuudella puututaan perustuslaissa ja kansainvälisissä ihmisoikeusvelvoitteissa suojattuihin oikeushyviin.

Rikollisuuden torjuntaa ja turvallisuutta edistävää vaikutusta on sillä, että poliisi ja muut esitutkintaviranomaiset voivat tehokkaasti selvittää rikoksia. Nykytilaan verrattuna kohdennetumpi eli rajatumpi säilyttäminen saattaa toisaalta vaikuttaa heikentävästi viranomaisten mahdollisuuksiin puuttua vakaviin rikoksiin ja selvittää niitä, sillä tietoja ei välttämättä olisi yhtä laajasti saatavilla.

Jos säilytysvelvollisuudesta säädettäisiin kansallisesti siten kuin unionin tuomioistuin on linjannut, voidaan sääntelyn katsoa lähtökohtaisesti täyttävän EU:n perusoikeuskirjan määräykset. Tämä perustuu siihen, että unionin tuomioistuimen ratkaisukäytäntö säilytysvelvollisuudesta perustuu sähköisen viestinnän tietosuojadirektiiviin ja perusoikeuskirjaan, erityisesti sen 7, 8, 11 ja 52 artikloihin. Sen sijaan jos kansallisesti säädetään jotenkin muutoin kuin unionin tuomioistuimen linjaamalla tavalla, kansallista sääntelyä tulee arvioida myös perusoikeuskirjaa vasten.

Unionin tuomioistuimen oikeuskäytännön valossa vaikuttaa perustellulta, että kansalliseen lakiin täsmennettäisiin nykyistä selvemmin tietojen säilytysperuste ja käyttötarkoitus. Tämän voidaan arvioida selkeyttävän nykytilaa, ja siten vaikuttavan positiivisesti sekä perusoikeusrajoituksen kohteisiin että säilytysvelvollisten yritysten oikeusvarmuuteen. Myös perustuslakivaliokunnan lausuntokäytännön perusteella tätä voidaan pitää kannatettavana. (Ks. esim. PeVL 3/2008 vp säilytysvelvoitteen oikeuttavan viranomaistarpeen yksilöimisestä).

Jatkovalmistelussa tulee lisäksi tehdä tarkempi perusoikeusarviointi sen osalta, säilytetäänkö ja käytetäänkö välitystietoja sekä vakavien rikosten selvittämiseksi että rikosten ennalta estämiseksi ja paljastamiseksi.

Kohdennettu säilyttäminen maantieteellisen kriteerin perusteella

Maantieteelliseen kriteeriin perustuvan kohdennetun säilyttämisvelvollisuuden voidaan arvioida aiheuttavan vaikutuksia viestintäpalveluiden käyttäjien yksityiselämän suojaan, luottamuksellisen viestin salaisuuden suojaan, henkilötietojen suojaan sekä jossain määrin myös liikkumisvapauteen.

Nykytilaan verrattuna maantieteelliseen kriteeriin perustuva kohdennettu säilyttäminen voisi parantaa kansalaisten yksityiselämän suoja, sillä säilyttäminen olisi nykyistä rajatumpaa ja kohdennetumpaa. Tämän vaikutuksen merkitys kuitenkin riippuu siitä, miten maantieteellinen kriteeri asetettaisiin ja miten laajaksi säilytysvelvollisuus tällä perusteella voisi muodostua. Perusoikeuksien rajoittamisen hyväksyttävyyden kannalta tilanne paranisi kuitenkin siltä osin, että säilyttäminen perustuisi unionin tuomioistuimen edellyttämällä tavalla objektiiviseen kriteeriin, jolla pyrittäisiin luomaan yhteys vakavan rikollisuuden torjunnan tavoitteen ja säilytettävien tietojen välille.

Mikäli maantieteellinen kriteeri asetettaisiin siten, että osa Suomen maantieteellisestä alueesta jäisi säilytysvelvollisuuden ulkopuolelle, saattaisi tämä asettaa rikoksen uhrit eriarvoiseen asemaan. Tältä osin unionin tuomioistuin on kuitenkin oikeuskäytännössään todennut, että kohdennettu eli rajatumpi säilyttäminen ei ole vastoin uhrien yhdenvertaisen kohtelun vaatimusta (Spetsializirana prokuratura (Bulgaria) 44 kohta).

Kohdennettu säilyttäminen henkilöpiirin perusteella

Henkilöperusteisesti kohdennetun säilyttämisvelvollisuuden voidaan arvioida vaikuttavan viestintäpalveluiden käyttäjien oikeuksiin. Kohdennettu säilyttäminenkin muodostaa rajoituksen käyttäjän perusoikeutena turvattuun yksityiselämän, luottamuksellisen viestinnän ja henkilötietojen suojaan.

Henkilöpiirin perusteella kohdennetun säilyttämisvelvollisuuden voidaan katsoa parantavan näiden oikeuksien toteutumista verrattuna nykytilaan, sillä tietojen säilyttäminen olisi nykyistä käytäntöä huomattavasti rajatumpi. Erityisesti tällainen säilyttäminen parantaisi sivullisten yksityiselämän suojaa, sillä toimenpiteen kohteiden joukko olisi tarkkaan rajattu sellaisiin henkilöihin, joilla on tunnistettu olevan yhteys vakavaan rikollisuuteen.

Henkilöperusteisesti kohdennetun säilyttämisen arviointiin liittyy erityisesti toimenpiteen ennakollinen ulottuvuus. Tiettyjen henkilöiden osoittaminen toimenpiteen kohteeksi esimerkiksi aikaisemman rikostaustan vuoksi ei vaikuta ongelmattomalta syyttömyysolettaman kannalta. Unionin tuomioistuin on kuitenkin nimenomaisesti katsonut, että kohdennettu säilyttäminen ei ole syyttömyysolettaman vastaista (Spetsializirana prokuratura (Bulgaria) kohta 46).

Henkilöllistä kohdentamista unionin tuomioistuin ei ole itsessään pitänyt syrjivänä, joskin tuomioistuin viittaa henkilöpiirin määrittämisessä kansallisessa oikeudessa tarkemmin määriteltäviin objektiivisiin ja syrjimättömiin seikkoihin (G.D. 75–78 kohta).

Toimenpiteen hyväksyttävyyttä heikentää kuitenkin arviot siitä, että aikaisemman rikostaustan perusteella muodostettavaa henkilöiden piiriä ei voida pitää tehokkaana toimenpiteenä rikollisuuden torjunnan kannalta.

Viestinnän välitystietojen säilyttämisestä johtuvan perusoikeuksien rajoituksen lisäksi henkilöllisen säilyttämiskriteerin yhteydessä on syytä erityisesti kiinnittää huomiota säilytystoimenpiteen kohteeksi joutuvien henkilöiden henkilötietojen käsittelyyn säilyttämismääräyksen täytäntöönpanon yhteydessä. Tällainen säilyttämisperuste johtaisi näet käytännössä siihen, että viranomaisten tulisi toimittaa teleyrityksille tiedot sellaisista henkilöistä, keiden viestintään liittyvät tiedot säilytettäisiin. Rikostuomioihin ja rikoksiin liittyvät henkilötiedot voidaan myös lukea valtiosääntöisesti arkaluonteisiksi. (PeVL 15/2018 vp, s. 38) Siispä annettaessa sääntelyä, jolla sallittaisiin tai jopa edellytettäisiin tällaisten tietojen käsittelyä, tulee käsittelystä säätämisen yhteydessä arvioida ja säätää myös riittävistä erityisistä suojakeinoista.

Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa henkilötietojen käsittelystä säädettäessä erityisesti se, että henkilötietojen suoja osittain sisältyy perustuslain 10 §:n samassa momentissa turvatun yksityiselämän suojan piiriin. Lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Valiokunta on tämän vuoksi arvioinut erityisesti arkaluonteisten tietojen käsittelyn sallimisen koskevan yksityiselämään kuuluvan henkilötietojen suojan ydintä (PeVL 37/2013 vp, s. 2/I), minkä johdosta esimerkiksi tällaisia tietoja sisältävien rekisterien perustamista on arvioitava perusoikeuksien rajoitusedellytysten, erityisesti rajoitusten hyväksyttävyyden ja oikeasuhtaisuuden, kannalta (PeVL 29/2016 vp, s. 4—5 ja esimerkiksi PeVL 21/2012 vp, PeVL 47/2010 vp sekä PeVL 14/2009 vp). Valiokunta on kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on syytä rajata täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään (ks. esim. PeVL 3/2017 vp, s. 5). Perustuslakivaliokunta on painottanut arkaluonteisten tietojen käsittelyn aiheuttamia uhkia. Valiokunnan mielestä arkaluonteisia tietoja sisältäviin laajoihin tietokantoihin liittyy tietoturvaan ja tietojen väärinkäyttöön liittyviä vakavia riskejä, jotka voivat viime kädessä muodostaa uhan henkilön identiteetille (PeVL 13/2016 vp, s. 4, PeVL 14/2009 vp, s. 3/I).

Sähköisen viestinnän tietosuojadirektiivissä ei säädetä, millä edellytyksin viranomaiset voivat toimittaa teleyrityksille sellaisia henkilötietoja, joiden avulla teleyritykset voisivat kohdentaa säilyttämistä henkilöllisin perustein. Direktiivissä ei myöskään säädetä teleyrityksille erillistä käsittelyperustetta valikoida kyseisen listan perusteella välitystiedot ja säilyttää ne. Viranomaisten tietojenluovutuksen osalta kyseinen sääntely kuu-

luisi todennäköisesti nk. rikosasioiden tietosuojadirektiivin (EU) 2016/680 soveltamisalaan, sillä tietojen luovutuksen tarkoitus liittyy rikosten ennalta estämiseen, tutkimiseen tai paljastamiseen[133]. Sen sijaan teleyritysten osalta tällaisten henkilötietojen käsittely kuuluisi todennäköisesti sekä sähköisen viestinnän tietosuojadirektiivin että yleisen tietosuoja-asetuksen soveltamisalaan (lakisääteinen velvoite).[134]

Perustuslakivaliokunnan mukaan tietosuoja-asetuksen yksityiskohtainen sääntely, jota tulkitaan ja sovelletaan EU:n perusoikeuskirjassa turvattujen oikeuksien mukaisesti, muodostaa yleensä riittävän säännöspohjan myös perustuslain 10 §:ssä turvatun yksityiselämän ja henkilötietojen suojan kannalta. Henkilötietojen suoja tulee turvata ensisijaisesti EU:n yleisen tietosuoja-asetuksen ja kansallisen yleislainsäädännön nojalla. Kansallisen erityislainsäädännön säätämiseen tulee siten suhtautua pidättyvästi ja rajata sellainen vain välttämättömään tietosuoja-asetuksen salliman kansallisen liikkumavaran puitteissa (ks. PeVL 14/2018 vp, s. 4–5 ja PeVL 52/2022 vp, 4 kohta). Perustuslakivaliokunnan mukaan on kuitenkin selvää, että erityislainsäädännön tarpeellisuutta on arvioitava myös tietosuoja-asetuksenkin edellyttämän riskiperustaisen lähestymistavan mukaisesti kiinnittämällä huomiota tietojen käsittelyn aiheuttamiin uhkiin ja riskeihin. Mitä suurempi riski käsittelystä aiheutuu luonnollisen henkilön oikeuksille ja vapauksille, sitä perustellumpaa on yksityiskohtaisempi sääntely. Tällä seikalla on erityistä merkitystä arkaluonteisten tietojen käsittelyn osalta (ks. PeVL 14/2018 vp, s. 5). Arkaluonteisten tietojen käsittelyn on oltava välttämätöntä ja sääntelyn täsmällistä ja tarkkarajaista (ks. PeVL 52/2022 vp, 7 kohta).

Tässä tapauksessa kyse olisi sekä laajuudeltaan ja lajiltaan sellaisesta henkilötietojen käsittelystä, josta muodostuu erityisiä riskejä rekisteröidyn oikeuksille. Henkilöllisen kohdentamisen mahdollistavien henkilötietojen luovuttamisesta ja niiden käsittelystä teleyrityksissä tulisi säätää erikseen – ottaen huomioon myös yleisen tietosuoja-asetuksen 10 artikla.[135]

---

[133] Liikkumavara ei siten tulisi sähköisen viestinnän tietosuojadirektiivin 15(1) artiklasta, koska kyseisten henkilötietojen luovuttamisessa ei suoraan ole kyse viestinnän luottamuksellisuuden rajoittamisesta.

[134] Vrt. EU:n tietosuojaneuvoston lausunto 5/2019 sähköisen viestinnän tietosuojadirektiivin ja yleisen tietosuoja-asetuksen vuorovaikutuksesta erityisesti tietosuojaviranomaisten toimivallan, tehtävien ja valtuuksien osalta, 31 ja 34 kohta. Rinnakkaisen soveltamisen kannalle on päädytty myös oikeuskirjallisuudessa, ks. Marko Priiki, Sähköisen viestinnän välitystietojen ja henkilötietojen käsittelyperusteiden suhteesta – kansallinen lainsäädäntö suoraan sovellettavan tietosuoja-asetuksen aikana. Oikeustiede - Jurisprudentia LVI:2023 s. 213–303, 256–257.

[135] Kyseisessä artiklassa säädetään rikostuomioihin ja rikkomuksiin liittyvien henkilötietojen käsittelystä. Rikostuomioihin ja rikkomuksiin tai niihin liittyviin turvaamistoimiin liittyvien henkilötietojen käsittely 6 artiklan 1 kohdan perusteella suoritetaan vain viranomaisen valvonnassa tai silloin, kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa säädetään asianmukaisista suojatoimista rekisteröidyn oikeuksien ja vapauksien suojelemiseksi. Kattavaa rikosrekisteriä pidetään vain julkisen viranomaisen valvonnassa.

Kohdennettu säilyttäminen muiden objektiivisten ja syrjimättömien kriteereiden perusteella

Unionin tuomioistuimen oikeuskäytännön mukaan myös muut kuin henkilöpiiriin tai maantieteelliseen kriteeriin perustuvat seikat voidaan ottaa huomioon sen varmistamiseksi, että kohdennettu säilyttäminen perustuu objektiivisiin ja syrjimättömiin kriteereihin. Selvityksen laatimisen aikaan tällaisena muuna kohdentamisperusteena on tunnistettu ainoastaan tiettyyn vakavalle rikollisuudelle alttiiseen suureen yleisötapahtumaan liittyvä säilyttäminen. Kyseinen säilyttämistoimenpide vastaisi käytännössä maantieteelliseen kriteeriin perustuvaa kohdennettua säilyttämismääräystä. Siten sillä ei arvioida olevan maantieteellisen kriteerin mukaisesta säilyttämisestä eroavia vaikutuksia käyttäjien perusoikeuksiin.

Quick freeze –säilyttämismääräys

Myös quick freeze –säilyttämismääräystä on syytä arvioida käyttäjiin kohdistuvien yksityiselämän ja henkilötietojen suojan rajoituksen näkökulmasta. Nykytilaan verrattuna quick freeze –määräyksen voidaan katsoa vaikuttavan näihin perusoikeuksiin pääsääntöisesti niitä parantavasti.

Käsitellyistä säilyttämistoimenpiteistä tämä olisi kaikista kohdennetuin toimenpide, sillä se tulisi käytettäväksi lähinnä konkreettisten ja yksilöityjen rikosepäilyjen tilanteissa. Verrattuna muihin toimenpiteisiin, tämä toimenpide ei sisältäisi käytännössä lainkaan ennakollista puuttumista perusoikeuksiin, sillä säilyttämismääräys voitaisiin antaa vasta rikoksen selvittämisen alettua.

Toisaalta ainoana säilyttämistoimenpiteenä quick freeze –määräys vaikuttaisi viranomaisten mahdollisuuksiin selvittää ja torjua vakavaa rikollisuutta heikentävästi, sillä tietojen saatavuus olisi sattumanvaraista ja riippuisi pitkälti kunkin teleyrityksin omista käytännöistä. Yritysten välillä saattaisi olla suuriakin eroja. Tämä myös saattaisi vaikuttaa heikentävästi rikosten uhrien yhdenvertaisuuteen.

IP-osoitteiden säilyttäminen

Liittymän lähteelle annettujen IP-osoitteiden yleinen ja erotukseton säilyttämisvelvollisuus vaikuttaisi viestintäpalveluiden käyttäjien yksityiselämän suojaan rajoittavasti. Lisäksi tämän säilyttämisperusteen voidaan arvioida vaikuttavan ennalta ehkäisevästi sananvapauden harjoittamiseen.

IP-osoitteiden säilyttämistä ja analysointia on arvioitu perusoikeusnäkökulmasta erityisesti unionin tuomioistuimen ja myös korkeimman oikeuden oikeuskäytännössä. Vaikka IP-osoitteet eivät ole yhtä arkaluonteisia tietoja kuin muut viestinnän välitystiedot, kuuluvat ne yksityiselämän suojan alaan. (QdN kohta 152, ks. myös

KKO:2022:47 ja KKO:2022:23) IP-osoitteiden säilyttäminen ja analysointi merkitsee vakavaa puuttumista internetin käyttäjän perusoikeuksiin. (QdN kohdat 152-153)

Säilyttämistoimenpiteen hyväksyttävyyttä kuitenkin lisää se, että joissain tapauksissa IP-osoite saattaa olla ainoa tutkintakeino, jolla voidaan yksilöidä henkilö, jolle kyseinen IP-osoite on annettu tietyn rikoksen tekohetkellä. (QdN kohdat 153-154; ks. myös KKO:2022:47)

Liittymän lähteelle annettujen IP-osoitteiden yleisestä ja erotuksettomasta säilyttämisestä johtuva puuttuminen yksityiselämän suojaan ja henkilötietojen suojaan on kuitenkin vakavaa, joten ainoastaan vakavan rikollisuuden torjunta ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen sekä kansallisen turvallisuuden takaaminen voivat unionin tuomioistuimen mukaan oikeuttaa kyseisen puuttumisen. (QdN kohta 156)

IP-osoitteiden yleinen ja erotukseton säilyttäminen vastaisi pitkälti nykytilaa. Siten tällaisella säilyttämistoimenpiteellä ei arvioida olevan nykyiseen säilytysvelvollisuuteen verrattuna merkittävämpiä vaikutuksia käyttäjien perusoikeuksiin.

Tältäkin osin on tosin huomattava, että säilyttämistoimenpiteen laajuuteen vaikuttaisi käytännössä myös se, mitkä yritykset määrättäisiin jatkossa tällaiset tiedot säilyttämään. Jos säilytysvelvollisten yritysten joukko laajenisi nykytilaan verrattuna, myös säilytettyjen tietojen määrä oletettavasti kasvaisi.

Henkilöllisyyttä koskevien tietojen säilyttäminen

Henkilöllisyyttä koskevien tietojen säilytysvelvollisuuden voidaan arvioida vaikuttavan käyttäjien yksityiselämän ja henkilötietojen suojaan rajoittavasti. Unionin tuomioistuin on arvioinut tällaisia toimenpiteitä perusoikeuksien näkökulmasta, ja katsonut, ettei se lähtökohtaisesti ole vakava puuttuminen käyttäjän perusoikeuksiin, sillä nämä tiedot eivät voi paljastaa käyttäjien osoitteiden kaltaisia yhteystietoja lukuun ottamatta muita tietoja viestinnästä eikä käyttäjien yksityiselämästä. (QdN kohta 157 ja Ministerio Fiscal kohdat 59-60) Kynnys tällaisten tietojen säilyttämiseen on siis unionin tuomioistuimen mukaan matala.

Unionin tuomioistuimen mukaisesti tällaiset tiedot voidaan velvoittaa säilytettävän yleisesti ja erotuksetta. Tällainen säilyttäminen vastaisi käytännössä nykytilaa, sillä voimassa olevan sääntelyn mukaan säilytysvelvollisten yritysten tulee säilyttää palveluidensa käyttäjien yksilöimiseksi tarpeelliset tiedot.

Prepaid-liittymien rekisteröintivelvoite olisi uutta sääntelyä. Tällä voidaan katsoa olevan käyttäjien asemaa heikentävä vaikutus, sillä kansalaisten mahdollisuudet viestiä anonyymisti heikkenisivät. Ottaen huomioon anonyymien viestintäpalveluiden suuri

määrä, prepaid-liittymien rekisteröintivelvoitteella ei kuitenkaan täysin estettäisi anonyymiä viestintää. Toisaalta rekisteröimisvelvoite saattaisi vaikeuttaa tai estää sellaisten käyttäjien, jotka eivät voisi velvoitteen mukaisesti tunnistautua ja siten hankkia liittymiä, mahdollisuuksia käyttää välttämättömyyspalveluna pidettäviä puhelinliittymiä. Välttämättömyyspalvelun luonteesta johtuen tulee kiinnittää huomiota niiden yhdenvertaiseen saatavuuteen.

Yleinen ja erotukseton säilyttäminen kansallisen turvallisuuden takaamiseksi

Kansallisen turvallisuuden turvaamiseksi annettava yleinen ja erotukseton säilyttämismääräys edellyttää erittäin tärkeän yleisen edun mukaisen tavoitteen tasapainottamista viestintäpalveluiden käyttäjien perusoikeuksien, erityisesti yksityiselämän suojaan, luottamuksellisen viestin suojaan ja henkilötietojen suojaan nähden.

Perustuslakivaliokunnan mielestä kansallisen turvallisuuden suojaamiseen voi sinänsä sisältyä erittäin painavia perusteita rajoittaa henkilötietojen suojan ja yksityiselämän suojan perusoikeuksia. Kansallisella turvallisuudella voidaan myös EU-oikeudessa perustella toimenpiteitä, joilla puututaan perusoikeuksiin vakavammin kuin toimenpiteillä, joita perusteltaisiin jollain muulla tavoitteella (ks. myös esim. tuomio 6.10.2020, La Quadrature du Net ym., C-511/18, C-512/18 ja C520/18, 136 kohta). (PeVL 48/2022 vp, s. 4)

Yleinen ja erotukseton säilyttämismääräys kohdistuisi yhtäläisesti kaikkiin säilyttämismääräyksen kohteeksi määrättävien viestintäpalveluiden käyttäjiin ja heidän viestintäänsä. Tällainen säilyttämismääräys kohdistuisi siis myös sellaisiin henkilöihin, joilla ei ole mitään yhteyttä kansalliseen turvallisuuteen kohdistuvaan uhkaan. Tällainen säilyttämistoimenpide on siis erityisen vakava puuttuminen käyttäjien yksityiselämän ja henkilötietojen suojaan. Tällainen puuttuminen voi kuitenkin unionin tuomioistuimen mukaan täyttää oikeasuhteisuutta koskevan vaatimuksen tilanteissa, joissa jäsenvaltion kansalliseen turvallisuuteen kohdistuu vakava uhka, joka osoittautuu todelliseksi ja olemassa olevaksi tai ennakoitavissa olevaksi. Lisäksi edellytyksenä on, että tällaisen säilyttämisen kesto on rajoitettu täysin välttämättömään. (QdN kohta 177)

Yleinen ja erotukseton säilyttämismääräys kansallisen turvallisuuden perusteella tarkoittaisi käytännössä irtaantumista nykyisestä sääntelystä, jonka mukaan tietojen säilyttämistä on perusteltu lähinnä vakavan rikollisuuden torjuntaan liittyvällä hyväksyttävällä perusteella. Sen sijaan nykysääntelyssä on säädetty mahdollisuudesta käyttää näitä tietoja myös kansallisen turvallisuuden tarkoituksiin eikä säilyttämisvelvollisuus sinänsä ole sidottu pelkästään rikosperusteiseen toimintaan. Tämä ei kuitenkaan olisi nykytilaan verrattuna ongelmallisempaa, sillä nykyinenkään säilyttämisvelvollisuus ei ole sidoksissa rikosepäilyihin tai tilanteisiin, joissa tällainen epäily voisi syntyä.

Nykyisen sääntelyn mukaan säilytysvelvollisuutta ei ole määritelty ajallisesti, vaan sisäministeriön päätös säilytysvelvollisista yrityksistä on voimassa toistaiseksi. Koska unionin tuomioistuimen oikeuskäytännöstä seuraa tällaiselle säilyttämismääräykselle ajallinen rajoitus, voitaisiin tällaisen säilytysperusteen katsoa vaikuttavan nykytilaan verrattuna parantavasti kansalaisten yksityiselämän ja henkilötietojen suojan toteutumiseen, sillä säilyttämismääräyksen voimassaolo olisi sidottuna kansalliseen turvallisuuteen kohdistuvan uhan olemassa oloon.

Tällä perusteella säilytettävien tietojen määrän voidaan arvioida vastaavan pitkälti nykytilaa. Käytännössä määrä saattaisi kuitenkin lisääntyä, riippuen siitä, millaisille ja kuinka monelle yrityksille säilyttämisvelvollisuus määrättäisiin.

Kansallisen turvallisuuden turvaamiseksi annettava säilyttämismääräys ei vertaudu tiedustelulainsäädäntöön, mutta sillä olisi oletettavasti merkitystä erityisesti poliisilain 5a luvun ja sotilastiedustelulain 4 luvun mukaisilla tiedustelumenetelmillä saataviin tietoihin. Unionin tuomioistuimen oikeuskäytännössä on edellytetty, että tietojen säilytysperuste on oikeassa suhteessa tietojen käyttötarkoitukseen. (G. D. kohta 56) Yleisen edun mukaisten tavoitteiden hierarkian perusteella kansallisen turvallisuuden varmistamiseksi säädetyn säilytysvelvollisuuden mukaisesti säilytettyjä tietoja voidaan käyttää ainoastaan kansallisen turvallisuuden varmistamiseksi. Täten tällaisella säilyttämisperusteella ei laajennettaisi esitutkintaviranomaisten tiedonsaantimahdollisuuksia.

7. Tietojen säilytysvelvollisuuteen liittyvät erityiset kysymykset

7.1 Muiden kuin unionin tuomioistuimen oikeuskäytännöstä johtuvien muutostarpeiden tarkastelu

Arviomuistion laatimisen yhteydessä työyhmässä on tunnistettu tarve tarkastella eräitä säilytysvelvolliisuuteen liittyviä kysymyksiä, jotka eivät suoraan perustu unionin tuomioistuimen oikeuskäytännön linjauksiin. Liikenne- ja viestintäministeriön asettaman työryhmän ensisijaisena tavoitteena on laatia esiselvitys, jossa arvioidaan eri vaihtoehtoja, miten välitystietojen säilyttämistä ja viranomaisten pääsyä kyseisiin tietoihin koskeva kansallinen lainsäädäntö tulisi järjestää, jotta lainsäädäntö olisi Suomen perustuslain ja unionin tuomioistuimen oikeuskäytännön mukainen, rajoittuu yksityiselämän suojan kannalta välttämättömään ja samalla turvaa viranomaisille oikeutetun ja oikeasuhtaisen pääsyn tietoihin tehokkaan rikostorjunnan varmistamiseksi. Työryhmän tehtävä keskittyy siis selvittämään unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännön sekä Suomen perustuslain asettamat reunaehdot ja keinot yhteensovittaa nämä viranomaisten oikeutettujen tietotarpeiden kanssa.

Jotta varmistetaan, että toimenpiteet ovat tavoitteidensa kannalta tehokkaita, on tarkoituksenmukaista tarkastella näiden reunaehtojen lisäksi myös muita mahdollisia lainsäädäntöön kohdistuvia muutostarpeita. Tällaisia mahdollisia muutostarpeita, jotka eivät johdu suoraan unionin tuomioistuimen oikeuskäytännöstä, ovat esimerkiksi säilytysvelvollisuuden laajentaminen OTT-viestintäpalveluiden tarjoajiin, IP-osoitteiden säilyttämisvelvollisuuden laajentaminen sekä välitystietojen saanti poliisitutkintojen suorittamiseksi.

Lisäksi on kiinnitettävä huomiota myös niihin sekkoihin, joiden tunnistettiin jo vuoden 2021 arviomuistion laatimisen yhteydessä antavan aihetta yksityiskohtaisempaan tarkasteluun, mikäli lainsäädäntöä myöhemmässä vaiheessa päädyttäisiin tarkastelemaan.

7.2 Säilytysvelvollisuuden ulottaminen OTT-viestintäpalveluihin

Nykyisin säilytettävät tietokategoriat on yksilöity SVPL 157 §:ssä. Säilytysvelvollisuuden perusteella säilytettävien tietojen teknisistä yksityiskohdista on määrätty Viestintäviraston (nyk. Liikenne- ja viestintävirasto Traficom) määräyksessä.[136] Säilytysvelvollisuus on ulotettu sellaisiin tietoihin, joita säilytysvelvolliset yritykset käsittelevät joka tapauksessa. Suhteellisuusperiaatteen kannalta perustuslakivaliokunta on pitänyt tärkeänä, ettei palvelun tarjoajaa velvoiteta erikseen tuottamaan tai hankkimaan tietoja, vaan ainoastaan säilyttämään tarjoajan saatavilla muutenkin olevat tiedot (PeVL 3/2008 vp, s. 2/II, PeVL 3/2006 vp, s. 3/I, PeVL 35/2004 vp, s. 3/II). Jatkossakin tulisi kiinnittää huomiota siihen, ettei säilytysvelvollisuudella luoda velvoitetta kerätä sellaisia tietoja, jotka eivät ole välttämättömiä palvelun toteuttamisen kannalta. SVPL 157 §:n 3 momentin mukaan säilytettävät tiedot tulee rajata vain siihen, mikä on palvelun tekninen toteutus huomioon ottaen välttämätöntä laissa määriteltyjen seikkojen yksilöimiseksi. Jatkossakin tulee ottaa huomioon perustuslain 80 §:n sääntely lainsäädäntövallan siirtämisestä.

Tietoja hyödyntävien viranomaisten näkökulmasta nykyiset SVPL 157 §:ssä säilytettäväksi määrätyt tietokategoriat ovat edelleen tarpeellisia. Ainoa selvityksen laatimisen aikana viranomaisten puolelta esiin tuotu tarve tarkastella säilytettävien tietokategorioiden laajentamista koskee IP-osoite- ja porttitietojen säilyttämistä.[137]

Nykyisen lain säätämisen yhteydessä perustuslakivaliokunta edellytti, että liikenne- ja viestintävaliokunnan oli täsmennettävä, mitkä ehdotetun säännöksen perusteella säilytettävät tiedot ovat välttämättömiä sääntelyn taustalla olevan tarkoituksen eli vakavien rikosten tutkimisen, selvittämisen ja syyteharkintaan asettamisen kannalta. Sellaisia tietoja, jotka eivät ole tämän tarkoituksen kannalta välttämättömiä, ei voi vaatia säilytettäviksi. (PeVL 18/2014 vp, s. 7) Säilyttämisvelvollisuuden vähimmäissisällön kannalta perustuslakivaliokunta on pitänyt aivan olennaisena, mihin tietoihin tai tietotyyppeihin velvollisuus ulottuu. Tällaisten, sääntelyn kannalta olennaisten seikkojen ja rajausten tulee käydä säännöksistä ilmi täsmällisesti. (PeVL 3/2006 vp, s. 3/II, PeVL 35/2004 vp, s. 3/II).

SVPL 157 §:ssä säilytettävät tietokategoriat on määritelty palvelukohtaisesti. Säilyttämisvelvollisuuden piiriin kuuluvia palveluita ovat matkaviestinverkon puhelinpalveluun tai tekstiviestipalveluun, internetpuhelinpalveluun tai internetyhteyspalveluun liittyvät

[136] Viestintäviraston määräys teleyritysten tietojen säilytysvelvollisuudesta viranomaistarpeita varten. Viestintävirasto 53 B/2014 M.
[137] IP-osoitteisiin liittyvien tietojen säilyttämisen laajentamista käsitellään tarkemmin alempana jaksossa 7.3.

yksilöidyt tiedot. Lain säätämisen yhteydessä liikenne- ja viestintävaliokunta arvioi perustuslakivaliokunnan edellyttämällä tavalla tietojen säilyttämisen välttämättömyyttä. Tällöin valiokunta rajoitti säilytysvelvollisuuden edellä SVPL 157 §:ssä lueteltuihin palveluihin, ja hallituksen esityksestä poiketen säilytysvelvollisuuden piiristä poistettiin tietyt palvelut[138], joiden tietoja ei sen hetkisen arvion perusteella voitu katsoa olevan välttämätöntä säilyttää vakavien rikosten selvittämistä ja syyteharkintaa asettamista varten. (LiVM 10/2014 vp, s. 24-25)

Esimerkiksi perustuslakivaliokunta on todennut teknologisten muutosten ja järjestäytyneen rikollisuuden muotojen olevan omiaan vaikuttamaan telepakkokeinojen säätelyn tarpeeseen ja sisältöön. (PeVL 32/2013 vp, s. 8) Viestintäpalvelumarkkinoiden viimeisten kymmenen vuoden aikana tapahtuneiden muutosten vuoksi myös tässä yhteydessä on syytä arvioida säilytysvelvollisuuden piiriin kuuluvien palveluluokkien tarkoituksenmukaisuutta. Viestintä on yhä enenevissä määrin siirtynyt verkkoon, ja erityisesti internetin päällä tarjottavien ns. over-the-top- eli OTT-viestintäpalveluiden käyttö ja merkitys on kasvanut. OTT-viestintäpalveluita ovat esimerkiksi älypuhelinten pikaviestintäsovellukset ja sosiaalisen median viestintäpalvelut, kuten WhatsApp, SnapChat, Skype ja iMessage.[139]

Pikaviestien lähettäminen on kasvanut tasaisesti kymmenen vuoden aikana, kun taas perinteisten puheluiden ja tekstiviestien määrä on laskenut hieman. Lähes kaikki matkapuhelimen käyttäjät soittavat tavallisia puheluita ja lähettävät tekstiviestejä edelleen matkapuhelimella viikoittain, mutta ero pikaviestipalveluiden käyttöön on kaventunut. Vuonna 2022 86 % käyttäjistä lähetti pikaviestejä Facebook Messengerin ja WhatsAppin kaltaisissa palveluissa, kun vielä vuonna 2017 pikaviestipalveluita käytti kuukausittain vain 66 %. Noin puolet käyttäjistä soittivat vuonna 2022 internetin puhe- ja videopuheluita viikoittain.[140]

OTT-viestintäpalvelun käytöstä suomalaisille teleyrityksille näkyy vain yhteys päätelaitteen ja palvelimen välillä, eikä siitä käy ilmi tarkat tiedot viestinnän tyypistä tai sisällöstä. Teleyritykselle tallentuu vain tiedot internetyhteyden käytöstä. Nykyinen säilytysvelvollisuus ei koske esimerkiksi tietoa siitä, mihin OTT-viestintäpalveluun on oltu yhteydessä ja kelle siellä on viestitty.[141] SVPL 157 §:n esitöiden perusteella internetyhteyspalvelulla, johon liittyvät tiedot tulee tallentaa, tarkoitetaan esimerkiksi tilaajan

[138] Tietoja ei enää säilytetä viranomaistarpeita varten lainkaan säilytysvelvollisen yrityksen kiinteän verkon puhelinpalveluista (ns. lankapuhelin), sähköpostipalveluista, lisäpalveluista, EMS-palveluista ja multimediapalveluista.
[139] Keskeiset OTT-viestintäpalvelut eivät kuitenkaan ole suomalaisia viestintäpalveluita, vaan usein ne ovat sijoittautuneet toisiin EU-maihin tai EU:n ulkopuolelle. Sääntelyn soveltumista OTT-viestintäpalveluihin käsitellään myöhemmin jaksossa 5.1.5.
[140] Liikenne- ja viestintävirasto Traficom: Viestintäpalvelujen kuluttajatutkimus – Aikasarjoja vuodesta 2022 taaksepäin. https://www.traficom.fi/sites/default/files/media/publication/Viestintapalvelujen-kuluttajatutkimus-aikasarjakuviot.pdf
[141] Ks. vastaavasti vuoden 2017 selvitys, s. 12.

päätelaitteen, kuten modeemin ja julkisen internetin välistä yhteyttä. Määritelmä kattaa tiedonsiirron liittymästä julkiseen internetiin ja yhteyden kannalta pakolliset palvelut, kuten IP-osoitteiden hallinnan. Olennaista internetyhteyspalvelussa on, että se kattaa asiakkaan pääsystä internetiin sen osuuden, jota palvelua tarjoava teleyritys pystyy hallinnoimaan. Internetyhteyden päällä tarjottavat palvelut, kuten sähköposti tai internetpuhelinpalvelut eivät kuulu internetyhteyspalveluun, vaan ovat erillisiä viestintäpalveluja riippumatta siitä, tarjoaako niitä sama vai eri teleyritys. (HE 221/2013 vp, s. 85)

OTT-viestintäpalvelut vaikuttavat pääasiassa putoavan SVPL 157 §:n mukaisten palveluluokkien ulkopuolelle. SVPL 157 §:n 2 momentin 2 kohdan mukainen internetpuhelinpalvelu voitaisiin katsoa OTT-viestintäpalveluksi, koska viestintä voidaan välittää kolmannen osapuolen tarjoaman internetyhteyspalvelun välityksellä. Internetpuhelinpalvelu on määritelty samassa 2 momentin 2 kohdassa siten, että sillä tarkoitetaan palveluyrityksen tarjoamaa loppuasiakkaille asti internetyhteyskäyttöön perustuvaa puhelun mahdollistavaa palvelua. Lain esitöiden mukaan esimerkiksi internetpuhelut, jotka soitetaan internetpuheluja varten käytettävän ohjelmiston välityksellä yhdeltä tietokoneelta viestintäverkkojen välityksellä toiselle tietokoneelle ilman nimenomaan palveluyrityksen tarjoamaa internetpuhelinpalvelua, eivät kuulu tietojen säilyttämistä koskevien velvoitteiden piiriin. Pelkkä internetyhteyden käyttö viestinnän siirtämisen runkoverkossa ei kuitenkaan tekisi palvelusta internetpuhelinpalvelua, sillä palvelun tulisi perustua internetyhteyskäytäntöön loppuasiakkaalle saakka, jotta kyse olisi internetpuhelinpalvelusta. (HE 221/2013 vp, s. 156)

Internetpuhelinpalvelun määritelmästä ei käy ilmi, tarkoittaako se mitä tahansa reaaliaikaisen kahdensuuntaisen ääniviestinnän mahdollistavaa, internetyhteyskäytäntöön perustuvaa palvelua vai sellaista palvelua, jota voidaan pitää yleisenä puhelinpalveluna. Pikaviestit jäävät kuitenkin SVPL 157 §:n pykälän mukaisesti eroteltujen palvelutyyppien ulkopuolelle. Siltä osin kuin ainoastaan viestinnän lähteen eikä viestinnän vastaanottajan IP-osoitteet säilytettäisiin, kyse ei olisi muiden liikennetietojen kanssa yhtä arkaluonteisista tiedoista, sillä tällaiset tiedot eivät sellaisinaan paljasta mitään tietoa niistä kolmansista henkilöistä, jotka ovat olleet yhteydessä viestinnän alullepanijana olevaan henkilöön. (QdN kohta 152)

Esitutkinta- ja tiedusteluviranomaisten tiedonsaantimahdollisuudet OTT-viestintäpalveluissa tapahtuvaan viestintään ovat olleet esillä jo useiden vuosien ajan. Ruotsin säilytysvelvollisuutta koskevassa selvityksessä on tarkasteltu säilytysvelvollisuuden laajentamista myös numeroista riippumattomiin henkilöiden välisiin viestintäpalveluihin. Selvitykseen sisältyvän ehdotuksen mukaan säilytysvelvollisuus koskisi viestintää, joka tapahtuisi jossain määrin Ruotsissa, ja joka voitaisiin määrittää esimerkiksi IP-osoitteen sijaintitiedon perusteella. Selvityksen laatimisen aikaan tiedossa ei ole Belgian ja Unkarin lisäksi muita EU-jäsenmaita, jossa tietojen säilytysvelvollisuus olisi

laajennettu myös numeroista riippumattomiin henkilöiden välisiin viestintäpalveluihin.[142]

Keskeiset OTT-viestintäpalvelut ovat kuitenkin tällä hetkellä sijoittautuneet Suomen ulkopuolelle. Laissa sähköisen viestinnän palveluista ei ole erillistä sääntelyä sen 19 luvun maantieteellisestä soveltamisalasta. Vaikuttaa perustellulta ottaa lähtökohdaksi, että samoin kuin lakia yleensä, sovellettaisiin myös 19 lukua viestintäpalveluihin siltä osin kuin niiden vastaanottajat asuvat Suomessa.

Viranomaisten pääsy muuhun EU-jäsenvaltioon tai EU:n ulkopuolelle sijoittautuneen palveluntarjoajan hallussa oleviin tietoihin on tunnistettu yleisenä haasteena läpi unionin. Ruotsin EU-puheenjohtajuuskaudella on perustettu korkean tason ryhmä, jolle on annettu tehtäväksi kartoittaa viranomaisten tietoon pääsyn haasteita sekä mahdollisia ratkaisuja näihin yhteisesti jaettuihin haasteisiin. Kyseisen ryhmän työssä yhtenä yhteisenä jaettuna ongelmana on tunnistettu, että kansallisten tietojen säilytysvelvollisuuksien soveltuminen OTT-palveluntarjoajiin on EU-tasolla epäselvää. Niille osoitettuja tietopyyntöjä riitautetaan tai niihin jätetään kokonaan vastaamatta. Haasteena myös on, että osa OTT-palveluntarjoajista ei säilytä mitään tietoja viestitapahtumista. Ongelma on siis EU-tasolla yhteisesti jaettu.

Nykyisen lainsäädännön mukaan nimetyt säilytysvelvolliset yritykset ovat kaikki sijoittautuneet Suomeen, eikä muualle sijoittautuneita yrityksiä ole yritetty nimittää säilytysvelvollisiksi yrityksiksi. Tiedossa ei siis ole, että SVPL 157 §:n mukaisten velvoitteiden maantieteellistä soveltamisalaa olisi testattu. Ottaen huomioon yleisen EU-laajuisesti koetun ongelman sääntelyn epäselvyydestä suhteessa muualle sijoittautuneisiin yrityksiin, Suomen kansallisen lainsäädännön mukaisilla ratkaisuilla ei välttämättä saavuteta tyydyttävää ratkaisua ongelmaan. Sen sijaan voisi olla kannattavaa tavoitella tähän ratkaisua EU-tasolla.[143]

Jatkovalmistelun aikana tulisi arvioida yksityiskohtaisemmin tarve säätää jatkossakin säilytettävät tiedot palveluluokittain sekä tarkastella näiden palveluluokkien päivittämistä, jotta ne vastaavat tietojen säilyttämisperusteiden kannalta välttämättömiä tietoja. Tarvetta päivittää säilytysvelvollisuuden piiriin kuuluvia tietoja ja palveluita tukee

[142] SOU 2023:22, s. 341-342.
[143] Esimerkiksi ns. E-evidence-asetusta sovelletaan palveluntarjoajiin, jotka tarjoavat palveluita unionissa. Asetuksen 3 artiklan 3 kohdassa määritellään ”palveluntarjoaja” ja 4 kohdassa määritellään ”unionissa palveluita tarjoava” eli joka antaa luonnollisille henkilöille tai oikeushenkilöille jossakin jäsenvaltiossa mahdollisuuden käyttää 3 alakohdassa lueteltuja palveluja; ja jolla on erityisiin tosiseikkoihin perustuviin kriteereihin perustuva olennainen yhteys a alakohdassa tarkoitettuun jäsenvaltioon; tällaisen olennaisen yhteyden katsotaan olevan olemassa, jos palveluntarjoajalla on toimipaikka unionissa tai, jos tällaista toimipaikkaa ei ole, jos yhdessä tai useammassa jäsenvaltiossa on huomattava määrä palvelun käyttäjiä tai jos toimintoja on kohdennettu yhteen tai useampaan jäsenvaltioon.

myös nykyisen lainsäädännön laatimisen yhteydessä eduskunnan edellytys näiden tietojen tarkastelusta ja päivittämisestä, mikäli joidenkin tietojen merkitys rikostutkinnassa olennaisesti vähenee tai kasvaa. (LiVM 10/2014 vp)

7.3 IP-osoitteiden säilytysvelvollisuuden laajentaminen

Erityisen kysymyksen muodostaa IP-osoitteiden säilytysvelvollisuus. Internetyhteyspalvelussa säilytysvelvollisuus koskee tilaajan ja rekisteröidyn käyttäjän nimeä ja osoitetta, liittymän tunnistetta ja asennusosoitetta sekä tietoa, jonka avulla voidaan yksilöidä viestintäpalvelun käyttäjä, viestintään käytetty laite sekä palvelun käytön ajankohta ja kesto. Säilytettävät tiedot tulee rajata vain siihen, mikä on palvelun tekninen toteutus huomioon ottaen välttämätöntä tässä tarkoitettujen seikkojen yksilöimiseksi.

SVPL 157 §:ään sisältyy nimenomainen kirjaus siitä, että säilytysvelvollisuus ei koske verkkosivustojen selaamisesta kertyviä välitystietoja. Aikaisemmin perustuslakivaliokunta on todennut tallentamismahdollisuuden ulottamista verkkosivujen selaamisesta kertyviin tietoihin merkitsevän periaatteellisesti merkittävää puuttumista yksityiselämän ja henkilötietojen suojaan. Koska teleyritykset joutuvat joissain palveluissa jakamaan samaa IP-osoitetta yhtäaikaisesti useammalle eri käyttäjälle, saattaa viranomaisen tietopyyntö tuottaa vastauksena useiden käyttäjien tietoja. Verkkoteknologiaan liittyvistä syistä sääntelylle (eli käyttäjän tunnistamiseksi tarvittavien välitystietojen tallentamiselle) voi olla olemassa vakavan rikollisuuden torjumisen näkökulmasta hyväksyttävä peruste. (PeVL 18/2014 vp, s. 8) Sähköisen viestinnän palveluista annetun lain 157 §:n 5 momentissa kuitenkin päädyttiin säätämään, että säilytysvelvollisuus ei koske verkkosivustojen selaamisesta kertyviä välitystietoja.

Arviomuistion laatimisen yhteydessä tietoja hyödyntävät viranomaiset ovat tuoneet esiin tarpeen IP-osoitteisiin liittyvien tietojen laajemmalle säilyttämiselle. Nykyisin yllä esitetysti säilytysvelvollisuuden ulkopuolelle on rajattu verkkosivustojen selaamisesta kertyvät välitystiedot. Viestintäviraston määräyksessä 53 B/2014 M internetyhteyspalveluista säilytettävien tietojen on täsmennetty koskevan internetyhteyden aikaista staattista tai dynaamista IP-lähdeosoitetta sekä tiedot siihen liittyvistä osoitemuunnoksista. Tällä hetkellä säilytysvelvollisuuden alaisista tiedoista on rajattu pois IP-osoitteen tunnistamiseen tarkoitetuista tiedoista IP-kohdeosoite ja kohdeporttitieto, eli tietoja siitä, minne käyttäjä on ollut yhteydessä, ei säilytetä säilytysvelvollisuuden toteuttamiseksi. Näiden sisällyttäminen tallennettaviin tietoihin rajaisi huomattavasti poliisille tietopyyntöjen vastauksissa luovutettavien tietojen ja asiakkaiden määrää. IP-kohdeosoite on jo poliisin tiedossa kyselyä tehtäessä, koska rikostutkinta verkossa aloitetaan IP-kohdeosoitteen kautta. Jos IP-kohdeosoite olisi tallennettu DR-tietokantaan, saataisiin vastaukset useissa tapauksissa rajattua vain muutamaan mahdolliseen

henkilöön, joka tai jotka ovat mahdollisesti syyllistyneet rikokseen. Tietojen rajatulla tallentamisella pystyttäisiin siis rajaamaan teleoperaattorin vastauksiin vain ne asiakkaat, joilla on tosiasiallisesti ollut mahdollisuus olla rikoksen tapahtumapaikalla eli sillä palvelimella, jossa rikoksen todiste tai seuraus on syntynyt. Tällä hetkellä ilman näitä korrelaatiotietoja vastauksissa saadaan 16-256 mahdollista tekijää.[144]

Tällaisten tietojen tallentaminen tarkoittaisi käytännössä liittymän kaiken liikenteen metatietojen säilyttämistä. Kohdetietojen säilyttämisen avulla olisi mahdollista osoitteenmuunnosta käyttävien liittymien kohdalta selvittää erittäin tarkasti, mitä kaikkia palveluita on käytetty palvelimen, esimerkiksi verkkosivuston tasolla. Lokiin tallentuisi tieto muun muassa siitä, mistä kaikista lähteistä on haettu sivulle kuuluvia sisältöjä tai tehty muita verkkokutsuja. Teleyrityksellä ei ole syytä tallentaa tällaisia tietoja omia tarpeitaan varten.[145]

Kohdeosoitteiden tallentaminen internetyhteyspalveluntarjoajan toiminnasta johtaisi kuitenkin käytännössä merkittävään tietomassaan, josta olisi mahdollista tehdä hyvin pitkälle meneviä johtopäätöksiä käyttäjän yksityiselämästä. Tällaisten tietojen yhdistämisen perusteella yksilöstä voidaan laatia yksityiskohtainen profiili, joka on unionin tuomioistuimen mukaan yksityiselämän kunnioittamista koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö. (Tele2 kohdat 98-99 sekä Digital Rights Ireland kohdat 26-27) Myös perustuslakivaliokunta on pitänyt vierailtuja sivustoja koskevia tunnistamistietoja esimerkkinä sellaisista tiedoista, joiden perusteella yksilöstä voidaan selvittää hyvinkin tarkasti yksityiselämän suojan ydinalueelle kuuluvia tietoja. (PeVL 35/2018 vp, s. 24) Selvityksen yhteydessä on tuotu esiin, että arvioinnissa voitaisiin ottaa huomioon yllä todettu sitä, että tällainen säilyttäminen johtaisi käytännössä harvempien henkilöiden tietojen luovuttamiseen viranomaiselle tietopyyntöön vastattaessa. Toisaalta unionin tuomioistuimen oikeuskäytännön valossa tämä ei vaikuta painavalta perustelulta, sillä tuomioistuimen mukaan tietojen tallentamisen perusoikeuden rajoituksen kannalta ei ole merkitystä sillä, käytetäänkö säilytettyjä tietoja myöhemmin. Oikeus saada tietoja merkitsee erillistä puuttumista käyttäjän perusoikeuksiin riippumatta, miten niitä käytetään myöhemmin. (QdN kohdat 115-116 ja siinä viitattu oikeuskäytäntö)

Internetyhteyspalveluun liittyvien tietojen laajempi säilyttäminen olisi merkittävä muutos nykytilaan. Kuten perustuslakivaliokunta totesi nykyisen lain säätämisen yhteydessä, mahdollisuus tallentaa verkkosivujen selaamisesta kertyvät tiedot merkitsisi

[144] Kohde-IP tarvittaisiin korrelaatiotiedoksi tapauksissa, joissa yhteyden tarjoava teleoperaattori käyttää IPv4 CG-NAT (Carrier Grade NAT osoitteenmuunnosta) jakamaan yhden julkisen osoitteen usealle samanaikaiselle käyttäjälle.
[145] Vrt. aikaisemmin käsitelty perustuslakivaliokunnan lausuntokäytäntö, jossa valiokunta on pitänyt suhteellisuusperiaatteen kannalta tärkeänä, ettei palveluntarjoajaa velvoiteta erikseen tuottamaan tai hankkimaan tietoja, vaan ainoastaan säilyttämään tarjoajan saatavilla muutenkin olevat tiedot. (PevL 3/2003, s. 2/II, PeVL 3/2006 vp, s. 3/I, PeVL 35/2004 vp, s. 3/II)

periaatteellisesti merkittävää puuttumista yksityiselämän ja henkilötietojen suojaan. (PeVL 18/2014 vp, s. 8) Tämä kasvattaisi erityisesti säilytysvelvollisen yrityksen säilyttämien tietojen määrää merkittävästi. Käytännössä tämä johtaisi kaiken viestiliikenteen metatietojen säilyttämiseen yhden palveluntarjoajan järjestelmässä. Tällaisen tietomassan säilyttäminen edellyttäisi erityisiä toimia niiden luvattoman käytön tai muiden väärinkäytösten riskien estämiseksi.

Unionin tuomioistuin on tarkastellut oikeuskäytännössään IP-osoitteiden tallentamista vakavan rikollisuuden ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien torjumiseksi sekä kansallisen turvallisuuden suojaamiseksi. Yllä jaksossa 6.3.3.5 on käsitelty tarkemmin näitä edellytyksiä. Unionin tuomioistuimen mukaan unionin oikeus ei ole esteenä lainsäädännölliselle toimenpiteelle, jossa säädetään *pelkästään jonkin liittymän lähteelle annettujen* IP-osoitteiden yleisesti ja erotuksetta tapahtuvasta säilyttämisestä. Lisäksi edellytyksenä on, että tällaiseen mahdollisuuteen sovelletaan tiukasti aineellisia ja menettelyllisiä edellytyksiä, joita kyseisten tietojen käyttöön on sovellettava. (QdN kohta 155)

Näin ollen myös muiden kuin liittymän lähteelle annettujen IP-osoitteiden säilyttäminen yleisesti ja erotuksetta vaikuttaa ongelmalliselta unionin tuomioistuimen oikeuskäytännön valossa. Tästä syystä laajempi IP-osoitteisiin liittyvien tietojen tallentaminen ei vaikuta mahdolliselta, ainakaan siinä merkityksessä kuin jaksossa 6.3.3.5 tätä säilyttämismahdollisuutta on arvioitu. Laajempi säilyttäminen vaikuttaisi edellyttävän jonkin laista kohdentamista, jolla varmistetaan, että toimenpide on oikeassa suhteessa yleisen edun mukaisten tavoitteiden kanssa.

Unionin tuomioistuimen IP-osoitteiden säilyttämistä ja luovuttamista koskevan oikeuskäytännön osalta on erityisesti huomattava, että tuomioistuimessa on edelleen vireillä ennakkoratkaisupyyntö asiassa C-470/21 (Qdn II tai ns. Hadopi-ratkaisu). Vaikuttaa tarkoituksenmukaiselta, että IP-osoitteiden säilyttämiseen ja käyttöön liittyviä kysymyksiä tarkastellaan yksityiskohtaisesti kyseisen ratkaisun julkistamisen jälkeen.

7.4 Tietojen saantia koskevien pyyntöjen yksilöiminen

Unionin tuomioistuin on oikeuskäytännössään käsitellyt myös tietojen saannille asetettavia edellytyksiä. Tietojen saannin edellytyksenä on tuomioistuimen tai riippmattoman hallintoviranomaisen suorittama ennakkovalvonta. Riippumattomalla hallinnollisella elimellä on oltava asema, jossa se voi suorittaa tehtävänsä objektiivisesti ja puolueettomasti. Riippumattomuuden vaatimus siis edellyttää, että kyseinen viranomainen on ulkopuolinen siihen viranomaiseen nähden, joka pyytää kyseisten tietojen saantia. (Prokuratuur kohdat 53 ja 54) 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). Ennakkovalvontaa suorittavan tuomioistuimen tai elimen ratkaisu annetaan perustellusta pyynnöstä, jonka nämä viranomaiset esittävät rikoksen estämis-, selvittämis- tai syyteharkintamenettelyssä. (TS kohta 120) Toimivaltaisten 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)

Vuoden 2021 arviomuistiossa katsottiin, että unionin tuomioistuimen oikeuskäytännöstä ei tule välitöntä muutostarvetta tietojen saantia koskevalle sääntelylle. Siinä tuotiin kuitenkin esille, että unionin tuomioistuin on täydentänyt, että toimivaltaisten 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. Välitöntä muutostarvetta ei kuitenkaan nähty, sillä tämä voitaisiin huomioida kansalliseen sääntelyyn sisältyvien yleisten välttämättömyysvaatimusten kautta.

Pakkokeinolain 10 luvun 9 §:ssä säädetään televalvontaa koskevan vaatimuksen sisällöstä[146]. Siinä ei erikseen vaadita rajaamaan saatavia tietoja. Televalvontaa koskevassa vaatimuksessa on mainittava rikoksesta epäilty tai epäillyn ollessa tuntematon toimenpiteen kohteena oleva teleosoite tai telepäätelaite. Pakkokeinolain 1 luvun 3 §:ssä on asetettu yleinen välttämättömyysvaatimus. PKL 10:9:n mukaisen televalvonnan osalta 1 luvun 3 §:n mukaisen välttämättömyysvaatimuksen lisäksi relevantteja ovat 1 luvun 2 §:n mukainen suhteellisuusperiaate ja 10 luvun 2 §:n 1 momentti, jonka mukaan salaisen pakkokeinon käytön yleisenä edellytyksenä on, että käytöllä voidaan olettaa saatavan rikoksen selvittämiseksi tarvittavia tietoja.

Asian jäämistä yleisten välttämättömyyssäännösten piiriin voidaan pitää epätyydyttävänä unioninoikeuden näkökulmasta. Lainmuutos olisi kuitenkin vastoin viimeaikaista kansallista kehitystä, jossa menettelyä on pikemminkin pyritty keventämään. Aikaisemmin laissa säädettiin, että vaatimuksessa on esitettävä toimenpiteen kohteena oleva teleosoite tai telepäätelaite. 1.10.2023 voimaan tulleella muutoksella pakkokeinolakia (452/2023) ja poliisilakia (492/2023) muutettiin siten, että telekuuntelu- ja televalvontalupaa ei enää jatkossa haeta ja määrätä teleosoite- tai telepäätelaitekohtaisesti, vaan telepakkokeinoja voidaan kohdistaa mihin tahansa tietyn epäillyn käytössä

[146] Vastaavasti myös poliisilain 5:10.6 sekä 1:3 ja 5:2.2; laki rikostorjunnasta Rajavartiolaitoksessa 18.4 § ja 14.2 §; laki rikostorjunnasta Tullissa 3:6.5 sekä 1:6 ja 3:2.2.

olevaan osoitteeseen tai laitteeseen. Epäillyn käyttämien teleosoitteiden ja -päätelaitteiden yksilöintitietojen selvittäminen jää pidättämiseen oikeutetun virkamiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen virkavastuulla selvitettäväksi 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.

Perustuslakivaliokunnan käsityksen mukaan kyseinen muutos merkitsee huomattavaa ja periaatteellisesti merkittävää muutosta perustuslain 10 §:ssä turvatun luottamuksellisen viestin salaisuuden suojan rajoittamista koskevaan lainsäädäntöön, ja se on omiaan heikentämään telepakkokeinojen käyttöä koskevaa oikeussuojaa. (PeVL 98/2022 vp, PeVL 99/2022 vp) Perustuslakivaliokunta ei kuitenkaan ole arvioinut muutosta nimenomaan suhteessa unionin tuomioistuimen tietojen saantia koskevaan oikeuskäytäntöön.

Teleosoitteiden ja –päätelaitteiden yksilöintitiedon selvittäminen jää edelleen poliisin virkavastuulla selvitettäväksi asiaksi. Asiasta tehdään erillinen päätös, jossa tulee perustella, miksi toimenpiteen kohteeksi on valittu juuri toimenpiteen kohteena olevat teleosoitteet tai telepäätelaitteet. Päätös on pakkokeinolain 10:65 §:ssä tarkoitetun laillisuusvalvonnan piirissä. Jälkivalvonnan kannalta keskeistä on, että televalvontaa koskevassa ilmoituksessa epäillylle olisi jatkossa yksilöitävä toimenpiteen kohteena olleet teleosoitteet ja telepäätelaitteet. Epäillylle ilmoittamisesta on jatkossakin samalla kirjallisesti ilmoitettava luvan myöntäneelle tuomioistuimelle.

Unionin tuomioistuimen mukaan toimivaltaisten kansallisten viranomaisten tehtävänä on varmistaa, että tietopyynnöt rajataan tietoluokkien ja ajanjakson osalta välttämättömään. Kansallisessa laissa ei ole yleistä välttämättömyysvaatimusta tarkempaa sääntelyä tietopyynnön rajaamisesta tietokategorioittain ja ajallisesti välttämättömään. Jatkossakin tuomioistuin päättää televalvonnan kohdistamisesta tiettyyn henkilöön. Toimenpiteen laajuus ja kohdistuminen henkilön hallussa olevaan tai käyttämään laitteeseen tai osoitteeseen riippuu pidättämiseen oikeutetun virkamiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen päätöksestä, jossa tulee perustella, miksi toimenpiteen kohteeksi on valittu juuri toimenpiteen kohteena olevat teleosoitteet tai telepäätelaitteet. Päätökseen kohdistuu jälkivalvonta. Unionin tuomioistuimen edellytys kansallisen viranomaisen tehtävästä tietopyynnön rajaamisesta vaikuttaisi siis edelleen täyttyvän kansallisessa lainsäädännössä. Edelleen kuitenkin on kyseenalaista, onko kansallisessa lainsäädännössä asetettu riittävä velvoite tietopyynnön rajaamiseen siten kuin unionin tuomioistuin on oikeuskäytännössään edellyttänyt.

Arvion mukaan asiassa ei ole välitöntä muutostarvetta. Lisäksi asia vaatisi laajempaa selvittämistä tuomioistuinvalvonnan ja lain tasolla edellytettävän tietopyynnön yksilöimisen vaatimuksista, joten säädösmuutokselle ei nähdä välitöntä tarvetta.

7.5 Tietoja saavat viranomaiset ja tietojen käyttö rikosten ennalta estämiseksi

Sähköisen viestinnän palveluista annetun lain 322 §:n mukaan viranomaisten oikeudesta saada välitystietoja rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi säädetään poliisilaissa, rikostorjunnasta Rajavartiolaitoksessa annetussa laissa, henkilötietojen käsittelystä Rajavartiolaitoksessa annetussa laissa, rikostorjunnasta Tullissa annetussa laissa, henkilötietojen käsittelystä Tullissa annetussa laissa ja pakkokeinolaissa. 157 §:n perusteella säilytettäviä tietoja voivat saada säilytysvelvollisilta yrityksiltä ainoastaan ne viranomaiset, joilla on lain perusteella oikeus saada tiedot. Lain esitöiden mukaan kyseinen säännös vastaa teknisluonteisia muutoksia lukuun ottamatta sisällöltään entisen sähköisen viestinnän tietosuojalain 36 §:ää. Muutoksilla ei ole pyritty muuttamaan viranomaisten tiedonsaantioikeuden laajuutta. (HE 221/2013 vp, s. 228) Kyseinen säännös osoittaa lain keskeisen periaatteen, jonka mukaan ehdotetulla lailla säädetään vain tietojen säilyttämisestä. Tietojen hyödyntäminen eli viranomaisten tiedonsaantioikeudet määräytyvät muiden säännösten mukaisesti. (HE 158/2007 vp, s. 28)

Sähköisen viestinnän palveluista annetun lain 157 §:n mukaan säilytettäviä tietoja saa käyttää ainoastaan pakkokeinolain 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi. Tietojen käyttötarkoitukset on lisäksi laajennettu siviili- ja sotilastiedusteluun näitä koskevissa laeissa. Yllä olevien lisäksi viranomaisten oikeudesta saada viestinnän välitystietoja säädetään myös sotilastiedustelulaissa, jonka 103 §:n mukaan SVPL 157 §:n 1 momentissa säilytettävien tietojen käyttämisestä säädetyn lisäksi säilytettäviä tietoja saadaan käyttää myös tietojen hankkimiseksi sotilastiedustelun kohteena olevasta sotilastiedustelulain 4 §:ssä tarkoitetusta toiminnasta. Samoin poliisilain 5 a luvussa on säädetty näiden SVPL 157 §:n mukaisesti säilytettyjen tietojen käyttämisen sallimisesta, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Lisäksi tietoja voidaan saada, kuten yllä jaksossa 2.2 on tarkemmin käsitelty, myös poliisilain 4:3.2:n nojalla, jolloin tietojen käyttötarkoitus on SVPL 157.1:n sanamuotoa laajempi, sillä pakkokeinolain 10:6.2:ssa tarkoitettujen rikosten selvittämisen ja syyteharkintaan saattamisen lisäksi tietoja on pyydetty ja saatu rikosten ennalta estämiseksi ja paljastamiseksi. SVPL 157.1:n rajoituksen mukaan tietojen käytön edellytyksenä kuitenkin on, että kyseessä tulee olla televalvontarikos.

Nykyistä lainsäädäntöä valmisteltaessa perustuslakivaliokunta katsoi, SVPL 322 §:n sääntely täytti unionin tuomioistuimen tuomiossa tarkoitetun objektiivisen perusteen vaatimuksen rajoittaa tietoja saavien ja käyttävien henkilöiden määrää sekä käyttää niitä vain vakavien rikosten yhteydessä (PeVL 18/2014 vp, s. 7). SVPL 322 §:n 2 momentin nojalla säilytettäviä tietoja voivat saada ainoastaan ne viranomaiset, joilla on

jonkun muun lain perusteella oikeus saada tiedot. Tämä logiikka olisi edelleen tarkoituksenmukaista tai jopa välttämätöntä säilyttää.

Vuoden 2017 selvityksen eriävissä mielipiteissä ja vuoden 2021 arviomuistiossa kuvatusti viestintäpalvelulain 157 §:n ja 322 §:n keskinäisen suhteen tulkinnassa on ollut erimielisyyksiä. Kuten aikaisemmin selvityksessä on todettu, SVPL 157 §:n säätämisen yhteydessä tietojen käyttötarkoituksista on jätetty pois maininta aikaisemmin lakiin sisältyneestä mahdollisuudesta käyttää tietoja myös rikosten tutkimiseksi. Asiaa ei kuitenkaan ole valmisteluasiakirjoissa avattu.

Perustuslakivaliokunta on aikaisemmassa lausuntokäytännössään todennut, että mikä tahansa viranomaistarve ei voi oikeuttaa tietojen säilyttämisvelvollisuutta. (PeVL 3/2008 vp, s. 2/II) Tämän ja unionin tuomioistuimen oikeuskäytännön edellytysten johdosta myös jatkossa säilytysvelvollisuuden sääntelyn yhteydessä tulisi määritellä ne tarkoitukset, joihin tietoja voidaan vaatia säilytettäväksi. Tässä yhteydessä tulisi pyrkiä selventämään säilytettyjen tietojen saanti myös rikosten ennalta estämiseen. Asiaa tulee vielä arvioida sekä ePrivacy-direktiivin 15 artiklan mukaisten käyttötarkoitusten, eli rikosten torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamisen, lisäksi myös perustuslain näkökulmasta. Perustuslain 10 §:n 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana.

Edellä 6.3.2 jaksossa esitetysti säilyttämisperusteet on syytä eriyttää. Vaikuttaa perustellulta selkeyttää lainsäädäntöä siten, että säilytysvelvollisuutta koskevissa pykälissä säädettäisiin jatkossa selvemmin tietojen säilytysperusteesta ja 322 §:ssä informatiivisesti oikeudesta tietojen saantiin tiettyä tarkoitusta varten. Tässä yhteydessä voisi olla tarpeen säätää informatiivisesti poliisin oikeudesta saada tietoja eräitä poliisitehtäviä varten siten kuin poliisilaissa säädetään.

Pykälien keskinäissuhteessa olisi otettava huomioon unionin tuomioistuimen vaatimukset säilytysperusteen ja tietojensaantiperusteen symmetrisyydestä, eli tietojen saantiperusteen tulee vastata vakavuudeltaan sitä perustetta, jolla niiden säilyttäminen on oikeutettu. Toisaalta on huomioitava, että yleisen edun tavoitteiden hierarkiaopin mukaisesti tietojen käyttö voidaan sallia tärkeydeltään korkeampien tavoitteiden vuoksi myös alemman tason säilytysperusteen nojalla säilytettyihin tietoihin. Yleisen edun tavoitteiden lisäksi olisi syytä tarkastella tietojen käytön nimenomaista sallimista rikosten ennalta estämiseksi ja paljastamiseksi nykyisen tulkintaepäselvyyden poistamiseksi.

7.6 Tietojen säilyttäminen ja saanti eräissä poliisitutkinnoissa

Poliisilain televalvontaa koskevien säännösten lisäksi poliisilla on oikeus saada viestinnän välitystietoja eräissä poliisitutkinnoissa. Poliisitutkinnalla tarkoitetaan muuta poliisin toimitettavaksi laissa säädettyä tutkintaa kuin rikoksen johdosta toimitettavaa esitutkintaa.

Poliisilain 5:8.5 mukaan poliisille voidaan ensinnäkin antaa lupa kuolemansyyn selvittämisestä annetussa laissa (459/1973) tarkoitetussa kuolemansyyn selvittämisessä vainajan hallussa olleen teleosoitteen tai telepäätelaitteen televalvontaan, jos toimenpiteellä voidaan perustellusti olettaa saatavan kuolemansyyn selvittämisessä tarvittavia tietoja.

Toiseksi poliisilain 1:1.2 mukaan poliisin on ryhdyttävä tarpeellisiin toimenpiteisiin henkilön löytämiseksi, jos on perusteltua syytä olettaa henkilön kadonneen tai joutuneen onnettomuuden uhriksi. Tähän liittyen poliisilain 6:1.1 säädetään, että poliisin on suoritettava poliisitutkinta, jos se on ilmoituksen perusteella tai muusta erityisestä syystä tarpeen kadonneen henkilön löytämiseksi. Poliisille ei kuitenkaan ole säädetty oikeutta saada televalvontatietoja kadonneen löytämiseksi. Sen sijaan sähköisen viestinnän palvelulain 321 §:ssä säädetään niin kutsutusta hätäpaikantamisesta. Mainitun pykälän mukaan teleyritys on velvollinen luovuttamaan poliisille käsiteltäväksi sen liittymän tai päätelaitteen, josta hätäilmoitus on tehty, sijaintitiedot ja tiedot liittymän tunnisteesta, tilaajasta, käyttäjästä ja asennusosoitteesta sekä hätäilmoituksen kohteena olevan henkilön käyttämän liittymän tai päätelaitteen sijaintitiedot sekä tiedot liittymän tunnisteesta, tilaajasta, käyttäjästä ja asennusosoitteesta, jos henkilö on hätäilmoituksen vastaanottaneen viranomaisen perustellun käsityksen mukaan ilmeisessä hädässä tai välittömässä vaarassa.

Poliisitutkintaan liittyvien tilanteiden lisäksi poliisilla on poliisilain 5:8.3 mukaan oikeus televalvontaan 5:8.2 estämättä, jos sen välitön toteuttaminen on välttämätöntä henkeä tai terveyttä uhkaavan vaaran torjumiseksi.[147] Esitöiden mukaan kysymyksessä olisi siten henkilön eräänlainen kiirepaikantaminen, jos se on välttämätöntä henkeä tai terveyttä uhkaavan vaaran torjumiseksi. (HE 224/2010 vp, s. 98)

Sähköisen viestinnän palvelulain 157 §:ssä ei ole erikseen säädetty säilyttämisvelvollisuudesta näihin poliisitehtäviin. Vastaavia käyttötarkoituksia ei ole mainittu sähköi-

[147] Samoin laki rikostorjunnasta Tullissa 3:4.3.

sen viestinnän tietosuojadirektiivin 15(1) artiklassa, mutta ne voisi mahdollisesti kiinnittää joko yleiseen turvallisuuteen[148] tai rikosten torjuntaan, tutkintaan ja selvittämiseen. Perustuslain 10 §:n 4 momentin käyttötarkoituksista voitaisiin puolestaan kiinnittyä yksilön turvallisuutta vaarantavien rikosten tutkintaan. Tämän säilytysvelvollisuuden tulisi olla välttämätöntä.

Poliisilain 5:8.3 ja sähköisen viestinnän palvelulain 321 §:n mukaisissa tilanteissa kyse on kiiretilanteesta. Sääntelyn tarkoituksena on saada tietoja lyhyeltä ajalta taaksepäin. Näin ollen toimi kohdistuisi sellaisiin tietoihin, joita teleyritys tyypillisesti vielä säilyttää omia tarpeitaan varten. Erillistä säilytysvelvollisuutta ei siis olisi välttämätöntä säätää näitä varten.[149] Nimenomaisen sääntelyn puuttuminen voi kuitenkin johtaa tilanteeseen, jossa välttämättömät tiedot eivät ole saatavilla teleyritysten omien säilytystarpeiden muuttuessa.

Poliisilain 5:8.5 mukaisessa tilanteessa televalvontatietojen saaminen on arvioitu välttämättömäksi. Säännöskohtaisten perustelujen mukaan (HE 224/2010 vp, s. 99/I): ”Poliisilla ei ole voimassa olevan oikeuden mukaan oikeutta televalvontatietojen käyttöön momentissa tarkoitetussa tapauksessa. Kuolemansyyn selvittämisen intressi on kuitenkin tärkeä jo pelkästään henkirikoksen poissulkemisen vuoksi. Tällaiset tiedot voivat tuoda merkittävästi lisäselvitystä esimerkiksi vainajan viimeisten liikkeiden selvittämisen kautta. Näin voidaan saada selvitystä kuolemaan johtaneista olosuhteista.”

Televalvontaa käytetään kuolemansyyn selvittämiseksi vain poikkeuksellisissa tapauksissa, joissa voidaan poliisilain 5:8.5 edellytysten mukaisesti perustellusti olettaa saatavan kuolemansyyn selvittämisessä tarvittavia tietoja. Esimerkiksi vuonna 2022 televalvontatietoja on käytetty tuomioistuimen myöntämällä luvalla kuolemansyyn selvittämisessä 11 tapauksessa.[150]

Televalvontatietojen käyttämisen henkirikoksen poissulkemiseksi tai henkirikoksen paljastamiseksi voidaan katsoa rinnastuvan vakavuudeltaan vakavan rikollisuuden torjuntaan. Tietojen säilyttämisestä tätä tarkoitusta varten tulisi kuitenkin säätää erikseen. Toisaalta unionin tuomioistuimen yleisen edun mukaisten tavoitteiden hierar-

[148] Tällöin tosin mentäisiin perinteisestä turvallisuuskäsityksestä (suoja väkivallalta) kohti laajaa turvallisuuskäsitystä (myös muun muassa muun muassa köyhyyteen, terveyteen, ympäristöön ja henkilökohtaiseen koskemattomuuteen liittyvät uhat). Tällainen laajentuminen olisi kuitenkin hyväksytty perustuslakivaliokunnan käytännössä. (Niklas Vainio, Viestinnän yksityisyyden suojan turvallisuusperusteinen rajoittaminen perustuslakivaliokunnan käytännössä. Lakimies 6/2017 s. 813–837, 815–817.)
[149] On kuitenkin seurattava, mitä unionin tuomioistuin linjaa tapauksessa C-241/22 DX.
[150] Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2022, s. 16-17.

kiaopin kanssa yhteensopivasti toisena vaihtoehtona voitaisiin tarkastella mahdollisuutta säätää mahdollisuudesta käyttää vakavan rikollisuuden torjunnan tarkoituksiin säilytettyjä tietoja.

Unionin tuomioistuimen oikeuskäytännöstä seuraa, että liikenne- ja paikkatietojen säilyttämisestä johtuvan puuttumisen vakavuus tulee suhteuttaa yllä esitetyn yleisen edun mukaisten tavoitteiden luokkien mukaisesti. Unionin tuomioistuimen mukaan ainoastaan *vakavan* rikollisuuden torjuminen ja yleiseen turvallisuuteen kohdistuvien *vakavien* uhkien ehkäiseminen voivat suhteellisuusperiaatteen mukaisesti oikeuttaa liikenne- ja paikkatietojen säilyttämisestä johtuvan kaltaiset vakavat puuttumiset perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin. (QdN kohta 140) Unionin tuomioistuin on arvioinut oikeuskäytännössään käsittelemistä säilyttämistoimenpiteistä johtuvien perusoikeuden rajoituksen vakavuutta. Näistä vain henkilöllisyyttä vastaavien tietojen säilyttäminen on unionin tuomioistuimen mukaan suhteellisuusperiaate huomioiden yhteensopiva yleisesti rikollisuuden torjumisen ja yleiseen turvallisuuteen kohdistuvien uhkien ehkäisemisen tavoitteiden mukaista.

Vain sellaiset puuttumiset mainittuihin perusoikeuksiin, jotka eivät ole vakavia, voidaan oikeuttaa rikosten torjuntaa, tutkintaa, selvittämistä ja syyteharkintaa yleisesti koskevalla tavoitteella. (G. D. kohta 59)

Yllä esitetty yleisen edun mukaisten tavoitteiden hierarkiasta soveltuu soveltuvin osin sellaisten liikenne- ja paikkatietojen myöhempään käyttöön, joita sähköisten viestintäpalvelujen tarjoajat ovat säilyttäneet vakavan rikollisuuden torjumiseksi toteutetun toimenpiteen perusteella. Tällaisia tietoja ei nimittäin voida sen jälkeen, kun niitä on säilytetty ja annettu toimivaltaisten viranomaisten käyttöön vakavan rikollisuuden torjumiseksi, välittää muille viranomaisille eikä käyttää korruptiota muistuttavien virkavirheiden torjumisen kaltaisten sellaisten tavoitteiden saavuttamiseksi, jotka ovat yleisen edun mukaisten tavoitteiden hierarkiassa alempana kuin vakavan rikollisuuden torjunta ja yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäiseminen. (A. G. kohta 41)

7.7 Arkaluonteisten tietojen käsittelyyn ja automaattiseen käsittelyyn liittyvien erityisten suojakeinojen tarve

Unionin tuomioistuimen mukaan oikeasuhteisuutta koskevan edellytyksen täyttämiseksi säännöstössä on säädettävä selvistä ja täsmällisistä kyseessä olevan toimenpiteen laajuutta ja soveltamista koskevista säännöistä, joissa asetetaan vähimmäisvaatimukset, jotta henkilöillä, joiden henkilötiedoista on kyse, on riittävät takeet, joiden

avulla heidän henkilötietojaan voidaan tehokkaasti suojata väärinkäytön vaaroilta. Kyseisen säännöstön on oltava kansallisen oikeuden mukaan laillisesti sitova, ja siinä on erityisesti mainittava, missä olosuhteissa ja millä edellytyksin tällaisten tietojen käsittelyä koskeva toimenpide voidaan toteuttaa, jotta taataan, että puuttuminen rajoittuu täysin välttämättömään. Tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti, etenkin, kun on olemassa huomattava näiden tietojen lainvastaista saantia koskeva vaara. Nämä näkökohdat pätevät erityisesti silloin, kun on suojattava kyseistä henkilötietojen erityisryhmää eli arkaluonteisia tietoja. (QdN kohta 132)

Unionin tuomioistuin on katsonut, että tarve viranomaisten pääsyä rajoittaville edellytyksille on tärkeä etenkin silloin, kun henkilötietoja käsitellään automaattisesti. (Privacy International kohta 68)

Kansallisessa lainsäädännössä ei tällä hetkellä säädetä nimenomaisesti tietojen automaattisesta käsittelystä tai analysoinnista. Tällaista käsittelyä ei ole myöskään erikseen suljettu pois.[151] Tietojenkäsittelyssä ja siirtämisessä on aina kyse automaattisesta tietojenkäsittelystä (verrattuna manuaaliseen käsittelyyn), mutta ei sillä tavalla mitä unionin tuomioistuin vaikuttaa tässä yhteydessä tarkoittavana. Esimerkiksi SALPA-järjestelmän pitää erikseen luoda pyyntö saada tietoja ja teleoperaattorien pitää erikseen lähettää vastaus siihen.

Rikostuomioihin ja rikoksiin liittyvät henkilötiedot voidaan myös lukea valtiosääntöisesti arkaluonteisiksi (PeVL 15/2018 vp, s. 38). Niiden käsittelystä säädetään erikseen yleisen tietosuoja-asetuksen 10 artiklassa, jossa edellytetään asianmukaisten suojatoimien säätämistä. Nykyisessä lainsäädännössä ei ole katsottavissa olevan arkaluonteisten tietojen käsittelyn tarkempaa arviointia edellyttäviä kirjauksia. Unionin tuomioistuimen oikeuskäytännöstä on kuitenkin luettavissa, että säilytysmääräys olisi mahdollista kohdentaa tiettyihin henkilöihin esimerkiksi aikaisemman rikostuomion perusteella. Tällaisten tietojen mahdollista käsittelyä tunnistamismääräyksen toimeenpanemiseksi käsitellään yksityiskohtaisemmin yllä jaksossa 6.3.2.2.

7.8 Viranomaisten avustamisesta johtuvien kulujen korvaaminen

Lainmuutokset yhteydessä tulee arvioida edellytykset korvata teleyrityksille säilyttämisvelvollisuuden järjestämisestä ja tietojen toimittamisesta aiheutuvat kustannukset.

[151] Ks. vastaavasti arviomuistio 2021, s. 19, jolloin johtopäätöksenä oli, ettei kansallisessa laissa ole tältä osin välitöntä muutostarvetta, mutta asia tulee huomioida selvemmin, jos sääntelyä muutetaan.

Yllä tarkemmin käsitellysti SVPL 299 §:n mukaan järjestelmien, laitteistojen ja ohjelmistojen investoinneista ja ylläpidosta aiheutuneet välittömät kustannukset tulisivat valtion korvattavaksi. Tietopyyntöihin vastaamisesta aiheutuneista kustannuksista ei kuitenkaan makseta korvausta. Liikenne- ja viestintävaliokunta on edellyttänyt siviilitiedustelusääntelyn säätämisen yhteydessä, että viranomaisten avustamisesta aiheutuvien kustannusten tasoa seurataan tiiviisti ja ryhdytään viipymättä toimenpiteisiin korvaussääntelyn muuttamiseksi, jos kustannukset nousevat merkittävästi nykyisestään. (LiVL 26/2018 vp)

Työvoimakustannusten korvaamisella on yhteys perusoikeuksien toteutumiseen, kun teleyrityksellä on paremmat edellytykset tai kannustimet huolehtia järjestelmän tietoturvasta ja pyyntöjen asianmukaisesta käsittelystä. Perustuslaki ei näytä edellyttävän korvaamista. Oikeuskirjallisuudessa on katsottu, ettei perusoikeuksien kannalta olisi ongelmallista, jos tietojen keräämisestä jäävät henkilötyökustannukset jäävät operaattorin vastuulle, kunhan työmäärä ei ole kohtuuton. Oikeuskirjallisuudessa on kuitenkin todettu, että kehityskulkuna on ollut korvattavien tehtävien supistuminen ja korvauksettomien tehtävien laajentuminen.[152] Näin ollen kysymys on kohtuullisuuden arvioinnista ja lopulta eduskunnan harkintavallassa lainsäätäjänä ja budjettivallan käyttäjänä.

Selvityksen laatimisen yhteydessä säilytysvelvolliset yritykset ovat tuoneet esiin, että viranomaiskyselyiden aiheuttama henkilötyömäärä on lisääntynyt operaattoreilla viimeisten vuosien aikana. Sekä pyyntöjen että niihin sisältyvien kyselyiden määrä on kasvanut kaikissa tietopyyntötyypeissä. Yritysten mukaan kasvu on ollut 20-40 %:n luokkaa verrattuna vuoteen 2022. Suurin osa tietopyynnöistä pystytään käsittelemään tietojärjestelmin. Ongelmallisena nähdään erityisesti manuaalista työtä vaativat kyselyt, joissa on nähty merkittävää, paikoin jopa 70 %:n kasvua. Teleyritysten arvioiden mukaan kaikki lainsäädännön edellyttämät tekniset muutokset tulevat vaatimaan manuaalista työtä tietopyyntövastausten oikeellisuuden ja prosessin toiminnan varmistamiseksi.

Alueelliseen kriteeriin perustuva säilytysvelvollisuus on teleyritysten arvion mukaan haastavaa toteuttaa. Tällainen vaatimus tulisi ennen kaikkea vaatimaan panostuksia järjestelmäkehitykseen ja siihen, miten tietoja yhdistellään ja poistetaan. Muutoksen arvioidaan lisäävän myös henkilötyötä. Ensisijaisesti tulisi kuitenkin pyrkiä ratkaisemaan eri alueisiin kohdistuvat erilaiset velvoitteet ja määritelmät automatiikalla. Tällaiset investointi- ja kehityskustannukset tulisivat valtion korvattavaksi.

Jo syntyneiden ja tallennettujen tietojen jälkikäteinen määrittely esimerkiksi yllä arvioitujen kohdentamiskriteereiden tai säilyttämisperusteiden erottelun mukaisesti johtaisi

[152] Pekka Savola, Internet-operaattori ja perusoikeudet. Oikeustiede - Jurisprudentia XLVI:2013 s. 127–222, 185 ja 188.

merkittävään määrään manuaalista työtä. Siten lähtökohtaisesti on pidettävä tavoitteena varmistaa riittävän pitkä siirtymäaika ja selkeät siirtymäsäännökset, jotta tällaiselta tilanteelta vältyttäisiin.

Kustannusten korvaamisen arvioinnissa on myös syytä kiinnittää huomiota SVPL 299 §:n vaikutuksiin suhteessa muuhun lainsäädäntöön. Viranomaiset toivat selvityksen laatimisen yhteydessä esiin, että myös e-Evidence-sääntelyn mukainen korvausmalli noudattaa kansallista sääntelyä. Pyyntöjen korvaaminen EU:n laajuisen sääntelyn johdosta saattaa johtaa merkittäviin budjettivaikutuksiin.