PERUSTUSLAKIVALIOKUNNALLE

Asia: HE 243/2022 vp Hallituksen esitys eduskunnalle laeiksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain 29 §:n ja henkilötietojen käsittelystä poliisitoimessa annetun lain 22 §:n muuttamisesta

Esitän kunnioittaen seuraavaa.

Hallituksen esityksen tavoitteena on parantaa viranomaisten toimintaedellytyksiä tietoturvaloukkausten selvittämisessä. Esityksellä pyritään luomaan selkeät edellytykset viranomaisten tiedonvaihdolle tietoturvaloukkaustilanteissa säätämällä loukkausten selvittämisen kannalta keskeistenviranomaisten keskinäisestä oikeudesta vaihtaa välttämättömiä tietoja. Lisäksi tavoitteena on luoda edellytykset tarvittavaan virka-apuun viranomaisten välillä siten, että lainsäädäntö ei muodostu esteelle virka-avun pyytämisessä. Liikenne- ja viestintäviraston osalta tavoitteena on myös keventää virka-apumenettelyn päätöksentekoprosessia.

Keskeistä ehdotuksessa on nähdäkseni se, että sillä tähdätään tietojen liikkumiseen toisaalta viranomaisten välillä, toisaalta yksityisiltä toimijoilta – kuten teleyrityksiltä ja tietoturva-ammattilaisilta – viranomaisille. Ehdotuksella pyritään siihen, että tietoa voidaan vaihtaa kunkin viranomaisen tehtävän hoitamiseksi. Tiedonvaihdon sujuvuus korostuu erityisesti vakavissa tietoturvaloukkaustilanteissa, joissa viranomaisten on toimittava nopeasti loukkauksen selvittämiseksi ja vahinkojen minimoimiseksi. Tavoitteet ovat ilman muuta hyväksyttävät. Niillä pyritään ensisijaisesti turvallisuuden parantamiseen.

Tarkastelen lausunnossani sitä, miten turvallisuuden lisääminen tietojen vaihtoa sujuvoittamalla asettuu kotimaiseen valtiosääntöiseen kehikkoon sekä Euroopan unionin oikeudessa määriteltyyn perusoikeuksien suojaan.

Henkilötietojen suoja ja keskeisin sääntely

Keskeistä tässä kontekstissa on se, miten esitykset vastaavat tietosuojasääntelyn sisältämiä vaatimuksia. Perustuslakivaliokunta on katsonut, että EU:n yleisen 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. Valiokunnan mukaan tietosuoja-asetuksen sääntely vastaa asianmukaisesti tulkittuna ja sovellettuna myös Euroopan ihmisoikeussopimuksen mukaan määräytyvää henkilötietojen suojan tasoa (esim. PeVL 14/2018 vp).

Nyt tarkasteltavan hallituksen esityksen kontekstissa moni muukin EU-oikeudellinen normisto on otettava huomioon. Erityisen merkittävä perusoikeuksien suojaamisen kannalta on sähköisen viestinnän tietosuojadirektiivi (ePrivacy-direktiivi). Direktiivin 5 artiklan mukaan sähköisen viestinnän palveluiden välityksellä tapahtuva viestintä ja siihen liittyvät liikennetiedot ovat luottamuksellisia. Direktiivin kehikossa ei ole sallittua, että muut henkilöt ilman käyttäjän suostumusta kuuntelevat, salakuuntelevat, tallentavat tai muulla tavalla sieppaavat tai valvovat viestintää ja siihen liittyviä tietoja. Jäsenvaltiot voivat kuitenkin 15 artiklan mukaan toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan direktiivissä säädettyjen oikeuksien ja velvollisuuksien soveltamisalaa, jos rajoitukset ovat välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisen viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi. Nyt käsiteltävä hallituksen esitys olisi nähdäkseni sellainen lainsäädännöllinen toimenpide, jonka tulisi täyttää direktiivin asettamat vaatimukset välttämättömyydestä, asianmukaisuudesta ja oikeasuhteisuudesta.

Unionin tuomioistuimen ePrivacy-direktiivin tulkintaa koskevassa oikeuskäytännössä on korostettu viestinnän luottamuksellisuutta osana unionin perusoikeuskirjan 7 artiklan mukaista yksityiselämän ja 8 artiklan mukaista henkilötietojen suojaa. Oikeuskäytäntö elää, mutta siinä on vakiintuneesti katsottu, että ainoastaan vakavan rikollisuuden torjumiseksi tai yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemiseksi viranomaisille voidaan antaa kansallisen lainsäädännön nojalla oikeus saada sellaisia liikenne- ja paikkatietoja, joiden muodostama kokonaisuus voi mahdollistaa yksityiskohtaisten päätelmien tekemisen sähköisen viestintävälineen käyttäjän yksityiselämästä. Lisäksi toimivaltaisen viranomaisen tiedonsaantioikeus on rajattu täysin välttämättömään (Tele2 Sverige ja Watson ym. C-203/15 ja C-698/15; Ministerio Fiscal C-207/16; Prokuratuur C-746/18). Tuomioistuin on pitänyt olennaisena sitä, että viranomaisten tietojensaantia edeltää riippumattoman hallinnollisen toimielimen, kuten tuomioistuimen, etukäteisvalvonta (La Quadrature du Net ym. C-511/18, C-512/18 ja C-520/18; Prokuratuur C-746/18). Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntö on samansuuntaista (katso esim. Szabó ja Vissy v. Unkari 2016; Roman Zakharov v. Venäjä 2015; Ekimdzhiev ja muut v. Bulgaria 2022). EIT on myös painottanut oikeusturvakeinoja viimeaikaisissa ratkaisuissaan (Centrum för rättvisa v. Ruotsi 2021 sekä Big Brother Watch ja muut v. Yhdistynyt Kuningaskunta 2021). Hallituksen esitystä, joka mahdollistaa tietojen liikkuvuuden viranomaisten välillä – ja yksityisiltä toimijoilta viranomaisille – on tarkasteltava tässä kehikossa.

Mitä tietoja luovutettaisiin?

Merkittävää on, että ehdotettu lainsäädäntö laajentaisi eri viranomaisten mahdollisuuksia kerätä yksilöistä monenlaisia tietoja ja käyttää sekä säilyttää niitä. Hallituksen esityksessä liikkuvia tietoja ei ole rajattu käytännössä millään tavalla. Esityksen perusteluissa todetaan, ettei se ole mahdollista, sillä tietoturvaloukkauksia on niin monenlaisia, ettei etukäteen voida päätellä, mitä tietoja

viranomaiset milloinkin tarvitsevat. Perustelujen mukaan ehdotuksen nojalla voitaisiin vaihtaa mitä tahansa tietoturvaloukkauksen tai -uhkien selvittämisen kannalta välttämätöntä tietoa. Käytännössä tiedot olisivat usein viestintää, välitystietoja ja hyökkäystoimintaa koskevia tietoja, mutta mahdollisesti myös *muita tietoja*. Luovutettavien tietojen sisältöä ei hallituksen esityksessä ole katsottu mahdolliseksi rajata ottaen huomioon, että tietoturvaloukkaustilanteet voivat vaihdella luonteeltaan ja ominaisuuksiltaan erittäin laajasti, eikä näitä kaikkia tilanteita voida täsmällisesti ennakoida.

Siten liikuteltaviin ja luovuteltaviin tietoihin kuuluisi niin henkilötietoja kuin erityisiä henkilötietoryhmiä, niin salaisia tietoja kuin julkisia ja niin tavallisia henkilötietoja kuin arkaluonteisia. Huomionarvoista on, että tiedot olisivat sekä metatietoja – eli esimerkiksi liikenne- ja paikkatietoja, että viestien sisältöä koskevia tietoja. Tämä lainsäädäntöratkaisu herättää jo ensisilmäyksellä kysymyksiä perusoikeusrajoitusten tarkkarajaisuudesta sekä oikeasuhtaisuudesta.

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 (ks. PeVL 13/2016 vp, s. 4, PeVL 14/2009 vp, s. 3/I). Yleisen tietosuoja-asetuksen 51 johdantokappaleen mukaan asetuksen 9 artiklassa tarkoitettuja erityisiä henkilötietoja, jotka ovat erityisen arkaluonteisia perusoikeuksien ja -vapauksien kannalta, on suojeltava erityisen tarkasti, koska niiden käsittelyn asiayhteys voisi aiheuttaa huomattavia riskejä perusoikeuksille ja -vapauksille. Valiokunta on tämän johdosta kiinnittänyt erityistä huomiota siihen, että arkaluonteisten tietojen käsittely on rajattava täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään ja sääntelyn on oltava tietosuoja-asetuksen mahdollistamissa puitteissa yksityiskohtaista ja kattavaa (PeVL 65/2018 vp, s. 45, PeVL 15/2018 vp, s. 40, PeVL 17/2021 s. 40-41). Ehdotettu sääntely perusteluineen ei mielestäni täytä kaikkia näitä vaatimuksia, sillä siinä ei perustella arkaluonteisten tietojen käsittelyä eikä ehdoteta suojatoimia, joilla varmistettaisiin perusoikeuksien toteutuminen.

Tietosuojasääntelyn keskeisiä periaatteita on käyttötarkoitussidonnaisuuden periaate. Perustuslakivaliokunta on korostanut erityisesti arkaluonteisten tietojen käsittelyn käyttötarkoitussidonnaisuuden vaatimusta. Tietojen käyttämiseen varsinaisen keräämis- ja tallettamistarkoituksen ulkopuolelle jääviin tarkoituksiin on perustuslakivaliokunnan mukaan ollut syytä suhtautua kielteisesti esimerkiksi laajojen biometrisiä tunnisteita sisältävien rekisterien yhteydessä (PeVL 14/2009 vp, s. 4/II). Valiokunta on pitänyt mahdollisena tehdä käyttötarkoitussidonnaisuudesta vain täsmällisiä ja vähäisiksi luonnehdittavia poikkeuksia (PeVL 40/2021 vp, kappale 15, PeVL 23/2022, kappale 18). Tällainen sääntely ei saa johtaa siihen, että muu kuin alkuperäiseen käyttötarkoitukseen liittyvä toiminta muodostuu rekisterin pääasialliseksi tai edes merkittäväksi käyttötavaksi (ks. PeVL 15/2018 vp, s. 45, PeVL 1/2018 vp, s. 4, PeVL 14/2017 vp, s. 5-6). Ehdotetulla lainsäädännöllä olisi nähdäkseni se vaikutus, että käyttötarkoitussidonnaisuuden

periaatteesta poikettaisiin. Poikkeus kohdistuisi myös arkaluonteisiin tietoihin. Hallituksen esityksessä ei ole nähdäkseni perusteltu tätä ratkaisua eikä selvitetty tämän varsin merkittävän perusoikeusrajoituksen edellytyksiä sen enempää kansallisessa valtiosääntöoikeudellisessa kuin eurooppaoikeudellisessakaan kehikossa.

Ehdotettu uusi SVPL 319 a §

Hallituksen esityksen keskiössä on lakiin sähköisen viestinnän palveluista (SVPL) ehdotettava uusi 319 a §. Siinä säänneltäisiin tietojen luovuttamisesta merkittävässä tietoturvaloukkauksessa tai -uhkassa. Esityksen mukaan tämä viranomaisten välistä tiedonvaihtoa koskeva erityissäännös täydentäisi muuta tiedonvaihtoa koskevaa sääntelyä niiltä osin, kun siihen liittyy tiedonvaihtoa koskevia rajoitteita. Ehdotuksella ei kavenneta muuta tiedonvaihtoa tai käyttöä koskevaa nykyistä lainsäädäntöä. Lähtökohta on selvä: ehdotuksella on tarkoitus yksiselitteisesti lisätä tietojen vaihtoa ja käyttöä.

Ehdotetun 319 a §:n mukaan Liikenne- ja viestintävirastolla, poliisilla, suojelupoliisilla ja Puolustusvoimilla olisi salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa toisilleen sellaisia merkittävää tietoturvaloukkausta tai sen vakavaa uhkaa koskevia välitystietoja, tietoja viesteistä tai muita tietoja, jotka ovat välttämättömiä sellaisen merkittävän tietoturvaloukkauksen tai sen vakavan uhkan selvittämiseksi, ennalta ehkäisemiseksi tai vaikutusten poistamiseksi, jolla on tai uhkaa olla vakavia haitallisia vaikutuksia seuraaviin:

1) julkisen vallan päätöksentekokokykyyn tai viranomaisten toimintaedellytyksiin;
2) kansalliseen turvallisuuteen tai maanpuolustukseen;
3) välttämättömiin sosiaali- ja terveydenhuollon tai pelastustoimen palveluihin;
4) energia-, vesi, elintarvike- tai lääkehuoltoon taikka muihin välttämättömiin hyödykkeisiin;
5) välttämättömiin maksu- ja arvopaperipalveluihin;
6) yhteiskunnan kriittisiin liikenne- ja viestintäpalveluihin;
7) 1 – 6 kohdassa tarkoitettuja toimintoja ylläpitäviin tieto- ja viestintäteknisiin palveluihin tai tietoaineistoihin.

Jotta perusoikeusrajoituksen tarkkarajaisuutta ja oikeasuhtaisuutta voisi arvioida, tulee tietää, mitä merkittävällä tietoturvaloukkauksella, tietoturvauhkalla, selvittämisellä ja vaikutusten poistamisella tarkoitetaan. Hallituksen esityksen sivuilta 42-43 käy ilmi, että tietoturvaloukkauksella tarkoitetaan *mitä tahansa toimintaa, jolla on haitallisia vaikutuksia tietoturvallisuudelle*. Tietoturvaloukkauksena pidettään tekoa tai tapahtumaa, jonka seurauksena tietojen, televiestinnän tai tietojärjestelmien tietoturvan elementit tai jokin niistä vaarantuisivat. Tietoturvaloukkaus voisi aiheuttaa esimerkiksi tietojärjestelmän tai siitä riippuvien laitteiden tai palveluiden toimimattomuutta. Merkittävällä tietoturvaloukkauksella tarkoitetaan loukkausta, josta aiheutuu enemmän kuin vähäistä haittaa taikka

lievää vahinkoa tietoturvalle. Merkittävän tietoturvaloukkauksen tulisi ennalta arvioiden katsoa voivan aiheuttaa yhteiskunnalle huomattavaa haittaa ja vahinkoa. Hallituksen esityksessä todetaan edelleen, että merkittävyyttä arvioitaessa tulisi NIS-direktiivissäkin tarkoitetulla tavalla kiinnittää huomiota vaikutusten laajuuteen ja kestoon, maantieteelliseen levinneisyyteen sekä viestintäpalvelujen käytettävyyteen, eheyteen tai viestinnän luottamuksellisuuteen. Näin ollen vaikuttaa siltä, että tilanteet, joissa tietoja voitaisiin luovuttaa, olisivat varsin laajasti ja jossain määrin epämääräisesti määritelty.

Tietoturvaloukkauksen vakava uhka tarkoittaisi esimerkiksi haavoittuvuutta. Jotta kysymys olisi merkittävän tietoturvaloukkauksen vakavasta uhkasta, uhkan toteutumisen vaikutuksien tulisi olla vakavuudeltaan merkittävää tietoturvaloukkausta vastaavia ja uhkan haitallisen hyödyntämisen tai haitallisten vaikutusten aiheutumisen todennäköisyyden muutoin suuri. Kyseeseen ei siten voisi esimerkiksi tulla sinällään merkittäväkään haavoittuvuus, jos riski sen hyväksikäytölle on pieni tai lähinnä teoreettinen. Hallituksen esityksessä todetaan, että käytännössä tämän arviointi etukäteen voi kuitenkin olla vaikeaa.

Tietoturvaloukkauksen tai -uhkan selvittämisellä tarkoitettaisiin tapahtumien kulun sekä niiden teknisten tai muiden syiden selvittämistä, joista tietoturvaloukkaus tai sen uhka on aiheutunut. Tietoturvaloukkauksen tai sen uhkan vaikutusten poistamisella tarkoitettaisiin niitä teknisiä tai muita toimia, joilla poistetaan, lievennetään tai torjutaan selvitetyn loukkauksen tai sen uhan aiheuttama vaara tai muu vaikutus tietoturvallisuudelle tai muulle viestinnän luottamuksellisuudelle. Vaikutuksien poistamisella tarkoitetaan erityisesti toimia, joilla varmistetaan, ettei tietoturvaloukkauksesta tai sen uhkasta aiheudu haittaa tietoturvalle. Vaikutusten poistamisen osalta on kuitenkin huomioitava, että useassa tilanteessa vastuu vaikutusten poistamisesta on hyökkäyksen kohteeksi joutuneella toimijalla itsellään tai tämän palveluntarjoajalla. Viranomaiset voivat toiminnallaan tukea kohdeorganisaatioita vaikutusten poistamiseen liittyvissä toimenpiteissä, kuten selvittämällä hyökkäysten taustoja ja teknisiä seikkoja ja sitä kautta tukea eri toimijoita vaikutusten poistamisella. Tietoa voidaan tällaisessa tilanteessa käyttää siten vaikutusten poistamiseksi, vaikka viranomainen ei itse poista vaikutuksia.

Tietoja vaihtavat viranomaiset

Ehdotetun 319 a §:n 1 momentin mukaan tietoa voisivat vaihtaa keskenään Liikenne- ja viestintävirasto, poliisi, suojelupoliisi ja Puolustusvoimat. Tiedonvaihtoa olisi mahdollisuus tehdä vastavuoroisesti sekä oma-aloitteisesti että pyynnöstä kyseisten viranomaisten välillä jokaisen viranomaisen tietoturvaloukkauksiin liittyvien lakisääteisten tehtävien hoitamiseksi ja tilanteen mahdollisimman sujuvan koordinoinnin ja toiminnan yhteensovittamisen mahdollistamiseksi.

Pykälän nojalla vaihdettava tieto voisi olla peräisin mistä tahansa mainittujen viranomaisten toiminnasta saadusta tiedosta, jonka vaihtaminen tilanteessa on välttämätöntä. Liikenne- ja viestintäviraston osalta tämä voisi olla esimerkiksi sille tehtyjen ilmoitusten perusteella tulleesta tiedosta tai verkkojen havainnointipalvelusta saaduista tiedoista. Poliisin osalta kyse voisi olla sille tehtyjen rikosilmoitusten tai telepakkokeinojen kautta saadusta tiedosta. Suojelupoliisin tai Puolustusvoimien osalta tieto voisi olla esimerkiksi omilla toimivaltuuksillaan saadusta tiedosta. Tiedot olisivat luonteeltaan paitsi henkilötietoja, myös arkaluonteisia.

Näkisin, että tietojen luovuttaminen näin monien, toimivaltuuksiltaan erilaisten viranomaisten kesken edellyttää perusteellista perusoikeuspunnintaa. Kukin luetelluista viranomaisista kerää henkilötietoja hyvin erilaisin perustein hyvin erilaisiin tarkoituksiin ja hyvin erilaisten lakisääteisten rajoitusten nojalla. Tällaisten erittelemättömien tietomassojen laajamittainen vaihto, käyttö ja säilytys on selkeästi tietosuojasääntelyn ja ePrivacy-direktiivin hengen vastaista. Erityisesti olisikin pohdittava sitä, miten eri sektorilainsäädännöissä, kuten vaikkapa pakkokeinolaissa, vaaditut perusoikeuksien suojamekanismit tulisivat sovellettaviksi silloin, kun tietoja liikuteltaisiin ehdotetun 319 a §:n nojalla.

Perustuslakivaliokunta on painottanut, että tiedonhankinta voidaan osoittaa vain kansallisesta turvallisuudesta huolehtivien viranomaisten (nykyisin suojelupoliisi, pääesikunta ja puolustusvoimien tiedustelulaitos) tehtäväksi. Valiokunta on korostanut myös sitä, että lailla tulee säätää tyhjentävästi toimivaltuuksien kohdentumisesta. Valiokunta on todennut, että uusi perustuslain sääntely ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa. Sääntelyn välttämättömyyskriteeri puolestaan tarkoittaa, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman *kohdennetusti ja rajoitetusti*. Valiokunta on korostanut perusoikeuksien yleisten rajoitusedellytysten merkitystä uutta Pl 10 §:n rajoitusperustetta tulkittaessa. Valiokunta on tähdentänyt, että kansallisen turvallisuuden käsitettä tulee tulkita suppeasti ja asettaa säännöksessä mainittu uhan vakavuusaste korkealle (PeVM 4/2018 vp, s. 8-9, PeVL 35/2018 vp, s. 4). Nyt tarkasteltavan ehdotuksen kohdalla valiokunnan olisi nähdäkseni pohdittava, täyttääkö laaja ehdotettu tietojenvaihto näitä valiokunnan asettamia edellytyksiä.

Hallituksen esityksessä todetaan vain, että tietoja voitaisiin luovuttaa viranomaisten välillä salassapitosäännösten estämättä. Tämä koskisi ensinnäkin julkisuuslain nojalla salassa pidettävää tietoa, johon poliisin, suojelupoliisin ja Puolustusvoimien salassapitosääntely pääasiassa nojaa. Lisäksi tämä tarkoittaisi poikkeamista SVPL 136 §:ssä säädettyä viestin ja välitystietojen luottamuksellisuutta sekä 319 §:n 1 momentissa säädettyä velvollisuutta pitää salassa 316, 316 a ja 317 §:n nojalla hankitut tiedot viestistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta. Säännöksellä voitaisiin poiketa myös SVPL 318 §:n 6 momentissa tarkoitetusta ulkomaiselta viranomaiselta saadusta tiedosta huomioiden kuitenkin

ehdotetun 3 momentin rajoitukset. Suojelupoliisin ja Puolustusvoimien osalta tämä voisi liittyä rikosepäilystä ilmoittamiseen liittyviin rajoituksiin, jonka osalta on erikseen säädetty rikosten vakavuutta koskevat kriteerit niistä tilanteista, joissa tietoa on luovutettava rikostorjuntaan. Tästä on säädetty sotilastiedustelulain 79 §:ssä ja poliisilain 5 a luvun 44 §:ssä. Tältä osin hallituksen esityksessä todetaan ylimalkaan, että käytännössä ehdotuksessa tarkoitetuissa tilanteissa teot olisivat erittäin todennäköisesti niin vakavia, että kyseiset rikosten vakavuutta koskevat kriteerit täyttyvät joka tapauksessa.

Poliisin osalta kysymys voisi olla myös salaisilla pakkokeinoilla hankitun tiedon luovuttamisesta. Tieto voisi olla hankittu esimerkiksi suunnitelmallisella tarkkailulla, televalvonnalla, telekuuntelulla tai teknisellä laitetarkkailulla, mutta huomioiden tiedonhankinnan tarpeet eri tilanteissa kysymys voisi myös muista pakkokeinolain 10 luvun tai PolL 5 luvun mukaista tiedonhankintakeinoista. Säännös tarkoittaisi myös poikkeamista pakkokeinolain 55 § ja 56 § ylimääräisen tiedon käytölle asetetuista rajoituksista. Huomionarvoista ylimääräisen tiedon osalta on, että voimassa olevan pakkokeinolain nojalla ylimääräistä tietoa saa käyttää myös hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi. Hallituksen esityksessä todetaan tältäkin osin jossain määrin epämääräisesti, että käytännössä ehdotuksessa tarkoitetuissa tilanteissa teot olisivat erittäin todennäköisesti niin vakavia, että kyseiset rikosten vakavuutta koskevat kriteerit täyttyvät joka tapauksessa ja kyse voisi olla myös edellä kuvatun merkittävän vaaran tai vahingon estämisestä. Näin saattaa olla, mutta ehdotettu lainsäädäntö mahdollistaisi ilmeisesti tietojen vaihtamisen myös silloin, kun teot eivät olisi niin vakavia, että kyseisten rikosten vakavuutta koskevat kriteerit täyttyvät.

Näkisin, etteivät nämä hallituksen esityksen perustelut riitä oikeuttamaan poikkeamista pakkokeinolain ynnä muiden lakien asettamista rajoituksista. Perusoikeussuojaa kokonaisuutena arvioiden olisi huomattavan ongelmallista, jos esimerkiksi pakkokeinolain oikeussuojakeinot sekä muut tietojen keräämisen ja käytön rajoitukset vesittyisivät siinä vaiheessa, kun tietoja luovutetaan viranomaisilta toisille.

Hallituksen esityksessä ei, kuten sanottu, perustella arkaluonteisten tietojen käsittelyä erikseen. Siinä todetaan kyllä, että erityislainsäädäntöön sisältyy myös esimerkiksi biometrisiin tietoihin liittyviä tiedon luovuttamista koskevia rajoituksia. Esityksessä on kuitenkin päädytty siihen, että ne eivät kuitenkaan ole merkityksellisiä tietoturvaloukkausten selvittämisen näkökulmasta. Näin saattaa olla, mutta jos arkaluonteisia tietoja kerätään, käsitellään, luovutetaan ja käsitellään uudelleen, tulisi siitä säätää lailla kotimaisten valtiosäännöstä johtuvien sekä EU-oikeudesta ja kansainvälisistä ihmisoikeusvelvoitteista johtuvien velvoitteiden rajoissa. Tältä osin ehdotuksessa on sivuutettu mielestäni varsin merkittävä asia.

Tietojen käyttäminen

Hallituksen esityksestä saa sen kuvan, että vaikka tietoja luovutettaisiinkin esitettyjen pykälien perusteella vain tiettyihin tarkoituksiin, antaa se kuitenkin mahdollisuuden viranomaisille käsitellä tietoja myös muihin tarkoituksiin. Näin ollen tarkkarajaisuus nousee huomattavan kyseenalaiseksi. Esityksessä todetaan muun muassa, että poliisin rikostorjuntatehtävistä johtuen poliisi käyttäisi ehdotetun uuden 319 a §:n nojalla saatua tietoa *sen yleisten tehtävien, kuten oikeus- ja yhteiskuntarauhan turvaamiseksi, kansallisen turvallisuuden suojaamiseksi, yleisen järjestyksen ja turvallisuuden ylläpitämiseksi sekä rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi*. Poliisi käyttäisi tietoa esimerkiksi salaisten tiedonhankintakeinojen kohdistamiseksi. Lisäksi se saamansa tiedon avulla tutkisi tietoverkkorikoksia ja pitäisi niistä yllä kansallista kyberrikollisuuden tilannekuvaa. Näin ollen on ilmiselvää, ettei tietoja luovutettaisi viranomaisten välillä vain tiettyihin, ennalta tarkasti määriteltyihin tarkoituksiin. Käytännössä säännös vaikuttaa lähes blanco-sääntelyltä, joka antaisi poliisille jos jonkinmoisia mahdollisuuksia hyödyntää muiden viranomaisten muihin tarkoituksiin keräämiä henkilötietoja, mukaan lukien arkaluonteisia sellaisia. On vaikea nähdä, että tämä sääntelyratkaisu olisi perustuslakivaliokunnan näkemysten, EU-oikeuden keskeisten sääntöjen tai EIT:n käytännön kanssa sopusoinnussa.

Ehdotettu tietojen luovuttamistoiminta ei tarkoittaisi pelkästään sitä, että poliisi saisi käyttää tietoja lähes mihin tahansa. Samaa todetaan sekä suojelupoliisista että Puolustusvoimista. Nekin saisivat käyttää tietoja hyvin laajasti erilaisten tehtäviensä suorittamiseen. Mitään tarkkoja rajoja tietojen käytölle ei siis asettaisi. Myös Liikenne- ja viestintävirasto saisi käyttää tietoja muun muassa tietoturvaloukkausten tai uhkien tekniseen selvittämiseen ja kyberturvallisuuden kansallisen tilannekuvan laatimiseen.

Näkisin, että ehdotettu 319 a § rajoittaa kyllä jossain määrin sitä, missä tilanteissa viranomaiset voisivat luovuttaa niillä olevia tietoja toisille viranomaisille. Sen sijaan ehdotus ei rajoita sitä, mitä kaikkea tiedot vastaanottava viranomainen voisi tiedoilla tehdä.

Tietojen säilyttäminen ja poistaminen

Ehdotettuun SVPL 319 a §:ään sisältyy määräyksiä siitä, että tarpeeton tieto on poistettava. En ole aivan varma, onko tarpeettoman tiedon määrittely tässä yhteydessä niin tarkka, että soveltavat viranomaiset kykenisivät sitä mutkitta soveltaa. Ehdotuksen 2 momentin mukaan tietoturvaloukkausten ennalta ehkäisemisen, selvittämisen tai vaikutusten poistamisen kannalta tarpeeton tieto on poistettava. Koska tietoturvaloukkausten ja niiden ehkäisemisen, selvittämisen ja vaikutusten poistaminen on määritelty niin laajasti, ei liene milloinkaan mahdollista poistaa paljoakaan, sillä lähes mikä tahansa tieto voisi hallituksen esityksen perustelujen mukaan olla tarpeen kenties joskus.

Tiedon hävittämiseen sovellettaisiin mitä 316 §:n 4 momentissa säädetään tietojen hävittämisestä. Kyseisessä lainkohdassa määritellään, että tiedot viesteistä, välitystiedoista ja sijaintitiedoista on hävitettävä, kun ne eivät enää ole tarpeen tässä pykälässä tarkoitettujen tehtävien hoitamiseksi tai niitä koskevan rikosasian käsittelemiseksi. Tiedot viesteistä, välitystiedoista ja sijaintitiedoista on hävitettävä viimeistään kahden vuoden tai, jos on kysymys tietoturvaloukkausten selvittämistä koskevista tiedoista, viimeistään kymmenen vuoden kuluttua sen kalenterivuoden päättymisestä, jonka aikana tiedot saatiin tai rikosasiaa koskeva päätös taikka tuomio sai lainvoiman. Siten voidaan todeta, että tietojen säilyttämisaika on varsin pitkä.

Perusoikeuksien rajoittamisen perustelut

Hallituksen esityksessä perustellaan perusoikeuksien rajaamista muun muassa niin, että ehdotuksen nojalla on tarkoitus mahdollistaa välistystietojen ja viestin sisältöä koskevien tietojen, mutta myös muiden välttämättömien tietojen luovuttaminen viranomaisten välillä tietoturvaloukkauksen tai sen vakavan uhkan tilanteessa. Viestinnän luottamuksellisuuden ja yksityiselämän suojan kannalta ehdotukseen on esityksen mukaan tehty useita rajauksia. Soveltaminen olisi mahdollista vain, jos kyseessä olisi yhteiskunnan keskeisiin toimintoihin kohdistuvien vaikutusten näkökulmasta erityisen merkittävä tietoturvaloukkaus, joka käytännössä aina täyttäisi vähintään jonkin SVPL 316 §:n 2 momentissa luetellun tietoturvaan liittyvän rikoksen tunnusmerkistön.

Perustuslakivaliokunnan pohdittavaksi jää, onko tämä määritelmä tarpeeksi suppea ja tarkkarajainen. Huomioon olisi syytä ottaa se, että SVPL 316 §:n 2 momenttiin sisältyy monenlaisia rikoksia, kuten vaikkapa rikoslain 28 luvun 7 §:ssä tarkoitettu luvaton käyttö, joka ei ole erityisen törkeä rikos, ja jonka rangaistusasteikko lähtee sakosta ja päättyy yhteen vuoteen vankeutta. Entä tulisivatko tietojen luovuttamisen mahdollisuudet käyttöön myös silloin, kun epäiltäisiin SVPL 349 §:n mukaista sähköisen viestinnän tietosuojarikkomusta, josta voidaan tuomita vain sakkoa? Hallituksen esityksen mukaan se lienee mahdollista, jos mittariksi otetaan SVPL 316 §:n 2 momentti. Siten ei vaikuta siltä, että viranomaisten tietojensaanti olisi rajattu vain vakavaan rikollisuuteen, kuten EUT:n oikeuskäytäntö edellyttäisi.

Erityisen avointa ehdotettu sääntely on nähdäkseni tietoturvaloukkauksen uhan kohdalla. Tällöin kyse lienee preventiivisestä menettelystä, jolloin rikosepäily ei ole vielä aktualisoitunut. Perustuslakivaliokunnan on nähdäkseni pohdittava tätä kysymystä perustuslain 8 §:ssä säädetyn rikosoikeudellisen laillisuusperiaatteen kehikossa.

Perustuslakivaliokunta on painottanut, että erottelussa tietojen saamisen tai luovuttamisen tarpeellisuuden ja välttämättömyyden välillä on kyse tietosisältöjen laajuuden ohella myös siitä, että salassapitosäännösten edelle menevässä tietojen luovutuksessa tietojen vaihtoa perustelevat intressit

syrjäyttävät ne perusteet ja intressit, joita salassapidon avulla suojataan. Mitä yleisluonteisempi tietojensaantiin oikeuttava sääntely on, sitä suurempi on vaara, että tällaiset intressit voivat syrjäytyä hyvin automaattisesti. Tietojen luovuttaminen tulisi valiokunnan käsityksen mukaan sitoa välttämättömyysedellytykseen (PeVL 35/2018 vp, s. 26).

Välttämättömyys on ollut ohjenuorana myös unionin tuomioistuimen oikeuskäytännössä. Toimivaltaisten viranomaisten tiedonsaantioikeus on rajattu täysin välttämättömään muun muassa ratkaisuissa Tele2 Sverige ja Watson ym., C-203/15 ja C-698/15, Ministerio Fiscal, C-207/16, ja Prokuratuur, C-746/18. Viimeksi mainitussa ratkaisussa, joka annettiin vuonna 2021, tuomioistuin edellytti myös, että välitys- ja sijaintitietojen kohdalla lainvalvontaviranomaisten tietojensaanti on rajattava vakavaan rikollisuuteen myös niissä tapauksissa, kun tietojensaanti koskee vain vähäisä tietomääriä (kohta 45). Tuomioistuin totesi, että tietojensaannin rajoittaminen on välttämätöntä myös yleisessä tietosuoja-asetuksessa kodifioidun käyttötarkoitussidonnaisuuden periaatteen kannalta (kohta 31).

Nyt tarkasteltavalla ehdotuksella pyritään suojaamaan yhteiskunnan toimintakykyä ja kriittisiä toimintoja vakavilta tietoturvaloukkauksilta, joilla voi pahimmillaan olla vakavia vaikutuksia yhteiskunnalle. Hallituksen esityksessä todetaan, että yhteiskunnan turvallisuuden kannalta intressit näissä yksittäisissä tilanteissa ylittäisivät ne salassapitoa koskevat intressit, joita salassapitosäännöksillä suojataan. Lisäksi tietoturvaloukkauksien toteutuessa täysimääräisesti on mahdollista, että luottamuksellisen viestin suojaan kohdistuvat vaikutukset olisivat mittaluokaltaan huomattavasti haitallisemmat ja useampaa henkilöä koskevat kuin yksittäisessä tapauksessa viranomaisten välillä tapahtuva tiedon vaihtaminen. Näin voi olla esimerkiksi laajojen tietomurtojen yhteydessä. Hallituksen esityksen perustelut ovat vakuuttavat ja sääntelylle on varmasti olemassa oikea tarve. Epäilen kuitenkin, täyttävätkö ehdotukset kaikilta osin tarkkarajaisuuden, täsmällisyyden, suhteellisuuden ja välttämättömyyden vaatimuksia erityisesti ottaen huomioon, että kyseessä olisi mittava perusoikeuksien rajoitus.

Sääntelyn selkeys

Hallituksen esityksen perusteluissa todetaan monissa kohdin, että ehdotettu sääntely on tarpeen epäselvän oikeustilan selkeyttämiseksi ja nykyisten tulkintavaikeuksien vähentämiseksi. Katsoisin, että ehdotus ei kaikilta osin saavuta tätä tavoitetta. Osin syynä on se, että sääntelyala on valtavan laaja ja se kietoutuu monin tavoin myös voimassa olevaan ja valmisteltavaan EU-sääntelyyn sekä eurooppalaiseen perusoikeussääntelyyn. Toisaalta voidaan todeta, että pelkästään kotimainen sääntelykehikko on jo itsessään varsin sekava ja monitulkintainen, eikä ole varmaa, että nyt ehdotetuilla pykälillä saataisiin tähän apua.

Esimerkiksi ehdotettu SVPL 309 § virka-avusta on vaikea tulkita yhdessä samaisen lain 319 §:n kanssa, joka koskee tietojen luovuttamista. Konkreettiseksi esimerkiksi voidaan nostaa 309 §:n 4 momentti, jonka mukaan virka-avun antaminen *ei oikeuta* Liikenne- ja viestintävirastoa antamaan toiselle viranomaiselle tietoja viesteistä, välitystiedoista tai sijaintitiedoista taikka luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta. Silti 319 §:n mukaan Liikenne- ja viestintävirastolla on säädetyn salassapitovelvollisuuden tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja muun muassa viestinnän välittäjälle, yhteisölle, tilaajalle ja käyttäjälle sekä muissa valtioissa toimiville viranomaisille ynnä muille. Salassapito ei myöskään kyseisen pykälän kuudennen momentin mukaan estä välitystiedon antamista toiselle viranomaiselle, jos se on tarpeen radiohäiriön aiheuttamista koskevan rikoksen selvittämistä tai syytteeseen panoa varten taikka radioviestinnän häiriön poistamiseksi tai rajoittamiseksi. Saman lain 319 a § antaisi lisäksi mahdollisuuden Liikenne- ja viestintävirastolle luovuttaa tietoja, jos jonkinmoisille tahoille. SVPL on kokonaisuudessaan melko monimutkainen laki, eikä nyt ehdotetuilla muutoksilla nähdäkseni tule tähän pulmaan apua.

Oikeusturvatakeet

On ilmeistä, että ehdotetut uudet tietojen vaihtoa edistävät säännökset kaventavat PL 10 §:ssä suojattuja oikeuksia. Näkisin, että tässä yhteydessä yksilöiden oikeuksille tietää heidän omien tietojensa liikuttelusta ja luovutuksista tulisi kiinnittää huomiota. Lisäksi näkisin, että sääntelyn ollessa läheisessä yhteydessä rikosten selvittämiseen ja ennaltaehkäisyyn, olisi tarpeen pohtia myös mahdollisten epäiltyjen oikeusturvakeinoja. Näihin seikkoihin hallituksen esityksessä ei mielestäni oteta tarpeeksi selkeää kantaa.

On huomattava, että perustuslakivaliokunta on tiedustelulakeihin liittyvän perustuslain 10 §:n muutoksen säätämisen yhteydessä esittänyt keskeisiä perusteita, jotka on otettava huomioon arvioitaessa luottamuksellisen viestin salaisuuden rajoittamisen perusteena olevan perustuslain 10 §:n 4 momentissa tarkoitettua sotilaallista toimintaa tai muuta kansallista turvallisuutta vakavasti uhkaavaa toimintaa. Se on korostanut vahvoja oikeusturvatakeita, laaja-alaista ja tehokasta tiedusteluvaltuuksien käytön valvontaa sekä riittäviä soveltamisrajoituksia. Kyse on poikkeuksellisesta rajoitusperusteesta, jossa on irtauduttu rikosperusteisesta toiminnasta ja joka tulee siten sovellettavaksi tilanteissa, joissa ei tiedonhankintavaiheessa tai muutoinkaan voida kohdistaa konkreettista ja yksilöityä rikosepäilyä (PeVM 4/2018 vp, s. 8).

Nyt ehdotettujen lakimuutosten kontekstissa voi olla sellaisia tilanteita, joissa tietojen saamiseksi tiedusteluviranomainen hakisi muussa tilanteessa luvan tuomioistuimelta. Liikenne- ja viestintäviraston tehtävästä johtuen sillä on pääsy tai joissain tilanteissa hallussaankin sellaisia tietoja, joihin tiedusteluviranomaisilla, eikä myöskään rikostorjuntaviranomaisilla ole suoraan pääsyä ilman

tuomioistuimen myöntämää lupaa. Ehdotus tarkoittaisi nähdäkseni siis käytännössä sitä, että tuomioistuimen ennakollinen lupa ohitettaisiin monissa tulevissa tilanteissa.

Hallituksen esityksessä tätä sääntelyratkaisua perustellaan sillä, että ehdotuksessa olisi kokonaisuudessaan kyse rajatuista ja laissa määritellyistä tapauksista, eikä sääntelystä sen perusteella muodosta merkittävää poikkeusta tiedustelulle säädetyille periaatteille. Tiedon käyttötarkoitusta on pyritty tarkoin rajaamaan siten, että sitä voitaisiin käyttää vain tietoturvaloukkausten selvittämiseen, ennalta ehkäisemiseen ja vaikutusten poistamiseen. Kuten yllä on käynyt ilmi, nämä hallituksen esityksessä mainitut käyttötarkoitukset ovat laaja, epämääräinen joukko, joka ei vastanne perustuslakivaliokunnan vakiintuneita kantoja. Nähdäkseni hallituksen esityksessä useaan otteeseen painotettu näkemys siitä, että ehdotuksissa on kyse kokonaisuudessaan rajatuista ja laissa määritellyistä tapauksista on harhaanjohtava. Siten on vaikea nähdä perusteltuna sitä, että tuomioistuinten etukäteisvalvonta ohitettaisiin tällä lainsäädäntöratkaisulla. Eurooppalaisen perusoikeussääntelyn nykytulkintojen valossa se ei myöskään ole helposti perusteltavissa.

Kansainvälinen yhteistyö, mukaan lukien NATO

Hallituksen esitykseen sisältyy ehdotus SVPL 319 §:n muotoiluksi siten, että Liikenne- ja viestintävirastolla olisi salassapitovelvollisuuden tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja muussa valtiossa toimivalle viranomaiselle tai muulle vastaavalle taholle taikka Euroopan unionin tai Pohjois-Atlantin liiton sellaiselle toimielimelle, elimelle tai virastolle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturva-loukkauksia.

Säännöksen muotoilusta saa sen kuvan, että henkilötietoja voitaisiin salassapitosäännösten estämättä luovuttaa mahdollisesti melko paljonkin muiden maiden viranomaisille. Näitä maita olisivat myös kolmannet maat. Tietosuojasääntely, erityisesti unionin yleinen tietosuoja-asetus suhtautuu erittäin pidättyvästi tietojen luovutuksiin EU:n ulkopuolelle. Nähdäkseni tässä olisi syytä vielä miettiä, onko hallituksen esitys sopusoinnussa unionin lainsäädännön kanssa ottaen huomioon erityisesti EUT:n merkittävät Schrems-ratkaisut (C-311/18 ja C-362/14).

Mitä Nato-yhteistyöhön tulee, on perustuslakivaliokunta uuden edessä. On nähtävissä, että tietosuojasääntelyn ja Nato-yhteistyön yhteensovittamisessa on vielä monta mutkaa matkassa, ja yksi niistä on valiokunnan tarkasteltavana tämän hallituksen esityksen myötä.

Yhteenveto

Ehdotuksella pyritään siihen, että tietoa voidaan vaihtaa kunkin viranomaisen tehtävän hoitamiseksi. Ehdotuksella on hyväksyttäviä tavoitteita. Sillä pyritään edistämään turvallisuutta. Esityksellä olisi kuitenkin merkittäviä vaikutuksia PL 10 §:ssä ja eurooppaoikeudessa suojattuihin yksityisyysoikeuksiin. Tässä yhteydessä perusoikeuksien rajoittamisen tulisi täyttää ePrivacy-direktiivistä johdetut vaatimukset välttämättömyydestä, asianmukaisuudesta ja oikeasuhteisuudesta.

Lisäksi sen tulisi täyttää perustuslakivaliokunnan asettamat vaatimukset, joihin sisältyy niin ikään välttämättömyys, mutta myös muun muassa täsmällisyys ja tarkkarajaisuus. On syytä korostaa, että perustuslakivaliokunta on painottanut, että tiedonhankinta voidaan osoittaa vain kansallisesta turvallisuudesta huolehtivien viranomaisten (suojelupoliisi, pääesikunta ja puolustusvoimien tiedustelulaitos) tehtäväksi. Lisäksi lailla tulee säätää tyhjentävästi toimivaltuuksien kohdentumisesta. Sääntelyn välttämättömyyskriteeri puolestaan tarkoittaa, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti.

Perustuslakivaliokunta tarkastellee ehdotusta näiden edellytysten valossa. Oma näkemykseni on, että hallituksen esitys ei tässä muodossaan täytä täsmällisyyden ja tarkkarajaisuuden edellytyksiä. On myös epävarmaa, olisiko ehdotettu tietojen vaihto tarpeeksi kohdennettua ja rajoitettua ottaen huomion erityisesti sen, että vaihdettavien tietojen luonnetta ei ole määritelty tai rajattu lainkaan sekä sen, että viranomaisille sallittaisin niiden saamien tietojen käyttö hyvin monenlaisiin tarkoituksiin.

Helsingissä 15.12.2022
Susanna Lindroos-Hovinheimo