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

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Hallituksen esityksessä ehdotetaan muutettavaksi sähköisen viestinnän palveluista annettua lakia, henkilötietojen käsittelystä Puolustusvoimissa annettua lakia ja henkilötietojen käsittelystä poliisitoimessa annettua lakia. Lakeihin ehdotetaan muutoksia, jotka mahdollistaisivat sujuvamman viranomaisten välisen tiedonvaihdon yhteiskunnan elintärkeiden toimintojen kannalta merkittävissä tietoturvaloukkaustilanteissa ja niiden uhkissa. Ehdotuksessa Puolustusvoimien ja poliisin Liikenne- ja viestintävirastolle antamaa virka-apua ehdotetaan laajennettavaksi koskemaan merkittäviä tietoturvaloukkauksia ja -uhkia. Lisäksi ehdotetaan säädettäväksi viestinnän välittäjän oikeudesta oma-aloitteisesti luovuttaa Liikenne- ja viestintävirastolle tietoja viesteistä ja välitystiedoista tietoturvaloukkausten selvittämiseksi tai ennaltaehkäisemiseksi.

Lait on tarkoitettu tulemaan voimaan 1.2.2023.

_____

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Hallituksen esityksen taustalla on 10.6.2021 annettu valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla. Periaatepäätöksessä on lueteltu 37 toimenpidettä, joiden tavoitteena on parantaa tietosuojan ja tietoturvan tasoa ja tunnistaa turvallisuuskokonaisuuden merkitys palveluiden laadulle ja turvallisuudelle digitaalisessa yhteiskunnassa. Periaatepäätöksen ensimmäisenä toimenpiteenä on luoda yhtenäinen säädöspohja viranomaisten yhteistyölle tietoturvaloukkaustilanteissa, jonka seurausta ehdotus on. Tarkoituksena oli arvioida lisäksi viranomaisten välistä tiedonvaihtoa sekä virka-apusäännöksiä ja arvioida nykyisten melko toimivaksi todettujen yhteistyömenetelmien vahvistamista ja yhteistyötä yksityisen sektorin kanssa. Toimenpide toteuttaa periaatepäätöksen poliittista linjausta siitä, että viranomaiset toimivat yhdessä ja Liikenne- ja viestintäviraston Kyberturvallisuuskeskus tukee ja vahvistaa yhteistoimintaa. Esitys toteuttaa hallitusohjelman kirjausta turvallisesta oikeusvaltiosta ja turvallisuusviranomaisten toimintakyvyn varmistamisesta.

Lisäksi esityksellä vastataan muuttuneeseen turvallisuusympäristöön ja sen heijastumiseen kyberympäristössä. Kyberympäristön uhat ovat monimutkaistuneet ja lisääntyneet erityisesti yhteiskunnan eri sektoreiden digitalisaatiosta johtuen. Kuten turvallisuusympäristön muutoksesta annetussa ajankohtaisselonteossa (VNS 1/2022 vp) todetaan, uhkien tehokkaan torjunnan vahvistamiseksi tiivistetään entisestään siviili- ja sotilasviranomaisten yhteistyötä ja tiedonvaihtoa. Oikea-aikaista, kattavaa ja jaettua tilannekuvaa tarvitaan kyberuhkien ennakoimiseksi ja kyberpoikkeamien havaitsemiseksi mahdollisimman aikaisessa vaiheessa. Ne ovat edellytys hyökkäyksen pysäyttämiseksi ja sen vaikutusten rajaamiseksi.

Ehdotus on osa laajempaa kyberturvallisuuden kehittämiseen tähtäävää kokonaisuutta, jolla on tarkoitus kattaa sellaiset välittömät puutteet lainsäädännössä, jotka voidaan katsoa välttämättömiksi viranomaisten yhteistoiminnan mahdollistamiseksi yhteiskunnan toiminnan kannalta merkittävän tietoturvaloukkauksen selvittämisessä. Tietoturvaloukkaustilanteisiin liittyy myös laajempia, esimerkiksi viranomaisten tehtäväkenttiin tai laajamittaisen tilanneymmärryksen muodostamiseen liittyviä kysymyksiä, jotka osaltaan vaativat laajamittaisempaa selvittämistä ja joihin etsitään ratkaisuja sisäministeriön ja puolustusministeriön käynnissä olevassa selvityshankkeessa viranomaisten toimintaedellytyksistä kyberturvallisuudessa. Hankkeen tiedot löytyvät valtioneuvoston hankeikkunasta tunnuksella PLM003:00/2022.

1.2 Valmistelu

Hallituksen esitys on valmisteltu työryhmässä, jossa ovat olleet edustettuina liikenne- ja viestintäministeriö, sisäministeriö, puolustusministeriö, ulkoministeriö, valtiovarainministeriö ja valtion kyberturvallisuusjohtaja. Työryhmää koskevat tiedot löytyvät valtioneuvoston hankeikkunasta tunnuksella LVM71:00/2021. Työryhmä on tehnyt työnsä hallituksen esityksen muotoon. Työryhmän toimikausi oli 1.2.2022 – 31.3.2023.

Työryhmä on kuullut työnsä aikana hankkeen kannalta keskeisiä viranomaisia, kuten Liikenne- ja viestintäviraston Kyberturvallisuuskeskusta, poliisia, suojelupoliisia, Puolustusvoimia, Valtion tieto- ja viestintätekniikkakeskus Valtoria, sekä EU:n verkko- ja tietoturvadirektiivissä (EU) 2016/1148, jäljempänä *NIS-direktiivi*, määriteltyjä kriittisten toimialojen kansallisia valvontaviranomaisia eli niin kutsuttuja NIS-viranomaisia.

Ehdotus on käynyt arvioitavan lainsäädännön arviointineuvostossa ja oikeuskanslerinviraston ennakkotarkastuksessa.

2 Nykytila ja sen arviointi

2.1 Keskeisten viranomaisten tehtävät tietoturvaloukkausten selvittämisessä

Kyberturvallisuuteen ja tietoturvaloukkausten ja -uhkien selvittämiseen liittyvät viranomaisvastuut on Suomessa hajautettu eri viranomaisten kesken. Jokaisella viranomaisella on oma roolinsa kyberympäristössä tapahtuvien häiriöiden selvittämisessä ja yhteistyötä näiden viranomaisten välillä tehdään jatkuvasti vakiintuneilla toimintatavoilla. Yhteistyön toteuttamisen kannalta on tärkeää, että tietoa voidaan vaihtaa riittävässä laajuudessa kunkin viranomaisen tehtävän hoitamiseksi. Tiedonvaihdon sujuvuus korostuu erityisesti vakavissa tietoturvaloukkaustilanteissa, joissa viranomaisten on toimittava nopeasti loukkauksen selvittämiseksi ja vahinkojen minimoimiseksi. Yhteistyötä tehdään tiiviisti myös yksityisen sektorin toimijoiden, kuten teleyritysten ja tietoturva-ammattilaisten kanssa, joilla on suuri merkitys erityisesti vaikutusten poistamisessa.

2.1.1 Liikenne- ja viestintävirasto

Liikenne- ja viestintäviraston yleisistä tehtävistä säädetään Liikenne- ja viestintävirastosta annetun lain (935/2018) 2 §:ssä. Liikenne- ja viestintäviraston tehtävänä on muun muassa edistää liikenteen ja viestinnän turvallisuutta sekä alan teknistä kehitystä ja häiriöttömyyttä sekä huolehtia liikenteen ja sähköisen viestinnän sääntely-, lupa-, hyväksyntä-, rekisteri- ja valvontatehtävistä. Lisäksi viraston tehtävänä on huolehtia oman toimintansa varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin, edistää ja valvoa sähköisen viestinnän toimintavarmuutta sekä tukea toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin.

Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tehtävistä säädetään Liikenne- ja viestintävirastosta annetun lain 3 §:ssä. Kyberturvallisuuskeskuksen tehtävänä on tukea, ohjata ja valvoa tietoturvallisuutta ja yksityisuuden suojan toteutumista sähköisessä viestinnässä, ylläpitää kansallisen kyberturvallisuuden tilannekuvaa ja sen toimintaa sekä edistää ja varmistaa tietojärjestelmien ja tietoliikennejärjestelyiden tietoturvallisuutta. Kyberturvallisuuskeskus huolehtii viestintätoimialan varautumisesta normaaliolojen häiriötilanteisiin ja poikkeusoloihin, edistää ja valvoo sähköisen viestinnän toimintavarmuutta sekä tukee toimialallaan yhteiskunnan yleistä varautumista normaaliolojen häiriötilanteisiin ja poikkeusoloihin. Kyberturvallisuuskeskus toimii kansallisena NIS-koordinaatiopisteenä eri viranomaisten välillä.

Liikenne- ja viestintäviraston erityisistä tehtävistä säädetään sähköisen viestinnän palveluista annetun lain (917/2014, jäljempänä *SVPL*) 304 §:ssä. Säännöksen 1 momentin 1, 7, 9 ja 10 kohtien nojalla Liikenne- ja viestintäviraston tehtävänä on edistää sähköisen viestinnän toimivuutta, häiriöttömyyttä ja turvallisuutta sekä kerätä tietoa verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriötilanteista. Erityisenä tehtävänä on lisäksi tiedottaa tietoturva-asioista sekä viestintäverkkojen ja viestintäpalvelujen toimivuudesta sekä selvittää radioviestinnän häiriön sekä radiolaitteen tai telepäätelaitteen viestintäverkolle, radiolaitteelle, telepäätelaitteelle tai sähkölaitteistolle aiheuttaman häiriön syitä. Lisäksi Liikenne- ja viestintäviraston tehtävänä on selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

2.1.2 Poliisi

Poliisin tehtävänä on poliisilain (872/2011) 1 luvun 1 §:n mukaan oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi tehtävänä on suorittaa myös muut sille laissa erikseen säädetyt tehtävät sekä antaa jokaiselle tehtäväpiiriinsä kuuluvaa apua. Poliisi tutkii tietoverkkorikoksia ja saamansa tiedon avulla pyrkii myös estämään ennalta mahdollisia tulevia rikoksia. Poliisi ylläpitää tietoverkkorikosten kansallista tilannekuvaa.

2.1.3 Suojelupoliisi

Suojelupoliisin tehtävänä on ennaltaehkäistä ja torjua kaikkein vakavimpia kansallisen turvallisuuden uhkia, kuten terrorismia ja vieraiden valtioiden Suomeen kohdistamaa laitonta tiedustelua, kuten verkkotiedustelua. Sen tehtävänä on havaita, estää ja paljastaa sellaisia toimia, hankkeita ja rikoksia, jotka voivat uhata valtio- tai yhteiskuntajärjestystä tai Suomen sisäistä tai ulkoista turvallisuutta. Suojelupoliisi suorittaa poliisilain 5 a luvun 1 §:n mukaan tiedonhankintaa eli siviilitiedustelua muun muassa verkossa tapahtuvien kyberhyökkäysten taustojen ja motiivien selvittämiseksi kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohdon päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

2.1.4 Puolustusvoimat

Puolustusvoimista annetun lain (551/2007) 2 §:n mukaan Puolustusvoimien tehtävänä on muun muassa maa-alueiden, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen. Edelleen Puolustusvoimien tehtävänä on kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen sekä laillisen yhteiskuntajärjestyksen turvaaminen. Lisäksi sen tehtävänä on muiden viranomaisten tukeminen, johon kuuluu esimerkiksi virka-apu yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, terrorismirikosten estämiseksi ja keskeyttämiseksi sekä muuksi yhteiskunnan turvaamiseksi. Puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta. Puolustusvoimilla on velvollisuus torjua maanpuolustukseen ja puolustusjärjestelmään kohdistuva tietoverkkotiedustelu sekä kyberhyökkäykset etenkin silloin, kun kyseessä on valtiollinen toimija.

Sotilastiedustelusta annetussa laissa (590/2019, jäljempänä *sotilastiedustelulaki*) säädetään Puolustusvoimien tiedustelutoiminnasta (sotilastiedustelusta), jonka tarkoituksena on hankkia ja käsitellä tietoa Suomeen kohdistuvasta tai Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta, tuottaa tietoa ylimmälle valtiojohdolle päätöksenteon tukemiseksi vieraan valtion toiminnasta tai muusta toimista, jotka vakavasti uhkaavat Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja.

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa (255/2014) säädetään Puolustusvoimien rikostorjunnasta, joka käsittää ennalta estämisen, paljastamisen ja sotilaskurinpitomenettelyyn kuuluvan rikosten selvittämisen. Lain 9 luvussa säädetään rikosten ennalta estämisen ja paljastamisen tehtävistä. Näitä ovat sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estäminen ja paljastaminen. Kyseeseen voivat maanpuolustuksen alalla tulla esimerkiksi sellaiset hankkeet tai rikokset, jotka voivat uhata valtio- tai yhteiskuntajärjestystä tai Suomen ulkoista tai sisäistä turvallisuutta, kuten maanpetos, valtiopetos, vakoilu tai luvaton tiedustelutoiminta.

2.1.5 Muita keskeisiä viranomaisia

Valtion yhteisten tieto- ja viestintäteknisten palvelujen tuottajan (Valtion tieto- ja viestintätekniikkakeskus Valtori, jatkossa *Valtori*) tehtävänä on valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annetun lain (1226/2013) nojalla tuottaa valtion yhteisiä perustekniikkapalveluja sekä yhteisiä tietotekniikkapalveluja, joita valtion virastoilla ja laitoksilla on lähtökohtaisesti velvollisuus käyttää. Valtorilla on velvollisuus huolehtia siitä, että toiminta ja palvelujen tuotanto jatkuvat mahdollisimman häiriöttömästi normaaliolojen häiriötilanteissa sekä poikkeusoloissa.

Viranomaisten turvallisuusverkkotoiminnasta säädetään julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015, jäljempänä *TUVE-laki*). Turvallisuusverkko on valtion omistuksessa ja hallinnassa oleva viranomaisverkko, johon kuuluu viestintäverkko, siihen liittyvät laitetilat ja laitteet sekä yhteiset tieto- ja viestintätekniset palvelut. Turvallisuusverkko täyttää korkean varautumisen ja turvallisuuden vaatimukset siten kuin siitä laissa erikseen säädetään tai lain nojalla määrätään. Turvallisuusverkolla mahdollistetaan jokapäiväinen työskentely sekä operatiivisessa toiminnassa että hallinnollisissa tehtävissä. Turvallisuusverkon verkko- ja infrastruktuuripalveluja tuottaa valtion omistama Suomen Erillisverkot Oy, joka tuottaa myös TUVE-lain mukaisia viranomaisradioverkon sekä viranomaisten aikakriittisen laajakaistaisen matkaviestinnän tieto- ja viestintäpalveluja. Valtori tuottaa turvallisuusverkon muita tieto- ja viestintäteknisiä palveluja sekä integraatiopalveluja. Turvallisuusverkon palveluja tuottaville palveluntuottajille on TUVE-laissa asetettu vaatimukseksi vastata tehtäväalueellaan turvallisuusverkkoa koskevien turvallisuus-, valmius-, varautumis- ja jatkuvuusvaatimusten toteuttamisesta normaalioloissa ja niiden häiriötilanteissa sekä poikkeusoloissa. Turvallisuusverkon palvelut ovat keskeisiä viranomaisten kesken vaihdettavan tiedon välityksessä myös tietoturvaloukkausten häiriötilanteissa.

NIS-direktiivin mukaista tietoturvaloukkausten valvontaa tekevät kansallisesti useat eri sektoriviranomaiset. Voimassa olevan NIS-direktiivin valvontaviranomaisia ovat liikenteen (ilmailu, merenkulku, tieliikenne, raideliikenne) ja digitaalisen infrastruktuurin sekä digitaalisten palveluiden osalta Liikenne- ja viestintävirasto, energiasektorin osalta Energiavirasto, terveydenhuoltoalalta Valvira, finanssisektorilla Finanssivalvonta ja vesihuollon osalta ELY-keskus sekä maa- ja metsätalousministeriö. Jokainen NIS-viranomainen vastaa oman toimialansa merkittäviä tietoturvaloukkauksia koskevien ilmoitusten vastaanottamisesta. Ilmoitustavasta riippuen nämä ilmoitukset eivät välttämättä mene automaattisesti Kyberturvallisuuskeskukselle ilman erillistä ilmoitusta.

Valtioneuvoston ohjesäännön (262/2003) 12 §:n 7 kohdan mukaan valtioneuvoston kanslian toimialaan kuuluu valtioneuvoston yhteinen tilannekuva, varautuminen ja turvallisuus sekä häiriötilanteiden hallinnan yleinen yhteensovittaminen. Laissa säädetään valtioneuvoston tilannekeskuksen tehtävistä ja viranomaisten välisestä tiedonvaihdosta. Valtioneuvoston tilannekeskuksesta annetun lain (300/2017) 1 §:n mukaan valtioneuvoston tilannekeskuksen tehtävänä on tasavallan presidentin ja valtioneuvoston päätöksenteon ja toiminnan tueksi koota ja analysoida tietoa turvallisuustilanteesta ja sellaisista häiriöistä ja niiden uhista, jotka vaarantavat yhteiskunnan elintärkeitä toimintoja, hoitaa ja koordinoida tilannekuvan ylläpitämiseen, kokoamiseen, yhteensovittamiseen ja välittämiseen liittyviä poikkihallinnollisia tehtäviä sekä jakaa yhteen sovitettua tietoa tasavallan presidentille, valtioneuvostolle ja muille viranomaisille. Lisäksi laissa säädetään ministeriöiden sekä hallinnonalan viraston ja laitoksen velvollisuudesta ilmoittaa onnettomuudesta, vaaratilanteesta, poikkeuksellisesta tapahtumasta tai muusta vastaavasta häiriöstä tilannekeskukselle sekä tilannekeskuksen tiedonsaantioikeudesta sekä salassa pidettävän tiedon luovuttamisesta.

Valtioneuvoston tilannekeskus tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista koottua tilannekuvaa. Tilannekeskus yhdistää eri viranomaisilta ja avoimista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille. Tähän kuuluu myös kyberturvallisuuden tilannekuvan kokoaminen.

2.1.6 Viranomaisten tehtävien arviointi

Edellä esitetyn perusteella voidaan todeta, että kyberturvallisuuden alueella toimivia viranomaisia on useita ja tehtävät ovat jossain määrin limittäisiä. Usean viranomaisen toimintaan liittyy esimerkiksi tietoturvaloukkausten selvittämiseen liittyviä toimintoja, mutta tehtävistä johtuen selvittämisen tavoite ja tarkoitus poikkeavat toisistaan. Liikenne- ja viestintäviraston tarkoituksena on selvittää tietoturvaloukkauksia erityisesti tekniseltä kannalta, turvata siten viestinnän luottamuksellisuutta ja myös ennaltaehkäistä uusia hyökkäyksiä. Poliisin tietoturvaloukkausten selvittämiseen liittyvät intressit liittyvät rikosten ennaltaehkäisyyn ja toisaalta rikoksentekijöiden rikosoikeudelliseen vastuuseen saattamiseen. Suojelupoliisin selvittämiseen liittyvät intressit liittyvät laajemmin kansallisen turvallisuuden turvaamiseen ja uhkakuvan muodostamiseen esimerkiksi valtiollisia toimijoita vastaan. Puolustusvoimat taas pyrkii selvittämällä turvaamaan maanpuolustukseen liittyvät toiminnot. Sotilastiedustelun tavoitteena on selvittää kyberhäiriöiden aiheuttaja erityisesti, jos kyse on sotilaallisesta toiminnasta sekä taustalla olevan toimijan tarkoitusperästä. Kyberhäiriöiden selvittämisen menetelmät ovat jokseenkin samanlaisia viranomaisesta riippumatta, jolloin tähän tarvittavia kyvykkyyksiä löytyy useammasta viranomaisesta. Toiminnan tavoite ja tarkoitus vain vaihtelevat.

Toinen tehtävä, jossa viranomaisten tehtävissä on yhteneväisyyksiä, liittyy erilaisten tilannekuvien muodostamiseen. Liikenne- ja viestintäviraston tehtäviin kuuluu kyberturvallisuuden kansallisen tilannekuvan muodostaminen. Suojelupoliisi osaltaan tukee tätä tehtävää tuottamalla tietoa tilannekuvan muodostamiseksi. Toisaalta suojelupoliisin tehtävänä on myös muun tiedon tuottaminen esimerkiksi ylimmän valtionjohdon päätöksenteon tueksi. Puolustusvoimien sotilastiedustelutoiminnalla on vastaava tehtävä sotilaallisen toiminnan osalta. Poliisi ylläpitää kyberrikollisuuden tilannekuvaa. Tilannekuvaan liittyviä tehtäviä eri sektoreiden osalta liittyy myös eri NIS-sektoreiden valvontaviranomaisten tehtäviin, joiden tehtävänä on yleisesti valvoa tietyn sektorin toimintaa mukaan lukien niihin kohdistuvat tietoturvaloukkaukset. Valtori vastaa osaltaan julkisen sektorin järjestelmien toimivuudesta ja seuraa niiden toimintaa. Kokoavana tahona erilaiselle tilannekuvatiedolle on valtioneuvoston tilannekeskus, jonka tehtävänä on koota ja analysoida tietoa turvallisuustilanteesta ja häiriöistä sekä uhkista, jotka vaarantavat yhteiskunnan elintärkeitä toimintoja. Tilannekeskus jakaa tietoa edelleen ylimmän valtionjohdon päätöksentekoa varten.

Tehtävissä on edellä esitetyn perusteella siten paljon yhtäläisyyksiä ja näiden tehtävien keskiössä on tieto, jonka perusteella toimenpiteitä viranomaisissa tehdään. Viranomaisilla on tehtäviensä luonteesta johtuen erilaiset keinot hankkia tietoa velvoitteidensa hoitamiseksi. Tehtävien tavoitteista johtuen niihin liittyy myös erilaisia rajoitteita ja reunaehtoja, jotka joissain tilanteissa muodostavat haasteita. Seuraavassa jaksossa eritellään tarkemmin viranomaisten tiedonvaihtoon liittyvää lainsäädäntöä ja siihen liittyviä rajoitteita.

2.2 Viranomaisten välinen tiedonvaihto

Viranomaisten tiedonvaihtoa koskevaa sääntelyä on viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999, jäljempänä *julkisuuslaki*). Julkisuuslakia sovelletaan yleislakina, jos muualla lainsäädännössä ei toisin säädetä. Julkisuuslain 26 §:ssä säädetään yleisistä perusteista salassa pidettävän tiedon antamiseen. Tieto salassa pidettävästä viranomaisen asiakirjasta voi-

daan antaa, jos tiedon antamisesta tai oikeudesta tiedon saamiseen on laissa erikseen nimenomaisesti säädetty tai se, jonka etujen suojaamiseksi salassapitovelvollisuus on säädetty, antaa siihen suostumuksensa. Pykälän 3 momentin mukaan viranomainen voi antaa salassa pidettävästä asiakirjasta tiedon antamansa virka-aputehtävän suorittamiseksi sekä toimeksiannostaan tai muuten lukuunsa suoritettavaa tehtävää varten, jos se on välttämätöntä tehtävän suorittamiseksi. Salassa pidettäviä tietoja voi kuitenkin luovuttaa mainittuja tehtäviä varten myös silloin, kun salassa pidettävien tietojen poistaminen niiden suuren määrän tai muun niihin verrattavan syyn vuoksi ei ilmeisesti ole tarkoituksenmukaista. Viranomaisen on ennakolta varmistuttava siitä, että tietojen salassapidosta ja suojaamisesta huolehditaan asianmukaisesti. Viranomaiset voivat vaihtaa keskenään salassa pidettäviä tietoja myös ilman varsinaista säännöstä julkisuuslain 24 §:n 1 momentin vahinkoedellytyslausekkeiden rajoissa, kun tieto ei ole julkisuuslaissa säädetty ehdottomasti salassa pidettäväksi.

Hallintolain (434/2003) 10 §:n nojalla viranomaisen on toimivaltansa rajoissa ja asian vaatimassa laajuudessa avustettava toista viranomaista tämän pyynnöstä hallintotehtävän hoitamisessa sekä muutoinkin pyrittävä edistämään viranomaisten välistä yhteistyötä. Hallintolain esitöissä (HE 72/2002 vp) todetaan, että viranomaisten yhteistyövelvoitteesta ei olisi johdettavissa yleistä tietojenantovelvollisuutta, vaan viranomaiset toimivat oman hallinnonalansa tehtäviä täyttääkseen, omilla toimivaltuuksillaan ja oman salassapitovelvollisuutensa rajoissa.

2.2.1 Liikenne- ja viestintävirasto

Sähköisen viestinnän palveluista annetun lain 315 §:ssä säädetään viranomaisten yleisestä tiedonsaantioikeudesta siten, että lain säännöksiä valvovilla viranomaisilla on lain mukaisia tehtäviä suorittaessaan oikeus saada tehtäviensä suorittamiseksi tarvittavat tiedot niiltä, joiden oikeuksista ja velvollisuuksista laissa säädetään. Lisäksi tietoja voidaan velvoittaa keräämään. Tiedot viesteistä, välitystiedoista ja sijaintitiedoista eivät sisälly yleiseen tiedonsaantioikeuteen. Laissa ei ole tarkemmin määritelty, keitä ne tahot ovat, joilta tietoja voidaan saada, mutta lain velvoitteet tai oikeudet on usein kohdistettu johonkin tiettyyn tahoon. Lain esitöiden mukaan tiedonsaantioikeus voi koskea periaatteessa ketä tahansa, jota laki koskee.

Viestintää ja sijaintia koskevien tietojen käsittelystä ja hävittämisestä säädetään SVPL 316 §:ssä. Liikenne- ja viestintävirastolla on salassapitosäännösten tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada tarpeelliset välitystiedot ja sijaintitiedot vikatilanteiden tai häiriötilanteiden selvittämiseksi. Lisäksi virastolla on oikeus saada välitys- ja sijaintitiedot ja viestit, jos ne ovat tarpeen merkittävien tietoturvaloukkausten tai -uhkien selvittämiseksi. Tiedonsaantioikeuden edellytyksenä on lisäksi, että viraston arvion mukaan on syytä epäillä jonkun pykälässä mainitun rikoksen tunnusmerkistön täyttyvän. Säännöstä on käytännössä tulkittu siten, että oikeus saada viestintää ja sijaintia koskevia tietoja koskee samoja tahoja, joilta on oikeus saada muuta tietoa SVPL 315 §:n nojalla.

Sähköisen viestinnän palveluista annetun lain 318 §:ssä säädetään tietojen luovuttamisesta viranomaisesta salassapitosäännösten estämättä. Liikenne- ja viestintävirasto voi luovuttaa tietoja Energiavirastolle, Finanssivalvonnalle, Valviralle sekä ELY-keskukselle eli NIS-viranomaisille, jos se on niille säädettyjen tietoturvallisuuteen liittyvien tehtävien hoitamiseksi välttämätöntä. Liikenne- ja viestintävirastolla on lisäksi oikeus luovuttaa salassa pidettäviä asiakirjoja tai tietoja valtiovarainministeriölle, jos se on viranomaisverkon ja viranomaisviestintään liittyvien verkko- ja viestintäpalvelujen tarjoamiseen liittyvien tehtäviensä hoitamiseksi välttämätöntä. Oikeus luovuttaa tietoja ei lain 318 §:n 5 momentin mukaan koske tietoja viesteistä, välitystiedoista, paikkatiedoista tai luottamuksellisen radiolähetyksen sisällöstä tai olemassaolosta.

Lain 319 §:n 1 momentin mukaan Liikenne- ja viestintäviraston 316 ja 317 §:n nojalla saamat ja hankkimat tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta on pidettävä salassa. Tämän tai muiden tietojen luovuttamista koskevien rajoitusten estämättä Liikenne- ja viestintävirastolla on lain 319 §:n 2 momentin 1 kohdan mukaan oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja viestinnän välittäjälle, lisäarvopalvelun tarjoajalle, yhteisölle, tilaajalle ja käyttäjälle, jos sitä on käytetty hyväksi tietoturvaloukkauksessa, se on joutunut tietoturvaloukkauksen kohteeksi tai siihen todennäköisesti voi kohdistua tietoturvaloukkaus ja jos Liikenne- ja viestintäviraston arvion mukaan on syytä epäillä, että on tehty jokin SVPL 316 §:n 2 momentin 1–12 kohdassa mainittu rikos. Lisäksi tietoa voidaan luovuttaa muussa valtiossa toimivalle viranomaiselle tai vastaavalle taholle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia. Tämä määrittely tulee tehdä yhteistyössä liikenne- ja viestintäministeriön kanssa. Tiedot voidaan luovuttaa vain välttämättömässä laajuudessa. Huomionarvoista on, että lain nykymuotoilu ei mahdollista tiedon luovuttamista esimerkiksi EU:lle tai Natolle.

SVPL 322 §:n mukaan poliisin oikeudesta saada välitystietoja rikosten ennalta estämiseksi, paljastamiseksi ja selvittämiseksi säädetään poliisilaissa ja pakkokeinolaissa (806/2011, jäljempänä *PakkokeinoL*). Rajavartiolaitoksen ja Tullin rikostorjuntatoiminnan osalta säännökset ovat omissa säädöksissään.

Tällä hetkellä SVPL 275 §:ssä säädetään teleyrityksen ilmoitusvelvollisuudesta, jos sen palveluun kohdistuu tai sitä uhkaa merkittävä tietoturvaloukkaus tai muu tapahtuma, joka estää viestintäpalvelun toimivuuden tai häiritsee sitä olennaisesti. Vastaavasti SVPL 316 §:n 2 momentin nojalla Liikenne- ja viestintävirastolla on oikeus pyytää tietoonsa tulleeseen tietoturvaloukkaukseen liittyvät tiedot. Sääntelyyn liittyy kuitenkin epäselvyys sen suhteen, voivatko teleyritykset ja muut viestinnän välittäjät vapaaehtoisesti ja oma-aloitteisesti luovuttaa tietoturvaloukkauksiin liittyviä välitystietoja ja tietoja viesteistä virastolle, jos loukkaus ei muutoin tulisi viraston tietoon. Liikenne- ja viestintäviraston tehtävänä on tietoturvaloukkausten selvittäminen, mutta SVPL 137 §:n 2 momentin mukaan sähköisiä viestejä ja välitystietoja on sallittua luovuttaa ainoastaan niille tahoille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. SVPL 304 §:ssä säädetyn tehtävän ei kuitenkaan tulkita sellaisenaan muodostavan käsittelyperustetta välitystiedoille ja viestinnän sisällölle, jolloin on epäselvää, mihin tietojen luovuttaminen Liikenne- ja viestintävirastolle viestinnän välittäjän loukkausta selvitettäessä voisi perustua tilanteessa, jossa luovutus tapahtuisi oma-aloitteisesti ja jossa 275 § ei sovellu tai ei edellyttäisi viestintää koskevien tietojen antamista.

Liikenne- ja viestintävirastolla on edellä kuvatun perusteella laajat tiedonsaantioikeudet valvontaoikeuksiinsa perustuen. Tiedonsaantioikeus viesteistä, välitystiedoista ja sijaintitiedoista on kuitenkin rajatumpi. Näihinkin tietoihin virastolla on lakisääteinen saantioikeus tietoturvaloukkaustilanteissa. Edellä mainitun lisäksi virastolle tehdään huomattava määrä yksityisten toimijoiden toimesta myös vapaaehtoisuuteen perustuvia tietoturvaloukkausilmoituksia, jotka voivat sisältää tietoturvaloukkauksiin liittyviä erilaisia tietoja, kuten välitystietoja tai tietoja viestin sisällöstä. Tiedon luovuttamisesta edelleen on säädetty erikseen ja siihen liittyy jonkin verran rajoitteita erityisesti viestin sisältöä, välitystietoja ja sijaintitietoja koskien. Rajoitukset näihin tietoihin liittyen perustuvat perustuslaissa turvatun luottamuksellisen viestinnän suojaan.

2.2.2 Poliisi

Poliisin toimintaan liittyvä lainsäädäntö on moninainen poliisin erilaisista tehtävistä johtuen. Poliisilaissa säädetään yleisesti poliisin toiminnasta, toimivaltuuksista ja lisäksi salaisista tiedonhankintakeinoista, joita poliisi voi käyttää rikosten ennalta estämiseksi ja paljastamiseksi.

Poliisilaissa säädetään myös suojelupoliisin tehtäviin kuuluvasta siviilitiedustelusta, jota täydentää tietoliikennetiedustelusta siviilitiedustelussa annettu laki (582/2019). Esitutkintalakia (805/2011) sovelletaan rikosten esitutkintaan ja esitutkinnassa käytettyihin pakkokeinoihin ja tiedonhankintaan sovelletaan pakkokeinolakia. Henkilötietojen käsittelystä poliisitoimessa annetussa laissa (616/2019, jäljempänä *poliisin henkilötietolaki*) säädetään nimensä mukaisesti poliisin henkilötietojen käsittelystä.

Poliisilain 4 luvussa säädetään poliisin tiedonsaantioikeudesta. Lain 4 luvun 2 §:n mukaan poliisilla on päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada viranomaiselta ja julkista tehtävää hoitavalta yhteisöltä tarpeelliset tiedot ja asiakirjat poliisille kuuluvan tehtävän hoitamiseksi, ellei kyseisten tietojen antaminen ole nimenomaisesti kielletty tai rajoitettu. SVPL 318 §:n 1–4 momentin tulkitaan olevan tällainen nimenomainen kielto, koska siinä säädetään niistä viranomaisista, joille tietoja saa luovuttaa, eikä poliisia ole tässä yhteydessä mainittu. Poliisilain esitöissä (HE 57/1994 vp, s. 67) todetaan, että pykälässä määritelty tietojensaantioikeus syrjäyttäisi muualla laissa säädetyt salassapitovelvollisuudet, ellei salassapitovelvollisuutta koskevassa säännöksessä nimenomaisesti kielletä tietojen luovuttaminen poliisille. Kielto voidaan ilmaista myös luettelemalla tietojensaantiin oikeutetut viranomaiset mainitsemassa poliisia niiden joukossa. Viestintää koskevien tietojen osalta tilanne on tällainen 319 §:n osalta lukuun ottamatta 4 momentissa tarkoitettua tilannetta, joka koskee välitystiedon antamista toiselle viranomaiselle, jos se on tarpeen radiohäiriön aiheuttamista koskevan rikoksen selvittämistä tai syytteeseen panoa varten taikka radioviestinnän häiriön poistamiseksi tai rajoittamiseksi. Lain 319 §:n 2 momentin nojalla poliisille voitaisiin muutoin luovuttaa tietoa viesteistä, välitystiedoista, sijaintitiedoista ja radiolähetyksen sisällöstä ja olemassa olosta vain niissä tilanteessa, joissa poliisi olisi itse tietoturvaloukkauksen tai -uhkan kohteena.

Poliisilain 4 luvun 3 §:ssä säädetään tietojen saannista yksityiseltä yhteisöltä tai henkilöltä rikosten estämiseksi tai selvittämiseksi. Poliisilla on oikeus saada tietoja yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan salassapitovelvoitteen estämättä. Säännös ei oikeuta saamaan välitystietoja tai tietoja viestin sisällöstä, koska näiden tietojen saantiin sisältyy erityisiä edellytyksiä poliisi- ja pakkokeinolaissa.

Poliisilain 4 luvun 3 §:n 2 momentin mukaan poliisilla on yksittäistapauksissa oikeus saada teleyritykseltä tai yhteisötilaajalta yhteystiedot sellaisesta teleosoitteesta, jota ei mainita julkisessa luettelossa, taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi. Poliisin salaisen tiedonhankinnan (PolL 5 luku 61 §), Suojelupoliisin siviilitiedustelun (PolL 5a luku 51 §) ja salaisten pakkokeinojen (PakkokeinoL 10 luku 63 §) osalta säädetään yhtenevästi teleyrityksen avustamisvelvollisuudesta ja pääsystä eräisiin tietoihin.

Viranomaisen salassa pidettävän tiedon luovuttamisen osalta peruslähtökohta on julkisuuslain säännöksissä. Käytännössä tämä edellyttää siten laissa erikseen säädettyä perustetta tiedon luovuttamiselle, mikä asettaa käytännössä haasteita, koska kaikkia luovutustilanteita on vaikea arvioida ennakolta. Tietoa voidaan kuitenkin luovuttaa julkisuuslain 17 §:n 3 momentin ja 26 §:n nojalla rajatulle piirille, kuten toiselle viranomaiselle julkisuuslain 24 §:n 1 momentin tiedon luovuttamista koskevien vahinkoedellytyslausekkeiden asettamissa rajoissa.

Tiedon luovuttamisesta yksittäistapauksessa säädetään poliisilain 7 luvun 2 §:ssä. Pykälän mukaan poliisille säädetty vaitiolovelvollisuus ei estä tiedon antamista viranomaiselle, jolla on säädetyn tehtävänsä vuoksi tarve saada tieto muuten salassa pidettävästä seikasta. Tämä voi tarkoittaa esimerkiksi välitystietoa tai tietoa viestistä. Poliisilain esitöissä (HE 224/2010 vp s. 147) on todettu, että vaikka 7 luvun 2 §:n 1 momentin mukainen tietojen luovuttaminen tapahtuu yleensä toisen viranomaisen pyynnöstä, se ei kuitenkaan ole säännöksen soveltamisen edellytys.

Esitöiden mukaan poliisille voi tulla eteen tilanteita, joissa myös tietojen oma-aloitteinen luovuttaminen toiselle viranomaiselle on tarpeen ja perusteltua. Myös oikeuskirjallisuudessa on poliisilain esitöihin viitaten katsottu, ettei toisen viranomaisen pyyntö ole poliisilain 7 luvun 2 §:n 1 momentissa tarkoitettujen tietojen välttämätön edellytys, vaan tietojen luovuttaminen voi tapahtua myös oma-aloitteisesti. Myös apulaisoikeusasiamies on katsonut (EOAK/3813/2017) poliisin oma-aloitteisen tietojen luovuttamisen olevan ilmeisen vakiintunut toimintatapa, jolle on nähtävissä perusteita 7 luvun 2 §:n säännöksestä ja lainkohdan esitöistä. Kuitenkin huomionarvoista on hovioikeuden ratkaisu HO 4.3.2021 nro 263, jossa hovioikeus toteaa, että poliisilain 7 luvun 2 § ei ole toimivaltasäännös, jonka nojalla poliisi voisi luovuttaa ulosottoviranomaiselle oma-aloitteisesti tietoja. Asia on parhaillaan korkeimman oikeuden ratkaistavana. Poliisilain tiedonluovuttamisen säännös on ensisijainen henkilötietojen käsittelystä poliisitoimesta annetun lain 22 §:ään nähden.

Julkisuuslain 24 §:n 1 momentin 3 kohdassa säädetään poliisille muille esitutkintaviranomaisille ja syyttäjä sekä tarkastus- ja valvontaviranomaisille tehtyjen rikosilmoitusten, esitutkintaa ja syyteharkintaa varten saatujen ja laadittujen asiakirjojen salassapidosta. Kohdassa säädetyt tiedot ovat salassa pidettäviä, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna rikoksen selvittämistä tai tutkinnan tarkoituksen toteutumista tai ilman painavaa syytä aiheuta asiaan osalliselle vahinkoa tai kärsimystä tai estä tuomioistuinta käyttämästä oikeuttaan määrätä asiakirjojen salassapidosta oikeuden käynnin julkisuudesta yleisissä tuomioistuimissa annetun lain mukaan. Esitutkintalain 2 luvun 2 §:n mukaan esitutkintaa johtaa tutkinnanjohtaja ja päättää näin ollen muun muassa esitutkinnan aikana tietojen luovuttamisesta. Esitutkintalain 11 luvun 7 §:ssä säädetään esitutkinnasta tiedottamisesta.

Poliisi saa tietoja rikosten estämiseksi ja paljastamiseksi myös poliisilain 5 luvun mukaisilla salaisilla tiedonhankintakeinoilla ja esitutkintaa varten pakkokeinolain 10 luvussa tarkoitetuilla salaisilla pakkokeinoilla. Näitä keinoja ovat esimerkiksi telekuuntelu, televalvonta, tukiasematietojen hankkiminen sekä teleosoitteen ja telepäätelaitteen yksilöivien tietojen hankkiminen. Salaisten tiedonhankintakeinojen käytön edellytyksenä on, että sillä voidaan olettaa saatavan tarvittavia tietoja rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi. Salaisten pakkokeinojen käytön edellytyksenä on, että niiden käytöllä voidaan olettaa saatavan tarvittavia tietoja rikosten selvittämiseksi. Salaisella tiedonhankinnalla tai salaisilla pakkokeinoilla on oltava erittäin tärkeä merkitys rikosten selvittämiseen, ennaltaehkäisyyn tai paljastamiseen. Poliisilain 5 luvun 3 §:ssä on lueteltu rikokset, joiden selvittämiseen salaista tiedonhankintaa voidaan käyttää. Lupa salaiseen tiedonhankintaan ja salaisten pakkokeinojen käyttämiseen on haettava lähtökohtaisesti tuomioistuimelta. Joissakin kiireellisissä tilanteissa päätöksen voi tehdä väliaikaisesti myös pidättämiseen oikeutettu virkamies ennen kuin asiaan ehditään saada tuomioistuimen päätös.

Salaisten tiedonhankintakeinojen osalta poliisilain 5 luvun 52 §:ssä säädetään, että salaisella tiedonhankintakeinolla saatuja tallenteita voi erillisellä päätöksellä tutkia muu henkilö kuin poliisi, jota käytetään apuna tiedonhankintaa toteutettaessa. Siviilitiedustelun osalta vastaava säännös on poliisilain 5 a luvun 43 §:ssä ja salaisten pakkokeinojen osalta pakkokeinolaissa lain 10 luvun 54 §:ssä.

Suojelupoliisi saa tietoja poliisilain 5 a luvun mukaisilla tiedustelumenetelmillä, joka ovat vastaavia, mitä poliisin osalta on säädetty salaisista tiedonhankintakeinoista ja salaisista pakkokeinoista. Näiden keinojen käytön edellytyksenä on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Tiedustelumenetelmien käytöstä päättää kyberympäris-

tössä pääasiassa tuomioistuin. Joissakin kiireellisissä tilanteissa päätöksen voi tehdä väliaikaisesti myös suojelupoliisin päällikkö tai tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva virkamies ennen kuin asiaan ehditään saada tuomioistuimen päätös.

Poliisilain 5 a luvun 44 §:ssa säädetään siitä, missä tilanteissa suojelupoliisi ei saa ilmoittaa sekä missä tilanteessa sen on ilmoitettava tai missä tilanteissa se harkintansa mukaan saa ilmoittaa siviilitiedustelussa saadut tiedot keskusrikospoliisille. Sen lisäksi pykälässä säädetään ilmoittamisvelvollisuuksista vielä estettävissä olevan rikoksen osalta. Ilmoitusvelvollisuus tai -oikeus riippuu ilmi tulleen teon rangaistavuudesta. Tämä ilmoitus voidaan tehdään vain vakavimpien rikosten kohdalla. Lähtökohtaisesti tiedustelutoiminta on erotettu esitutkinnan tehtävistä ja näistä saadut tiedot pidetään erillään koska tiedustelumenetelmien käytön kynnys on alhaisempi kuin vastaavien menetelmien esitutkinnassa. Kyse on niin sanotusta palomuurisääntelystä.

Poliisilain 5 a luvun 55 §:ssä säädetään suojelupoliisin yhteistyöstä muiden viranomaisten, yritysten ja yhteisöjen kanssa. Suojelupoliisin on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi. Kansallisen turvallisuuden suojaamiseksi siviilitiedustelutehtävää toteutettaessa suojelupoliisilla on lupa luovuttaa salassapitosäännöksen estämättä muita kuin henkilötietoja koskevia tietoja muille viranomaisille, mutta myös yrityksille sekä muille yhteisöille.

Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 14 §:ssä säädetään tietoliikennetiedustelun käytössä kertyneiden tallenteiden tutkimisesta. Vastaavalla tavalla kuin muussakin tiedustelussa, tallenteita saa tutkia vain tuomioistuin tai suojelupoliisin päällystöön kuuluva poliisimies taikka tiedusteluvalvontavaltuutettu tai hänen määräämänsä virkamies. Suojelupoliisin päällystöön kuuluvan poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

Haitallista tietokoneohjelmaa tai käskyä koskevien tietojen luovuttamisesta viranomaiselle, yritykselle tai yhteisölle säädetään tietoliikennetiedustelusta siviilitiedustelussa annetun lain 16 §:ssä. Suojelupoliisi saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankitun tiedon haitallisesta tietokoneohjelmasta tai käskystä viranomaiselle, yritykselle tai yhteisölle, jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi. Tiedon luovuttamisesta rikostorjuntaan sovelletaan, mitä poliisilaissa asiasta säädetään.

Henkilötietojen käsittelystä poliisitoimesta annetun lain 22 §:ssä säädetään muusta henkilötietojen luovuttamisesta viranomaisille. Lain 5–8, 11 ja 12 §:ssä tarkoitettuja tietoja, kuten poliisin tehtävään, toimenpiteeseen ja tapahtumaan liittyvät yksilöintiä, kuvauksia ja luokituksia koskevia tietoja voidaan luovuttaa 22 §:n 1 momentin alakohdissa määritellyille viranomaisille. Lista ei kuitenkaan ole merkityksellinen kyberhäiriötilanteiden selvittämisen kannalta, vaan niiden osalta on sovellettava 22 §:n 3 momenttia, jonka mukaan poliisi saa perustellusta syystä luovuttaa salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona viranomaiselle henkilötietoja, jotka ovat välttämättömiä viranomaisen laissa säädetyn tehtävän suorittamiseksi. Tiedon luovuttamisen edellytyksenä ovat siten välttämätön syy ja laissa säädetty tehtävä.

Henkilötietojen käsittelystä poliisitoimessa annetun lain 21 §:n mukaan poliisi saa salassapitosäännösten estämättä luovuttaa laissa tarkoitettuja henkilötietoja muun muassa suojelupoliisille ja Puolustusvoimille henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain (1054/2018, jäljempänä *rikosasioiden tietosuojalaki*) 1

§:ssä tarkoitettua tehtävää varten. Näitä tehtäviä voivat olla esimerkiksi rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkinta.

Poliisin laajasta tehtäväkentästä johtuen myös poliisin tiedonsaantioikeuksia ja tiedon luovutusta koskeva sääntely on melko monimutkainen. Poliisilla on yleisesti ottaen tehtävänsä hoitamiseksi laajat yleiset tiedonsaantioikeudet, joita täydentävät tilanteen niin edellyttäessä salaisia tiedonhankintakeinoja ja pakkokeinoja koskevat säännökset. Erityisiä rajoituksia poliisin tiedonsaantioikeuksiin liittyy Liikenne- ja viestintäviraston suunnalta viestintää koskevien tietojen osalta. Vastaavien tietojen hankkimiseksi poliisin tulisi normaaliolosuhteissa käyttää omia tiedonhankintakeinojaan, jotka edellyttävät tuomioistuimen kontrollia.

Poliisin tiedon luovuttaminen perustuu yleisesti julkisuuslakiin, mutta myös poliisilain 7 luvun 2 §:n tiedonluovuttamista koskevaan säännökseen ja toisaalta poliisiin henkilötietolain henkilötietojen luovutusta koskevaan sääntelyyn. Esitutkinnan aikana tutkinnan johtaja harkitsee tapauskohtaisesti, mitä tietoa voidaan luovuttaa julkisuuslain 24 §:n 3 kohdan edellytysten nojalla. Lainsäädännössä on myös asetettu eräitä rajoituksia poliisiyksiköiden väliselle tiedonvaihdolle, mikä johtuu suojelupoliisin poikkeavasta roolista muussa poliisiorganisaatiossa. Kyse on lähinnä edellä kuvatusta niin sanotusta palomuurisääntelystä.

2.2.3 Puolustusvoimat

Puolustusvoimilla on Puolustusvoimista annetun lain 17 §:n nojalla oikeus saada viranomaisilta sekä julkista tehtävää hoitavalta yhteisöltä sille säädetyn tehtävän hoitamiseksi välttämättömät tiedot ja asiakirjat, jollei niiden antamista Puolustusvoimille tai tietojen käyttöä todisteena Puolustusvoimissa ole laissa kielletty tai rajoitettu. Tiedon luovuttamiseen sovelletaan julkisuuslakia.

Sotilastiedustelulain 17 §:n mukaan sotilastiedusteluviranomaisten on toimittava yhteistyössä suojelupoliisin kanssa tiedusteluviranomaisten tehtävien hoitamiseksi sekä annettava suojelupoliisille tarpeellisia tietoja salassapitovelvollisuuden estämättä. Lain 18 §:n mukaan sotilastiedusteluviranomaisten on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa tiedustelun tarkoituksenmukaiseksi hoitamiseksi. Sotilastiedusteluviranomainen voi tehtävänsä toteuttamiseksi luovuttaa muille viranomaisille salassapitosäännösten estämättä muita tietoja kuin henkilötietoja, jos tietojen luovuttaminen on tarpeen maanpuolustuksen kannalta tai kansallisen turvallisuuden suojaamiseksi. Henkilötietojen luovuttamisesta säädetään erikseen.

Lisäksi sotilastiedusteluviranomainen voi salassapitosäännösten estämättä tehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille tiedustelun menetelmien ja järjestelmien kehittämiseksi haittaohjelmaan liittyvän tunnistamistiedon tai luovuttaa muun kuin henkilötiedon, jos tietojen luovuttaminen on välttämätöntä Puolustusvoimien toiminnan tai kansallisen turvallisuuden suojaamiseksi.

Sotilastiedustelulain 74 §:n mukaan sotilastiedusteluviranomainen saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankittuja tietoja haitallisesta tietokoneohjelmasta ja sen toiminnasta yritykselle, yhteisölle tai viranomaiselle, jos tietojen luovuttaminen on tarpeen sotilaallisen maanpuolustuksen kannalta, kansallisen turvallisuuden suojaamiseksi tai yrityksen tai yhteisön etujen turvaamiseksi.

Sotilastiedustelulain 79 §:ssä säädetään rikosepäilystä ilmoittamisesta keskusrikospoliisille, jos tiedustelumenetelmän käytön aikana ilmenee, että voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Lisäksi ilmoituksen saa tehdä, jos ilmoituksella voidaan olettaa olevan erittäin tärkeä merkitys sellaisen rikoksen selvittämiselle,

josta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta. Lisäksi lain 80 §:n mukaan sotilastiedusteluviranomaisen on viipymättä ilmoitettava toimivaltaiselle viranomaiselle, jos tiedustelutoiminnan aikana ilmenee sellainen, vielä estettävissä oleva rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta ja ilmoituksen saa tehdä, jos ankarin rangaistus on vähintään kaksi vuotta. Kyse on vastaavanlaisesta palomuurisääntelystä, mitä aiemmin on esitetty suojelupoliisin ja keskusrikospoliisin välillä.

Sotilastiedustelulain 111 §:ssä säädetään tiedustelumenetelmillä kertyneiden tallenteiden tutkimisesta. Tietoja saa tutkia vain tuomioistuin, pääesikunnan tiedustelupäällikkö, sotilastiedusteluviranomaisen tehtävään määrätty sotilaslakimies tai muu virkamies taikka tiedusteluvalvontavaltuutettu tai hänen määräämänsä virkamies. Pääesikunnan tiedustelupäällikön määräyksestä tai tuomioistuimen myöntämän luvan perusteella tallennetta saa tutkia muu kuin edellä mainittu virkamies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

Henkilötietojen käsittelystä Puolustusvoimissa annetun lain (332/2019, jäljempänä Puolustusvoimien henkilötietolaki) 29 §:n mukaan Puolustusvoimat saa salassapitosäännösten estämättä luovuttaa muulle viranomaiselle henkilötietoja, jos ne ovat tarpeen viranomaisen laissa säädetyn tehtävän hoitamiseksi. Pykälässä on listattu viranomaiset ja tehtävät, joiden hoitamiseksi tietoja voidaan luovuttaa. Tietoja voidaan luovuttaa ensinnäkin poliisille poliisilain 1 luvun 1 §:n 1 momentissa tarkoitettuja tehtäviä varten, jotka liittyvät oikeus- ja yhteiskuntajärjestyksen turvaamiseen, yleisen järjestyksen ja turvallisuuden ylläpitämiseen tai rikosten ennalta estämiseen, paljastamiseen, selvittämiseen ja syyteharkintaan saattamiseen. Lisäksi tietoja voidaan luovuttaa Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle sen tehtävien hoitamista varten siten, kun se on määritelty Liikenne- ja viestintävirastosta annetun lain 3 §:ssä. Tämä pitää sisällään esimerkiksi kansallisen tilannekuvan ylläpitämisen sekä tietojärjestelmien ja sähköisen viestinnän tietoturvallisuuden edistämisen. Pykälässä ei kuitenkaan täsmällisesti viitata kaikkiin SVPL 304 §:ssä säädettyihin erityisiin tehtäviin, joista Kyberturvallisuuskeskus käytännössä vastaa ja joihin kuuluu muun muassa selvittää verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvia tietoturvaloukkauksia ja niiden uhkia.

Puolustusvoimat voi Puolustusvoimien henkilötietolain 30 §:n nojalla luovuttaa 29 §:n lisäksi yksittäisen tehtävän suorittamiseksi välttämättömiä tietoja viranomaiselle, jos on ilmeistä, ettei tiedon luovuttamisesta aiheudu olennaista haittaa niille eduille, jonka suojaamiseksi salassapitovelvollisuus on säädetty.

Edellä mainittujen säädösten lisäksi tiedon luovuttamista koskevaa lainsäädäntöä sisältyy myös sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain 92 ja 93 §:iin. Lain 92 §:n mukaan Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavilla virkamiehillä on oikeus saada viranomaiselta sekä julkista tehtävää hoitamaan asetetulta yhteisöltä ja henkilöiltä lain 86 §:n 1 momentissa tarkoitetun tehtävän suorittamiseksi tarpeelliset tiedot ja asiakirjat maksutta ja salassapitosäännösten estämättä, jollei tiedon tai asiakirjan antamista pääesikunnalle tai tietojen käyttöä todisteena ole laissa kielletty tai rajoitettu. Lisäksi lain 93 §:ssä säädetään oikeudesta saada tietoja yksityiseltä henkilöltä. Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavilla virkamiehillä on oikeus saada teleyrityksiltä ja yhteisötilaajilta tarpeelliset tiedot teleliittymästä, jota ei mainita julkisessa luettelossa, tai teleliittymän, sähköpostiosoitteen, muun teleosoitteen tai telepäätelaitteen yksilöivät tiedot 86 §:ssä tarkoitetun tehtävän suorittamiseksi.

Puolustusvoimilla on myös edellä esitetyn perusteella laaja yleinen tiedonsaantioikeus tehtävänsä hoitamiseksi. Sitä voidaan rajoittaa siitä nimenomaisesti säätämällä. Kuten poliisin osalta, myös Puolustusvoimien osalta on katsottu, että SVPL:ään sisältyy tällainen nimenomainen rajoite etenkin viestin sisältöä ja välitystietoja koskevan tiedon osalta.

2.2.4 Henkilötiedot ja sovellettava tietosuojalainsäädäntö

Koska vaihdettava tieto voi osittain olla luonteeltaan myös henkilötietoa, on tarpeen arvioida myös eri viranomaisia koskevaa tietosuojalainsäädäntöä. Lähtökohtaisesti viranomaisten toimintaan sovelletaan yleistä tietosuoja-asetusta (EU) 2016/679 ja sitä täydentäviä kansallisia säädöksiä, kuten tietosuojalakia (1050/2018). Kuitenkin huomattavaa on, että poliisin toiminnassa yleisen tietosuoja-asetuksen lisäksi rikosten ennaltaehkäisemiseen, paljastamiseen ja selvittämiseen sekä syyteharkintaan saattamisen osalta sovelletaan rikosasioiden tietosuojalakia. Henkilötietojen käsittelystä poliisitoimessa annettua lakia sovelletaan poliisilain 1 luvun 1 §:ssä tarkoitettujen perustehtävien suorittamiseen, jollei muualla laissa toisin säädetä.

Lisäksi rikosasioiden tietosuojalakia sovelletaan Puolustusvoimiin siltä osin, kun kyse on maa-alueen, vesialueen ja ilmatilan valvomisesta sekä alueellisen koskemattomuuden turvaamisesta sekä virka-avusta yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, terrorismin estämiseksi ja keskeyttämiseksi sekä muuksi yhteiskunnan turvaamiseksi. Rikosasioiden tietosuojalakia sovelletaan Puolustusvoimissa myös rikosasioiden ennalta estämiseen, paljastamiseen ja selvittämiseen. Tältä osin on säädetty erillinen Puolustusvoimien henkilötietolaki, jota sovelletaan rikosasioiden tietosuojalain rinnalla muutamin poikkeuksin.

Edellä mainittujen säädösten lisäksi sovellettavaksi voi tulla Euroopan parlamentin ja neuvoston direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (2002/58/EY) eli sähköisen viestinnän tietosuojadirektiivi. Direktiivi on pantu täytäntöön isolta osin SVPL:ssä. Sääntelyä sovelletaan erityisesti välitystietoihin.

2.2.5 Viranomaisten tiedonvaihtosääntelyn arviointi

Ehdotetun sääntelyn kohteena olevilla viranomaisilla on toiminnassaan laajat tiedonsaantioikeudet. Tiedon vaihtamista viranomaisten välillä rajoittavat käytännössä viestinnän luottamuksellisuutta turvaavat rajoitussäännökset ja toisaalta rikostorjunnan ja tiedustelun väliset palomuurisäännökset. Rajoitukset viranomaisten väliselle tiedonvaihdolle ovat siis olemassa perustellusta, perustuslain perusoikeussuojaan liittyvistä syistä. Käytännössä esimerkiksi poliisilla ja Puolustusvoimilla voi tarvittaessa olla pääsy myös niihin tietoihin, joita Liikenne- ja viestintävirastolla on hallussaan lakisääteisistä tehtävistään johtuen, mutta tiedon hankinta edellyttää erityisiä, tuomioistuinkontrollin alaisia menettelyjä. Nopeasti etenevissä tilanteissa tämä saattaa hankaloittaa tietoturvaloukkausten estämistä, koska kyseiset tilanteet voivat olla ohi nopeastikin. Normaalitilanteessa tiedonvaihtoon liittyvät rajoitteet ovat perustuslaillisista näkökohdista johtuen edelleen perusteltuja.

2.3 Virka-apusääntely

Virka-avulla tarkoitetaan viranomaisten toimintaa, jossa virka-apua antava viranomainen antaa virka-avun mahdollistavan lainsäädännön perusteella virka-apua sitä pyytävälle viranomaiselle sen lakisääteisen tehtävän hoitamiseksi. Lähtökohtaisesti kunkin viranomaisen on ylläpidettävä itse riittävää kyvykkyyttä viranomaiselle lain nojalla kuuluvien tehtävien suorittamiseksi. Virka-avussa on kyse viranomaisen toimivallan käyttämisestä toisen viranomaisen avustamiseksi tälle laissa säädetyn tehtävän toteuttamiseksi tavalla, joka ei virka-apua pyytävälle viranomaiselle ole mahdollista esimerkiksi erityistilanteessa toimivallan tai kyvykkyyden puutteen vuoksi.

Toimivalta virka-avun antamiseen ja oikeus sen saamiseen perustuvat erityissäännöksiin. Keskeiset virka-apusäännökset tietoturvaloukkausten selvittämisen ja ennalta ehkäisemisen kan-

nalta ovat SVPL:ssä, poliisilaissa ja Puolustusvoimista annetussa laissa. Lisäksi virka-apusäänte-lyä sisältyy TUVE-lakiin. Virka-avun antamista koskevien erityissäännöksien ohella hallinto-laissa säädetään viranomaisen yleisestä yhteistoimintavelvoitteesta.

Hallintolain 10 §:n nojalla viranomaisen on toimivaltansa rajoissa ja asian vaatimassa laajuu-dessa avustettava toista viranomaista tämän pyynnöstä hallintotehtävän hoitamisessa sekä muu-toinkin pyrittävä edistämään viranomaisten välistä yhteistyötä. Hallintolain tarkoittama yhteis-työ ei kuitenkaan tarkoita virka-apua, josta säädetään erikseen.

Hallintolain esitöissä (HE 72/2002 vp) erotetaan avustaminen ja virka-apu toisistaan siten, että avustamisella tarkoitetaan lähinnä hallintoasian selvittämisen ja ratkaisujen kannalta tarpeellis-ten lausuntojen ja selvitysten antamiseen niitä pyytäneelle viranomaiselle. Säännös ei sinällään edellytä yhteistyön perustuvan vireillä olevan asian käsittelyyn, vaan kyse voi olla myös asian vireilletuloa edeltävästä tai päätöksen antamisen jälkeisestä avustamisesta. Viranomaisyhteis-työn sisältöä tulisi tulkita laajasti siten, että se voisi kattaa erilaisia yhteistyön muotoja kirjallis-ista menettelyistä erilaisiin neuvotteluihin. Virka-avulla sen sijaan tarkoitetaan esitöiden mu-kaan tavanomaisesti sitä, että viranomainen avustaa toista tosiasiallisessa hallintotoiminnassa tai tosiasiallisessa julkisen vallan käyttöön kuuluvien virkatehtävien hoitamisessa, kuten edellä on kuvattu. Hallintolain esitöissä todetaan lisäksi, että viranomaisten yhteistyövelvoitteesta ei olisi johdettavissa yleistä tietojenantovelvollisuutta, vaan viranomaiset toimivat oman hallin-nonalansa tehtäviä täyttääkseen, omilla toimivaltuuksillaan ja oman salassapitovelvollisuutensa rajoissa.

Liikenne- ja viestintäviraston oikeudesta saada ja mahdollisuudesta antaa virka-apua säädetään SVPL 309 §:ssä. Liikenne- ja viestintävirastolla on SVPL 309 §:n 1 momentin nojalla oikeus saada virka-apua poliisilta, Tullilta ja Rajavartiolaitokselta lain ja sen nojalla annettujen sään-nösten ja määräysten noudattamisen valvomiseksi ja täytäntöön panemiseksi sekä Puolustus-voimilta radioviestinnän häiriöiden syiden selvittämiseksi. Edellä mainittujen virka-apusään-nösten ei ole katsottu ainakaan täysimääräisesti mahdollistavan virka-avun pyytämistä ky-berhäiriötilanteissa. SVPL 309 §:n 2 momentin nojalla Liikenne- ja viestintävirasto voi pyyn-nöstä antaa virka-apuna asiantuntija-apua toiselle viranomaiselle. Virka-avun antamisesta päät-tää liikenne- ja viestintäministeriö. SVPL 309 §:n 3 momentin nojalla Liikenne- ja viestintävi-raston virka-avun antaminen ei oikeuta antamaan toiselle viranomaiselle tietoja viesteistä, väli-tystiedoista tai sijaintitiedoista taikka luottamuksellisen radiolähetyksen sisällöstä ja olemassa-olosta.

Poliisilain 9 luvun 1 §:ssä säädetään poliisin antamasta virka-avusta. Poliisin on annettava virka-apua toiselle viranomaiselle, jos siitä on erikseen säädetty tai jos virka-apua tarvitaan laissa säädetyn valvontavelvollisuuden toteuttamiseksi silloin, kun viranomaista estetään hoita-masta valvontatehtävää. Päätöksen virka-avun antamisesta tekee päällystöön kuuluva poliisi-mies, jollei siitä ole erikseen säädetty.

Poliisilain 9 luvun 2 §:ssä säädetään poliisille annettavasta virka-avusta. Viranomaisen on an-nettava poliisille virka-apua poliisille kuuluvan tehtävän suorittamiseksi, jos viranomainen on toimivaltainen sen antamiseen. Päätöksen virka-avun pyytämisestä tekee päällystöön kuuluva poliisimies, jollei erikseen toisin säädetä tai asian kiireellisyys muuta vaadi. Puolustusvoimien virka-avusta poliisille säädetään erikseen Puolustusvoimien virka-avusta poliisille annetussa laissa, jota käsitellään jäljempänä.

Puolustusvoimista annetun lain 2 §:n 1 momentin 2 kohdan nojalla Puolustusvoimien tehtävänä on muun ohella muiden viranomaisten tukeminen, johon kuuluu virka-apu yleisen järjestyksen ja turvallisuuden ylläpitämiseksi, terrorismirikosten estämiseksi ja keskeyttämiseksi sekä

muuksi yhteiskunnan turvaamiseksi. Saman lain 11 §:n mukaan Puolustusvoimat voi antaa virka-apua yhteiskunnan turvaamiseksi siten kuin öljyvahinkojen torjuntalaissa (1673/2009) tai muussa laissa säädetään.

Puolustusvoimat voi antaa virka-apua myös muuksi yhteiskunnan turvaamiseksi Puolustusvoimista annetun lain 11 §:n nojalla. Lain esitöiden yksityiskohtaisten perusteluiden mukaan tällä tarkoitetaan, että Puolustusvoimat voi antaa virka-apua silloin kun yhteiskunnan turvaaminen edellyttäisi sellaista henkilöstöä, materiaalia ja osaamista, mitä Puolustusvoimilla on. Puolustusvoimat voi organisaationa antaa virka-apua Puolustusvoimien muihin tehtäviin kuulumattomaan tehtävään. Tämä vaatii kuitenkin, että virka-avusta on säädetty myös virka-avun vastaanottajaa koskevassa lainsäädännössä. Näin ollen esimerkiksi Liikenne- ja viestintäviraston Kyberturvallisuuskeskus voisi nykytilanteessa antaa Puolustusvoimille asiantuntija-apua virka-apuna SVPL 309 §:n nojalla, kun taas Puolustusvoimat ei voi antaa Liikenne- ja viestintävirastolle virka-apua kuin radioviestinnän häiriöiden syiden selvittämiseksi. Toisaalta Puolustusvoiminen oikeudesta saada virka-apua ei ole Puolustusvoimissa annetussa laissa erikseen säädetty.

Puolustusvoimien virka-avusta poliisille säädetään Puolustusvoimien virka-avusta poliisille annetussa laissa (342/2022, *virka-apulaki*). Lain 2 §:n mukaan poliisin on mahdollista saada virka-apua Puolustusvoimilta vain, jos se on poliisin voimavarojen riittämättömyyden vuoksi tarpeellista poliisille laissa säädetyn tehtävän suorittamiseksi ja se ei vaaranna Puolustusvoimien omien, Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdassa säädetyn tehtävän suorittamista. Virka-apulain 12 §:n mukaan poliisi vastaa virka-aputehtävän kannalta tarpeellisesta yleisjohtamisesta ja poliisin ja Puolustusvoimien toimintojen yhteensovittamisesta.

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain 90 §:ssä säädetään poliisin antamasta avusta ja yhteistoiminnasta poliisin kanssa rikosten ennalta estämisessä ja paljastamisessa. Kyse ei ole varsinaisesta virka-avusta vaan viranomaisen avustamisesta. Säännöksen mukaan poliisi voi suorittaa toimivaltaansa kuuluvan yksittäisen toimenpiteen, jos puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavilla ei ole toimivaltaa lain 86 §:n 1 momentissa tarkoitetun tehtävän hoitamiseksi. Asian laadun vaatiessa tehtävä suoritetaan yhteistoiminnassa poliisin kanssa. Tämä voi koskea joko yksittäisten toimivaltuuksien käyttöä tai koko kyseisen tehtäväkokonaisuuden toteuttamista yhdessä.

2.4 EU-lainsäädäntö ja unionin tuomioistuimen käytäntö

Euroopan unionin toiminnasta tehdyn sopimuksen 346 artiklan perusteella kansallisen turvallisuuden toimenpiteet on rajattu ulkopuolelle unionin toimivallasta, jolloin näistä tulee säätää kansallisesti. Tästä syystä unionin lainsäädäntöön sisältyy usein kansallista turvallisuutta koskevia poikkeuksia. Ehdotukseen liittyy kuitenkin myös EU-sääntelyä, joka on tarpeen ottaa huomioon.

2.4.1 NIS-direktiivi

Merkittävistä tietoturvaloukkauksista on annettu Euroopan parlamentin ja neuvoston direktiivi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa eli niin kutsuttu NIS-direktiivi. Direktiivissä säädetään muun muassa keskeisten palvelujen tarjoajien sekä digitaalisten palvelujen tarjoajia koskevasta turvallisuus- ja ilmoitusvaatimuksesta. NIS-direktiivin liitteessä II on määritelty toimialat ja toimialojen osa-alueet, jotka nähdään keskeisiksi palvelujen tarjoajiksi tietoturvaloukkaustilanteissa. Nämä toimijat on mielletty direktiivin kannalta sellaisiksi, jotka tarjoavat palvelua, joka on keskeinen yhteiskunnan ja/tai talouden kriittisten toimijoiden ylläpitämiseksi, palvelun tarjoaminen on

riippuvainen verkko- ja tietojärjestelmistä tai tietoturvapoikkeamalla olisi merkittäviä haitallisia vaikutuksia kyseisen palvelun tarjoamiseen.

Direktiivin mukaan eri toimialojen toimivaltaisten viranomaisten on tehtävä yhteistyötä tietoturvaloukkauksiin reagoiviin ja niitä tutkiviin yksiköihin (CSIRT). Suomessa CSIRT-toimija on Liikenne- ja viestintäviraston Kyberturvallisuuskeskus ja toimivaltaisia viranomaisia ovat Energiavirasto, Finanssivalvonta, Valvira, ELY-keskus, maa- ja metsätalousministeriö sekä Liikenne- ja viestintävirasto. Kriittisten palvelujen ja digitaalisten palvelujen tarjoajille on asetettu turvallisuusvaatimukset ja merkittävistä tietoturvapoikkeamista tulee ilmoittaa ilman aiheetonta viivytystä toimivaltaiselle viranomaiselle. Poikkeaman merkittävyyttä arvioitaessa tulee huomioida niiden lukumäärä, joihin palvelun häiriö vaikuttaa, poikkeaman kesto sekä maantieteellinen levinneisyys.

EU:n neuvosto ja parlamentti ovat päässeet toukokuussa 2022 alustavaan yhteisymmärrykseen uudesta kyberturvallisuusdirektiivistä (NIS2-direktiivi), joka tulee korvaamaan voimassa olevan NIS-direktiivin.

2.4.2 Sähköisen viestinnän tietosuojadirektiivi

Sähköisen viestinnän tietosuojadirektiivissä (2002/58/EY, *ePrivacy-direktiivi*) säädetään henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla. Direktiivin mukaan sähköisen viestinnän palveluiden välityksellä tapahtuva viestintä ja siihen liittyvät liikennetiedot ovat luottamuksellisia. Erityisesti on kiellettävä se, että muut henkilöt ilman käyttäjän suostumusta kuuntelevat, salakuuntelevat, tallentavat tai muulla tavalla sieppaavat tai valvovat viestintää ja siihen liittyviä tietoja, jollei se ole laillisesti sallittua direktiivin 15 artiklan 1 kohdan mukaisesti. Kyseisen kohdan mukaan jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan tämän direktiivin 5 artiklassa, 6 artiklassa, 8 artiklan 1, 2, 3 ja 4 kohdassa sekä 9 artiklassa 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 direktiivin 95/46/EY 13 artiklan 1 kohdan mukaisesti.

Unionin tuomioistuimen ePrivacy-direktiivin tulkintaa koskevassa oikeuskäytännössä on korostettu viestinnän luottamuksellisuutta osana unionin perusoikeuskirjan 7 artiklan mukaista yksityiselämän kunnioittamisen sekä 8 artiklan mukaista henkilötietojen suojaa. Oikeuskäytännön mukaisesti ainoastaan vakavan rikollisuuden torjumista tai yleiseen turvallisuuteenkohdistuvien vakavien uhkien ehkäisemistä koskevilla tavoitteilla voidaan perustella se, että viranomaisille annetaan tätä koskevan 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 rajataan täysin välttämättömään (tuomio 5.4.2022 Comissioner of an Garda Síochána ym. C-140/20 110 kohta tuomio 21.12.2016, Tele2 Sverige ja Watson ym., C-203/15 ja C-698/15, EU:C:2016:970, 99 ja 118 kohta, tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 54 kohta, tuomio 2.3.2021, Prokuratuur, C-746/18, EU:C:2021:152, 35 kohta). Edellä mainittujen edellytysten noudattamisen varmistamiseksi on katsottu olennaiseksi, että viranomaisten tietojensaanti edellyttää riippumattoman hallinnollisen toimielimen, kuten tuomioistuimen, etukäteisvalvontaa. (tuomio 6.10.2020, La Quadrature du Net ym., C-511/18, C-512/18 ja C-520/18, EU:C:2020:791, 189 kohta ja Prokuratuur, 51 kohta).

2.4.3 Yleinen tietosuoja-asetus

EU:n yleisessä tietosuoja-asetuksessa (EU) 2016/679 (jäljempänä *TSA*) säädetään luonnollisten henkilöiden henkilötietojen käsittelystä ja niiden tietojen vapaasta liikkuvuudesta. Asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista sekä sellaiseen henkilötietojen käsittelyyn muussa kuin automaattisessa muodostaa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa. Alueellisesti asetusta sovelletaan henkilötietojen käsittelyyn unionin alueella sijaitsevan rekisterinpitäjän tai käsittelijän toiminnan yhteydessä. Lisäksi asetusta sovelletaan unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn, vaikka rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittunut unioniin, jos käsittely liittyy rekisteröidyn käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa. Viranomaisten välillä vaihdettavat tiedot, jotka katsotaan henkilötiedoiksi, kuuluvat siten lähtökohtaisesti asetuksen soveltamisalaan.

Asetuksen 5 artiklan mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi ja ne on kerättävä tiettyä nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla (käyttötarkoitussidonnaisuus). Käsittelyn on asetuksen 6 artiklan mukaan laillista muun muassa, jos se on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi tai rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi. Lisäksi lainmukaisuuden vaatimus täyttyy, jos käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi. Silloin, kun käsittely tapahtuu yleistä etua koskevan tehtävän suorittamiseksi, käsittelyn perustasta on säädettävä joko unionin oikeudessa tai rekisterinpitäjään sovellettavassa jäsenvaltion lainsäädännössä.

Olennaista viranomaisten välisen tiedon vaihdon kannalta merkittävien tietoturvaloukkausten tilanteessa on tiedonkäsittely muuta kuin alkuperäistä tarkoitusta varten. Asetuksen 6 artiklan 4 kohdan mukaan on ensinnäkin huomioitava 23 artiklan 1 kohdassa asetetut tavoitteet ja lisäksi on huomioitava, että muuhun tarkoitukseen tapahtuva käsittely on yhteensopivaa sen tarkoituksen kanssa, jota varten tiedot alun perin kerättiin. Huomioitavina seikkoina ovat henkilötietojen keruun tarkoitusten ja aiotun myöhemmän käsittelyn tarkoitusten väliset yhteydet henkilötietojen keruun asiayhteys erityisesti rekisteröityjen ja rekisterinpitäjän välisen suhteen osalta, käsitelläänkö erityisiä henkilötietoryhmiä tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja, aiotut myöhemmät seuraamukset rekisteröidylle ja asianmukaiset suojatoimet.

Asetuksen 23 artiklan 1 kohdan mukaan rekisterinpitäjään tai henkilötietojen käsittelijään sovellettavassa unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan lainsäädäntötoimenpiteellä rajoittaa asetuksessa säädettyjä oikeuksia ja velvollisuuksia, kuten 5 artiklassa tarkoitettua käyttötarkoitussidonnaisuutta ja säädettyjen velvollisuuksien ja oikeuksien soveltamisalaa, jos kyseisessä rajoituksessa noudatetaan keskeisiltä osin perusoikeuksia ja –vapauksia ja se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhtainen toimenpide, jotta voidaan taata muun muassa kansallinen turvallisuus, puolustus, yleinen turvallisuus tai rikosten ennalta estäminen, tutkinta, paljastaminen. Artiklan 2 kohdassa on lueteltu seikkoja, jotka tulee tarpeen mukaan huomioitavaksi edellä mainittuja lainsäädäntötoimenpiteitä tehtäessä.

2.4.4 Rikosasioiden tietosuojadirektiivi

Yleisen tietosuoja-asetuksen ohella esityksen kannalta on huomioitava Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680 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 eli rikosasioiden tietosuojadirektiivi. Direktiivi ja yleinen tietosuoja-asetus muodostavat yhdessä niin sanotun tietosuojapaketin, joka muodostaa voimassa olevan EU:n tietosuojalainsäädännön yhdessä ePrivacy-direktiivin kanssa. Rikosasioiden tietosuojadirektiivi on kansallisesti pantu täytäntöön rikosasioiden tietosuojalailla.

Rikosasioiden tietosuojadirektiivin tarkoituksena on varmistaa henkilötietojen suoja direktiivin soveltamisalalla sekä helpottaa tietojen vapaata liikkuvuutta jäsenvaltioiden poliisi- ja oikeusviranomaisten välillä. Rikosasioiden tietosuojadirektiivissä on yleisten säännösten lisäksi säännökset yleisistä periaatteista, rekisterinpitäjästä, henkilötietojen käsittelijästä, henkilötietojen siirtämisestä kolmansiin maihin tai kansainvälisille järjestöille, valvontaviranomaisista, yhteistyöstä, oikeussuojakeinoista, vastuusta sekä seuraamuksista.

2.5 Nykytilan arviointi

Viranomaisten yhteistoiminnalla tietoturvaloukkaustilanteissa on tavanomaisissa tilanteissa olemassa varsin vakiintuneet menettelyt ja pääsääntöisesti viranomaiset kokevat yhteistyön toimivan monelta osin melko hyvin. Kuten edellä viranomaisten tehtäviä koskevan arvioinnin yhteydessä on todettu, viranomaisten tehtävät ovat jossain määrin limittäiset erityisesti tietoturvaloukkausten selvittämiseen liittyen ja niiden hoitamiseen sovelletaan samankaltaisia menetelmiä viranomaisesta riippumatta, mutta selvittämisen tavoite ja tarkoitus vaihtelevat. Myös tilannekuvan ja tilannetiedon tuottamisen osalta on osin vastaavan kaltaista lomittaisuutta.

Viranomaisten välistä tiedonvaihtoa koskevassa sääntelyssä normaalitilanteessa ei ole vakavia puutteita. Joitakin luottamuksellisen viestin suojan kannalta tarkoituksenmukaisia rajoitteita liittyy Liikenne- ja viestintäviraston oikeuteen luovuttaa viestiin, välitystietoihin, sijaintitietoihin sekä luottamuksellisen radiolähetyksen sisältöön tai olemassaoloon liittyvä tietoja erityisesti poliisin tai Puolustusvoimien suuntaan silloin, kun niihin ei suoraan kohdistu tietoturvaloukkausta tai –uhkaa. Toinen Puolustusvoiminen ja poliisin sisäistä tiedonvaihtoa rajoittava tekijä on niin sanottu palomuurisääntely rikostorjunnan ja tiedustelutoiminnan välillä. Myös tämä sääntely on perusteltua perustuslaillisista, oikeusturvaan ja myös viestinnän luottamuksellisuuden suojaan tietoverkkoympäristössä tapahtuvan toiminnan osalta palautuvista lähtökohdista. Nykysääntelystä kuitenkin jossain määrin aiheutuu haasteita teknisen tason tilannekuvan muodostamisen kannalta normaalioloissakin, koska esimerkiksi välitystiedot ovat salassapidon piirissä. Toisaalta voimassa olevan sääntelyn ei katsota toimivan parhaalla mahdollisella tavalla sellaisissa vakavissa tilanteissa, joissa viranomaisilta edellytettäisiin nopeaa ja yhteistyössä toteutettavaa reagointia vakavaan tietoturvaloukkaustilanteeseen.

Tiedon luovuttamisesta on siten osin säännelty, mutta luovuttamiselle on asetettu eritasoisia kynnyksiä ja käyttötarkoituksia, mikä aiheuttaa haittaa käytännön tilanteissa erityisesti silloin, kun sääntely ei ole yhteismitallista, johdonmukaista tai kattavaa. Epäselvyyttä voi aiheuttaa se, missä määrin kyseessä olevia tietoja voidaan luovuttaa varsinkin, kun molemmilla osapuolilla sinällään voi olla oikeus saada käsitellä kyseisiä tietoja. Nykyinen tiedonvaihtosääntely on lisäksi jossakin määrin rakentunut kaksinkertaiseksi siten, että säädetään erikseen viranomaisten oikeudesta saada tiettyjä tietoja ja toisaalta viranomaisten oikeudesta luovuttaa tietoja. Tällainen sääntely on perustuslakivaliokunnankin näkökulmasta omiaan synnyttämään tulkintaongelmia, vaikka se ei varsinaisesti olekaan valtiosääntöoikeudellisesti ongelmallista (PeVL 71/2014 vp, s. 3).

Tulkinnallista epäselvyyttä ovat aiheuttaneet henkilötietojen luovuttamiseen liittyvät kysymykset. Osa viranomaisten välillä vaihdettavista, erityisesti teknisemmän tason tiedoista, kuten välitystiedot, katsotaan usein henkilötiedoiksi, koska niiden perusteella henkilö on tietyillä edellytyksillä tunnistettavissa. Tällaisissa tilanteissa jossain määrin epäselväksi on muodostunut,

miten tällaisia tietoja viranomaisten välillä voidaan luovuttaa yleisen tiedonluovuttamista koskeva sääntelyn nojalla varsinkin, jos tietoa käytetään yleisen tietosuoja-asetuksen tarkoittamassa mielessä muuhun kuin alkuperäiseen käyttötarkoitukseen, mikä tietosuoja-asetuksen nojalla edellyttää lailla säätämistä. Osa poliisin ja Puolustusvoimien tehtävistä kuuluu myös rikosasioiden tietosuojalainsäädännön piiriin, jonka lisäksi poliisilla ja Puolustusvoimilla on omat henkilötietolakinsa, jotka osaltaan täydentävät sekä yleistä tietosuoja-asetusta että rikosasioiden tietosuojalakia, mikä on omiaan tekemään sovellettavasta henkilötietolainsäädännöstä epäselvän. Lisäksi tietoturvaloukkausten selvittämisen yhteydessä usein käytetään IP-osoitteita loukkausten lähteiden selvittämiseksi. Tulkinta, jonka mukaan IP-osoitteet tulkitaan lähtökohtaisesti henkilötiedoiksi, on kuitenkin joissakin tapauksissa ongelmallinen, koska kaikki IP-osoitteet eivät ole yksittäisen henkilön käytössä vaan kyse voi olla muun muassa verkkolaitteiden IP-osoitteista tai internet-sivuston käyttämästä IP-osoitteesta, jolloin kyseessä ei olisi henkilötieto Henkilötietokysymys liittyy osittain myös siihen, että välitystiedon käsitteeseen liittyy myös tulkinnanvaraisuutta.

Virka-apusääntelyn osalta menettelyt erityisesti poliisin ja Puolustusvoimien välillä ovat vakiintuneet perinteiseen fyysiseen toimintaan liittyen. Kybertoimintaympäristön osalta tilanne ei ole toistaiseksi vielä vastaavalla tavalla vakiintunut. Lisäksi on huomioitava, että Puolustusvoimille ei ole säädetty Puolustusvoimista annetussa laissa oikeutta vastaanottaa virka-apua toiselta viranomaiselta. Myös Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselta pyydetään virka-apuna asiantuntija-apua muiden viranomaisten tehtävien suorittamisen tukemiseksi. Liikenne- ja viestintäviraston mahdollisuus antaa virka-apua on kirjattu lainsäädäntöön yleisluonteisesti, eikä sen voi katsoa aiheuttavan rajoitteita virka-avun pyytämiselle. Sen sijaan Liikenne- ja viestintäviraston mahdollisuus saada virka-apua esimerkiksi vakavien tietoturvaloukkausten selvittämiseen, jossa viraston omat resurssit loppuisivat kesken, on puutteellista. Suomessa tällaista kyvykkyyttä on Liikenne- ja viestintäviraston lisäksi tällä hetkellä poliisilla, suojelupoliisilla ja Puolustusvoimilla. Jatkossa olisi tarpeellista laajentaa viraston oikeutta pyytää virka-apua mainituilta viranomaisilta tietoturvaloukkaustilanteissa.

Tulkinnallista epäselvyyttä on liittynyt viestinnän välittäjien oikeuteen luovuttaa oma-aloitteisesti tietoturvaloukkauksia koskevia viestejä ja välitystietoja Liikenne- ja viestintävirastolle. Teleyrityksien osalta ilmoitusvelvollisuus on olemassa merkittävissä tietoturvaloukkaustilanteissa, mutta pienempiin loukkauksiin tätä ei voida soveltaa, vaikka niistä saatavalla tiedolla voitaisiin mahdollisesti myös ehkäistä tietoturvaloukkauksia. Sääntely kohdistuu lisäksi vain teleyrityksiin, kun viestinnän välittäjiä ovat muutkin toimijat, joiden osalta olisi tarkoituksenmukaista mahdollistaa tiedon luovutus tietoturvaloukkausten ehkäisemiseksi.

Yksittäisinä huomioina nykyiseen lainsäädäntöön sisältyy myös Liikenne- ja viestintäviraston toimintaan liittyviä päätöksentekoprosesseja, kuten virka-apupäätöksien tekeminen ja tietoturvaloukkauksia koskevien tietojen luovuttaminen muiden maiden tietoturvasta vastaaville viranomaisille. Menettelyjä olisi tarpeen keventää siten, että liikenne- ja viestintäministeriön sijaan virasto itse päättäisi kyseisistä toimenpiteistä.

Lainsäädännön asettamien rajoitteiden lisäksi jonkin verran haasteita voi aiheuttaa henkilöstön tiedon taso siitä, mitä tietoa olisi luovutettavissa ja millä perusteella. Näihin seikkoihin on kiinnitettävä erityistä huomiota henkilöstön koulutuksessa.

Nykytilaan liittyy myös isompia kysymyksiä esimerkiksi viranomaisten toimivaltuuksiin ja velvollisuuksiin liittyen, joita ei arvioida tarkemmin tämän hankkeen puitteissa. Nämä tulevat kuitenkin osaltaan arvioiduksi sisäministeriön ja puolustusministeriön käynnistämässä laajemmassa selvityshankkeessa, jossa arvioidaan viranomaisten toimintaedellytyksiä kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa ja kyberpuolustuksessa.

3 Tavoitteet

Esityksen tavoitteena on parantaa yhteiskunnan turvallisuutta ja perusoikeuksien, erityisesti luottamuksellisen viestinnän suojan, toteutumista parantamalla viranomaisten toimintaedellytyksiä sellaisten tietoturvaloukkausten selvittämisessä, joiden haitalliset vaikutukset voivat vakavissa tilanteissa kohdistua laajalle yhteiskunnan toiminnan kannalta keskeisiin toimintoihin. Hallituksen esityksen tavoitteena on parantaa viranomaisten yhteistoimintaa virka-apusääntelyä ja tiedonvaihtoa kehittämällä merkittävien ja vaikutuksiltaan vakavien tietoturvaloukkausten ja -uhkien selvittämisessä ja niiden vaikutusten poistamisessa.

Esityksen tavoitteena on luoda selkeät edellytykset viranomaisten tiedonvaihdolle vakavissa tietoturvaloukkaustilanteissa säätämällä loukkausten selvittämisen kannalta keskeisten viranomaisten 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.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

Esityksen keskeisin ehdotus koskee viranomaisten keskinäistä tiedonvaihtoa merkittävissä tietoturvaloukkaustilanteissa tai niiden vakavissa uhkissa, joissa vaikutukset kohdistuisivat yhteiskunnan toiminnan kannalta keskeisiin toimintoihin. Ehdotus olisi yksittäistapauksia koskeva uusi tiedonvaihtosäännös, jota sovellettaisiin edellä mainituissa, vakavissa tilanteissa. Sääntely on tarkoituksenmukaista rakentaa yksittäistapauksia koskevan, normaalista tiedonvaihtosääntelystä poikkeavan sääntelyn varaan, koska normaalitilanteissa tiedonvaihtoa koskevat rajoitukset ovat perusteltuja erityisesti luottamuksellisen viestin suojaan kohdistuvan perusoikeussuojan vuoksi.

Virka-apusääntelyä ehdotetaan täydennettäväksi Liikenne- ja viestintäviraston saaman virka-avun osalta sellaisilta viranomaisilta, joilla on käytännössä kyvykkyyttä tietoturvaloukkausten tai uhkien selvittämiseksi. Näitä viranomaisia ovat poliisi, suojelupoliisi ja Puolustusvoimat. Vaikka virka-apumenettely mielletään jossakin määrin raskaaksi menettelyksi muun viranomaisyhteistyön rinnalla, on tästä kuitenkin tarpeen säätää poikkeuksellisia tilanteita varten, jotta lainsäädäntö ei muodostu esteeksi virka-apua tarvitsevan viranomaisen tehtävän hoitamisessa.

Liikenne- ja viestintäviraston virka-apupyynnön käsittelyä ehdotetaan kevennettäväksi siten, että jatkossa virasto itse päättäisi virka-avun antamisesta liikenne- ja viestintäministeriön sijaan. Vastaava muutos päätöksentekoprosessiin ehdotetaan tehtäväksi luovutettaessa tietoja muussa valtiossa toimivalle viranomaiselle tai muulle vastaavalle taholle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja –palveluihin kohdistuvia tietoturvaloukkauksia. Lisäksi tietoja voitaisiin jatkossa luovuttaa myös EU:n ja Pohjois-Atlantin liitto Naton tietoturvaloukkauksia selvittäville toimielimille.

Esityksessä ehdotetaan myös lisättäväksi uusi säännös viestinnän välittäjän oikeudesta vapaaehtoisesti luovuttaa tietoa viesteistä ja välitystiedoista Liikenne- ja viestintävirastolle, jos tiedon luovuttaminen olisi tarpeen tietoturvaloukkausten tai –uhkien selvittämiseksi taikka ennalta ehkäisemiseksi.

Henkilötietojen käsittelystä poliisitoimesta annettua lakia ja henkilötietojen käsittelystä Puolustusvoimissa annettua lakia ehdotetaan täsmennettäväksi lähinnä selkeyttävillä säännöksillä siitä,

että Liikenne- ja viestintävirastolle voitaisiin sen tiettyjä tietoturvaloukkauksia koskevia tehtäviä varten luovuttaa henkilötietoja. Säännöksillä ei kuitenkaan ole huomattavaa merkitystä käytännön tilanteissa, vaan kyse on lainsäädännön yhdenmukaistamisesta ja selkeyttämisestä tulkinnanvaraisuuksien välttämiseksi.

4.2 Pääasialliset vaikutukset

4.2.1 Vaikutukset viranomaisten toimintaan

Esityksen keskeiset suorat vaikutukset kohdistuvat viranomaisten keskinäisiin suhteisiin, menettelytapoihin sekä hallinnollisiin menettelyihin merkittävissä tietoturvaloukkauksissa ja uhkissa. Kokonaisvaikutus viranomaisten toimintaan arvioidaan vähäiseksi, sillä ehdotettu tiedonvaihtosääntely viranomaisten välillä tullee sovellettavaksi vain poikkeuksellisissa tilanteissa, mikäli niiden määrä ei merkittävästi nousisi. Esityksessä ehdotetaan parannettavan viranomaisten yhteistoiminnan mahdollisuuksia tiedonvaihtoa tehostamalla. Ehdotuksen voidaan katsoa helpottavan ja selkeyttävän viranomaisten välistä vuorovaikutusta ja nopeuttavat toimintaa näissä tilanteissa. Selkeä oikeus tiedonvaihtoon viranomaisten välillä nopeuttaa viranomaisten mahdollisuuksia reagoida merkittäviin tietoturvaloukkauksiin.

Valmistelun aikana käytiin viranomaisten välillä ehdotuksen mukainen tiedonvaihtoharjoitus, jossa arvioitiin ehdotuksen soveltuvuutta käytäntöön. Harjoituksen yhtenä tuloksena todettiin, että tiedon vaihtamisen kynnysarvon ylittämisen arviointi saattaa osoittautua käytännössä haastavaksi varsinkin, kun kokonaiskuva tietoturvaloukkauksesta ja sen merkittävyydestä voi voi muodostua monesti vasta tietoja vaihtamalla. Niitä ei kuitenkaan voisi vaihtaa ennen edellytysten arviointia, joka perustuu niiden yhdistämiseen.

Ehdotus ei suoraan vaikuta viranomaisten tehtäviin sellaisina kuin ne on tällä hetkellä säädetty. Viranomaisten tehtäviin vähäisesti vaikuttava muutos liittyy Puolustusvoimien, poliisin ja suojelupoliisin antamaan virka-apuun Liikenne- ja viestintävirastolle. Poliisin ja Puolustusvoimien osalta tämä mahdollisuus on vain jossakin määrin uusi, koska virasto on voinut saada näiltä viranomaisilta virka-apua myös tähän asti. Käytännössä tähän mennessä Liikenne- ja viestintävirasto ei ole pyytänyt muilta viranomaisilta tietoturvaloukkauksiin liittyvää virka-apua eli oletettavasti vaikutukset tässä suhteessa tulevat jäämään vähäisiksi. Normaalin yhteistyön viranomaisten välillä on tarkoitus jatkua samaan tapaan kuin tähänkin asti.

Laajemman viranomaiskentän erityisosaamisen hyödyntäminen voidaan olettaa parantavan tietoturvaloukkausten ja -uhkien hallintaa ja analysointia, mikä toisaalta antaa hyökkäyksen kohteella olevalle taholle paremmat edellytykset hankkia tilanteen korjaamiseksi tarvittavat palvelut. Tietoturvan osalta korostuu myös henkilöstön osaaminen, mikä etenkin erityisissä teknistä osaamista vaativissa tapauksissa voi olla vain muutamilla henkilöillä Suomessa tai jopa koko maailmassa.

Ehdotuksessa on mukana kaksi päätöksentekoprosesseihin kohdistuvaa muutosta, joiden tarkoituksena on keventää hallinnollisia menettelyjä Liikenne- ja viestintävirastossa. Hallinnollisia menettelyitä keventävät ehdotukset siitä, että liikenne- ja viestintäministeriö ei enää päättäisi Liikenne- ja viestintäviraston antamasta virka-avusta tai tietojen luovuttamisesta ulkomaisille tietoturvaloukkausten selvittämisen kannalta toimivaltaisille viranomaisille.

Ehdotuksella pyritään turvaamaan merkittävissä tietoturvaloukkaustilanteissa tai tietoturvauhkassa muun muassa julkisen vallan päätöksentekokykyyn vaikuttavat toiminnot ja viranomaisten toimintaedellytykset. Viranomaisten yhteistoiminnan edistämisen uhkiin toteutumisen ehkäisyssä ja toisaalta jo havaittujen loukkausten osalta voidaan arvioida vaikuttavan positiivisesti

julkisen vallan päätöksentekokykyyn myös vakavissa tietoturvaloukkaustilanteissa. Vaikutusten arvioidaan olevan vastaavanlaiset myös muuhun viranomaistoimintaan.

Ehdotus viestinnän välittäjän oikeudesta luovuttaa välitystietoja ja tietoja viesteistä Liikenne- ja viestintävirastolle parantaa viraston edellytyksiä selvittää ja ennalta ehkäistä tietoturvaloukkauksia sekä mahdollistaa kattavamman tilannekuvan muodostamisen. Säännöksellä on siten vaikutusta myös päivittäiseen toimintaan. Lausunnossa esitetyn näkemyksen perusteella on mahdollista, että viestinnän välittäjän kynnys tiedon luovuttamiselle nousee, koska viranomainen saattaisi ryhtyä tutkimaan, onko SVPL:n mukainen käsittelyoikeus kyseiselle tiedolle syntynyt. Tämä saattaa olla haaste erityisesti pk-yrityksille.

4.2.2 Taloudelliset vaikutukset

Esityksellä arvioidaan olevan vähän taloudellisia vaikutuksia. Liikenne- ja viestintäviraston tekemien virka-apupyyntöjen mahdollisuuden laajentaminen poliisin, suojelupoliisin ja Puolustusvoimien osalta aiheuttaisi toteutuessaan jonkin verran kustannuksia julkiseen talouteen, mutta kyse olisi tuolloinkin vain kertaluonteisista ja vähäisiksi arvioiduista kustannuksista. Virka-apu olisi asiantuntija- tai laiteapua, jolloin kustannukset rajoittuisivat käytännössä näihin toimintoihin. Virka-avun pyytäjä vastaisi virka-avusta aiheutuvista kustannuksista talousarvion nykyisten määrärahojen puitteissa. Virka-avun määrän ei odoteta kasvavan esityksen johdosta merkittävästi.

4.2.3 Yritysvaikutukset

Ehdotuksenmukaista tiedonvaihtosääntelyä sovellettaisiin yhteiskunnan toiminnan kannalta keskeisiin toimintoihin kohdistuvissa tietoturvaloukkaustilanteissa. Monet tällaiset toiminnot ovat yksityisten toimijoiden tuottamia. Viranomaisten puuttumiskyvykkyyden ja yhteistoiminnan parantaminen merkittävien tietoturvaloukkausten ehkäisemisessä, selvittämisessä ja jossain määrin myös vaikutuksien poistamisessa osaltaan rajoittaa tietoturvaloukkauksista aiheutuvien haitallisten kustannusten syntymistä. Vaikutusten poistamisen osalta viranomaisten toiminnan vaikutus yritystoimintaan on jossakin määrin rajallinen, koska vastuu näistä on usein toimijalla itsellään. Viranomainen voi kuitenkin tukea yrityksiä tällaisissa tilanteissa. Viranomaisten laajempi tiedonvaihto parantaa tilannetietoisuutta, mikä edesauttaa niitä toimimaan paremmin myös suhteessa hyökkäyksen kohteeksi joutuneeseen yritykseen.

Ehdotuksella arvioidaan olevan vaikutuksia yrityksiin lähinnä niissä tilanteissa, joissa merkittävä tietoturvaloukkaus tai sen vakava uhka kohdistuisi yhteiskunnan toiminnan kannalta keskeiseksi katsotun yrityksen toimintaan. Lausuntokierroksella saatujen näkemysten perusteella vaikutukset saattavat vaihdella voimakkaasti riippuen siitä, mistä toimialasta on kyse. Elinkeinoelämän keskusliitto on todennut, että vaikutukset olisivat todennäköisesti merkittäviä erityisesti telekommunikaatio- ja finanssisektorilla sekä muilla kriittisimmillä toimialoilla. Toisaalta näillä toimialoilla yhteistyö on vahvasta sääntelystä johtuen jo nykyiselläänkin melko säännöllistä ja toimivaa.

Tietoturvaloukkaustilanteissa viranomaisten paremmat toimintamahdollisuudet voidaan arvioida yritysten kannalta pääosin positiivisena, jolloin mahdollisen tietoturvauhkan realisoituminen pystytään parhaassa tapauksessa estämään ja viranomaiset voivat tukea yrityksiä tietoturvaloukkausten vaikutusten poistamisessa. Tietoturvaloukkauksista aiheutuneita kustannuksia on vaikea arvioida, mutta edellä esitetyn ohella esimerkiksi kiristyshaittaohjelmista voi aiheutua yrityksille miljoonien eurojen tappiot, mikäli pyydetyt lunnaat maksetaan tai toiminta keskeytyy. Dataa tuhoavien haittaohjelmien vaikutukset yrityksiin voivat olla toiminnan kannalta vieläkin lamauttavampia erityisesti, jos yrityksen toiminta suurelta osin perustuu tietojärjestelmien

toimintaan ja tietojärjestelmissä olevaan dataan. Ehdotuksella tavoiteltaisiin tietoturvaloukkauksista aiheutuvien haitallisten vaikutusten vähentämistä parantamalla viranomaisten kyvykkyyttä ja yhteistoimintaa merkittäviin ja vakavia haitallisia vaikutuksia omaaviin tietoturvaloukkauksiin puuttumiseksi ja niiden uhkien ehkäisemiseksi.

Tietoturvaongelmien ja niistä aiheutuvien toimintahäiriöiden kokonaiskustannuksia on arvioitu muun muassa Tietoturvan ja tietosuojan parantamista yhteiskunnan kriittisillä toimialoilla arvioineen työryhmän loppuraportissa (Liikenne- ja viestintäministeriön julkaisuja 2021:1, s. 52–54). Tietoturvan ja tietosuojan murtuminen kriittisillä toimialoilla aiheuttaa monenlaisia kustannuksia, sillä yritystason kustannusten lisäksi kustannuksia aiheutuu yhteiskunnalle laajemmin esimerkiksi keskinäisriippuvuuksien kautta. Pienten ja keskisuurten yritysten tietomurtojen kokonaiskustannukset vuonna 2015 olivat Yhdysvalloissa noin 50 000 dollaria. Sen sijaan suurilla, yli 1500 henkilöä työllistävillä, yrityksillä kokonaiskustannukset olivat noin 620 000 dollaria. Siirryttäessä yritysvaikutuksista kansantalouden tasolla kriittisten toimialojen toimintaan kohdistuviin häiriöihin, kustannusvaikutukset voivat kasvaa kymmenien miljoonien tai miljardien eurojen suuruusluokkaan (Ronikonmäki, Niko-Matti – Sirviö, Tom Henrik: Taloustieteellisiä näkökulmia kyberturvallisuuteen. Kansantaloudellinen aikakausikirja – 117 vsk 2/2021, s. 268). Vuoteen 2015 nähden toiminta on lisäksi edelleen laajentunut ja ammattimaistunut, minkä vuoksi vaikutukset voivat tällä hetkellä olla jo edellä esitettyä huomattavasti laajemmat. Tarkkoja kokonaistilastoja tietoturvaloukkauksista on ylipäätään vaikea saada, koska monesti esimerkiksi mainehaitan pelossa loukkauksista ei ilmoiteta viranomaisille.

Liikenne- ja viestintävirastolle luovutettuja välitystietoja ja viestin sisältöä koskevia tietoja koskee salassapitovelvollisuus, johon nyt ehdotetaan tehtäväksi poikkeusta. Salassapitoa on pidetty luottamuksellisen viestinnän suojan ja toiminnan kannalta keskeisenä. Ehdotuksen mukaisessa tilanteessa tietoturvaloukkauksia tai -uhkia koskevia tietoja voitaisiin luovuttaa poliisin, suojelupoliisin, Puolustusvoimien ja Liikenne- ja viestintäviraston välillä aiempaa laajemmin esityksen mukaisissa vakavissa tilanteissa, joissa yhteiskunnan turvallisuus uhkaa vaarantua. Ehdotus sinällään asettaisi rajoituksia viranomaiselle luovutetun tiedon luottamuksellisuudelle ja esimerkiksi tietoturvaloukkauksen uhritieto saattaa monissa tilanteissa aiheuttaa herkkyyksiä erityisesti mainehaitan vuoksi. Ottaen huomioon tällaisten tilanteiden poikkeuksellisuus ja toisaalta vakavuusaste, voidaan arvioida, että ehdotus ei merkittävästi vaikuttaisi yritysten luottamukseen viranomaisten ja erityisesti Kyberturvallisuuskeskuksen toimintaa kohtaan, johon vapaaehtoisia ilmoituksia tehdään. Sinällään ehdotus ei vaikuta yleisesti tiedon salassa pidettävyyteen eli salassa pidettäväksi säädetty tieto on sitä myös vastaanottavassa viranomaisessa.

4.2.4 Vaikutukset kansalaisten asemaan yhteiskunnassa

Ehdotuksen vaikutuksia voidaan arvioida kohdistuvan myös kansalaisten asemaan ja erityisesti yksityiselämän suojaan. Tietoturvaloukkauksilla sinällään voi olla yritysten lisäksi laajamittaisia vaikutuksia myös tavallisiin kansalaisiin ja kotitalouksiin, joiden tiedot ovat esimerkiksi olleet osana jotain isompaa tietojärjestelmää, joka on joutunut tietoturvaloukkauksen kohteeksi. Tuolloin riskinä on, että järjestelmissä olevia arkaluonteisia tietoja vuodettaisiin julkisuuteen tai niitä käytetään hyväksi muilla tavoin. Viranomaistoiminnan tehostamisella vakavissa tilanteissa parannetaan mahdollisuuksia tietoturvaloukkausten selvittämiseen, syyllisten kiinni saamiseen ja parhaassa tapauksessa niiden ennalta ehkäisemiseen, mikäli merkittävä tietoturvauhka voidaan havaita riittävän varhaisessa vaiheessa. Ehdotus parantaisikin välillisesti kansalaisten ja kotitalouksien asemaa parantamalla viranomaisten toimintakykyä puuttua ja selvittää sellaisia merkittäviä tietoturvaloukkauksia, joista voisi olla merkittäviä haittoja kansalaisille ja kotitalouksille yhteiskunnassa.

Ehdotus mahdollistaa aikaisempaa laajemman viestinnän välittäjien oikeuden luovuttaa tietoja Liikenne- ja viestintävirastolle välitystiedoista ja viestien sisällöstä. Tällä on vaikutusta kansalaisten yksityisyyden suojaan ja luottamuksellisen viestinnän suojaan. Viestien sisältö on viestinnän luottamuksellisuuden ytimessä. Muutoksen vaikutus tässä suhteessa ei kokonaisuutena arvioiden ole erityisen merkittävä, koska Kyberturvallisuuskeskuksella on tälläkin hetkellä oikeus pyytää tietoturvaloukkauksia koskevia tietoja ja toisaalta esimerkiksi haittaohjelmia sisältävät viestit eivät ole viestinnän luottamuksellisuuden olennaisin ydin, joten tältä osin vaikutus arvioidaan kokonaisuudessaan kuitenkin vähäiseksi. Kokonaisuudessaan ehdotus kuitenkin välillisesti parantaisi viestinnän luottamuksellisuutta tietoturvaloukkauksien ennaltaehkäisyn kautta.

4.2.5 Vaikutukset rikostentorjuntaan ja turvallisuuteen

Ehdotuksen arvioidaan vaikuttavan kansallista turvallisuutta parantavasti ja edistävän kyberrikollisuuden torjuntaa. Yhteistoiminnasta tähän mennessä saatujen kokemusten perusteella tiedonvaihtoon sisältyy joitakin haasteita, jotka voisivat vakavimmissa ja nopeita toimenpiteitä vaativissa tilanteissa vaikeuttaa tilanteen kokonaisvaltaista hallintaa ja havainnointia viranomaisten kesken. Sääntelyn selkeyttämisellä näissä tilanteissa helpotettaisiin viranomaisten yhteistoimintaa. Yhteiskunnan turvallisuustilanteen muuttuessa on ennakoitava mahdollisia vakavia tietoturvatilanteita ja ehdotuksella pyritään vastaamaan näihin haasteisiin.

Koska yhteiskunnan toiminta nojaa nykyisellään huomattavassa määrin verkkoyhteyksien ja tietojärjestelmien varaan ja ne sisältävät myös huomattavan määrän sekä yksityisiä että yhteisöjä koskevaa tietoa, niiden toimivuus on kriittisessä asemassa yhteiskunnan toiminnassa. Erityisesti tietoliikenneyhteydet ja sähkönjakelu ovat luonteeltaan laajasti moniin eri toimintoihin vaikuttavia toimintoja. Sähköverkkojen toimintaan kohdistuvalla tietoturvaloukkauksella voisi olla erittäin merkittäviä vaikutuksia koko yhteiskuntaan lähes kaiken toimiessa sähköllä sairaaloista kotitalouksiin tai esimerkiksi liikenteen ohjausjärjestelmiin. Tieto- tai viestintäverkkojen toiminnan häiriöillä olisi yhtä lailla laajalle ulottuvia vaikutuksia yhä useamman toiminnon ollessa liitettynä verkkoon. Moni teollisuudenala, viranomaisten toiminnot, terveydenhuollon järjestelmät perustuvat usein verkkoon yhteydessä oleviin järjestelmiin. Näiden järjestelmien toiminnan estymisellä olisi merkittäviä haitallisia vaikutuksia kyseisen toimijan toimintaan ja voi pahimmillaan vaarantaa yhteiskunnan turvallisuutta myös laajemminkin. Tästä syystä tietoturvaloukkauksiin reagoiminen ja niistä aiheutuvien vaikutusten minimoiminen kaikin mahdollisin keinoin on tärkeää.

Vakavissa tietoturvauhkissa tehtävä yhteistyö on suorassa yhteydessä rikostentorjuntaan, koska uhkatilanteessa mahdolliset rikokset ovat vielä ennalta ehkäistävissä. Rikollisten kiinnisaaminen kyberrikoksissa on kuitenkin haastavaa ensinnäkin siitä syystä, että rikollisten jäljittäminen on vaikeaa, mutta myös sen vuoksi, että kyberrikokset eivät tunne valtioiden välisiä rajoja, jolloin rikoksen tekijä voi olla käytännössä missä päin maailmaa tahansa. Rikostorjuntaa saattaa jossain määrin edesauttaa myös ehdotettu poikkeuksellisissa tilanteissa tapahtuvaa tiedonvaihtoa koskeva säännös siltä osin, kun poliisin saamat tiedot ovat hyödynnettävissä rikoksen selvittämiseksi ja rikosvastuun kohdentamiseksi.

Viranomaisarvion mukaan viestinnän välittäjän vapaaehtoista tiedonluovutusta koskeva ehdotus edistää kyberturvallisuuden kansallisen tilannekuvan ylläpitämistä sekä tietoturvaloukkausten selvittämistä ja niitä koskevaa tiedonjakoa sekä sitä kautta tietoturvaloukkausten ennalta estämistä. Se myös välillisesti edistää viestintäverkkojen, palvelujen ja niihin liitettyjen tietojärjestelmien tietoturvallisuutta, mikä osaltaan turvaa myös yksityisyyden suojan toteutumista viestintäpalveluita käytettäessä.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Ehdotuksen vaihtoehtona on arvioitu nollavaihtoehtoa, eli tiedon vaihtamista ja virka-apua koskevan sääntelyn jättämistä nykyisen sääntelyn varaan. Viranomaiset tekevät tietoturvaloukkausten selvittämiseksi, ennaltaehkäisemiseksi ja vaikutuksien poistamiseksi yhteistyötä nykyisen sääntelyn varassa ja niille säädettyjen tehtävien puitteissa. Viranomaiset voivat vaihtaa tietoturvaloukkauksia koskevia tietoja keskenään laissa säädettyjen reunaehtojen mukaisesti. Erittäin vakavien tietoturvaloukkausten osalta on havaittu tarvetta nykyistä nopeammille vastavuoroisille tiedonvaihtokanaville, joita ei aivan kaikkien tietojen, kuten viestien, välitystietojen ja sijaintitietojen osalta ole ollut olemassa. Asia on nostettu esille myös valtioneuvoston periaatepäätöksessä tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla ja sitä edeltäneessä työryhmän loppuraportissa. Tästä syystä on katsottu aiheelliseksi, että nykytilaa on tarve näiltä osin muuttaa, eikä lainsäädännön tilaa voida pitää nykyisellään.

Vaihtoehtoisena ratkaisukeinona on arvioitu, voitaisiinko laajamittaisia häiriöitä koskevat tilanteet ratkaista niitä koskevalla omalla lainsäädännöllä, joka olisi rakennettu nimenomaisesti vakavia tietoturvaloukkauksia varten ja niiden ratkaisemiseksi tehtävää yhteistoimintaa silmällä pitäen. Valmistelun aikana kuitenkin arvioitiin, että nykyiset toimintamallit ovat keskeisiltä osin havaittu toimiviksi, eikä niitä ole yleisellä tasolla tarpeen muuttaa myöskään vakavissa tilanteissa. Viranomaiset toimisivat joka tapauksessa säädettyjen toimivaltuuksiensa nojalla. Lisäksi arvioitiin, että uusi yksittäisiä tilanteita koskeva lainsäädäntö on omiaan sekoittamaan jo nykyiselläänkin melko monimutkaista tiedonvaihtolainsäädäntöä luomalla siihen uuden kerroksen. Viranomaisten yhteistyöstä säätäminen sellaisenaan ei lisäksi ole yleistä, joten kyse olisi muutoinkin ollut tässä suhteessa poikkeavasta toimintamallista. Sinällään tämänkaltaisella lainsäädännöllä voitaisiin päästä ehdotuksen kanssa vastaaviin vaikutuksiin, mutta soveltajan kannalta erillinen laki voisi käytännössä osoittautua haastavaksi.

Valmistelun aikana on arvioitu erilaisia vaihtoehtoja sille, miten voitaisiin määritellä sellainen vakava tietoturvaloukkaus, jolla on merkittäviä vaikutuksia yhteiskunnan toiminnan kannalta merkityksellisille toimialoille eli käytännössä sitä, milloin tiedonvaihdon poikkeussääntely tulisi sovellettavaksi. Valitun lähestymistavan lisäksi on arvioitu yhtenä vaihtoehtona soveltaa NIS-direktiivin liitteen listausta määriteltäessä yhteiskunnan kriittisiä toimintoja, mutta sen haasteesi koettiin liika yksityiskohtaisuus, jolloin jää riski väliin putoaville toiminnoille. Vastakotana olisi lausunnollakin ollut versio yleisemmästä kirjauksesta, joka mahdollistaisi laajan soveltamisalan tarpeen mukaan, mutta sen sisältö nähtiin liian täsmentymättömäksi, eikä siten käyttökelpoiseksi soveltajan kannalta, mutta myös perusoikeuksien rajoitusten tarkkarajaisuuden vaatimuksesta johtuen.

Soveltamiskynnystä koskevan kirjauksen osalta on arvioitu erilaisia määrittelyjä, joita sisältyy esimerkiksi julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) 18 §:ään tai SVPL 244 a §:ään. Ehdotuksen mukaisen listauksen esikuvana on käytetty valmiuslain 3 §:n 6 kohdan listausta, mutta senkään ei katsottu suoraan soveltuvan ehdotuksen mukaiseen tilanteeseen.

Esityksen valmistelun yhteydessä on arvioidu ulkomailla Ruotsissa, Norjassa, Saksassa, Iso-Britanniassa ja Ranskassa toteutettua sääntelyä ja viranomaisten tehtäviä. Ulkomaita koskevaa arviointia kuvataan jaksossa 5.2. Arvioinnin lopputuloksena on kuitenkin todettu viranomaisten tehtävien ja toimivaltuuksien vaihtelevan valtioittain niin suuresti, ettei ulkomaisia kokemuksia ja käytäntöjä ole voitu suoraan hyödyntää kansallisen ratkaisun löytämiseksi, vaan suomalaisten viranomaisten kansallista yhteistoimintaa koskeviin haasteisiin on täytynyt löytää ratkaisu kansallisen sääntelyn ja siitä yhteistoiminnalle aiheutuvien haasteiden näkökulmasta.

5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot

5.2.1 Ruotsi

5.2.1.1 Toimivaltaiset viranomaiset

Suomen tavoin Ruotsiin on muodostettu keskitetty kyberturvallisuustoimijaviranomainen, johon on koottu koko yhteiskuntaa palvelevia digitaalisen turvallisuuden ja kyberturvallisuuden tehtäviä. Ruotsin kyberturvallisuuden viranomaisyhteisön keskeisin toimija on MSB (Myndigheten för samhällsskydd och beredskap) ja sen alaisuudessa toimiva kyberturvallisuuden ja turvayhteyksien osasto (Avdelningen för cybersäkerhet och säkra kommunikationer). Osaston vastuualueelle kuuluu muun muassa CERT-SE:n (Computer Emergency Response Team) ylläpito ja kansainvälisenä yhteyspisteenä toimiminen erityisesti EU:n suuntaan. Osasto seuraa toimintaympäristöä, vastaanottaa viranomaisilmoituksia, kehittää yhteistyömuotoja eri viranomaisten ja muiden toimijoiden välille sekä tarjoaa kyberturvallisuuden tilannekuvapalveluita. MSB:n vastuulla on siviilipuolustusta, yleistä turvallisuutta ja hätätilanteiden hallintaa koskevat toimet silloin, kun mikään muu viranomainen ei ole niistä vastuussa.

Ruotsin uuden kyberturvallisuuskeskuksen (Nationellt cybersäkerhetscenter) tavoitteena on vahvistaa viranomaisten valmiuksia ratkaista omat toimeksiantonsa ja samalla tarjota paremmat mahdollisuudet lisätä kansallista kykyä ehkäistä, havaita ja hallita kyberhyökkäyksiä ja muita verkossa tapahtuvia tapauksia, jotka uhkaavat vahingoittaa Ruotsin turvallisuutta. Kyberturvallisuuskeskuksen perustamisessa ovat olleet mukana FRA (Försvarets radioanstalt), Ruotsin puolustusvoimat, MSB ja Säpo (Säkerhetspolisen). Kyberturvallisuuskeskus tekee laajaa yhteistyötä Ruotsin posti- ja televiestintäviranomaisen (Post- och telestyrelsen), poliisin ja puolustustarvikehallinnon (Försvarets materielverk) kanssa. Kyseisille organisaatioille annetaan mahdollisuus myös osallistua keskuksen toimintaan. Kyberturvallisuuskeskus tekee laajaa yhteistyötä yksityisten ja julkisten toimijoiden kanssa.

Ruotsissa kaikkien valtion virastojen on ilmoitettava kyberhäiriöistä, jotka tapahtuvat viraston tietojärjestelmässä tai viranomaisen toiselle organisaatiolle tarjoamissa palveluissa. Kriisivalmiudesta ja vastuuviranomaisten toimista lisääntyneen varautumisen yhteydessä annetun asetuksen (2015:1052) mukaan kyberhäiriöistä, jotka voivat vakavasti vaikuttaa viranomaisen vastuulla olevan tiedonhallinnan turvallisuuteen, tai palveluista, joita viranomainen toimittaa toiselle organisaatiolle, on ilmoitettava MSB:lle.

Kansallisesta kyberpuolustuksesta vastaa Ruotsin puolustusvoimat ja sen alaisuudessa toimivat virastot. Päävastuussa on pääesikunnan alaisuudessa toimiva johtamisjärjestelmäpäällikkö ja kyberpuolustusyksikkö. Kyberpuolustus ei ole kuitenkaan pelkästään asevoimien tehtävä, sillä työhön osallistuu ajoittain myös Säpo ja MSB.

Kansallisella tasolla kyberturvallisuuden toimijoita on useita. Pääasiallisesti vastuussa kansallisesta kyberturvallisuudesta ja sen kehityksestä ovat MSB, Ruotsin puolustusvoimat, Säpo sekä FRA. Kyberturvallisuudesta huolehditaan myös useilla viranomaisyhteistyön alustoilla, joista keskeisin on SAMFI (Samverkansgruppen för informationssäkerhet). SAMFI:n jäseniin kuuluu kyberturvastrategian toimintasuunnitelmasta vastanneiden viranomaisten lisäksi myös Ruotsin asevoimien tiedustelupalvelu Must (militära underrättelse- och säkerhetstjänsten). NSIT (Nationell samverkan till skydd mot allvarliga IT-hot) toimii yhteistyöelimenä vakavien ja kriittisiin toimintoihin kohdistuvien uhkien varautumisen osalta. Siinä edustettuna ovat Säpo, FRA, Must ja Ruotsin puolustusvoimat.

Ruotsissa on myös monia muita viranomaisia, joille kuuluu keskeisiä kyberturvallisuuteen liittyviä tehtäviä. Ruotsin posti- ja televiestintäviranomainen PTS vastaa posti- ja sähköisen viestinnän alasta ja muun muassa pilvipalveluiden valvonnasta. Verkkoihin ja kyberturvallisuuteen liittyvien rikoslakirikosten tutkinta on poliisin, syyttäjäviranomaisen ja Ruotsin turvallisuuspalvelun vastuulla. Henkilötietojen suojaa koskevissa tapauksissa toimivaltainen viranomainen on Ruotsin tietosuojaviranomainen IMY (Integritetsskydds myndigheten).

Ruotsin lainsäädäntöä on kehitetty kyberturvallisuuden osalta, ja erityisesti vuoden 2018 kansallisen turvallisuuden lainsäädäntö (Säkerhetsskyddslag) asettaa velvoitteita kriittisen infrastruktuurin parissa työskenteleville toimijoille ja laajentaa Säpon toimivaltuuksia valvonnan suhteen. Suomesta poiketen Ruotsissa ei ole valmius- tai poikkeuslainsäädäntöä, joka lisäisi hallituksen valtaa suhteessa parlamenttiin. Tämän sijaan juridisista perusteista kriisiolosuhteisiin varautumiseksi ja toiminnasta poikkeuksellisissa olosuhteissa säädetään perustuslaissa (erityisesti Regeringsformen; 1974) ja normaalilainsäädännössä. Ruotsalaisen kriisijohtamisen mallin läheisyysperiaatteen mukaan kriisitilanteeseen tulee mahdollisuuksien mukaan vastata alimmalla mahdollisella hallinnon tasolla.

5.2.1.2 Lainsäädäntö

Ruotsissa ei ole yhtä kattavaa kyberturvallisuuslakia. Kyberturvallisuutta koskeva oikeudellinen kehys on jaettu useisiin eri lakeihin. Rikoksiin, kuten tietoverkkorikollisuuteen sovelletaan Ruotsissa rikoslakia (Brottsbalken). Terroriteoista ja kyberhyökkäyksistä säädetään Ruotsin terrorismirikosvastuusta annetussa laissa (Lag om straff för terroristbrott). Rikosten ehkäisemisestä, tutkinnasta ja syytteeseenpanosta vastaavien valtion viranomaisten suorittamasta henkilötietojen käsittelystä säädetään Ruotsin rikoksiin liittyvien henkilötietojen käsittelystä annetussa laissa (Brottsdatalagen). Sähköisten viestintäpalvelujen tarjoajiin sovelletaan Ruotsin sähköistä viestintää koskevaa lakia (Lag om elektronisk kommunikation). Tiettyihin elintärkeisiin kriittisen infrastruktuuriin palveluihin sovelletaan Ruotsin säädöstä elintärkeiden infrastruktuurien ja digitaalisten palvelujen tarjoajia koskevasta tietoturvasta (Lag om informationssäkerhet för samhällsviktiga och digitala tjänster). Lisäksi tietyistä Ruotsin kansalliselle turvallisuudelle tärkeiksi katsotuista toiminnoista säädetään Ruotsin turvallisuussuojalailla (Säkerhetsskyddslag).

5.2.1.3 Virka-apu

Ruotsissa puolustusvoimien poliisille antama virka-apu perustuu puolustusvoimia koskevaan asetukseen (Förordning 2007:1266 med instruktion för Försvarsmakten), ja erikseen on säädetty virka-avun antamisesta siviilitoiminnan avustamisessa, helikopterikuljetuksissa ja terrorismin torjunnassa. Laki virka-avusta terrorismin torjunnassa (Lag 2006:343 om Försvarsmaktens stöd till polisen vid terrorismbekämpning) mahdollistaa virka-avun antamisen poliisille sekä Ruotsin poliisin tiedustelu- ja turvallisuuspalvelu Säpolle.

5.2.1.4 Yhteiskunnan kriittiset toiminnot

Ruotsissa yhteiskunnan elintärkeiksi toiminnoiksi määritellään sellainen toiminta, palvelu tai infrastruktuuri, joka ylläpitää tai varmistaa yhteiskunnan perustarpeiden, arvojen tai turvallisuuden kannalta välttämättömiä toimintoja. MSB on julkaissut ohjeet tärkeiden toimintojen tunnistamiseksi (Identifiering av samhällsviktig verksamhet: metod). Ruotsissa ei ole yksittäistä nimettyä viranomaista, joka olisi vastuussa kaikkien kansallisesti tärkeiden toimien kokoamisesta koko Ruotsin osalta. Lääninhallitusten ja keskusviranomaisten on yksilöitävä sosiaalisesti merkittävät toiminnot omilla toiminta-alueillaan. Kansallisella tasolla turvallisuusviranomaiset määrittelevät, mikä on tärkeää heidän omalla vastuualueellaan.

5.2.2 Norja

5.2.2.1 Viranomaiset

Vuonna 2018 perustetun Norjan Kyberturvallisuuskeskuksen (Nasjonalt cybersikkerhetssenter) tehtävänä on toimia kansallisena ja kansainvälisenä yhteyspisteenä ja yhteistyöelimenä kyberturvallisuuteen liittyvien tapahtumien analysointiin, tutkimukseen ja konsultointiin liittyen. Kyberturvallisuustoimijalle keskitetyt tehtävät palvelevat yhteiskunnan teknisiä tieto- ja kyberturvallisuuden operatiivisia tarpeita. Keskuksella on kumppaneita niin elinkeinoelämän, puolustuksen kuin julkisen hallinnon piirissä.

Kansallisella tasolla kyberturvallisuuden toimijoita on useita. Kyberturvallisuudesta vastuussa ovat erityisesti oikeus- ja varautumisministeriö, puolustusministeriö, paikallishallinto- ja modernisaatioministeriö, liikenne- ja viestintäministeriö sekä ulkoministeriö. Normaalioloissa koordinaatiovastuu siviilipuolen kyberturvallisuusjärjestelyistä keskittyy OVM:lle ja sen alaisille virastoille, pääasiassa poliisille ja NSM:lle (Nasjonal sikkerhetsmyndighet), sekä sektorikohtaisesti eri toimivaltaisille viranomaisille, kuten Norjan televiestintävirastolle (Nasjonal kommunikasjonsmyndighet). NSM on kansallisen turvallisuuden viranomainen, joka vastaa kyberturvallisuuden ohella muun muassa kriittisen infrastruktuurin suojaukseen liittyvistä toimista. NSM:n vastuu siviilikyberturvatoimista on merkittävä, sillä viraston alaisuudessa toimii kansallinen kyberturvallisuuskeskus ja tähän kuuluva Nor-CERT (kansallinen CERT-toiminta).

Puolustushallinnon näkökulmasta keskiössä on puolustusministeriö ja sen alainen sotilastiedustelulaitos NIS (Etterretningstjenesten) sekä vuonna 2012 aloittanut Norjan asevoimien kyberpuolustushaara. NIS:n tehtäviin osana Norjan asevoimia kuuluu ennakkovaroituksen antaminen Norjaan kohdistuvasta sotilaallisesta uhasta. Tässä suhteessa sen tehtäväkenttään kuuluu myös tiedustelutiedon kerääminen ja uhka-analyysien tuottaminen maan kyberpuolustukseen kohdistuvasta vaikuttamisesta. Oikeus- ja varautumisministeriön alaisella siviilivarautumisvirastolla DSB:llä (Direktoratet for samfunnssikkerhet og beredskap) on merkittävä rooli kansallisen varautumistoiminnan kehittämisessä ja siviilipuolustuksessa. DSB:n tehtävänkuvaan kuuluu poikkihallinnollisen tilannekuvan ylläpito kansallisesti merkittävistä riskeistä ja haavoittuvuuksista, ja viraston vastuulla on myös kansallisen riskiarvion ja yhteiskunnan kriittisten toimintojen strategian laatiminen.

Ministeriöiden ja niiden alaisten viranomaisten yhteistyötä ja tiedonvaihtoa parantamaan perustettiin kyberkoordinaatiokeskus FCKS (Felles cyberkoordineringssenter), joka tuo yhteen Keskusrikospoliisin, kansallisen turvallisuusviranomaisen sekä sotilas- ja siviilitiedustelun toimijat. Koordinaatiokeskuksessa toimivat edellä mainittujen lisäksi myös Norjan keskusrikospoliisi Kripos, jonka yhteyteen perustettiin hiljattain uusi kyberrikoskeskus (NC3). Kyberkoordinaatiokeskus tuo yhteen toimijoita siviili- ja sotilastahoilta tarkoituksena muodostaa yhteinen ja jaettu uhkatilannekuva sekä koordinoida toimintaa uhkiin vastaamiseksi.

Keskeisistä vuosittain julkaistavista kansallisen tason riskianalyyseista vastaavat siviilivarautumisviraston ohella turvallisuuspoliisi PST (Politiets sikkerhetstjeneste), Norjan sotilastiedustelu NIS sekä kansallisen turvallisuuden viranomainen (NSM). Siinä missä PST (sisäiset uhat, väkivaltainen liikehdintä, kansalliset intressit yms.), NIS (ulkoiset uhat) ja NSM (kyberturvallisuus, kriittinen infrastruktuuri yms.) keskittyvät tyypillisesti sektorikohtaisiin lyhyen aikavälin kriiseihin ja riskeihin, on DSB:n tehtävänä yhdistää näitä tietoja yhteen ja luoda analyysiä pidemmän aikavälin kokonaiskuvasta.

Norjan kriisijohtamisen malli on keskusjohtoinen, ja viimeisen vuosikymmenen aikana erityisesti oikeus- ja varautumisministeriön rooli on kasvanut yleisenä siviilikriisinhallinnan osaajana. Ylimpänä kriisitilanteiden päätöksenteon tasona toimii Norjan ulko- ja turvallisuuspoliittinen ministerivaliokunta, joka käsittelee keskeiset turvallisuuspolitiikkaa ja varautumista koskevat asiakysymykset. Kriisitilanteista vastuussa on lähtökohtaisesti se ministeriö, jonka toimialaan tilanne normaalioloissa kuuluu. Vastuuministeriö voi kutsua koolle kriisikomitean, jonka pääasiallisiin tehtäviin kuuluu eri hallinnonalojen toimien koordinaation vahvistaminen ja käytännön tukitoiminta. Kriisikomiteaa tukee oikeus- ja varautumisministeriöön kuuluva kriisivarautumisyksikkö. Maan hallituksella on viimekädessä vastuu varautumisesta ja kriisitilanteiden hallinnasta.

5.2.2.2 Lainsäädäntö

Norjassa ei ole yhtä kattavaa kyberturvallisuuslakia. Kyberturvallisuutta koskeva oikeudellinen kehys on jaettu useisiin eri lakeihin. Henkilötietojen käsittelyyn sovelletaan yleistä tietosuoja-asetusta (GDPR) ja vuonna2018 annettua henkilötietolakia. Vuoden 2018 kansallisella turvallisuuden lailla (Lov om nasjonal sikkerhet) pyritään ehkäisemään, havaitsemaan ja torjumaan kansallista suvereniteettia uhkaavaa toimintaa. Sähköisestä viestinnästä annetun lain (Lov om elektronisk kommunikasjon) tavoitteena on tarjota turvallisia ja nykyaikaisia viestintäpalveluita. Vuonna 1990 annetulla energialailla (Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m.) pyritään turvaamaan energiansaanti Norjassa. Edellä mainittujen säädösten lisäksi kyberturvallisuutta koskevaa lainsäädäntöä löytyy myös muista säädöksistä.

5.2.2.3 Virka-apu

Norjassa säännökset puolustusvoimien virka-avusta poliisille lisättiin poliisilakiin (Lov om politiet) vuonna 2015. Säännösten sisältö johdettiin ennen lain voimaantuloa sovelletusta käytännöstä, joka perustui puolustusvoimien antamaan ohjeistukseen poliisille annettavasta virka-avusta. Lain mukaan virka-apua voidaan antaa erityisen vahingollisten tai laajojen hyökkäysten estämiseksi ja torjumiseksi. Virka-apua voidaan antaa ihmisten hengen ja terveyden, omaisuuden ja yleisen turvallisuuden suojaamiseksi onnettomuuksissa, luonnon katastrofeissa ja muissa näihin rinnastuvissa tilanteissa. Virka-apua annetaan puolustusvoimien kaluston ja erityiskoulutetun henkilöstön muodossa.

Virka-apua sääntelee lisäksi virka-apua koskeva määräys (instruks om Forsvarets bistand til politiet), jonka mukaan virka-apua voidaan antaa vain, jos virka-aputehtävä on yhteensopiva puolustusvoimien ensisijaisten tehtävien kanssa ja poliisin omat resurssit ovat riittämättömät tai eivät ole käytettävissä tehtävän suorittamiseksi. Määräys edellyttää, että puolustusvoimat toimii virka-aputehtävän aikana erillään poliisista itsenäisen avustustehtävän hoitajana.

5.2.2.4 Yhteiskunnan kriittiset toiminnot

Kansallisella tasolla Norjan varautuminen perustuu lainsäädäntöön sekä riskianalyyseihin ja -arvioihin. Oikeus- ja varautumisministeriön alaisella siviilivalmiusvirastolla on merkittävä rooli yhteiskunnan riskien ja haavoittuvuuksien arvioinnissa. Yhteiskunnan kriittisten toimintojen julkaisussa tunnistetaan kriittisten toimintojen ohella kustakin vastaava ministeriö, suojattava kohde tai palvelu ja keskeiset näiden parissa työskentelevät viranomaiset ja muut toimijat.

Kriittiset toiminnot on määritelty niin, että yhteiskunta ei pärjäisi ilman niitä yli seitsemää päivää ilman, että väestön toimintakyky vaarantuisi. Toiminnot jaetaan kolmeen luokkaan, joita ovat hallinto ja suvereniteetti, väestön turvallisuus ja väestön toimintakyky. Lisäksi oikeus- ja

varautumisministeriö ylläpitää julkista listaa suojattavien kohteiden ja palveluiden parissa työskentelevien viranomaisten avainhenkilöstöstä. Norjassa on määritelty kriittisten toimintojen lisäksi myös ns. tärkeät toiminnot. Näitä ovat muun muassa vaarallisten aineiden käsittely, mediapalvelut ja hautaustoiminta.

5.2.3 Saksa

5.2.3.1 Viranomaiset

Saksan liittovaltion ylimpänä kyberturvallisuusviranomaisena toimii BSI (Bundesamt für Sicherheit in der Informationstechnik), jonka tehtävänä on parantaa valtion, liike-elämän ja yhteiskunnan kyberturvallisuutta ennaltaehkäisyn, havaitsemisen ja reagoinnin keinoin. BSI on ennen kaikkea Saksan liittohallituksen keskeinen tietoturvapalvelujen tarjoaja ja sen tehtävänä on estää liittovaltion tietotekniikkaan kohdistuvat uhat sekä avustaa muita viranomaisia tietotekniikan turvallisuuteen liittyvissä asioissa. BSI vastaa kyberturvallisuudesta valtakunnallisesti ja se tarjoaa neuvontaa ja tuottaa digitaalisen toimintaympäristön turvallisuutta koskevia ohjeita hallinnolle, yrityksille ja yksityishenkilöille. BSI toimii suoraan sisäministeriön alaisuudessa.

Kansallinen kyberpuolustuskeskus Cyber-AZ (Das Nationale Cyber-Abwehrzentrum) perustettiin vuonna 2011 osana liittovaltion hallituksen kyberturvallisuusstrategian täytäntöönpanoa. Cyber-AZ on eri turvallisuusviranomaisten yhteistyö-, viestintä- ja koordinointifoorumi, joka tuottaa ajantasaista ja kattavaa kyberturvallisuustilannekuvaa. Cyber-AZ tavoitteena on parantaa ja nopeuttaa asianomaisten viranomaisten ja laitosten välistä tietojenvaihtoa sekä tehostaa suojaus- ja puolustustoimenpiteiden koordinointia tietoturvapoikkeamia vastaan. Foorumiin kuuluu kahdeksan keskeistä viranomaistahoa sekä muita kumppanivirastoja.

5.2.3.2 Lainsäädäntö

Kyberturvallisuuteen sovelletaan monia säädöksiä Saksassa. Tärkeimmät kyberturvallisuuteen liitty-vät säädökset ovat GDPR, liittovaltion tietosuojalaki ja laki liittovaltion tietoturvavirastosta (Gesetz uber das Bundesamt fur Sicherheit in der Informationstechnik, BSI-laki). Lisäksi kyberturvallisuuden alakohtaisia osia säädetään mm. televiestintälailla (Telekommunikationsgesetz), pankkilailla (Kreditwesengesetz) ja energiateollisuuslailla (Energiewirtschaftsgesetz). Tietoturvalaissa (IT-Sicherheitsgesetz 2.0) säädetään kriittisen infrastruktuurin kyberturvallisuudesta.

Vuoden 2009 annetussa BSI-laissa määritellään BSI:n toimintaa. Laissa säädetään myös tiedonvaihdosta viranomaisilta BSI:lle. Poikkeuksena tiedonvälittämiselle on kuitenkin sellainen tieto, jota ei voi luovuttaa salassapitosäännösten tai osapuolten kanssa tehtyjen sopimusten vuoksi. Myöskään henkilötietojen suojaan ei saa puuttua.

IT-Sicherheitsgesetz 2.0 on ollut voimassa toukokuusta 2021 lähtien. Se laajentaa merkittävästi vuoden 2015 asetusta (KRITIS-asetus), sillä operaattoreille asetetaan enemmän velvoitteita ja valtiolle annetaan enemmän valtuuksia. BSI voi merkittävän häiriön aikana yhteisymmärryksessä asianomaisen toimivaltaisen liittovaltion valvontaviranomaisen kanssa vaatia, että elintärkeiden infrastruktuurien operaattorit tai organisaatiot luovuttavat häiriön hallitsemiseksi tarvittavat tiedot virastolle, mukaan lukien henkilötiedot.

5.2.3.3 Yhteiskunnan kriittiset toiminnot

Saksassa on hyväksytty vuonna 2015 IT-Sicherheitsgesetz 2.0, joka luo pohjan kriittisen infrastruktuurin suojelemiselle. Kriittisten infrastruktuurien ylläpitäjien, joihin tätä lakia sovelletaan,

on osoitettava liittovaltion tietoturvavirastolle (BSI), että ne täyttävät tietotekniset turvallisuusstandardit. Toimijoiden on myös ilmoitettava tietoteknisistä tietoturvapoikkeamista BSI:lle.

Kriittinen infrastruktuuri on määritelty Saksassa seuraavasti: liittovaltion tietoturvavirastosta annetussa laissa tarkoitettu kriittinen infrastruktuuri käsittää energia-, tietotekniikka-, televiestintä-, liikenne-, terveys-, vesi-, elintarvike-, rahoitus-, jätehuolto- ja vakuutusalalle kuuluvat laitokset, järjestelmät ja niiden osat, jotka ovat välttämättömiä yhteiskunnan toiminnan kannalta, koska niiden kaatuminen tai häiriöt johtaisivat huomattavaan toimitusvajeeseen tai yleiseen turvallisuuteen kohdistuviin riskeihin Saksassa.

5.2.4 Iso-Britannia

5.2.4.1 Viranomaiset

Iso-Britannian National Cyber Security Center (NCSC) on aloittanut toimintansa vuonna 2016 ja toimii Iso-Britannian kyberturvallisuuden ja kyberuhkien teknisenä viranomaisena. Iso-Britanniassa kyberturvallisuustoimijaviranomainen kuuluu osaksi keskitettyä turvallisuusvirastoa, jolla on kyberturvallisuuden lisäksi vastuullaan mm. tietotekninen tiedustelutoiminta, terrorismin ja ääriliikkeiden torjunta, vakavan ja järjestäytyneen rikollisuuden torjunta sekä tietoturvallisuuden tukeminen. Keskuksen tehtävänä on tukea kansallisia kriittisiä toimijoita, julkista sektoria, yrityksiä ja yksityisiä kansalaisia. Keskus tuottaa kyberturvallisuuteen liittyvää tietoa ja reagoi kyberturvallisuuspoikkeamiin vähentääkseen organisaatioille ja yhteiskunnalle aiheutuvia vahinkoja. Keskitetyn toimijan tehtäviin kuuluvat mm. kyberturvallisuushäiriöiden hallinta, eli ns. CERT- ja CIRT toiminta. Keskus kuuluu Iso-Britannian tiedustelu- ja turvallisuuspalvelu GCHQ:n (Government Communications Headquarters) alaisuuteen.

GCHQ on tiedustelu-, kyberturvallisuus-, ja turvallisuusvirasto, jonka tehtäviin kuuluvat terrorismin torjunta, kyberturvallisuuden parantaminen ja vakavan ja järjestäytyneen rikollisuuden torjuminen. Virasto kokoaa tiedustelutietoa ja tekee laajaa yhteistyötä kansainvälisten viranomaisten kanssa. Iso-Britannian ulkoministeri vastaa GCHQ:n toiminnasta, mutta GCHQ ei kuuluu suoraan ulkoministeriön alaisuuteen.

Iso-Britanniassa National Crime Agency (NCA) vastaa vakavan ja järjestäytyneen rikollisuuden tutkinnasta. NCA:n tehtäviin kuuluu rikostiedustelu ja kansainvälinen yhteistyö rikollisuuden torjumiseksi ja tutkimiseksi. NCA:n tehtäviin kuuluu näin ollen myös vakavan ja rajat ylittävän kyberrikollisuuden tutkinta. Iso-Britanniassa organisaatiot voivat ilmoittaa kyberhyökkäyksistä National Fraud and Cyber Crime Reporting Centrelle, joka toimii petos- ja verkkorikollisuuden raportointikeskuksena. Raportointikeskuksen rinnalla toimii myös National Fraud Intelligence Bureau (NFIB), jonka tehtävänä on analysoida verkkorikoksista tehtyjä ilmoituksia ja toimittaa niitä muun muassa paikallispoliisin tutkittavaksi.

Iso-Britanniassa toimii myös puolustus- ja tiedusteluviranomaisten yhteistyöhön perustuva National Cyber Force. Sen vastuisiin kuuluu toiminta kyberympäristössä Iso-Britanniaan kohdistuvien uhkien torjumisessa ja edistää valtion etuja koti- ja ulkomailla.

5.2.4.2 Lainsäädäntö

Iso-Britanniassa ei ole yhtä kattavaa kyberturvallisuuslakia. Viestintälaki (The Communications Act 2003) sisältää kyberturvallisuusvelvoitteet, joita sovelletaan sähköisten verkkojen tarjoajiin ja yleisiin sähköisten viestintäpalveluiden tuottajiin. Tutkintavaltuuksia koskevassa laissa (Regulation of Investigatory Powers Act 2000) säädetään tietyistä lainvalvontavaltuuk-

sista, kuten verkkovalvonnasta. IPA-sopimuksessa (IPA 2016) laajennetaan viranomaisten kyberrikollisuuteen liittyviä tutkintavaltuuksia. Tietokoneen väärinkäyttöä koskevassa laissa (Computer Missuse Act 1990) säädetään erilaisista rikoksista, jotka liittyvät tietoverkkoihin. Tämän lisäksi on monia muita säädöksiä, joissa käsitellään kyberturvallisuutta.

Iso-Britannian yleisen tietosuoja-asetuksen mukaan henkilötietoja ovat sellaiset tiedot, joiden avulla luonnollinen henkilö on tunnistettavissa. Tällaisia tietoja voivat olla esimerkiksi IP-osoite, MAC-osoitteet ja evästetunnisteet. Jos henkilötiedot voidaan anonymisoida, ei niihin enää sovelleta Iso-Britannian yleistä tietosuoja-asetusta.

5.2.4.3 Yhteiskunnan kriittiset toiminnot

Iso-Britannian kyberturvallisuuskeskuksen vastuulle kuuluu kriittisen infrastruktuurin suojaaminen kyberhyökkäyksiltä. Keskus tekee laajaa yhteistyötä Centre for the Protection of National infrastructuren (CPNI) kanssa. CPNI:n tehtävänä on avustaa ja tarjota apua organisaatioille, joiden vastuulla on kansallisen kriittisen infrastruktuurin suojaaminen.

Iso-Britannian hallituksen virallisen määritelmän mukaan kriittiseen infrastruktuuriin kuuluu sellainen omaisuus, laitteet, järjestelmät, verkot ja prosessit sekä niitä käyttävät työntekijät, joiden katoaminen tai vaaraan joutuminen voi aiheuttaa merkittävää haittaa keskeisten palvelujen saatavuuteen, eheyteen tai tarjoamiseen, mukaan lukien palvelut, joiden eheys voi vaarantuessaan johtaa merkittäviin ihmishenkien menetyksiin tai merkittäviin taloudellisiin tai sosiaalisiin vaikutuksiin taikka merkittävää haittaa kansalliseen turvallisuuteen, maanpuolustukseen tai valtion toimintaan.

5.2.5 Ranska

5.2.5.1 Viranomaiset

Ranskan kansallinen kyberturvallisuusvirasto (ANSSI) on kyberturvallisuuden sekä verkko- ja tietoturvallisuuden viranomainen, jonka tehtävänä on edistää ranskalaista tekniikkaa, järjestelmiä ja osaamista sekä valvoa jäljempänä kuvattuja keskeisten palveluiden tuottajia. Keskitetyn toimijan tehtäviin kuuluvat mm. kyberturvallisuushäiriöiden hallinta, eli ns. CERT- ja CIRT toiminta. ANSSI:n toimintaa tehostettiin joulukuussa 2013 annetulla sotilasohjelmointilailla, jossa säädettiin toimenpiteistä, joilla lisätään elintärkeiden operaattoreiden turvallisuutta, ja ANSSI:lle myönnettiin pääministerin puolesta uusia oikeuksia, joiden avulla se voi panna täytäntöön turvallisuus- ja valvontatoimenpiteitä elintärkeiden operaattoreiden kriittisimmissä verkko- ja tietojärjestelmien osalta. Lisäksi laissa säädetään, että erittäin tärkeiden toimijoiden on ilmoitettava järjestelmissä havaituista vaaratilanteista ANSSI:lle.

Tietosuojaviranomainen CNIL (Commission Nationale de l'Informatique et des Libertés) valvoo Ranskan tietosuojalakja (FDPA) yleisen tietosuoja-asetuksen asianmukaista soveltamista rekisterinpitäjien ja henkilötietojen käsittelijöiden toimesta. CNIL:llä on merkittävät valvonta- ja tutkintavaltuudet Ranskassa. FDPA:n tehokkaan valvonnan turvaamiseksi CNIL voi suorittaa laajoja tarkastuksia kaikille rekisterinpitäjille ja henkilötietojen käsittelijöille.

Kyberturvallisuuden valvonta kuuluu Ranskassa pääosin puolustusministeriön ja sisäministeriön toimialalle. Ranskassa on monia poliisiyksiköitä, jotka ovat erikoistuneet kyberturvallisuuteen, ja jotka voivat suorittaa rikostutkintaa, tiedonkeruuta, etsintöjä, datan keräämistä ja muita poliisin toimivaltaan kuuluvia toimenpiteitä kyberrikollisuuden torjumiseksi ja rikosten tutkimiseksi.

5.2.5.2 Yhteiskunnan kriittiset toiminnot

Ranskassa on verkko- ja tietoturvalakien mukaisesti nimetty keskeiset palveluiden tuottajat eri aloilla, kuten energia-, liikenne-, pankki-, rahoitusmarkkinainfrastruktuurit, terveyspalvelut ja apteekkialalla. Näitä toimijoita oli vuonna 2018 yksilöity yhteensä 122, ja määrän odotetaan kasvavan tulevaisuudessa. Toimijat tarjoavat keskeisiä palveluita, joiden keskeytys vaikuttaisi merkittävästi talouden tai yhteiskunnan toimintaan. ANSSI tukee näitä toimijoita niiden suojaamisen varmistamiseksi suunnitellun kyberturvallisuuskehyksen mukaisesti. Kriittisiin operaattoreihin sovellettavaa kyberturvallisuuskehys otettiin käyttöön vuonna 2013 annetulla elintärkeiden infrastruktuurien tietosuojaa koskevalla lailla.

6 Lausuntopalaute

Hallituksen esityksestä pyydettiin lausuntoja 25 eri taholta. Lausuntoja pyydettiin laajasti ministeriöiltä, joita pyydettiin kokoamaan lausuntoonsa hallinnonalansa yhteen sovitettu näkemys. Lisäksi lausuntoja pyydettiin laajasti elinkeinoelämän edunvalvontajärjestöiltä sekä kriittisten toimialojen edunvalvontajärjestöiltä. Lausuntoa pyydettiin myös Ahvenanmaalta. Lausuntoja annettiin yhteensä 12.

Lausunnon antoivat valtiovarainministeriö, sosiaali- ja terveysministeriö, sisäministeriö, puolustusministeriö, oikeusministeriö, Liikenne- ja viestintävirasto Traficom, Teknologiateollisuus ry, Finnish Information Security Cluster FISC – Kyberala ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Elinkeinoelämän keskusliitto EK, Finanssiala ry, Tieto- ja viestintätekniikan ammattilaiset TIVIA ry. Lausuntoyhteenveto on nähtävillä valtioneuvoston hanketietopalvelussa tunnuksella LVM071:00/2021. Alle on koottu lausunnoissa esiin nousseet keskeisimmät näkemykset.

Lausunnoissa ehdotuksen tavoitteisiin ja ehdotuksiin suhtauduttiin pääosin positiivisesti ja ehdotusta pidettiin tärkeänä ja tarpeellisena. Ehdotukseen annettiin kuitenkin jonkin verran muutosehdotuksia ja nostettiin esille täsmennystarpeita niin säännösehdotusten kuin perustelujen osalta.

Puolustusministeriön lausunnossa nostettiin esille yleisiä näkökohtia siitä, että ehdotus on välivaihe laajemman kyberpuolustuksen näkökulmasta ja laajemmat kysymykset on tarkoitus ratkaista sisäministeriön ja puolustusministeriön vetämässä kyberturvallisuuden selvityshankkeessa. Jatkovalmistelussa on tehty perusteluihin lisäys laajemmasta asiaan liittyvästä valmistelutarpeesta ja ehdotuksen suhteesta siihen.

Virka-avun osalta Traficom nosti esille, että tulisi tehdä tarkemmin selkoa siitä, miten vaikutusten poistamisen käsite suhteutuu viranomaisten toimivaltaan, sillä esimerkiksi virka-aputilanteessa virka-apupyynnön tulee liittyä sitä pyytävän viranomaisen tehtäväpiiriin. Lisäksi tulisi tehdä selkoa siitä, miten ehdotus suhteutuu yksityisen sektorin toimintaan. Tähän kiinnittivät huomiota myös EK, Teknologiateollisuus ja FISC omassa lausunnossaan. Virasto lisäksi nosti esille, että ehdotuksen loppuun ehdotettu lisäys ”jollei muualla laissa toisin säädetä” on tarpeeton. Esitykseen on tehty tarkempaa selkoa vaikutusten poistamisesta sekä suhteesta viranomaisten toimivaltuuksiin ja toisaalta yksityiseen sektoriin. Lisäksi poistettu maininta ”jollei muualla laissa toisin säädetä”. Lisäksi puolustusministeriö esitti joitakin täsmennyksiä virka-avun käsitteeseen esityksen perusteluihin. Nämä ehdotukset on otettu huomioon jatkovalmistelussa.

Oikeusministeriö nosti virka-apuun liittyvän säännöksen osalta tarpeen arvioida sen suhdetta voimankäyttöä koskevan virka-avun sijaan virka-avun antamisen yleisempien edellytysten nojalla. Lisäksi olisi tarpeen täsmentää perusteluihin Puolustusvoimien toimivaltaa ehdotuksen

mukaisen tehtävän hoitamiseen säädöskohtaisia perusteluja vastaavasti. Jatkovalmistelussa perusteluja on täydennetty näiltä osin.

Elinkeinoelämän keskusliitto EK, Teknologiateollisuus ry ja FISC esittävät, että lakiin tulisi sisällyttää tarpeelliset säännökset yksityisten antamasta virka-apuun rinnastettavasta avustamisesta. Koska merkittävän ja seurauksiltaan vakavan tietoturvaloukkaustilanteen havainnointi, torjunta ja selvittäminen voi vaatia käytännössä kaikkien relevanttien viranomaisten henkilöstön käyttämistä omiin päätehtäviinsä, tarvittavaa asiantuntemusta voidaan joutua hankkimaan muualta, eritoten elinkeinoelämän toimijoilta. Esimerkkinä voisivat olla poliisilakiin sisältyvät säännökset avustamistyöstä, joiden tarkoituksena on mahdollistaa poikkeuksellisissa tilanteissa nopeasti tarkoitukseen sopivan ulkopuolisen avun käyttäminen. Kyse olisi tässä tapauksessa Liikenne- ja viestintäviraston oikeudesta saada apua yksityiseltä sektorilta sopimusperusteisesti korvausta vastaan. Ehdotusta ei ole voitu sen laajuudesta ja siihen liittyvistä selvitystarpeista johtuen ottaa huomioon ehdotuksen jatkovalmistelussa, mutta lausuntopalaute on annettu tiedoksi sisäministeriön ja puolustusministeriön vetämään laajempaan selvitystyöhön, jossa tietoturvaloukkauksiin liittyvää yhteistyötä pohditaan laajemmin.

Tiedonvaihdon osalta keskeinen lausuntopalaute koski ehdotuksen merkittävää tietoturvaloukkausta koskevan vastavuoroisen tiedonvaihdon soveltamiskynnystä ja siihen liittyvää käsitteistöä. Erityisesti kriittisten toimialojen käsite nähtiin epäselvänä ja tarkentamista vaativana. Tähän kiinnittivät huomiota sekä viranomaiset että yksityisen sektorin toimijat. Oikeusministeriö katsoi yleisesti, että ehdotuksen väljä muotoilu vaikuttasi muodostavan jännitteisen suhteen perustuslain 10 §:n 4 momentin kvalifioidun lakivarauksen kannalta, eikä perusteluista selkeästi ilmene perustuisiko rajoitus aina tai ainakin joiltain osin yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkintaan. Lisäksi kriittisen infrastruktuurin käsitteen osalta oikeusministeriö viittaa perustuslakivaliokunnan lausumaan valmiuslain muutosesityksen yhteydessä. Valtiovarainministeriö on katsonut, että kriittisiin toimintoihin pitäisi sisältyä valtion velan- ja kassahallinta. Myös kriittinen infrastruktuuri pitäisi pyrkiä määrittelemään yksiselitteisemmin. Sisäministeriö pitää hyvänä, että poikkeussäännöksen soveltamisen kynnystä pidetään verrattain korkealla perusoikeussyistä johtuen. Elinkeinoelämän keskusliitto EK, Teknologiateollisuus ry sekä FISC näkevät haasteena ehdotuksen 319 a §:n määritelmän. Tavoite säännöksessä on kannattava, mutta ottaen huomioon perusoikeussuoja, tulisi säännökseltä edellyttää mahdollisimman suurta selkeyttä. Esimerkiksi yhteiskunnan kriittisillä toiminnoilla ei ole yhtä täysin vakiintunutta tarkkarajaista sisältöä. Määritelmää esitetään vielä tarkemmin harkittavaksi.

Traficom katsoo, että ehdotuksessa tulisi löytää tasapaino yhtäältä viranomaisten tiedonjaon mahdollistamisen ja toisaalta viestinnän luottamuksellisuuteen tai salassapitoperusteisiin tehtävien rajoitusten välillä. Virasto katsoo, että ehdotuksen soveltamiskynnys voi muodostua korkeaksi ja rajoittaa käytännössä säännöksen hyödynnettävyyttä. Traficom kiinnittää huomiota kriittisen infrastruktuurin käsitteeseen, joka voi muodostua tulkinnanvaraiseksi tai rajata soveltamista yksittäistapauksissa epätarkoituksenmukaisesti. Se ehdottaa, että kriittisen infrastruktuurin sijaan voisi olla perusteltua viitata laajemmin yhteiskunnan elintärkeisiin toimintoihin, kuten SVPL 244 a §:ssä on aiemmin tehty. Traficom viittaa myös valmiuslain hiljattain valmistuneen muutoksen esitöihin. Lisäksi se kiinnittää huomiota poliisitoimen ja Puolustusvoimien henkilötietolakien ehdotuksiin. Viraston mukaan ehdotuksen 319 a §:n suhde henkilötietojen käsittelystä annettuihin lakeisin mahdollistaisi jatkossa salassapitosäännösten estämättä tapahtuvan henkilötietojen luovuttamisen Liikenne- ja viestintävirastolle laista riippuen joko tarpeellisuus- tai välttämättömyyskriteerillä osin päällekkäisistä tilanteista SVPL 319 a §:ään nähden. Jatkovalmistelussa ehdotusta on muokattu täsmällisempään muotoon hyödyntäen valmiuslain muutoksen poikkeusolojen määritelmässä määriteltyjä yhteiskunnan elintärkeitä toimintoja.

Henkilötietolakeihin sisältyvät ehdotukset eivät käytännössä muuta merkittävästi voimassaolevaa oikeustilaa nykyisestä. Sinällään soveltamistilanteet ovat osittain päällekkäisiä, mutta ehdotuksen 319 a §:n nojalla voidaan vaihtaa muutakin kuin henkilötiedoksi luettavaa tietoa.

Sisäministeriö lisäksi katsoi, että perusteluja olisi hyvä täydentää siten, että viranomaiset käyttävät saatuja tietoja omien toimivaltasäännösten puitteissa ja että erityislainsäädäntöön liittyy tiettyjen tietojen luovuttamiseen koskevia rajoituksia (esimerkiksi biometriset tunnisteet). Myös tiedon edelleen luovutuksesta olisi tarpeen säätää. Tämä lisäys on tehty perusteluihin. Tiedon edelleen luovuttamiselle ei ole kuitenkaan ehdotettu erityisiä rajoituksia, sillä eri viranomaisten toiminta perustuu myös kansainvälisten verkostojen hyödyntämiseen. Ottaen huomioon tietoturvaloukkausten rajat ylittävän luonteen, jatkovalmistelussa katsottiin aiheelliseksi säilyttää mahdollisuus vaihtaa tietoa sellaisten tahojen kanssa, joiden osalta lainsäädäntö sen nykyisellään mahdollistaa tietoturvaloukkaustilanteissa. Tiedon luovuttaminen edelleen on myös tiukasti säänneltyä tarkoitukseen ja tarpeeseen perustuen sekä luottamuksellisen viestinnän suojaa ja yksityisyyden suojaa mahdollisimman vähän rajoittaen, mikä osaltaan rajaa tiedon luovuttamista edelleen. Jatkovalmistelussa kuitenkin huomioitiin eräät tiedon edelleen luovuttamista koskevat rajoitteet, jotka käyvät ilmi ehdotuksen 319 a §:n 3 momentin perusteluista.

Sisäministeriö kiinnitti huomiota, ettei esityksessä käsitellä tietosuojalainsäädännön mukaista tarkastusoikeutta esityksen mukaisen lainsäädännön perusteella saatuihin tietoihin. Esimerkiksi poliisin tietojen osalta niin sanottua omien tietojen suoraa tarkastusoikeutta on rajoitettu poliisin henkilötietolain 42 §:ssä, jotta tarkastusoikeus ei vaaranna poliisin lakisääteisten tehtävien suorittamista. Poliisin lakisääteisten tehtävien suorittaminen ei saisi vaarantua myöskään siitä syystä, että henkilö saisi toisen viranomaisen kautta pääsyn poliisin luovuttamiin tietoihin, joihin kohdistuu poliisissa tarkastusoikeuden rajoituksia. Tämä huomio on lisätty ehdotukseen.

Puolustusministeriö on nostanut esille IP-osoitteen henkilötiedoksi tulkitsemisen yksiselitteisyyden ja todennut, että liian suoraviivaista tulkintaa siitä, että näin aina on, tulisi välttää. Ehdotuksen perustelujen sanamuotoa tältä osin on hieman täsmennetty. Lisäksi ministeriö esitti huomioita hallinnonalansa lainsäädännön täydentämiseltä sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetulla lailla. Myös nämä täydennykset on lisätty esitykseen.

Sosiaali- ja terveysministeriö huomauttaa, että ehdotuksessa ei ole käsitelty erityisen arkaluonteisia tietoja ja ehdottaa, että säännöstä täydennettäisiin tarpeettoman tiedon poistamista koskevalla säännöksellä. Tarpeettoman tiedon poistamista koskeva säännös on lisätty ehdotukseen ja perusteluja täydennetty arkaluonteisia tietoja koskevilla lisäyksillä.

Finanssiala ry ja Elinkeinoelämän keskusliitto EK, Teknologiateollisuus ry ja FISC kannattavat viranomaisten tiedonvaihdon parantamista, mutta näkee tarpeellisena, että tiedonvaihdossa huomioitaisiin myös yksityinen sektori. Järjestöt näkevät outona, että viranomaiset vaihtaisivat tietoa tai ryhtyisivät toimenpiteisiin ilman, että kohteeksi joutunut yritys ei saisi tietoa tai olisi mukana selvittämisessä. Lisäksi Finanssiala ja EK korostavat, että tiedonvaihdon menettelyt on laadittava niin, että ne täyttävät tietoturvallisuus-, tietosuoja- ja dokumentointivaatimukset, minkä lisäksi jatkuvalla seurannalla varmistetaan, että tietopyynnöt ja niihin annettavat vastaukset ovat muodollisesti ja sisällöllisesti asianmukaisia. Ulkomaisten viranomaisten osalta on varmistettava, että tiedonvaihto tapahtuu kaikissa tilanteissa soveltuvien säädösvaatimusten, yleisen tietosuojaperiaatteiden ja hyvien tietojenkäsittelykäytäntöjen mukaisesti. Jatkovalmistelussa on arvioitu, että tiedonvaihtoon liittyvään lainsäädäntöön ei yksityisten, tietoturvaloukkausten kohteeksi joutuneiden toimijoiden osalta sisälly vastaavanlaisia esteitä, mitä viranomaisten välillä on havaittu. Yksityisille toimijoille voidaan luovuttaa tietoa sähköisen viestinnän palvelusta annetun lain nojalla laajasti silloin, kun tietoturvaloukkaus koskee heitä itseään.

Viranomaisten tiedonvaihto-oikeus tietoturvaloukkaustilanteissa laajenee käytännössä ehdotuksen jälkeen tätä vastaavalle tasolle. Tiedonvaihto ulkomaille tapahtuu aina yksilöidysti ja vakiintuneilla menettelyillä vain tarpeellisessa laajuudessa. Näin myös käytännössä toimitaan.

Lisäksi edellä mainitut edunvalvontajärjestöt ehdottavat, että säännöstä täsmennettäisiin siten, että luovutettua tietoa ei saa luovuttaa edelleen muille tahoille kuin pykälässä mainituille suomalaisille viranomaisille. Lisäksi viranomaisten luovuttaessa tietoja toisilleen, tulee niiden ilmoittaa sille yritykselle, jonka tietoja on luovutettu, mitä tietoja ja milloin on luovutettu ja kenelle. Lisäksi ehdotukseen ehdotetaan lisättäväksi 316 a §:n 4 momenttia vastaava tietojen hävittämistä koskeva säännös. Ehdotukseen on lisätty tiedon hävittämistä koskeva säännös. Jatkovalmistelussa tietojen edelleen luovutusta ei katsottu tarkoituksenmukaiseksi kieltää erityisesti siitä syystä, että tietoturvaloukkausten selvittämisen kannalta voi olla erittäin olennaista pystyä jakamaan tarpeellisia tietoja esimerkiksi ulkomaisten kumppaneiden kanssa. Hyökkäykset eivät usein tapahdu Suomen rajojen sisäpuolelta, minkä vuoksi kansainvälinen yhteistyö näyttelee merkittävää roolia tietoturvaloukkausten selvittämisessä ja myös tulevien hyökkäysten ennalta ehkäisemisessä.

Ulkomaille luovutettavan tiedon osalta Traficom esitti, että nyt tehtävien lainsäädäntömuutosten yhteydessä muutettaisiin myös 319 §:n 2 momentin 2 kohtaa siten, että tietojen luovuttaminen esim. Euroopan unionille ja NATO:lle viestintäverkkoihin ja –palveluihin kohdistuvien tietoturvaloukkausten ehkäisemiseksi tai selvittämiseksi olisi mahdollista. FiCom ry nostaa esille, että voimassa oleva laki (319 § 2 ja 3 momentti) mahdollistaa muun muassa massaluovutuksen ja siitä puuttuvat merkittävyys-, vaikutus- ja välttämättömyyskriteerit, edelleenluovutuskielto sekä ehdoton käyttötarkoitus. FiCom pitää menettelyn keventämistä ymmärrettävänä, mutta luovuttamisen edellytyksiä pitäisi tiukentaa. Lisäksi FiCom lisäksi nostaa esille, että yrityksille on viestinnän luottamuksellisuuden takia tarpeen saada tietoa luovutuksista, joten liikenne- ja viestintäviraston tulee tehdä yhteistyötä niiden yritysten kanssa, joiden tietoja luovutetaan. Tämänkaltainen säännös on poistettavaksi ehdotetussa 5 momentissa, mutta viraston tulisi vähintään ilmoittaa yritykselle, jonka tietoja on luovutettu, mitä tietoa ja milloin on luovutettu ja kenelle. Ehdotukseen on lisätty maininnat EU:sta ja Natosta. FiComin näkemykseen massaluovutuksesta todetaan, että nykyinen lainsäädäntö rajaa ulkomaille luovutettavaa tietoa SVPL 319 §:n 3 momentissa tarpeellisuusperusteella ja viestinnän luottamuksellisuus ja yksityisyyden suoja huomioiden. Kysymys ei siten missään tilanteessa ole erittelemättömästä massaluovutuksesta. Huomionarvoista on, että kansallisessa lainsäädännössä ei voida määritellä toisen valtion viranomaisen tiedonkäyttöä ilman valtiosopimusta. Tällä hetkellä tietojen luovuttamiselle pyydetään käytännössä lupa ennakollisesti, eikä tähän periaatteeseen ole tarkoitus tehdä normaalitilanteessakaan muutosta.

Viestinnän välittäjän vapaaehtoisesta tiedonluovutuksesta Traficomille Sosiaali- ja terveysministeriö toteaa, että ehdotus on lähtökohtaisesti kannatettava, mutta esityksestä ei käy missä tilanteissa ja minkälaisia menetelmiä hyödyntäen viestinnän välittäjä voisi oma-aloitteisesti havaita sellaisen toteutuneen tai ennakoitavan tietoturvaloukkauksen tai –uhkan, johon liittyen se voisi luovuttaa sekä välitystietoja että viestejä. Ministeriö huomauttaa, että luovutettuihin tietoihin liittyvien erityisen arkaluonteisten ja muun lain nojalla salassa pidettävien tietojen hävittämisestä ja kiellosta käyttää tietoja muihin tarkoituksiin pitäisi säätää. Jatkovalmistelun osalta Traficom katsoo, että olisi hyvä arvioida olisiko ehdotusta tarpeen täydentää luovutettavan tiedon minimointia korostavalla säännöksellä. Lisäksi olisi hyvä harkita pitäisikö tietojen luovuttaminen rajoittaa selvyyden vuoksi tilanteisiin, joissa luovutettavat tiedot liittyvät tiettyyn (epäiltyyn) tietoturvalle haittaa aiheuttavaan häiriöön. Ehdotusta tulisi tältä osin myös käsitellä säätämisjärjestysperusteluissa perustuslain 10 §:n osalta ja arvioida suhteessa sähköisen viestinnän tietosuojadirektiivin 15 artiklaan. Myös Finanssiala ry ja EK esittävät säännöstä rajatta-

vaksi perustelujen mukaisesti. Ehdotukseen on pyritty avaamaan tiedon luovuttamisen menetelmiä ja arkaluonteisen tiedon käsittelyä koskevia perusteluja. Säännöstä on täsmennetty ehdotuksen perusteluista ilmenevillä rajauksilla lausuntopalautteen mukaisesti.

TIVIA ry on nostanut esityksen kannalta yleisinä kommentteina huolensa esityksen suhteesta tietosuojaan ja siihen, onko viranomaisilla riittävät pääsynrajoitukset ja käyttövaltuudet eli se, miten varmistutaan siitä, että asiattomat henkilöt eivät pääse katsomaan tarpeettoman laajasti tietoja. Lisäksi nostetaan esille auditointien riittävyys ja laajuus. TIVIA nostaa esille myös terminologian selkeyttämisen tarpeen. Ehdotuksessa on pyritty huomioimaan tietosuojaan liittyvät kysymykset mahdollisimman laajasti ja jatkovalmistelussa on tehty tietosuojaan liittyviä lisähuomioita. Viranomaiset toimivat tietosuojaan liittyvien vaatimusten mukaisesti myös ehdotuksen mukaisissa tilanteissa, eikä tähän esitetä sen suhteen muutoksia.

Oikeusministeriön lausunnossa kiinnitettiin erityistä huomiota ehdotuksen säätämisjärjestystä koskeviin perusteluihin. Siinä nostettiin esille tarve ensinnäkin täydentää perusteluja ehdotetun 316 a §:n osalta ja arvioida sen suhdetta perustuslain 10 §:ään. Lisäksi katsottiin tarpeelliseksi tehdä tarkempaa erottelua salassa pidettävän tiedon luovutuksia koskevan arvioinnin ja luottamuksellisen viestinnän suojaa koskevan arvioinnin välillä. Tämän lisäksi ministeriö katsoi, että ehdotetun 319 a §:n suhde muuhun sääntelyyn on paikoin epäselvästi ilmaistu ja kaipaa tältä osin selkeyttämistä. Se on katsonut, että kyse olisi uudesta tiedonluovutussäännöksestä, joka koskee osin sellaisia tietoja, joita nykyisen sääntelyn perusteella ei ole mahdollista luovuttaa. Ehdotuksen kuvaaminen poikkeuksesta nykyiseen sääntelyyn ei kuvaa tältä osin ehdotusta täsmällisesti. Jatkovalmistelussa perusteluja on pyritty täydentämään lausunnossa esitetyllä tavalla.

Oikeusministeriö on lisäksi todennut, että tiedonsaantioikeuden ulkopuolelle eivät rajaudu esimerkiksi arkaluonteiset tiedot. Jatkovalmistelussa tulisi ministeriön mukaan arvioida, onko tarkoitettu, että onko tarkoitettu, että kaikki mainitut viranomaiset voivat luovuttaa tai saada tietoja kaikkiin pykälässä tarkoitettuihin käyttötarkoituksiin vai olisiko sääntelyä mahdollista täsmentää tältä osin. Lisäksi tulisi arvioida, ovatko uhkaan liittyvät tiedontarpeet identtisiä tapahtuneeseen tietoturvaloukkaukseen nähden. Jatkovalmistelussa säännöstä on joiltain osin täsmennetty, joskin luovutettavien tietojen laajuus on katsottu aiheelliseksi pitää asiallisesti samana, mutta luovutettavien tietojen kuvausta on täsmennetty. Tietoturvaloukkausten moninaisuudesta ja ennakoimattomuudesta johtuen selvittämisen kannalta tarvittavien tietojen yksilöiminen tarkemmin on käytännössä erittäin haastavaa ja voi johtaa soveltamisvaikeuksiin, jos tarpeellinen luovutettava tieto ei löydykään yksityiskohtaisesta tietojen listasta. Vastaava moninaisuuden haaste liittyy myös uhkia koskevaan tiedonvaihtoon, jonka osalta on vaikea ennakolta arvioida, mitä tietoa on tarpeen vaihtaa.

Oikeusministeriö on myös esittänyt tarpeen tarkemmin kuvata laajemmin esityksen suhdetta tiedustelulainsäädännön säätämisen yhteydessä perustuslakivaliokunnan tärkeänä pitämään ns. palomuurisääntelyyn. Lisäksi säätämisjärjestys perusteluihin on katsottu tarpeelliseksi lisätä kuvaus henkilötietojen suojaan liittyen. Lisäksi ministeriö on esittänyt yksittäisiä täydennystarpeita eri säännösten perusteluihin. Kyseiset täydennystarpeet on tehty esityksen jatkovalmistelussa.

Esityksen varsinaisista vaikutuksista lausuttiin melko vähän, mutta Traficom nosti esille epäselvän terminologian mahdolliset haitalliset vaikutukset soveltamiseen. EK huomautti, että vaikutukset voivat vaihdella aloittain ja osalla aloista yhteistyö on tälläkin hetkellä jo melko toimivaa ja säännöllistä. FiCom nosti esille, että epäselväksi jää, miten viranomaisten keskinäinen tiedonvaihto auttaa yritystä tilanteissa, jossa se on joutunut merkittävän tietoturvaloukkauksen kohteeksi. Vaikutusarviointia ja muita perusteluja on täydennetty näiltä osin.

Muita lausunnoissa esitettyjä näkemyksiä olivat jo edellä mainittu yksityisen sektorin parempi kytkeminen tietoturvaloukkaustilanteisiin ja esitetään selvitettäväksi esteet julkisen ja yksityisen sektorin välisen tiedon vaihdon esteistä. Lisäksi yksityisen sektorin toimijat nostivat esille ns. yhden luukun periaatteen eri ilmoitusvelvollisuuksiin liittyen, joita on kertynyt runsaasti. Myös tiedonvaihtosääntelyä sähköisen viestinnän palveluista annettuun lakiin ehdotetaan tehtäväksi kokonaisarviointi. Edellä mainittuja ehdotuksia ei ole edistetty tässä lainsäädäntöhankkeessa, mutta ne on viety käsiteltäväksi sisäministeriön ja puolustusministeriön vetämässä kyberturvallisuuden selvityshankkeessa, jossa eri aiheita käsitellään laajemmin ja yleisemmällä tasolla.

7 Säännöskohtaiset perustelut

7.1 Laki sähköisen viestinnän palveluista

250 § *Viranomaisliittymät*. Pykälän 4 momenttiin ehdotetaan tehtäväksi lainsäädäntötekninen muutos siten, että säännös siirrettäisiin 316 §:n 5 momentin yhteyteen ja voimassa oleva 250 §:n *4 momentti* kumottaisiin. Voimassa olevassa 4 momentissa säädetään, ettei viranomaistehtävien hoidossa harjoitettuun viestintään viranomaisverkossa tai viranomaisviestintään liittyvässä viestintäpalvelussa sovelleta, mitä 316 §:ssä säädetään. Säännös siirrettäisiin 316 §:ään sen vuoksi, että kyseessä on 316 §:n soveltamisrajoitus, joka olisi soveltajan kannalta helpommin löydettävissä kyseisen pykälän yhteydestä kuin hajautettuna muualle lainsäädäntöön. Muutos olisi siten säädöstekninen eikä sillä tarkoitettaisi muutettavaksi voimassa olevaa oikeustilaa 316 §:n soveltamisalarajaukseen viranomaistehtävien osalta.

309 § *Virka-apu.* Pykälän *1 momenttia* ehdotetaan muutettavaksi Puolustusvoimien, poliisin ja suojelupoliisin Liikenne- ja viestintävirastolle antaman virka-avun osalta. Momentin muu virka-apusääntely ei muuttuisi. Kyseessä olisi erityissäännös suhteessa poliisilaissa (872/2011) ja Puolustusvoimista annetussa laissa (551/2007) näiden viranomaisten virka-avusta säädettyyn. Päätöksentekoon virka-avun antamisesta ja pyytämisestä päättämiseksi sovellettaisiin, mitä päätöksenteosta on muualla lainsäädännössä säädetty. Momenttiin lisättäisiin Liikenne- ja viestintävirastolle oikeus saada Puolustusvoimilta, poliisilta ja suojelupoliisilta virka-apua merkittävien tietoturvaloukkausten tai -uhkien selvittämiseksi sekä niistä aiheutuvien vaikutusten poistamiseksi. Puolustusvoimista annetun lain 11 §:n mukaan Puolustusvoimat voi antaa virka-apua yhteiskunnan turvaamiseksi siten kuin öljyvahinkojen torjuntalaissa (1673/2009) tai muussa laissa säädetään. Poliisilain 9 luvun 1 §:n nojalla poliisin on annettava pyynnöstä virka-apua muulle viranomaiselle, jos niin erikseen säädetään. Virka-apu voisi olla luonteeltaan asiantuntija-apua, välineistöä, tiloja tai laitteita.

Virka-avun tarve ja pyytäminen liittyisi tilanteisiin, joissa olisi kyse merkittävän tietoturvaloukkauksen tai sen vakavan uhkan selvittämisestä sekä siitä aiheutuvien vaikutusten poistamisesta. Virka-avun pyytäminen voisi tulla kyseeseen tilanteessa, jossa Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksella ei olisi riittävästi teknisiä tai asiantuntemukseen liittyviä voimavaroja tietoturvaloukkauksen selvittämiseen ja vaikutusten poistamiseen, ja Puolustusvoimilla, poliisilla tai suojelupoliisilla olisi käytössä tähän puutteeseen vastaavia voimavaroja ja kyvykkyyttä, joiden avulla Liikenne- ja viestintäviraston Kyberturvallisuuskeskus kykenisi tehtävästään suoriutumaan. Virka-apupyynnön tulisi liittyä kyseien viranomaisen tehtäväpiiriin. Loukkaukset voisivat olla mitä tahansa tilanteita, joissa kyse on merkittävästä tietoturvaloukkauksesta tai -uhkasta, mutta virka-apua annettaisiin viranomaisten omien toimivaltuuksien rajoissa. Esimerkiksi hyökkäyksen kohdeorganisaation asiakkaiden, yhteistyökumppanien tai muiden osallisten tai muutoin vaikutusten alaisten tahojen oikeuksien turvaaminen voi ylittää vastuutahon tosiasiallisen kyvykkyyden ja siten edellyttää laajojakin viranomaisten koordinoimia lisätoimia.

Virka-avun tarkoituksena olisi tukea Kyberturvallisuuskeskuksen suorituskykyä poikkeuksellisissa tilanteissa, minkä vuoksi virka-apu tarkoittaisi asiantuntija-apua esimerkiksi henkilöstön osalta taikka laitteiden, välineiden tai tilojen luovuttamista.

Tietoturvaloukkauksella tarkoitetaan mitä tahansa toimintaa, jolla on haitallisia vaikutuksia tietoturvallisuudelle. Sähköisen viestinnän palveluista annetun lain 3 §:n 28 kohdan nojalla tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. 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 tai oikeudetonta pääsyä tietojärjestelmän tietoihin taikka tietojärjestelmässä olevien tietojen luottamuksellisuuden vaarantumisen muulla tavoin. Tietoturvaloukkauksen haitalliset vaikutukset voisivat kohdistua esimerkiksi tietojen luottamuksellisuuteen, eheyteen ja saatavuuteen tai tietojärjestelmän avulla tarjotun tai sen välityksellä käytetyn palvelun toimintaan. Tietoturvaloukkauksena olisi ainakin pidettävä sellaista rikoksena syyksi luettavaa tekoa, jonka tunnusmerkistötekijöihin liittyisi oikeudetonta tunkeutumista tietojärjestelmään tai siellä olevien tietojen muuttamista, kopiointia, poistamista tai muuta oikeudetonta käsittelyä. Rikoslaissa säädetään rangaistavaksi viestintäsalaisuuden loukkaukset, tietoliikenteen häirintä, tietojärjestelmän häirintä ja tietomurto.

Merkittävällä tietoturvaloukkauksella tarkoitetaan vastaavaa tietoturvaloukkausta, jota sovelletaan esimerkiksi NIS-direktiivin ilmoitusvelvollisuuden kynnysarvona. Virka-apu ei koskisi tilanteita, joissa tietoturvaloukkaus aiheuttaa vain vähäisiä haittaa ja lievää vahinkoa tietoturvalle. Virka-apua edellyttävässä merkittävässä tietoturvaloukkauksessa tai –uhkassa on huomioitava myös niiden mahdolliset vaikutukset. Merkittävän tietoturvaloukkauksen tulisi ennalta arvioiden katsoa voivan aiheuttaa yhteiskunnalle huomattavaa haittaa ja vahinkoa. Merkittävyyttä arvioitaessa tulisi NIS-direktiivissäkin tarkoitetulla tavalla kiinnittää huomiota vaikutusten laajuuteen ja kestoon, maantieteelliseen levinneisyyteen sekä viestintäpalvelujen käytettävyyteen, eheyteen tai viestinnän luottamuksellisuuteen.

Virka-apua voitaisiin antaa myös tilanteessa, jossa on kyse merkittävän tietoturvaloukkauksen vakavasta uhkasta. Uhkalla tarkoitettaisiin tilannetta, joka syntyisi ilman ihmisen välitöntä tahallista aiheuttamista, ja jonka hyödyntäminen haitallisessa tarkoituksessa aiheuttaisi tietoturvaloukkauksen. Tällainen vakava uhka voisi olla esimerkiksi vakava haavoittuvuus laajasti käytössä olevassa ohjelmistossa tai järjestelmässä, jonka hyväksi käyttäminen rikollisissa tarkoitusperissä aiheuttaisi vakavia haitallisia vaikutuksia tietoturvalle. Uhkan vakavuutta arvioitaessa huomiota olisi kiinnitettävä haavoittuvuuden tai muun tietoturvauhkan laatuun, hyödynnettävyyteen haitallisessa tarkoituksessa, haitallisten vaikutuksien aiheutumisen todennäköisyyteen ja hyödyntämisestä aiheutuvien haitallisten vaikutuksien vakavuuteen. 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 ja lisäksi haitalliset vaikutukset olisivat epätodennäköisiä tai vain vähäisin keinoin estettävissä. Käytännössä tämän arviointi etukäteen voi kuitenkin olla haasteellista. Lisäksi haitallisten vaikutusten ehkäiseminen edellyttäisi viranomaisilta laajamittaisia toimenpiteitä tai hyvin edistynyttä teknistä osaamista, minkä vuoksi virka-apu voisi joissakin hyvin rajatuissa tilanteissa olla perusteltua myös ennalta ehkäisevässä toiminnassa uhkatilanteessa esimerkiksi vakavan haavoittuvuuden tai vakavan akuutin merkittävän

tietoturvaloukkauksen uhkan haitallisten vaikutuksien ehkäisemiseksi. Merkittävän tietoturvaloukkauksen vakavaa uhkaa tulisi siten tulkita suppeasti ja haavoittuvuuden hyväksikäytön todennäköisyyttä, vakavuutta ja hyväksikäytöstä aiheutuvien vaikutuksien haitallisuuden astetta painottaen.

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.

Pykälän *2 momenttia* ehdotettaisiin muutettavaksi siten, että Liikenne- ja viestintäviraston virka-avun antamisesta päättäisi jatkossa virasto itse liikenne- ja viestintäministeriön sijaan. Säännöksellä pyritään yhtenäistämään virka-apusääntelyä muiden virastojen vastaavien säännösten kanssa ja toisaalta tarkoituksenmukaista on, että virasto itse päättää toimivaltansa käyttämisestä. Virastolla itsellään on myös paras käsitys siitä, missä laajuudessa ja millaista virka-apua se voi antaa, minkä vuoksi on tarkoituksenmukaista, että virasto itse päättäisi virka-avun antamisesta. Kyse ei myöskään olisi esimerkiksi voimakeinojen käyttöä edellyttävästä virka-avusta, jolloin korkeamman tason päätöksentekoa ei ole tarpeen edellyttää tässäkään mielessä. Toisena muutoksena momentissa olisi, että virka-apu olisi luonteeltaan asiantuntija-apua, välineitä, tiloja tai laitteita vastaavalla tavalla, mitä poliisin, suojelupoliisin ja Puolustusvoimienkin osalta.

Nykyisestä 2 momentista ehdotetaan siirrettäväksi omaksi, uudeksi *3 momentikseen* maininta virka-avusta aiheutuneista kustannuksista, jolloin kustannuksia koskeva maininta toimisi vastavuoroisena säännöksenä eri viranomaisten virka-avusta aiheutuvien kustannusten osalta, eikä koskisi pelkästään Liikenne- ja viestintäviraston antamaa virka-apua. Muutoin virka-avun kustannuksista vastaamiseen ei esitetä muutosta. Uuteen 3 momenttiin lisättäisiin myös maininta siitä, että virka-avun antamisen edellytyksenä olisi, että se ei vaarantaisi virka-apua antavalle viranomaiselle säädettyjen muiden tärkeiden tehtävien suorittamista. Kyseessä olisi nykyisen virka-apusääntelyn osalta tavanomainen täsmennys, joka vastaisi muihin virka-avun antamista koskeviin erityissäännöksiin viime aikoina otettuja edellytyksiä. Säännös vastaisi esimerkiksi tartuntatautilain virka-apua koskevaan 89 §:ään 22.2.2021 alkaen lisättyä edellytystä virka-avun antamiselle. Tartuntatautilain 89 §:n muutoksen käsittelyn yhteydessä sosiaali- ja terveysvaliokunta sekä hallintovaliokunta edellyttivät virka-apusäännöksien edellytyksiltä riittävää täsmällisyyttä (StVM 1/2021 vp ja HaVL 29/2020 vp). Lisäys täsmentäisi voimassa olevaa oikeustilaa tältä osin.

Voimassa olevan lain *3 momentti* siirrettäisiin uudeksi *4 momentiksi*. Momentin sisältö on tarkoitus säilyttää pääasiassa sellaisenaan. Momentissa viitattaisiin kuitenkin jatkossa sekä 1 että 2 momentissa tarkoitettuun virka-apuun eli tilanteisiin, joissa Liikenne- ja viestintävirasto antaa virka-apua tai toisaalta saa virka-apua toisilta viranomaisilta. Sen mukaan 1 ja 2 momentissa

tarkoitettu virka-avun antaminen ei oikeuta Liikenne- ja viestintävirastoa antamaan toiselle viranomaiselle tietoja viesteistä, välitystiedosta tai sijaintitiedosta taikka luottamuksellisen radiolähetyksen sisällöstä.

316 § *Viestintää ja sijaintia koskevien tietojen käsittely ja hävittäminen.* Pykälän *5 momentin soveltamisalarajauksiin* ehdotetaan lisättäväksi 250 §:n 4 momentista kumottava säännös. Voimassa oleva 250 §:n 4 momentissa säädetään 316 §:n soveltamisen rajoittamisesta viranomaistehtävien hoitoon harjoitetun viestinnän osalta viranomaisverkoissa ja viranomaisviestintään liittyvässä viestintäpalvelussa. Muutos olisi säädöstekninen ja tehtäisiin sääntelyn selkeyttämiseksi siirtämällä soveltamisalarajaus voimassa olevan 316 §:n 5 momentissa olevien soveltamisalarajauksien yhteyteen. Muutoksella ei tarkoitettaisi muutettavaksi oikeustilaa siltä osin, kun 316 §:n soveltumista viranomaistoimintaan on kumottavalla 250 §:n 4 momentilla rajattu.

316 a § *Viestinnän välittäjän oikeus antaa tietoja Liikenne- ja viestintävirastolle.* Ehdotettu pykälä on uusi. Ehdotuksen mukaan viestinnän välittäjä voisi vapaaehtoisesti ja oma-aloitteisesti luovuttaa tietoja Liikenne- ja viestintävirastolle, jos se on tarpeen tietoturvaloukkausten tai uhkien selvittämiseksi tai ennaltaehkäisemiseksi. Viestinnän välittäjä määritellään SVPL 3 §:n 36 kohdassa. Viestinnän välittäjällä tarkoitetaan siten teleyritystä, yhteisötilaajaa ja sellaista muuta tahoa, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin. Tällaisia ovat siten myös esimerkiksi VPN-palvelujen tarjoajat (KKO 2022:23 kohta 13). Luovutettava tieto olisi välitystietoja tai tietoja viesteistä, joita viestinnän välittäjällä on oikeus käsitellä SVPL 272 §:n nojalla. Lain 272 §:ssä säädetään viestinnän välittäjän toimenpiteistä tietoturvan toteuttamiseksi. Säännöksellä ei luotaisi velvollisuutta luovuttaa tietoja vaan se perustuisi vapaaehtoisuuteen. Säännös olisi vastaava, kuin mitä saman lain 317 §:n 2 momentissa säädetään radiohäiriöihin liittyen.

Sähköisen viestinnän palveluista annetun lain 137 §:n 2 momentin mukaan sähköisiä viestejä ja välitystietoja on sallittua luovuttaa ainoastaan niille tahoille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa. Viestinnän välittäjät voivat luovuttaa toisilleen välitystietoja muun muassa silloin, kun tietoturvatoimenpiteiden toteuttaminen edellyttää teleyritysten yhteistyötä. Sen sijaan sähköisen viestinnän palveluista annetussa laissa ei tällä hetkellä ole nimenomaista säännöstä, jossa viestinnän välittäjä oikeutettaisiin luovuttamaan havaitsemiinsa tietoturvaloukkauksiin liittyviä välitystietoja tai viestin sisältöä oma-aloitteisesti Liikenne- ja viestintävirastolle, jonka lakisääteisenä tehtävänä kuitenkin on kerätä tietoja tietoturvaloukkauksista. Tällainen tilanne voi tulla esimerkiksi silloin, kun viestinnän välittäjä on havainnut SVPL 272 §:n mukaisten toimenpiteiden avulla tietoturvahäiriön tai tietoturvaa vaarantavan viestin sisällön. Teleyritysten ilmoitusvelvollisuudesta merkittävissä tietoturvaloukkauksissa tai muissa tapahtumissa, jotka voivat estää viestintäpalvelun toimivuuden tai häiritsevät sitä olennaisesti, säädetään SVPL 275 §:ssä. Viestinnän välittäjiä ovat kuitenkin myös muut kuin teleyritykset, jolloin viestinnän luottamuksellisuus ja henkilötietojen suoja rajoittavat muiden kuin teleyritysten tietojen antamista. Toisaalta teleyritystenkin ilmoituskynnys on asetettu merkittäviin tietoturvaloukkauksiin, jolloin pienemmät tietoturvaloukkauksia koskevat tiedot jäisivät tämän kynnyksen alapuolelle. Näillä tiedoilla voi olla merkitystä esimerkiksi tietoturvaloukkausten ennalta ehkäisemisessä.

Voimassa olevaan lainsäädäntöön sinällään sisältyy ajatus siitä, että Liikenne- ja viestintävirasto voi pyytää tietoonsa tulleen merkittävän tietoturvaloukkauksen tai sen uhkan kohdalla välitystietoja ja viestin sisältöä viestinnän välittäjältä. Tapahtuma ei kuitenkaan välttämättä ikinä tule Liikenne- ja viestintäviraston tietoon, sillä jo tieto viestin olemassaolosta on lähtökohtaisesti viestinnän luottamuksellisuuden piirissä. Viestinnän välittäjä voi myös tarvita Kyberturvallisuuskeskuksen tukea havaitsemansa tietoturvaloukkauksen selvittämiseen, kuten haittaohjelman toimintaperiaatteen selvittämiseen. Uusi säännös selkeyttäisi välitystietojen ja viestin

sisällön luovuttamista tällaisessa tilanteessa Kyberturvallisuuskeskukselle. Nykytilanteeseen liittyvät epäselvyydet ovat joissakin tapauksissa hidastaneet tapahtumien selvittämistä, kun tietoja viestinnän välittäjältä ei ole saatu kuin tekemällä useita perättäisiä tietopyyntöjä 316 §:n 2 momentin nojalla.

Luovutettavilla tiedoilla tarkoitetaan esimerkiksi tietoja haittaohjelmia sisältävistä tai levittävistä viesteistä ja niiden lähettäjiä tai komentopalvelimia koskevista välitystiedoista. Tietoja voisi luovuttaa myös havaituista palvelunestohyökkäyksistä ja niiden kohteista. Ehdotuksen nojalla luovutettuja tietoja voitaisiin käyttää Liikenne- ja viestintäviraston kansallisen tilannekuvan muodostamiseen esimerkiksi palvelunestohyökkäyksistä saatavien tietojen osalta. Lisäksi viestien sisältöjä voitaisiin käyttää tunnistamaan ja suodattamaan vastaavia viestejä, joilla pyritään levittämään haittaohjelmia. Viestejä koskevien tietojen luovuttaminen on olennaista myös haittaohjelmia sisältävien tekstiviestikampanjoiden ehkäisyssä. Pykälässä tarkoitetut tiedot viestin sisällöstä tarkoittaisivat siis lähtökohtaisesti sellaisia tietoja, jotka ovat luottamuksellisen viestinnän kannalta vähämerkityksellisiä, kuten lähinnä haittaohjelmia sisältäviä tai levittämiä, automaattisesti luotuja viestin sisältöjä tai muuten haitallisia käskyjä. Säännös mahdollistaisi myös automatisoidun tiedon luovuttamisen tapauksissa, joissa viestinnän välittäjän määrittelemät kriteerit tietojen luovuttamiselle sen SVPL 272 §:n nojalla toteuttamien toimenpiteiden kohdalla täyttyvät.

Viestinnän välittäjän yleisistä käsittelyperiaatteista säädetään sähköisen viestinnän palveluista annetun lain 137 §:ssä. Näitä ovat käsittely vain tarkoituksen vaatimassa laajuudessa, yksityisyyden suojan ja luottamuksellisuuden viestin suojan loukkauksen minimointi. Lisäksi käsittelyperiaatteisiin kuuluu se, että tietoja voidaan luovuttaa ainoastaan käsittelyoikeuden omaaville tahoille ja tietojen hävittäminen käsittelyn jälkeen, ellei muuta laissa säädetä. Lain 137 §:n 4 momentissa säädetään siitä, että viestejä ja välitystietoja saa käsitellä vain viestinnän välittäjän tai tilaajan lukuun toimiva, joka käsittelee viestejä ja välitystietoja tässä luvussa erikseen säädettyjen tarkoitusten toteuttamiseksi. Säännökseen otettaisiin viittaus 137 §:ssä viestinnän välittäjän yleistä käsittelyperiaatteista säädettyyn sen selkeyttämiseksi. Lisäksi sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetty salassapitovelvollisuus ehdotetaan ulottumaan myös 316 a §:n nojalla saatuihin tietoihin, jotta myös 316 a §:n nojalla mahdollisesti luovutettu tieto viesteistä, välitystiedoista, sijaintitiedoista tai luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta olisi sähköisen viestinnän palveluista annetun lain pääsäännön mukaisesti viranomaisessa salassa pidettävää.

Ehdotuksen nojalla saatua tietoa voitaisiin luovuttaa edelleen ainoastaan siten kuin 319 §:ssä säädetään viestintää ja välitystä koskevan tiedon luovuttamisesta. Lisäksi tietoja voisi luovuttaa muille viranomaisille ehdotetun 319 a §:n mukaisesti eli käytännössä vain erityisen poikkeuksellisissa tilanteissa.

319 § *Vaitiolovelvollisuus ja viesteihin liittyvien tietojen luovuttaminen.* Pykälän *1 momenttiin* ehdotetaan lisättäväksi maininta ehdotetusta 316 a §:stä. Momentin nojalla Liikenne- ja viestintäviraston ja tietosuojavaltuutetun saamat ja hankkimat tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta on pidettävä salassa. Ehdotetun lisäyksen johdosta ehdotettavan 316 a §:n nojalla saataviin tietoihin viesteistä tai välitystiedoista sovellettaisiin 319 §:ssä säädettyä salassapitovelvollisuutta. Voimassa olevan 319 §:n ja sen esitöiden nojalla on pääsääntö, että Liikenne- ja viestintäviraston ja tietosuojavaltuutetun on pidettävä salassa sähköisen viestinnän palveluista annetun lain nojalla saamansa tiedot viesteistä, välitystiedoista, sijaintitiedoista ja luottamuksen radiolähetyksen sisällöstä ja olemassaolosta (HE 221/2013, s. 226). Koska ehdotettavan 316 a §:n nojalla viestinnän välittäjillä olisi oikeus antaa oma-aloitteisesti näitä tietoja Liikenne- ja viestintävirastolle, olisi tarpeen säätää tarkennukseksi 319 §:ssä tarkoitetun salassapitoa koskevan pääsäännön ulottuvan

myös 316 a §:n nojalla saatuihin tietoihin, jotta tiedot eivät tulisi julkisiksi. Ehdotetun 1 momentin lisäyksen mukaisesti myös 316 § a:n nojalla luovutettavien säännöksessä tarkoitettujen tietojen osalta salassapitovelvollisuus olisi pääsääntö, josta voitaisiin poiketa ainoastaan laissa nimenomaisesti säädetyissä tilanteissa.

Pykälän *2 momentin 1 kohtaan* ehdotetaan tehtäväksi lakitekninen muutos, jolla poistetaan viittaus 316 §:n 2 momentin kohtiin ja jatkossa viitattaisiin vain kyseiseen momenttiin. Muutoksella ei ole merkitystä käytännön soveltamisen kannalta. Momentin *2 kohtaan* ehdotetaan lisättäväksi mahdollisuus luovuttaa tietoa myös Euroopan unionin ja Pohjois-Atlantin liitto Naton tietoturvaloukkauksia hoitaville tahoille. Tällaisia tahoja ovat käytännössä näiden organisaatioiden CERT-toiminnot. Voimassa oleva 2 kohta mahdollistaa tiedon luovuttamisen muussa valtiossa toimiville viranomaisille tai muille vastaaville tahoille, mutta ei kansainvälisille organisaatioille. Säännöstä olisi tarpeen täsmentää ehdotettavalla lisäyksellä, sillä tiedon luovuttaminen voi joissain tilanteissa olla tarpeen ottaen huomioon Suomen osallistumisen EU:n ja Naton toimintaan ja erityisesti näiden organisaatioiden CERT-toiminnot, jossa selvitetään muun muassa tietoturvaloukkauksia ja niiden uhkia. Tiedon luovuttaminen olisi aikaisempaa vastaavalla tavalla mahdollista vain sellaisille toimielimille, elimelle tai virastolle joiden tehtävän on ennalta ehkäistä tai selvittää viestintäverkkoihin ja –palveluihin kohdistuvaa tietoturvaloukkausta. Aikaisempaa vastaavasti pykälän 3 momentti asettaa rajoituksia luovutettavan tiedon laajuudelle. Tietoja on oikeus luovuttaa 3 momentin nojalla ainoastaan siinä laajuudessa, kun se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi, eikä tiedon luovuttamisella saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Pykälän 3 ja 4 momentteihin ei ehdoteta muutoksia.

Pykälän *5 momentti* ehdotetaan kumottavaksi. Jatkossa Liikenne- ja viestintävirasto päättäisi itse siitä, mille 2 §:n 2 momentissa tarkoitetulle taholle se voisi luovuttaa tietoturvaloukkausten yhteydessä saamiaan välitystietoja ja muita tietoja. Liikenne- ja viestintävirastolla itsellään on parhaat keinot arvioida sitä, mille muussa valtiossa toimivalle viranomaiselle tai muulle vastaavalla taholle, jonka tehtävänä on selvittää tietoturvaloukkauksia, se voi luovuttaa hallussaan olevaa tietoa.

319 a § *Tietojen luovuttaminen merkittävässä tietoturvaloukkauksessa tai -uhkassa.* Ehdotettu *pykälä on uusi*. 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 Ehdotuksen mukaan Liikenne- ja viestintävirastolla, poliisilla, suojelupoliisilla ja Puolustusvoimilla olisi salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa merkittävää tietoturvaloukkausta tai -uhkaa koskevat välttämättömät tiedot toisilleen. Tietoja voitaisiin luovuttaa tilanteessa, jos merkittävä tietoturvaloukkauksen tai sellaisen vakavan uhkan vaikutukset kohdistuvat pykälässä lueteltuihin, yhteiskunnan toiminnan kannalta elintärkeisiin toimintoihin tai niihin liittyviin tietoaineistoihin. Ehdotuksella on tarkoitus kattaa sellaiset tietoturvaloukkaustilanteet, jotka olisivat luonteeltaan vakavia.

Merkittävällä tietoturvaloukkauksella, tietoturvauhkalla, selvittämisellä ja vaikutusten poistamisella tarkoitetaan vastaavaa, mitä edellä on esitetty 309 §:n perustelujen yhteydessä. Soveltamisen lisäedellytyksenä olisi, että tietoturvaloukkauksen vaikutukset kohdistuisivat pykälässä lueteltuihin yhteiskunnan toiminnan kannalta elintärkeisiin toimintoihin. Esitetyllä säännöksellä katettaisiin myös tilanteet, joihin liittyy valtiollinen toimija tai vahva epäilys valtiollisesta toimijasta. Ehdotus kattaa myös tilanteet, joissa valtiollinen toimija käyttää tai sen voidaan perustellusti epäillä käyttävän ohjauksessaan ei-valtiollista toimijaa tavoitteidensa saavuttamiseksi.

Ehdotetun 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 lakisääteisen tehtävän hoitamiseksi ja tilanteen mahdollisimman sujuvan koordinoinnin ja toiminnan yhteensovittamisen mahdollistamiseksi. Viranomaisten lakisääteisiä tietoturvaloukkauksiin liittyviä tehtäviä on avattu tarkemmin nykytilan kuvausta koskevassa jaksossa.

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 ole katsottu mahdolliseksi rajata yksityiskohtaisesti tiettyihin tietoihin ottaen huomioon, että tietoturvaloukkaustilanteet voivat vaihdella luonteeltaan ja ominaisuuksiltaan erittäin laajasti, eikä näitä kaikkia tilanteita voida täsmällisesti ennakoida.

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. Tietojen luovuttaminen olisi määritelty rajoittumaan vain vastaanottavan viranomaisen toiminnan kannalta välttämättömiin tietoihin merkittävän tietoturvaloukkauksen tai sen vakavan uhkan selvittämisessä, ennaltaehkäisemisessä tai vaikutusten poistamisessa. Viranomaiset käyttäisivät tietoja toimivaltasäännöstensä puitteissa. Tiedot voisivat olla luonteeltaan myös henkilötietoja. Ehdotus sinällään mahdollistaa myös arkaluonteisen tiedon luovuttamisen, mutta käytännössä tällaisia tietoja sisältävää tietoa ei ole tarpeen vaihtaa viranomaisten välillä, koska esimerkiksi viestin sisällöstä ilmenevillä arkaluonteisilla tiedoilla ei ole merkitystä tietoturvaloukkauksen selvittämisen kannalta, jonka perusteella nämä tiedot jäävät luovuttamatta.

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. 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. 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. Erityislainsäädäntöön sisältyy myös esimerkiksi biometrisiin tietoihin liittyviä tiedon luovuttamista koskevia rajoituksia, jotka eivät kuitenkaan suoranaisesti ole merkityksellisiä tietoturvaloukkausten selvittämisen näkökulmasta.

Poliisin rikostorjuntatehtävistä johtuen poliisi käyttäisi säännöksen 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 ja saamansa tiedon avulla tutkii tietoverkkorikoksia ja pitää niistä myös yllä kansallista kyberrikollisuuden tilannekuvaa. Suojelupoliisin tiedon tarve perustuu erityisesti kansallisen turvallisuuden suojaamiseen, kuten laittoman verkkotiedustelun ja -vaikuttamisen havaitsemiseen, estämiseen ja paljastamiseen. Suojelupoliisi voisi käyttää ehdotuksen nojalla saatua tietoa siviilitiedustelutoiminnan kohdentamiseen ja tietoturvaloukkausten taustojen ja motiivien ja vaikutusten selvittämiseen siten, että se pystyy tuottamaan tietoa valtionjohdon ja muiden viranomaisten päätöksentekoon.

Puolustusvoimat vastaa Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta ja sen lakisääteisiä tehtäviä. Tehtävän suorittaminen edellyttää ajantasaista tilannekuvaa. Lisäksi Puolustusvoimien on pystyttävä arvioimaan maanpuolustuksen kannalta kriittisiin toimintoihin tai maanpuolustusjärjestelmään kohdistuvia tietoturvaloukkauksia ja -uhkia. Puolustusvoimilla on myös käytössään tietoa, osaamista ja laitteistoa, joka on keskittynyt etenkin näihin kaikkein vaativimpien tietoturvaloukkausten ja -uhkien analysointiin. Analyysin ja mahdollisen toteuttajan tunnistamisen ja paikantamisen kautta tieto siirtyy osaksi Puolustusvoimien tilannekuvaa, jonka avulla havaitaan ja tunnistetaan valtiolliset ja muut uhkatoimijat. Tilannekuvan perusteella voidaan käynnistää tarvittavat toimenpiteet valtiollisten ja muiden uhkatoimijoiden tunnistamiseksi sekä estää niiden pääsy puolustusjärjestelmän kannalta keskeisiin järjestelmiin ja tietoihin tai torjua uhkatoimijoiden operaatiot niitä vastaan. Puolustusvoimat käyttäisivät ehdotuksen nojalla saatua tietoa rikosten ennalta estämiseen, paljastamiseen ja selvittämiseen sekä esimerkiksi salaisten tiedonhankintakeinojen kohdentamiseen niiltä osin, kun ne kuuluvat Puolustusvoimien lakisääteisten tehtävien piiriin vastaavalla tavalla, mitä poliisin osalta on kuvattu. Puolustusvoimien sotilastiedustelun tarve liittyisi suojelupoliisin suorittaman siviilitiedustelun tavoin sotilastiedustelulaissa säädettyjen tehtävien hoitamiseen. Ehdotuksen nojalla saatua tietoa voitaisiin käyttää sotilastiedustelutoiminnassa käytettävien tiedustelumenetelmien kohdentamiseen sekä tietoturvaloukkausten taustojen, motiivien ja vaikutusten selvittämiseen siten, että sotilastiedustelu pystyy tuottamaan tietoa valtiojohdon päätöksenteon tukemiseksi ja laissa erikseen mainittujen Puolustusvoimien tehtävien suorittamiseksi..

Liikenne- ja viestintäviraston tarve tiedolle liittyy tietoturvaloukkausten tai uhkien tekniseen selvittämiseen ja vastaavien tilanteiden ennaltaehkäisemiseen sekä havaitsemiseen, joka tukisi osaltaan myös muiden viranomaisten toimintaa. Lisäksi virasto muodostaisi saadun tiedon avulla kyberturvallisuuden kansallista tilannekuvaa. Toisaalta Liikenne- ja viestintävirasto pystyisi osaltaan täydentämään ja rikastamaan muiden viranomaisten muilla tavoin hankkimaa tietoa oman tilannekuvansa perusteella, jolloin on mahdollista saada yksityiskohtaisempi kuvaus tilanteen kokonaisuudesta.

Ehdotuksen mukaisesti tietoja voitaisiin luovuttaa silloin, kun merkittävä tietoturvaloukkaus aiheuttaa tai uhkaa aiheuttaa vakavia haitallisia vaikutuksia julkisen vallan päätöksentekokyvylle, viranomaisten toimintaedellytyksille, kansalliselle turvallisuudelle tai maanpuolustukselle, tai

muille yhteiskunnan kriittisille toiminnoille. Nämä olisivat sellaisia toimintoja, joihin kohdistuva tietoturvaloukkaus tai sellaisen vakava uhka aiheuttaa tai uhkaa aiheuttaa yhteiskunnan toimintaedellytyksille merkittävää haittaa

Momentin *1 kohdassa* julkisen vallan päätöksentekokyvyllä tarkoitetaan pääosin vastaavaa, mitä on tarkoitettu valmiuslain ja asevelvollisuuslain 79 §:n muuttamisesta annetussa hallituksen esityksessä (HE 63/2022 vp, s. 40) julkisen vallan päätöksentekokyvyllä. Näin ollen sillä tarkoitetaan sellaisia toimia, joilla pyritään estämään tai muutoin merkittävästi haittaamaan ylimpien valtionelinten, eli eduskunnan, tasavallan presidentin tai valtioneuvoston päätöksentekoa taikka niiden toimintaa. Kyse voisi olla myös tietoturvaloukkausten selvittämisen kannalta keskeisten viranomaisten eli poliisin, suojelupoliisin, Puolustusvoimien ja Liikenne- ja viestintäviraston päätöksentekokyvystä. Kyse voisi olla esimerkiksi päätöksenteon kannalta tärkeisiin tieto- ja viestintäteknisiin palveluihin sekä tietojärjestelmiin kohdistuvasta häirinnästä, tietomurroista, haitta- tai vakoiluohjelmien levittämisestä, palvelunestohyökkäyksistä taikka äänestys- tai vaalituloksen manipuloinnista.

Kohdassa viranomaisten toimintaedellytyksien vaarantumisella tarkoitetaan viranomaisten lakisääteisten tehtävien hoitamisen vaarantumista. Tämä voi toteutua esimerkiksi julkisen sektorin digitaalisiin palveluihin kohdistuvan tietoturvaloukkauksen tai uhkan kautta.

Momentin *2 kohdassa* kansallisella turvallisuudella tarkoitettaisiin esimerkiksi ihmisten henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavaa toimintaa, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille taikka ulkomaalaista tiedustelutoimintaa. Kansallisen turvallisuuden käsitteen ydinalueeseen on perinteisesti katsottu kuuluvan myös maanpuolustus, mutta selkeyden vuoksi asia mainitaan nimenomaisesti ehdotettavassa pykälässä kansallisen turvallisuuden rinnalla. Kansallista turvallisuutta uhkaavalla toiminnalla tarkoitettaisiin lähtökohtaisesti toimintaa, joka ei ensisijaisesti kohdistu kehenkään yksilönä vaan yleisemmin yhteiskuntaan ja sen ihmisyhteisöön (ks. HE 198/2017 vp).

Momentin 2 kohdassa maanpuolustukseen kohdistuvilla vakavilla vaikutuksilla tarkoitetaan sellaisiin toimintoihin kohdistuvaa haittaa, joilla olisi merkitystä Suomen maanpuolustuksen kannalta. Näitä olisivat esimerkiksi Puolustusvoimien käytössä olevat johtamisjärjestelmät ja siihen sisältyvät tietojärjestelmä sekä viranomaisverkot taikka muut tietoliikenneyhteydet. Yhtä lailla maanpuolustukseen vaikuttavat katsotut maanpuolustuksen varusteluun liittyvät toimitusketjut ja palvelut.

Momentin *3 kohdan* mukaan tietoja voitaisiin vaihtaa myös silloin, kun merkittävän tietoturvaloukkauksen haitalliset vaikutukset kohdistuisivat välttämättömiin sosiaali- ja terveydenhuollon tai pelastustoimen palveluihin. Vaikutukset voisivat joko suoraan tai välillisesti vaarantaa potilasturvallisuutta esimerkiksi järjestelmien tai verkkoon kytkettyjen terveydenhuollon laitteiden tai järjestelmien kautta. Pelastustoimen osalta vaikutuksia voisivat olla esimerkiksi viiveet tai esteet pelastustoimen tehtävien hoitamisessa, jotka aiheutuisivat esimerkiksi järjestelmähäiriöistä hälytyksien tai muun pelastustoimen viestinnän välityksessä tai esimerkiksi sijaintipalveluiden häiriöistä.

Momentin *4 kohdassa* kohdassa on lueteltu energia-, vesi-, elintarvike- ja lääkehuolto sekä muut välttämättömät hyödykkeet. Näiden toimintojen ylläpitäminen perustuu pitkälti varsinaisen tuotannon lisäksi erilaisiin tietojärjestelmiin, joilla prosesseja hallinnoidaan. Energiasektorin on erityisen merkityksellinen yhteiskunnan toimintojen ylläpitämisen kannalta. Siihen kohdistuvilla häiriöillä on laajat seurannaisvaikutukset myös muihin elintärkeisiin toimintoihin. Kriitti-

siksi energia-alan toiminnoiksi voidaan katsoa eri energianlähteet ja tuotantorakenteet, polttoaineet, sähkön ja lämmön tuotanto sekä siirto- ja jakelujärjestelmät. Myös vesihuolto, elintarvikkeet, lääkkeet ovat alttiita haitallisille vaikutuksille joko valmistusprosessin aikana tapahtuville hyökkäyksille tai niiden jakeluun puuttuville hyökkäyksille. Muilla välttämättömillä hyödykkeillä voitaisiin tarkoittaa esimerkiksi välttämättömän teollisuustuotannon ylläpitämiseen tarkoitettujen raaka-aineiden huoltoa.

Momentin *5 kohdan* mukaan yhteiskunnan elintärkeitä toimintoja olisivat välttämättömät maksu- ja arvopaperipalvelut. Näitä ovat rahoitus- ja vakuutuspalvelujen tarjoaminen, kaikki maksuliikenne, arvopaperien selvitys-, toimitus- ja säilytystoiminta, käteisrahahuoltojärjestelmä, korttimaksamisen infrastruktuurin ja korttivarmennukset sekä päivittäiskaupan finanssitoiminnot. Maksu- ja arvopaperipalvelut toimivat nykyisin pitkälti verkkoympäristössä erilaisten tietojärjestelmien varassa, minkä vuoksi ne ovat sen vuoksi alttiita myös hyökkäyksille. Esimerkiksi maksuliikenteen häiriöillä on laajoja vaikutuksia yhteiskunnan toimintakykyyn yksilötasolta organisaatiotasolle aina valtion maksuliikenteeseen ulottuen.

Momentin *6 kohdan* mukaan viranomaiset voisivat vaihtaa tietoja myös, jos tietoturvaloukkauksella olisi vakavia vaikutuksia yhteiskunnan kriittisten liikenne- ja viestintäpalvelujen saatavuuteen. Liikennepalvelut ja niiden ohjausjärjestelmät toimivat esimerkiksi elintarvikelogistiikan elinehtona niin maalla, merellä kuin ilmassa. Lisäksi esimerkiksi liikenteen automaatiojärjestelmällä on merkittäviä vaikutuksia liikenneturvallisuuteen. Käytännössä kaikkien edellä mainittujen toimintojen järjestelmien toiminnan edellytyksenä on niihin liittyvät viestintäpalvelut ja viestintäverkot. Yleisiin viestintäpalveluihin kohdistuvilla tietoturvaloukkauksilla voi energiasektorin tavoin olla kauaskantoisia kerrannaisvaikutuksia usealle eri toimialalle.

Momentin *7 kohdassa* on mainittu erikseen 1-6 kohdissa lueteltujen toimintojen ylläpitävät tieto- ja viestintätekniset palvelut sekä niiden tietoaineistot. Sinällään on selvää, että merkittävä tietoturvaloukkaus yleensä kohdistuu nimenomaan toimintoja ylläpitäviin järjestelmiin palveluihin, mutta näiden ylläpitäminen voi olla myös ulkoistettu taholle, joka ei varsinaisesti tuota kyseistä palvelua vaan tuottaa esimerkiksi laajasti käytössä olevaa ohjelmistoa, jonka varaan yhteiskunnan toiminnan kannalta keskeistä toimintoa ylläpitävä järjestelmä nojaa. Kohdassa on myös mainittu erikseen 1–6 kohtiin liittyvät tietoaineistot. Kohdalla katettaisiin tilanteet, joissa kriittisiin toimintoihin liittyviin tietoaineistoihin kohdistuisi tietomurto, jonka seurauksena on mahdollista, että kyseiset tiedot vuotavat hyökkääjien toimesta laajasti julkisuuteen tai päätyvät tietoa oikeudetta hyväksikäyttävän tahon haltuun. Yhteiskunnan toiminnan kannalta keskeisiin toimintoihin liittyvät tietoaineistot sisältävät paljon salassa pidettävää, luottamuksellista ja luonnollisiin henkilöihin liittyvää arkaluonteista tietoa, johon kohdistuvan tietoturvaloukkauksen tai sellaisen vakavan uhkan tilanteessa viranomaisten on pakko pystyä toimimaan sujuvasti yhdessä. Tietomurroille ominaista on, että niiden tapahtuminen ei välttämättä vaikuta esimerkiksi jonkin keskeisen palvelun saatavuuteen, mutta sillä voi olla merkittäviä haitallisia vaikutuksia muiden oikeushyvien, kuten yksityiselämän suojan tai kansallisen turvallisuuden kannalta riippuen siitä, mihin tietomurto kohdistuisi.

Edellä mainittuihin yhteiskunnan elintärkeisiin toimintoihin joko suoraan tai välillisesti vaikuttava tietoturvaloukkaus tai sellaisen uhka on omiaan vaikuttamaan laajasti koko yhteiskuntaan varsinkin, jos loukkauksen vaikutukset kohdistuisivat samanaikaisesti useammalle kuin yhdelle alueelle. Laajoista keskinäisriippuvuuksista johtuen vaikutukset voisivat ulottua varsinaista hyökkäyksen kohdetta laajemmalle. Tällainen keskinäisriippuvuuksien kannalta merkittävä toiminto olisi esimerkiksi sähköntuotanto tai –jakelu taikka viestintäverkot. Vaikutukset voivat kohdistua yhteen tai useampaan toimintoon. Mikäli yhteen toimintoon kohdistuva vaikutus ei yksin olisi vakava, vakavia haitallisia vaikutuksia voi kuitenkin syntyä useampiin toimintoihin kohdistuvien vaikutuksien yhteisvaikutuksesta.

Ehdotuksen mukaiseen tiedonvaihtoon liittyvää salassapitosäänteleystä ja tiedon luovutuksen rajoituksista poikkeamisen kynnystä on pidettävä verrattain korkealla. Voimassa olevilla tiedonvaihtoa rajoittavilla säännöksillä on lähtökohtaisesti tarkoitus turvata perustuslaissa turvattua yksityiselämän suojaa ja luottamuksellisen viestin suojaa ja siitä poikkeamista voidaan pitää perusteltuna vain erittäin poikkeuksellisissa tilanteissa. Myös yritykset voivat pitää niihin kohdistuneisiin tietoturvaloukkauksiin liittyviä tietoja sensitiivisinä ja ne voivat olla myös salassa pidettäviä.

Päätöksen lainsäädännön soveltamisesta tekisi joku 1 momentissa mainituista viranomaisista, jonka tietoon on tullut perusteltu epäilys momentin kriteerit täyttävästä tietoturvaloukkauksesta tai uhkasta, ja jolla on hallussaan siihen liittyvää tietoa. Viranomaisten tavanomaisen yhteistoiminnan ja siinä vaihdettavan tiedon yhteydessä voisi myös muodostua tilanne, että eri lähteistä saatuja tietoja yhdistämällä voidaan päätyä lopputulokseen, että kyse on 1 momentissa tarkoitetusta tilanteesta. Viranomaiset voisivat päätyä johtopäätökseen myös yhdessä tavanomaisen yhteistoiminnan kautta.

Ehdotetussa *2 momentissa* täsmennettäisiin tiedon käyttötarkoitusta. Tiedon käytön rajoittaminen koskisi vain niitä tietoja, joiden luovuttamiseen liittyy rajoituksia tai salassapitovelvoitteita ja joista 1 momentissa ehdotetaan poikettavaksi. Käyttöä ei siten ole tarkoitettu rajattavaksi niiden tietojen osalta, joiden luovuttaminen muissakin olosuhteissa olisi mahdollista ilman käyttötarkoitukseen liittyviä rajoituksia. Tietoa voitaisiin käyttää tietoturvaloukkausten tai vakavien uhkien selvittämiseksi, ennalta ehkäisemiseksi tai vaikutusten poistamiseksi. Ensi sijassa tietoa käytännössä käytettäisiin sen tietoturvaloukkauksen tai selvittämiseksi, jonka tapahtumisen seurakusena tietoa on viranomaisten välillä luovutettu. Tietoa voitaisiin käyttää kuitenkin myös vastaavan kaltaisten tietoturvaloukkausten havaitsemiseksi ja sitä kautta uusien tilanteiden ennaltaehkäisemiseksi. Siten momentti mahdollistaisi esimerkiksi tietojen käytön samaa haavoittuvuutta tai komentopalvelinta hyödyntävien myöhempien tieturvaloukkausten tai niiden uhkien tunnistamiseen Liikenne- ja viestintäviraston ylläpitämän HAVARO-järjestelmän avulla. Tietoa voitaisiin lisäksi hyödyntää esimerkiksi poliisin, suojelupoliisin ja Puolustusvoimien teletiedonhankintaan liittyvien toimenpiteiden kohdistamisen ja niitä koskevien vaatimusten perusteena, joiden hyväksymisestä sinällään vastaisi kuitenkin tuomioistuin.

Ehdotuksen 2 momentin mukaan tietoturvaloukkausten ennalta ehkäisemisen, selvittämisen tai vaikutusten poistamisen kannalta tarpeeton tieto on poistettava. Muutoin tiedon hävittämiseen sovelletaan SVPL 316 §:n 4 momentin säännöstä tietojen hävittämisestä.

Ehdotuksen *3 momentissa* säädettäisiin tiedon käyttörajoituksista ja edelleen luovuttamisesta. Tiedon luovuttajan olisi luovutuksen yhteydessä ilmoitettava, mikäli tiedon käyttöön sisältyisi rajoituksia sen käyttötarkoituksen, edelleen luovuttamisen tai sen palauttamisen osalta. Tällaisia rajoituksia voisivat olla esimerkiksi poliisitoimen henkilötietolain 42 §:ssä tai Puolustusvoimien henkilötietolain 25 §:ssä säädetty henkilötietojen tarkastusoikeuden rajoitus. Näiden säännösten tarkoituksena on turvata rikostutkinta ja ehdotettu 3 momentti ulottaisi näitä rajoituksia myös muihin viranomaisiin. Vastaavanlaisia rajoituksia voisi sisältyä myös esimerkiksi eri viranomaisten kansainvälisten kumppaneiden luovuttamien tietojen edelleen luovuttamiseen tai käyttötarkoituksen rajoittamiseen.

7.2 Laki henkilötietojen käsittelystä Puolustusvoimissa

29 § *Oikeus luovuttaa henkilötietoja lakisääteisten tehtävien suorittamiseksi.* Pykälän *1 momentin* 18 alakohtaa ehdotetaan muutettavaksi siten, että Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen tehtävien osalta viitattaisiin myös sen erityisiin tehtäviin, joista on säädetty sähköisen viestinnän palveluista annetussa laissa. Lisäksi ehdotetaan poistettavaksi kohdasta

sana ’kyberturvallisuuskeskus’, sillä SVPL:n mukaisia erityisiä tehtäviä hoidetaan Liikenne- ja viestintävirastossa muuallakin kuin sen Kyberturvallisuuskeskuksessa.

SVPL 304 §:n 1, 7, 9 ja 10 kohdassa määriteltyjä erityisiä tehtäviä ovat sähköisen viestinnän toimivuuden, häiriöttömyyden ja turvallisuuden edistäminen, kerätä tietoa verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvista tietoturvaloukkauksista ja niiden uhkista sekä viestintäverkkojen ja viestintäpalvelujen vika- ja häiriö-tilanteista. Lisäksi näitä tehtäviä olisivat radioviestinnän häiriön sekä radiolaitteen tai telepäätelaitteen viestintäverkolle, radiolaitteelle, telepäätelaitteelle tai sähkölaitteistolle aiheuttamien häiriöiden syiden selvittäminen sekä verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin sekä tietojärjestelmiin kohdistuvien tietoturvaloukkausten ja niiden uhkien selvittäminen.

Kyberhäiriötilanteisiin liittyvien tehtävien hoitamisessa on tarve vaihtaa erilaista tietoa viranomaisten välillä, kuten on kuvattu edellä 319 a §:n perusteluissa. Ehdotettu muutos täydentäisi muuta tiedonvaihtoa koskevaa sääntelyä Puolustusvoimien ja Liikenne- ja viestintäviraston välillä. Huomionarvoista on, että sääntely koskee vain henkilötietoja, eikä sen nojalla voida luovuttaa viestinnän luottamuksellisuuden piirissä olevia tietoja ilman erillistä käsittelyperustetta näille tiedoille.

7.3 Laki henkilötietojen käsittelystä poliisitoimessa

22 § *Muu henkilötietojen luovuttaminen viranomaisille.* Ehdotuksen mukaan poliisitoimesta voitaisiin jatkossa luovuttaa henkilötietoja pyynnöstä tai oma-aloitteisesti Liikenne- ja viestintävirastolle myös SVPL:ssä säädetyn tehtävän hoitamiseksi vastaavasti, mitä on edellä ehdotettu Puolustusvoimien oikeudesta luovuttaa henkilötietoja Liikenne- ja viestintävirastolle. Tähänkin asti tietoja on voitu luovuttaa 22 §:n 3 momentin nojalla, jonka mukaan poliisi saa perustellusta syystä luovuttaa salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona viranomaiselle henkilötietoja, jotka ovat välttämättömiä viranomaisen laissa säädetyn tehtävän suorittamiseksi. Ehdotus selkeyttäisi osaltaan poliisin ja Liikenne- ja viestintäviraston välistä tiedonvaihtosääntelyä.

8 Voimaantulo

Ehdotetaan, että lait tulevat voimaan 1.2.2023.

9 Toimeenpano ja seuranta

Esityksen toimenpanotoimenpanon yhteydessä on tarkoitus tiedottaa laajasti tietoturvallisuuden kannalta merkityksellisiä viranomaisia uuden lainsäädännön sisällöstä. Keskeiset viranomaiset ovat jo valmistelun aikana harjoitelleet säännöksen soveltamista ja olleet tiiviisti mukana sen valmistelussa. Lainsäädännön toimivuutta seurataan tapauskohtaisella arvioinnilla, mikäli sitä joudutaan soveltamaan käytännössä.

10 Esityksen riippuvuus muista esityksistä

Lakiehdotukset liittyvät kahteen muuhun vireillä olevaan sähköisen viestinnän palveluista annetun lain muutokseen. Hallituksen esitys laiksi sähköisen viestinnän palveluista annetun lain muuttamisestä sekä Liikenne- ja viestintävirastosta annetun lain muuttamisesta (HE 170/2022 vp) on annettu eduskunnan käsiteltäväksi ja koskee julkisesti säänneltyä satelliittipalvelua. Lisäksi tämän esityksen jälkeen annetaan hallituksen esitys sähköisen viestinnän palveluista annetun lain muuttamisesta, joka koskee television- ja radio-ohjelmien siirtovelvoitteita. Ehdotukset eivät koske samoja pykäliä.

11 Suhde perustuslakiin ja säätämisjärjestys

Lakiehdotus sisältää perustuslain kannalta merkityksellisiä ehdotuksia suhteessa perustuslain 2 §:n 3 momentissa säädettyyn edellytykseen julkisen vallan käytön perustumisesta lakiin virka-avun osalta, perustuslain 10 §:ssä turvattuun yksityiselämän ja luottamuksellisen viestin suojaan tietojen vaihtamista koskevien ehdotusten osalta ja perustuslain 12 §:n 2 momentissa turvattuun viranomaistoiminnan julkisuusperiaatteeseen.

11.1 Virka-apu

Ehdotetulla 309 §:llä säädettäisiin poliisin, suojelupoliisin ja Puolustusvoimien antamasta virka-avusta Liikenne- ja viestintävirastolle merkittävien tietoturvaloukkausten ennalta ehkäisemiseksi, selvittämiseksi ja vaikutusten poistamiseksi. Virka-apusääntely on merkityksellistä perustuslain oikeusvaltioperiaatteen kannalta. Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Lähtökohtana on, että julkisen vallan käytön tulee aina olla palautettavissa eduskunnan säätämässä laissa olevaan toimivaltaperusteeseen. Toimivaltasääntely on yleensä merkityksellistä myös perustuslaissa turvattujen perusoikeuksien näkökulmasta (PeVL 51/2006 vp, s. 2/I). Ehdotetulla virka-apusääntelyllä on merkitystä myös perustuslaissa turvatun yksityisyyden suojan ja luottamuksellisen viestin suojan kannalta.

Virka-avussa olisi kysymys Liikenne- ja viestintäviraston toiminnasta ja sille laissa säädettyjen tehtävien suorittamisesta. Liikenne- ja viestintävirasto voisi pyytää poliisilta, suojelupoliisilta tai Puolustusvoimilta virka-apua siten, että virka-apua antava viranomainen hyödyntäisi suorituskykyään Kyberturvallisuuskeskukselle kuuluvan tehtävän suorittamiseksi. Ehdotuksella ei luotaisi Kyberturvallisuuskeskukselle uusia tehtäviä tai toimivaltuuksia, vaan kysymys olisi Liikenne- ja viestintävirastolle SVPL 304 §:ssä ja erityisesti sen 10 kohdassa säädetyn tehtävän toteuttamisesta. Virka-apua voisi pyytää ja antaa vain merkittävissä tietoturvaloukkaustilanteissa, joissa intressi tietoturvaloukkauksen selvittämiselle ja torjumiselle on korkeampi kuin tavanomaisissa tietoturvaloukkauksissa. Virka-apu olisi rajattu merkittäviä tietoturvaloukkauksia koskeviin tilanteisiin, mutta myös vakaviin uhkiin, joilla voidaan säännöskohtaisissa perusteluissa tarkemmin kuvatulla tavalla tarkoittaa lähtökohtaisesti sellaisia vakavia ja laajalle ulottuvia järjestelmähaavoittuvuuksia, jonka hyödyntämisellä voisi olla vakavia vaikutuksia julkisen vallan päätöksentekokykyyn, yhteiskunnan kriittiseen infrastruktuuriin, yleiseen järjestykseen tai turvallisuuteen. Vakavaa uhkaa koskevaa kirjausta tulisi perustelujen mukaan tulkita suppeasti ja haavoittuvuuden hyväksikäytöstä aiheutuvat vaikutukset huomioiden.

Sinällään jonkin asteista uhkaan perustuvaa virka-apusääntelyä sisältyy myös Puolustusvoimien virka-avusta poliisille annetun lain (342/2022) säännöksiin, joka on säädetty perustuslakivaliokunnan myötävaikutuksella. Sääntely sisältää virka-avun antamista muun muassa ihmisten hengelle tai terveydelle vakavaa vaaraa aiheuttavan rikoksen estämiseksi ja keskeyttämiseksi.

Perustuslakivaliokunta on lausuntokäytännössään todennut, että viranomaisen toimintaa ei voida rakentaa virka-apuinstituution varaan (PeVL 3/2022 vp. s. 2). Ehdotettu sääntely ei olisi ristiriidassa tämän periaatteen kannalta vaan kyse olisi aiempaa vastaavalla tavalla poikkeuksellisesta järjestelystä, jota hyödynnettäisiin vasta, jos Liikenne- ja viestintäviraston omat resurssit eivät olisi riittävät sen lakisääteisten tehtävien hoitamiseksi ja muulla viranomaisella olisi tarvittavaa osaamista ja muita resursseja tämän tehtävän tukemiseksi. Resurssit ja suorituskyky, jonka pyytämisestä ja antamisesta virka-apuna näiden tehtävien suorittamisessa on kysy-

mys, ovat erityisesti tietoteknisiä voimavaroja ja -kyvykkyyttä. Virka-avussa olisi kysymys viranomaisten yhteisen kyvykkyyden hyödyntämisestä, jos Liikenne- ja viestintävirasto ei poikkeuksellisesti kykenisi omin voimavaroin suoriutumaan sille säädetyistä tehtävistä, kuten esimerkiksi erityisen laajassa tai poikkeuksellisen vakavassa kyberhyökkäystilanteessa.

Virka-apua koskevien ehdotusten yhteydessä hallintovaliokunta on nostanut esiin, että yksinomaan virka-avun antamisesta säätäminen toiselle viranomaiselle ei vielä ilmaise virka-avun antamiseen liittyvää toimivaltaa, vaan virka-avun antamiseen tulee olla joko yksilöidympi tai yleisempi sisällöllinen toimivaltuus lainsäädännössä (HaVL 29/2020 vp s. 6–7). Ehdotus sisältää virka-avun rajaukset tietoturvaloukkaustilanteisiin tai sellaisten vakaviin uhkiin ja toisaalta virka-avun luonnetta on rajattu ehdotuksessa koskemaan asiantuntija-apua, välineistöä, tiloja tai laitteita.

Virka-avun osalta perustuslakivaliokunta on kiinnittänyt huomiota siihen, että virka-avun tulee perustua viranomaisten toimivaltaan hoitaa jotain tehtävää (PeVL 10/2005 vp, s. 2/II). Poliisin ja suojelupoliisin osalta virka-avun antaminen perustuu poliisin perustehtäviin oikeus- ja yhteiskuntajärjestyksen ja kansallisen turvallisuuden sekä erityisesti rikosten ennalta estämisen, paljastamisen ja selvittämisen osalta. Poliisille on säädetty verkkoympäristöön liittyen lukuisia toimivaltuuksia esimerkiksi poliisilain 5 tai 5 a luvun säännöksissä. Puolustusvoimien osalta kyse olisi sen perustehtävään liittyvästä Suomen alueellisen koskemattomuuden turvaamisesta ja toisaalta Puolustusvoimista annetun lain 2 §:ssä tarkoitetusta virka-avun antamisesta muun muassa yhteiskunnan turvaamiseksi. Virka-apu ei ole ehdotuksessa katsottu sisältävän niinkään erityisten toimivaltuuksien käyttämiseen liittyviä ehdotuksia, vaan kyse olisi enemmän vastaavassa ympäristössä toimivaltuuksiensa nojalla toimiville viranomaisille käyttöön annettavista resursseista, kuten osaamisen ja laitteistojen hyödyntämisestä. Ehdotuksen ei ole tältä osin arvioitu olevan ristiriidassa perustuslain 2 § :n kanssa.

Ehdotuksen mukaan Liikenne- ja viestintäviraston antamasta virka-avusta päättäisi jatkossa liikenne-ja viestintäministeriön sijaan virasto itse. Ehdotus perustuu siihen, että viranomainen itse päättää toimivaltaansa kuuluvista asioista, eikä ministeriöllä ole tässä erityistä roolia. Perustuslakivaliokunta on lausuntokäytännössään ottanut kantaa päätöksenteosta virka-avun antamisessa. Puolustusvoimien voimankäyttöapuun kohdistuvassa virka-avussa valiokunta on pitänyt tärkeänä, että myös kiiretilanteissa virka-apupäätökset tehtäisiin eduskunnalle vastuunalaisen ministeriön johdolla, mikäli päätöstä ei ole kiireen vuoksi mahdollista tehdä valtioneuvoston yleisistunnossa (PeVL 23/2005 vp, s. 5/II, PeVL 3/2022 vp, s. 5). Valiokunta on kuitenkin rajannut tällaiset korkeatasoista päätöksentekoa vaativat virka-apukysymykset voimankäyttötilanteisiin. Nyt käsiteltävänä oleva ehdotus ei olisi tämän periaatteen kanssa ristiriidassa, koska Liikenne- ja viestintäviraston antama virka-apu olisi luonteeltaan asiantuntija-apua ja muita resursseja, eikä virka-apu edellyttäisi voimakeinojen käyttöä. Myös Puolustusvoimien poliisille antaman, muun kuin vaativaa virka-apua koskevan virka-avun antamisesta päättää pääesikunta taikka Maavoimien, Merivoimien tai Ilmavoimien esikunta.

Virka-apua koskevien ehdotusten ei edellä esitetyn perusteella katsota olevan ristiriidassa perustuslain kanssa.

11.2 Viranomaisten välinen tiedonvaihto ja tiedon käyttötarkoitus

11.2.1 Viestinnän luottamuksellisuus

Hallituksen esityksen keskeinen perusoikeudellinen kysymys liittyy perustuslain 10 §:ssä suojattuun yksityiselämän suojaan, erityisesti sen 2 momentissa turvattuun luottamuksellisen viestin suojaan. Euroopan unionin perusoikeuskirjan 7 artiklassa on säädetty siitä, että jokaisella on

oikeus siihen, että hänen viestejään kunnioitetaan ja 8 artiklassa säädetään oikeudesta henkilötietojen suojaan. Lisäksi henkilötietojen käsittely tulee tapahtua tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Luottamuksellisen viestin suoja on turvattu myös Euroopan ihmisoikeussopimuksen (SopS 63/1999) 8 artiklassa, jonka mukaan jokaisella on oikeus nauttia kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen paitsi, kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraaliin suojaamiseksi tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi. Perustuslakivaliokunta on todennut, että perustuslain 10 §:ssä turvatun yksityiselämän suojan lähtökohtaan 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).

Perustuslain 10 §:n 4 momenttiin on sisällytetty erityisiä rajoituslausekkeita, joissa annetaan tavallisen lain säätäjälle valtuus perusoikeuden rajoittamiseen ja toisaalta asetetaan lainsäätäjän harkintavaltaa rajoittavia lisäkriteerejä. 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). 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. Ehdotuksessa olisi kyse perustuslain 10 §:n 4 momentissa tarkoitetusta välttämättömästä rajoituksesta yksilön tai yhteiskunnan turvallisuuden takaamiseksi mutta myös vakavan kansallisen uhkan vuoksi.

Esityksessä ehdotetaan tehtäväksi poikkeus salassapitosäännöksiin ja tiedon luovuttamista koskeviin rajoituksiin, joiden estämättä poliisi, suojelupoliisi, Puolustusvoimat ja Liikenne- ja viestintävirasto voisivat vastavuoroisesti luovuttaa tietoja merkittävissä tietoturvaloukkaustilanteissa tai sellaisten vakavissa uhkissa. Tietojen luovuttaminen käytännössä koskisi erityisesti viestintään liittyvien tietojen luovuttamista, joiden luovuttamista koskevia rajoituksia on erityisesti Liikenne- ja viestintävirastoa koskevassa lainsäädännössä. Tietojen luovuttaminen koskisi myös henkilötiedoksi katsottuja tietoja. Ehdotus siten laajentaa tiedon luovuttamista yksittäisissä tilanteissa nykyisestä.

Yleisesti arvioituna ehdotuksella on ensisijaisesti luottamuksellisen viestin suojaa rajoittava vaikutus tiedonvaihtotilanteissa. Toisaalta tiedonvaihdon perusteena on muun muassa luottamuksellisen viestinnän suojaaminen, jolloin luottamuksellisen viestinnän suojaamista välillisesti edistettäisiin sitä yksittäisessä tilanteessa rajoittamalla. Luottamuksellisen viestin suojaamista koskeva perusoikeusvaikutus olisi siten välillinen seuraus niistä toimenpiteistä, joita viranomaiset tietoturvaloukkauksen selvittämisen, ennaltaehkäisemisen ja vaikutusten poistamisen yhteydessä tekevät.

Luottamuksellisen viestin suojaan liittyen perustuslakivaliokunta on todennut viestien tunnistamistietojen, joista sittemmin on alettu käyttää termiä välitystieto, jäävän luottamuksellisen viestin salaisuuden ydinalueen ulkopuolelle, minkä vuoksi valiokunta on esimerkiksi pitänyt mahdollisena, että tunnistamistietojen saamisoikeus jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset (PeVL 7/1997 vp, s. 2/I, PeVL 26/2001 vp, s. 3/II). Ehdotuksessa on kyse välitystietojen lisäksi myös esimerkiksi viestin sisältöä koskevista tiedoista, joiden suojaamiseksi on säädetty erityisiä salassapitovelvoitteita ja tiedon luovuttamista koskevia rajoituksia.

Perustuslakivaliokunta on pitänyt perustuslain kannalta hyväksyttävänä erilaiset tietoturvallisuuden toteuttamista koskevat toimenpiteet mukaan lukien luottamuksellisen viestin sisältöön puuttumisen tietyin vakavaan rikosepäilyyn liittyvin edellytyksin silloin, kun sääntelyllä turvataan viestinnän eri osapuolien tietoverkkojen toimivuutta ja turvallisuutta sekä luodaan näin edellytyksiä sananvapauden käyttämiselle ja viestinnän luottamuksellisuudelle tietoverkoissa. Perusoikeuksien käyttämiseen ja niiden toteutumisen edistämiseen tällä tavoin liittyvät seikat on katsottu hyväksyttäviksi ja painaviksi perusteiksi tietoverkoissa harjoitetun viestinnän luottamuksellisuuteen kohdistuville rajoituksille. Oikeasuhtaisuuden näkökulmasta toimia on pidetty perusteltuina, jos ne ovat välttämättömiä palvelujen tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi. Lisäksi haittaohjelmiin liittyvää viestintää ei ole katsottu kuuluvaksi luottamuksellisen viestin salaisuuden ydinalueeseen, koska kyse ei ole sellaisesta henkilön lähettämästä tai hänelle osoitetusta viestistä, jonka sisällön luottamuksellisuus voidaan katsoa olevan perustuslaissa turvatun viestinnän luottamuksellisuuden keskiössä (PeVL 9/2004 vp s. 4). Tällä perusteella voidaan katsoa mahdolliseksi myös ehdotuksen kaltainen tiedonvaihto viranomaisten välillä.

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 tehty tästä syystä 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 tai esimerkiksi vakoilurikosten tunnusmerkistön. Tietoturvaloukkauksen uhkan osalta on edellä perusteluissa avattu sellaisia poikkeuksellisen vakavia uhkatilanteita, joiden toteutuminen aiheuttaisi esityksen mukaista tietoturvaloukkausta vastaavia vaikutuksia. Lisäksi on painotettu toteutumisen todennäköisyyden merkitystä. Uhkan osalta tulkintaa on esitetty tehtävän suppeasti johtuen uhkaan liittyvän arvioinnin suuremmasta tulkinnanvaraisuudesta. Tiedon luovuttaminen on sidottu välttämättömyyskriteeriin perustuslakivaliokunnan tulkintakäytännön edellyttämällä tavalla. Perustuslakivaliokunta on kiinnittänyt huomiota siihen, että mikäli laissa ei voida eritellä tyhjentävästi luovutettavia tietosisältöjä, on sääntelyyn tullut sisällyttää vaatimus tietojen välttämättömyydestä jonkin tarkoituksen kannalta (PeVL 62/2010 vp, s. 4/1 ja siinä mainitut lausunnot). Ehdotuksessa tällaiseksi tarkoitukseksi on määritelty merkittävien tietoturvaloukkausten selvittäminen, ennalta ehkäiseminen tai vaikutusten poistaminen.

Ehdotusta ei sinällään ole suoraan sidottu tiettyjen rikosten tunnusmerkistön täyttymiseen, vaikka käytännössä merkittävissä tietoturvaloukkaustilanteissa jokin tieto- tai viestintärikoksen taikka esimerkiksi vakoilurikosten tunnusmerkistö täyttyisi. Säännöksen soveltamisen sitominen tiettyihin tunnusmerkistöihin olisi haastaa erityisesti uhkiin reagoimisen näkökulmasta.

11.2.2 Salassapito ja tiedon luovuttamisen rajoitukset

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). Ehdotuksella pyritään suojaamaan yhteiskunnan toimintakykyä ja kriittisiä toimintoja vakavilta tietoturvaloukkauksilta, joilla voi pahimmillaan olla vakavia vaikutuksia yhteiskunnalle. Siten voidaan katsoa, 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.

11.2.3 Suhde tiedustelutoimintaan ja rikostorjuntaan

Koska Liikenne- ja viestintäviraston hallussa olevaa, salassa pidettäväksi säädettyä ja luottamuksellisen viestin suojaa nauttivaa tietoa voitaisiin vastavuoroisessa tiedonvaihdossa luovuttaa suojelupoliisille ja Puolustusvoimille sekä tarpeen vaatiessa myös näiden välillä, on tarpeen arvioida ehdotuksen suhdetta tiedustelutoimintaan ja siitä seuraaviin perusoikeuskysymyksiin erityisesti viestinnän luottamuksellisuuden kannalta. Kyse olisi sinällään hyvin rajatussa tilanteessa, yksittäistapausta koskevasta tiedonvaihdosta, eikä laajasta kohdentumattomasta tiedonvaihtokanavasta, jonka suhteen perustuslakivaliokunta on vahvasti linjannut, että perustuslain muutos ei mahdollista yleistä, kohdentamatonta ja kaiken kattavaa tietoliikenteen seurantaa tiedustelutoiminnassa (PeVM 4/2018 vp, s. 8). Myös EUT on käytännössään todennut, että tiedonhankinnan on oltava riittävän kohdennettua ja yksilöityä. EUT:n mukaan yksityiselämän kunnioitusta koskevan perusoikeuden suoja unionin tasolla edellyttää, että henkilötietojen suojaa koskevat poikkeukset ja rajoitukset toteutetaan sen rajoissa, mikä on ehdottomasti välttämätöntä (tuomio Digital Rights Ireland ym. 52 kohta oikeuskäytäntöviittauksineen). Myös perustuslakivaliokunta on tuonut kohdentamista ja rajaamista koskevan kannan esille tiedustelutoiminnassa (PeVM 4/2018 vp, s. 7–8). Ehdotuksen ei katsota olevan ristiriidassa näiden tiedonhankinnan kohdentamista ja rajaamista koskevien reunaehtojen kanssa.

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).

Vaikka kyse ei sinällään ole tiedustelun tiedonhankintakeinosta, vaihdettu tieto saattaisi ehdotuksen mukaisessa tilanteessa olla sellaista, jonka 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. 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. Tietoa voisi siten käyttää myös erityisesti ennaltaehkäisevään toimintaan viranomaisien lakisääteisten tehtävien mukaisesti myös muussa kuin tiedonluovutuksen aiheuttaneessa tilanteessa. Oikeusturvakeinojen takeiden kannalta tiedon käyttötarkoituksen rajaaminen on olennaisessa roolissa. On kuitenkin kokonaisuuden kannalta tarkoituksenmukaista, että vakavia tilanteita koskevaa tietoa voitaisiin käyttää kansallisen turvallisuuden edistämiseen, minkä vuoksi tietoa voisi käyttää tiedustelutoiminnan kohdentamiseen, jonka oikeusturvan takeena toimii tuomioistuin ja toisaalta ennalta ehkäiseviin toimiin.

Tietoa luovutettaessa poliisille ja Puolustusvoimille on tiedustelutoiminnan lisäksi arvioitava tiedonvaihdon suhdetta rikostorjuntaan ensinnäkin siitä näkökulmasta, että tiedustelutoiminnan ja rikostorjunnan välille on tiedon vaihdon osalta säädetty erityinen niin sanottu palomuuri. Palomuurilla tarkoitetaan sitä, että tiedustelutoimivaltuuksilla saatuja tietoja ei saa siirtää esitutkintaviranomaiselle ilman laissa säädettyjen kriteerien täyttymistä Tiedon luovuttaminen rikostorjuntaan on mahdollista harkinnanvaraisesti tiettyjen vakavien rikosten kohdalla ja toisaalta pakollista erityisen vakavissa rikoksissa. Keskeinen harkintaa ohjaava elementti on tiedon luovuttamisen vaikutus kansalliseen turvallisuuteen. Perustuslakivaliokunta on pitänyt tärkeänä varmistua siitä, että tiedustelutoimivaltuuksin saatujen tietojen vaihtamista koskeva sääntely ei avaisi mahdollisuuksia poliisilain salaisia tiedonhankintakeinoja ja pakkokeinolain salaisia pakkokeinoja koskevan sääntelyn kiertämiseen, joiden käytön kynnys on käytännössä korkeampi (PeVL 35/2018 vp, s. 22). Koska ehdotuksen mukaisessa tilanteessa viranomaiset voisivat vastavuoroisesti luovuttaa toisilleen tietoja, olisi olemassa mahdollisuus, että tiedustelumenetelmällä saatua tietoa olisi oikeus luovuttaa tiedonvaihdon yhteydessä myös esitutkintaviranomaiselle.

Sekä sotilastiedustelulaissa että siviilitiedustelua koskevassa poliisilain 5 a luvussa on säädetty tiedustelumenetelmällä hankitun tiedon luovuttamisesta esitutkintaviranomaiselle. Tiedusteluviranomaisilla on oikeus ilmoittaa vain sellaista tiedustelumenetelmällä paljastuneista rikoksista, joista säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta. Estettävissä olevista vakavista rikoksista on ilmoitettava viipymättä esitutkintaviranomaiselle, ja oikeus ilmoittaa rikoksesta, josta säädetty ankarin rangaistus on kaksi vuotta vankeutta. Harkinnanvaraisen ilmoittamisen edellytyksenä on, että ilmoituksella arvioidaan olevan erittäin tärkeä merkitys sellaisen rikoksen selvittämiselle, josta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta. Ehdotuksen kaltaisissa tilanteissa usein toteutuisivat esimerkiksi rikoslaissa säädetyt tietojärjestelmän häirinnän ja tietomurron törkeiden tekomuotojen tunnusmerkistö, jolloin myös esitutkintaan luovutettavan tiedon osalta tiedon luovuttaminen olisi mahdollista ilman poikkeussäännöksiäkin. Vastaava tilanne olisi esimerkiksi vakoilurikosten ja turvallisuussalaisuuden paljastamisen ja luvattoman tiedustelutoiminnan osalta, jolloin tiedon luovuttaminen rikostorjuntaan on osin säädetty jopa pakolliseksi. Näiltä osin ehdotus ei muodosta ristiriitaa edellä esitetyn perustuslakivaliokunnan kannan kanssa. Vähäisempien rikosten osalta saattaisi joissain tilanteissa tulla vastaan tilanne, jossa tällaiseen rikokseen liittyvää tietoa tulisi tiedustelutoiminnasta esitutkintaviranomaisen tietoon. Esimerkiksi tietojärjestelmän häirintärikoksesta tai tietomurrosta rangaistus on enintään kaksi vuotta vankeutta, jolloin edellä mainittu kynnys tiedon luovuttamiselle alittuisi, ellei rikos olisi vielä estettävissä. Tällaisissa tilanteissa ehdotuksen mukainen merkittävä tietoturvaloukkaus voisi tulla kyseeseen tilanteissa, jossa vähäisemmäksi rikokseksi määriteltyä toimintaa toteutetaan useampaan kohteeseen samaan aikaan, jolloin sen kerrannaisvaikutukset kasvavat. Tässäkin kohtaa tulee arvioitavaksi, onko kyseessä näiden rikosten törkeä tekomuoto, joka mahdollistaa tiedon luovuttamisen rikostorjuntaan. Tämän perusteella voidaan arvioida, että ehdotus ei tältä osin aiheuttaisi merkittävää poikkeusta tiedon luovuttamisen rajoituksiin.

Toinen näkökulma rikostorjuntaan liittyen koskee Liikenne- ja viestintäviraston toiminnassa saadun tiedon luovuttamista rikostorjuntaan. Liikenne- ja viestintäviraston tehtävänä on turvata viestinnän luottamuksellisuutta esimerkiksi sen Kyberturvallisuuskeskuksen tehtävien kautta. Viraston eri tehtävien nojalla saaduille tiedoille ja Kyberturvallisuuskeskukselle tehtyjen vapaaehtoisten ilmoitusten kautta virasto saa tietoonsa myös sellaista tietoa, jonka saamiseksi rikostorjuntaviranomaiset ja tiedusteluviranomaiset joutuvat hakemaan luvan tuomioistuimesta oikeusturvan toteutumiseksi. Osin tästä syystä viraston hallussa olevalle tiedolle on säädetty erityisiä salassapitovelvoitteita ja luovuttamista koskevia rajoituksia. Viestin sisältöä, välitystietoja ja sijaintitietoja voidaan lähtökohtaisesti luovuttaa muille viranomaisille ainoastaan sil-

loin, kun viranomainen itse on joutunut tai uhkaa joutua tietoturvaloukkauksen kohteeksi. Ehdotus muodostaisi tähän periaatteeseen poikkeuksen viranomaisten vastavuoroisen tiedon luovuttamisen tilanteessa. Jo edellä esitettyihin perusteluihin nojaten voidaan todeta, että poikkeuksen nojalla saatava hyöty viestinnän luottamuksellisuuden kannalta on huomattava suhteessa aiheutuneeseen haittaan. Toisaalta tiedon käyttötarkoituksen rajaamisella on tarkoitus varmistaa oikeusturvakeinojen toteutuminen jatkossakin

11.2.4 Perusoikeuksien rajoitusedellytysten arviointi

Perusoikeuksien yleisten rajoitusedellytysten ja perustuslain 10 §:n 4 momentin rajoitusedellytyksen kannalta katsottuna ehdotus täyttäisi lailla säätämisen vaatimuksen. Täsmällisyyden ja tarkkarajaisuuden osalta tietoturvaloukkauksia koskevan tiedon vaihdon rajaaminen kaikilta osin on kokonaisuutena haastava. Tietoturvaloukkaus tai sen vakava uhka on käsitteenä laaja kattaen monenlaisia tekotapoja. Tekotavat myös kehittyvät jatkuvasti teknologian kehittyessä. Toisaalta myös loukkauksen tai uhkan kohteella on merkitystä. Loukkaus voi kohdistua yksittäiseen toimijaan tai laajasti tuhansiin yksityishenkilöihin ja olla siten yhtä lailla ehdotuksen tarkoittamalla tavalla merkittävä. Tietoturvaloukkauksen kohteeksi voivat joutua hyvin laajasti sekä yksityiset henkilöt, yritykset, yhteisöt tai viranomaiset. Tästä moninaisuudesta johtuen sääntelyn rajaaminen yksityiskohtaisesti on erittäin haastavaa, jotta voidaan turvata viranomaisten toimintamahdollisuus näissä kaikissa tilanteissa.

Käsitteet kansallisesta turvallisuudesta, maanpuolustuksesta, ja julkisen vallan päätöksentekokyvystä ovat sisällöllisesti laajoja ja jossain määrin täsmentymättömiä. Ehdotuksessa ei myöskään ole ollut mahdollista tyhjentävästi luetella tiedon vaihdon kohteena olevia tietoja edellisessä kappaleessa esitetystä tilanteiden moninaisuudesta johtuen. Tästä syystä ehdotuksessa on pyritty tekemään muita rajauksia, joiden perusteella ehdotuksen voi katsoa täyttävän täsmällisyyden ja tarkkarajaisuuden vaatimuksen. Vaikka siis tietoturvaloukkauksen tai uhkan vaikutusten kohdentuminen on määritelty tietyiltä osin väljästi, ei ehdotuksen soveltamisesta käytännössä seuraa muita kuin välttämättömään tiedonvaihtoon liittyviä oikeuksia. Ehdotus eroaa tässä suhteessa merkittävästi esimerkiksi valmiuslain kirjauksista ehdotuksen oikeusvaikutusten ollessa huomattavasti suppeammat. Salassapito ei myöskään lakkaa vaihdettaessa tietoja viranomaisten välillä. Ehdotuksen mukainen tiedonvaihto on rajattu tiettyihin viranomaisiin, tiedot on rajattu koskemaan vain välttämättömiä tietoja ja niitä saisi käyttää vain tietoturvaloukkausten selvittämiseksi, ennalta ehkäisemiseksi tai vaikutusten poistamiseksi. Lisäksi vaikutusten tulee olla luonteeltaan vakavia. Vakavaa uhkaa koskien olisi lisäksi tehtävä suppeaa tulkintaa ja huomiota on kiinnitettävä vaikutusten toteutumisen todennäköisyyteen, jonka tulee olla suuri. Tältä osin voidaan arvioida, että täsmällisyyden ja tarkkarajaisuuden vaatimus kaikkinensa täyttyisi.

Henkilötietoihin liittyen perustuslakivaliokunta on käytännössään täsmentänyt aiempiin tiedonvaihtoa koskeviin kriteereihin nähden, että salassa pidettävien henkilötietojen luovuttaminen ei ole mahdollista edes välttämättömyyskriteeriin perustuen, jos tiedonsaantioikeudet muutoin on määritelty väljästi ja yksilöimättä. (PeVL 19/2012 vp, s. 4/I ja siinä mainitut lausunnot). Ehdotuksen mukainen tiedonvaihto on määritelty tältä osin välttämättömyyskriteeriin sitoen ja toisaalta myös viranomaiset, joiden välillä tietoa voidaan vaihtaa, on määritelty yksilöiden, eikä ehdotuksen voida tältä osin katsoa olevan ongelmallinen perustuslain kannalta.

Luottamuksellisen viestinnän suojan rajoittamisen hyväksyttävyyden kannalta erityistä merkitystä katsotaan olevan rajoituksen taustalla olevalla vakavalla yhteiskunnantoiminnan kannalta keskeisten toimintojen turvaamisen tarpeella. Myös perustuslain 10 §:n 4 momentissa edellytetään, että rajoitukset viestin salaisuuteen tulee olla välttämättömiä muun muassa yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa taikka tiedon hankkimiseksi sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Vakavilla tietoturvaloukkauksilla voi olla kauaskantoisia ja monipolvisia vaikutuksia eri sektoreille ja sitä kautta sekä yksilön tai yhteiskunnan turvallisuuteen, että kansalliseen turvallisuuteen. Tietoturvaloukkaukset ovat omiaan heikentämään yksityiselämän suojaa ja toisaalta vaikutukset voivat kohteesta riippuen kohdistua myös esimerkiksi henkeen ja terveyteen. Tästä näkökulmasta ehdotuksella on katsottu olevan hyväksyttävä ja välttämättömyysvaatimuksen täyttävät perusteet luottamuksellisen viestinnän suojan rajoittamiselle.

Suhteellisuusvaatimuksen kannalta oikeus tiedon luovuttamiseen tulisi kyseeseen vain yksittäisissä tapauksissa. Myös tiedon käyttöä on kohdennettu ja sen käyttötarkoitusta on rajoitettu. Taustalla oleva yhteiskunnallisten toiminnan kannalta keskeisten toimintojen turvaamiseen nähden rajoituksen on katsottu olevan oikeasuhtainen. Sääntelyn soveltamiselle on asetettu myös korkea soveltamiskynnys, mikä korostaa sääntelyn tarpeen välttämättömyyttä kyseisessä, jo erittäin vakavassa, turvallisuutta uhkaavassa tilanteessa. Tuolloin olisi tarpeen soveltaa poikkeuksellisia tiedonvaihto-oikeuksia.

Oikeusturvajärjestelyjen riittävyyden osalta oikeusturvakeinot liittyvät käytännössä niihin viranomaisten toimintoihin, joiden nojalla tietoa varsinaisesti kerätään. Näitä olisivat siten erityisesti henkilötietojen käsittelyn, tiedustelutoiminnan ja rikostorjunnan yhteydessä käytettyjen salaisten tiedonhankintakeinojen ja tiedustelutoimintaan liittyvät toimivaltuudet. Ehdotuksen nojalla tällaiseen tietoon ei sisältyisi mahdollisuutta käyttää saatua tietoa syyksilukemiseksi, vaan tätä varten olisi käytettävä tavanomaisia keinoja. Ehdotuksella ei muodosteta viranomaisille varsinaista uutta tapaa hankkia tietoja muiden lakisääteisten tehtäviensä hoitamiseksi, vaan tietoa käytetään vain tietoturvaloukkausten selvittämisen yhteydessä. Lisäksi niiltä osin, kuin kyse on henkilötiedoista, ovat käytettävissä tietosuojaan liittyvät oikeusturvakeinot. Oikeusturvakeinojen katsotaan näiltä osin olevan riittävät.

Esityksen katsotaan olevan yhdenmukainen ihmisoikeusvelvoitteiden kanssa. Tässä yhteydessä on erityinen merkitys Euroopan ihmisoikeussopimuksella, sellaisena kuin sen sisältö näyttäytyy Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa. Ihmisoikeustuomioistuimen oikeuskäytännön mukaan luottamuksellisen viestinnän salaisuuden rajoitukselle on aina oltava painava yhteiskunnallinen tarve, puuttumisen ja tavoiteltavan hyväksytyn päämäärän tulee olla oikeassa suhteessa keskenään ja puuttumiselle pitää olla riittävän painavat ja hyväksyttävät perustelut. Lisäksi rajoitusten on oltava lain sallimia. Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä on painotettu lain laatua, kuten täsmällisyyttä sekä viranomaistoiminnan ennustettavuutta turvaavaa ja vallan väärinkäyttöä estävää sääntelyä. Ehdotuksen katsotaan täyttävän nämä vaatimukset.

11.2.5 Tietosuoja viranomaisten välisessä tiedonvaihdossa

Perustuslain 10 §:n 1 momentin mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunta on katsonut, että henkilötietojen suoja tulee ensisijaisesti toteuttaa EU:n yleisen tietosuoja-asetuksen ja kansallisen lainsäädännön nojalla ja rajata se vain välttämättömään tietosuoja-asetuksen salliman liikkumavaran puitteissa (PeVL 14/2018 vp, s. 4–5).

Ehdotuksen 319 a §:n nojalla vaihdettaisiin myös henkilötiedoiksi katsottuja tietoja. Viranomaisten käsittelyoikeus näiden tietojen osalta laajenisi nimenomaan luovuttamisen näkökulmasta. Muilta osin käsittelyoikeus kyseisille tiedoille sinällään on jo olemassa. Ehdotuksessa kyse olisi siten yleisessä tietosuoja-asetuksen 4 artiklassa sekä rikosasioiden tietosuoja-lain 3 §:n 1 momentin 2 kohdassa tarkoitetusta tiedon käsittelystä, koska viranomaiset luovuttaisivat ja yhdistäisivät hallussaan olevia tietoja, kuten välitystietoja. Ehdotuksessa tarkoitettujen viranomaisten toimintaan tai toiminnan johonkin osaan sovelletaan osaltaan eri tietosuojasääntelyä,

kuten on kuvattu nykytilaa koskevassa jaksossa 2.2.4. Ehdotuksen mukaisessa tilanteessa on siis mahdollista, että henkilötietoja vaihdettaessa tietoja käytettäisiin muuhun kuin alkuperäiseen käyttötarkoitukseen erityisesti, jos siirretään tietoja rikostorjuntaviranomaisten piiristä Liikenne- ja viestintävirastolle tai päinvastoin.

Välitystiedot sinällään kuuluvat sähköisen viestinnän tietosuojadirektiivin kansallisen täytäntöönpanosääntelyn piiriin, jota on erityisesti SVPL:ssä. Merkitystä on erityisesti direktiivin 15 artiklan 1 kohdalla, jonka mukaan jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan direktiivissä säädettyjä tiettyjä oikeuksia ja velvollisuuksia. Rajoitusten tulee olla välttämättömiä, asianmukaisia ja oikeasuhtaisia demokraattisen yhteiskunnan toimenpiteitä kansallisen turvallisuuden sekä puolustuksen, yleisen turvallisuuden tai rikosten tai sähköisten viestintäjärjestelmän luvattoman käytön torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi. Näiden kriteerien mukainen arviointi on arvioitu olevan yhdenmukainen edellä perusoikeuksien rajoitusoikeuksien mukaiseen arviointiin ja toisaalta yksityisyyden suojaa koskevan sääntelyn arviointiin.

Säännös sinällään mahdollistaa kaiken välttämättömän tiedon vaihtamisen, mikä ei kategorisesti sulje pois mahdollisuutta henkilötietolaissa (1050/2018) määriteltyihin erityksiin henkilötietoryhmiin kuuluvien henkilötietojen vaihtamiselle. Ehdotetun sääntely rajaus luovutettavan tiedon välttämättömyydestä tietoturvaloukkauksen selvittämisen, ennalta ehkäisemisen ja vaikutusten poistamisen kannalta kuitenkin rajaa rajaa tällaisen tiedonvaihdon lähinnä teoreettiselle tasolle. Tällaisella tiedolla ei ole merkitystä tietoturvaloukkauksen selvittämisessä ja käsiteltäessä tällaisia tietoja mahdollisesti sisältäviä tietoja muiden käsittelyperusteiden nojalla esimerkiksi tietomurtoon liittyvän aineiston käsittelyn yhteydessä, niitä ei ole tarpeen luovuttaa toiselle viranomaiselle vaan ne on säännöksen mukaan hävitettävä tarpeettomina, ellei muualta laista muuta johdu.

Yleisen tietosuoja-asetuksen 4 artiklassa säädettyjen henkilötietojen käsittelyä koskevien yleisten periaatteiden mukaan olennaista on erityisesti vaatimukset lainmukaisuudesta, kohtuullisuudesta ja läpinäkyvyydestä. Lisäksi henkilötietoja on kerättävä tiettyä, nimenomaista käyttötarkoitusta varten, eikä niitä saa käsitellä myöhemmin nähden tarkoitusten kanssa yhteen sopimattomalla tavalla. Henkilötiedon käyttötarkoituksesta poikkeamisesta säädetään tietosuoja-asetuksen 6 artiklan 4 kohdassa. Poikkeaminen voisi artiklan mukaan perustua jäsenvaltion lainsäädäntöön, joka muodostaa demokraattisessa yhteiskunnassa välttämättömän ja oikeasuhtaisen toimenpiteen 23 artiklan 1 kohdassa tarkoitettujen tavoitteiden turvaamiseksi. Tietosuoja-asetuksen johdanto-osan kohdassa 50 on todettu, että jos käsittely perustuu jäsenvaltion lainsäädäntöön, joka muodostaa demokraattisessa yhteiskunnassa välttämättömän ja oikeasuhtaisen toimenpiteen, jolla pyritään turvaamaan erityisesti yleiseen julkiseen etuun liittyviä tärkeitä tavoitteita, rekisterinpitäjälle olisi sallittava henkilötietojen myöhempi käsittely riippumatta tarkoituksen yhteensopivuudesta. Kaikissa tapauksissa olisi kuitenkin varmistettava erityisesti, että sovelletaan asetuksessa vahvistettuja periaatteita ja varmistettava erityisesti, että rekisteröidylle ilmoitetaan näistä muista tarkoituksista ja hänen oikeuksistaan, kuten oikeudesta vastustaan henkilötietojen käsittelyä.

Ehdotuksessa käytettäisiin yleisen tietosuoja-asetuksen 23 artiklassa säädettyä kansallista liikkumavaraa siten, että ehdotetulla lainsäädäntötoimenpiteellä rajoitettaisiin 5 artiklassa säädettyä käyttötarkoitussidonnaisuutta. Ehdotuksella tavoiteltavien kansallista turvallisuutta turvaavien ja toisaalta rikosten ennaltaehkäisemistä mahdollistavien ehdotusten on katsottu olevan välttämättömiä sekä oikeasuhtaisia tavoiteltavaan oikeushyvään nähden. Käyttötarkoituksesta poikkeamiselle katsotaan olevan painavat yhteiskunnalliset perusteet yhteiskunnan kriittisten toi-

mintojen suojaamisessa. Toisaalta oikeasuhtaisuuden vaatimusta on ehdotuksessa toteutettu rajaamalla tiedot välttämättömiin ja toisaalta pitämällä poikkeussäännöksen soveltamisen kynnyksen verrattain korkealla koskien vain vakavia tilanteita.

Ehdotuksen mukainen tietojen luovuttaminen voisi joissakin tilanteissa tapahtua myös suoraan julkisuuslain 16 §:n 3 momentin nojalla. Aina kyse ei ole henkilötietojen käyttötarkoitussidonnaisuudesta poikkeamisesta, vaan käsittely voi tapahtua alkuperäisen tai sen kanssa yhteensopivan käsittelyperusteen nojalla. Tällöin henkilötietojen käsittelyperuste olisi yleisen edun mukaisen tehtävän suorittaminen ja rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen. Muussa tapauksessa käsittelyn perustan muodostaisi asetuksen ehdotettu lainsäädäntö ja 6 (3) artiklan mukainen yleisen edun mukainen tavoite on yleisen turvallisuuden turvaaminen tietoturvaloukkaustilanteissa. Tietojen luovuttamista koskevan säännöksen katsotaan olevan oikeasuhtainen siihen liittyvät, edellä esitetyt rajaukset huomioiden, suhteessa tavoiteltuun päämäärään.

11.3 Viestinnän välittäjän oikeus luovuttaa tietoja liikenne- ja viestintävirastolle

Myös ehdotuksen 316 a §:llä on merkitystä perustuslain 10 §:ssä turvatun yksityiselämän suojan kannalta. Ehdotuksen mukaan viestinnän välittäjällä olisi vapaaehtoisesti mahdollisuus luovuttaa tietoturvaloukkaukseen liittyviä tietoja sähköisen viestin sisällöstä tai välitystiedoista. Ehdotus jossakin määrin rajoittaa viestinnän luottamuksellisuutta, koska ehdotus sisältää viestin sisältöä koskevan tiedon luovuttamista. Ehdotuksessa tarkoitettu viestin sisältöä koskeva tiedon jakaminen ei ole arvioitu olevan viestinnän luottamuksellisuuden kannalta erityisen ongelmallinen, koska kyse olisi lähinnä haittaohjelmia sisältävien tai esimerkiksi tietoturvaloukkauksia aiheuttavien viestien sisällön, jonka toisena osapuolena ei usein edes ole luonnollista henkilöä vaan esimerkiksi viestejä automaattisesti luova tietokoneohjelma. Ehdotuksen ei ole katsottu muodostavan merkittävää muutosta nykyiseen vastaavien tietojen käsittelyoikeuksiin, mutta sen on katsottu parantavan mahdollisuuksia puuttua tietoturvaloukkauksiin ja edistävän loukkausten kohteeksi joutuneiden henkilöiden viestinnän luottamuksellisuuden ja yksityiselämän suojaa. Esimerkiksi haitallisia viestejä suodattamalla voidaan estää luonnollisten henkilöiden joutuminen huijausviestinnän kohteeksi. Toisaalta osa luovutettavasta tiedosta saattaa sisältää sinällään asiallistakin viestintää, jolloin rajoitus yksityisyyden suojaan ja viestinnän luottamuksellisuuteen on merkittävämpi.

Tiedon käsittelyn kannalta ehdotuksessa on säännökset niistä käsittelyperiaatteista ja salassapitovelvoitteista, joita kyseisessä tiedon luovuttamisessa tulee noudattaa. Niiden perusteella käsittely on sallittua ainoastaan tarkoituksen vaatimassa laajuudessa ja siten, ettei sillä rajoiteta luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Säännös sisältää myös vaatimukset käsittelyn jälkeisestä tietojen hävittämisestä ja tunnistamattomaksi tekemisestä, jollei laissa toisin säädetä. Säännöksen mukaiseen tietojen antamiseen sovellettaisiin 319 §:n mukaista salassapitoa ja sekä siinä että 319 a §:ssä säädettyjä tiedon luovuttamista koskevia säännöksiä. Ehdotuksen on arvioitu olevan tässä suhteessa sopusoinnussa perustuslain 10 §:n vaatimusten kanssa.

Jo voimassa olevankin lainsäädännön nojalla sekä viestinnän välittäjällä että Liikenne- ja viestintävirastolla on oikeus käsitellä ehdotuksen mukaisia tietoja tietoturvan toteuttamiseksi. Virastoon on myös mahdollisuus pyytää viestinnän välittäjältä kyseisiä tietoja, mikäli se havaitsee tällaisen tarpeen. Ehdotus ei siten muodosta merkittävää muutosta nykytilaan ja kokonaisarvioinnin perusteella sen voidaan katsoa olevan sopusoinnussa perustuslain 10 §:n kanssa.

Ehdotus koskee lisäksi henkilötietojen käsittelyä ja erityisesti sähköisen viestinnän henkilötietoja. Koska tiedon luovuttaminen katsotaan myös henkilötietojen käsittelyksi, muodostaisi ehdotus tässä suhteessa uuden käsittelyperusteen pykälässä tarkoitetulle tiedolle. Viestinnän välittäjän kohdalla kyse olisi sähköisen viestinnän tietosuojadirektiivin 4 artiklan mukaisesta käsittelyn turvallisuusvaatimuksen täyttämisestä, mutta koska tiedon luovuttamisesta Liikenne- ja viestintävirastolle ei suoraan synny velvoitetta kyseisen artiklan nojalla syntyisi siitä siten jossakin määrin rajoite luottamuksellisen viestinnän suojaamiselle. Rajoittaminen on mahdollista sen 15 artiklassa säädettyjen rajoitusperusteiden perusteella ja tältä osin käytettäisiin kansallista liikkumavaraa. Rajoittaminen olisi perusteltu yleisen turvallisuuden ja rikosten ennaltaehkäisyn tarkoituksessa. Liikenne- ja viestintäviraston myöhäisemmän käsittelyn kohdalla kyse oli TSA:n mukaisesta henkilötietojen käsittelystä. Henkilötietojen käsittelyn näkökulmasta kyse olisi tiedon luovuttamisesta toiselle samaa tai yhteensopivaa käyttötarkoitusta varten. Käsittely olisi tarpeen TSA 6 artiklassa tarkoitetusta käsittelytarpeesta yleistä etua koskevan tehtävän suorittamiseksi. Käsittelyn perusta on säädetty kansallisessa lainsäädännössä SVPL 243, 247 ja 272 §:ssä viestinnän välittäjän osalta ja 304, 316 ja ehdotetussa 316 a §:ssä sekä liikenne- ja viestintävirastosta annetun lain (935/2018) 2 ja 3 §:ssä Liikenne- ja viestintäviraston osalta. Kummassakin tilanteessa käsittelyoikeus perustuu tietoturvasta huolehtimista koskeviin ja tietoturvaloukkausten selvittämistä koskeviin säännöksiin.

11.4 Julkisuusperiaate

Esityksen 316 a §:än ja 319 §:än sisältyvä ehdotus Liikenne- ja viestintävirastolle ja tietosuojavaltuutetulle 316 a §:n nojalla luovutettavien tietojen salassapitovelvollisuudesta on merkityksellinen perustuslain 12 §:n 2 momentissa turvatun julkisuusperiaatteen kannalta. Salassapitovelvollisuudessa olisi kysymys rajoituksesta perustuslain 12 §:n 2 momentissa turvatulle julkisuusperiaatteelle, sillä ehdotettavan 316 a §:n nojalla viranomaiselle luovutettavat tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta olisi pidettävä salassa, ellei laissa nimenomaisesti säädetä poikkeusta salassapidolle.

Julkisuusperiaatteen ydinaluetta on turvata vallankäytön ja viranomaistoiminnan kritiikin ja valvonnan edellytyksiä (HE 309/1993 vp, s. 58 ja PeVL 43/1998 vp, s. 2–3). Salattavissa tiedoissa olisi kysymys tietoturvaloukkauksiin tai niiden uhkiin liittyvien tietojen luovuttamisesta tietoturvaloukkausten tai uhkien selvittämiseksi ja ennalta ehkäisemiseksi. Tiedot eivät ole luonteeltaan julkisuusperiaatteen ydinalueeseen liittyviä. Mikäli luovutettavat tiedot olisivat tietoturvaloukkauksen selvittämisen aikana julkisia, on sen ennakoitava aiheuttavan olennaista haittaa sille tarkoitukselle, jota varten tietoja viranomaiselle luovutetaan. Lisäksi on tehtävä intressipunnintaa julkisuusperiaatteen suhteesta perustuslain 10 §:ssä turvattuun luottamuksellisen viestinnän suojaan, joka puoltaa luovutettavien tietojen salassapitämistä luottamuksellisen viestinnän suojaan liittyvien oikeushyvien johdosta. Tietojen julkisuuden rajoittaminen parantaisi ehdotuksen hyväksyttävyyttä perustuslain 10 §:ssä turvatun luottamuksellisen viestinnän suojan näkökulmasta. Lisäksi voimassa olevassa sähköisen viestinnän palveluista annetussa laissa on hyväksytty lähtökohdaksi se, että Liikenne- ja viestintäviraston on pidettävä salassa lain nojalla saamansa tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta, ellei salassapidolle ole säädetty laissa nimenomaista poikkeusta. Edellä esitetyistä seikoista johtuen katsotaan, että 316 a §:än ja 319 §:än ehdotetussa muutoksissa on julkisuusperiaatteen rajoittamisen osalta kyse muutoksesta, joka on yleisten perusoikeuksien rajoittamista koskevien vaatimuksien kannalta hyväksyttävä.

11.5 Yhteenveto

Hallitus katsoo, että esityksessä ei ehdoteta sellaista sääntelyä, jonka vuoksi lakiesitystä ei voitaisi käsitellä tavallisessa lainsäätämisjärjestyksessä. Edellä kuvattujen luottamuksellisen viestin salaisuuden suojaan liittyvien näkökulmien vuoksi hallitus pitää kuitenkin suotavana, että esityksestä pyydettäisiin perustuslakivaliokunnan lausunto.

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset

1.

Laki

sähköisen viestinnän palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

kumotaan sähköisen viestinnän palveluista annetun lain (917/2014) 250 §:n 4 momentti, sellaisena kun se on laissa 52/2019;

muutetaan 309 §, 316 §:n 5 momentti ja 319 §, sellaisina kuin ne ovat laissa 1003/2018, sekä *lisätään* lakiin uusi 316 a ja 319 a § seuraavasti:

309 §

Virka-apu

Liikenne- ja viestintävirastolla on oikeus saada virka-apua poliisilta, Tullilta ja Rajavartiolaitokselta tämän lain sekä sen nojalla annettujen säännösten ja määräysten noudattamisen valvomiseksi ja täytäntöön panemiseksi. Liikenne- ja viestintävirastolla on oikeus saada virka-apuna poliisilta, suojelupoliisilta ja Puolustusvoimilta asiantuntija-apua, välineistöä, tiloja ja laitteita merkittävän tietoturvaloukkauksen tai sen vakavan uhkan selvittämiseksi sekä niistä aiheutuvien vaikutusten poistamiseksi. Liikenne- ja viestintävirastolla on oikeus saada virka-apua Puolustusvoimilta radioviestinnän häiriöiden syiden selvittämiseksi.

Liikenne- ja viestintävirasto voi pyynnöstä antaa virka-apuna asiantuntija-apua, välineistöä, tiloja ja laitteita toiselle viranomaiselle.

Virka-avusta aiheutuneista kustannuksista vastaa virka-avun pyytäjä, jollei asiasta toisin sovita. Virka-avun antamisen edellytyksenä on, että se ei vaaranna virka-apua antavalle viranomaiselle säädettyjen muiden tärkeiden tehtävien suorittamista.

Edellä 1 ja 2 momentissa tarkoitettu virka-avun antaminen ei oikeuta Liikenne- ja viestintävirastoa antamaan toiselle viranomaiselle tietoja viesteistä, välitystiedoista tai sijaintitiedoista taikka luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta.

316 §

Viestintää ja sijaintia koskevien tietojen käsittely ja hävittäminen

— —

Tässä pykälässä säädetty tiedonsaantioikeus ei koske luottolaitostoiminnasta annetun lain (610/2014) 15 luvun 14 §:ssä tai oikeudenkäymiskaaren 17 luvun 20 §:n 1 momentissa tarkoitettuja tietoja eikä viranomaistehtävien hoidossa harjoitettua viestintää viranomaisverkossa tai viranomaisviestintään liittyvässä viestintäpalvelussa.

316 a §

Viestinnän välittäjän oikeus antaa tietoja Liikenne- ja viestintävirastolle

Mitä 136 §:n 4 momentissa säädetään, ei estä viestinnän välittäjää antamasta Liikenne- ja viestintävirastolle tietoa 272 §:n nojalla käsittelemästään välitystiedosta tai sähköisestä viestistä, jos se on tarpeen tietoturvaloukkausten tai –uhkien selvittämiseksi taikka ennalta ehkäisemiseksi. Tiedon käsittelyyn sovellettavista viestinnän välittäjän yleisistä käsittelyperiaatteista säädetään 137 §:ssä. Tiedon salassapitoon ja luovuttamiseen sovelletaan, mitä 319 ja 319 a §:ssä säädetään tiedon salassapidosta ja luovuttamisesta.

319 §

Vaitiolovelvollisuus ja viesteihin liittyvien tietojen luovuttaminen

Liikenne- ja viestintäviraston ja tietosuojavaltuutetun 316, 316 a ja 317 §:n nojalla saamat ja hankkimat tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta on pidettävä salassa.

Liikenne- ja viestintävirastolla on 1 momentissa säädetyn salassapitovelvollisuuden tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja:

1) viestinnän välittäjälle, lisäarvopalvelun tarjoajalle, yhteisölle, tilaajalle ja käyttäjälle, jos sitä on käytetty hyväksi tietoturvaloukkauksessa, se on joutunut tietoturvaloukkauksen kohteeksi tai siihen todennäköisesti voi kohdistua tietoturvaloukkaus ja jos Liikenne- ja viestintäviraston arvion mukaan on syytä epäillä, että on tehty jokin 316 §:n 2 momentissa mainittu rikos;

2) 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 tietoturvaloukkauksia.

Liikenne- ja viestintävirastolla on oikeus luovuttaa tietoja siten kuin 2 momentissa säädetään ainoastaan siinä laajuudessa kuin se on tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi. Tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Mitä 1 momentissa säädetään, ei estä välitystiedon antamista toiselle viranomaiselle, jos se on tarpeen radiohäiriön aiheuttamista koskevan rikoksen selvittämistä tai syytteeseen panoa varten taikka radioviestinnän häiriön poistamiseksi tai rajoittamiseksi.

319 a §

Tietojen luovuttaminen merkittävässä tietoturvaloukkauksessa tai -uhkassa

Sen lisäksi mitä muualla laissa säädetään, Liikenne- ja viestintävirastolla, poliisilla, suojelupoliisilla ja Puolustusvoimilla on 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:

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.

Edellä 1 momentin nojalla luovutettua tietoa saa käyttää vain tietoturvaloukkauksen tai sen vakavan uhkan selvittämiseksi tai ennalta ehkäisemiseksi taikka niiden vaikutusten poistamiseksi. Tietoa ei saa käyttää muussa tarkoituksessa. Tarpeettomat tiedot on poistettava. Tiedon hävittämiseen sovelletaan mitä 316 §:n 4 momentissa säädetään tietojen hävittämisestä.

Edellä 1 momentin nojalla luovutettujen tietojen käsittelyssä on noudatettava, mitä luovuttajan asettamissa ehdoissa määrätään tietojen käytön rajoituksista, tietojen edelleen luovutuksesta tai luovutetun aineiston palauttamisesta. Luovuttavan viranomaisen on ilmoitettava luovuttamisen yhteydessä, jos luovutettavaan tietoon liittyy kyseisiä rajoituksia.

Tämä laki tulee voimaan päivänä kuuta 20 .

2.

Laki

henkilötietojen käsittelystä Puolustusvoimissa annetun lain 29 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan henkilötietojen käsittelystä Puolustusvoimissa annetun lain (332/2019) 29 §:n 1 momentin 18 kohta seuraavasti:

29 §

Oikeus luovuttaa henkilötietoja lakisääteisten tehtävien suorittamiseksi

Puolustusvoimat saa salassapitosäännösten estämättä luovuttaa teknisellä käyttöyhteydellä tai tietojoukkona muulle viranomaiselle ja julkista tehtävää hoitamaan asetetulle yhteisölle henkilötietoja, jotka ovat tarpeen tämän laissa säädetyn tehtävän suorittamiseksi, seuraavasti:

— —

18) Liikenne- ja viestintäviraston Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:ssä ja sähköisen viestinnän palveluista annetun lain (917/2014) 304 §:n 1, 7, 9 ja 10 kohdassa säädettyjen tehtävien hoitamista varten;

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

3.

Laki

henkilötietojen käsittelystä poliisitoimessa annetun lain 22 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan henkilötietojen käsittelystä poliisitoimessa annetun lain (616/2019) 22 §:n 1 momentin 1 kohta seuraavasti:

22 §

Muu henkilötietojen luovuttaminen viranomaisille

Poliisi saa salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona 5–8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi, seuraavasti:

1) Liikenne- ja viestintävirastolle liikenteen palveluista annetun lain 197 ja 217 §:n mukaisesti tietoja, jotka ovat välttämättömiä sen laissa säädettyjen tehtävien hoitamista varten, sekä Liikenne- ja viestintäviraston Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:ssä ja sähköisen viestinnän palveluista annetun lain 304 §:n 1, 7, 9 ja 10 kohdassa säädettyjen tehtävien hoitamista varten;

— —

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä 27.10.2022

Pääministeri

Sanna Marin

Liikenne- ja viestintäministeri Timo Harakka

Liite
Rinnakkaistekstit

1.

Laki

sähköisen viestinnän palveluista annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
kumotaan sähköisen viestinnän palveluista annetun lain (917/2014) 250 §:n 4 momentti, sellaisena kun se on laissa 52/2019;
muutetaan 309 §, 316 §:n 5 momentti ja 319 §, sellaisina kuin ne ovat laissa 1003/2018, sekä *lisätään* lakiin uusi 316 a ja 319 a § seuraavasti:
Eduskunnan päätöksen mukaisesti säädetään:

Voimassa oleva laki	*Ehdotus*
250 §	250 §
Viranomasiliittymät	*Viranomaisliittymät*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
Viranomaistehtävien hoidossa harjoitettuun viestintään viranomaisverkossa tai viranomaisviestintään liittyvässä viestintäpalvelussa ei sovelleta 316 §:ää.	(Kumotaan)
309 §	309 §
Virka-apu	*Virka-apu*
Liikenne- ja viestintävirastolla on oikeus saada virka-apua poliisilta, Tullilta ja Rajavartiolaitokselta tämän lain sekä sen nojalla annettujen säännösten ja määräysten noudattamisen valvomiseksi ja täytäntöön panemiseksi. Liikenne- ja viestintävirastolla on oikeus saada virka-apua puolustusvoimilta radioviestinnän häiriöiden syiden selvittämiseksi.	Liikenne- ja viestintävirastolla on oikeus saada virka-apua poliisilta, Tullilta ja Rajavartiolaitokselta tämän lain sekä sen nojalla annettujen säännösten ja määräysten noudattamisen valvomiseksi ja täytäntöön panemiseksi. *Liikenne- ja viestintävirastolla on oikeus saada virka-apuna poliisilta, suojelupoliisilta ja Puolustusvoimilta asiantuntija-apua, välineistöä, tiloja ja laitteita merkittävän tietoturvaloukkauksen tai sen vakavan uhkan selvittämiseksi sekä niistä aiheutuvien vaikutusten poistamiseksi.* Liikenne- ja viestintävirastolla on oikeus saada virka-apua Puolustusvoimilta radioviestinnän häiriöiden syiden selvittämiseksi.

Voimassa oleva laki	*Ehdotus*
Liikenne- ja viestintävirasto voi pyynnöstä antaa virka-apuna asiantuntija-apua toiselle viranomaiselle. *Virka-avun antamisesta päättää liikenne- ja viestintäministeriö. Liikenne- ja viestintäviraston antamasta* virka-avusta aiheutuneista kustannuksista vastaa virka-avun pyytäjä, jollei asiasta toisin sovita.	Liikenne- ja viestintävirasto voi pyynnöstä antaa virka-apuna asiantuntija-apua, *välineistöä, tiloja ja laitteita* toiselle viranomaiselle.
(uusi)	Virka-avusta aiheutuneista kustannuksista vastaa virka-avun pyytäjä, jollei asiasta toisin sovita. *Virka-avun antamisen edellytyksenä on, että se ei vaaranna virka-apua antavalle viranomaiselle säädettyjen muiden tärkeiden tehtävien suorittamista.*
Edellä 2 momentissa tarkoitettu virka-avun antaminen ei oikeuta Liikenne- ja viestintävirastoa antamaan toiselle viranomaiselle tietoja viesteistä, välitystiedoista tai sijaintitiedoista taikka luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta.	Edellä *1 ja* 2 momentissa tarkoitettu virka-avun antaminen ei oikeuta Liikenne- ja viestintävirastoa antamaan toiselle viranomaiselle tietoja viesteistä, välitystiedoista tai sijaintitiedoista taikka luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta.
316 §	316 §
Viestintää ja sijaintia koskevien tietojen käsittely ja hävittäminen	*Viestintää ja sijaintia koskevien tietojen käsittely ja hävittäminen*
— — — — — — — — — — — — — — —	— — — — — — — — — — — — — — —
Tässä pykälässä säädetty tiedonsaantioikeus ei koske luottolaitostoiminnasta annetun lain (610/2014) 15 luvun 14 §:ssä tai oikeudenkäymiskaaren 17 luvun 20 §:n 1 momentissa tarkoitettuja tietoja.	Tässä pykälässä säädetty tiedonsaantioikeus ei koske luottolaitostoiminnasta annetun lain (610/2014) 15 luvun 14 §:ssä tai oikeudenkäymiskaaren 17 luvun 20 §:n 1 momentissa tarkoitettuja tietoja *eikä viranomaistehtävien hoidossa harjoitettua viestintää viranomaisverkossa tai viranomaisviestintään liittyvässä viestintäpalvelussa.*
	316 a §
	Viestinnän välittäjän oikeus antaa tietoja Liikenne- ja viestintävirastolle
(uusi)	*Mitä 136 §:n 4 momentissa säädetään, ei estä viestinnän välittäjää antamasta Liikenne-*

Voimassa oleva laki

Ehdotus

ja viestintävirastolle tietoa 272 §:n nojalla käsittelemästään välitystiedosta tai sähköisestä viestistä, jos se on tarpeen tietoturvaloukkausten tai –uhkien selvittämiseksi taikka ennalta ehkäisemiseksi. Tiedon käsittelyyn sovellettavista viestinnän välittäjän yleisistä käsittelyperiaatteista säädetään 137 §:ssä. Tiedon salassa pitoon ja luovuttamiseen sovelletaan, mitä 319 ja 319 a §:ssä säädetään tiedon salassapidosta ja luovuttamisesta.

319 §

Vaitiolovelvollisuus ja viesteihin liittyvien tietojen luovuttaminen

Liikenne- ja viestintäviraston ja tietosuojavaltuutetun 316 ja 317 §:n nojalla saamat ja hankkimat tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta on pidettävä salassa.

Liikenne- ja viestintävirastolla on 1 momentissa säädetyn salassapitovelvollisuuden tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja:

1) viestinnän välittäjälle, lisäarvopalvelun tarjoajalle, yhteisölle, tilaajalle ja käyttäjälle jos sitä on käytetty hyväksi tietoturvaloukkauksessa, se on joutunut tietoturvaloukkauksen kohteeksi tai siihen todennäköisesti voi kohdistua tietoturvaloukkaus ja jos Liikenne- ja viestintäviraston arvion mukaan on syytä epäillä, että on tehty jokin 316 §:n 2 momentin *1–12 kohdassa* mainittu rikos;

2) muussa valtiossa toimivalle viranomaiselle tai muulle vastaavalle taholle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia.

Liikenne- ja viestintävirastolla on oikeus luovuttaa tietoja siten kuin 2 momentissa säädetään ainoastaan siinä laajuudessa kuin se on

319 §

Vaitiolovelvollisuus ja viesteihin liittyvien tietojen luovuttaminen

Liikenne- ja viestintäviraston ja tietosuojavaltuutetun 316, *316 a* ja 317 §:n nojalla saamat ja hankkimat tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemassaolosta on pidettävä salassa.

Liikenne- ja viestintävirastolla on 1 momentissa säädetyn salassapitovelvollisuuden tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja:

1) viestinnän välittäjälle, lisäarvopalvelun tarjoajalle, yhteisölle, tilaajalle ja käyttäjälle, jos sitä on käytetty hyväksi tietoturvaloukkauksessa, se on joutunut tietoturvaloukkauksen kohteeksi tai siihen todennäköisesti voi kohdistua tietoturvaloukkaus ja jos Liikenne- ja viestintäviraston arvion mukaan on syytä epäillä, että on tehty jokin 316 §:n 2 momentissa mainittu rikos;

2) 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 tietoturvaloukkauksia.

Liikenne- ja viestintävirastolla on oikeus luovuttaa tietoja siten kuin 2 momentissa säädetään ainoastaan siinä laajuudessa kuin se on

Voimassa oleva laki	*Ehdotus*
tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi. Tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.	tarpeen tietoturvaloukkausten ehkäisemiseksi ja selvittämiseksi. Tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.
Mitä 1 momentissa säädetään, ei estä välitystiedon antamista toiselle viranomaiselle, jos se on tarpeen radiohäiriön aiheuttamista koskevan rikoksen selvittämistä tai syytteeseen panoa varten taikka radioviestinnän häiriön poistamiseksi tai rajoittamiseksi.	Mitä 1 momentissa säädetään, ei estä välitystiedon antamista toiselle viranomaiselle, jos se on tarpeen radiohäiriön aiheuttamista koskevan rikoksen selvittämistä tai syytteeseen panoa varten taikka radioviestinnän häiriön poistamiseksi tai rajoittamiseksi.
Liikenne- ja viestintäviraston on 2 momentin 2 kohdassa tarkoitettuja viranomaisia ja muita tahoja määritellessään toimittava yhteistyössä liikenne- ja viestintäministeriön kanssa. Jos luovutuksen kohteesta päättämisellä voi olla huomattavaa yhteiskunnallista merkittävyyttä tai vaikutuksia sähköisen viestinnän palvelujen yleiseen kehitykseen, liikenne- ja viestintäministeriö päättää, mille viranomaisille tai muille tahoille Liikenne- ja viestintävirasto voi 2 momentissa tarkoitettuja tietoja luovuttaa.	(kumotaan)
	319 a §
(uusi)	*Tietojen luovuttaminen merkittävässä tietoturvaloukkauksessa tai -uhkassa*
	Sen lisäksi mitä muualla laissa säädetään, Liikenne- ja viestintävirastolla, poliisilla, suojelupoliisilla ja Puolustusvoimilla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa toisilleen sellaisia merkittävää tietoturva-loukkausta tai sen vakavaa uhkaa koskevia välitystietoja, tietoja viesteistä tai muita tietoja, jotka ovat välttämättömiä sellaisen merkittävän tietoturvaloukkauksen tai sen vakavanuhkan selvittämiseksi, ennalta ehkäisemiseksi tai vaikutusten poistamiseksi, jolla on tai uhkaa olla vakavia haitallisia vaikutuksia:
	1) julkisen vallan päätöksentekokokykyyn tai viranomaisten toimintaedellytyksiin;
	2) kansalliseen turvallisuuteen tai maanpuolustukseen;

Voimassa oleva laki	*Ehdotus*
	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.* *Edellä 1 momentin nojalla luovutettua tietoa saa käyttää vain tietoturvaloukkauksen tai sen vakavan uhkan selvittämiseksi tai ennalta ehkäisemiseksi taikka niiden vaikutusten poistamiseksi. Tietoa ei saa käyttää muussa tarkoituksessa. Tarpeettomat tiedot on poistettava. Tiedon hävittämiseen sovelletaan mitä 316 §:n 4 momentissa säädetään tietojen hävittämisestä.* *Edellä 1 momentin nojalla luovutettujen tietojen käsittelyssä on noudatettava, mitä luovuttajan asettamissa ehdoissa määrätään tietojen käytön rajoituksista, tietojen edelleen luovutuksesta tai luovutetun aineiston palauttamisesta. Luovuttavan viranomaisen on ilmoitettava luovuttamisen yhteydessä, jos luovutettavaan tietoon liittyy kyseisiä rajoituksia.*
	————
	———
	Tämä laki tulee voimaan päivänä kuuta 20

2.

Laki

henkilötietojen käsittelystä Puolustusvoimissa annetun lain 29 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan henkilötietojen käsittelystä Puolustusvoimissa annetun lain (332/2019) 29 §:n 1 momentin 18 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
29 §	29 §
Oikeus luovuttaa henkilötietoja lakisääteisten tehtävien suorittamiseksi	*Oikeus luovuttaa henkilötietoja lakisääteisten tehtävien suorittamiseksi*
Puolustusvoimat saa salassapitosäännösten estämättä luovuttaa teknisellä käyttöyhteydellä tai tietojoukkona muulle viranomaiselle ja julkista tehtävää hoitamaan asetetulle yhteisölle henkilötietoja, jotka ovat tarpeen tämän laissa säädetyn tehtävän suorittamiseksi, seuraavasti:	Puolustusvoimat saa salassapitosäännösten estämättä luovuttaa teknisellä käyttöyhteydellä tai tietojoukkona muulle viranomaiselle ja julkista tehtävää hoitamaan asetetulle yhteisölle henkilötietoja, jotka ovat tarpeen tämän laissa säädetyn tehtävän suorittamiseksi, seuraavasti:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
18) Liikenne- ja viestintäviraston *kyberturvallisuuskeskukselle* Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:ssä säädettyjen tehtävien hoitamista varten;	18) Liikenne- ja viestintäviraston Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:ssä *ja sähköisen viestinnän palveluista annetun lain (917/2014) 304 §:n 1, 7, 9 ja 10 kohdassa* säädettyjen tehtävien hoitamista varten;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

———

Tämä laki tulee voimaan päivänä kuuta 20 . .

3.

Laki

henkilötietojen käsittelystä poliisitoimessa annetun lain 22 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan henkilötietojen käsittelystä poliisitoimessa annetun lain (616/2019) 22 §:n 1 momentin 1 kohta seuraavasti:

Voimassa oleva laki	*Ehdotus*
22 §	22 §
Muu henkilötietojen luovuttaminen viranomaisille	*Muu henkilötietojen luovuttaminen viranomaisille*
Poliisi saa salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona 5–8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi, seuraavasti:	Poliisi saa salassapitosäännösten estämättä luovuttaa teknisen käyttöyhteyden avulla tai tietojoukkona 5–8, 11 ja 12 §:ssä tarkoitettuja henkilötietoja viranomaisen laissa säädetyn tehtävän suorittamiseksi, seuraavasti:
1) Liikenne- ja viestintävirastolle liikenteen palveluista annetun lain 197 ja 217 §:n mukaisesti tietoja, jotka ovat välttämättömiä sen laissa säädettyjen tehtävien hoitamista varten;	1) Liikenne- ja viestintävirastolle liikenteen palveluista annetun lain 197 ja 217 §:n mukaisesti tietoja, jotka ovat välttämättömiä sen laissa säädettyjen tehtävien hoitamista varten, *sekä Liikenne- ja viestintäviraston Liikenne- ja viestintävirastosta annetun lain (935/2018) 3 §:ssä ja sähköisen viestinnän palveluista annetun lain 304 §:n 1, 7, 9 ja 10 kohdassa säädettyjen tehtävien hoitamista varten;*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
	————
	———
	Tämä laki tulee voimaan päivänä kuuta 20 . .