

Outi Slant
TIO / TTU**Lausuntoyhteenveto**
16.8.2022
VN/30823/2021

Julkinen

Lausuntoyhteenveto luonnoksesta hallituksen esitykseksi laeiksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä puolustusvoimista annetun lain ja henkilötietojen käsittelystä poliisitoimissa annetun lain muuttamisesta

Liikenne- ja viestintäministeriö on pyytänyt lausuntoja luonnoksesta hallituksen esitykseksi laeiksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä puolustusvoimista annetun lain ja henkilötietojen käsittelystä poliisitoimissa annetun lain muuttamisesta. Lausuntoaika oli xx.5.-26.7.2022. Lausuntoja pyydettiin 25 eri taholta, jotka viranomaisten lisäksi edustivat ehdotuksessa kriittisiksi toimialoiksi katsottuja toimialoja. Ministeriöitä pyydettiin kokoamaan lausuntoihinsa hallinnonalansa yhteen sovitettut näkemykset.

Lausuntoja annettiin yhteensä 12. Lausunnon antoivat seuraavat tahot:

Valtiovarainministeriö
Sosiaali- ja terveystieteiden ministeriö
Sisäministeriö
Puolustusministeriö
Oikeusministeriö
Liikenne- ja viestintävirasto Traficom
Teknologiateollisuus ry (yhteinen lausunto Kyberala ry:n kanssa)
Finnish Information Security Cluster (FISC) – Kyberala ry
Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry
Elinkeinoelämän keskusliitto EK
Finanssiala ry
Tieto- ja viestintäteknikan ammattilaiset TIVIA ry

Lausuntojen keskeinen sisältö***Yleisiä havaintoja***

Puolustusministeriön lausunnossa nostetaan esille, että käsiteltävänä olevan hallituksen esitys on vasta välivaihe laajemman kyberpuolustuksen näkökulmasta. Pääosa kyberturvallisuuden kehittämisohjelmassa kuvatusista toimivaltuustyöistä tehdään erillisessä sisäministeriön ja puolustusministeriön vastuulla olevassa selvitystyössä ja sen jälkeen käynnistyvässä lainsäädännön uudistamistyössä. Ministeriö huomauttaa lisäksi, että nykytilan kuvausta olisi tietyiltä osin tarve täsmentää. Luonnos antaa tällä hetkellä kuvan, että tilanne olisi valtaosin hyvä ja kattava kyberturvallisuus olisi saavutettavissa verraten pienemmillä muutoksilla. Puolustushallinnon osalta yhteistyö koetaan pinnalliseksi eikä sen pohjalta saavuteta kansallista tilanneymmärrystä eikä koordinoitua vastetta. Se huomauttaa, että valtaosa työn alussa tunnistetuista haastavammista ja periaatteellisemmista kehitystarpeista on siirretty sisäministeriön ja puolustusministeriön yhteiselle selvitysryhmälle. Viranomaisyhteistyö on tällä hetkellä kuitenkin pinnallista ja yksittäistapauksia koskevaa, minkä vuoksi laajempia kysymyksiä tullaan tarkastelemaan laajemmin poikkihallinnollisessa työryhmässä. Tämä tulisi mainita hallituksen esityksessä. Ministeriö on lisäksi ehdottanut muutamia täydennyksiä viranomaisten tehtäviin ja kansainväliseen vertailuun liittyen.

Virka-apu*Lausunnolla ollut ehdotus:*

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-apua poliisilta, suojelupoliisilta ja Puolustusvoimilta merkittävien tietoturvaloukkausten tai -uhkien 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 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 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, jollei muualla laissa toisin säädetä.

Sisäministeriö pitää virka-apua koskevia ehdotuksia kannatettavina ja perusteltuina. Poliisin resurssien ja ajankäytön näkökulmasta on tärkeää, että SVPL:n 309 §:n 3 momenttiin olisi selkeästi kirjattu se, että virka-avusta aiheutuneista kustannuksista vastaa virka-avun pyytäjä, jollei asiasta toisin sovita ja että virka-avun antamisen edellytyksenä on, että se ei vaaranna virka-apua antavalle viranomaiselle säädettyjen muiden tärkeiden tehtävien suorittamista. Traficom in päätöksentekomenettelyjen keventämistä pidetään myös kannatettavana, sillä vakavien tietoturvahukien ja -loukkausten estäminen, selvittäminen ja hallinta vaativat lähes aina kiireellisiä toimenpiteitä.

Sosiaali- ja terveysministeriö pitää virka-apuun ehdotettuja muutoksia perusteltuina ja kannatettavina.

Puolustusministeriö on lausunnossaan todennut, että ehdotetut lainsäädäntömuutokset todennäköisesti parantavat viranomaisten toimintaedellytyksiä esityksessä kuvattujen tavoitteiden mukaisesti. Ministeriö esittää muutoksia esityksen perustelujen virka-avun kuvaamista koskevaan jaksoon.

Oikeusministeriön mukaan ehdotuksessa tulisi keskittyä enemmän virka-avun yleisempien edellytysten valossa, eikä pelkästään verraten vaatimaan virka-apuun. Lisäksi Puolustusvoimien toimivalta ehdotuksen mukaisen tehtävän hoitamiseen jää epäselväksi.

Traficom pitää tärkeänä virka-apuun ehdotettavaa lisäystä. Viraston mukaan olisi kuitenkin hyvä tehdä tarkempaa selkoa siitä, mikä on ehdotuksen 309 ja 319 a §:ssä käytetyn vaikutusten poistamisen käsitteen suhde eri viranomaisten tehtäviin ja toimivaltaan. Traficom toteaa, että sen tehtäväksi on säädetty mm. tietoturvaloukkauksia koskeva tiedonkeruu, tiedottaminen ja selvittäminen. Virka-apupyynnön tulee liittyä sitä pyytävän viranomaisen tehtäväpiiriin, joten viranomaisten tehtävien suhde toisiinsa tulisi olla selkeä. Lisäksi suhteesta yksityiseen sektoriin todetaan, että viranomaiset voivat tukea organisaatioita vaikutusten poistamista koskevissa toimenpiteissä.

Traficom kannattaa virka-avun päätöksentekoprosessiin liittyvää muutosta. Traficom pitää tarpeettomana ehdotuksen uuden 4 momentin lisäystä ”jollei muualla laissa toisin säädetä” johtuen ehdotuksen uudesta 319 a §:stä. Voimassa oleva momentti sisältää luonteeltaan informatiivisen

säännöksen siitä, että virka-apun antaminen ei itsessään laajenna luottamuksellisen viestinnän käsittelyä tai luovuttamista koskevia oikeuksia, joista tulisikin säätää erikseen. Virasto ehdottaa, että ehdotetussa 4 momentissa otettaisiin selkeästi kantaa siihen, ettei myöskään 309 §:n 1 momentin mukaisen virka-apun vastaanottaminen antaisi virastolle sinänsä oikeutta luovuttaa välitystietoja virka-apua antavalle viranomaiselle vaan välitystietojen luovuttamiseen sovellettaisiin 319 ja 319 a §:ää. Nyt jää osin epäselväksi, voisiko ehdotuksen nojalla luovuttaa virka-apua antavalle viranomaiselle välitystietoja.

Finanssiala ry on pitänyt tärkeänä, että vakavissa tietoturvaloukkauksissa viranomaisille turvataan riittävät mahdollisuudet hyödyntää toistensa osaamista ja resursseja. Toiminnan tulee olla poikkeuksellisesta luonteestaan huolimatta suunnitelmallista eli viranomaisten tulee tunnistaa ne tilanteet ja olosuhteet, joissa virka-apun saaminen olisi tarpeen. Suunnittelun avulla varmistettaisiin myös, että virka-apua on todellisuudessa myös saatavilla.

Elinkeinoelämän keskusliitto EK esittää, että yhteistyötä tulisi ulottaa myös yksityisen sektorin toimijoihin. Epäselväksi jää, miten ehdotus toteuttaa tavoitetta tietoturvaloukkausten tai uhkien vaikutusten poistamisessa, kun usein vastuun näissä tilanteissa on yksityisillä. Epäselväksi jää, miten viranomaisten välinen tiedonvaihto parantaa tätä tilanteessa. Tältä osin perusteluja tulisi täsmentää.

EK, Teknologiateollisuus sekä FISC esittävät myös, että ehdotuksen 309 §:ssä tai muussa soveltuvassa säännöksessä tulisi määritellä virka-apun harkintaan liittyvät kriteerit. Tällä on suora yhteys siihen, minkälaisia tapauksia voidaan pitää merkittävänä ja seurauksiltaan vakavina tietoturvaloukkaustilanteina, ja jotka voivat siten laukaista oikeuden ehdotuksessa tarkoitettuun tiedonvaihtoon ja virka-apuun. EK huomauttaa, että myös virka-aputilanteessa toisen viranomaisen henkilöstö saa tosiasiallisesti tietoa muutoin tiedonvaihtoa rajoittavien säännösten estämättä. Säännökseen tulisi kirjata asiallisen soveltamisalan lisäksi tilanteen intensiivisyyttä ja merkittävyyttä koskevat kriteerit (vaikutusten laajuus, kesto, maantieteellinen levinneisyys, viestintäpalvelujen käytettävyyttä, eheys, viestinnän luottamuksellisuus).

EK, Teknologiateollisuus ry sekä FISC esittävät lisäksi, 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.

FISC nostaa lisäksi esille, että kuten ehdotuksessa asianmukaisesti todetaankin, että ”useassa tilanteessa vastuu vaikutusten poistamisesta on hyökkäyksen kohteeksi joutuneella toimijalla itsellään tai tämän palveluntarjoajalla” tarkoittaa käytännössä sitä, että hyökkäyksen kohteen kaikki omat resurssit voivat olla käytössä tai jopa ylityöllistyneinä pitkän aikaa. On kuitenkin perusteltua olettaa, että merkittävissä ja seurauksiltaan vakavissa tietoturvaloukkaustilanteissa esim. kohdeorganisaation asiakkaiden, yhteistyökumppanien, muiden osallisten tai muutoin vaikutusten alaisten tahojen oikeuksien turvaaminen voi ylittää vastuutahon tosiasiallisen kyvykkyyden ja siten edellyttää laajojakin viranomaisten koordinoimia lisätoimia.

Teknologiateollisuus ry ja FISC nostavat esille, että erityisesti vaikutusten poistamista koskevaa käsitettä tulisi tehdä ehdotuksessa ymmärrettäväksi, koska kyse on käytännössä yksityisen sektorin toiminnasta. Ehdotuksessa tulisi tehdä selväksi, miten tiedonvaihto edesauttaisi vaikutusten poistamista eritoten, kun lisäperusteena ehdotuksessa on esitetty, että tiedonvaihtoa tarvitaan viranomaisten ”päätoimintakokyyden turvaamiseksi”. Kysymys on siis siitä, millaisia päätöksiä

viranomaisen tulisi kyetä tekemään? Olisiko kyse tietoturvaloukkaustilanteen johtamisesta vai kenties selvittämistyön suuntaamisesta vai jostain muusta. Miten viranomaistoiminnalla voitaisiin edesauttaa vaikutusten poistamista?

Tiedonvaihto

Lausunnolla ollut ehdotus:

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.

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.

319 a §

Tietojen luovuttaminen merkittävässä tietoturvaloukkauksessa tai -uhkassa

Sen lisäksi mitä muualla laissa on säädetty Liikenne- ja viestintävirastolla, poliisilla, suojelupoliisilla ja Puolustusvoimilla on salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa sellaisia merkittävää tietoturvaloukkausta tai -uhkaa koskevia tietoja toisilleen, jotka ovat välttämättömiä sellaisen merkittävän tietoturvaloukkauksen tai -uhkan selvittämiseksi, ennalta ehkäisemiseksi tai vaikutusten poistamiseksi, jolla on tai uhkaa olla vakavia haitallisia vaikutuksia kansalliseen turvallisuuteen, maanpuolustukseen, kansainvälisiin suhteisiin, julkisen vallan päätöksentekokykyyn, yhteiskunnan kriittiseen infrastruktuuriin taikka yleiseen järjestykseen ja turvallisuuteen.

Edellä 1 momentin nojalla luovutettua tietoa saa käyttää vain tietoturvaloukkausten ja -uhkien selvittämiseksi, ennalta ehkäisemiseksi tai niiden vaikutusten poistamiseksi. Tietoa ei saa käyttää muussa tarkoituksessa.

Valtiovarainministeriö on tunnistanut eri viranomaisten tehtäviin liittyvät limittäisyydet ja yhteneväisyydet. Se katsoo tarpeelliseksi, että eri viranomaisten välisen yhteistyön osalta tunnistetaan tiedonjakoon liittyviä ongelmia ja että lainsäädäntöä pyritään tältä osin yhtenäistämään esitetyin lakimuutoksien. Valtiovarainministeriön Haukka-hankkeessa on käynnissä julkisen hallinnon digitaalisen turvallisuuden yhteistoiminta- ja hallintamalliselvitys. Kun viranomaisten yhteistyöhön liittyvää lainsäädäntöä kehitetään edelleen, on tämän selvityksen pohjalta mahdollista tarkastella viranomaisten tehtäviä myös tiedonvaihtoa laajemmin ja arvioida kuinka toiminta olisi mahdollisimman tehokasta sekä mahdollisia tarpeita tehdä hallinnollisia muutoksia.

Valtiovarainministeriö nostaa esille kriittisten toimintojen käsitteen ja katsoo, että toimijoiden joukkoon pitäisi kuulua myös valtion velan- ja kassahallinta. Valtiokonttori vastaa valtion lainanotosta, kassahallinnasta ja valtionvelan riskienhallinnasta. Valtion velanhallinnassa korostuu ajantasainen ja kattava riskienhallinta, joista aiemmin hallinnoitavia ovat olleet jo mm. markkinariski, rahoitusriski, luottoriski, oikeudelliset ja toiminnalliset riskit sekä malliriski. Valtiokonttorille mm. tietoturva- ja kyberriskien hallinnoiminen on keskeistä. Ministeriö nostaa esille, että kriittisen infrastruktuurin toimijoiden yksiselitteisempi tunnistaminen lainsäädännössä olisi tarpeen. Tulkintojen yhtenäistäminen eri lainsäädäntöjen välillä olisi tarpeen (esim. yritysostolaki 2 § 1 mom. tai verkkoinfrastruktuurin yhteisrakentamisesta ja käytöstä annettu laki 2 § 7 kohta).

Sisäministeriö pitää esityksen tavoitteita pääosin kannatettavina ja pitää tiedonvaihdon ja virka-avun merkitystä tärkeänä tietoturvaloukkausten havainnoinnissa, torjunnassa ja selvittämisessä. Sisäministeriö pitää perusteltuna, että esityksessä ehdotetulla tavalla tiedonvaihtoon liittyvästä salassapitosäätelystä ja muista tiedonluovutuksen rajoituksista poikkeamisen kynnystä pidetään verrattain korkeana, jotta muun muassa perustuslaissa turvattu yksityiselämän suoja ja luottamuksellisen viestin suoja sekä tietosuojalainsäädännöstä tuleva käyttötarkoitussidonnaisuuden periaate toteutuvat asianmukaisesti.

Sisäministeriö katsoo, että esityksen perusteluihin voisi kirjata, että kukin viranomainen toimii saatuja tietoja hyödyntäen omassa roolissaan toimivaltasäännösten puitteissa. Ministeriö huomauttaa, että erityislainsäädännössä (esim. passilaissa ja henkilökorttilaissa) on säädettyjen tehtävien suorittamiseksi käsiteltyjen biometristen tietojen luovuttaminen henkilötietojen käsittelystä poliisitoimessa annetussa laissa rajattu tarkasti vain määrätyille viranomaisille ja määrättyihin tarkoituksiin. Jatkovalmistelussa olisi perusteltua arvioida tarve säätää siitä, onko SVPL:n 319 a §:n nojalla saatuja tietoja oikeus luovuttaa eteenpäin. Edelleen luovutukselle voisi olla tarkoituksenmukaista vähintäänkin asettaa rajoituksia.

Sisäministeriö kiinnittää 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 lakisäätteisten tehtävien suorittamista. Poliisin lakisäätteisten tehtävien suorittaminen ei saisi vaarantua myöskään siitä syystä, että henkilö saisi toisen viranomaisen kautta pääsyn poliisin luovuttamiin tietoihin, joihin kohdistuu poliisissa tarkastusoikeuden rajoituksia.

Puolustusministeriö ehdottaa terminologian osalta käytettäväksi tiedon luovuttamisen sijaan käsiteparia tietojen luovuttaminen ja vastaanottaminen en vuoksi, että tiedonvaihtoon sisältyy myös tiedon vastaanottamisen toimivaltuudet ja vastuut. Ministeriö nostaa esille lisäksi sitä, että sääätämisyjärjestysperusteluissa esitetyistä asioista osa on sellaisia, että ne ovat vaikeasti tulkittavia. Tämä pätee erityisesti henkilötietojen suhteeseen tiettyihin teknisluonteisiin tunnistetietoihin. Esimerkiksi esityksen sivulla 20 viitattu voimassa oleva tulkinta IP-osoitteiden tulkittamisesta kaikissa tilanteissa henkilötiedoksi saattaa johtaa ratkaisemattomiin ongelmiin. Ministeriö toteaa, että soveltamiskynnystä tiedonvaihdolle on kuvattu kiitettävästi, mutta se millainen tapahtuma muodostaa vakavan tietoturvaloukkaustilanteen jäänee viime kädessä kuitenkin soveltamiskäytännön varaan.

Puolustusministeriö on esittänyt perusteluihin lisäyksiä hallinnonalansa lainsäädännöstä ja lisäksi esittänyt tarkennusehdotuksia Puolustusvoimien tehtävien kuvaukseen liittyen. Ministeriö on korostanut, että Kriittisen infrastruktuurin toimijoissa ja yhteiskunnan elintärkeiden toimintojen toteuttajissa valtaosa on siviiliyrityksiä. Ilman siviilialan toimijoilta saatavan tiedon parantamista, nimenomaan lisävelvoitteiden kautta, ei viranomaistoiminnankaan kehittämisellä saavuteta haluttua tulosta. Puolustusministeriön näkemyksen mukaan kansallisen turvallisuuden ja maanpuolustuksen edellyttämä tiedonsaanti siviilitoimijoilta kybertoimintaympäristön asioista ei tule jäädä vapaaehtoisuuden varaan silloin, kun esimerkiksi EU:n verkko- ja tietoturvadirektiivin (EU) 2016/1148,

jäljempänä NIS-direktiivi, ilmoitusvelvollisuus ei täyty. Tämä tulee huomioida uudistuksen jälkeisessä valmistelutyössä.

Oikeusministeriö on lausunnossaan nostanut esille 319 a §:n säännöksen tarkkarajaisuutta koskevan haasteen. Haasteeksi on erityisesti havaittu ehdotuksen suhde PL 10.4 §:n kvalifioituun lakivaraukseen, jossa mainitut edellytykset ja tarkoitukset perusoikeuden rajoituksen tulisi täyttää. Perusteluista ei selkeästi ilmene esimerkiksi se, perustuisiko rajoitus aina tai ainakin joltain osin yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkintaan. Luonnoksesta ei myöskään ilmene selvästi se, miltä osin tiedonluovutuksessa olisi kyse tiedustelutoiminnassa saatujen tietojen luovutuksesta. Myös oikeusministeriö kiinnittää huomiota kriittisen infrastruktuurin käsitteen väljyyteen, joka osaltaan saattaa edellyttää täsmentämistä.

Oikeusministeriö on kiinnittänyt huomiota ehdotuksen tietoturvaloukkauksen uhkaa koskeviin seikkoihin. Säännösluonnoksesta ei kuitenkaan ilmene selvästi sitä, että tietoja voitaisiin luovuttaa jo siinä vaiheessa, kun tietoturvaloukkauksesta on olemassa perusteltu epäily, vaan säännös mahdollistaa tiedonluovutukset silloin, kun kyse on tietoturvaloukkauksen tai –uhkan selvittämisestä, ennalta ehkäisemisestä tai vaikutusten poistamisesta. Oikeusministeriö esittää harkittavaksi, olisiko tietoturvaloukkausten uhkaan ja ennalta ehkäisyyn liittyvä tiedonsaantioikeus ja toisaalta tapahtuneiden loukkausten selvittämiseen liittyvä tiedonsaantioikeus mahdollista määritellä erikseen asianmukaisilla kriteereillä, joka voisi täsmentää sääntelyä.

Oikeusministeriö on esittänyt, että 319 a §:n suhde muuhun lainsäädäntöön on paikoin epäselvästi ilmaistu ja perustelut tältä osin kaipaavat täsmentämistä siten, että ne kuvaavat ehdotusta täsmällisesti. Ministeriö katsoo lisäksi, että ehdotusluonnoksen 319 a §:ään kirjattu tiedonluovutussäännös jää myös perustuslakivaliokunnan tiedonluovutussääntelyä koskevan käytännön valossa väljäksi. Sääntämisperusteluissa on asianmukaisesti tunnistettu asiaa koskeva perustuslakivaliokunnan käytäntö, joskin käytännön arviointi sekoittuu osin luottamuksellisen viestinnän suojaa koskevan rajoituksen arviointiin ja jää näin ollen hieman epäselväksi. Lisäksi oikeusministeriön käsityksen mukaan ainakaan säännösperusteisesti tiedonsaantioikeuden ulkopuolelle ei rajaudu esimerkiksi arkaluonteiset henkilötiedot, vaan myös näitä voitaisiin säännöksen perusteella luovuttaa. Perustuslakivaliokunnan käytännön mukaan arkaluonteisten tietojen käsittely on rajattava täsmällisillä ja tarkkarajaisilla säännöksillä vain välttämättömään.

Oikeusministeriö on lisäksi nostanut esille, että ns. palomuurisääntelyn perustelut ovat verrattain suppeat suhteessa siihen, että lakiehdotuksesta seuraa poikkeus perustuslakivaliokunnan tärkeänä pitämään palomuurisääntelyyn nähden

Sosiaali- ja terveysministeriö huomauttaa, että ehdotuksessa ei ole käsitelty asiaa erityisen arkaluonteisten tietojen osalta. Jos viestin tai yhteyksien tunnistetietoja välitetään massamaisesti viranomaisten välillä, on todennäköistä, että joukossa on myös täysin asiallista liikennettä. Edelleen on mahdollista, että osa asiallisesta tietoliikenteestä on erityisen arkaluonteista. Viranomaisilla ei ole oikeutta saada tietoonsa esimerkiksi asianajajan tai asiakkaan tai lääkärin tai muun terveydenhuollon ammattihenkilön ja potilaan välistä taikka sosiaalipalveluissa asiointiin liittyviä asioita. Tässä yhteydessä on huomattava, että jo tieto yhteydenotosta on salassa pidettävää. Asia tulisi arvioida perusteluissa ja lakeihin tulisi kirjata, että salassa pidettävä ja käsillä olevan tilanteen kannalta ilmeisen tarpeeton tieto tulee poistaa välittömästi, jos sellaista havaitaan, eikä tietoa saa hyödyntää mihinkään käyttötarkoitukseen. Pelkkä salassapitovelvoite ei ole tältä osin riittävä.

Traficom kannattaa ehdotettuja muutoksia ja korostaa yhteistyön merkitystä kyberturvallisuuden kehittämiseksi ja varmistamiseksi. Ehdotuksessa on tärkeää löytää tasapaino yhtäältä viranomaisten tiedonjaon mahdollistamisen ja toisaalta viestinnän luottamuksellisuuteen tai salassapitoperusteisiin tehtävien rajoitusten välillä. Se kannattaa ehdotuksia vastavuoroisesta tiedonluovutuksesta vakavissa tietoturvaloukkaustilanteissa tai niiden uhkissa. Ilman muilta viranomaisilta saatavaa tietoa

merkittävistä ja vakavista tietoturvaloukkauksista tai niitä koskevista uhkista, virasto voi joutua reagoimaan loukkauksiin ja uhkiiin vajavaisin tiedoin. Virasto kuitenkin 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 tässä yhteydessä myös valmiuslain hiljattain valmistuneen muutoksen esitöihin. Yhtenä mahdollisena ratkaisuna se esittää, että lisätään suojattavien etujen luetteloon esimerkiksi tilanteet, joissa tietoturvaloukkauksella on vakavia haitallisia vaikutuksia muuhun erittäin tärkeää yleiseen etuun tai yksityiseen etuun, kuten kansalaisten yksityisyyden suojaan, riippumatta siitä kohdistuuko loukkaus esimerkiksi kriittiseen infrastruktuuriin.

Traficom kannattaa sitä, että tietojen käyttöä ei rajoiteta yksittäisen tapauksen selvittämiseen, jolloin tietoja voidaan käyttää myös vastaavan kaltaisten tietoturvaloukkausten havaitsemiseksi ja selvittämiseksi. Virasto kiinnittää huomiota, että säätämisyjärjestysperusteluissa ei ole arvioitu esityksen suhdetta omaisuudensuojaan, vaikka ehdotus mahdollistaisi myös ehdottoman salassapitovelvollisuuden piiriin kuuluvien liikesalaisuustietojen luovuttamisen.

Traficom kiinnittää huomiota myös poliisitoimen ja Puolustusvoimien henkilötietolakien ehdotuksiin. Viraston mukaan ehdotuksen 319 a §:n suhde henkilötietojen käsittelystä annettuihin lakeisiin mahdollistaisi jatkossa salassapitosäännösten estämättä tapahtuvan henkilötietojen luovuttamisen Liikenne- ja viestintävirastolle laista riippuen joko tarpeellisuus- tai välttämättömyyskriteerillä osin päällekkäisistä tilanteista SVPL 319 a §:ään nähden. Tämän johdosta myös salassa pidettäviä henkilötietoja voitaisiin luovuttaa lievemmillä kriteereillä kuin ehdotuksen mukaisessa 319 a §:ssä. Tällöin epäselväksi jää, mitä tietoja jäisi SVPL 319 a §:n mukaisen korkeamman luovutuskynnyksen soveltamisen piiriin ja mitä voitaisiin luovuttaa erityislakien perusteella. Virasto huomauttaa myös käsitteistön osalta, että tiedonhallintalain tarkoituksena on mahdollistaa teknistä käyttöyhteyttä koskevan toimialakohtaisen sääntelyn purkamista.

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.

Elinkeinoelämän keskusliitto EK, Teknologiateollisuus ry sekä FISC näkevät haasteena ehdotuksen 319 a §:n määritelmän. Tavoite säännöksessä on kannattava, mutta ottaen huomioon esimerkiksi perusoikeussuojan, tulisi säännökseltä edellyttää mahdollisimman suurta selkeyttä. Esimerkiksi yhteiskunnan kriittisillä toiminnoilla ei ole yhtä täysin vakiintunutta tarkkarajaista sisältöä. Määritelmää esitetään vielä tarkemmin harkittavaksi.

EK nostaa esille myös sen, että koska media-ala on nostettu kriittiseksi toimialaksi, siihen liittyvää lähdesuojaa ei ole esityksessä tarkasteltu. Ehdotusta tulisi jatkossa tarkastella myös lähdesuojan kannalta.

FiCom ry pitää tiedonvaihtoa koskevaa ehdotusta pääosin kannatettavana ja perusteltuna. *FiCom*, Teknologiateollisuus ry sekä *FISC* ehdottavat, että säännöstä täsmennettäisiin siten, että luovutettua tietoa ei saa luovuttaa edelleen muille tahoille kuin pykälässä mainituille suomalaisille viranomaisille. Lisäksi se ehdottaa, että 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. *FiCom* perustelee täsmennysehdotuksiaan erityisesti luottamuksellisen viestin ja yksityisyyden suojaan kohdistuvan perusoikeussuojan vuoksi.

FISC kannattaa esityksen tavoitteita, mutta huomauttaa, että esitetyt muutokset eivät ole yksinään riittäviä, erityisesti kun tavoitellaan tietoturvaloukkausten ja –uhkien ehkäisemistä (torjunta), mahdollisimman varhaista havaitsemista sekä haitallisten vaikutusten poistamista. Tämä johtuu siitä, että yksityinen sektori tulisi huomioida ehdotuksessa paremmin.

Tietojen luovuttaminen ulkomaisille viranomaisille

Lausunnolla ollut ehdotus:

319 §

(kumotaan) Liikenne- ja viestintäviraston on 2 momentin 2 kohdassa tarkoitettuja viranomaisia ja muita tahoja määriteltäessä 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.

Traficom esittää, 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. Lisäksi luovutuksen kohde on hyvin avoin ja siitä puuttuvat kaikki ehdotetun 319 a §:n mukaiset edellytykset. *FiComin* mukaan ei voi olla niin, että ulkomaiselle toimijalle voidaan luovuttaa tietoja huomattavasti kevyemmällä perusteella kuin rajoitetulle joukolle kotimaisia viranomaisia. *FiCom* pitää menettelyn keventämistä ymmärrettävänä, mutta luovuttamisen edellytyksiä pitäisi tiukentaa. Lähtökohtana tulisi olla ehdotetun 319 a §:n edellytykset, kuten merkittävyys, vaikuttavuus, välttämättömyys, suhteellisuus ja käyttötarkoitus.

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.

Viestinnän välittäjän oikeus luovuttaa tietoa Traficomille

Lausunnolla ollut ehdotus:

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. Tietojen hävittämiseen sovelletaan, mitä 316 §:n 4 momentissa säädetään tietojen hävittämisestä.

Oikeusministeriö on huomauttanut, että ehdotuksen säätämisyjärjestysperustelujen osalta tulisi täydentää arviointia ehdotuksen 316 a §:n suhteesta perustuslain 10 §:ään. Myös säännöskohtaisissa perusteluissa tulisi ilmetä, että kyseessä on poikkeuslainsäädäntö lain 136 §:n 4 momenttiin.

Sosiaali- ja terveysministeriö toteaa, että ehdotus laajentaa viestinnän välittäjien tiedonluovutus-oikeutta. Se pitää ehdotusta lähtökohtaisesti kannatettavana. Viestinnän välittäjän käsite on laaja, eikä esityksestä käy tarkemmin ilmi, 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.

Traficom kannattaa ehdotusta vapaaehtoisesta tiedonluovuttamisesta, sillä nimenomaisen säännöksen puute on aiheuttanut epäselvyyttä ja viivästystä joidenkin tapausten selvittämisessä, kun viestinnän välittäjä ei ole katsonut voivansa luovuttaa tietoja kuin yksilöidystä viranomaisten tietopyynnöistä. Jatkovalmistelun osalta virasto katsoo, että olisi hyvä arvioida olisiko ehdotusta tarpeen täydentää luovutettavan tiedon minimointia korostavalla säännöksellä. Vaikka yleissäännös asiasta on, erityinen säännös korostaisi luovutettavan tiedon välttämättömyyttä. Koska ehdotuksen voidaan katsoa pitävän sisällään kokonaisuudessa sen tietoliikenteen, mitä havainnoidaan tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, tulisi harkita, pitäisikö tietojen luovuttaminen rajoittaa selvyden vuoksi tilanteisiin, joissa luovutettavat tiedot liittyvät tiettyyn (epäilyyn) tietoturvalle haittaa aiheuttavaan häiriöön.

Traficom nostaa lisäksi esille, että ehdotusta tulisi arvioida säätämisyjärjestysperusteluissa PL 10 §:n kannalta. Ehdotus koskee käytännössä sen selventämistä, että viestinnän välittäjä voi oma-aloitteisesti luovuttaa Liikenne- ja viestintävirastolle havaitsemiinsa tietoturvaloukkauksiin liittyviä luottamuksellisia välitystietoja ja viestejä tilanteissa, joissa se käsittelee niitä tietoturvasta huolehtimiseksi jo voimassa olevan SVPL 272 §:n perusteella. Vaikka tällaista oikeutta tietojen luovuttamiseen voidaan pitää perusoikeuden rajoituksena, sääntely rajoittaa käsittelyn minimiin ja turvaa viestinnän säilymistä mahdollisimman pitkälle luottamuksellisena. Lisäksi ehdotusta tulisi arvioida suhteessa sähköisen viestinnän tietosuojadirektiivin 15 artiklan sääntelyyn.

FiCom ry pitää virka-apua koskevia ehdotuksia kannatettavina ja perusteltuina. Se pitää ehdotuksen perustumista vapaaehtoisuuteen tärkeänä, eikä sitä saa myöhemmin muuttaa velvoittavaan muotoon. Jos yrityksellä ei ole tällä hetkellä menetelmiä ja keinoja ryhtyä selvittämään 272 §:n mukaisia tilanteita, ei näitä keinoja tule luoda nyt ehdotetun säännöksen toteuttamiseksi. Viestinnän välittäjän

luovutusosoikeuden kannalta ongelmalliseksi voi muodostua se, että tietojen luovuttaminen viranomaiselle voi nostaa kynnystä, koska tällöin viranomaisen tutkii, onko 272 §:n mukainen käsittelyoikeus syntynyt. Tämä saattaa olla erityisesti pk-yritysten haaste. FiComin mukaan ehdotus voi paikata sääntelyssä olevan mahdollisen aukon tilanteissa, joissa kyse ei ole ilmoitusvelvollisuuden kynnyksen ylittävästä merkittävästä tietoturvaloukkaustilanteesta ja viestinnän välittäjä haluaisi tehdä ilmoituksen Kyberturvallisuuskeskukselle. Näissä ei merkittävässä tilanteissa viestinnän välittäjä voi tarvita Kyberturvallisuuskeskuksen tukea havaitsemiensa tietoturvaloukkausten, kuten haittaohjelmien toimintaperiaatteen selvittämiseen, sillä haasteita on käytännössä aiheuttanut näiden tietojen luovuttaminen Liikenne- ja viestintävirastolle.

Finanssiala ry ehdottaa, että SVPL 316 a §:n perusteluissa esitetyt sääntelyn rajaukset sisällytettäisiin pykälään. Finanssiala ja Elinkeinoelämän keskusliitto EK ovat huomauttaneet, että mikäli tietoja viesteistä ja välitystiedoista edelleen luovutetaan ulkomaisille viranomaisille tai muille tahoille, on varmistettava, että tietojenluovutus kaikissa tilanteissa tapahtuu soveltuvien säädösvaatumusten, yleisten tietosuojaperiaatteiden ja hyvien tietojenkäsittelykäytäntöjen mukaisesti.

EK on nostanut esille, että viestinnän välittäjien kannalta on keskeistä, että ne voivat luottaa toimivansa oikein niitä sitovan muun lainsäädännön ja asiakassopimuksia koskevien vahingonkorvaussäännösten ja sopimuslausekkeiden kannalta. Myös *EK* esittää perusteluissa ilmeneviä rajoituksia tuotavaksi säännökseen.

FiCom pitää ehdotusta viestinnän välittäjän vapaaehtoisesta tiedonluovutuksesta kannatettavana.

Muut kommentit

Oikeusministeriö on lausunnossaan nostanut esille useita säätämisyjärjestystä koskevia täydennys- ja selkeytystarpeita. Se on ensinnäkin nostanut esille, että perusteluissa sekoittuu osin viranomaisten välisen salassa pidettävän tiedon arviointi ja toisaalta luottamuksellisen viestinnän suoja koskeva arviointi. Nämä voisi mahdollisesti erottaa selkeyden vuoksi omiksi jaksoikseen. Perusteluissa pitäisi lisäksi ilmaista mihin PL 10 §:n 4 momentin lakivarauksen sisältyvää tarkoitukseen tai edellytykseen perusoikeuden rajoitus nojaa.

Oikeusministeriö on huomauttanut henkilötietojen suojaan liittyen, että henkilötietojen käsittelyä koskevia perusteluja on syytä lisätä säätämisyjärjestysperustelujen yhteyteen. Ministeriö on nostanut esiin niitä seikkoja, joita henkilötietojen käsittelyä koskevissa perusteluissa tulisi käsitellä.

TIVIA ry on lausunnossaan nostanut esille henkilötietojen suojan ehdotuksessa. Erityisesti huolta herättää viranomaisten riittävät pääsynrajoitukset ja käyttövaltuudet eli se, miten varmistutaan siitä, että asiattomat henkilöt eivät pääse katsomaan mahdollisesti entistä laajempia tietoja. Lisäksi kysytään, tehdäänkö jälkepäin auditointeja riittävästi ja oikealla laajuudella.

Oikeusministeriö on huomauttanut, että esitysluonnoksessa on käytetty tietoturvaloukkaukseen ja –uhkan määrittelyssä paikoin erilaisia käsitteitä ja terminologiaa tulisi tältä osin yhdenmukaistaa.

TIVIA ry on nostanut esille tarpeen tarkentaa ja määritellä tarkemmin tiettyjä ehdotuksessa käytettyjä käsitteitä. Näitä ovat tietoturvaan liittyvät uhkat, vakavat uhkat, merkittävien uhkien ennalta ehkäisevä toiminta ja laajamittainen häiriö.

Finanssiala ry, Elinkeinoelämän keskusliitto EK, Teknologiateollisuus ja FISC ovat nostaneet esiin, että kansallisen turvallisuuden osalta käytetty käsite ei välttämättä vastaa sitä, mitä EU:n perustamissopimuksissa tai niiden nojalla annetuissa säädöksissä tai oikeuskäytännössä tarkoitetaan. Asia on tärkeä arvioitaessa ehdotuksen yhteensopivuutta mm. tietosuojasääntelyyn, NIS-direktiiviin sekä DORA-asetukseen.

Lausunnonantajien havainnot vaikutuksista

Traficom katsoo, että esitys parhaimmillaan edistää ja selkeyttää tietojen luovuttamista viranomaisten yhteistoimintaa edellyttävissä merkittävässä tietoturvahäiriöissä, mutta vaarana on, että tavoitteita ei saavuteta täysimääräisesti, jos ehdotuksen mukaisiin tiedonluovuttamisen edellytyksiin liittyy tulkinnanvaraisuuksia. Tällainen riski liittyy esimerkiksi kriittisen infrastruktuurin käsitteeseen. Lisäksi kumulatiivisen kriteeristön mukainen soveltaminen saattaa nostaa käytännön soveltamiskynnystä varsin korkealle, mikä saattaa käytännössä rajoittaa uusien säännösten hyödynnettävyyttä. Viranomaisten tietojen luovuttamisen harkinnanvaraisuus on kannatettavaa ottaen huomioon vapaaehtoisesti tietoja luovuttavien tahojen luottamus.

*Traficom*in näkemyksen 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. Asianmukaisesti muotoiltuna ehdotus ei suhteettomasti eikä ilman asianmukaisia perusteita rajoittaisi viestinnän luottamuksellisuutta, minkä lisäksi se välillisesti edistää viestintäverkkojen, palvelujen ja niihin liitettyjen tietojärjestelmien tietoturvallisuutta, mikä osaltaan turvaa myös yksityisyyden suojan toteutumista viestintäpalveluita käytettäessä.

Elinkeinoelämän keskusliitto EK on nostanut esille, että säännöksen vaikutukset eroavat luultavasti voimakkaasti riippuen siitä, mistä toimialasta on kyse. Vaikutukset olisivat todennäköisesti merkittäviä erityisesti telekommunikaatio- ja finanssisektorilla sekä muillakin kriittisimmillä toimialoilla. Toisaalta näillä aloilla yhteistyö on vahvasta sääntelystä johtuen jo muutenkin melko säännöllistä ja toimivaa.

FiCom ry toteaa, että luonnoksessa on pääasiassa keskitytty siihen, miten säännöksen mukainen tietojenvaihto auttaa viranomaisia tietoturvaloukkauksen tai –uhkan selvittämiseksi, ennaltaehkäisemiseksi tai vaikutusten poistamiseksi. Epäselväksi jää, miten viranomaisten keskinäinen tiedonvaihto auttaa yritystä tilanteessa, jossa se on joutunut merkittävän tietoturvaloukkauksen kohteeksi. Luoko tietojenvaihto sellaisia kyvykkyyksiä, jotka edesauttavat yritystä pysäyttämään loukkauksen, turvaamaan jatkuvuuden tai palauttamaan toiminnan tasolle ennen loukkausta? Onko säännöksen tarkoitus ehkäistä loukkauksen vaikutusten laajenemista esimerkiksi muihin yrityksiin sekä jakaa tietoa ja varoituksia niille? *FiCom*in mukaan esitys kaipaa tältä osin täydentämistä jatkovalmistelussa.

Lausunnoissa esitetyt muut muutostarpeet

Finanssiala ry:n, Elinkeinoelämän keskusliiton EK:n lausunnoissa on nostettu esille, että valtaosa yhteiskunnan toiminnan kannalta elintärkeiden tieto- ja viestintätekniisten infrastruktuurin toiminnasta sekä niihin liittyvien ja niitä hyödyntävien palveluiden toiminnasta on yksityisen sektorin vastuulla. Ilman yksityisen sektorin toimijoiden aktiivista mukanaoloa tietoturvaloukkausten selvittämistä koskevat tavoitteet jäävät vajaiksi. *Finanssiala* ehdottaa selvitettäväksi jatkovalmistelussa viranomaisten ja yksityisen sektorin välisen tiedonvaihdon esteet ja selvitetään keinot niiden korjaamiseksi sekä laadittaisiin tarvittavat säädösehdotukset.

EK nostaa esille lisäksi sen, että viranomaisten ja yksityisten välisen tiedonvaihdon säännöt on määritelty kaikkialla selkeästi ja sen vuoksi täysi hyöty saadaan vasta, kun yksityinen sektori on mukana. Lisäksi viranomaisten resurssien rajallisuudesta ja viranomaistoiminnan luonteesta seuraa se, että niiden toiminta väistämättä painottuu enemmän jo tapahtuneiden häiriöiden ja loukkausten tai vähintään jo toteutuneiden ja havaittujen uhkien selvittelyyn. Yhteiskunnan tulisi kaikessa toiminnassa panostaa enemmän ennaltaehkäisyyn. Erityisesti sen kannalta kattava, luottamuksellinen ja selkeisiin säännöksiin perustuva tietojenvaihto ja tilannekuvan ylläpito viranomaisten kesken, mutta myös

viranomaisten ja elinkeinoelämän välillä on aivan keskeinen. Siksi kehittäminen ei saa jäädä vain viranomaisten väliseen tiedonvaihtoon keskittyväksi ja siksi on niin tärkeää, että elinkeinoelämän toimijat ovat mukana kehittämisessä.

EK on esittänyt säännöstä yksityisten antaman virka-apuun rinnastettavan avustamisen mahdollistamisesta. Esimerkkinä voisivat olla poliisilakiin sisältyvät säännökset avustamistyöstä, joiden tarkoituksena on mahdollistaa poikkeuksellisissa tilanteissa nopeasti tarkoitukseen sopivan ulkopuolisen avun käyttäminen.

Elinkeinoelämän keskusliitto EK, Teknologiateollisuus ry sekä FISC ovat nostaneet esille, että jatkossa tulee aiempaa useammin tilanteita, joissa sama tapahtuma tulee ilmoittaa lainsäädännön vaatimusten mukaisesti useammalle viranomaiselle. Näihin ilmoituksiin tulisi luoda yhtenäiset menettelyt ja yksi ilmoitus pohja, eikä jokaiselle viranomaiselle ja ilmoitukselle omaansa. Näin säästettäisiin aikaa tietoturvaloukkauksen ilmitulon jälkeen ja toiminta pääsisi heti alkuun tehokkaammin käyntiin. Teknologiateollisuus ja FISC nostavat lisäksi esille, että koska laajemman viranomaiskentän erityisosaamisen hyödyntäminen oletetaan parantavan tietoturvaloukkausten ja -uhkien hallintaa ja analysointia ja sen tarjoavan hyökkäyksen kohteena olevalle taholle (pääosin yritykset) paremmat edellytykset hankkia tilanteen korjaamiseksi tarvittavat palvelut, olisi ehdotetun palvelumallin kehittäminen perusteltua vähintään samassa yhteydessä muiden muutosten kanssa. Ilman tällaista palvelumallin muutosta eivät myöskään muut, huomattavasti merkittävimmät salassapidon avulla suojattavien oikeushyvien vähäisenkään heikentämiseen ole asianmukaisesti perusteltavissa.

Lisäksi EK, Teknologiateollisuus ry sekä FISC ovat pitäneet tärkeänä, että elinkeinoelämä otetaan alusta lähtien mukaan nyt lausuttavana olevaan esitykseen liittymättömässä sisäministeriön ja puolustusministeriön käynnistämässä laajemmassa selvityshankkeessa (PLM003:00/2022), jossa arvioidaan tätä esitystä laajemmin viranomaisten toimintaedellytyksiä kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa ja kyberpuolustuksessa.

FiCom ry kiinnittää huomiota siihen, että sähköisen viestinnän palvelulaissa on useita eri viranomaisille koskevia tietojen luovutusta koskevia velvollisuuksia. Lisäksi laissa on runsaasti tietojen käsittelyä koskevia säännöksiä eri viranomaisissa. Luovutus- ja käsittelysäännösten edellytykset poikkeavat toisistaan useassa kohtaa, sillä säännöksiä on lisätty ja muutettu vuosien saatossa eikä kokonaisuus ole enää selkeä. *FiCom* esittää, että käsittely- ja luovutusedellytyksistä tehdään lähiaikoina kokonaisarviointi.