

Asia: VN/30823/2021-LVM-15

Lausuntopyyntö luonnoksesta hallituksen esitykseksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain ja henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta

Yleiset kommentit viranomaisten toimintamahdollisuuksista tietoturvaloukkauksien selvittämiseksi

Yleisiä kommentteja esityksestä ja sen tavoitteista, ehdotetuista keinoista ja vaikutuksista

Kiitämme lausuntomahdollisuudesta. Viittaamme jäsenyhdistystemme Finanssiala ry:n sekä Teknologiateollisuus ry:n yhdessä Kyberala ry:n asiassa antamiin lausuntoihin ja toteamme seuraavaa:

Kannatamme esitystä. Katsomme, että toimijoiden välinen tiedonvaihto on tärkeimpiä ja tehokkaimpia tapoja torjua, havaita ja selvittää tietoturvaloukkauksia. On erittäin tärkeää, että viranomaisilla on tehokkaat, nopeasti käyttöön otettavissa ja toteutettavissa olevat keinot toimia vakavissa häiriötilanteissa tai niiden selvästi uhatessa. Nyt esitetyt muutokset eivät kuitenkaan yksinään ole riittäviä, erityisesti kun tavoitellaan tietoturvaloukkausten ja -uhkien ennalta ehkäisemistä ja mahdollisimman varhaista havaitsemista.

Muistutamme, että valtaosa yhteiskunnan toiminnan kannalta elintärkeän tieto- ja viestintätekni­sen infrastruktuurin toiminnasta sekä siihen liittyvien ja sitä hyödyntävien palveluiden tarjonnasta on yksityisen sektorin vastuulla. On selvää, että ilman yksityisen sektorin toimijoiden aktiivista mukanaoloa tietoturvaloukkausten torjumista, havaitsemista ja selvittämistä koskevat tavoitteet jäävät vajaiksi. Ehdotamme, että hallituksen esitysluonnoksen jatkovalmistelussa kartoitettaisiin viranomaisten ja yksityisen sektorin välisen tietojenvaihdon esteet, selvitettäisiin keinot myös niiden poistamiseksi ja laadittaisiin tarvittavat säädösehdotukset tilanteen korjaamiseksi.

Jatkossa tulee aiempaa useammin tilanteita, joissa sama tapahtuma tulee ilmoittaa lainsäädännön vaatimusten mukaisesti useammalle viranomaiselle, esim. tietosuoja-asetuksen ja tulevan NIS2-direktiivin Suomea koskevan täytäntöönpanolain velvoittamana. Tämä tulisi tehdä toimijoille helpoksi, eikä niin, että jokaiselle viranomaiselle ilmoitetaan niiden omalla lomakkeella. Tulisi luoda yksi sähköinen ilmoituspohja, jota käyttämällä toimija voisi yhden ilmoituksen tekemällä ohjata sen kaikille sitä tarvitseville viranomaistahoille. Näin säästettäisiin aikaa tietoturvaloukkauksen ilmitulon jälkeen ja toiminta pääsisi heti alkuun tehokkaammin käyntiin.

On myös tärkeää, 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.

Kiinnitämme huomiota myös esityksessä käytettyihin käsitteisiin. Luonnoksessa tai perustuslain 10 §:n muuttamisen yhteydessä käytetty kansallisen turvallisuuden käsite ei nähdäksemme välttämättä vastaa EU:n perussopimuksissa tai niiden nojalla annetuissa oikeudellisesti sitovissa säädöksissä (asetukset, direktiivit ja päätökset) käytettyä ja EU-tuomioistuimen vakiintuneeseen käytäntöön perustuvaa kansallisen turvallisuuden käsitettä. Korostamme asian tärkeyttä, koska sillä on merkitystä arvioitaessa ehdotusten yhteensopivuutta mm. EU:n tietosuoja sääntelyn, verkko- ja tietoturvadirektiivin (NISD) ja sen päivityksen (NIS2D) sekä valmisteilla olevan rahoitusmarkkinoiden digitaalista häiriönsietokykyä koskevan asetuksen (DORA) kanssa.

Esityksen haasteena näemme myös jossain määrin esitetyn 319 a §:n määritelmän. Säännöksen tavoite on ymmärrettävä ja sinällään kannatettava. Esityksessä ei ole kyse poikkeusolojen lainsäädännöstä, vaan sillä luodaan normaaliaikoina viranomaisille valtuuksia poikkeuksellisissa tilanteissa käytettäväksi, joihin viranomaisilla ei normaalisti olisi mahdollisuutta. Koska tietojenvaihto säännöksen tarkoittamissa tilanteissa voi kohdistua myös mm. perustuslailla ja tietosuojalainsäädännöllä suojattuun yksityiselämän suojaan ja määritelmän täyttyminen laukaisee viranomaisten oikeuden antaa tietoja, määritelmältä on voitava edellyttää mahdollisimman suurta selkeyttä. Näemme jossain määrin haasteena sen, että lainsäädännössämme yhä useammin viitataan yhteiskunnan kriittisiin toimintoihin tai toimijoihin tai kriittiseen infrastruktuuriin, mutta näille termeille ei ole yhtä täysin vakiintunutta, kaikkialla lainsäädännössä tunnustettua tarkkarajaista sisältöä. Tyypillisesti, kuten tässäkin esityksessä viitataan valtioneuvoston huoltovarmuuspäätökseen (1048/2018). Luonnoksen sivulla 40 todetaan: ”Yhteiskunnan kriittisellä infrastruktuurilla tarkoitetaan jokseenkin vastaavaa, mitä kriittisellä infrastruktuurilla on tarkoitettu valtioneuvoston huoltovarmuuspäätöksessä (1048/2018).” Myöhemmin esityksessä todetaan sivulla 42: ”Edellä mainittuihin kriittiseen infrastruktuuriin kuuluviin 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.” Käytetyistä sanoista, mm. ”jokseenkin” ja ”tai välillisesti” seuraa väistämättä, että tulkinta ei voi olla kovin tarkkarajainen sen suhteen, milloin säännöksen

tarkoittama tilanne on käsillä. Esitämme harkittavaksi, voisiko ja tulisiko määritelmää pyrkiä vielä tarkentamaan.

Virka-apua koskevat ehdotukset

Lausunnonantajien näkemyksiä virka-apua koskevista ehdotuksista

Kannatamme viranomaisten välisen tiedonvaihdon parantamista ja tähän liittyvien virka-apun käyttömahdollisuuksien kehittämistä, mutta katsomme edellä yleisissä kommentteissa todetun mukaisesti, että se tulisi ulottaa myös keskeisten tieto- ja viestintätekniisten infrastruktuureiden toiminnasta sekä niihin liittyvien ja niitä hyödyntävien palveluiden tarjonnasta vastaaviin yksityisen sektorin toimijoihin. Ajatus siitä, että viranomaiset vaihtaisivat keskenään tietoa tai ryhtyisivät muihin toimenpiteisiin esim. tietoturvaloukkauksen johdosta ilman, että sen kohteeksi joutunut yritys saisi asiasta tietoa tai olisi mukana sen selvittämisessä, tuntuisi oudolta.

Erityisesti näin on siksi, että esityksen tavoitteena on pyrkiä poistamaan tietoturvaloukkauksen tai sen uhan vaikutuksia, mutta kuten esityksessäkin aivan oikein todetaan, ”Vaikutusten poistamisen osalta on kuitenkin huomioitava, että useassa tilanteessa vastuu vaikutusten poistamisesta on hyökkäyksen kohteeksi joutuneella toimijalla itsellään tai tämän palveluntarjoajalla.” Tässä suhteessa jääkin epäselväksi, miten viranomaisten tiedonvaihto edesauttaisi tätä tavoitetta, jonka kuitenkin todetaan olevan erityisesti toimijan itsensä vastuulla. Tältä osin esityksen perusteluja tulisi täsmentää.

Sähköisen viestinnän palveluista annetun lain 309 §:ssä tai muussa soveltuvassa säännöksessä tulisi myös määritellä virka-apua koskevassa harkinnassa käytettävät kriteerit, sillä niillä on suora yhteys siihen, minkälaisia tapauksia voidaan pitää merkittävänä ja seurauksiltaan vakavana tietoturvaloukkaustilanteina, ja jotka voivat siten laukaista oikeuden ehdotuksessa tarkoitettuun tiedonvaihtoon ja virka-apuun. On huomattava, että myös virka-aputilanteessa toisen viranomaisen henkilöstö saa tosiasiallisesti tietoa muutoin tiedonvaihtoa rajoittavien säännösten estämättä.

Säädökseen tulisiakin siten kirjata merkittävän ja seurauksiltaan vakavan tietoturvaloukkaustilanteen asiallisen soveltamisalan lisäksi tilanteen intensiivisyyttä ja merkittävyyttä koskevat kriteerit, kuten vaikutusten laajuus ja kesto, maantieteellinen levinneisyys sekä viestintäpalvelujen käytettävyys, eheys tai viestinnän luottamuksellisuus.

Lisäksi lakiin tulisi lisätä tarpeelliset säännökset yksityisen antamasta virka-apuun rinnastettavasta avustamisesta. Ehdotuksen sivulla 23 todetaan, että ”tietoturvan osalta korostuu myös henkilöstön osaaminen, mikä etenkin erityisissä teknistä osaamista vaativissa tapauksissa voi olla vain muutamilla henkilöillä Suomessa tai jopa koko maailmassa.” 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.

Tässä esimerkkinä voisivat olla esim. poliisilakiin sisältyvät säännökset avustamistyöstä, joiden tarkoituksena on mahdollistaa poikkeuksellisissa tilanteissa nopeasti tarkoitukseen sopivan ulkopuolisen avun käyttäminen. Tällöin säännösten avulla voitaisiin mahdollistaa Liikenne- ja viestintäviraston käyttää apunaan soveltuvaa henkilöä yksittäisessä havainnointi-, torjunta- ja selvittämistehtävissä, joihin ei sisälly merkittävää julkisen vallan käyttöä. Avustustyöhön osallistunut on oikeutettu saamaan valtion varoista työhön käytetyn ajan mukaan lasketun kohtuullisen palkkion. Avustustyöstä voidaan laatia sopimus joko henkilön tai soveltuvaa osaamista tarjoavan yrityksen kanssa.

Pidämme myös selvänä, että tiedonvaihtoa koskevat menettelyt on laadittava niin, että ne täyttävät soveltuvat tietoturvasääntö-, tietosuojaj- ja dokumentointivaatimukset, minkä lisäksi jatkuvalla seurannalla varmistetaan, että tietopyynnöt ja niihin annettavat vastaukset ovat muodollisesti ja sisällöllisesti asianmukaisia.

Ehdotuksessa todetaan, että media-ala on yksi kriittisen infrastruktuurin osa-alueista. Media-alalle puolestaan esimerkiksi lähdesuoja on erittäin keskeinen asia, mutta sitä ei ole tarkasteltu esityksessä ehdotettujen säännösten valossa. Pidämme erittäin tärkeänä, että jatkovalmistelussa asiaa pohdittaisiin myös lähdesuojavaatimusten kannalta ja lähdesuojan vaatimukset huomioitaisiin riittävässä määrin esityksessä.

Sikäli kuin tietoa vaihdetaan ulkomaisten viranomaisten kanssa, on varmistettava, että tiedonvaihto kaikissa tilanteissa tapahtuu soveltuvien säädösvaatimusten, yleisten tietosuojaperiaatteiden ja hyvien tietojenkäsittelykäytäntöjen mukaisesti.

Viranomaisten välinen tiedonvaihto

Lausunnonantajien näkemyksiä viranomaisten välistä tiedonvaihtoa koskevista ehdotuksista

Viittaamme soveltuvien osin edellä kohdassa Virka-apua koskevat ehdotukset toteamaamme.

Viestinnän välittäjän oikeus luovuttaa tietoja viesteistä ja välitystiedoista

Lausunnonantajan näkemyksiä viestinnän välittäjän oikeudesta luovuttaa tietoturvaloukkauksia koskevia tietoja Liikenne- ja viestintävirastolle

Esitetyn uuden 316 a §:n säännösteksti on suhteellisen lyhyt, mutta perusteluista on kuvattu pidemmältä. Säännöksen soveltamisalaan kuuluvien viestinnän välittäjien kannalta on keskeistä, että ne voivat luottaa toimivansa oikein niitä sitovan muun lainsäädännön ja asiakassopimuksia

koskevien vahingonkorvaussäännösten ja sopimulausekkeiden kannalta. Esitämme sen vuoksi, että perusteluista ilmenevät rajaukset sisällytettäisiin perusteluihin asemesta suoraan säännöstekstiin.

Mikäli tietoja näin saaduista viesteistä ja välitystiedoista edelleen luovutetaan ulkomaisille viranomaisille tai muille tahoille, on varmistettava, että tietojenluovutus kaikissa tilanteissa tapahtuu soveltuvien säädösvaatimusten, yleisten tietosuojaperiaatteiden ja hyvien tietojenkäsittelykäytäntöjen mukaisesti.

Muita havaintoja

Muita havaintoja ehdotuksen sisällöstä

-

Vaikutukset

Millaisia vaikutuksia ehdotuksella on lausunnonantajan toimialalla?

Esitettyjen säännösten vaikutukset tulisivat todennäköisesti eroamaan voimakkaasti riippuen siitä, mistä toimialasta on kyse. Osa toimialoista säännöksillä ei todennäköisesti tulisi olemaan merkittävää vaikutusta, mutta erityisesti telekommunikaatio- ja finanssisektoreilla sekä muillakin kriittisimmillä toimialoilla vaikutuksia olisi merkittävästi enemmän. Toisaalta nämä toimialat ovat jo nyt voimakkaasti säänneltyjä ja valvottuja toimialoja, joilla käsityksemme mukaan yhteistyö viranomaisten ja alan välillä on suhteellisen säännöllistä, kattavaa ja pääosin hyvin toimivaa. Pidämme tärkeänä, että viranomaisten ja yksityisen sektorin toimijoiden välisen, keskinäisen ja sisäisen tiedonvaihdon säännöt on määritelty kaikkialla selkeästi ja sen vuoksi katsomme, että lainsäädäntöhankeen todelliset hyödyt toteutuvat vasta, kun yksityisen sektorin toimijat kytketään tiiviimmin mukaan tietojenvaihtoon ja viranomaisyhteistyöhön. 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 kuitenkin kaikessa toiminnassa panostaa enemmän ennalta ehkäisyyn. 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.

Rajamäki Markku

Elinkeinoelämän keskusliitto EK - Lainsäädäntö ja hallinto