

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

FiComin pääviestit:

- Ehdotetut muutokset ovat lähtökohtaisesti kannatettavia ja perusteltuja.
- Luovutettaessa tietoja viranomaisten kesken, tulee näiden ilmoittaa luovutuksesta yritykselle, jonka tietoja on luovutettu.
- Viranomaisten tietojenluovutussäännöstöä tulee täydentää lisäyksellä, ettei luovutettua tietoa saa luovuttaa edelleen muille kuin pykälässä mainituille suomalaisille viranomaisille.
- Liikenne- ja viestintäviraston oikeudesta luovuttaa tietoja ulkomaiselle viranomaiselle koskevia edellytyksiä on tiukennettava huomattavasti (319 §).
- Esityksen jatkovalmistelussa tulee täydentää yritysvaikutusarviointia siitä, miten viranomaisten keskinäinen tiedonvaihto auttaa tietoturvaloukkauksen kohteeksi joutunutta yritystä.
- Ehdotetussa 319 a §:ssä ei ole 316 §:n 4 momentin mukaista tietojen hävittämistä koskevaa säännöstä ja velvoitetta, kun ne eivät enää ole tarpeen pykälässä tarkoitettujen tehtävien hoitamiseksi. FiCom ehdottaa, että tällainen tietojen hävittämissäännös lisätään esityksen jatkovalmistelussa.
- Sähköisen viestinnän palvelulaissa on runsaasti tietojen käsittely- ja luovutusedellytyksiä koskevia säännöksiä eri viranomaisille, eikä kokonaisuus ole enää selkeä. FiCom esittää, että käsittely- ja luovutusedellytyksistä tehdään lähiaikoina kokonaisarviointi.

1. Yleiset kommentit viranomaisten toimintamahdollisuuksista tietoturvaloukkauksien selvittämiseksi

Luonnos koskee viranomaisten yhteistoimintaa yhteiskunnan kriittisten toimintojen kannalta merkittävässä tietoturvaloukkaustilanteissa. Tavoitteena on luoda edellytykset viranomaisten tiedonvaihdolle ja virka-avulle vakavissa tietoturvaloukkaustilanteissa ja -uhkissa säätämällä loukkausten selvittämisen kannalta keskeisten viranomaisten keskinäisestä oikeudesta vaihtaa tietoturvaloukkauksen selvittämiseksi välttämättömiä tietoja. Keskeiset edellytykset jakaantuvat neljään osaan:

- 1) Viranomaisten (Liikenne- ja viestintävirasto, poliisi, suojelupoliisi ja Puolustusvoimat) tiedonvaihto-oikeuksien laajentaminen vakavissa tietoturvaloukkaustilanteissa tai uhkissa mukaan lukien henkilötietosääntely,
- 2) Liikenne- ja viestintäviraston mahdollisuus saada poliisilta, suojelupoliisilta ja puolustusvoimilta virka-apua,
- 3) viestinnän välittäjien oikeus oma-aloitteiseen tiedonluovutukseen Liikenne- ja viestintävirastolle viestien sisällön ja välitystietojen osalta sekä
- 4) päätöksentekomenettelyjen keventäminen Liikenne- ja viestintäviraston antaman virka-avun ja ulkomaille luovutettavan tiedon osalta.

FiCom pitää luonnosesityksen tavoitteita kannatettavina ja tarpeellisina. Luonnoksessa on kuitenkin muutamia kohtia, jotka kaipaavat selvennystä ja muuttamista esityksen jatkovalmistelussa.

Virka-apua koskevat ehdotukset

Lausunnonantajien näkemyksiä virka-apua koskevista ehdotuksista

2. Virka-apua koskevat ehdotukset

Ehdotus on kannatettava ja perusteltu.

Viranomaisten välinen tiedonvaihto

Lausunnonantajien näkemyksiä viranomaisten välistä tiedonvaihtoa koskevista ehdotuksista

3. Viranomaisten välinen tiedonvaihto

Ehdotus on pääosin kannatettava ja perusteltu. Tiedonvaihdon edellytykselle on asetettu ehdotetussa säännöksessä useita kriteereitä, kuten merkittävyys- ja välttämättömyyskriteerit. Lisäedellytyksiä ovat loukkauksen tai uhkan vakavat ja haitalliset vaikutukset kansalliseen turvallisuuteen, maanpuolustukseen, kansainvälisiin suhteisiin, julkisen vallan päätöksentekokykyyn, yhteiskunnan kriittiseen infrastruktuuriin taikka yleiseen järjestykseen ja turvallisuuteen. Esitys

näyttäisi täyttävän myös suhteellisuusperiaatteen edellytykset, sillä kyse on yksittäistapausta koskevasta tiedonvaihdosta, eikä esimerkiksi massaluovutuksista.

FiCom pitää hyvänä säännöksen 2 momentin tiedon käyttötarkoituksen täsmennystä, jossa luovutettuja tietoja saa käyttää vain tietoturvaloukkausten ja -uhkien selvittämiseksi, ennalta ehkäisemiseksi tai niiden vaikutusten poistamiseksi eikä tietoa ei saa käyttää muussa tarkoituksessa. Ehdotuksen mukaan sillä ei muodosteta viranomaisille varsinaista uutta tapaa hankkia tietoja muiden lakisääteisten tehtäviensä hoitamiseksi, vaan tietoa käytetään vain tietoturvaloukkausten selvittämisen yhteydessä.

Selvyyden vuoksi FiCom ehdottaa, että säännökseen lisätään, ettei luovutettua tietoa saa luovuttaa edelleen muille tahoille kuin pykälässä mainituille suomalaisille viranomaisille.

Lisäksi FiCom ehdottaa, että viranomaisten luovuttaessa tietoja toisilleen, tulee niiden ilmoittaa sille yritykselle, jonka tietoja on luovutettu, mitä tietoa ja milloin on luovutettu ja kenelle.

Ehdotetussa 319 a §:ssä ei ole 316 §:n 4 momentin mukaista tietojen hävittämistä koskevaa säännöstä ja velvoitetta, kun ne eivät enää ole tarpeen pykälässä tarkoitettujen tehtävien hoitamiseksi tai niitä koskevan rikosasian käsittelemiseksi. FiCom ehdottaa, että tällainen tietojen hävittämissäännös lisätään esityksen jatkovalmistelussa.

FiCom toteaa, että tiedonvaihtoa koskevat rajoitukset ovat perusteltuja erityisesti luottamuksellisen viestin ja yksityisyyden suojaan kohdistuvan perusoikeussuojan vuoksi. Pykälässä säädetyt edellytykset kokonaisuutena arvioiden luovat asianmukaiset lainsäädännölliset raamit ja riittävän korotetun tason mainituille oikeussuojille, jos siihen lisätään edellä mainitut edelleenluovutus- ja hävittämissäännökset.

Tietojen luovuttaminen ulkomaille

Luonnoksessa esitetään päätöksentekomenettelyn keventämistä ulkomaille luovutettavan tiedon osalta siten, että jatkossa asiasta päättäisi Liikenne- ja viestintävirasto ilman liikenne- ja viestintäministeriön myötävaikutusta tai päätöstä. Voimassa oleva laki (319 § 2 ja 3 mom) mahdollistaa muun muassa massaluovutuksen ja siitä puuttuvat merkittävyys-, vaikutus- ja välttämättömyyskriteerit, edelleenluovutuskielto sekä ehdoton käyttötarkoitus. Lisäksi luovutuksen kohde on siinä hyvin avoin. Säännöksestä puuttuvat kaikki ehdotetun 319 a §:n mukaiset edellytykset. Ei voi olla niin, että ulkomaiselle toimijalle voidaan luovuttaa tietoja huomattavasti kevyemmällä perusteilla kuin rajoitetulle joukolle kotimaisia viranomaisia.

Säännöksen 2 momentin mukaan Liikenne- ja viestintävirastolla on salassapitovelvollisuuden tai muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus luovuttaa

tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saamiaan välitystietoja ja muita tietoja muussa valtiossa toimivalle viranomaiselle tai muulle vastaavalle taholle, jonka tehtävänä on ennalta ehkäistä tai selvittää viestintäverkkoihin ja -palveluihin kohdistuvia tietoturvaloukkauksia.

Liikenne- ja viestintävirastolla on 3 momentin mukaan oikeus luovuttaa tietoja 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.

Sinänsä menettelyn keventäminen on ymmärrettävää, mutta luovuttamisen edellytykset ovat huomattavasti kevyempiä kuin nyt ehdotetussa 319 a §:ssä, jossa edellytyksinä ovat merkittävyys sekä vakavat ja haitalliset vaikutukset muun muassa kansalliseen turvallisuuteen. Esitystä tulee sen jatkovalmistelussa täydentää siihen suuntaan, että edellytykset ulkomaille luovutettavien tietojen osalta ovat vaativampia kuin kotimaisille viranomaisille luovutetuissa tiedoissa. Lähtökohtana tulee pitää ehdotetun 319 a §:n edellytyksiä kuten merkittävyyttä, vaikuttavuutta, välttämättömyyttä, suhteellisuutta ja käyttötarkoitusta.

Yrityksille on viestinnän luottamuksellisuuden takia tarpeen saada tietoa luovutuksista, joten liikenne- ja viestintäviraston tulee tehdä yhteistyötä niiden yritysten kanssa, joiden tietoja luovutetaan. Tämänkaltaisen säännös on poistettavaksi ehdotetussa 5 momentissa viraston ja liikenne- ja viestintäministeriön kesken. Liikenne- ja viestintäviraston tulee vähintäänkin ilmoittaa yritykselle, jonka tietoja on luovutettu, mitä tietoa ja milloin on luovutettu ja kenelle.

Viestinnän välittäjän oikeus luovuttaa tietoja viesteistä ja välitystiedoista

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

4. Viestinnän välittäjän oikeus luovuttaa tietoja viesteistä ja välitystiedoista

Ehdotus on kannatettava ja perusteltu, koska viestinnän välittäjä voisi vapaaehtoisesti ja oma-aloitteisesti luovuttaa tietoa Liikenne- ja viestintävirastolle tilanteissa, jossa se voi olla tarpeen tietoturvaloukkausten tai -uhkien selvittämiseksi taikka ennalta ehkäisemiseksi. Ehdotus koskee 272 §:n mukaisia tilanteita, jossa viestinnän välittäjällä ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus ryhtyä pykälän 2 momentissa tarkoitettuihin välttämättömiin toimiin tietoturvasta huolehtimiseksi.

Ehdotus on systematiikaltaan looginen 272 §:n kanssa: molemmissa tilanteissa on kysymys viestinnän välittäjän oikeudesta ryhtyä säännöksissä mainittuihin toimenpiteisiin eivätkä ne luo velvoitetta. Tämä vapaaehtoisuus on yksi keskeisimmistä soveltamiskeinoista eikä siitä saa tulla myöhemmin velvoittavaa. Jos yrityksillä ei tällä hetkellä ole menetelmiä ja keinoja ryhtyä

selvittämään 272 §:n mukaisia tilanteita ja tapauksia, ei näitä keinoja tule luoda nyt ehdotetun säännöksen toteuttamiseksi.

Toisaalta viestinnän välittäjä harkitessaan luovutuksen käyttöoikeuttaan joutuu arvioimaan, onko kyse 272 §:n mukaisista tilanteista. Luonnoksen mukaan tietojen luovuttamisessa olisi kyse tilanteesta, jossa viestinnän välittäjällä olisi jo valmiiksi laissa säädetty käsittelyperuste SVPL 272 §:n 1 momentin nojalla eikä kyse olisi uudesta oikeudesta käsitellä välitystietoja ja tietoja viesteistä. Luovuttajan kannalta ongelmaksi voi muodostua se, että tietojen luovuttaminen viranomaiselle voi nostaa luovutuskynnystä, koska tällöin viranomainen tutkii, onko 272 §:n käsittelyoikeus syntynyt. Tällainen kynnys saattaa olla enemmän pk-yritysten haaste.

Ehdotuksen mukaan pykälässä tarkoitetut tiedot viestin sisällöstä tarkoittaisivat lähtökohtaisesti sellaisia tietoja, jotka eivät olisi luottamuksellisen viestinnän kannalta merkityksellisiä, vaan lähinnä haittaohjelmia sisältäviä tai levittäviä, 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.

Toisaalta ehdotus voi paikata sääntelyssä olevan mahdollisen aukon tilanteissa, joissa kyse ei ole ilmoitusvelvollisuuden kynnyksen ylittävstä merkittävästä tietoturvaloukkaustilanteesta ja viestinnän välittäjä haluaisi tehdä ilmoituksen Kyberturvallisuuskeskukselle. Näissä ei-merkittävissä tilanteissa viestinnän välittäjä voi tarvita Kyberturvallisuuskeskuksen tukea havaitsemansa tietoturvaloukkauksen, kuten haittaohjelman toimintaperiaatteen selvittämiseen, sillä haasteita käytännössä on aiheuttanut näiden tietojen luovuttaminen Liikenne- ja viestintävirastolle.

Muita havaintoja

Muita havaintoja ehdotuksen sisällöstä

5. Muita havaintoja

FiCom haluaa 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.

Vaikutukset

Millaisia vaikutuksia ehdotuksella on lausunnonantajan toimialalla?

6. Vaikutukset

Luonnoksessa on pääasiassa keskitytty siihen, miten säännöksen mukainen tietojenvaihto auttaa viranomaisia tietoturvaloukkauksen tai -uhkan selvittämiseksi, ennalta ehkäisemiseksi tai vaikutusten poistamiseksi.

Luonnoksen yritysvaikutuksia koskevassa kohdassa on puolestaan todettu, että ehdotuksella arvioidaan olevan vaikutuksia yrityksiin lähinnä tilanteissa, joissa tietoturvauhkan realisoituminen mahdollisesti pystytään estämään tai tietoturvaloukkauksen vaikutukset poistamaan mahdollisimman nopeasti.

Loukkauksen estäminen on kaikille positiivista.

Hieman 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? Esitys kaipaa tältä osin täydentämistä jatkovalmistelussa.

Lahtinen Marko
Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry