18.1.2023

Eduskunta
Liikenne- ja viestintävaliokunta

Viite: HE 243/2022 vp, asiantuntijapyyntö

Lausunto: luonnos hallituksen esitykseksi sähköisen viestinnän palveluista annetun lain, henkilötietojen käsittelystä Puolustusvoimissa annetun lain ja henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta

Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys, joka edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Kiitämme mahdollisuudesta lausua asiasta. Lausunto on Teknologiateollisuuden ja Kyberalan yhteinen.

Hallituksen esitys koskee viranomaisten yhteistoimintaa yhteiskunnan kriittisten toimintojen kannalta merkittävissä tietoturvaloukkaustilanteissa. Esityksen taustalla on 10.6.2021 annettu valtioneuvoston periaatepäätös tietoturvan ja tietosuojan parantamiseksi yhteiskunnan kriittisillä toimialoilla, ja toimenpiteenä on luoda yhtenäinen säädöspohja viranomaisten yhteistyölle tietoturvaloukkaustilanteissa. *”Tarkoituksena oli arvioida lisäksi viranomaisten välistä tiedonvaihtoa sekä virka-apusäännöksiä ja* ***arvioida nykyisten toimivaksi todettujen yhteistyömenetelmien vahvistamista ja yhteistyötä yksityisen sektorin kanssa****. 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.”*

Näistä lähtökohdista haluamme kiinnittää huomiota seuraaviin kohtiin:

1. **Ehdotuksen tavoitteet**

Kannatamme esityksen tavoitteita ja katsomme, että toimijoiden välinen tiedonvaihto on tarpeen tietoturvaloukkauksien ehkäisemisessä, selvittämisessä ja mahdollisesti jossain määrin myös vaikutuksien poistamisessa. Yleisesti katsoen viranomaisilla tulisi olla soveltuvat keinot tukea tietoturvaloukkauksen kohdetta/kohteita vakavissa tietoturvaloukkaustilanteissa tai niiden selvästi uhatessa.

Vaikka nyt esitetyt keinot tarjoaisivat tehokkaamman viranomaistoiminnan kautta perusoikeutena parempaa omaisuuden suojaa, samalla ne kuitenkin heikentävät niin yritysten kuin kansalaistenkin yksityiselämää ja viestinnän luottamuksellisuutta koskevaa perusoikeuksien suojaa. Näin on, koska ehdotukseen on lausuntopalautteen perusteella tehty lisäyksiä, joista tarkemmin lisää kohdassa 3. Muutoinkaan ehdotetut toimet eivät ole riittäviä, erityisesti kun tavoitellaan vakavien tietoturvaloukkausten ja -uhkien ennalta ehkäisemistä sekä haitallisten vaikutusten poistamista.

Ehdotus keskittyykin tosiasiassa erityisesti vakavien tietoturvaloukkausten selvittämiseen eli tutkintaan, ja vaikkakin merkityksellinen tavoite, sitä ei kuitenkaan voida pitää yhteiskunnan toiminnan kannalta keskeisimpänä toimena. Kuten

Eteläranta 10, PL 10, 00131 Helsinki

selvityksessä todetaan, ”*esityksessä ehdotetaan parannettavan viranomaisten yhteistoiminnan mahdollisuuksia tiedonvaihtoa tehostamalla*”. Muistutamme, että valtaosa yhteiskunnan toiminnan kannalta elintärkeän tieto- ja viestintäteknisen infrastruktuurin toiminnasta sekä siihen liittyvien ja sitä hyödyntävien palveluiden tarjonnasta on yksityisen sektorin vastuulla. Toisin sanoen yhteiskunnan keskeiset toiminnot ovat valtaosin yksityisten toimijoiden vastuulla (kuten ruoka- ja energiatuotanto, logistiikka, rahoitus, teollisuus ja ICT). Näin ollen yhteiskunnan toiminnan kannalta keskeiseksi katsottujen yritysten (järjestelmiensä omistajina ja haltijoina) vaikuttavimmista toimista tietoturvaloukkausten ehkäisemisessä ja vaikutusten poistamisissa vastaavat edelleen yritykset. Lisäksi on selvää, että todennäköisimmin vakavan tietoturvaloukkauksen kohteena on yksityinen toimija, kuten Suomesta ja ulkomailta kertyneet tilastot kiistatta osoittavat. Myös tietoturvaloukkausten teknisten syiden selvittämistä voidaan hankkia palveluna kotimaisilta markkinoilta, sillä Suomessa on maailman parhaita asiaan perehtyneitä toimijoita. **Ehdotetut säädösmuutokset välittävät osin virheellistä kuvaa, että viranomaistoiminnalla, eritoten tiedonvaihdolla, voitaisiin olennaisesti vaikuttaa yksityisten hallinnassa olevien järjestelmien tietoturvallisuuteen. Ylivoimainen osa Suomessa olevista järjestelmistä on yksityisten hallinnassa.**

2. **319 a § Tietojen luovuttaminen merkittävässä tietoturvaloukkauksessa tai -uhkassa**

Esityksessä ei ole kyse poikkeusolojen lainsäädännöstä, vaan sillä luodaan viranomaisille poikkeustilanteissa käytettäväksi valtuuksia, joihin viranomaisilla ei normaaliaikoina tarkoitettu olevan mahdollisuutta.

Esityksessä todetaan, että ”*vakavissa tietoturvauhkissa tehtävä yhteistyö on suorassa yhteydessä rikostentorjuntaan*” ja että ”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.

Ensinnäkin niiltä osin, kun tietoja luovutettaisiin esitukintaviranomaiselle (poliisi ja Puolustusvoimat) olisi siis kyse aina tiedoista, jonka perusteella esitutkintaviranomaisen tulee esitutkintalain 3:1 §:n mukaisesti kirjata rikosilmoitus ja 3:3 §:n mukaisesti toimitettava rikosperustainen esitutkinta, kun sille tehdyn ilmoituksen perusteella tai muuten on syytä epäillä, että rikos on tehty. Asiassa on otettava huomioon lisäksi, että osa mainituista rikoksista on ns. asianomistajarikoksia, jolloin tietoturvaloukkauksen kohteena olevalla asianomistajalla on ollut alun perinkin oikeus pidättäytyä ilmoittamasta tekoa syytteeseen pantavaksi. Ehdotuksessa kuitenkin ehdotetaan, että asianomistajalla ei olisikaan käytännössä oikeutta olla saattamatta tapahtumaa esitutkintaan, kun tieto välittyisikin toisen viranomaisen kautta esitutkintaviranomaiselle, pahimmassa tapauksessa asianomistajan tietämättä. Asiaa ei ole käsitelty ehdotuksessa miltään osin.

Toiseksi SVPL 319 a §:n ehdotettu muotoilu synnyttää ns. kehäpäätelmän, jossa ensin luetellaan yhteiskunnan keskeiset toiminnot, mukaan lukien ”*julkisen vallan päätöksentekokokyky tai viranomaisten toimintaedellytykset; sekä kansallinen turvallisuus tai maanpuolustus*” (1 mom. kohdat 1–2). Tämän jälkeen 2-momentissa säädetään tarkemmin käyttötarkoituksesta: ”*luovutettua tietoa saa käyttää vain*

tietoturvaloukkauksen tai sen vakavan uhkan selvittämiseksi tai ennalta ehkäisemiseksi taikka niiden vaikutusten poistamiseksi. Tietoa ei saa käyttää muussa tarkoituksessa."

Kun tietoja käsitellään merkittävän tietoturvaloukkauksen tai sen vakavan uhkan selvittämiseksi, ennalta ehkäisemiseksi tai vaikutusten poistamiseksi, jolla on tai uhkaa olla vakavia haitallisia vaikutuksia on tiedonvaihdossa kyse tapahtumaa koskevasta tutkinnasta tai Poliisilain 5a-luvun 1 §:n mukaisesti selvästi tiedustelulakien soveltamisalaan ulottuvasta toiminnasta ja siten myös perustuslain 10 § koskevan muutoksen edellytyksiä mm. kansallisen turvallisuuden käsitteen osalta. Näin ollen tiedustelulakien yhteydessä edellytetyt periaatteet, rajoitukset sekä muut vaatimukset, mukaan lukien ns. palomuurisääntely tulee ottaa kattavasti huomioon.

Kolmanneksi ehdotus muodostaa ilmeisen riskin, että hiljattain selonteon kohteena olleita tiedustelulakeja kierrettäisiin erityisesti tietoturvaloukkausten vakavaa uhkaa koskevassa tietojenvaihdossa mm. tuomioistuinvalvontaa sekä palomuurisääntelyä koskevilta osin. Eduskunnan oikeusasiamies on huomauttanut hiljattain rikostorjunnasta Puolustusvoimissa annetun lain muutosesityksen yhteydessä[1], että "*kehityksen tulisi kulkea siihen suuntaan, että rikostorjunta kuuluisi poliisille ja tiedustelutoimivaltuuksia käyttävä viranomainen ei osallistuisi rikostorjuntaan eikä sillä siten olisi sen enempää rikosten estämis- ja paljastamistehtäviä kuin selvittämistehtäviä. Tämä koskee niin Puolustusvoimia kuin Suojelupoliisia*".

Neljänneksi ehdotuksen säännöskohtaisissa perusteluissa korostetaan tietojen luovuttamisen lisäedellytyksenä, että tietoturvaloukkauksen vaikutukset kohdistuisivat pykälässä lueteltuihin yhteiskunnan toiminnan kannalta elintärkeisiin toimintoihin. Perusteluissa jatketaan, että säännöksellä katettaisiin myös tilanteet, joihin liittyy valtiollinen toimija tai vahva epäilys valtiollisesta toimijasta. Ehdotus kattaisi myös tilanteet, joissa valtiollinen toimija käyttää tai sen voidaan perustellusti epäillä käyttävän ohjauksessaan ei-valtiollista toimijaa tavoitteidensa saavuttamiseksi.

Säännöksen ei tule johtaa tilanteeseen, jossa valtiollisen toimijan epäiltyä tai edes todettua "läsnäoloa" tulkittaisiin kategorisesti merkittäväksi tietoturvaloukkaukseksi tai sellaisen vakavaksi uhaksi. On syytä huomioida, että valtiollisen toimijan läsnäoloon viittaavia tietoja Suomessa tapahtuvista tietoturvaloukkauksista ilmenee päivittäin. Koska kyse on myös tiedustelulainsäädäntöä koskevien säännösten ja periaatteiden alueelle ulottuvasta toiminnasta, ja toisin kuin ehdotuksessa väitetään, tiedustelulainsäädännön tavoite, eli tiedonhankinta kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvista uhista, on merkittäviltä osin yhtenevä ehdotuksen tavoitteen eli tietoturvaloukkausten selvittämisen, ennalta ehkäisemisen ja vaikutusten poistamisen kanssa.

Liikenne- ja viestintävaliokunta on tiedustelulakien arvioinnin yhteydessä pitänyt keskeisenä, että yksityisyyden suoja ja luottamuksellisen viestin suoja toteutuvat asianmukaisesti[2]. Kyberala on kehottanut tarkentamaan ehdotusta jo lausuntopalautteen aikana, mutta asiaa ei ole tarpeellisilta osin huomioitu. **Tiedonvaihdon rajaus tuleekin selkeyttää**, sillä sekä rikollisten että valtiollisten toimijoiden (suoraan tai ohjauksen kautta) toimintatavat, teknologiset työkalut sekä infrastruktuuri ovat hyvin pitkälle samanlaisia, tai jopa täysin samoja, jolloin on ilmeinen

[1] Asia VN/3229/2019, lausunto EOAK/3938/2022, 19.08.2022.
[2] LiVL 13/2022 vp– VNS 11/2021 vp

riski, että suurta osaa rikollisesta toiminnasta voidaan pitää myös ”valtiollisena” toimintana ja siten kiertää tiedonvaihdon rajoituksia.

3. **Puolustusvoimien tehtävät ja toimivalta**

Ehdotuksessa Puolustusvoimien osalta on todettu, että ”*Puolustusvoimat voi antaa virka-apua silloin kun yhteiskunnan turvaaminen edellyttäisi sellaista henkilöstöä, materiaalia ja osaamista, mitä Puolustusvoimilla on.*” Laki Puolustusvoimista on kuitenkin yksiselitteinen: tietoturvaloukkausten näkökulmasta Puolustusvoimien tehtävä on Suomen sotilaallinen puolustaminen eli sotilaan henkilökohtaisen **aseen ja sitä voimakkaamman asevoiman käyttöä** sekä **virka-avun antaminen** muille viranomaisille (esim. hengelle tai terveydelle vakavaa vaaraa aiheuttavien rikosten estämiseksi ja keskeyttämiseksi).

Puolustusvoimien tehtävänä ei siten ole itse kehittää julkisilla varoilla kykyjä digitaalisen infrastuktuurin ”turvaamiseen” yleisesti tai muutoinkaan poikkeusoloihin liittymättömästi, eikä siten ryhtyä hoitamaan Traficomin tai sisäministeriön alaisille virastoille kuuluvia tehtäviä vakavan tietoturvaloukkauksen (eli vakavan rikoksen) torjuntaan liittyen. Ehdotuksessa todetaan, että ”*käytännössä merkittävissä tietoturvaloukkaustilanteissa jokin tieto- tai viestintärikoksen taikka esimerkiksi vakoilurikosten tunnusmerkistö täyttyisi.*” On huomioitava, että Puolustusvoimat ei myöskään ole yleinen esitutkintaviranomainen eikä tätä oikeustilaa ole ehdotettu muutettavaksi.

Puolustusvoimien määrärahojen käytön osittainen läpinäkymättömyys, julkisuusperiaatteen laajamittainen toteutumattomuus, perustuslain 10 § ja 22 § sekä Perustuslakivaliokunnan asettamat ”kansallisen turvallisuuden” täsmällisyyden ja tarkkarajaisuuden vaatimukset edellyttävät **tietojen jakamisen rajoittamista yksinomaan tilanteisiin, joissa merkittävä tietoturvaloukkaus aiheuttaa tai uhkaa aiheuttaa vakavia haitallisia vaikutuksia maanpuolustukselle. Näin ollen ehdotettua SVPL 319 a § (1 mom. 2-kohta) tulee muuttaa niin, että tietojen luovuttaminen Puolustusvoimille on mahdollista vain, kun kyse on vakavista haitallisista vaikutuksista maanpuolustukseen.**

Suomen vallitsevan yhteiskuntajärjestyksen mukaisesti elinkeinoelämän on voitava luottaa siihen, että vuosikymmenten aikana huolellisesti rakennetun viranomaisvastuiden selkeyden ja viranomaistoiminnan korkean luottamuksen säilyttämiseksi **puolustushallinnon tehtävänä säilyy yksinomaan yhteiskunnan sotilaallinen puolustaminen**. On syytä huomioida, että vakaviakaan tietoturvaloukkauksia ei ole koskaan pidetty sotilaallista eli aseellista puolustusta edellyttävänä uhkana. Puolustusvoimilla ei ole itsenäistä toimivaltaa vakavien tietoturvaloukkauksien ehkäisemisessä, selvittämisessä eikä vaikutuksien poistamisessa sen ulkopuolella, mikä koskee sotilaallisen puolustuksen järjestelmiä. Näin ollen Puolustusvoimien oikeutta vastaanottaa ja käsitellä tietoa ”vastatessaan Suomen sotilaallisesta kyberpuolustuksesta osana kansallista kyberturvallisuutta ja sen lakisääteisiä tehtäviä” jää perustelematta ja kyseenalaiseksi.

Vastaavasti SVPL 319 § 2 mom. 2-kohdassa Traficomin oikeus luovuttaa tietoa Pohjois-Atlantin liiton (NATO) toimielimelle, elimelle tai virastolle ei tule hyväksyä, sillä tiedon luovuttaminen johtaisi sen laajamittaiseen leviämiseen 30 valtion käyttöön, joista osan ei voida katsoa täyttävän demokraattisen hallinnon, kansainvälisten ihmis- ja

perusoikeuksien vähimmäisvaatimuksia ja luovutus rikkoisi myös niitä olennaisia takeita, joita EU:n tuomioistuin on ratkaisukäytännössään (mm. Schrems II[3]) asettanut henkilötietojen luovuttamiselle kolmansiin maihin[4]. Euroopan tietosuojaneuvosto tiivistää sovellettavat oikeudelliset vaatimukset, joilla voidaan oikeuttaa perusoikeuskirjassa tunnustettujen tietosuojaa ja yksityisyyttä koskevien oikeuksien rajotukset seuraavasti:

- käsittelyn täytyy perustua selviin, täsmällisiin ja avoimiin sääntöihin
- käsittelyn oikeutettujen tavoitteiden tarpeellisuus ja oikeasuhteisuus on osoitettava
- käytössä on oltava riippumaton valvontamekanismi
- henkilöiden käytettävissä on oltava tehokkaita oikeussuojakeinoja.

Ehdotuksessa ei ole esitetty mitään sellaista perustetta, jonka perusteella tiedon jakaminen tietosuojan ja yksityisyyden olennaisten takeiden, perusoikeuksien yleisten rajoitusedellytysten, perustuslain 10 §:n 4 momentin sekä perustuslakivaliokunnan lausuntokäytännön[5] mukaan olisi välttämätöntä. Myöskään valvonta- ja oikeussuojakeinoja ei käsitellä. Mikäli Suomella olisi tulevaisuudessa NATOn jäsenvaltiona tarve tukeutua NATOn peruskirjan ns. kollektiivisen puolustuksen artiklaan – sen lisäksi, että se on toissijainen kansalliseen puolustusvelvoitteeseen nähden – tulee Suomen ilmaista kyseinen kollektiivisen puolustuksen tarve kansallisen poliittisen päätöksenteon perusteella, eikä siten ole tarvetta etukäteisesti luovuttaa tietoja liittokunnan jäsenvaltioiden käyttöön.

Näin ollen ehdotus hämärtäisi edelleen puolustusliiton perustamisasiakirjan 3-artiklassa määrättyä kansallisen puolustusvastuun ensisijaisuutta. Säännös sekä sen perustelut jättävät epäselväksi myös sen, luovutettaisiinko tieto myös Puolustusvoimille suoraan ja erikseen vai puolustusliiton kautta, ja olisivatko luovuttamisen edellytykset eriävät, mikäli tieto luovutettaisiin vain Puolustusvoimille. **Näin ollen ehdotuksesta tulee poistaa oikeus luovuttaa tietoturvaloukkauksia koskevan tiedonkeruun ja selvittämisen yhteydessä saatuja tietoja NATOn rakenteille.**

4. **Virka-apua koskevat ehdotukset: yksityisen avunanto ja tieturvaloukkausten yhteisilmoitus useammalle toimivaltaiselle viranomaiselle kerralla:**

Kyberala on ehdotuksen valmistelussa esittänyt kahta ehdotuksen tavoitteita tehokkaammin toteuttavia keinoa, joista toinen sisältyykin jo EU:n kyberpuolustusta koskevaan politiikkaehdotukseen ja toinen ratkaisisi merkittäviltä osin perusoikeussuojaan liittyviä ongelmia olemassa olevan oikeusperustan (julkisuuslaki 26 § sekä EU:n perusoikeuskirja artikla 8) avulla:

- **Lakiin tulisi lisätä tarpeelliset säännökset yksityisen antamasta virka-apuun rinnastettavasta avustamisesta**

[3] Unionin tuomioistuimen tuomio, annettu 16. heinäkuuta 2020, Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems, asia C-311/18, ECLI:EU:C:2020:559.
[4] Myös 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).
[5] Perustuslakivaliokunnan tulkintakäytännön mukaan tiedon luovuttaminen on sidottu välttämättömyyskriteeriin (PeVL 35/2018 vp, s. 26). 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).

Ehdotusta on kuitenkin käsitelty ehdotuksessa todeten: ”*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 tieto-turvaloukkauksiin liittyvää yhteistyötä pohditaan laajemmin*.”

- **Ns. yhden luukun periaatteen eri ilmoitusvelvollisuuksiin ja -oikeuksiin liittyen**[6]
  Ehdotuksessa todetaan: ”*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*.”

Vaikka palaute onkin annettu tiedoksi toiseen selvitystyöhön, jatkovalmistelun tavoitteista, rajauksista tai työstä ylipäätään ei ole saatavissa tietoa, jonka perusteella voitaisiin olettaa, että ehdotukset käsiteltäisiin lakiehdotukseen johtavalla tavalla. **Näin ollen asiat tulisikin käsitellä nimenomaan tässä lakiehdotuksessa.**

Lisätiedot:

Toimitusjohtaja Peter Sund
sähköposti: peter.sund@teknlogiateollisuus.fi
puhelin: 050 565 0621

[6] Mm. ehdotuksen sisältyvä viestinnän välittäjän oikeus luovuttaa tietoja liikenne- ja viestintävirastolle, rikosilmoitus, tietosuojailmoitukset, NIS- ja rahoitusmarkkinaperustaiset ilmoitukset jne.