Hallintovaliokunta

HE 243/2022 vp

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

Keskusrikospoliisin lausunto

Hallintovaliokunta on pyytänyt Keskusrikospoliisilta lisäselvitystä liittyen tiedonvaihdon kynnykseen ja virka-apuun liittyen. Keskusrikospoliisi on lausunnossaan kuvannut esimerkinomaisesti tilanteita, joissa kynnys tiedonvaihdolle ja virka-avulle ei toteudu. Valiokunta on pyytänyt esimerkinomaisesti tarkentamaan, minkälaiset tapaukset jäävät kynnyksen alle ja minkälaiset tapaukset ylittäisivät KRP:n arvion mukaan kynnyksen.

Taustaksi

Ehdotuksessa HE 243/2022 vp tuodaan esille tarve kattavaan tilannekuvaan kyberuhkien ennakoimiseksi ja poikkeamien havaitsemiseksi mahdollisimman aikaisessa vaiheessa. Tiedonvaihdolle asetettu korkea kynnys ei tässä mielessä tue aikaista reagointia ja vahinkojen ja vaikutusten estämistä sekä tapausten selvittämistä. Ehdotuksen kattamien yhteiskunnan elintärkeiden toimintoihin kohdistuvien tietoturvaloukkausten ja uhkien vakavuuden alapuolelle jää joukko edelleen erittäin vakavaksi katsottuja rikoksia, joissa yksikön tai yritystoiminnan kannalta on vahva selvittämisintressi ja vahinkojen estämisintressi. Tapausten jälkikäteinen selvittäminen on erittäin haastavaa eikä tällä selvittämisellä joka tapauksessa voida vaikuttaa kansalaisille tai yrityksille jo aiheutuneisiin merkittäviin vahinkoihin.

Virka-avun tarve ja tapaukset

Virka-avun tilanteita on ehdotuksessa luonnehdittu tilanteiksi, joissa intressi tietoturvaloukkauksen selvittämiselle ja torjumiselle on korkeampi kuin tavanomaisissa tietoturvaloukkaustilanteissa. Poliisin tutkimien tapausten osalta kysymys olisi joko taloudellisilta vaikutuksiltaan tai kohteena olevan henkilöjoukon laajuuden vuoksi merkittävistä tapauksista. Maantieteellisesti vaikutuksiltaan tapaukset voisivat olla alueellisia tai valtakunnallisia.

Kysymys voi olla tilanteesta, jossa aikaisessa vaiheessa havaitaan tunnistettuun haavoittuvuuteen liittyvä tai leviämässä oleva uusi hyökkäystapa, osa tietoturvaloukkauksista on jo realisoitunut ja havaitaan, että potentiaalisia hyökkäyksen kohteita, tai kohteita, joihin on jo yritetty hyökätä, siinä vielä onnistumatta on paljon.

Käytännössä tapaukset voivat olla kiristyshaittaohjelmatapauksia, koskea suomalaista kansainvälistä liiketoimintaa harjoittavaa pörssiyhtiötä ja ajaa alas sen operatiivisen toiminnan, tehtaat ja tuotannon. Tapaukset voivat olla myös isoihin tai pienempiin korkean teknologian yrityksiin kohdistuvia tietomurtoja, joissa tietomurron motiivina voi olla yritysvakoilu tai kaupankäynti saavutetuilla tiedoilla. Toisaalta tapauksella voi olla vaikutuksia jopa kymmenien tuhansien kansalaisten päivittäiseen elämään, vaikka kyse ei kuitenkaan ole 319 a § 1 momentin 1 – 7 -kohdan mukaisesta toiminnasta tai toimialasta, esimerkiksi välttämättömästä terveydenhuollon palveluista. Kysymys voi olla myös kuntien palveluihin ja järjestelmiin kohdistuvasta hyökkäyksestä, jotka voivat olla vaikutuksiltaan ja alueellisesti rajatumpia. Joissakin tilanteessa esiin voi tulla seikkoja, joiden nojalla on syytä epäillä, että tapauksen taustalla on valtiollinen toimija, joka muuttaa tapauksen luonnetta tekijään motiivin vuoksi yhteiskunnallisesti merkittävämpään suuntaan.

Pitkittyessään tapaukset voisivat vaikuttaa myös yhteiskunnan toimintaan, mutta näin ei ensivaiheessa olisi. Tapaus voisi muuttua tai osoittautua laajetessaan myös 319 a § mukaiseksi tilanteeksi. Parhaimmillaan virka-avulla ja tehokkaalla viranomaisyhteistyöllä voidaan vaikuttaa siihen, että tapaus ei pääse leviämään vaikutuksiltaan yhteiskunnallisesti merkittäväksi, jollaisesta tilanteesta 319 a § on kysymys. Käynnistämällä myös rikostorjuntatoimet varhaisessa vaiheessa poliisin pakkokeinoilla tai poliisilain mukaisilla toimivaltuuksilla voitaisiin asiaa selvittää, toimintaan puuttuu ja sen vaikutuksia estää laajemmin, kuin hallinnollisilla toimivaltuuksilla.

Virka-apua viranomaisten välillä tarvitaan, koska kyberympäristön monimutkaisuuden ja jatkuvasti kehittyvien tekotapojen vuoksi viranomaisille on mahdotonta varautua ja ylläpitää erityisosaamista, laitteita tai o-jelmistoja, joilla voidaan reagoida kattavasti erilaisiin uhkiin ja tietoturva-loukkauksiin. Toisella viranomaisella voi olla käytössää teknistä laitteistoja tai ohjelmistoja tai erikoiskoulutettua henkilöstöä, joita juuri kyseisen tapauksen selvittämisessä nimenomaisesti tarvitaan. Tapauksen analysoimisessa tarvitaan välttämättä yksilöivää tietoliikennetietoa.

Miksi tunnistetietoja, sijaintitietoja ja sisältötietoja tulee voida luovuttaa virka-avun tilanteissa

Hyökkäyksen torjuminen, sen vahinkojen ja vaikutusten estäminen sekä tapauksen rikosoikeudellinen selvittäminen edellyttävät hyökkääjän, hänen menetelmiensä, käyttämänsä infrastruktuurin sekä hyökkäyksen motiivien

selvittämistä. Tapauksen selvittäminen edellyttää sekä teknistä attribuutiota eli tapauksen teknisten yksityiskohtien ja mahdollisen hyökkääjän laiteympäristön teknistä tunnistamista, että rikosoikeudellista attribuutiota, joka on teknistä selvittämistä laajempi käsite ja kattaa myös tekijän henkilöllisyyden, tahallisuuden ja motiivien selvittämistä (esimerkiksi taloudellisen hyödyn tavoittelu, vahingon aiheuttaminen, yhteiskunnan toimintaedellytyksiin vaikuttaminen). Tapausten tekninen attribuutio on ensi sijassa Liikenne – ja viestintäviraston mielenkiinnon kohteena, kun taas rikosoikeudellinen attribuutio on teknisen attribuution ohella poliisin tehtävänä.

Olennainen osa selvittämistä ja tapauksen ensivaiheen tilanneanalyysiä on tekninen attribuutio eli tiedot hyökkäysliikenteen laadusta eli siitä mistä laitteista hyökkäysliikenne tulee, kuinka voimakasta toiminta on, miten kohdeorganisaatiota on lähestytty sekä millaista ohjelmistoa ja infrastruktuuria hyökkäyksen toteuttamisessa on mahdollisesti käytetty. Teknisellä attribuutiolla on merkitystä tekijän motiivien ja henkilöllisyyden selvittämisessä tietoturvauhan tai loukkauksen vaikutusten poistamisen lisäksi. Yksilöivillä tiedoilla voidaan edelleen kohdentaa poliisin tiedonhankintaa kotimaassa tai hankkia tietoa toisilta valtiolta. Tapauksesta yleisellä tasolla keskustelu ei mahdollista teknistä tai rikosoikeudelliseen vastuuseen johtavaa attribuutiota.

Keskusrikospoliisi on ehdottanut, että tietojen luovuttaminen tunnistetietojen/välitystietojen, sijaintitietojen ja sisältötietojen osalta mahdollistettaisiin näissä tilanteissa. Tavanomaisesti selvittämisessä voi olla tarve käsitellä käyttäjätietoja sekä välitystietoja ja sijaintitietoja ja enemminkin kyse on laitteiden välisestä signalointiliikenteestä kuin yksityishenkilöiden välisestä luottamuksellista viestinnästä ja sen sisällöstä.

Erityisesti tunnistetiedoilla/välitystiedoilla ja sijaintitiedoilla on asian selvittämisen kannalta keskeinen merkitys. Tekijän tunnistamiseksi myös sisältötiedot ovat tärkeitä, mutta eivät ensisijaisia tietoja. Ensin mainittujen tietojen hankkiminen edellyttäisi poliisilta joiltakin osin televalvontalupaa. Sisältötietojen hankkiminen edellyttää telekuuntelu tai tietojen hankinta telekuuntelun sijaan toimivaltuuden käyttämistä. Huomionarvoista kuitenkin on, että televalvonnan osalta tietojen hankkimiskynnys on asetettu siten, että televalvonta on mahdollista tapauksissa, joissa on kyse teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Tyypillisesti kyse voi olla juuri näistä rikoksista.

Tavanomaisesti kysymys on seuraavista rikoksista tai niiden törkeistä tekomuodoista; Rikoslain 38-luvun osalta viestintäsalaisuuden loukkaus (3 ja 4 §), tietoliikenteen häirintä (5 ja 6 §), tietojärjestelmän häirintä (7 a ja 7 b §) ja tietomurto (8 ja 8 a §) sekä datavahingonteko (35 luku 3 a ja 3 b §), törkeästä kiristys (31 luku 3 ja 4§) §), vakoilu (12 luku 5 ja 6 §) tai yritysvakoilu

(30 luku 4 §).

Keskusrikospoliisi on myös ehdottanut, että tietojen luovuttaminen rajataan vain asian selvittämisen kannalta välttämättömiin tietoihin ja vastaavalla tavalla kuin 319 § 3 momentissa on säädetty muiden luovutuksen kohteiden, kuten ulkomaisten viranomaisten osalta, luovuttaminen olisi rajattava siten, että tietojen luovuttamisella ei rajoiteta luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Miksi poliisi ei hanki itse näitä tietoja omilla toimivaltuuksillaan?

Osin kysymys voi olla tiedoista, jotka eivät ensinkään kuulu televalvonnan tai telekuuntelun alaan eli tiedot voi olla hankittu tietoturvaloukkauksen kohteena olleelta yritykseltä itseltään, joka on ollut viestinnän, esimerkiksi hyökkäysliikenteen, osapuolena (Laki sähköisen viestinnän palveluista 136 § 1 momentti) tai tiedot on hankittu ulkomailta Liikenne – ja viestintäviraston vastaavilta yksilöiltä. Poliisi koskevat toimivaltuudet (televalvonta, telekuuntelu) koskevat tietojen hankkimista teleyrityksiltä, yhteisötilaajilta tai muilta viestinnän välittäjiltä. Lisäksi tiedot voivat olla sellaisia, ettei niitä voitaisi kohdennetusti poliisin toimivaltuuksilla hankkia (esimerkiksi Havaro tiedot).

Tieto voi siis olla kohdeyritykseltä saatua, ulkomailta saatua tietoa, Ha-varo järjestelmän kautta saatua mutta myös Liikenne – ja viestintäviraston omilla toimivaltuuksillaan teleyritykseltä saatua tietoa. Sen lisäksi, että tietojen hankkimisen ei edes kuulu pakkokeinojen piirin (kohdeyritykseltä itseltään saatu tieto, on viestinnän osapuolena), niiden hankkiminen voi olla tietolähteistä johtuen mahdotonta (Havaro-tieto, ulkomailta saatu tieto) tai aiheuttaa ajallisesti merkittävää viivettä (ulkomailta saadun tiedon selvittäminen oikeusaputeitse tai EIO menettelyssä).

Millaiset tapaukset voivat jäädä 319 a § soveltamiskynnyksen alapuolelle ja millaisissa tapauksissa kynnys ylittyisi?

Keskusrikospoliisi korostaa, että ehdotettu 319 a § on tärkeä edistysaskel viranomaisyhteistyön tiivistämisessä. Tärkeää kuitenkin on, ettei konkreettinen yhteistyö ja tiedonvaihto mahdollistu vain näiden 319 a §:n mukaisten tapausten osalta, kuten edellä on kuvattu. Keskusrikospoliisi on tuonut lausunnossaan esiin, että haasteeksi jää 319 a §:n osalta se, että jotta tilanne voitaisiin tunnistaa riittävän laajamittaiseksi ja vakavaksi, sen vaikutusten tulisi olla jo laajahkolle levinneitä ja suhteellisen täsmällisesti tunnistettuja. Vakavien tietoturvaloukkausten selvittelyn alkuvaiheissa tällaista täsmällistä tietoa ei ole välttämättä saatavilla ja tilannekuva täsmentyy asian selvittämisen edetessä.

Käytännössä 319 a § pykälän soveltaminen edellyttää tapauksen liittyvän 1 – 7 alakohdissa tarkoitettuihin toimintoihin ja palveluihin, lisäksi arviointia kyseisen sektorin sisällä palvelun välttämättömyydestä ja edelleen päättelyä vaikutusten laajuudesta. Perusteluissa nimittäin todetaan, että merkittävän tietoturvaloukkauksen tai sen uhkan vaikutukset tulee kohdistua yhteiskunnan kannalta elintärkeisiin toimintoihin ja niihin liittyviin tietoaineistoihin. Perusteluilla on hieman nostettu soveltamiskynnystä siitä, mitä varsinaisen pykälän sanamuodon perusteella voi päätellä.

Käytännössä arvioitavaksi voi tulla onko alueellisesti rajattu tapaus riittävän vakava (esimerkiksi kuntiin kohdistuvat hyökkäykset tai esimerkiksi jonkin liikenteenohjausjärjestelmän alueellisen osan lamaantuminen) vai edellytetäänkö, että tapauksella olisi valtakunnallisia vaikutuksia. Onko merkitystä kunnan osalta sillä, millaisiin palveluihin viranomaisten toimintaedellytyksiin vaikuttava hyökkäys kohdistuu (viime aikaisissa tapauksissa kohteen olleet esimerkiksi oppilaitokset, terveydenhuoltoalan palvelut).

Voiko yksittäiseen kaupalliseen yritykseen kohdistuva tietoturvaloukkaus, joka aiheuttaa mittavaa taloudellisesta vahinkoa (esimerkiksi maa-ilmanlaajuinen maatalouskoneiden tuottaja ja jakelija, jolla on yli tuhat työntekijää mutta yrityksen toimiala ei ole olla luettelokohtien 1) – 7) mukainen) olla yhteiskunnan elintärkeisiin toimintoihin kohdistuva, pitääkö ja voidaanko päätellä, että sen tuotteilla ja palveluilla on merkitystä elintarvikeketjun osana tai ainakin kyse voi olla välttämättömästä hyödykkeestä. Kuinka välillisiä ja välittömiä vaikutuksia voidaan ja tulee arvioida.

Miten arvioidaan tapaukset, jotka kohdistuvat mittavaan määrään kansalaisia, esimerkiksi tietomurron kohteen kymmenien tuhansien henkilöiden henkilötiedot, mutta kyse ei ole 1-7 alakohtien mukaisesta toiminnasta. Tietomurron kohteena olevilla tiedoilla käydään kauppaa pimeässä verkossa ja niillä tehdään esimerkiksi petoksia.

Miten tulee arvioida tilanteita, joissa taustalla vaikuttaa olevan valtiollinen toiminta (vakoilu, yritysvakoilu) mutta kohteena oleva yritys ei kuitenkaan ole suoraan, keskinäisriippuvuuksista johtuen tunnistettavissa alakohtien 1-7 mukaiseksi toimialaksi.

Tuleeko 4-7 -kohtien mukaisten toimialojen sisällä tehdä arviota, millainen yhteiskunnallinen vaikutus jonkin yksittäisen toimijan toiminnan lamaantumisella on yhteiskunnan kannalta (kansainvälinen liikepankki, kotimainen pankki, joilla yksityishenkilöasiakkaita).

Keskusrikospoliisi on lausunnossaan tuonut esiin, että soveltamiskynnystä ei saisi asettaa liian korkealle, vaikka pykälän soveltaminen merkitseekin

laajamittaista tietojen vaihtoa viranomaisten välillä. Tilannetta saattaisi selkiyttää se, että perusteluluissa olevaa tapauksen yhteiskunnallista merkittävyyttä avattaisiin tarkemmin tai että mahdolliseksi harkintakriteeriksi nostettaisiin myös tapauksen taloudellinen vaikuttavuus tai vaikutus erittäin laajaan henkilöjoukkoon.

Lopuksi

On syytä huomioida, että rikosilmoituksen tekeminen on tietoturvaloukkauksen kohteena olleen yrityksen harkinnan varassa. Edes niin sanotun NIS-direktiivin piiriin kuuluvilla yrityksillä eli keskeisillä huoltovarmuuskriittisillä toimijoilla ja palveluntarjoajilla ei ole velvollisuutta tehdä tapauksista rikosilmoitusta. Ilmoitus tehdään sektorikohtaiselle valvovalle viranomaiselle ja vapaaehtoisen ilmoittamisen myötä tapaukset voivat tulla myös Liikenne – ja viestintäviraston tietoon.

Yhteiskunnan kriittisten toimintojen verkko- ja tietoturvallisuuden kokonaisuuden kannalta olisi tärkeää, että tietoturvahäiriöistä ja poikkeamista olisi mahdollista jatkossa informoida nykyistä tehokkaammin myös poliisia ja jos erittäin tärkeä yleinen etu vaatii syytteen nostamista, asiassa tehtäisiin myös rikostutkinta. Näissä tilanteissa asia ei voi jäädä yksinomaan kohdeyrityksen harkinnan varaan. Myös tämä seikka puoltaa sitä, että tiedonvaihdon viranomaisten välillä on oltava riittävän kattavaa ja tehokasta.

Keskusrikospoliisin päällikkö
Poliisineuvos Robin Lardot

Rikostarkastaja Anu Jaakkola

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 28.11.2022 klo 11:59. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Jakelu Sisäministeriö

Tiedoksi Poliisihallitus