Liikenne- ja viestintäministeriö
VN/18157/2023

Poliisihallituksen lausunto asiassa luonnos hallituksen esitykseksi

1 Lausuntopyynnöstä

Liikenne- ja viestintäministeriö on pyytänyt 3.10.2023 lähettämällään pyynnöllä Poliisihallituksen lausuntoa luonnoksesta hallituksen esitykseksi kyber-turvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Esityksellä Esityksessä ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta sekä muutoksia erinäisiin esityksessä mainittuihin lakeihin, jotka liittyvät kyberturvallisuusdirektiivin kansalliseen toimeenpanoon.

2 Poliisihallituksen kommentit luonnoksesta hallituksen esitykseksi

2.1 Luonnoksesta hallituksen esitykseksi

Esityksen pääasiallisen sisällön kuvauksessa todetaan esityksen tukevan Petteri Orpon hallitusohjelman kirjausta, jonka mukaan kyberturvallisuutta koskevaa yhteistyötä vahvistetaan viranomaisten ja elinkeinoelämän välillä. Kirjauksesta huolimatta luonnoksessa hallituksen esitykseksi ei ole juurikaan huomioitu poliisin roolia vakavien kyberrikosten estämisessä ja selvittämisessä.

Poliisi saa tiedonhankinnan ja rikosten esitutkinnan kautta tietoa kyberturvallisuuden kannalta merkittävistä uhista, mutta tätä ei ole huomioitu poliisin tiedonsaannin kannalta esityksessä. Poliisia ei ole myöskään kutsuttu osallistumaan esitystä valmistelevan työryhmän tai alatyöryhmien toimintaan. Kyberturvallisuusdirektiivin valmisteluvaiheessa EU jäsenvaltioiden lainvalvontaviranomaiset ovat esittäneet huolestuneisuutensa siitä, että kyberturvallisuuden uhkien torjunnassa ole riittävästi huomioitu sitä, että lainvalvontaviranomaiset saisivat tietoa kyberturvallisuuden uhista, jotta uhkien selvittäminen olisi mahdollista. Kyberturvallisuusdirektiivin kansallisessa toimeenpanossa oltaisiin voitu huomioida se, että kyberturvallisuuden uhkien torjunta vaatii laajaa yhteistyötä viranomaisten ja yrityssektorin kanssa. Esityksen johdannossa todetaan, että täytäntöönpanoa esitetään toteutettavaksi vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen. Kansallisen liikkumavaran käyttöä ei ole kuitenkaan toteutettu täysimääräisesti tiedonvaihdon osalta, vaan päinvastoin on

luotu tiedonvaihdon esteitä esimerkiksi poliisin suuntaan tapahtuvalle tiedonvaihdolle.

Poliisihallitus kiinnittää huomiota myös ns. CER-direktiivin valmisteluun ja siihen, että em. direktiivin ja nyt esitetyn NIS2-direktiivin täytäntöönpano ovat osin samanaikaisia. Esitysten valmistelun osalta toivotaan hyvin toimivaa koordinaatiota, jotta lainsäädännöllä saadaan luotua kestävä ja toimiva kokonaisuus.

3 Riskienhallinta- ja raportointivelvollisuus

Esityksessä laiksi kyberturvallisuuden hallintatoimenpiteiksi 4 §:ssä säädetään lain soveltamisalan rajauksista. Poliisi rajattaisiin em. pykälän perusteella lain soveltamisalan ulkopuolelle ja sen osalta voi olla tarpeen kiinnittää huomiota niihin palveluntarjoajiin, jotka toimittavat poliisille tietoturvaan tai tietojärjestelmiin liittyviä palveluita. Pykälän ei anna yksiselitteistä vastausta siihen, mitkä palveluntarjoajat olisivat soveltamisalan ulkopuolella.

Soveltamisalan osalta täsmennetään 4 §:n 5 momentissa siten, ettei laissa velvoiteta "*sellaisen tiedon antamiseen, jonka luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua.* " Edellä mainittu kirjaus jättää ulkopuolelle muut salassa pidettävän tiedon antamisen tilanteet, joissa tiedon antaminen voisi vaarantaa jotain muuta tärkeää etua kuin maanpuolustukseen tai kansalliseen turvallisuuteen liittyen. Pykälän voidaan tulkita velvoittavan tiedon luovutukseen, vaikka tiedon luovuttamisella voisi olla merkittävää haittaa viranomaisten toiminnalle, jos sillä ei olisi suoraa yhteyttä kansalliseen turvallisuuteen.

4 Kansallisen liikkumavaran kohdentaminen paikallistason toimijoihin

"Esityksessä ei ehdoteta käytettäväksi kansallista liikkumavaraa NIS2-direktiivin soveltamisesta paikallistason julkishallinnon toimialan toimijoihin tai opetus- ja koulutusalan laitoksiin. Poikkeuksena velvoitteita sovellettaisiin Helsingin kaupunkiin siltä osin kuin se hoitaa tehtäviä, jotka on laissa säädetty hyvinvointialueen järjestämisvastuulle." Kansallisen liikkumavaran ulottamista paikallistason toimijoihin tulisi harkita, koska näillä toimijoilla ei välttämättä ole tällä hetkellä kykyä ja tarvittavia resursseja varmistaa kyberturvallisuuden riittävä taso omassa toiminnassa. Paikallistason toimijat voivat käsitellä merkittäviäkin määriä henkilötietoja tai muuta yksityisyyteen kuuluvia tietoja. Edellä mainitun tiedon turvallinen käsittely, poikkeamista raportointi ja poikkeamien hallinta jäävät esityksen mukaan velvoitteiden ulkopuolelle ja tätä ei voida pitää kannatettavana koko yhteiskunnan kyberturvallisuuden kannalta.

5 Verkkotunnusvälittäjiin kohdistuvat velvoitteet

Suomessa aluetunnusrekisterin ylläpitäjänä toimii Liikenne ja viestintävirasto. Esityksessä ei tuoda esille sitä, millä tavalla valvonta olisi riippumatonta ja läpinäkyvää mikäli aluetunnusrekisterin valvonnasta vastaisi sama virasto, jolle valvottava toiminto kuuluu.

Lakia sähköisen viestinnän palveluista 167 §:ää esitetään muutettavaksi mm. verkkotunnusvälittäjien velvollisuuksista. Pykälän 2 momentissa todetaan, että *Liikenne- ja viestintävirasto voi estää verkkotunnuksen rekisteröinnin verkkotunnusrekisteriin, jos se epäilee 1 momentissa tarkoitettujen tietojen olevan puutteellisia tai virheellisiä eikä verkkotunnusvälittäjä kehotuksesta huolimatta todenna tietoja oikeiksi määräajassa.* Kirjaus jättää viranomaiselle tulkintavaraa sen osalta, että se voi halutessaan ja niin harkitessaan sallia rekisteriin merkittäväksi puutteelliset tai jopa virheelliset tiedot. Kysymys on viranomaisten ja muiden tahojen ylläpitämien rekistereiden luotettavuudesta ja tiedon oikeellisuudesta rekistereissä. On kestämätön tilanne, että viranomainen voi sallia virheellisten ja puutteellisten rekisteritietojen tallentamisen ja sen vuoksi esityksen kohta tuli muuttaa muotoon *Liikenne- ja viestintävirasto estää verkkotunnuksen rekisteröinnin verkkotunnusrekisteriin, jos se epäilee 1 momentissa tarkoitettujen tietojen olevan puutteellisia tai virheellisiä eikä verkkotunnusvälittäjä kehotuksesta huolimatta todenna tietoja oikeiksi määräajassa*. Suomen poliisin ja kansainvälisten lainvalvontaviranomaisten käsityksen mukaan verkkotunnuksia rekisteröitäessä käytetään varsin usein puutteellisia tai virheellisiä henkilö- ja yhteystietoja.

6 Salauksen käyttö tietoturvallisuuden varmistamiseksi

Liikenne- ja viestintäministeriö on tuonut lainvalmistelussa esiin useita kertoja päästä päähän salauksen kriittisyyden tietoturvaan liittyvänä olennaisena osatekijänä. Lausunnoissa on viitattu NIS2-direktiivin resitaaliin (98). Nyt esitetyssä lainsäädännössä salauksen käyttöön ei ole kuitenkaan viitattu tai siihen ei velvoiteta eri toimijoita. Mikäli päästä päähän salauksen käyttö edelleen arvioidaan kriittiseksi ja siihen velvoitetaan, niin Poliisihallitus pyytää huomioimaan edellä mainitun resitaalin täsmennys, jossa kyseiset salaukseen liittyvät toiminnot olisi *sovitettava jäsenvaltioiden toimivaltaan varmistaa keskeisten turvallisuusetujensa ja yleisen turvallisuuden suojelu ja mahdollistaa rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet unionin oikeuden* mukaisesti.

7 11 § Poikkeamailmoitukset viranomaiselle

Esityksessä laiksi kyberturvallisuuden riskienhallinnasta 11 §:ssä säädettäisiin poikkeamailmoituksista viranomaisille. Laissa tarkoitetun toimijan olisi ilmoitettava merkittävästä poikkeamasta. Pykälän 2 momentissa kuvataan ensi-ilmoitukseen sisältyvistä seikoista. Ensi-ilmoituksessa otetaan kantaa mm. siihen epäilläänkö merkittävän poikkeaman johtuvan rikoksesta tai

muusta lainvastaisesta tai vihamielisestä teosta. Kun kantaa otetaan siihen, epäilläänkö teon johtuvan rikoksesta, niin poikkeamailmoituksella luodaan käytännössä erillinen menettely rikoksista ilmoittamiselle. Poliisi vastaa poliisilain mukaan mm. yleisestä järjestyksen ja turvallisuuden ylläpitämisestä sekä rikosten ennalta estämisestä, paljastamisesta ja selvittämisestä. Tässä roolissa poliisi ottaa vastaan ilmoituksia rikoksista ja selvittää niitä. Nyt ehdotetulla menettelyllä todetaan, että rikoksista voitaisiin ilmoittaa toiselle viranomaiselle, jolla ei kuitenkaan olisi velvollisuutta siirtää tietoja ilmoitetusta rikoksesta toimivaltaiselle viranomaiselle. Mahdollisen rikoksen asianomistajien oikeus mm. vaatia asiassa rangaistusta tai vahingonkorvausta olisi erilainen riippuen siitä, tekisikö kyberpoikkeaman kohteeksi joutunut taho ilmoituksen poliisille tai keskusviranomaiselle.

8 Haavoittuvuusskannaus

Esitys laiksi kyberturvallisuuden riskienhallinnassa 20 § säädettäisiin yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjaisesta haavoittuvuuskartoituksesta. Pykäläkohtaisessa perustelussa on kerrottu, että 20 §:llä pantaisiin täytäntöön NIS2-direktiivin 11 artiklan 3 kohdan 1 alakohdan e-luetelmakohdassa ja saman artiklan 3 kohdan 2 alakohdassa CSIRT-yksikölle säädetyt tehtävät. Viitatussa direktiivin kohdassa lukee

> e) suorittaa keskeisen tai tärkeän toimijan pyynnöstä asianomaisen toimijan verkko- ja tietojärjestelmien ennakoiva skannaus sellaisten haavoittuvuuksien havaitsemiseksi, joilla voi olla merkittävä vaikutus;

Esitetyssä 20 §:ssä ei kuitenkaan säädetä siitä, että haavoittuvuuskartoitus tehtäisiin keskeisen tai tärkeän toimijan pyynnöstä ja kyseessä on merkittävä laajennus direktiivissä kuvattuihin CSIRT-yksikön tehtäviin. Haavoittuvuusskannaus voitaisiin tehdä viestintäverkon tai tietojärjestelmän suostumuksetta ja tietämättä. Kyse on merkittävästä viranomaisen toimivaltuudesta, joka voi vaikuttaa kolmannen tahon tietojärjestelmiin ja luottamukselliseen viestintään. Vähimmillään pykälää olisi muutettava siten, että sinänsä kannatettava haavoittuvuusskannaus perustuu kohteena olevan verkon tai tietojärjestelmän haltijan suostumukseen, jolloin voidaan selvittää myös viestinnän luottamuksellisuuden suojaan liittyvät kysymykset. Koska haavoittuvuuskartoituksen yhtenä tarkoituksena on pykälän mukaan tietoturvaa vaarantavista seikoista ilmoittaminen *asianomaisille tahoille*, niin kartoituksesta olisi sovittava. Asianomaisia tahoja ei ole tässä yhteydessä myöskään täsmennetty ja se olisi tarpeen, jotta viranomainen ilmoittaa kartoituksesta ja havainnoista oikealle taholle.

20 §:n 2 momentissa säädettäisiin, ettei haavoittuvuuskartoituksella saa hankkia tietoa yleisessä viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä. Kuitenkin 5 momentissa todetaan, että viestinnän sisältötietoja ei saa käsitellä ilman viestinnän

osapuolten suostumusta. Onko 2 momentissa oleva toteamus turha, jos asiaa täsmennetään välitystietojen tai sisällön osalta myöhemmin?

Haavoittuvuusskannauksen tuloksena voidaan saada varsin yksityiskohtaista tietoa luottamuksellisesta viestinnästä, mutta laissa ei säädettäisi kenellä olisi oikeus tehdä päätös haavoittuvuusskannauksesta tai kenellä olisi sellaisen toteuttamiseen oikeus. Koska kyseessä voi olla varsin merkittävästäkin luottamuksellisen viestinnän suojaan kajoavasta toimenpiteestä olisi syytä vähimmillään säätää siitä, millä virkamiehellä on oikeus tehdä päätös ja kenellä on toimenpiteen suorittamisen oikeus. Toimenpiteestä päättävällä taholla ja sen suorittajalla tulisi olla virka-aseman lisäksi riittävä perehtyneisyys asiaan liittyvään lainsäädäntöön ja suoritettavaan toimenpiteeseen.

Pykäläkohtaisessa perustelussa sallituksi menetelmäksi on kuvattu esimerkiksi oletuskäyttäjätunnuksen ja salasan yhdistelmän kokeileminen, mutta ei tämän jälkeen jatkuvat toimenpiteet järjestelmässä. Poliisihallitus kiinnittää huomiota rikoslain (1889) 38 luvun 8 §:n tietomurtoon, jonka teonkuvaus on seuraava.

> Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava *tietomurrosta* sakkoon tai vankeuteen enintään kahdeksi vuodeksi.

Kuten aiemmin on todettu, niin suostumus haavoittuvuusskannaukseen tietojärjestelmän tai verkon haltijalta olisi tärkeää saada myöskin teon rangaistavuuden poistamisen osalta.

9 24 § Kyberuhkiin ja poikkeamiin liittyvien eräiden tietojen luovuttaminen

Laissa kyberturvallisuuden riskienhallinnasta 24 §:ssä säädettäisiin Kyberuhkiin ja poikkeamiin liittyvien eräiden tietojen luovuttamisesta. 3 momentissa säädettäisiin seuraavasti.

> Siitä riippumatta, mitä viranomaisten oikeudesta saada salassa pidettäviä tietoja muualla laissa säädetään, CSIRT-yksikön tämän lain mukaista tehtävää hoitaessaan saamaa, muuta kuin pakollisen ilmoitusvelvollisuuden piiriin kuuluvaa tietoa ei saa käyttää tiedon luovuttanutta koskevassa rikostutkinnassa eikä hallinnollisessa tai muussa tiedon luovuttanutta koskevassa päätöksenteossa. Poikkeuksena on kuitenkin tilanne, jossa CSIRT-yksikön riskiarvion perusteella on tarpeen merkittävän kyberuhkan torjumiseksi ilmoittaa epäillystä vakavasta ja tahallisesta tämän lain rikkomisesta valvovalle viranomaiselle.

3 momentin kirjaus on monella tavalla ongelmallinen. Tietoa merkittävästäkin tahallisesta ja vahingollisesta tietoturvapoikkeamasta ei saisi käyttää tiedonluovuttanutta koskevassa rikostutkinnassa kuin siinä tapauksessa, että ilmoittaja ei kuuluisi ilmoitusvelvollisten piiriin. Tämä rajaisi merkittävän määrän tietoa sen ulkopuolelle, mitä tietoa voitaisiin tietoverkkorikosta tutkittaessa käyttää.

Toiseksi tiedon käyttämisen rajoitukset asettaisivat lainsäädännön mukaan ilmoitusvelvolliset eri asemaan kuin ne, joilla ei olisi lakiin perustuvaa ilmoitusvelvollisuutta tietoturvapoikkeamasta. Tätä kohtaa tulisi tarkastella perustuslain yhdenvertaisuuden näkökulmasta.

Kyseistä lainkohtaa on perusteltu luottamuksellisuuden säilyttämisen tarpeesta, mutta tästä ei ole esitykseen annettu konkreettisia esimerkkejä tai huomioitu sitä, että joissain maissa esimerkiksi viranomaisille on lainsäädännössä asetettu velvollisuus ilmoittaa epäillyistä rikoksista ja yhteistyö yksityisen sektorin sekä viranomaisten kanssa on toimivaa.

Kieltoa tiedon käyttämiseksi esitutkinnassa ei voida perustella myöskään itsekriminointisuojan osalta, koska ensinnäkin tietoa ei annettaisi suoraan esitutkintaviranomaiselle ja ennen kaikkea siksi, että tiedon käyttö olisi kiellettyä tiedon luovuttanutta koskevassa rikostutkinnassa, jolloin ilmoittaja voisi olla asiassa myös esimerkiksi asianomistajan asemassa.

Vastaavaa näin ehdotonta ja laajaa kieltoa jonkun tiedon hyödyntämiseksi rikostutkinnassa ei ole muualla lainsäädännössä ja sen vuoksi tiedon hyödyntämistä koskevan kiellon kirjaus tulisi joko kokonaisuudessaan poistaa tai kirjoittaa uudelleen siten, että varmistetaan vähimmillään törkeimpiä tietoverkkorikoksia koskevan tiedon luovuttaminen ja täsmennetään sitä, missä asemassa ilmoittaja olisi ilmoittavassa organisaatiossa tai esitutkinnassa.

Vaikka poliisi saisi muuta kautta tarvittavan tiedon hankittua epäillystä tietoverkkorikoksesta, niin osa tiedosta ei välttämättä olisi muilla kuin CSIRT-viranomaisilla käytössä. Tällainen tilanne saattaisi johtaa siihen, että epäillyissä rikoksissa asianomistajat olisivat eri asemassa sen mukaan, onko ilmoituksen tehnyt ilmoitusvelvollisuuden piiriin kuulunut vai vapaaehtoisen ilmoituksen tehnyt taho.

10 27 §. Valvovan viranomaisen tiedonsaantioikeus

27 §:ssä säädettäisiin valvovan viranomaisen oikeudesta saada tieto. Valvontaa suorittavalla viranomaisella tulee olla oikeus saada tarvittavat tiedot valvonnan suorittamiseksi ja maksutta, mikäli pyyntö on kohtuudella toteutettavissa. Sen sijaan vaatimus siitä, että tieto olisi toimitettava pyytävän viranomaisen edellyttämässä muodossa voi olla käytännössä mahdotonta toteuttaa. Mikäli tietojen toimittaminen edellyttäisi tietojen toimittamista valvovan viranomaisen käytössä olevan ohjelman mukaisessa muodossa ja tiedon luovuttajalla ei ole tällaista käytössä, voitaisiin ajautua mahdotto-

maan tilanteeseen ja tietopyyntöön ei voitaisi vastata lain edellyttämällä tavalla. Vastaavaa viranomaisen tiedonsaantioikeutta ei ole Poliisihallituksen tietojen mukaan muualla lainsäädännössä.

11 28 § Valvovan viranomaisen tiedonsaantioikeus välitystiedosta, sijaintitiedosta ja haitallisen tietokoneohjelman tai käskyn sisältävästä sähköisestä viestistä sijaintitiedosta ja haitallisen tietokoneohjelman tai käskyn sisältävästä sähköisestä viestistä.

Kuten haavoittuvuusskannauksenkin osalta, niin tällä toimivaltuudella puututtaisiin viestinnän luottamuksellisuuteen. Tiedon saamisen osalta edellytykseksi on asetettu tiedon saamisen välttämättömyys. Kuten haavoittuvuusskannauksesta koskevassa pykälässä, niin myöskään tässä ei ole säädetty siitä, kuka voisi tehdä päätöksen siitä, että esimerkiksi viestinnän sisältöä koskevaa tietoa pyydetään joltain toimijalta. Esitutkintaviranomaisten osalta on säädetty tarkkarajaisesti ne toimivaltuudet, joilla tietoa voidaan saada ja mikä taho toimivaltuuksia käyttää. Lainsäädännössä on asetettu edellytyksiä virka-asemalle ja asiaan perehtyneisyydelle.

12 Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta 18 d ja 18 e §:t

Laissa säädetään viranomaisten toiminnasta kyberpoikkeamatilanteissa ja esityksen 18 d §:ssä säädettäisiin merkittävistä poikkeamista ilmoittamisesta, jossa siinäkin ensi ilmoituksen yhteydessä olisi tuotava esiin, epäilläänkö tapahtuman johtuvan rikoksesta. Tämänkin osalta luodaan myös viranomaisille poliisin rikosilmoitusten kanssa rinnakkainen prosessi, jossa voitaisiin ilmoittaa rikoksista muulle viranomaiselle kuin poliisille. Tätäkään tietoa ei luovutettaisi poliisille suoraan. Koska kyseessä on ilmoitusvelvollisuus ja samanlaista luottamuksellisuuteen tai maineeseen liittyvää kysymystä ei viranomaisten osalta ole, niin voidaan aiheellisesti kysyä, miksi rikosta koskevaa tietoa ei voitaisi säätää suoraan poliisille luovutettavaksi. Tässä tapauksessa on kyse kansalaisten luottamuksesta viranomaistoimintaan ja jos nyt esitetty menettely mahdollistaisi sen, että viranomaisten tekemäksi epäiltyjä tai viranomaisiin kohdistuneita rikoksia ei ilmoitettaisi poliisille, vaan ne käsiteltäisiin muussa kuin rikosprosessissa, niin se väistämättä heikentäisi kansalaisten luottamusta viranomaistoimintaan.

18 e §:ssä säädettäisiin poikkeamailmoituksen vastaanottamisesta ja siinä yhteydessä säädettäisiin, että epäillyssä rikostapauksessa annettaisiin ohjeet rikoksesta ilmoittamiseen. Rikoksista ilmoittamista ei voida kuitenkaan säätää pelkän ohjeen varaan, vaan kokonaisuuden ja resurssien tehokkaan käytön kannalta olisi säädettävä CSIRT:in velvollisuudesta toimittaa tiedot poliisille varsinkin, kun kyse on merkittävistä kyberpoikkeamista.

45 §:ssä säädettäisiin laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelmasta. Kyberturvallisuuspoikkeamien hallintasuunnitelman sisällyttäminen lakiin ja olennaisten viranomaisten huomioiminen on kannatettavaa.

Poliisijohtaja Sanna Heikinheimo

Poliisitarkastaja Kimmo Ulkuniemi

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 29.11.2023 klo 08:28. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.