Sisäministeriö
Inrikesministeriet

Lausunto

1.12.2023

VN/18157/2023
VN/18157/2023-SM-134

Liikenne- ja viestintäministeriö

Sisäministeriön lausunto luonnoksesta hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Liikenne- ja viestintäministeriö on pyytänyt sisäministeriön lausuntoa luonnoksesta hallituksen esitykseksi eduskunnalle kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi. Sisäministeriön poliisiosasto on koonnut sisäministeriön yhteisen pois lukien Rajavartiolaitos, jolle on mennyt lausuntopyyntö erikseen.

Esityksellä pannaan täytäntöön Euroopan parlamentin ja neuvoston direktiivi (EU) 2022/2555 toimenpiteistä kyberturvallisuuden yhteisen korkean tason varmistamiseksi kaikkialla unionissa, asetuksen (EU) N:o 910/2014 ja direktiivin (EU) 2018/1972 muuttamisesta sekä direktiivin (EU) 2016/1148 kumoamisesta (jäljempänä NIS2-direktiivi). NIS2-direktiivin tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta kriittisten sektoreiden ja toimijoiden osalta. Luonnoksessa hallituksen esitykseksi ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta, jossa säädettäisiin yhteiskunnan toiminnan kannalta kriittisten toimijoiden kyberturvallisuuden riskienhallinnasta- ja raportointivelvoitteista.

Ehdotuksessa ehdotetaan säädettäväksi laki kyberturvallisuuden riskienhallinnasta. Lisäksi esityksessä ehdotetaan muutettavaksi muun muassa julkisen hallinnon tiedonhallinnasta annettua lakia ja sähköisen viestinnän palveluista annettua lakia.

Sisäministeriö lausuu esityksestä seuraavaa:

1. Yleistä

Esityksen mukaan Petteri Orpon hallituksen esityksen mukaan kyberturvallisuutta koskevaa yhteistyötä viranomaisten ja elinkeinoelämän välillä vahvistetaan. Hallitus myös parantaa tietoturvaakriittisillä toimialoilla ja toteuttaa kyberturvallisuuden kehittämisohjelman. Sisäministeriön arvion mukaan NIS2-direktiivin kansallinen toimeenpano ei ole täysin linjassa hallitusohjelman kirjausten tai viranomaisten toimintaedellytyksiä kyberturvallisuudessa annetun selvityksen (Valtioneuvoston julkaisuja 2023:31) ns. kyberselvityshankkeen kehittämistoimenpiteiden kanssa. Kyberselvityshankkeessa keskeiset kehittämistoimeenpiteet liittyvät tiedonvaihdon kehittämiseen viranomaisten välillä. Selvityshankkeen raportti valmisteltiin laajassa yhteistyössä kyberturvallisuuteen liittyvien ministeriöiden ja virastojen kanssa. Liikenne- ja viestintäministeriö ja Kyberturvallisuuskeskus olivat hankkeessa keskeisiä tahoja puolustusministeriön ja sisäministeriön kanssa.

Toimenpide-ehdotuksista NIS2-direktiivin toimeenpanoa koski kehittämistoimenpide, jonka mukaan parannetaan tietoturvaloukkauksiin liittyvien ilmoitusten nojalla luovutettujen tietojen jaka-

Postiosoite Postadress Postal Address	Käyntiosoite Besöksadress Office	Puhelin Telefon Telephone	Faksi Fax Fax	s-posti, internet e-post, internet e-mail, internet
Sisäministeriö				
PL 26 00023 Valtioneuvosto	Kirkkokatu 12 Helsinki	0295 480 171 +358 295 480 171	09 160 44635 +358 9 160 44635	kirjaamo.sm@gov.fi www.intermin.fi

mista viranomaisten välillä nykyistä laajemmin. Kehittämistoimenpiteissä ehdotetaan mahdollistettavaksi Puolustusvoimien, poliisin, suojelupoliisin ja Liikenne- ja viestintäviraston tiedon koordinoitu tuottaminen, analysointi ja jakaminen yhteisen tilanneymmärryksen muodostamiseksi. Jäljempänä pykäläkohtaisissa huomioissa on tarkemmin tuotu esille viranomaisten tietojen vaihtoon liittyvät huomiot.

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.

Liikenne- ja viestintäministeriö on tuonut lainvalmistelussa esiin useita kerto-ja 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.

Sisäministeriö myös kiinnittää huomiota siihen, että ehdotuksessa laiksi kyberturvallisuuden riskienhallinnasta käytetään paikoin yleiskielelle vieraita sanoja kuten systeeminen, rekursiivinen ja ei-intrusiivinen.

2. Pykäläkohtaiset huomiot luonnokseen laiksi kyberturvallisuuden riskienhallinnasta

4 § Soveltamisalan rajoitukset

Esityksen 4 §:ssä säädetään lain soveltamisalan rajauksista. Soveltamisalan rajoitusten osalta julkisen hallinnon toimijoista tullaan säätämään tarkemmin julkisen hallinnon tiedonhallintalaissa, johon huomiot asianomaisessa kohdassa jäljempänä.

Sisäministeriö kiinnittää 4 §:n 5 momenttiin, jonka mukaan "tässä laissa velvoiteta sellaisen tiedon antamiseen, jonka luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua. " Muotoilu jättää ulkopuolelle muut salassa pidettävän tiedon antamisen tilanteet, joissa tiedon antaminen voisi vaaran-taa 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.

9 § Kyberturvallisuuden riskienhallinnan toimenpiteet

Kyberturvallisuusdirektiivin 21 artiklan 2 kohdassa on luettelo niistä kyberriskienhallinnan vähimmäisvaatimuksista osa-alueittain, joita sääntelyn piirin kuuluvien toimijoiden on velvoitettava huomioimaan riskienhallinnassaan. Artiklan 2 d-kohdassa velvoitetaan toimijoita huomioimaan toimitusketjun turvallisuus seuraavasti: toimitusketjun turvallisuus, mukaan lukien kunkin toimijan ja sen välittömien toimittajien tai palveluntarjoajien välisten suhteiden turvallisuusnäkökohdat. Artiklan 3. kohdassa täsmennetään, että toimijoiden on tältä osin huomioitava kunkin välittömän toimittajan ja palveluntarjoajan erityiset haavoittuvuudet, ja toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleisen laadun mukaan lukien näiden turvalliset kehittämismenettelyt.

lakiehdotuksen 9 §:ssä sekä tiedonhallintalakiin lisättäväksi esitettävässä 18 c §:ssä kyseinen kohta on typistynyt muotoon: toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt, jättäen huomioimatta direktiivin tarkentavan viittauksen erityisiin haavoittuvuuksiin toimitusketjun laitetoimittajissa tai palveluntarjoajissa. Erityisten haavoittuvuuksien voidaan tulkita viittaavan

teknisten haavoittuvuuksien lisäksi tuotantoketjun laitevalmistajien kotimaan lainsäädäntöön liittyviin velvoitteisiin ja niiden mukanaan tuomiin haavoittuvuuksiin koskien viestinnän luottamuksellisuutta.

Niin ikään kyberturvallisuusdirektiivin artiklan 7 toisen kappaleen a-kohdassa edellytetään jäsenmaiden kyberturvallisuusstrategioissa toimijoiden ottavan huomioon ICT tuotteiden ja palveluiden tuotantoketjujen kyberturvallisuus. Sisäministeriön näkemyksen mukaan hallituksen esityksessä ei riittävällä tavalla huomioida laitevalmistajaan tai palveluntarjoajaan mahdollisesti liittyviä erityisiä haavoittuvuuksia, kuten direktiivi edellyttäisi. Strateginen riski tulisikin huomioida vähintään tiedonhankintalaissa. Muuten kansallinen sääntely suojaa tiedonhallintayksikköä, sen käsittelemää dataa, sekä rekisteröityjen oikeusturvaa huomattavasti kapeammin kuin direktiivi.

11 § Poikkeamailmoituksen viranomaiselle

Lakiehdotuksen 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. On syytä huomioida, että poikkeamissa voi olla kyse rikoksista, joissa on sekä yksilön että yhteiskunnan kannalta vahva selvittämisintressi ja vahinkojen estämisintressi (kuten Vastaamo-tapaus). Jos rikosilmoituksen tekeminen viivästyy, voi poliisin mahdollisuudet hankkia sähköistä todistusaineistoa hävitä. Tällä voi olla vaikutuksia merkittävän joukon asianomistajien oikeuksiin vaatia rangaistusta tai saada vahingonkorvausta.

Traficom on laatimassa ilmoitusvelvollisuuden täyttämiseen verkkolomaketta. Sisäministeriö ehdottaa, että samalla ilmoituksella toimija voisi tehdä NIS2- ilmoitusten lisäksi myös rikosilmoituksen sekä CER-direktiivin mukaiset ilmoitukset. CER-valmistelussa onkin toistuvasti kriittisten yritysten taholta esitetty pyyntö yhden sähköisen portaalin toteuttamiseksi kaikkien turvallisuuteen liittyvien viranomaisilmoitusten hoitamiseksi (NIS-CER-Poliisi jne), mitä sisäministeriö lämpimästi kannattaa yrityksiin kohdistuvan hallinnollisen taakan vähentämiseksi.

20 § Haavoittuvuusskannaus

Pykäläehdotuksen 20 § säädettäisiin yleisten viestintäverkkojen ja tietojärjestelmien verkkopohjaisesta haavoittuvuuskartoituksesta. Pykälässä annettaisiin CSIRT-yksikölle oikeus ennakoivalla, ei-intrusiivisella tavalla tehdä pykälässä tarkemmin kuvattu haavoittuvuustarkastus. Sisäministeriö kiinnittää huomiota siihen, että haavoittuvuusskannaus voitaisiin tehdä viestintäverkon tai tietojärjestelmän suostumuksetta ja tietämättä.

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. Viitatun direktiivin e) kohdan mukaan CSIRT-yksikkö voi 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, joten kyseessä on merkittävä laajennus direktiivissä kuvattuihin CSIRT-yksikön tehtäviin. Sinänsä haavoittuvuustarkastus on kannatettava, mutta sisäministeriö esittää arvioitavaksi toimivaltuuden sitomista haavoittuvuusskannauksen kohteen suostumukseen.

Haavoittuvuuskartoituksen tuloksena voidaan saada varsin yksityiskohtaista tietoa luottamuksellisesta viestinnästä, mutta laissa ei säädettäisi kenellä olisi oikeus tehdä päätös haavoittuvuuskartoitus 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. Vastaava koskee ehdotetun lain 28 §:ää. Kuten haavoittuvuuskartoituksen osalta 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.

Haavoittuvuusskannauksen pykäläkohtaisessa perustelussa sallituksi menetelmäksi on kuvattu esimerkiksi oletus-käyttäjätunnuksen ja salasan yhdistelmän kokeileminen, mutta ei tämän jälkeen jatkuvat toimenpiteet järjestelmässä. Sisäministeriö kiinnittää huomiota rikoslain (1889) 38 luvun 8 §:n tietomurron tunnusmerkistöön: "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. Sisäministeriön käsityksen mukaan tietojärjestelmän tai verkon haltijan suostumus haavoittuvuuskartoitukseen olisi oleellinen seikka myöskin teon rangaistavuuden poistamisen osalta.

23 § Kyberuhkiin ja poikkeamiin liittyvien eräiden tietojen luovuttaminen

Ehdotuksessa huomio kiinnittyy poliisin ja muidenkin turvallisuusviranomaisten mahdollisuuksiin saada tietoa merkittävistä tietoturvaloukkauksista. Uuden ehdotettavan kyberturvallisuuden riskienhallinnasta annetun lain 24 §:n 3 momenttiin ollaan rakentamassa palomuuria. Direktiivi ei edellytä tällaista sääntelyä. Lakiehdotuksen 24 §:n 3 momentin mukaan: "Siitä riippumatta, mitä viranomaisten oikeudesta saada salassa pidettäviä tietoja muualla laissa säädetään, CSIRT-yksikön tämän lain mukaista tehtävää hoitaessaan saamaa, muuta kuin pakollisen ilmoitusvelvollisuuden pii-riin 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*.

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 tietoverkko-rikosta tutkittaessa käyttää.

Toiseksi tiedon käyttämisen rajoitukset asettaisivat lainsäädännön mukaan ilmoitusvelvolliset eri asemaan kuin ne, joilla ei olisi lakiin perustuvaa ilmoitusvelvollisuutta tietoturva-poikkeamasta. 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.

Vastaava 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.

40 § Seuraamusmaksujen enimmäismäärä

Ottaen huomioon sen, että tieto- ja viestintäpalvelut ovat yhteiskunnan kriittisiä toimintoja, sisäministeriö kiinnittää huomiota siihen, että NIS2-direktiivin edellyttämien hallinnollisten sanktioiden enimmäismäärät olisivat tasolla, joka on direktiivin *alin* sallima enimmäismäärä.

45 § Laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelma

Pykälässä säädettäisiin kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman laatimisesta sekä kyberkriisinhallintaviranomaisesta. Ehdotuksen mukaan Liikenne- ja viestintävirasto vastaa kansallisen laajamittaisten kyberturvallisuuspoikkeamisen ja kriisien hallintasuunnitelman laatimisesta yhteistoiminnassa 25 §:ssä tarkoitettujen valvovien viranomaisten, Poliisihallituksen, suojelupoliisin, Puolustusvoimien ja huoltovarmuuskeskuksen kanssa. Sisäministeriö kannattaa laajamittaisten kyberpoikkeamien ja -kriisien hallintasuunnitelmien tekemiseen ehdotettua yhteistoimintamallia.

46 § Viranomaisten yhteistyö

Pykälän 2 momentissa säädettäisiin valvovien viranomaisten, CSIRT-yksikön ja keskitetyn yhteyspisteen velvollisuudesta tehdä tarvittaessa yhteistyötä poliisin tai muun esitutkintaviranomaisen, tietosuojavaltuutetun, siviili-ilmailun turvallisuudesta vastaavan viranomaisen, eIDAS-asetuksen mukaisten valvontaelinten, DORA-asetuksen mukaisen toimivaltaisen viranomaisen, teledirektiivin mukaisen kansallisen sääntelyviranomaisen ja CER-direktiivin mukaisen toimivaltaisen viranomaisen kanssa. Sisäministeriö kannattaa ehdotettua yhteistoimintavelvoitettua.

3. Pykäläkohtaiset huomiot julkisen hallinnon tiedonhallinnasta annetun lain muuttamiseen

3 § Lain soveltamisala ja sen rajoitukset

Esityksessä olevan tiedonhallintalain 3 §:n 2 momentin mukaan 4 a lukua sovellettaisiin tiedonhallintalain 4 §:n 1 momentin 1 kohdassa tarkoitettuihin valtion virastoihin ja laitoksiin, valtion liikelaitoksiin, 4 §:n 1 momentin 9 kohdassa tarkoitettuihin itsenäisiin julkisoikeudellisiin laitoksiin sekä hyvinvointialueisiin, hyvinvointiyhtymiin ja Helsingin kaupunkiin niiden hoitaessa laissa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä. Lisäksi 4 a lukua sovellettaisiin [CER-lain] nojalla julkishallinnon toimialan kriittisiksi toimijoiksi määriteltyihin toimijoihin.

Esityksessä ehdotetaan säädettäväksi kansallisen liikkumavaran sallima poikkeus NIS2-direktiivistä aiheutuvien velvoitteiden soveltamiseen erityisiin toimijoihin, jotka tarjoavat palveluita sellaisille julkishallinnon toimijoille, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet, tai harjoittavat sellaista toimintaa itse. Kansallista liikkumavaraa käytettäisiin täysimääräisesti NIS2-direktiivin sallimalla tavalla velvoitteiden kohdistumisesta näihin toimijoihin.

Tiedonhallintalain 4 a lukua ei sovellettaisi sisäministeriön hallinnonalalla poliisin hallinnosta annetussa laissa (110/1992) tarkoitettuihin poliisiyksiköihin eikä Rajavartiolaitokseen. eikä julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015), tarkoitettuun turvallisuusverkon palvelutuotantoon ja palveluiden käyttöön. Sisäministeriö kannattaa soveltamisrajoitusta jäljempänä Hätäkeskuslaitosta ja Pelastusopistoa koskevin huomioin.

Säännöskohtaisten perustelujen (s. 156) mukaan 4 a luvun soveltamisalaan kuuluisivat hyvinvointialueet ja hyvinvointiyhtymät ja Helsingin kaupunki, jotka olisi katsottava kansallisen lainsäädännön mukaisesti direktiivissä tarkoitetuiksi aluetason julkishallinnon toimijoiksi niiden toteuttaessa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä. Hyvinvointialueiden, hyvinvointiyhtymien ja Helsingin kaupungin järjestämisvastuulle kuuluvat lakisääteisesti sosiaali- ja terveydenhuolto sekä pelastustoimi. Julkisen ja yksityisen terveydenhuollon tarjoajat kuuluvat NIS2-direktiivin liitteen I kohdan 5 Terveystoimialaan, jonka osalta direktiivissä säädetyistä velvoitteista ja valvonnasta säädettäisiin ehdotetussa kyberturvallisuuden riskienhallintaa koskevassa laissa. Tällöin ehdotettu tiedonhallintalain sääntely ulottaisi direktiivin velvoitteet koskemaan myös hyvinvointialueiden ja hyvinvointiyhtymien hallintoa sekä Helsingin kaupungin hallintoa sosiaali- ja terveydenhuollon ja pelastustoimen osalta. Lisäksi sääntely koskisi sosiaalihuollon ja pelastustoimen viran omaisia hyvinvointialueilla, hyvinvointiyhtymissä ja Helsingin kaupungissa. Hallinnon toimivuus on edellytys sille, että hyvinvointialueet ja –yhtymät sekä Helsingin kaupunki voivat toteuttaa niille säädetyt yhteiskunnan kriittisisiksi toiminnoiksi lukeutuvat tehtävät.

Hyvinvointialueen pelastustoimi

Ehdotettu tiedonhallintalain sääntely ulottaisi NIS2 -direktiivin velvoitteet koskemaan hyvinvointialueiden ja hyvinvointiyhtymien hallintoa sekä Helsingin kaupungin hallintoa pelastustoimen osalta. Sisäministerin pelastusosasto toteaa, että hyvinvointialueet kuuluvat direktiivin pakolliseen soveltamisalaan. Lisäksi ehdotettu tiedonhallintalain sääntely koskisi pelastustoimen viranomaisia hyvinvointialueilla, hyvinvointiyhtymissä ja Helsingin kaupungissa. Pelastusosaston näkemyksen mukaan pelastustoimi voidaan nähdä direktiivin 2 artiklan 7 kohdan mukaisena yleisen turvallisuuden toimijana. Direktiivin velvoitteet julkishallinnon osalta lisättäisiin tiedonhallintalakiin, jolloin ne koskisivat tiedonhallintayksikköä.

Tiedonhallintayksikön yhtenäiset kyberturvallisuuden hallintakeinot ja –mallit parantavat kyberturvallisuutta ja ehkäisevät siilojen muodostumista.

Sisäministeriön pelastusosasto katsoo, että hallinnon toimivuus on edellytys sille, että hyvinvointialueet ja Helsingin kaupunki voivat toteuttaa niille säädetyt yhteiskunnan kriittisisiksi toiminnoiksi lukeutuvat pelastustoimen tehtävät. Tältä osin tiedonhallintalain mukainen soveltamisala ja sääntelyesitys ovat perusteltua.

Hätäkeskuslaitos

Hallituksen esitysluonnoksen mukaan NIS2-direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen. Esityksen mukaan Hätäkeskuslaitosta ei ole suljettu pois tiedonhallintalain 4 a luvun soveltamisalasta.

Hätäkeskuslain (692/2010) mukaan Hätäkeskuslaitoksen tehtävänä on hätäkeskuspalvelujen tuottaminen. Hätäkeskustoiminnalla tarkoitetaan hätäkeskuspalveluja ja Hätäkeskuslaitoksen välittämään hätäilmoitukseen tai tehtävään liittyviä pelastustoimen, poliisin ja sosiaali- ja terveystoimen ja Rajavartiolaitoksen välittömiä toimenpiteitä edellyttävien lakisääteisten tehtävien hoitamista Hätäkeskuslaitoksen tuella. Hätäkeskuslaitos vastaanottaa hätäkeskuksissa hätäilmoituksia eli hätätilanteita koskevia ja muita vastaavia pelastustoimen, poliisin sekä sosiaali- ja terveystoimen ja Rajavartiolaitoksen välittömiä toimenpiteitä edellyttäviä ilmoituksia. Hätäkeskuslaitos arvioi hätäilmoituksen ja tarvittaessa välittää ilmoituksen tai tehtävän asianomaiselle viranomaiselle tai viranomaisen tehtäviä sopimuksen perusteella hoitavalle. Hätäkeskuslaitos tuottaa myös kiireellisiä ja muita tukipalveluja edellä mainituille viranomaisille. Hätäkeskuslaitos on julkishallinnon toimija, jonka tehtävät liittyvät yleisen turvallisuuden turvaamiseen. Merkittävä osa hätäkeskusten välittämistä tehtävistä kuuluu poliisille, joka on rajattu tiedonhallintalain 4 a luvun soveltamisalan ulkopuolelle. Lisäksi Hätäkeskuslaitoksen operatiiviset ja hallinnolliset tietojärjestelmät ovat turvallisuusverkossa, joka lakiesityksessä on rajattu pois tiedonhallintalain 4 a luvun soveltamisalasta.

Sisäministeriön pelastusosasto katsoo, että myös *Hätäkeskuslaitos tulee rajata tiedonhallintalain 4 a luvun soveltamisalan ulkopuolelle.*

Hätäkeskuslaitos tulee antamaan oman lausuntonsa asiassa.

Pelastusopisto

Esityksessä olevan tiedonhallintalain säännöskohtaisten perustelujen (s.155) mukaan 3 §:n 2 momentissa ehdotettu sääntely kattaisi direktiivissä säädetyn vähimmäissoveltamisalan julkishallinnon toimijoiden osalta. Momentissa tarkoitettuihin valtion virastoihin ja laitoksiin lukeutuisivat tiedonhallintalain 4 §:n 1 momentin 1 kohdan mukaisina tiedonhallintoyksikköinä toimivat valtion virastot ja laitokset mukaan lukien niissä toimivat viranomaiset. Julkisoikeudellinen laitos on itsenäinen julkisoikeudellinen oikeushenkilö, joka on yleensä perustettu erityisellä säädöksellä julkisoikeudellisen laitoksen asemaan.

Itsenäisillä julkisoikeudellisilla laitoksilla on tavallisesti myös oma talous ja hallinto. Itsenäiset julkisoikeudelliset laitokset ovat oikeustoimikelpoisia. Julkisoikeudellinen laitos ei kuulu varsinaiseen hallinto koneistoon, mutta se hoitaa erikseen määriteltyä julkista tehtävää ja käyttää julkista valtaa. Ne päättävät ihmisiin kohdistuvista oikeuksista ja velvollisuuksista ja niiden toiminnasta on säädetty laissa. Laitoksen itsenäisyys merkitsee lähinnä sen korostettua riippumattomuutta hallintokoneiston ohjauksesta. Niiden toimintaa valvoo kuitenkin valtio. Valinta eri organisaatiomuotojen välillä (esimerkiksi valtion virasto vai julkisoikeudellinen laitos) on ollut

epäsystemaattista ja osin satunnaista. Edellä todettu huomioon ottaen itsenäiset julkisoikeudelliset laitokset olisi luettava NIS2-direktiivin liitteen I kohdassa 10 tarkoitettuihin keskustason julkishallinnon toimijoihin, joihin pääsääntöisesti on sovellettava direktiiviä.

Paikallistason julkishallinnon toimijoiden sekä opetus- ja koulutusalan laitoksien saattaminen direktiivin edellyttämän sääntelyn soveltamisalaan on kansallisen liikkumavaran alassa ja niitä ei ehdoteta kuuluvaksi ehdotetun tiedonhallintalain 4 a luvun soveltamisalaan.

Pelastusopistosta annetussa laissa (607/2006) säädetään valtion ylläpitämän sisäministeriön alaisen Pelastusopiston tehtävistä ja hallinnosta, Pelastusopistossa annettavasta koulutuksesta sekä opiskelijoiden oikeuksista ja velvollisuuksista. Pelastusopisto on siten tiedonhallintalain tarkoittama itsenäinen julkisoikeudellinen laitos.

Pelastusopiston tehtävänä on antaa pelastustoimen ja hätäkeskustoiminnan ammatillista peruskoulutusta, pelastustoimen päällystön ammattikorkeakoulututkintoon johtavaa koulutusta, normaaliolojen häiriötilanteisiin ja poikkeusoloihin varautumiseen valmentavaa koulutusta sekä huolehtia osaltaan pelastustoimen tutkimus- ja kehittämistoiminnasta, tutkimistoiminnan koordinoinnista sekä tarvittaessa muistakin opiston toimialaan soveltuvista tehtävistä.

Esitystä tulisi tarkentaa siltä osin, kuuluuko Pelastusopisto tiedonhallintalain soveltamisalaan vai ei. Pelastusopisto on tiedonhallintalain tarkoittama itsenäinen julkisoikeudellinen laitos, johon pääsääntöisesti on sovellettava direktiiviä. Mutta toisaalta Pelastusopisto on myös opetus- ja koulutusalan laitos. Opetus- ja koulutusalan laitoksien saattaminen direktiivin edellyttämän sääntelyn soveltamisalaan on kansallisen liikkumavaran alassa ja niitä ei ehdoteta kuuluvaksi ehdotetun tiedonhallintalain 4 a luvun soveltamisalaan.

Kun huomioidaan, että NIS2-direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja Pelastusopisto toimii osittain myös turvallisuusverkossa, voitaisiin Pelastusopisto rajata tiedonhallintalain 4 a soveltamisalan ulkopuolelle.

Pelastusopisto tulee antamaan oman lausuntonsa asiassa.

18 d § Ilmoitusvelvollisuus merkittävästä poikkeamasta

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 käytän kannalta olisi säädettävä CSIRT:in velvollisuudesta toimittaa tiedot poliisille erityisesti, kun kyse on merkittävistä kyberpoikkeamista.

Lisäksi vaikka turvallisuusverkon palvelun tarjoaja on rajattu 4 a luvun sääntelyn ulkopuolelle, on muitakin tilanteita, joissa sääntelyn piiriin kuuluva toimija jakaa tietoverkon sääntelyn ulkopuolelle yleisen turvallisuuden perusteella suljetun toimijan kanssa. Ehdotuksessa on epäselvää, miten raportointi- ja valvontatoimenpiteet toteutetaan tällaisessa tilanteessa. Poikkeamien raportointivelvoitteita tulisi myös täsmentää niissä tilanteissa, kun poikkeamasta syntyy ilmoitusvelvollisuus useammalle valvovalle viranomaiselle.

4. Lopuksi

Lopuksi sisäministeriö toteaa, että hallituksen esitys on NIS-direktiivin laajuus ja täytäntöönpanolle annetun ajan niukkuus huomioon ottaen perusteellisesti valmisteltu.

Sisäministeriön näkemyksen mukaan NIS2- ja CER-direktiivien täytäntöönpano vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa sekä kriittisen infrastruktuurin suojaa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta.

Sisäministeriöllä ei ole muuta lausuttavaa toimialaansa liittyen.

Poliisijohtaja Stefan Gerkman

Lainsäädäntöneuvos Tiina Ferm

Liitteet

Jakelu

Tiedoksi

VN/18157/2023-SM-134

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Ferm Tiina 91297491B	GERKMAN STEFAN 91260077E
2023-12-01	2023-12-01