Eduskunnan oikeusasiamiehen kanslia

Lausunto

29.11.2023 EOAK/6393/2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

-

Soveltamisalaa koskevat huomiot

-

Riskienhallintavelvoitetta koskevat huomiot

-

Raportointivelvoitetta koskevat huomiot

-

Valvontaa koskevat huomiot

Hallituksen esitysluonnoksen mukaisesti valvovat viranomaiset nimettäisiin jatkossakin sektorikohtaisesti NIS1-direktiivin mukaista valvontamallia jatkaen. Valvovia viranomaisia olisivat sektorikohtaisen toimijan mukaan Liikenne- ja viestintävirasto, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Sosiaali- ja terveydenalan lupa- ja valvontavirasto, Etelä-Savon ELY-keskus, Ruokavirasto, Lääkealan turvallisuus ja kehittämiskeskus sekä Finanssivalvonta. Tiedonhallintalakiin ehdotettavien säännösten valvovana viranomaisena olisi Liikenne- ja viestintävirasto.

Valittua sektorikohtaisesti hajautettua valvontamallia on ehdotuksessa arvioitu monipuolisesti, eikä siitä ole huomauttamista. Esityksessä esiin tuotuja tarpeita valvonnan lisäresursointiin voidaan pitää kannatettavina ja valvonnan uskottavuutta lisäävänä.

Valvonnan järjestämisen vaihtoehtojen arvioinnissa (otsikko 5.1.4, s 98) on kuitenkin tuotu esiin, että NIS1-direktiivin täytäntöönpanossa omaksuttu sektorikohtainen valvontamalli on koettu pääosin toimivaksi, ja nykyisten valvovien viranomaisten ja valvonnan kohteena olevien toimijoiden välille on muodostunut luottamussuhteita ja yhteistyötä, jonka tarkoituksena on parantaa kyberturvallisuuden tasoa, riskienhallintaa ja kriisinkestävyyttä. Kansallisesti olemassa oleva viranomaisten keskinäinen sekä yritysten välinen yhteistyö on kehittynyt vuosien aikana pääosin toimivaksi, eikä tätä yhteistyötä ole esitysluonnoksen mukaan tarkoituksenmukaista kaventaa NIS2-direktiivin täytäntöönpanon yhteydessä.

Vaikka valvovien viranomaisten ja valvonnan kohteiden yhteistyö voi edistää kyberturvallisuutta, esityksessä ei mielestäni riittävästi arvioida sitä, miten valvovien viranomaisten ja valvonnan kohteena olevien toimijoiden läheinen yhteistyö vaikuttaa valvonnan riippumattomuuteen. Viranomaisten valvontaroolia ja valvonnan riippumattomuuden turvaamisen tärkeyttä olisi hyvä korostaa vaihtoehtojen arvioinnissa, jotta ei tarpeettomasti synny mielikuvaa valvojan ja valvottavan suhteen muodostumisesta yhteistyösuhteeksi.

Lisäksi voi olla tarvetta arvioida kyberturvallisuuden riskienhallintalain valvontasäännösten (4 luku) soveltamisalan selkiyttämistä suhteessa eduskunnan oikeusasiamiehen kanslian toimintaan ylimpänä laillisuusvalvojana. Näin erityisesti huomioiden, että eduskunnan virastot (eduskunnan oikeusasiamiehen kanslia mukaan lukien) on nimenomaisesti suljettu julkishallinnon toimijoina johdon toiminnan rajoittamista (33 §:n 3 momentti) ja seuraamusmaksun määräämistä (37 §:n 2 momentti) koskevan sääntelyn soveltamisalan ulkopuolelle.

Seuraamusmaksua koskevat huomiot

Uudessa laissa säädettäisiin hallinnollisesta seuraamusmaksusta, jonka määräisi ehdotetun 38 §:n mukaan valvovan viranomaisen esityksestä seuraamusmaksulautakunta. Esityksen perusteluissa on perustuslakivaliokunnan käytäntöön viitaten arvioitu tällaisen merkittävää julkista valtaa käyttävän toimielimen yleisistä perusteista lailla säätämistä. Luonnoksen mukaisessa 38 §:ssä määritellään valiokunnan lausuntokäytäntö huomioiden yleisistä perusteista toimielimien nimi, toimiala, pääasialliset tehtävät ja toimivaltuudet, sekä se miten lautakunta asetetaan ja sekä mikä on sen kokoonpano ja toimikausi.

Esitysluonnoksessa olisi kuitenkin hyvä vielä selkiyttää minkä viranomaisen yhteydessä seuraamusmaksulautakunta mahdollisesti toimisi, sekä se, mikä taho sitä valvoisi. Toteuttamisvaihtoehtojen arvioinnin yhteydessä (otsikko 5.1.5 Seuraamusmaksu) on tuotu esiin, että seuraamuslautakunta toimisi Liikenne- ja viestintäviraston yhteydessä. Itse pykälästä tai sen perusteluista asia ei käy esille.

Lisäksi perusteluissa voisi olla syytä selkiyttää miten eri viranomaisista koostuvan ja vain tarvittaessa seuraamusmaksun määräämistä koskevan asian käsittelemiseksi kokoontuvan lautakunnan jäsenten virkavastuu rikosoikeudellisena virkavastuuna, kurinpidollisena virkavastuuna sekä

vahingonkorvausvastuuna kohdentuisi. Sinällään on selkeää, että lautakunnan jäsenet ovat virkasuhteisia, mutta vähintään perusteluissa olisi hyvä selventää olisiko virkasuhde olemassa vain jäsenen nimeävään valvovaan viranomaiseen vai myös uuteen seuraamusmaksulautakuntaan.

Kyberturvallisuuden riskienhallintalaki luonnoksen 41.3 §:n mukaisesti seuraamusmaksua ei saa määrätä sille, jota epäillään samasta teosta esitutkinnassa, syyteharkinnassa tai tuomioistuimessa vireillä olevassa rikosasiassa. Seuraamusmaksua ei saa määrätä myöskään sille, jolle on samasta teosta annettu lainvoimainen tuomio. Perusteluissa tämän ne bis in idem -periaatteen soveltamista voisi täsmentää, sillä ei ole täysin poissuljettua, etteikö seuraamusmaksun määräämistä voisi selvittää tai maksua määrätä esimerkiksi oikeushenkilölle tilanteessa, jossa sen henkilöstöä epäillään samasta teosta esitutkinnassa, syyteharkinnassa tai tuomioistuimessa vireillä olevassa rikosasiassa tai saanut samasta teosta lainvoimaisen tuomion

Säätämisjärjestysperusteluissa (otsikko 12.4 Hallinnollinen seuraamusmaksu, s. 199) ne bis in idem -periaate todetaan huomioidun 37 §:n 3 momentissa. Tällä tarkoitettaneen kuitenkin lakiluonnoksen 41 §:n 3 ja 4 momentteja.

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Esitysluonnoksen mukaan yksinomaan julkishallinnon toimialaan kohdistuvista velvoitteista ja niiden noudattamisen valvonnasta säädettäisiin erikseen tiedonhallintalaissa. Tiedonhallintalaki olisi erityislaki suhteessa esitettyyn kyberturvallisuuden riskienhallinnasta annettuun lakiin. Jos julkinen toimija toimii jollain NIS2-direktiivin muista toimialoista, se voi kuulua NIS2-sääntelyn piiriin myös tai vain kyberturvallisuuden riskienhallinnasta annetun lain nojalla.

Lisättäväksi ehdotettavan uuden 4 a luvun erillinen uusi soveltamisalasäännös (tiedonhallintalain 3 §:ään ehdotettu uusi 2 momentti) on osin vaikeatulkintainen.

Ehdotetun monipolvisen soveltamisalasäännöksen (tiedonhallintalain 3 §:ään ehdotettu uusi 2 momentti) perusteella on sinällään pääteltävissä, että tiedonhallintalakiin ehdotettavaksi lisättävää uutta 4 a lukua ei sovellettaisi eduskunnan oikeusasiamiehen kanslian toimintaan. NIS2-direktiivissä säädetyt kyberturvallisuuteen liittyvät velvoitteet ja niiden noudattamisen valvonta julkishallinnon toimialalla eivät siten koskisi oikeusasiamiestä.

Sääntelytapa ei kuitenkaan ole kaikista selkein. Tulkintavaikeuksia aiheuttaa esimerkiksi ehdotetun 3 §:n 2 momentin viimeinen virke, jonka mukaan valvovan viranomaisen valvontatoimivaltuuksia ja tiedonsaanti- sekä tarkastusoikeutta (4 a luvun 18 h-18 l §:ää) ei sovellettaisi tasavallan presidentin kansliaan, valtioneuvoston oikeuskanslerin toimintaan eikä Kansaneläkelaitokseen. Vaikka

valtioneuvoston oikeuskansleria nimenomaisesti koskeva sääntely tiedonhallintalain luonnoksen mukaisesti ehdotetussa systematiikassa vaikuttaisi sinällään olevan perusteltu, herättää se tarpeettomasti kysymyksen miksi säännöksessä mainitaan vain oikeuskansleri ja toisen ylimmän laillisuusvalvojan, Eduskunnan oikeusasiamiehen toimintaa ei ole nimenomaisesti suljettu pois kyseisten säännösten soveltamisalasta.

Erityisesti tulkintaa vaikeuttaa se, että oikeusasiamiehen kanslian toiminta on nimenomaisesti suljettu voimassa olevan tiedonhallintalain 3 §:n 3 momentin (siirtyisi ehdotuksen mukaisesti 4 momentiksi) mukaisesti julkisen hallinnon tiedonhallintaa koskevan 3 luvun soveltamisalan ulkopuolelle.

Muiltakaan osin valittua soveltamisalan rajaussäännöstä ei voi pitää erityisen helppolukuisena ja sääntelyn selkiyttämistä olisi syytä harkita. Osa soveltamisalasäännöksen tulkintavaikeuksista voi aiheutua valitusta sääntelytavasta, jossa tiedonhallintalain sisälle tuotavaa NIS2-sääntelyä ehdotetaan sovellettavan rajatumpaan joukkoon kuin tiedonhallintalain tietoturvallisuuden tai sen valvonnan sääntelyä. Sääntelyn keskittämistä ehdotettuun lakiin kyberturvallisuuden riskienhallinnasta voisi olla esityksessä tarpeen vielä kerran harkita ja arvioida yhtenä toteuttamisvaihtoehtona.

Samalla voisi olla syytä arvioida onko luonnoksessa esitetyn 18 §:n 3 momentin mukaisessa tiedotusvelvollisuudessa merkittävästä kyberuhasta ja poikkeamasta joltain osin kyse sellaisesta valvonnasta, jota ei tulisi kohdistaa ylimpiin laillisuusvalvojiin (erityisesti velvoittaminen tiedottamaan merkittävästä poikkeamasta).

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

-

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

Hallituksen esitysluonnoksessa on arvioitu tarvetta laajentaa tiedonhallintalakiin sisältyvän turvallisuusluokitteluvelvollisuuden koskemaan uusia toimijoita. Luonnoksena nyt olevan Suomen Erillisverkot Oy:n lisäksi jatkovalmistelun yhteydessä voisi olla tarpeen selvittää onko luokitteluvelvoitetta tarpeen laajentaa myös muihin toimijoihin, kuten esimerkiksi eduskunnan kansliaan, joka on ottanut luokittelun oma-aloitteisesti käyttöön.

Råman Jari
Eduskunnan oikeusasiamiehen kanslia - Apulaisoikeusasiamies Maija Sakslin, esittelijänä kansliapäällikkö Jari Råman