Liikenne- ja viestintäministeriön lausunto perustuslakivaliokunnalle hallituksen esityksestä 57/2024 vp

Perustuslakivaliokunta on pyytänyt liikenne- ja viestintäministeriöltä lisäselvitystä koskien vireillä olevaa hallituksen esitystä eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (HE 57/2024 vp).

Valiokunta on pyytänyt ministeriöltä hallituksen esityksessä esitettyä seikkaperäisempää kirjallista selvitystä siitä, miten valvonta on tarkoitus käytännössä järjestää, kiinnittäen huomiota erityisesti siihen, joudutaanko, ja jos niin missä tilanteissa joudutaan, ottamaan selkoa luottamuksellisen viestin sisällöstä. Valiokunta pyysi lisäselvitystä myös sääntelyn soveltamisalasta eduskunnan virastojen osalta.

Liikenne- ja viestintäministeriö kiittää pyynnöstä ja esittää kunnioittavasti seuraavaa.

Valvonnan järjestäminen

NIS 2 -direktiivin 31(1) artiklan nojalla jäsenvaltioiden on varmistettava, että niiden toimivaltaiset viranomaiset valvovat tosiasiallisesti direktiivin noudattamista ja toteuttavat tarvittavat toimenpiteet sen varmistamiseksi. Direktiivin 31(2) artiklan mukaisesti jäsenvaltiot voivat sallia, että niiden toimivaltaiset viranomaiset asettavat valvontatoimenpiteitä etusijalle riskiperusteista lähestymistapaa soveltaen. Artiklat 31–33 sekä johdantokappaleet 122–128 ilmentävät direktiivin lähtökohtaa riskiperusteisesta valvonnasta. Direktiivi edellyttää, että valvova viranomainen kohdistaa ennakollista valvontaa keskeisiin toimijoihin, ja jälkikäteistä valvontaa muihin kuin keskeisiin toimijoihin.

Kyberturvallisuuslain mukaisten velvoitteiden valvonnasta säädettäisiin lain 4 luvussa. Valvovina viranomaisina eli NIS 2 -direktiivin tarkoittamina toimivaltaisina viranomaisina toimisivat 26 §:n 1 momentissa tarkoitetut viranomaiset. Valvontavastuu olisi momentissa säädetyllä tavalla jaettu toimialakohtaisesti viranomaisille. Pykälän 2 momentissa säädettäisiin valvovien viranomaisten yhteistyövelvoitteesta, mikä olisi merkityksellistä erityisesti sellaisessa tilanteessa, jossa toimija harjoittaa toimintaa useilla eri toimialoilla ja valvontatoimivaltaa olisi siten useammalla kuin yhdellä viranomaisella. Julkisen hallinnon tiedonhallinnasta annetun lain uutta 4 a lukua valvoisi Liikenne- ja viestintävirasto.

Edeltävän verkko- ja tietoturvadirektiivin eli NIS1-direktiivin mukaisten velvoitteiden valvonta on Suomessa järjestetty toimialakohtaisesti. Valvovina viranomaisina ovat toimineet Energiavirasto, Liikenne- ja viestintävirasto, Finanssivalvonta, Valvira sekä Etelä-Savon elinkeino-, liikenne- ja ympäristökeskus. Toimialakohtaista valvontaa esitetään jatkettavaksi. Lisäksi, direktiivin soveltamisalan laajentumisen johdosta, uusina viranomaisina NIS 2 -direktiiviin perustuvia velvoitteita valvoisivat toimialoillaan Turvallisuus- ja kemikaalivirasto, Ruokavirasto ja Lääkealan

turvallisuus- ja kehittämiskeskus. Esityksessä luvussa 5.1.4 arvioidaan valvontavastuun hajauttamisen vaihtoehtona valvonnan keskittämistä.

Kyberturvallisuuslain 27.1 §:n nojalla valvonta olisi kohdistettava keskeisiin toimijoihin. Keskeisiä toimijoita olisivat 27.2 §:n mukaisesti keskisuuren yrityksen kynnysarvot ylittävät toimijat, jotka harjoittavat lain liitteessä I tarkoitettua toimintaa. Kyberturvallisuuslain 27.1 §:n nojalla valvova viranomainen voisi kohdistaa valvontaa muuhun kuin keskeiseen toimijaan tilanteessa, jossa on perusteltua syytä epäillä, että toimija ei ole noudattanut lakia, sen nojalla annettuja määräyksiä tai NIS 2 -direktiivin nojalla annettuja säädöksiä. Perusteltu syy voisi ilmetä esimerkiksi julkisesti saatavilla olevista tiedoista, merkittävää poikkeamaa koskevasta ilmoituksesta tai muussa valvonnassa saadusta tiedosta. NIS 2 -direktiivin vähimmäisharmonisoinnin mukaisesti kyberturvallisuuslain ennakollinen valvonta kohdistuisi siten keskeisiin toimijoihin ja vain perustellusta syystä muuhun kuin keskeiseen toimijaan.

Kyberturvallisuuslain 27.3 §:n nojalla valvova viranomainen voisi asettaa sille kyberturvallisuuslaissa säädetyt tehtävät tärkeysjärjestykseen riskiperusteisesti. Valvonnan kohdistamisessa ja valvontatoimivaltuuksien käytöstä päättämisessä olisi otettava huomioon toimijan harjoittaman liitteessä I tai II tarkoitetun toiminnan laatu ja laajuus, tietojärjestelmän tai viestintäverkon merkitys liitteessä I tai II tarkoitetulle toiminnalle sekä 37 §:n mukaiset hallinnollisen seuraamusmaksun kokonaisarvioinnissa huomioitavat seikat.

Valvonta olisi tarkoitettu järjestettäväksi riskiperusteisesti sekä kyberturvallisuuslain että julkisen hallinnon tiedonhallinnasta annetun lain 4 a luvun osalta. Käytännössä myös valvontaan käytettävissä olevat resurssit edellyttäisivät valvonnan priorisoimista sääntelyn soveltamisalan laajuuden vuoksi. Valvova viranomainen voisi riskiperusteisesti kohdentaa valvontaa esimerkiksi yhteiskunnan toiminnan kannalta kriittisiin toimijoihin ja tietojärjestelmiin. Valvontaa voitaisiin kohdentaa esimerkiksi sellaisten toimialojen toimijoihin, joihin kohdistuvia hyökkäyksiä tapahtuu usein tai sellaisten toimialojen toimijoihin, joiden kybermaturiteetin taso on keskimääräistä matalampi. Valvontaa voitaisiin kohdentaa myös esimerkiksi tiettyyn ohjelmistoon tai haavoittuvuuteen liittyvällä perusteella taikka tunnettuun hyökkäysmenetelmään liittyvällä perusteella. Valvontaa voitaisiin kohdentaa myös esimerkiksi kansallisen kyberturvallisuusstrategian perusteella, laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelman perusteella, kyberturvallisuuslain 45 §:ssä tarkoitetun viranomaisten yhteistyön perusteella tai Euroopan unionin kyberturvallisuusvirasto ENISA:n julkaisemien suosituksien perusteella. Ehdotetun 27 §:n säännöskohtaisten perusteluiden nojalla kyberturvallisuusriskien arvioinnissa olisi otettava huomioon toimijoihin kohdistuvien kyberturvallisuusriskien laatu ja määrä, mahdollisesta poikkeamasta aiheutuvat vaikutukset yhteiskunnalle, toimijoiden yleisen kyberturvallisuusmaturiteetin laatu, valvontaviranomaisten käytettävissä olevat resurssit sekä yhteistyö muiden viranomaisten kanssa (HE 57/2024 vp, s. 193). Valvonta olisi siten suhteutettava toiminnan laatuun ja riskeihin.

Valvonnan tarkoituksena olisi kyberturvallisuuslain 26.1 §:n mukaisesti lain, sen nojalla annettujen määräysten ja NIS 2 –direktiivin nojalla annettujen säännösten noudattamisen valvonta. Käytännössä valvonta kohdistuisi velvoitteisiin kyberturvallisuutta koskevan riskienhallinnan järjestämisestä (7–10 §), merkittävistä poikkeamista ilmoittamisesta (11–15 §) ja toimijaluetteloon ilmoittautumisesta (41 §) (tiedonhallintalain vastaavat säännökset 18 a–d § ja 18 g §). Valvovan viranomaisen toimivaltuuksista säädettäisiin kyberturvallisuuslain 28–34 §:ssä ja tiedonhallintalain 4 a luvun 18 h–18 k §:ssä.

Valvovalla viranomaisella olisi 28 §:n nojalla oikeus saada toimijalta kyberturvallisuutta koskevien riskien hallintaa, riskienhallinnan toimintamallia, hallintatoimenpiteitä ja merkittävää poikkeamaa koskevat tiedot sekä muut edellä mainittuihin tietoihin välittömästi liittyvät tiedot, jotka ovat välttämättömiä kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen ja merkittävästä poikkeamasta ilmoittamisen ja raportoinnin valvontaa varten. Tiedonsaantioikeus koskisi myös välitystietoa, sijaintitietoa ja tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä edellä mainittua tarkoitusta varten. Lisäksi valvovalla viranomaisella olisi 29 §:n nojalla toimivalta suorittaa tarkastus toimijan muussa kuin pysyväisluonteiseen asumiseen tarkoitetussa tilassa tai viestintäverkossa ja tietojärjestelmässä. Valvova viranomainen voisi 31 §:n nojalla velvoittaa toimijaa määräajassa korjaamaan tai julkistamaan puutteita lain noudattamisessa taikka antaa toimijalle kirjallisen varoituksen. Valvova viranomainen voisi 30 §:n nojalla määrätä teetettäväksi kyberturvallisuuden riskienhallintaan kohdistuva turvallisuusauditointi sekä 32 §:n nojalla rajoittaa henkilön toimimista toimijan ylimmän johdon tehtävässä. Toimivaltuudet perustuvat NIS 2 -direktiivin 32 ja 33 artikloissa edellytettävään toimivaltuuksien laajuuteen valvonnassa.

Käytännössä riskiperusteisen ja oikeasuhtaisen valvonnan toteuttamisessa valvovan viranomaisen 28 §:n mukaisella tietojensaantioikeudella olisi keskeinen merkitys. Tietojensaantioikeuden avulla valvova viranomainen voisi hankkia tietoja siitä, miten toimija on arvioinut kyberturvallisuutta koskevia riskejä ja määrittänyt riskienhallintatoimenpiteitä, sekä arvioida toimenpiteiden oikeasuhtaisuutta riskeihin nähden. Tietopyyntö voisi kohdistua tyypillisesti esimerkiksi kyberturvallisuuden riskienhallinnan toimintamallia koskeviin tietoihin, riskiarviointia koskeviin tietoihin tai riskienhallintatoimenpiteiden määrittämistä ja toteuttamista koskeviin tietoihin. Valvova viranomainen voisi saatujen tietojen perusteella myös ohjata ja neuvoa toimijaa riskienhallinnan kehittämiseksi. Erityisesti sääntelyn soveltamisen alkuvaiheessa viranomaisen ohjauksella ja neuvonnalla olisi keskeinen merkitys toimijoille lain noudattamisen kannalta.

Luottamuksellisen viestin sisällöstä selon ottaminen

Toimijoihin kohdistettavassa ennakollisessa valvonnassa riskienhallinnan toteuttamisesta tai merkittävien poikkeamien ilmoittamisesta ei lähtökohtaisesti olisi tarvetta käsitellä luottamuksellista viestintää koskevia tietoja. Liikenne- ja viestintäministeriön alustavan arvion mukaan olisi hyvin poikkeuksellista, että ennakollisessa valvonnassa olisi välttämätön tarve saada tietoja haitallisen tietokoneohjelman tai käskyn sisältävän viestin sisällöstä. Lähtökohtaisesti tällaista tarvetta ei ole tunnistettavissa valvonnan toteuttamiseksi, sillä edellä kuvatulla tavalla tietopyyntö ennakollisessa valvonnassa kohdistuisi ennakoitavasti riskiarviointia koskeviin tietoihin ja riskienhallintatoimenpiteiden määrittämistä ja toteuttamista koskeviin tietoihin.

Sen sijaan merkittävää poikkeamaa koskevan ilmoituksen käsittelyssä tai tapahtuneen poikkeaman jälkeen toimijaan kohdistettavassa valvonnassa on ennakoitavissa, että valvovalle viranomaiselle voi syntyä säännöllisesti tarve käsitellä *välitystietoja*, sillä välitystietoja voisi sisältyä esimerkiksi poikkeaman teknisiin vaarantumisindikaattoreihin. Liikenne- ja viestintäministeriön alustavan arvion mukaan on myös mahdollista, että merkittävän poikkeaman tapahduttua voisi yksittäistapauksessa syntyä välttämätön tarve käsitellä tietoa haitallisen tietokoneohjelman tai käskyn sisältävän *viestin sisällöstä*. Tarpeen syntyminen olisi kuitenkin poikkeuksellista ja riippuisi muun ohella merkittävän poikkeaman teknisestä toteutumistavasta sekä mahdollisuuksista selvittää poikkeaman teknisiä syitä muilla tavoin kuin haitallisen tietokoneohjelman tai käskyn sisältävän viestin sisällöstä selkoa ottamalla. Liikenne- ja viestintäministeriön alustavan arvion mukaan ei ole ennakoitavissa, että toimijoihin kohdistettavassa jälkikäteisessä valvonnassa olisi

säännöllisesti välttämätön tarve käsitellä tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, eikä ensimmäisen lakiehdotuksen 28 §:ssä tai toisen lakiehdotuksen 18 i §:ssä ehdotettua toimivaltuutta olisi tarkoitettu säännölliseen tai yleiseen haitallista tietokoneohjelmaa tai käskyä koskevan tiedon käsittelyyn.

Ehdotetun kyberturvallisuuslain 28.2 §:n mukainen tiedonsaantioikeus kohdistuu määritelmällisesti haitallisen tietokoneohjelman tai käskyn sisältäviin viesteihin. Tiedonsaantioikeus ei siten kohdistuisi muuhun sähköiseen viestintään tai sähköiseen viestiin kuin sellaiseen, joka sisältää haitallisen tietokoneohjelman tai käskyn. Jos perustuslakivaliokunta katsoisi hallituksen esityksessä perusteltua tulkintaa vastaavalla tavalla, että tällainen haitallinen viestintä ei nauttisi perustuslain 10.2 §:n mukaista perusoikeussuojaa, valvovien viranomaisten tiedonsaantioikeus ei tällöin kohdistuisi perusoikeussuojaa nauttivan luottamuksellisen viestin sisältöön. Perustuslain 10.2 §:n mukaista perusoikeussuojaa nauttivan luottamuksellisen viestin sisältö jäisi tässä tilanteessa tiedonsaantivaltuuden ulkopuolelle.

Valvovan viranomaisen valvontatoimintaan liittyvä 28.2 §:n mukainen tiedonsaantitarve voisi kohdistua haitallisen tietokoneohjelman tai käskyn sisältävään haitalliseen viestiin esimerkiksi silloin, jos merkittävä poikkeama olisi aiheutunut ehdotetun kyberturvallisuuslain soveltamisen piiriin kuuluvassa toimijassa työskentelevälle työntekijälle ulkopuolisen lähettämästä viestistä. Tiedonsaantioikeudella valvova viranomainen voisi pyytää kyberhyökkäyksen ensimmäisenä sisäänpääsykeinona toimineen ja merkittävään poikkeamaan johtaneen haitallisen viestin, teknisen komennon tai käskyn sen haitallisen sisällön arvioimiseksi kyberturvallisuuslain riskienhallintavelvoitteiden noudattamisen näkökulmasta. Jos esimerkiksi haitallisessa viestissä oleva liite sisältäisi tunnettua haavoittuvuutta hyväksikäyttävän haittaohjelman, valvova viranomainen voisi arvioida, onko toimija noudattanut asianmukaisesti kyberturvallisuuden riskienhallintavelvoitteitaan pyrkimällä estämään tunnetun haavoittuvuuden hyväksikäytön, esimerkiksi asentamalla oikea-aikaisesti haavoittuvuuden korjaava ohjelmistopäivitys. Haitallisen tietokoneohjelman tai käskyn sisältävää viestiä koskeva tiedonsaantioikeus mahdollistaisi myös valvovalle viranomaiselle itselleen sen, että se voi tarvittaessa tehdä poikkeamiin liittyvää teknistä analyysiä ja arvioida poikkeamien juurisyitä itsenäisesti, jolloin valvova viranomainen ei olisi tältä osin vain toimijoiden ilmoittamien tietojen ja analyysin varassa arvioidessaan valvonnan ja riskienhallinnan asianmukaisuuden kannalta merkityksellisiä kyberturvallisuutta koskevia riskejä toimialalla. Ministeriön alustavan arvion mukaan valvovalle viranomaiselle merkityksellisintä olisi mahdollisuus saada tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä silloin, jos välttämätön tarve kohdistuu viestin teknisiin tietoihin tai sellaiseen koneiden välisiin teknisiin tietoihin, komentoihin tai käskyihin, jotka olisivat tulkittavissa viesteiksi tai sähköiseksi viestinnäksi, mutta eivät sisällä ihmisten välistä semanttista viestintää.

Oikeus saada tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestin sisällöstä rajoittuisi välttämättömään, mikä voisi tapauksen mukaan tarkoittaa myös sitä, että tieto viestin sisällöstä luovutettaisiin vain osittain eli siltä osin kuin se on valvontaviranomaiselle välttämätöntä edellä mainittujen valvontatehtävien kannalta. Vaikka ehdotuksen mukainen tiedonsaantioikeus voisi kohdistua myös esimerkiksi haitallisen tietokoneohjelman tai käskyn sähköpostiviestin tekstiosaan, rajautuisi tiedonsaantioikeuden piiristä pois viestin sellainen sisältö, jolla ei ole valvonnan kannalta merkitystä. Esimerkiksi tilanteessa, jossa muutoin toivottuun sähköpostiviestiin on lähettäjän tietokoneen haittaohjelmatartunnan takia tahattomasti sisältynyt haitallinen liite, ei valvovalle viranomaiselle olisi välttämätöntä saada tietoa tästä lähettäjän tuottamasta viestin sisällöstä, vaan tietopyyntö olisi rajattava tapauksen mukaan esimerkiksi kyseiseen haitalliseen liitetiedostoon

(mahdollisesti välttämättömien välitystietojen lisäksi). Sähköpostiviestin sisältökenttä voisi sen sijaan olla valvontaviranomaiselle välttämätön esimerkiksi silloin, kun kyseessä olisi esimerkiksi nimenomaan haittaohjelmien levittämiseen tai käyttäjätunnusten kalasteluun tarkoitettu, tyypillisesti koneellisesti tuotettu viesti, jolloin kyseinen sisältö liittyy suoraan viestin haitallisuuteen; sisältöä voidaan tällöin hyödyntää myös vastaavien muiden haitallisten viestien tunnistamisessa ja torjumisessa. Niin ikään ei ole ennakoitavissa, että haitallisen tietokoneohjelman automaattisesti käyttäjän tililtä lähettämien viestien tai niihin saatujen vastausten sisällön tarkastelu olisi välttämätöntä tiedonsaantioikeudelle laissa säädettyjen tarkoituksien kannalta.

Mikäli perustuslakivaliokunta katsoisi myös haitallisen tietokoneohjelman tai käskyn sisältävän viestin nauttivan perustuslain 10.2 §:n mukaista perusoikeussuojaa, ehdotetussa kyberturvallisuuslain 28.2 §:ssä ja julkisen hallinnon tiedonhallinnasta annetun lain 18 i.2 §:ssä olisi kyse siitä, että lailla säädettäisiin rajoituksista viestin salaisuuteen perustuslain 10.4 §:n mukaisesti. Liikenne- ja viestintäministeriö kuitenkin arvioi hallituksen esityksessä (s. 249–251) perustellulla tavoin, ettei haitallisen tietokoneohjelman tai käskyn sisältävä viesti niine reunaehtoineen, joita esitetyn tiedonsaantioikeuden käyttämiseen liittyisi, nauti mainittua perusoikeussuojaa.

Liikenne- ja viestintäviraston sekä tietosuojavaltuutetun voimassa olevaan lakiin perustuva toimivaltuus saada välitystietoja, sijaintitietoja tai viestejä

Liikenne- ja viestintäministeriö tuo vielä perustuslakivaliokunnan kysymykseen liittyen kunnioittavasti esiin, että voimassa olevasta lainsäädännössä lähin ensimmäisen lakiehdotuksen 28 §:n 2 momenttia ja toisen lakiehdotuksen 18 i §:n 2 momenttia vastaava säännös sisältyy sähköisen viestinnän palveluista annetun lain 316 §:n 2 momenttiin. Sähköisen viestinnän palveluista annetun lain 316.2 §:ssä säädetään Liikenne- ja viestintäviraston sekä tietosuojavaltuutetun oikeudesta saada salassapitosäännösten tai muiden tietojen luovuttamista koskevien rajoitusten estämättä välitystiedot, sijaintitiedot ja viestit, jos ne ovat tarpeen lain VI osassa tarkoitettua käsittelyä, ja 24 luvussa tarkoitettua evästeiden käyttöä tai suoramarkkinointia koskevien säännösten valvomiseksi taikka merkittävien tietoturvaloukkausten tai -uhkien selvittämiseksi. Edellytyksenä on lisäksi, että Liikenne- ja viestintäviraston tai tietosuojavaltuutetun arvion mukaan on syytä epäillä momentissa tarkoitetun rikoksen tunnusmerkistön täyttyvän.

Liikenne- ja viestintäministeriö tuo kunnioittavasti esiin, että sähköisen viestinnän palveluista annetun lain 316 §:n 2 momentti on säädetty perustuslakivaliokunnan myötävaikutuksella. Alkuperäisessä muodossaan säännös sisältyi hallituksen esitykseen eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi (HE 125/2003 vp). Perustuslakivaliokunnan lausunnon mukaan sääntely ei muodostunut ongelmalliseksi perustuslain 10 §:n säännösten kannalta (PeVL 9/2004 vp). Myös säännöksen myöhempi, teknisluontoinen muutos (HE 48/2008 vp) samoin kuin hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta (HE 221/2013 vp) on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 29/2008 vp ja PeVL 18/2014). Perustuslakivaliokunta ei tällöin lausunut esityksistä erikseen kyseisiltä osin.

Sähköisen viestinnän palveluista annetun lain 316 §:n 2 momenttiin nähden 1. ja 2. lakiehdotuksissa esitetyt säännökset ovat rajatumpia. Ehdotettu valvovien viranomaisten tiedonsaantioikeus olisi rajattu viestinnän sisällön osalta ainoastaan "tietoon haitallisen

tietokoneohjelman tai käskyn sisältävästä viestistä". Lisäksi ehdotetun 28.2 §:n mukainen tiedonsaantioikeus on sidottu "välttämättömyyteen", kun voimassa olevassa sähköisen viestinnän palveluista annetun lain 316.2 §:ssä on kyse "tarpeellisista" tiedoista. Perustuslakivaliokunnan myötävaikutuksella säädetyssä muussa lainsäädännössä säädetään siis nykyisinkin viranomaisen oikeudesta saada haittaohjelmaan liittyviä tietoja myös viestin sisällöstä vastaavien viestinnän luottamuksellisuuden turvaamiseen liittyvien oikeushyvien turvaamiseksi.

Soveltamisala eduskunnan virastojen osalta

NIS 2 -direktiivin 2 artiklassa säädetään sen vähimmäissoveltamisalasta julkishallinnon toimijoihin. Artiklan 2 kohdan f alakohdan mukaan direktiiviä sovelletaan, kun toimija on julkishallinnon toimija,

i) jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt keskustason julkishallinnon toimijaksi;

ii) jonka jäsenvaltio on kansallisen lainsäädäntönsä mukaisesti määritellyt aluetason julkishallinnon toimijaksi ja joka riskiperusteisen arvioinnin perusteella tarjoaa palveluja, joiden häiriintymisellä voisi olla merkittävä vaikutus yhteiskunnan tai talouden kriittisiin toimintoihin.

Direktiivin 6 artiklan 35 kohdassa määritellään julkishallinnon toimija. Sillä tarkoitetaan jäsenvaltiossa kansallisen lainsäädännön mukaisesti julkishallinnon toimijaksi tunnustettua toimijaa, lukuun ottamatta oikeuslaitosta, parlamentteja ja keskuspankkeja, joka täyttää seuraavat kriteerit:

a) se on perustettu tyydyttämään yleisen edun mukaisia tarpeita, eikä sillä ole teollista tai kaupallista luonnetta;

b) se on oikeushenkilö tai sillä on lain nojalla oikeus toimia toisen sellaisen toimijan puolesta, joka on oikeushenkilö;

c) sitä rahoittavat pääosin valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset, sen johto on näiden viranomaisten tai laitosten valvonnan alainen taikka valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset nimittävät yli puolet sen hallinto-, johto- tai valvontaelimen jäsenistä;

d) sillä on valtuudet osoittaa luonnollisille henkilöille tai oikeushenkilöille hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat näiden oikeuksiin henkilöiden, tavaroiden, palvelujen tai pääoman rajatylittävässä liikkuvuudessa.

NIS 2 -direktiivin 2 artiklan 7 kohdan mukaan direktiiviä ei sovelleta julkishallinnon toimijoihin, jotka harjoittavat toimintaa kansallisen turvallisuuden, yleisen turvallisuuden, puolustuksen tai lainvalvonnan alalla, mukaan lukien rikosten ennalta estäminen, tutkiminen, paljastaminen ja rikoksiin liittyvät syytetoimet. – Ehdotuksen soveltamisalaa on tällä perusteella rajattu, mutta poikkeus ei koske eduskunnan virastoja.

Keskustason julkishallinnon toimijan määrittely kansallisesti

NIS 2 -direktiivi ei sisällä yllä mainitun 2 artiklan 7 kohdan lisäksi sellaista kansallista liikkumavaraa, jonka perusteella keskustason julkishallinnon toimijoita voitaisiin kansallisin ratkaisuin rajata pois sääntelyn soveltamisalasta. Kansallisen liikkumavaran niukkuuden johdosta direktiivin soveltamisalan määrittämisessä keskeiseksi muodostuu kysymys siitä, miten yllä viitattua keskustason julkishallinnon toimijan käsitettä tulkitaan.

Yllä todetusti NIS 2 -direktiivi viittaa kuitenkin kansalliseen lainsäädäntöön keskustason julkishallinnon toimijoiden määrittämiseksi. NIS 2 -direktiivin johdanto-osan perustelukappaleen 8 mukaan direktiivin on tarkoitus kattaa laajasti julkishallinnon toimijat ja direktiivin soveltamisalan ulkopuolelle jätettäviä julkishallinnon aloja tulkitaan suppeasti. Kun tämä otetaan huomioon, kyse ei ole siitä, että jäsenvaltio voisi NIS 2 -direktiivin soveltamisalan määrittämiseksi vapaasti valita soveltamisalaan tulevat keskustason julkishallinnon toimijat vaan siitä, miten kyseisten toimijoiden asema jäsenvaltion sisäisessä oikeudessa määräytyy. Muu tulkinta merkitsisi, että direktiivin 2(7) artiklan mukainen poikkeus samoin kuin julkishallinnon toimijan määritelmään sisältyvä oikeuslaitosta, parlamentteja ja keskuspankkeja koskeva rajaus menettäisi merkityksensä.

Direktiivin soveltamisalaa määrittävä keskustason julkishallinnon toimijan käsite ei suoraan vastaa Suomen valtiosääntöoikeudellisia tai muussa kansallisessa lainsäädännössä käytettyjä käsitteitä julkisesta hallinnosta. Tästä syystä valmistelussa on jäljempänä tarkemmin kuvatusti haettu direktiivin julkishallintoa koskevan vähimmäissoveltamisalan määrittämiseksi suuntaviivoja siitä, miten kansallisia hallinnon yleislakeja sovelletaan viranomaisiin.

Tiedonhallintalain soveltaminen perustuu julkisuuslain viranomaisen määritelmään. Ehdotetun 4 a luvun soveltamisalan määrittelyssä on otettu huomioon myös se, kuinka tietosuojalakia sovelletaan viranomaisiin. Hallinnon yleislakeja ja tiedonhallintalakia sovelletaan myös eduskunnan virastoihin, minkä on katsottu merkitsevän sitä, että kyse on keskustason julkishallinnon toimijasta. Hallituksen esityksessä todetun ohella voidaan ratkaisua verrata myös julkisia hankintoja koskevan lainsäädännön soveltamiseen eduskunnan virastoihin.

Ehdotuksen soveltamisala julkishallinnon toimijoiden osalta

Kuten hallituksen esityksessä (s. 269) todetaan, ehdotettua tiedonhallintalain 4 a luvun NIS 2 -direktiiviin perustuvaa sääntelyä sovellettaisiin lähtökohtaisesti julkisuuslain 4 §:n 1 momentissa tarkoitettuihin viranomaisiin eli myös eduskunnan virastoihin sekä valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen toimintaan. Tiedonhallintalain 3 §:n 3 momentissa suljettaisiin tietyt viranomaiset pois uuden 4 a luvun soveltamisalasta, mutta eduskunnan virastoja ei mainittaisi luettelossa.

Tämän muistion lopussa käsitellään ehdotetun kyberturvallisuuslain soveltamista erikseen.

Eduskunnan valtiopäivätoiminta

NIS 2 -direktiivin 6 artiklan 35 kohdan mukaisen julkishallinnon toimijan käsitteen ulkopuolelle jäävät kansalliset oikeuslaitokset, parlamentit ja keskuspankit.

Esityksessä on omaksuttu käsitys, jonka mukaan käsitteellä ”parlamentti” viitataan kansanedustuslaitoksen toimintaan, eli Suomessa eduskunnan valtiopäivätoimintaan. Näin ollen myöskään tiedonhallintalakiin ehdotettu 4 a luku ei koskisi eduskunnan valtiopäivätoimintaa (hallituksen esityksen s. 269).

Eduskunnan virastojen on katsottu jäävän seuraavassa todetuin perustein parlamentin käsitteen ulkopuolelle.

Siltä osin kuin eduskunnan virastojen tietojärjestelmät ovat yhteisiä valtiopäivätoimintaan järjestettävien tietojärjestelmien kanssa, ministeriö pitää direktiivissä sallitun liikkumavaran puitteissa mahdollisena valvontaviranomaisen valvontatoimivallan rajaamista eduskunnan virastojen tietojärjestelmien osalta, jos perustuslakivaliokunta katsoo, että eduskunnan valtiopäivätoiminnan perustuslaillinen asema sitä edellyttää.

Esityksen valmistelu ja parlamentteja koskevan poikkeuksen ala

Hallituksen esityksen luonnoksessa oli vielä lausuntovaiheessa omaksuttu tulkinta, jonka mukaan ”parlamentin” käsitteen johdosta olisi voitu soveltamisalan piiristä sulkea pois paitsi eduskunnan valtiopäivätoiminta myös eduskunnan virastot.[1]

Lausuntoyhteenvedossa[2] kuvataan asiaa koskevien lausuntojen keskeiset huomiot (s. 15). Vaikka eduskunnan kanslia piti lausunnossaan eduskunnan virastot poissulkevaa soveltamisalarajausta asianmukaisena, muutettiin ratkaisua oikeuskanslerinviraston lausunnon johdosta. Oikeuskanslerinviraston lausunnon mukaan direktiivin 6 artiklan 35 kohta ei edellyttäisi jättämään eduskunnan virastoja ja eduskunnan oikeusasiamiestä uuden 4 a luvun soveltamisalan ulkopuolelle, sillä direktiivissä käytetyllä käsitteellä ”parlamentti” viitataan kansanedustuslaitoksen toimintaan, Suomessa eduskunnan valtiopäivätoimintaan. Eduskunnan virastot on lausunnon mukaan yleensä kansallisessa lainsäädännössä säädetty yleislakien piiriin kuuluviksi. Oikeuskanslerinvirasto kehotti jatkovalmistelussa tarkistamaan tiedonhallintalain 3 §:n säännöksiä näiltä osin.[3]

Kuten hallituksen esityksessä todetaan (s. 136), tiedonhallintalain uuden 4 a luvun soveltamisalaa koskevaa 3 §:ää on lausuntopalautteen johdosta muotoiltu uudelleen ja eduskunnan virastojen osalta sääntelyä muutettiin jatkovalmisteluvaiheessa siten, että mainitut virastot kuuluisivat soveltamisalaan. Oikeuskanslerinviraston esittämien näkökohtien johdosta on siten katsottu, että direktiivin ulkopuolelle jää eduskunnan valtiopäivätoiminta, kun taas eduskunnan virastot eivät kuulu parlamentteja koskevan soveltamisalapoikkeuksen alaan.

Jatkovalmistelun aikana tästä muutoksesta käytiin keskustelu valtiovarainministeriön ja eduskunnan virastojen välillä. Esitykseen myös lisättiin eräiden valtioelinten ja viranomaisten asemaa koskeva jakso 12.9. Samoin lisättiin maininta siitä, että muun muassa tästä syystä hallitus pitää suotavana, että perustuslakivaliokunta antaisi lausunnon ehdotuksesta näiden valtioelinten aseman kannalta (s. 272).

Ehdotuksen vertailu muuhun eduskunnan virastoja koskevaan lainsäädäntöön

Seuraavassa tuodaan esiin julkishallintoa koskevaa sääntelyä, jota sovelletaan eduskunnan virastoihin. Julkisten hankintojen sääntelyn kohdalla eduskunnan virastoja on myös pidetty

[1] Luonnos hallituksen esitykseksi, s. 157, https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?proposalId=4433cf2a-00ca-412e-8f47-20c55031b8dd&attachmentId=21084.
[2] Lausuntoyhteenveto, https://api.hankeikkuna.fi/asiakirjat/2b11d230-a4ff-47be-89f9-29e396f2c7bf/03587ba9-674e-4575-90f5-e917ddf14e40/MUISTIO_20240515124812.pdf.
[3] Oikeuskanslerinviraston lausunto, https://api.hankeikkuna.fi/asiakirjat/2b11d230-a4ff-47be-89f9-29e396f2c7bf/1f218244-10e4-4379-813e-9f0deeb6c830/LAUSUNTO_20231201120434.PDF.

nimenomaan keskushallinnon viranomaisina, mikä voitaneen rinnastaa NIS 2 -direktiivissä tarkoitettuihin keskustason julkishallinnon toimijoihin.

- Henkilötietojen suoja

Ehdotuksen mukainen ratkaisu, jonka mukaan eduskunnan virastot olisivat sen soveltamisalassa, vastaa tietosuojalain soveltamisalaa.

Eduskunnan valtiopäivätoiminta on perustuslakivaliokunnan kannan mukaisesti (PeVL 14/2018 vp) rajattu tietosuojalain soveltamisalan ulkopuolelle (tietosuojalaki 2 § 2 mom.). Eduskunnan virastot kuuluvat muutoin tietosuojalain soveltamisalaan.

NIS 2 -direktiivin ja EU:n yleisen tietosuoja-asetuksen soveltamisaloissa on kuitenkin selvä ero siinä, että direktiivistä poiketen tietosuoja-asetus ei sulje parlamentteja sen soveltamisalan ulkopuolelle. Euroopan unionin tuomioistuin (EUT) on oikeuskäytännössään omaksunut suppean tulkinnan tietosuoja-asetuksen soveltamisalan ulkopuolelle jäävästä toiminnasta (tuomio 9.7.2020, C-272/19, Land Hessen, 74 kohta). Lisäksi EUT on tulkinnut tietosuoja-asetuksen sisältämää kansallista turvallisuutta koskevaa poikkeusta soveltamisalasta kapeasti. Tänä vuonna antamassaan ratkaisussa EUT totesi, että yleistä tietosuoja-asetusta sovelletaan lähtökohtaisesti myös parlamentin toimeenpanoa koskevaa valvontavaltaansa käyttäessään perustaman tutkintavaliokunnan toimintaan (tuomio 16.1.2024 (suuri jaosto) C-33/221, Österreichische Datenschutzbehörde, 40–42 ja 50–51 kohta). Säädösten soveltamisalan eroista johtuen näistä ratkaisuista ei voi suoraan päätellä, mitä ”parlamentti” käsitteenä kattaa NIS 2 -direktiivissä, mutta lähtökohtaisesti unionin soveltamisalan poikkeuksia tulkitaan suppeasti.

- Hallinnon yleislait

Kuten ehdotuksessa todetaan, perustuslakivaliokunta on todennut tietosuojalain hallituksen esityksestä antamassaan lausunnossa PeVL 14/2018 vp, että lähtökohtaista estettä ei ole sille, että hallintoa koskevat yleislait ulotetaan koskemaan eduskunnan virastoja (hallituksen esitys, s. 269). Kuten edellä tuotiin esiin, eduskunnan virastot onkin yleensä kansallisessa lainsäädännössä säädetty hallinnon yleislakien piiriin kuuluviksi. Tietosuojalakiehdotusta koskevassa lausunnossaan perustuslakivaliokunta katsoi, että sen sijaan valtiopäivätoiminnan rajaaminen ehdotuksen soveltamisalan ulkopuolelle oli edellytyksenä sille, että lakiehdotus voitiin käsitellä tavallisen lain säätämisjärjestyksessä (PeVL 14/2018 vp, s. 11).

Julkisuuslain 4 §:n 1 momentin 6 kohdan mukaisesti viranomaisilla, joihin lakia sovelletaan, tarkoitetaan myös eduskunnan virastoja ja laitoksia. Julkisuuslaissa eduskunnan virastoilla ja laitoksilla on tarkoitettu samaa kuin eduskunnan virkamiehistä annetussa laissa (1197/2003). Lain 2 §:n 2 momentin mukaan eduskunnan virastoja ovat eduskunnan kanslia ja eduskunnan oikeusasiamiehen kanslia sekä eduskunnan yhteydessä olevat valtiontalouden tarkastusvirasto ja kansainvälisten suhteiden ja Euroopan unionin asioiden tutkimuslaitos, joka käyttää nimeä Ulkopoliittinen instituutti.

Julkisuuslakia ei sovelleta eduskunnan eikä sen toimielimien toimintaan, vaan niissä julkisuus määräytyy perustuslain ja eduskunnan työjärjestyksen mukaan. Julkisuuslaki ei siten koske eduskunnan täysistunnon ja valiokuntien toimintaa. (Olli Mäenpää: Julkisuusperiaate, Helsinki 2020, s. 135.)

- Julkiset hankinnat

EU:n hankintadirektiivissä (2014/24/EU) käytetään ”keskushallinnon viranomaisen” käsitettä, joka vaikuttaa sovellettaviin hankintojen kynnysarvoihin. Hankintadirektiivissä keskushallinnon viranomaisilla tarkoitetaan direktiivin liitteessä I mainittuja hankintaviranomaisia ja, jos kansallisella tasolla on tehty korjauksia tai muutoksia, niiden tilalle tulleita yksikköjä. Liitteessä mainitaan valtiontalouden tarkastusvirasto mutta ei muita eduskunnan virastoja. Liitteen luettelo on kuitenkin ohjeellinen, koska tosiasiallinen hankintayksikön toiminnan luonne on ratkaiseva harkittaessa sitä, onko kyseessä valtion keskushallintoviranomainen hankintadirektiivin ja hankintalain tarkoittamalla tavalla (HE 108/2016 vp).

Hankintalain esitöissä (HE 108/2016 vp) todetaankin, että ”[v]altion keskushallintoviranomaisina pidetään muun muassa valtioneuvostoa, ministeriöitä, ministeriöiden välittömään alaisuuteen tai niiden hallinnonalalle muuten kuuluvia virastoja, laitoksia ja muita toimielimiä sekä eduskunnan alaisuuteen kuuluvia virastoja, laitoksia ja muita toimielimiä sekä tuomioistuimia.”

Ehdotus on siten soveltamisalaratkaisun kannalta linjassa hankintalainsäädännön soveltamisen ja kansallisen tulkinnan kanssa. Vaikka hankintadirektiivin ja NIS 2 -direktiivin käsitteistöissä on eroja, lienee perusteltua tulkita keskustason julkishallinnon toimijan (public administration entity of central government) käsitettä keskushallinnon alan suhteen lähtökohtaisesti samoin kuin hankintalainsäädännön valtion keskushallinnon viranomaisen (central government authority) käsitettä. NIS 2 -direktiivin mukaiseen käsitteeseen sisältyy kuitenkin myös muita osatekijöitä, joita käsitellään jäljempänä.

Julkishallinnon toimijan määritelmän muut osatekijät

Edellä todetusti direktiivin määritelmä edellyttää, että julkishallinnon toimija täyttää seuraavat kriteerit: a) se on perustettu tyydyttämään yleisen edun mukaisia tarpeita, eikä sillä ole teollista tai kaupallista luonnetta; b) se on oikeushenkilö tai sillä on lain nojalla oikeus toimia toisen sellaisen toimijan puolesta, joka on oikeushenkilö; c) sitä rahoittavat pääosin valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset, sen johto on näiden viranomaisten tai laitosten valvonnan alainen taikka valtio, alueviranomaiset tai muut julkisoikeudelliset laitokset nimittävät yli puolet sen hallinto-, johto- tai valvontaelimen jäsenistä; d) sillä on valtuudet osoittaa luonnollisille henkilöille tai oikeushenkilöille hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat näiden oikeuksiin henkilöiden, tavaroiden, palvelujen tai pääoman rajatylittävässä liikkuvuudessa.

Eduskunnan virastot täyttävät ilmeisesti kriteerit a–c. NIS 2 -direktiivin julkishallinnon toimijan määritelmään sisältyvä luettelo on kohdiltaan a–c olennaisesti sama kuin EU:n hankintadirektiivin mukaisen julkisoikeudellisen laitoksen määritelmän osatekijät.

Niiden lisäksi NIS 2 -direktiivissä edellytetään d luetelmakohdassa, että toimijalla on ”valtuudet osoittaa luonnollisille henkilöille tai oikeushenkilöille hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat näiden oikeuksiin henkilöiden, tavaroiden, palvelujen tai pääoman rajatylittävässä liikkuvuudessa”. Tämän kriteerin täyttyminen eduskunnan virastojen osalta on tulkinnanvaraisempaa kuin kriteerien a–c. Kuten Ruotsin NIS 2 -direktiivin täytäntöönpanoa koskevassa selvityksessä on katsottu, voidaan kriteeriä itsessään pitää epäselvänä.[4]

Kun otetaan huomioon direktiivin tavoitteena oleva soveltamisalan laajentaminen NIS1-direktiivin nähden, ei vaikuta tarkoituksenmukaiselta pyrkiä tulkitsemaan määritelmää suppeasti. Valmistelun

[4] Nya regler om cybersäkerhet, SOU 2024:18, s. 130, https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2024/03/sou-202418/.

aikana lähtökohtana on pidetty, että kriteerin voidaan olettaa täyttyvän, jos toimijalla on toimivalta tehdä hallintopäätöksiä, joilla on vaikutusta päätöksen kohteen oikeuteen, velvollisuuteen tai etuun. Näyttää siltä, että ainakin hankintalainsäädännön puitteissa (julkiset hankinnat) myös eduskunnan virastoissa tehdään tai voidaan tehdä hallinnollisia tai sääntelyyn liittyviä päätöksiä, jotka vaikuttavat henkilöiden oikeuksiin tavaroiden ja palvelujen rajatylittävässä liikkuvuudessa. Näin ollen on perusteltua katsoa, että myös kriteeri d täyttyisi eduskunnan virastojen kohdalla.

Kaiken yllä esitetyn perusteella ministeriö arvioi, että eduskunnan virastojen voitaisiin tulkita jäävän NIS 2 -direktiivin velvoittavan vähimmäissoveltamisalan ulkopuolelle vain seuraavissa tapauksissa:

a) eduskunnan virastoilla ei yllä olevasta arviosta poiketen katsottaisi olevan d luetelmakohdan mukaista päätösvaltaa tai

b) erotuksena hankintalakiin ja muihin hallinnon yleislakeihin eduskunnan virastoja ei pidettäisikään NIS 2 -direktiivin kontekstissa keskustason julkishallinnon toimijoina.

Kuvatun tulkinnan tapahtuessa eduskunnan alainen virasto ei siten täyttäisi NIS 2 -direktiivin soveltamisalaa määrittävää (keskustason) julkishallinnon toimijan määritelmää. Muussa tapauksessa ministeriön arvio on, että asiaan ei liity direktiiviin sisältyvää kansallista liikkumavaraa.

Ruotsin selvityksessä ehdotettu soveltamisalaratkaisu

Ruotsin selvityksessä SOU 2024:18 on päädytty esittämään toisenlaista ratkaisua Ruotsin eduskunnan virastojen kannalta. Selvityksessä ehdotetaan suljettavaksi ehdotettavan lain soveltamisalasta eduskunnan alaiset viranomaiset (Riksrevisionen, Riksdagens ombudsmän, Sveriges Riksbank, Riksdagsförvaltningen), kun taas soveltamisalaan kuuluisivat hallituksen (regeringen) ohjauksen alaiset viranomaiset (s. 128–129 ja 365–366). Suomalainen lähin vastine tälle vaikuttaisi olevan jako valtioneuvoston alaiseen hallintoon erotuksena eduskunnan virastoista. Tämä saattaa johtua siitä, että direktiivien kieliversioissa on eroavaisuuksia. Ruotsinkielinen käännös direktiivistä on jossain määrin erilainen kuin suomenkielinen, joka käyttää hallitukseen viittaavan käsitteen sijasta julkishallinnon käsitettä. Ruotsinkielisessä direktiivin toisinnossa liitteen I 10 kohta kuuluu seuraavasti: ”Offentliga förvaltningsentiteter hos nationella regeringar såsom de definieras av en medlemsstat i enlighet med nationell rätt.”[5] Suomenkielisessä: ”Keskustason julkishallinnon toimijat, sellaisina kuin jäsenvaltio on ne kansallisen lainsäädännön mukaisesti määrittänyt.” Englanninkielisessä puolestaan seuraavasti: “Public administration entities of central governments as defined by a Member State in accordance with national law.” Ranskankielisessä toisinnossa taas käytetään käsitettä “pouvoirs publics centraux”.

Ruotsin hallituksen esitystä ei ole vielä saatavilla, joten on epävarmaa, kuinka Ruotsissa lopulta tulkitaan NIS 2 -direktiiviä eduskunnan virastojen osalta. Muiden verrokkimaiden ratkaisuista ei ole tätä taustoitusta laadittaessa ollut käytettävissä tietoja.

Riippumatta siitä, miten direktiivin mukaista parlamentin käsitettä olisi tulkittava, keskushallinnon toimijoiden määräytyminen siis tapahtuu kansallisen lainsäädännön mukaisesti. Aiempana todetusti, vaikka myös hankintadirektiivin kohdalla käytetään central government -käsitettä, ei

[5] Ks. SOU 2024:18, s. 129, jossa todetaan, että ”Ordet ”hos” bör också exkludera myndigheter som lyder under riksdagen, dvs. Riksrevisionen, JO, Sveriges Riksbank och Riksdagsförvaltningen.”

käsitteen ole hankintalainsäädännön alallakaan Suomessa katsottu rajaavan eduskunnan virastoja pois soveltamisalasta. Vastaava ratkaisu on omaksuttu myös tietosuojalaissa.

Se, että keskustason julkishallinnon toimijan käsite määräytyy kansallisen lainsäädännön mukaisesti, voi merkitä, että jäsenvaltioiden välille syntyy niiden kansallisten oikeusjärjestelmien eroista johtuen eroavuuksia myös siinä suhteessa, mihin julkishallinnon toimijoihin direktiivi tulee kussakin jäsenvaltiossa sovellettavaksi.

Valvontaviranomaisen toimivaltaa koskevat rajoitukset

Edellä todetun perusteella ehdotus on laadittu siten, että tiedonhallintalain uusi 4 a luku soveltuisi eduskunnan virastoihin. Näin olisi lähtökohtaisesti siitä huolimatta, että eduskunnan virastojen tietojärjestelmät tukevat osin myös valtiopäivätoimintaa. Velvoitteet ja valvonta kohdistuisivat ehdotuksen nojalla toiminnassa käytettäviin viestintäverkkoihin ja tietojärjestelmiin kohdistuvien kyberriskien hallintaan. Ehdotuksen soveltamisella eduskunnan virastoihin arvioidaan olevan positiivinen vaikutus tietoturvaan samoin kuin muiden julkishallinnon toimijoiden kohdalla.

Ehdotuksen johdosta syntyy tilanteita, joissa osa valvottavan toimijan toiminnasta jää soveltamisalan ulkopuolelle. Valvontaviranomaisen tehtävänä on yksittäistapauksessa ratkaista, mikä osa toiminnasta jää soveltamisalan ulkopuolelle. 2. lakiehdotuksen 3 §:n 3 momentin mukaan 4 a lukua sovellettaisiin julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015) tarkoitettuun turvallisuusverkon palvelutuotantoon ja turvallisuusverkon palvelujen käyttönä pidettävään viranomaisen toimintaan vain, jos viranomainen on CER-direktiivissä tarkoitettu kriittinen toimija. Ehdotusta ei siten lähtökohtaisesti sovellettaisi siihen osaan toimijan toiminnasta, joka on turvallisuusverkon palvelujen käyttöä. Tämäkin poikkeus voisi tulla sovellettavaksi eduskunnan virastojen toiminnassa.

Ehdotetun tiedonhallintalain 18 i §:n 3 momentin mukaan valvontaviranomaisen tiedonsaantioikeus ei koskisi salassa pidettäviä tietoja julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa tarkoitetusta turvallisuusverkon palvelutuotannosta tai palvelujen käytöstä eikä tietoja, joiden luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin niihin liittyvää tärkeää etua. Vastaava rajoitus koskisi tarkastusoikeutta (18 j § 3 mom.). Nämä rajoitukset voisivat tapauskohtaisesti tulla sovellettavaksi myös eduskunnan virastoihin.

Eduskunnan oikeusasiamiehen valvontaa koskevat erityiset rajaukset

Vaikka ehdotusta sovellettaisiin eduskunnan oikeusasiamiehen kansliaan, Liikenne- ja viestintäviraston valvontatoimivaltuuksia tai tiedonsaanti- ja tarkastusoikeutta ei ehdotetun tiedonhallintalain 3 §:n 4 momentin mukaan sovellettaisi eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan (hallituksen esitys, s. 270).

Ehdotettu sääntely vastaa tietosuojalain 14 §:n 2 momentissa noudatettua sääntelytapaa, jossa oikeuskanslerinviraston lausunnossa toteamin tavoin ylimpien laillisuusvalvojien toiminnan valvonta suljetaan nimenomaisilla säännöksillä muun viranomaisvalvonnan ulkopuolelle.[6] Ehdotuksen yksityiskohtaisten perustelujen mukaisesti tämä tarkoittaisi, että ylimpien laillisuusvalvojien toimintaan ei sovellettaisi miltään osin valvontaa tai valvovan viranomaisen toimivaltuuksia (s. 212).

[6] Oikeuskanslerinviraston lausunto, s. 2, https://api.hankeikkuna.fi/asiakirjat/2b11d230-a4ff-47be-89f9-29e396f2c7bf/1f218244-10e4-4379-813e-9f0deeb6c830/LAUSUNTO_20231201120434.PDF.

Ehdotuksessa tätä valvontatoimivallan rajausta perustellaan eduskunnan oikeusasiamiehen perustuslaissa säädetyllä asemalla, jonka perusteella valtion keskushallintoon kuuluvien viranomaisten ohjaustoimivaltaa ei voida ulottaa näiden organisaatioiden sisäisen hallinnon ohjaukseen tai lainkäyttöön (esim. PeVL 46/2010 vp ja PeVL 14/2028 vp) (s. 270).[7]

NIS 2 -direktiivissä lähtökohtana on julkishallinnon toimijoidenkin osalta, että valvontaviranomaisen toimivaltuudet ulottuvat kaikkiin soveltamisalassa oleviin toimijoihin. Direktiivissä ei nimenomaisesti säädetä kansallisesta liikkumavarasta, joka mahdollistaisi valvontatoimivaltuuksien rajaamisen tiettyjen, direktiivin soveltamisalaan kuuluvien toimijoiden kohdalla. NIS 2 -direktiivin 31 artiklan 4 kohdan mukaan valvontaan velvoittamisella ei kuitenkaan rajoiteta kansallisten lainsäädäntö- ja toimielinkehysten soveltamista. Johdanto-osan kohdassa 124 todetaan vastaavasti, että julkishallinnon toimijoiden suhteen valvontavaltuuksia olisi käytettävä kansallisten lainsäädäntö- ja toimielinkehysten mukaisesti.

Tämä mahdollistaa ministeriön näkemyksen mukaan hallituksen esityksen mukaisen, ylimpien laillisuusvalvojien perustuslailliseen asemaan perustuvan rajoituksen valvontaviranomaisen toimivaltuuksiin. Valmistelussa on otettu huomioon perustuslakivaliokunnan tietosuojalakiehdotusta koskeva lausunto, jossa edellytettiin, että ylimpien laillisuusvalvojien harjoittamaan laillisuusvalvontaan ei kohdistu tietosuojalaissa tarkoitetun valvontaviranomaisen valvontatoimivaltaa (PeVL 14/2018 vp; hallituksen esitys, s. 270–271). Toisin kuin tietosuoja-asetuksen 55, 57 ja 58 artiklat, NIS 2 -direktiivin 31(4) artikla itsessään jo näyttää tunnistavan, että kansallisessa täytäntöönpanossa voi olla tarpeen tehdä esimerkiksi kansallisten perustuslakien erityispiirteiden edellyttämiä mukautuksia.

Kyberturvallisuuslain soveltaminen

Tiedonhallintalain soveltamisalaan kuuluva viranomainen voi kuulua myös kyberturvallisuuslain soveltamisalaan, mikäli se harjoittaisi toimintaa NIS 2 -direktiivin ja kyberturvallisuuslain liitteessä tarkoitetulla toimialalla (hallituksen esitys, s. 140). Ehdotettuun kyberturvallisuuslakiin ei sisälly erityisiä soveltamisalarajauksia eduskunnan, sen virastojen tai ylimpien laillisuusvalvojien osalta. Kuten hallituksen esityksessä tuodaan esiin, tämä on tarpeetonta, koska eduskunnan virastot eivät tarjoa palveluja kyberturvallisuuslain liitteissä tarkoitetuilla toimialoilla eivätkä siten tulisi lain soveltamisalaan (s. 271).

Kattavuuden vuoksi ehdotuksen 35 §:ssä säädettäisiin joka tapauksessa, että seuraamusmaksua ei voitaisi määrätä valtion viranomaisille, valtion liikelaitoksille, hyvinvointialueille eikä -yhtymille, kunnallisille viranomaisille, itsenäisille julkisoikeudellisille laitoksille, eduskunnan virastoille, tasavallan presidentin kanslialle eikä Suomen evankelisluterilaiselle kirkolle ja Suomen ortodoksiselle kirkolle eikä niiden seurakunnille, seurakuntayhtymille ja muille elimille.

[7] Perustuslakivaliokunta katsoi tietosuojalakiehdotusta käsitellessään, että ehdotusta oli muutettava siten, että ylimpien laillisuusvalvojien harjoittamaan laillisuusvalvontaan ei kohdistu tietosuojalaissa tarkoitetun valvontaviranomaisen valvontatoimivaltaa (PeVL 14/2018 vp).