Perustuslakivaliokunnalle

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

Perustuslakivaliokunta on pyytänyt liikenne- ja viestintäministeriöltä asiantuntijalausuntoa hallituksen esityksestä eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (HE 57/2024 vp).

Liikenne- ja viestintäministeriö kiittää lausuntopyynnöstä ja esittää kunnioittavasti lausuntonaan seuraavaa.

Esityksen valmistelu ja tavoite

Esityksen valmisteluun on johtanut EU:n uusi kyberturvallisuusdirektiivi eli 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 (NIS 2 -direktiivi). Direktiivi on tullut voimaan 16.1.2023. Direktiivi edellyttää jäsenvaltioita saattamaan sitä täytäntöönpanevat säännökset osaksi kansallista lainsäädäntöä 17.10.2024 mennessä sekä soveltamaan niitä viimeistään 18.10.2024 alkaen.

Liikenne- ja viestintäministeriö asetti tammikuussa 2023 säädöshankkeen valmistelemaan direktiivin kansallisen toimeenpanon edellyttämiä lainsäädäntömuutoksia. Hallituksen esityksessä esitetään lainsäädäntömuutoksia, jotka ovat tämän valmistelutyön tulos.

Esityksen valmistelua on tukenut liikenne- ja viestintäministeriön puheenjohtama työryhmä, jossa olivat edustettuina oikeusministeriö, valtiovarainministeriö, ympäristöministeriö, maa- ja metsätalousministeriö, työ- ja elinkeinoministeriö, sosiaali- ja terveysministeriö, sisäministeriö, puolustusministeriö sekä ulkoministeriö.

Julkishallintoon kohdistuvien velvoitteiden osalta valmistelua on tukenut valtiovarainministeriön puheenjohtama alatyöryhmä, jossa olivat edustettuina liikenne- ja viestintäministeriö, oikeusministeriö, työ- ja elinkeinoministeriö, ympäristöministeriö, maa- ja metsätalousministeriö, sosiaali- ja terveysministeriö, sisäministeriö, puolustusministeriö, ulkoministeriö, valtioneuvoston kanslia, opetus- ja kulttuuriministeriö, Verohallinto ja Kuntaliitto.

Esityksessä ehdotetuilla laeilla pantaisiin täytäntöön EU:n uusi kyberturvallisuusdirektiivi (NIS 2), jonka tavoitteena on vahvistaa EU:n yhteistä ja jäsenvaltioiden kansallista kyberturvallisuuden tasoa yhteiskunnan toiminnan kannalta keskeisillä toimialoilla. Lisäksi esityksen tavoitteena on vähentää kyberhäiriöiden määrää ja välttää kyberturvallisuuteen liittyvien poikkeamien aiheuttamia keskeytyksiä ja häiriöitä yhteiskunnan toiminnan kannalta keskeisille palveluille ja toiminnoille. Esityksellä edistettäisiin näitä tavoitteita. Esityksessä ehdotetaan tehtäväksi direktiivin täytäntöönpano sen vähimmäistason edellyttämällä tavalla sekä soveltamisalan ja velvoitteiden

laajuuden osalta. Esityksen valmistelussa on pyritty hyödyntämään direktiivin sallimaa kansallista liikkumavaraa mahdollisimman laajasti.

Esityksen keskeinen sisältö

Esityksessä ehdotetaan säädettäväksi uusi kyberturvallisuuslaki. Laissa säädettäisiin NIS 2 -direktiivin edellyttämistä kyberturvallisuuden riskienhallintaa ja poikkeamaraportointia koskevista vähimmäisvelvoitteista direktiivin soveltamisalaan kuuluville toimijoille. Laissa säädettäisiin myös velvoitteiden valvonnasta sekä muista NIS 2 -direktiivin täytäntöönpanon edellyttämistä viranomaistehtävistä, kuten tietoturvaloukkauksia tutkivan ja niihin reagoivan CSIRT-yksikön tehtävästä, joka osoitettaisiin Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle. Yksinomaan julkishallinnon toimialaan kohdistuvista velvoitteista ja niiden noudattamisen valvonnasta ehdotetaan säädettäväksi erikseen julkisen hallinnon tiedonhallinnasta annetussa laissa.

Sähköisen viestinnän palveluista annetussa laissa ehdotetaan säädettäväksi direktiivin verkkotunnusten rekisteröintitietojen tietokantaa koskevan artiklan täytäntöönpanemiseksi tarpeellisista muutoksista. Lisäksi esityksellä ehdotetaan tehtäväksi toimialakohtaisiin lakeihin eräitä kyberturvallisuuslain säätämiseksi tarpeellisia teknisiä muutoksia. Lisäksi toimialakohtaisista laeista ehdotetaan kumottavaksi nykyisin voimassa olevat verkko- ja tietoturvallisuusdirektiivin täytäntöönpanoa koskevat säännökset, koska mainittu direktiivi kumotaan NIS 2 -direktiivillä.

Esityksen suhde perustuslakiin

Esitys sisältää perustuslain kannalta merkityksellisiä ehdotuksia suhteessa perustuslain 2 §:n 3 momentissa säädettyyn julkisen vallan käytön lakisidonnaisuuteen, perustuslain 10 §:ssä turvattuun yksityiselämän, henkilötietojen ja luottamuksellisen viestinnän suojaan, perustuslain 15 §:ssä turvattuun omaisuudensuojaan, perustuslain 18 §:ssä turvattuun elinkeinovapauteen, perustuslain 21 §:ssä turvattuun oikeusturvaan, perustuslain 80 §:ssä asetuksen antamisesta ja lainsäädäntövallan siirtämisestä säädettyyn sekä perustuslain 124 §:ssä hallintotehtävän antamisesta muulle kuin viranomaiselle säädettyyn.

Esityksen valmistelussa on arvioitu suotavaksi pyytää perustuslakivaliokunnalta lausunto esitykseen sisältyvän haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan ehdotuksen sekä eräiden valtioelinten ja viranomaisten asemasta esitetyn arvion johdosta.

Haitallisen tietokoneohjelman tai käskyn sisältävä viestin käsittely

Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu, ja henkilötietojen suojasta säädetään tarkemmin lailla Pykälän 2 momentin nojalla kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Pykälän 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen momentissa säädetyillä perusteilla. Perustuslain 10 §:n 2 momentin esitöiden mukaan säännöksen tarkoituksena on suojata luottamuksellisena pidettävän viestin sisältö ulkopuolisilta puuttumisilta.

Esityksen 1. lakiehdotuksen 28 §:n 2 momentin nojalla valvovalla viranomaisella olisi salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada kyberturvallisuuslain soveltamisalaan kuuluvalta toimijalta välitystieto, sijaintitieto sekä tieto haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä, jos se on välttämätöntä

kyberturvallisuuslaissa säädetyn velvoitteen noudattamisen valvomiseksi, eli kyberturvallisuutta koskevan riskienhallintavelvoitteen noudattamisen tai merkittävistä poikkeamista ilmoittamisen ja raportoinnin valvomista varten.

Esityksen 2. lakiehdotuksen 18 i §:n 2 momenttiin sisältyisi vastaava säännös valvovan viranomaisen tiedonsaantioikeudesta kohdistuen tiedonhallintalain 4 a luvussa säädettyjen kyberturvallisuutta koskevien velvollisuuksien valvontaan.

Tiedonsaantioikeuden nojalla saadut tiedot olisi pidettävä salassa valvovassa viranomaisessa. 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. Tiedonsaantioikeuden käyttämisellä tai tietojen luovuttamisella ei saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä.

Esityksen 1. lakiehdotuksen 23 §:ssä säädettäisiin CSIRT-yksikön koordinoimista kyberturvallisuustietojen vapaaehtoisista jakamisjärjestelyistä. Järjestelyn tarkoituksena olisi niihin osallistuvien yhteisöjen sekä niiden asiakkaiden viestintäverkkoihin, tietojärjestelmiin tai palveluihin kohdistuvien kyberuhkien ehkäisemiseksi ja havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi ja niiden vaikutusten lieventämiseksi. Mainitun pykälän 3 ja 4 momentin nojalla CSIRT-yksikkö ja jakamisjärjestelyyn osallistuva saisi luovuttaa oma-aloitteisesti lain mukaiseen vapaaehtoiseen jakamisjärjestelyyn osallistuvalle tietoa kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä. Jakamisjärjestelyyn osallistuminen olisi vapaaehtoista ja säännös ei velvoittaisi jakamaan tietoa jakamisjärjestelyyn osallistuville. Säännöksellä pantaisiin täytäntöön NIS 2 –direktiivin 29 artikla kyberturvallisuustietojen vapaaehtoisista jakamisjärjestelyistä.

Tiedon käsittelyn ja luovuttamisen tarve liittyy ennen kaikkea kyberuhkan, poikkeaman tai haavoittuvuuden haitallisten vaikutusten estämiseen ja sen teknisiin jälkiin. Tiedon käsittelyn ja luovuttamisen tarkoituksena olisi varautua, varoittaa tai estää vastaavan häiriötilanteen tapahtumista muissa viestintäverkoissa ja tietojärjestelmissä ja siten estää ennakoitavissa olevasta häiriötilanteesta aiheutuvien haitallisten vaikutuksien aiheutumista muissa organisaatioissa. Tiedon käsittelyn ja luovuttamisen tarve kohdistuu ennen kaikkea haitallisen tietokoneohjelman tai käskyn teknisiin ominaisuuksiin, teknisiin jälkiin tai muuhun kyberuhkaan tai poikkeaman toteuttamiseen liittyvään tekniseen tietoon. Koska kyse on tietokoneiden, laitteiden tai ohjelmistojen välisestä sähköisestä viestinnästä, tekniset tiedot ovat usein kiinteänä ja erottamattomana osana sähköisiä viestejä tai siihen sisältyvää haitallista tietokoneohjelmaa tai käskyä tavalla, jossa tekniset tiedot voivat olla tulkittavissa osaksi viestin sisällöksi luettavaa tietoa, vaikka kyse ei olisi viestin semanttisesta sisällöstä. Tästä aiheutuu välttämätön tarve käsitellä sähköiseen viestiin liittyviä teknisiä tietoja säännöksen tavoitteen toteuttamiseksi. Välttämätöntä tarvetta ei kohdistuisi haitallisen tietokoneohjelman sisältävän viestin semanttiseen sisältöön.

Kyberturvallisuustietojen vapaaehtoisen jakamisjärjestelyn tarkoituksen toteuttamiseksi olisi välttämätöntä, että vapaaehtoiseen jakamisjärjestelyyn osallistuvat voisivat jakaa tietoja haitallisista tietokoneohjelmista ja käskyistä jakamisjärjestelyyn osallistuvien kesken. CSIRT-yksiköllä ja jakamisjärjestelyihin osallistuvilla olisi mahdollisuus antaa muille jakamisjärjestelyyn osallistuville oma-aloitteisesti tietoa haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä ja sen välitystiedoista siltä osin kuin se liittyy haitalliseen tietokoneohjelmaan tai käskyn teknisiin

ominaisuuksiin ja teknisiin jälkiin tai muuhun kyberuhkan tai poikkeaman toteuttamiseen liittyvään tekniseen tietoon, mikä olisi välttämätöntä jakamisjärjestelyn tarkoitusta varten, eli kyberuhkien ja poikkeamien hallitsemiseksi ja haitallisten vaikutusten ehkäisemiseksi. Säännös kattaisi esimerkiksi tiedon antamisen haitalliseen tietokoneohjelmaan liittyvistä lokitiedoista. Jos pykälän nojalla tapahtuvassa luovuttamisessa olisi kyse henkilötiedoista, olisi erikseen noudatettava myös, mitä yleisessä tietosuoja-asetuksessa ja tietosuojalaissa henkilötiedoista säädetään. Kuten edellä, tiedonvaihdon tarve ei tässäkään yhteydessä kohdistuisi sähköisen viestinnän semanttiseen eli ihmisen luomaan sisältöön viestinnässä, vaan viestin teknisiin ominaisuuksiin.

Esitykseen sisältyvien edellä kuvattujen haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevien ehdotuksien perustuslainmukaisuuden arvioinnin kannalta ratkaisevaa on tulkinta siitä, nauttiiko haitallisen tietokoneohjelman tai käskyn sisältävä viesti luottamuksellisen viestinnän suojaa perustuslain 10 §:n 2 momentin mukaisena luottamuksellisena viestintänä siten, että perustuslain 10 § momentissa olevaa erityistä lakivarausta on sellaisenaan sovellettava, vai onko kysymys suojan ydinalueen ulkopuolelle sijoittuvasta toiminnasta, jota on arvioitava perusoikeuksien yleisten rajoitusedellytysten mukaisesti. Kysymyksestä on niukasti lainvalmisteluasiakirjoja, perustuslakivaliokunnan aineistoa tai muuta tulkinta-aineistoa erityisesti siltä osin, kun kysymys on kuvatun kaltaisesta sähköiseen viestinnän liittyvästä teknisestä tiedosta, joka voi olla osana sähköistä viestiä, ja jonka käsittely on tarpeellista kyberuhkan, poikkeaman tai haavoittuvuuden haitallisten vaikutusten ehkäisemiseksi.

Luottamuksellisen viestin tai luottamuksellisen viestinnän sisällön tai soveltamisalan tarkempaa määritelmää ei sisälly perustuslain 10 §:n 2 momenttiin eikä tavalliseen lakiin. Viestin sisältö on sellaisenaan nauttinut perinteisesti vahvasti perusoikeussuojaa ja yksityisen viestin sisällön on tulkittu olevan viestinnän luottamuksellisuuden suojan ydinalueella (PeVL 36/2018 vp, s. 23). On kuitenkin arvioitava, voiko kaikki sähköinen viestien tai teknisten käskyjen lähettäminen ja vastaanottaminen olla kaikissa olosuhteissa perusoikeussuojan kohteena olevaa luottamuksellista viestintää. Perustuslakivaliokunta on lausunnossaan PeVL 15/2024 vp pitänyt mahdollisena arvioida välitystietojen käsittelyä koskevaa sääntelyä perusoikeuksien yleisten rajoitusedellytysten mukaan. Perustuslakivaliokunta arvioi asiassa radioviestinnän välitystietojen käyttöä radioteknisessä valvonnassa ja katsoi, että sääntely radioteknisestä valvonnasta muodostui käsillä olleessa sääntely-yhteydessä ja ehdotetussa laajuudessa, ottaen erityisesti huomioon valvonnalle laissa ehdotetut rajoitukset, suhteellisen vähäiseksi puuttumiseksi luottamuksellisen viestin salaisuuden suojaan (PeVL 15/2024 vp, s. 4).

Perustuslakivaliokunta on lisäksi aiemmin lausunnossaan PeVL 22/2020 vp arvioinut mahdolliseksi käsitellä miehittämättömän ilma-aluksen käyttöön liittyvää radioviestintää, välitystietoja ja sijaintitietoja miehittämättömän ilma-aluksen kulkuun puuttumiseksi tai sen yksilöimiseksi ja sijainnin määrittelemiseksi lausunnossa kuvatuissa olosuhteissa, joissa lennättäminen oli oikeudetonta (PeVL 22/2020 vp, s. 5). Valiokunta on myös arvioinut, viitaten toiminnan luonteeseen ja henkilöiden taltiointia koskevaan tietoisuuteen, ettei liikenteen ohjauksessa syntyvä puhe- ja viestiliikenne ole perustuslain 10 §:ssä tarkoitetun luottamuksellisen viestin salaisuuden piiriin kuuluvaa toimintaa (ks. PeVL 62/2010 vp, s. 5). Perustuslakivaliokunnan käytännöstä on siten välillisesti perusteltavissa, ettei mitä tahansa sähköiseksi viestinnäksi tulkittavissa olevaa toimintaa voitaisi katsoa kuuluvan edes viestin sisällön osalta perustuslain turvaaman luottamuksellisen viestin salaisuuden alaan. Näin on ollut ainakin kuvatuissa tapauksissa, joissa viestin sisältö on luonnehdittavissa eri tavoin teknisluontoiseksi ja ensin mainitussa tapauksessa myös oikeudenvastaiseen tekoon liittyväksi.

Tämän ohella korkein oikeus on tapauksessa KKO 2023:14 katsonut, arvioidessaan tietyn viestinnän luottamuksellisuutta loukkaavan menettelyn vakavuutta, että merkitystä voidaan antaa sille, että viestit liittyivät lähinnä vakavien rikosten suunnitteluun ja tekemiseen. Lisäksi KKO totesi olevan selvää, että kun viestintä oli pääasiassa koskenut rikosten suunnittelua tai tekemistä, kysymys ei ollut yksityiselämän suojan ydinalueesta.

Erityisesti tulisi ottaa huomioon, että ehdotetuilla kyberuhkiin liittyvillä tiedon käsittelyn ja luovuttamisen toimenpiteillä osaltaan turvataan erilaisten perusoikeuksien toteutumista torjumalla kyberhäiriöitä. Kyberturvallisuuteen liittyvät poikkeamat voivat aiheuttaa keskeytyksiä ja häiriöitä yhteiskunnan toiminnan kannalta keskeisiin palveluihin ja toimintoihin ja johtaa esimerkiksi yksityisyyden suojan loukkauksiin.

Luottamuksellisen viestin suojan kohteena on viestin lähettäjän ja sen vastaanottajan välisen semanttisen eli viestinnän osapuolien luoman, henkilökohtaisen ja toisen osapuolen vastaanotettavaksi tarkoitetun sisällön pysyminen luottamuksellisena ja suojattuna ulkopuolisten puuttumiselta. Luottamuksellisen viestin suojan voidaan katsoa siten kohdistuvan edes jollain tavoin merkitykselliseen viestintään ja kommunikointiin luonnollisten henkilöiden välillä. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelytarpeen tarkoituksena ei olisi saada selkoa viestin semanttisesta sisällöstä, eikä tämänkaltaisen viestin sisällössä pääasiallisesti ole luottamuksellisen viestinnän suojan ydinalueeseen kuuluvaa henkilökohtaista, vain toisen osapuolen vastaanotettavaksi tarkoitettua viestintää.

Haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä on usein kyse haitallisen tietokoneohjelman automaattisesti luomasta viestistä, jossa viestin lähettäjänä ei ole luonnollista henkilöä vaan haittaohjelma tai sen ohjelmoinut taho. Kysymys on tyypillisesti teknisestä käskystä, ohjelmasta tai komennosta, jolla pyritään aiheuttamaan haittaa viestintäverkon tai tietojärjestelmän toiminnalle. Kysymys voi olla tietokonejärjestelmien välisestä automatisoidusta ja teknisestä toimesta, jonka suoranaisina osapuolina ei ole luonnollisia henkilöitä tai jossa ei ole teknisten ominaisuuksien ohella lainkaan semanttista sisältöä. Esimerkiksi palvelunestohyökkäyksellä tarkoitetaan pyrkimystä häiritä verkossa olevan resurssin tai palvelun käyttöä, mikä tehdään yleisesti kohdistamalla palveluun ylimääräistä ja tarpeetonta verkkoliikennettä hajautetuista kohteista poikkeuksellisen suuri määrä. Tämä haitallinen ja automatisoitu verkkoliikenne voi olla, palvelunestohyökkäyksen teknisestä toteutustavasta riippuen, olla osittain tai kokonaan tulkittavissa sähköiseksi viestinnäksi. Haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä voi olla kysymys esimerkiksi myös automaattisesti ohjelman luomasta luodusta kalasteluviestistä, jonka tarkoituksena on saada kohde erehdytettyä suorittamaan toimi, joka mahdollistaa haitallisen tietokoneohjelman suorittamisen viestintäverkossa ja tietojärjestelmässä taikka viestintäverkon ja tietojärjestelmän suojauksen murtamisen. Haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä ei tällöin olisi kysymys viestinnän osapuolten välisestä luottamuksellisen viestinnän suojan ydinalaan perinteisesti kuuluvasta viestistä, jolla on yksilöityä semanttista tai kommunikatiivista merkitystä osapuolille. Haittaohjelma voi olla myös tahattomasti mukana viestissä, jolloin tiedonsaannin ja käsittelyn tarve kohdistuu haittaohjelman teknisiin ominaisuuksiin viestin semanttisen sisällön sijaan. Kuvatuissa esimerkeissä viestin lähettäjänä on taho, jonka pyrkimyksenä on toteuttaa kyberhyökkäys tai aiheuttaa haittaa viestintäverkon ja tietojärjestelmän toiminnalle ja siten niille oikeushyville, joiden toteutumista järjestelmän toimivuus turvaa, sekä järjestelmässä olevien henkilö- ja muiden tietojen luottamuksellisuudelle.

Haitallisen tietokoneohjelman tai käskyn sisältävässä viestissä semanttinen tai kommunikatiivinen sisältö jää edellä kuvatulla tavalla hyvin vähäiseksi tai puuttuu kokonaan, jos kysymys on

teknisestä koneiden välisestä viestinnästä taikka haitallisen tietokoneohjelman automaattisesti tai kyberhyökkäystä suorittavan tahon ennalta tuntemattomalle ja hyvin laajalle vastaanottajajoukolle lähettämästä kalasteluviestistä. Kysymys on yksipuolisesta toimesta, jonka tarkoituksena on pyrkiä toteuttamaan kyberhyökkäys tai teknistä haittaa viestintäverkolle tai tietojärjestelmälle. Vaikka kyberhyökkäyksen tai –häiriön toteuttamisen aiheuttamiseksi tähtäävää toimintaa voitaisiin sellaisenaan pitää viestinä, sen kuuluminen luottamuksellisen viestinnän perusoikeussuojan piiriin ei ole ilmeistä. Koska viestinnällinen ja kommunikatiivinen sisältö, tarkoitus ja merkitys joko puuttuvat kokonaan tai jäävät hyvin vähäiseksi, viestin ei voida katsoa kuuluvan ainakaan luottamuksellisen viestin suojan ydinalueelle, sikäli kun jaottelulle perusoikeussuojan reuna- ja ydinalueeseen on valtiosääntöoikeudellisia perusteita. Viestin voidaan arvioida jäävän kokonaan myös suoja-alueen ulkopuolelle. Luottamuksellisen viestinnän perusoikeussuojan soveltamisalan arvioinnille on tarve erityisesti sähköisessä viestinnässä, koska teknologian kehittyessä sähköisten viestien alaan luettavissa olevien erilaisten teknisten sisältöjen, komentojen, käskyjen ja viestien tekninen monipuolistuminen, käyttömahdollisuuksien laajentuminen, ja sähköisen viestinnän teknisten toteutumismuotojen ja –tapojen muutokset luovat tilanteita, joissa sähköisten viestien alaan luettavien toimien merkityksellisyys luottamuksellisen viestinnän perinteisesti suojaamien oikeushyvien kannalta eroavat toisistaan merkittävällä, olennaisella ja painavalla tavalla.

Edellä esitetyn lisäksi oikeusjärjestelmässä yleisesti omaksutun oikeuksien väärinkäytön kiellon näkökulmasta voidaan argumentoida, että luottamuksellisen viestinnän suojaa ei tulisi tulkita tavalla, joka estäisi haittaohjelmaviestin teknisten tietojen käsittelemistä kyberuhkien ehkäisemiseksi, milloin luottamuksellisen viestinnän suojalla suojattaisiin toimintaa, jonka tarkoituksena on vakavasti vaarantaa juuri luottamuksellisen viestinnän suojaa sähköisessä viestinnässä tai muita perusoikeuksia. Erityisesti yhteiskunnan kriittisten toimijoiden kybervarautumisen kannalta olisi tärkeää, että hyökkäyksissä käytettäviä haittaohjelmia koskevia tietoja voitaisiin jakaa hyökkäysten potentiaalisten kohteiden kesken ja siten pyrkiä ehkäisemään esimerkiksi tietomurtoja tai muita luottamuksellisen viestinnän suojaa vaarantavia kyberhyökkäyksiä. Kyberhyökkäykset voisivat toteutuessaan johtaa merkittäviin luottamuksellisen viestinnän suojan tai henkilötietojen suojan loukkauksiin. Oikeuksien väärinkäytön kiellosta säädetään esimerkiksi Euroopan unionin perusoikeuskirjan (2016/C 202/02) 54 artiklassa, jonka nojalla perusoikeuskirjan määräysten ei saa tulkita antavan oikeutta ryhtyä sellaiseen toimintaan tai tehdä sellaista tekoa, jonka tarkoituksena on tehdä tyhjäksi jokin tässä perusoikeuskirjassa tunnustettu oikeus tai vapaus tai rajoittaa sitä laajemmalti kuin tässä perusoikeuskirjassa on sallittu.

Edellä esitetyt seikat huomioon ottaen hallituksen esityksen valmistelussa on päädytty arvioon, jossa kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä viesti ei kuuluisi viestinnän luottamuksellisuuden suojan ydinalueelle, etenkään sen teknisten haittaohjelmaan liittyvien ominaisuuksien taikka automatisoidusti luodun sisällön osalta, viestinnän osapuoliksi luettavien luonnollisten henkilöiden välisen sisällön puutteen vuoksi. Näin ollen kysymys ei olisi perustuslain 10 §:n 2 momentissa tarkoitetusta luottamuksellisesta viestinnästä, eli sen käsittelyä voitaisiin arvioida perustusoikeuksien yleisten rajoitusedellytysten mukaisesti. Hallituksen esityksen valmistelussa edellä kuvattujen ehdotuksien on arvioitu täyttävän perusoikeuksien yleiset rajoitusedellytykset välttämättömyydestä, asianmukaisuudesta ja oikeasuhtaisuudesta sillä tavoiteltavan hyväksyttävän ja painavan yhteiskunnallisen tarpeen mukaisten tavoitteiden toteuttamiseksi.

Eräiden valtioelinten ja viranomaisten asema

Hallituksen esityksen jatkovalmistelussa on arvioitu, että NIS 2 –direktiivin soveltamisalan ulkopuolelle jää eduskunnan valtiopäivätoiminta, kun taas eduskunnan virastot eivät kuulu parlamentteja koskevan soveltamisalapoikkeuksen alaan. Oikeuskanslerinvirasto antoi esityksestä lausunnon, jonka 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.[1]

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

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; ja (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.

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

NIS2-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

NIS2-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 NIS2-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.

NIS2-direktiivin toimeenpanoa julkishallinnon toimialalla koskevan tiedonhallintalain 4 a luvun soveltamisalan sekä valvovan viranomaisen toimivallan rajaamisessa on perustuslaista johtuvista syistä noudatettu pitkälti vastaavaa sääntelytapaa kuin, mihin yleisen tietosuoja-asetuksen ja tietosuojalain soveltamisen osalta päädyttiin perustuslakivaliokunnan lausunnossa (PeVL 14/2018 vp) esitetyn johdosta. NIS2-direktiivi sisältää jonkin verran yleistä tietosuoja-asetusta laajemmin liikkumavaraa kansallisessa soveltamisessa.

Ehdotetun tiedonhallintalain 3 §:n 1 momentin lähtökohdan mukaan lakia, mukaan lukien ehdotettua 4 a luvun NIS2-direktiiviin perustuvaa sääntelyä, sovellettaisiin julkisuuslain 4 §:n 1 momentissa tarkoitettuihin viranomaisiin eli myös eduskunnan virastoihin sekä valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen toimintaan. Tiedonhallintalain 4 a lukua sovellettaisiin eduskunnan virastoihin julkisuuslain 4 §:n 1 momentin 6 kohdasta ja sen perusteluista ilmenevällä tavalla, sillä direktiivin 6 artiklan 35 kohdassa käytetyllä käsitteellä ”parlamentti” viitataan kansanedustuslaitoksen toimintaan, eli Suomessa eduskunnan valtiopäivätoimintaan. Myös perustuslakivaliokunta on todennut tietosuojalain hallituksen esityksestä antamassaan lausunnossa PeVL 14/2018 vp, ettei lähtökohtaista estettä ole sille, että hallintoa koskevat yleislait ulotetaan koskemaan eduskunnan virastoja. 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) Näin ollen myöskään tiedonhallintalaki tai sen 4 a luku ei koske eduskunnan valtiopäivätoimintaa.

Tasavallan presidentin kansliaan tai tuomioistuimiin taikka valitusasioita käsittelemään perustettuihin lautakuntiin ehdotettua 4 a lukua ei sovellettaisi ehdotettujen 3 §:n 3 momenttiin sisältyvien poikkeusten perusteella, ellei mainittua katsottaisi kriittiseksi toimijaksi. Tuomioistuinten ja valitusasioita käsittelemään perustettujen lautakuntien osalta rajaus perustuu NIS2-direktiivin 6 artiklan 35 kohtaan. Tasavallan presidentin kanslian osalta valmistelussa on katsottu, että se ei kuulu direktiivin pakolliseen soveltamisalaan, vaikka sen tyyppistä toimijaa ei ole nimenomaisesti mainittu direktiivin soveltamisalaa koskevissa poikkeuksissa. Direktiivin poikkeukset koskevat

keskushallinnon viranomaisia ja lisäksi soveltamisessa on jätetty kansallista liikkumavaraa viittauksella jäsenvaltion kansallisen lainsäädännön mukaiseen keskustason julkishallinnon toimijan määrittelyyn. Tasavallan presidentin kanslian osalta nimenomainen poikkeus NIS2-sääntelyn osalta perustuu Tasavallan presidentin asemaan valtioelimenä ja Suomen puolustusvoimien ylipäällikkönä sekä tasavallan presidentin kanslian tehtäviin tasavallan presidentin avustamisessa (laki tasavallan presidentin kansliasta 2 §). Tasavallan presidentin kansliaa ei myöskään voida pitää perustuslain 119 §:ssä tarkoitettuna valtion keskushallinnon viranomaisena eikä myöskään ole selvää, onko sillä NIS2-direktiivin 6 artiklan 35 kohdan d alakohdassa tarkoitettua toimivaltaa.

NIS2-direktiivin valvovan viranomaisen eli julkishallinnon toimialalla Liikenne- ja viestintäviraston valvontatoimivaltuuksia tai tiedonsaanti- ja tarkastusoikeutta ei ehdotetun tiedonhallintalain 3 §:n 4 momentin mukaan sovellettaisi eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeuskanslerin toimintaan. Valvontatoimivaltuuksia ei sovellettaisi myöskään tasavallan presidentin kansliaan taikka tuomioistuinten tai valitusasioita käsittelemään perustettujen lautakuntien lainkäyttöön siinä tapauksessa, että mainittuihin sovellettaisiin 4 a lukua kriittisenä toimijana, joka yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain nojalla olisi määritetty julkishallinnon toimialan kriittiseksi toimijaksi. Valvontatoimivallan rajoitukset johtuvat pääosin näiden julkiseen sektoriin kuuluvien organisaatioiden perustuslaissa säädetystä asemasta, 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).

Mainittujen viranomaisten osalta ei ehdotetussa tiedonhallintalain 3 §:n 4 momentissa ole suljettu pois velvoitetta ilmoittautua toimijaksi (tiedonhallintalain 18 a §) eikä velvoitetta ilmoittaa merkittävistä poikkeamista valvovalle viranomaiselle (18 d §). Näiden säännösten voidaan nähdä jossain suhteessa palvelevan valvonnallisia tarkoituksia, mutta tarkoituksena on myöskin toimijoiden ja niiden määrän tilastointi sekä tietojen kerääminen kriittisillä toimialoilla käytetyistä IP-osoitealueista sekä tilannekuvatiedon kerryttäminen merkittävistä poikkeamista. Valvonnallista tarkoitusta rajaa myös se, että valvovan viranomaisen tiedonsaantioikeus ei koskisi ylimpiä laillisuusvalvojia, eli niillä ei olisi velvoitetta luovuttaa valvovalle viranomaiselle salassa pidettäviä tietoja. Tiedonsaantioikeus ei koskisi myöskään tasavallan presidentin kansliaa tai tuomioistuimia taikka valitusasioita käsittelemään perustettujen valiokuntien lainkäyttöä, jos näihin sovellettaisiin 4 a lukua yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain johdosta. Tietojen luovuttamiseen liittyviä näkökulmia on esitetty tarkemmin valvovan viranomaisen tiedonsaantioikeutta koskevan tiedonhallintalain 18 i §:n ja vapaaehtoista ilmoittamista koskevan 18 f §:n säännöskohtaisissa perusteluissa.

Tiedonhallintalain voimassa olevan 3 §:n 3 momentin mukaan lain tiedonhallinnan yleistä ohjausta koskevaa 3 lukua ei sovelleta eduskunnan oikeusasiamiehen eikä valtioneuvoston oikeus-kanslerin toimintaan, tuomioistuimien eikä valitusasioita käsittelemään perustettujen lautakuntien toimintaan, tasavallan presidentin kansliaan, eduskunnan virastoihin, Kansaneläkelaitokseen, Suomen Pankkiin, muihin itsenäisiin julkisoikeudellisiin laitoksiin, yliopistolaissa tarkoitettuihin yliopistoihin eikä ammattikorkeakoululaissa tarkoitettuihin ammattikorkeakouluihin. Lain 3 lukua sovelletaan hyvinvointialueisiin, hyvinvointiyhtymiin, kuntiin ja kuntayhtymiin vain niiden hoitaessa laissa säädettyjä tehtäviä.

Mainittuja tiedonhallinnan yleistä ohjausta koskevia rajauksia ei ole eduskunnan virastojen, itsenäisten julkisoikeudellisten laitosten, yliopistojen, ammattikorkeakoulujen (jos sääntelyä

sovellettaisiin niihin kriittisinä toimijoina) taikka hyvinvointialueiden ja hyvinvointiyhtymien osalta sisällytetty NIS2-direktiivin valvontatoimivaltuuksien soveltamisen rajauksiin. Tämä johtuu siitä, että NIS2-direktiivissä lähtökohtana on julkishallinnon toimijoidenkin osalta valvonnan kohdistaminen kaikkiin toimijoihin, joskin NIS2-direktiivin 31artiklan 4 kohdan mukaan valvontaan velvoittamisella ei rajoiteta kansallisten lainsäädäntö- ja toimielinkehysten soveltamista. Tietosuojalain hallituksen esityksestä annetussa perustuslakivaliokunnan lausunnossa PeVL 14/2018 vp on arvioitu mahdollisuuksia poiketa EU-oikeuden täysimääräisestä soveltamisesta seuraavasti: ”Perustuslakivaliokunnan käsityksen mukaan on kuitenkin selvää, että kansallista valtiosäännön rakenteisiin kiinnittyvää identiteettiä koskeva sopimusmääräys voi muodostaa vain kapeasti sovellettavissa olevan oikeasuhtaisen perusteen poiketa EU-oikeuden täysimääräisestä soveltamisesta. Unionin tuomioistuimen vakiintuneessa oikeuskäytännössä on katsottu, että unionin oikeuden ensisijaisuuden periaatteen, joka on unionin oikeusjärjestyksen olennainen ominaisuus, mukaan se, että jäsenvaltio vetoaa kansallisen oikeutensa säännöksiin, edes perustuslain tasoisiin säännöksiin, ei voi heikentää unionin oikeuden vaikutusta tämän jäsenvaltion alueella (ks. mm. asia 11/70, Internationale Handelsgesellschaft, tuomio 17.12.1970, 3 kohta ja asia C 409/06, Winner Wetten, tuomio 8.9.2010, 61 kohta ja erityisesti asia C-399/11, Melloni, tuomio 26.2.2013, k. 59).”

NIS2-direktiivin 6 artiklan 35 kohdan mukaisen julkishallinnon toimijan käsitteen ulkopuolelle jäävät kansalliset oikeuslaitokset, parlamentit ja keskuspankit. I 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 eduskunnan valtiopäivätoiminnan perustuslaillinen asema sitä edellyttää.

Kyberturvallisuuslakiin ei esitetä tiedonhallintalakia vastaavia soveltamisalaa taikka valvovan viranomaisen toimivaltaa koskevia yleisiä rajauksia, koska tässä kuvatut perustuslaillisten näkökohtien nojalla merkitykselliset valtioelimet ja viranomaiset eivät tarjoa palveluja kyberturvallisuuslain liitteissä tarkoitetuilla toimialoilla eivätkä siten tulisi lain soveltamisalaan. NIS2-direktiivin liitteessä tarkoitetun julkishallinnon toimialan osalta toimijoiden velvoitteista ja niiden noudattamisen valvonnasta säädettäisiin tiedonhallintalaissa, vaikka harjoittaessaan muuta NIS2-direktiivin liitteessä tarkoitettua toimintaa, myös viranomainen voisi tulla eräissä tilanteissa kyberturvallisuuslain soveltamisalaan. Tämän johdosta eräiden seuraamusten osalta (johdon toiminnan rajoittaminen ja hallinnollinen seuraamusmaksu) kyberturvallisuuslaissa kuitenkin rajattaisiin julkishallinto kattavasti mainittujen seuraamusten soveltamisen ulkopuolelle, koska osa julkishallinnon toimialan toimijoista (esimerkiksi hyvinvointialueet ja hyvinvointiyhtymät) kuuluisivat tiedonhallintalain ohella kyberturvallisuuslain soveltamisalaan, koska ne harjoittavat lain liitteessä tarkoitettua toimintaa.

Julkisen hallintotehtävän antaminen muulle kuin viranomaiselle

Kyberturvallisuuslain 29 §:n nojalla valvova viranomainen voisi tehdä toimijaa koskevan tarkastuksen käyttäen apunaan tarkastuksen suorittamisessa tietoturvallisuuden arviointilaitosta tai ulkopuolista tietotekniikan asiantuntijaa, jos se on tarkastuksen laadun tai siihen liittyvien teknisten syiden vuoksi tarpeellista. Myös ehdotetun tiedonhallintalain 18 k §:n nojalla Liikenne- ja viestintävirasto voisi antaa tarkastustehtävään liittyvän avustavan tehtävän tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle. Ehdotukset ovat merkityksellisiä perustuslain 124 §:n kannalta, jonka mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se

on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Tarkastuksen suorittamisessa lähtökohtana olisi se, että valvova viranomainen suorittaa itse tarkastuksen. Ulkopuolisen asiantuntijan käyttämisen tarve koskisi tilannetta, jossa tarkastuksen kohdistuisi sellaisiin seikkoihin, joiden tarkastaminen vaatisi sellaista teknistä erityisosaamista tai poikkeuksellista osaamista, jota viranomaisella itsellään ole hallussa. Valvova viranomainen ei myöskään voisi siirtää tehtävää kokonaisuudessaan tietoturvallisuuden arviointilaitoksen tai ulkopuolisen asiantuntijan suoritettavaksi, vaan vastuu tarkastustehtävän suorittamisesta säilyisi valvovalla viranomaisella myös silloin, kun se olisi päättänyt käyttää tarkastuksessa apuna tietoturvallisuuden arviointilaitosta tai ulkopuolista asiantuntijaa.

Elinkeinovapaus

Esitykseen sisältyy ehdotus soveltamisalaan kuuluvien toimijoiden velvollisuudesta ilmoittaa valvovalle viranomaiselle kyberturvallisuuslain 41 §:ssä tarkoitetut tiedot toimijaluettelon ylläpitämiseksi. Lisäksi sähköisen viestinnän palveluista annetun lain 165 §:ssä säädettäisiin nykyistä yksityiskohtaisemmin verkkotunnusvälittäjän tiedoista, jotka on ilmoitettava ennen toiminnan aloittamista. Ehdotukset tarkoittaisivat käytännössä soveltamisalaan kuuluvan toimijan ilmoitusvelvollisuutta toiminnasta valvovalle viranomaiselle ja ne olisivat siten merkityksellisiä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta. Ehdotuksilla pantaisiin täytäntöön NIS2-direktiivi säännös, joka edellyttää ilmoitusvelvollisuuden mukaisten tietojen keräämistä näiltä toimijoilta. Lisäksi ilmoittautumisvelvollisuus toisi valvovan viranomaisen tietoon kyberturvallisuuslain soveltamisalaan kuuluvat toimijat ja mahdollistaisi valvonnan kohdentamisen näihin toimijoihin. Ilmoitusvelvollisuutta koskevat säännökset ovat täsmällisiä ja tarkkarajaisia. Ilmoituksen vastaanottava viranomainen ei tee ilmoituksen johdosta päätöstä eikä ilmoittamista ole asetettu elinkeinotoiminnan harjoittamisen ehdoksi. Ilmoituksen tekemättä jättäminen olisi kuitenkin sanktioitu hallinnollisella seuraamusmaksulla.

Esitykseen sisältyy luvanvaraisen toiminnan rajoittamista tai luvan peruuttamista koskevia ehdotuksia, jotka ovat merkityksellisiä perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta. Luvan peruuttamista koskevia ehdotuksia olisivat sähkö- ja maakaasumarkkinoiden valvonnasta annetun lain 23 §:n, maa-asemista ja eräistä tutkista annetun lain 8 §:n ja 260 vaarallisten kemikaalien ja räjähteiden käsittelyn turvallisuudesta annetun lain 109 §:n muutokset. Ehdotuksilla pantaisiin osin täytäntöön NIS2-direktiivin 32 artiklan 5 kohta, joka ei sisällä kansallista liikkumavaraa. Luvanvaraisen toiminnan rajoittamista tai luvan peruuttamista koskevat ehdotukset kohdistuisivat vain sellaiseen toimintaan, joka on jo aiemmin säädetty luvanvaraiseksi. Muutokset eivät myöskään vaikuttaisi kyseisten lupien myöntämisen edellytyksiin, vaan niissä on kyse jo myönnetyn toimiluvan muuttamisesta tai peruuttamisesta tilanteessa, jossa luvanhaltija ei ole noudattanut siihen kohdistuvia laissa säädettyjä velvoitteita. Luvan peruuttaminen olisi sidottu vakavaan ja olennaiseen laiminlyöntiin sekä siihen, että laiminlyönti on siten toistuvaa, että viranomaisen antama huomautus tai varoitus ei ole johtanut korjaaviin toimenpiteisiin. Luvan peruuttaminen olisi viimesijainen keino puuttua lain vastaiseen menettelyyn suhteessa muihin valvovan viranomaisen toimivaltuuksiin.

Kyberturvallisuuslain 32 §:n mukaan valvova viranomainen voisi kieltää henkilöä toimimasta keskeisen toimijan hallituksen jäsenenä ja varajäsenenä, hallintoneuvoston jäsenenä ja varajäsenenä, toimitusjohtajana tai muussa siihen rinnastettavassa asemassa, jos tämä on toistuvasti ja vakavasti rikkonut johdon vastuusta 10 §:ssä säädettyjä velvoitteita. Päätös voisi olla voimassa enintään niin kauan, kuin sen perusteena oleva puute tai laiminlyönti on korjaamatta ja

kuitenkin enintään viisi vuotta. Ehdotuksella pantaisiin täytäntöön NIS2-direktiivin 32 artiklan 5 kohdan valvovalta viranomaiselta edellyttämä toimivalta. Ehdotus on merkityksellinen perustuslain 18 §:ssä turvatun elinkeinovapauden kannalta. Toimintakieltoa koskeva säännös on lain tasoinen, täsmällinen ja perusteeltaan hyväksyttävä. Rajoitus kohdistuisi luonnollisen henkilön toimintaan yksittäisen toimijan tietyissä johtotehtävissä. Kielto ei olisi yleinen kielto, vaan kohdistuisi täsmällisesti tietyn luonnollisen henkilön toimintaan tietyn toimijan ylimpään johtoon kuuluvassa tehtävässä. Edellytyksenä olisi varoitus ja laiminlyönti korjata valvovan viranomaisen osoittama puute tai laiminlyönti kohtuullisessa määräajassa. Kielto ei rajoittaisi luonnollisen henkilön muuta elinkeinoharjoittamista tai mahdollisuutta toimia valitsemassaan ammatissa.

Hallinnollinen seuraamusmaksu

Kyberturvallisuuslain 5 luvussa säädettäisiin NIS2-direktiivin edellyttämällä tavalla hallinnollisen seuraamusmaksun määräämisestä toimijalle, joka tahallaan tai törkeästä huolimattomuudesta laiminlöisi laissa säädettyä riskienhallintavelvoitetta, ilmoitusvelvollisuutta merkittävistä poikkeamista tai laissa säädetyn ilmoituksen tekemisestä toimijaluetteloa varten. Kysymys olisi lainvastaisesta teosta määrättävästä sanktioluonteisesta hallinnollisesta seuraamuksesta, joka voisi olla määrällisesti huomattava. Laissa säädettäisiin täsmällisesti, tarkkarajaisesti ja tyhjentävästi teosta tai laiminlyönnistä, joka voisi olla toimijaan kohdistuvan seuraamusmaksun määräämisen perusteena. Seuraamusmaksun määräämistä ehdotetaan monijäsenisen elimen tehtäväksi oikeusturvaan liittyvistä syistä. Seuraamusmaksun määräisi seuraamusmaksulautakunta, joka koostuisi valvovien viranomaisten nimeämistä jäsenistä. Seuraamusmaksulautakunta tekisi aina päätöksensä esittelystä. Hallinnollista seuraamusmaksua ei voitaisi määrätä viranomaiselle.

Yhteenveto

Hallituksen esityksen perustuslain kannalta merkityksellisten ehdotuksien arvioidaan olevan täsmällisiä, tarkkarajaisia, ja perustellussa suhteessa niiden tarkoitukseen ja suojeltavaksi pyrittäviin oikeushyviin nähden. Ehdotuksilla ei puututa perustuslaissa turvattujen oikeuksien ydinalueelle. Ehdotettu sääntely on rajattu siihen laajuuteen, jota NIS 2 -direktiivin täytäntöönpano vähimmäistasolla edellyttää ja jonka on katsottava olevan sen taustalla olevien tavoitteiden toteutumisen kannalta välttämätöntä ja oikeasuhtaista.