

Lausunto

29.11.2023

VN/18157/2023
VN/18157/2023-OM-22

Liikenne- ja viestintäministeriö

Oikeusministeriön lausunto luonnoksesta hallituksen esitykseksi kyberturvallisuudirektiivin (NIS 2 – direktiivi) täytäntöönpanemiseksi

Liikenne- ja viestintäministeriö on pyytänyt oikeusministeriöltä lausunnon luonnoksesta hallituksen esitykseksi kyberturvallisuudirektiivin (NIS 2 – direktiivi) täytäntöönpanemiseksi. Esitysluonnoksessa ehdotetaan säädettäväksi uusi laki kyberturvallisuuden riskienhallinnasta ja muutettavaksi useita muita lakeja. Esitysluonnoksessa ehdotetaan myös kumottavaksi tiettyjä lainkohtia useista laeista. Oikeusministeriö on ollut edustettuna esitystä valmistelleessa työryhmässä, mutta aikataullisista syistä ei ole pystynyt kommentoimaan valmistelun aikana kaikkia yksityiskohtia, vaan osa on jouduttu jättämään jatkovalmistelun varaan. Oikeusministeriö toteaa lausuntonaan seuraavan.

Laki kyberturvallisuuden riskienhallinnasta

1.

Lain 3 §:n 3 momentin mukaan valtioneuvoston asetuksella säädettäisiin kyseisen lain soveltamisesta sellaiseen lain liitteessä I tai II tarkoitettua toimintaa harjoittavaan tai toimijatyyppiä olevaan toimijaan sen koosta riippumatta, jos 1) toimija tarjoaa ainoana palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen; 2) häiriö toimijan tarjoamassa palvelussa vaikuttaisi merkittävästi yleiseen järjestykseen, yleiseen turvallisuuteen tai kansanterveyteen; 3) häiriö toimijan tarjoamassa palvelussa voisi aiheuttaa merkittävän systeemisen riskin erityisesti aloilla, joilla tällaisella häiriöllä voisi olla rajat ylittäviä vaikutuksia; tai 4) toimija on kriittinen, koska sillä on erityisen suuri merkitys kansallisella tai alueellisella tasolla kyseisen toimialan tai palvelutyyppin tai jäsenvaltion muiden keskinäisriippuvaisten toimialojen kannalta.

Säännös vastaisi alakohtiensa 1-4 osalta NIS 2 –direktiivin 2 artiklan 2 kohdan alakohdissa b-e säädettyä. Säännöksen säännöskohtaisissa perusteluissa (HE-luonnos s. 114) todetaan, että lainsäädäntövallan siirto olisi lakiteknisesti tarpeen, sillä kysymys olisi hyvin yksityiskohtaisesta toimijoiden määrittämisestä, jotka toiminnan erityisen laadun vuoksi kuuluisivat poikkeuksellisesti lain ja NIS 2 –direktiivin velvoitteiden soveltamisalaan toimijan koosta riippumatta. Soveltamisala näitä toimijoita koskien olisi perustelujen mukaan myös altis muutoksille jatkossa, jos toimijoiden toiminnan laatu tai koko muuttuvat tai tiettyjen sektorien kannalta kriittiset toimijat vaihtuvat.

Esitysluonnoksen suhdetta perustuslakiin ja säätämisyjärjestystä koskevassa jaksossa (s. 200) viitataan säännöskohtaisten perustelujen tapaan lakitekniiseen tarpeeseen. Esitysluonnoksessa todetaan, että ehdotus vastaa perustuslain 80 §:n 1 momentin edellytyksiä asetuksenantovaltuudelle siten, että lailla säädetään yksilön oikeuksien ja velvollisuuksien perusteista, ja yksityiskohtainen ja teknisluontoinen poikkeuksellisesti koosta riippumatta sovellettavien toimijoiden määrittely voitaisiin jättää asetuksen tasolle.

Postiosoite
Postadress
Postal Address
Oikeusministeriö

Käyntiosoite
Besöksadress
Office

Puhelin
Telefon
Telephone

Faksi
Fax
Fax

s-posti, internet
e-post, internet
e-mail, internet

PL 25
00023 Valtioneuvosto

Eteläesplanadi 10
Helsinki

0295 16001
+358 295 16001

09 1606 7730
+358 9 1606 7730

kirjaamo.om@gov.fi
oikeusministerio.fi

Perustuslain 80 §:n 1 momentin mukaan tasavallan presidentti, valtioneuvosto ja ministeriö voivat antaa asetuksia perustuslaissa tai muussa laissa säädetyn valtuuden nojalla. Lailla on kuitenkin säädettävä yksilön oikeuksien ja velvollisuuksien perusteista sekä asioista, jotka perustuslain mukaan muuten kuuluvat lain alaan. Jos asetuksen antajasta ei ole erikseen säädetty, asetuksen antaa valtioneuvosto.

Lain soveltamisalan määrittelyllä on keskeinen vaikutus siihen, kuka tai mikä on lain nojalla oikeutettu tai velvoitettu johonkin. Lausuttavana olevan lakiehdotuksen 3 §:n 1 ja 2 momenttien nojalla lain velvoittavuus tiettyihin toimijoihin osoitettaisiin tarkemmin lain liitteiden avulla. Toimijoiden tulisi siis ilmeisesti näin ollen lähtökohtaisesti itse todeta lain ja sen liitteiden perusteella, kuuluisivatko ne lain soveltamisalaan, ja olisivat niin ollen lain velvoitteiden piirissä (esitysluonnoksen perusteluissa s. 50 todetaan: ”toimijoiden velvollisuutena olisi itse tunnistaa, kuuluvatko he sääntelyn soveltamisalaan, sekä ilmoittautua valvovalle viranomaiselle toimijaluetteloon”). Lakiluonnoksen 43 §:n mukaan toimijoiden tulisi – tunnistettuaan itsensä lain velvoitteiden piiriin kuuluvaksi – ilmoittaa valvovalle viranomaiselle erinäisiä tietoja toimijaluettelon ylläpitämiseksi.

Huomioitavaa on myös, että lain 4 §:ssä säädettäisiin soveltamisalan rajauksista, joiden nojalla tietyt kriteerit täyttävät toimijat voisivat katsoa olevansa lain soveltamisalan ulkopuolella.

Asian arviointia vaikeuttaa se, ettei lausuttavana olevan esitysluonnoksen mukana ole luonnosta ko. valtioneuvoston asetukseksi.

Oikeusministeriö ei pidä kaikilta osin mahdollisena eikä toisaalta tarpeellisena sääntelytapana 3 §:n 3 momentissa valtioneuvostolle osoitettua asetuksenantovaltuutta. Ensinnäkin momentin 1-4 kohdissa olevia määritelmiä toimijan palvelujen merkityksestä voinee pitää jo siinä määrin yksilöivinä, että ko. toimijoiden tulisi niiden perusteella tunnistaa itsensä ja lain 43 §:n nojalla ilmoittaa itsensä toimijaluetteloon. Asetuksenantovaltuus vaikuttaisi tästä näkökulmasta tarpeettomalta. Toisena seikkana on perusteltua tarkastella sitä, voidaanko lain soveltamisalan määrittelyä delegoida pois lainsäätäjältä.

Perustuslakivaliokunnan mukaan lain soveltamisalan sääntely asetuksella on perustuslain 80 §:n ja säädösten hierarkkisten suhteiden näkökulmasta ongelmallista. Perustuslakivaliokunta on tosin todennut, että asetuksella voidaan säätää esimerkiksi lain soveltamisen kannalta vähäisen teletoininnan rajaamisesta lain soveltamisalan ulkopuolelle, kun asetuksenantajan toimivalta on riittävästi rajattu (PeVL 8/2002 vp, s. 3; ks. myös PeVL 14/2005 vp, s. 3). Kun toiminnan *rajaaminen lain soveltamisalan ulkopuolelle* asetuksenantovaltuuden nojalla voi olla asetuksenantajan tarkoin rajatulla toimivallalla ja merkitykseltään vähäisehköissä asioissa mahdollista, ei kuitenkaan siitä ole suoraan johdettavissa, onko nyt lausuttavana olevassa asiayhteydessä – jossa olisi kyse päinvastoin lain soveltamisalan ulottamisesta (soveltamisalan laajentamisesta) asetuksella tiettyihin toimijoihin, joiden toiminta on yhteiskunnan kannalta merkittävää tai kriittistä – kyse asialliselta merkitykseltään sellaisista asioista, joiden osalta perustuslakivaliokunta olisi katsonut, että soveltamisalasta säätäminen asetuksella on mahdollista.

Kolmantena seikkana, lain soveltamisalan määrittäminen asetuksenantovaltuuden ja sen nojalla annettavan asetuksen perusteella on hyvin ongelmallinen myös laillisuusperiaatteen toteutumisen kannalta, kun toimijan joutuminen mahdollisesti hyvin suurenkin seuraamusmaksun kohteeksi voisi johtua asetuksenantajan harkinnasta, eikä perustuisi laillisuusperiaatteen edellyttämällä tavalla suoraan lakiin. Laki voisi tulla sovellettavaksi niin oikeushenkilöihin kuin luonnollisiin henkilöihin.

Oikeusministeriö katsoo, että ehdotettu huomattavan väljä asetuksenantovaltuus, joka merkitsee lain soveltamisalan määrittämistä asetuksella, ei ole perustuslain näkökulmasta mahdollinen. Ehdotettu sääntely merkitsisi sitä, että toimijoita velvoittava sääntely jäisi asetuksen varaan. Säännöstä on välttämätöntä tarkentaa siten, että riittävät perussäännökset perustuslain 80 §:n ja 8 §:n edellyttämällä tavalla ovat laissa. Mikäli 3 §:n 3 momentissa nyt olevaa asetuksenantovaltuutta ehdotetaan edellä esitetystä huolimatta säädettäväksi, on perusteltua pyytää kyseisen asetuksenantovaltuuden perustuslainmukaisuudesta perustuslakivaliokunnan kannanottoa.

2.

Lain 5 §:n 1 momentissa olisi säännös, jonka mukaan, jos muussa laissa on tästä laista poikkeavia säännöksiä, joilla varmistetaan korkeampi kyberturvallisuuden taso, niitä sovelletaan tämän lain lisäksi. Säännös on muotoiltu epäselvästi. Säännöksiä, joista poiketaan, ei ole mahdollista soveltaa ”lisäksi”. Kyseenalaista on, onko laissa sinänsä tarpeellista olla säännös, jonka mukaan muuta voimassa olevaa oikeutta voidaan soveltaa. Säännöksellä voisi ymmärtää olevan oikeudellista merkitystä lähinnä silloin, jos säädettäisiin, että jokin muu sääntely on sovellettavissa nyt kyseessä olevan sääntelyn asemesta.

Ehdotuksesta ei ilmene, mitä säännöksellä pyritään ilmaisemaan. Jatkovalmistelussa säännöstä tulee selkeyttää. Oikeusministeriö korostaa, että säädöksen soveltamisala ja säädöksen suhde muihin säädöksiin on oltava selkeä.

Luonnoksen perusteluissa todetaan, että yksinomaan julkishallinnon toimialaan kohdistuvista velvoitteista ja niiden noudattamisen valvonnasta säädettäisiin erikseen tiedonhallintalain ja että tiedonhallintalaki olisi erityislaki suhteessa esitettyyn kyberturvallisuuden riskienhallinnasta annettuun lakiin. (s. 47). Tämä ei kuitenkaan ole täysin selvää ehdotuksen perusteella. Näiden kahden lain välistä suhdetta tulisi jatkovalmistelussa selkeyttää säädösperusteisesti. Esimerkiksi 1. lakiehdotuksen perusteluissa todetaan, että keski-suurella toimijalla tarkoitettaisiin julkista tai yksityistä toimijaa. Ehdotetun sääntelyn perusteella ei vaikuta olevan yksiselitteistä, etteikö 1. lakiehdotus soveltuisi myös julkisiin toimijoihin (esim. 1. lakiehdotuksessa säädettäisiin toimivallasta määrätä seuraamusmaksuja keski-suurelle toimijalle. – vrt. PeVL 13/2023 vp, kohdat 7-10).

3.

Lain 14 §:n 3 momentin mukaan, jos merkittävästä poikkeamasta ilmoittaminen olisi yleisen edun mukaista, valvova viranomaisena voisi velvoittaa toimijan tiedottamaan asiasta tai kuultuaan ilmoitusvelvollista tiedottaa asiasta itse. Oikeusministeriö toteaa, että kuulemisvelvoite koskee myös tilannetta, jossa valvova viranomaisena velvoittaisi toimijan tiedottamaan asiasta (ja tekisi hallintopäätöksen). Sääntelyn osalta on sinänsä huomioitava, että hallintolain (434/2003) 34 § asettaa velvoitteen asianosaisten kuulemiseen, jolloin kuulemisesta erikseen säätämiseksi ei vaikuttaisi olevan tarvetta. Hallintolain 34 §:ssä säädetään myös niistä edellytyksistä, joiden perusteella asiaa saa ratkaista asianosaista kuulematta.

4.

Lakiluonnoksen 19 §:n 1 momentissa säännellään CSIRT-yksikköä. CSIRT-yksikkö toimisi Liikenne- ja viestintävirastossa ja sen olisi täytettävä NIS 2 –direktiivin 11 artiklan 1 kohdassa tarkoitettujen vaatimukset ja sen toiminta olisi järjestettävä erilliseksi 25 §:n nojalla tehtävästä valvontatoiminnosta.

Direktiivin 11 artiklan 1 kohdan mukaan CSIRT-yksiköiden on täytettävä seuraavat vaatimukset: a) CSIRT-yksiköiden on varmistettava viestintäkanaviensa kattava saatavuus välttämättä viestinnän täysin katkaisevia yksittäisiä vikaantumispisteitä ja ylläpidettävä useita viestintäkeinoja, joilla muut voivat ottaa niihin ja ne voivat ottaa muihin yhteyttä milloin tahansa. CSIRT-yksiköiden on määritettävä selkeästi viestintäkanavat ja tiedotettava niistä kohderyhmilleen ja yhteistyökumppaneilleen; b) CSIRT-yksiköiden toimitilat ja niiden toimia tukevat tietojärjestelmät on sijoitettava suojattuihin paikkoihin; c) CSIRT-yksiköillä on oltava tarkoituksenmukainen järjestelmä pyyntöjen hallintaa ja reititystä varten, erityisesti tapausten tulokset ja tehokkaan edelleenohjauksen helpottamiseksi; d) CSIRT-yksiköiden on varmistettava toimintonsa luottamuksellisuus ja luotettavuus; e) CSIRT-yksiköillä on oltava riittävä henkilöstö palvelujensa jatkuvan saatavuuden varmistamiseksi, ja niiden on varmistettava henkilöstönsä asianmukainen koulutus; f) CSIRT-yksiköillä on oltava varajärjestelmät ja -työtilat palvelujensa jatkuvuuden varmistamiseksi.

Perustuslakivaliokunta on pitänyt lähtökohtana, että kansallisia täytäntöönpanotoimia edellyttävät Euroopan unionin säädökset tulee pääsääntöisesti sisällyttää kansalliseen lainsäädäntöön EU-säädösten asiasisältöä vastaavilla kansallisilla säädöksillä. Perustuslakivaliokunta on pitänyt tietyin reunaehdoin mahdollisena sääntelyä, jossa lain tasolla viitataan teknisluonteisten ja yksityiskohtaisten vaatimusten osalta suoraan direktiivin säännöksiin. Kyse on tuolloin ollut varsin teknisluonteisesta ja yksityiskohtaisesta direktiivisääntelystä, joka on kohdistunut rajalliseen joukkoon ammattimaisia toimijoita, ja siitä, ettei jäsenvaltiolla ole sääntelyn aineellisen sisällön osalta kansallista liikkumavaraa. Perustuslakivaliokunta on korostanut, että viittaustekniikan käyttämistä direktiivin täytäntöönpanossa tulee pääsääntöisesti välttää. (ks. PeVL 34/2022 vp, s. 2-3 sekä siinä viitatuksi lausunnot)

Oikeusministeriö katsoo että – perustuslakivaliokunnan aiempi tulkintakäytäntö huomioon ottaen – CSIRT-yksikön direktiivin 11 artiklan 1 kohdassa tarkoitetuista vaatimuksista on säädettävä nimenomaisesti kansallisessa laissa, eikä jättää yksikölle asetettavien vaatimusten sääntelyä direktiiviviitauksen varaan.

Yleisesti ottaen esitysluonnoksen lakiehdotuksissa on varsin monta säännöstä, joissa viitataan direktiivin säännöksiin. Oikeusministeriö korostaa, että lähtökohtana tulee olla, että direktiiviä ei panna täytäntöön viittaustekniikalla. Sikäli kuin direktiiviin viittaaminen katsotaan säännöksessä perustelluksi – perustuslakivaliokunnan tulkintakäytäntö huomioon ottaen – tulee säännöksen perusteluissa asianmukaisesti todeta nimenomaisen viittaamisen tarve (teknisluonteinen syy tms.).

5.

Lain 19 §:n 6 momentissa olisi asetuksenantovaltuus, jonka mukaan liikenne- ja viestintäministeriön asetuksella säädettäisiin sellaisesta 19 §:n 2 momentin 1 ja 2 kohdassa sekä 20 §:n 4 momentissa tarkoitettua palvelusta perittävistä maksuista tai niiden perusteista, joka on tarjottu toimijan tai muun tahon pyynnöstä.

Oikeusministeriö toteaa, että valtion viranomaisten suoritteiden maksullisuuden ja suoritteista perittävien maksujen suuruuden yleisistä perusteista sekä maksujen muista perusteista säädetään valtion maksuperustelaissa (150/1992). Kyseisessä laissa on mm. säännökset siitä, että ministeriö päättää, mitkä ministeriön ja hallinnonalan muiden viranomaisten suoritteet tai suoriteryhvät ovat maksullisia ja mistä suoritteesta tai suoriteryhmästä maksu määrätään omakustannusarvon perusteella sekä mitkä suoritteet hinnoitellaan liiketaloudellisin perustein.

Valtion maksuperustelaki vaikuttaisi soveltuvan myös nyt lausuttavana olevaan lakiehdotukseen, jolloin 19 §:n 6 momentin asetuksenantovaltuutta voidaan pitää turhana. Vaikuttaisi myös siltä, ettei sääntely ehdotetussa muodossaan täyttäisi perustuslain 81 §:n 2 momentin vaatimusta siitä, että valtion viranomaisten virkatoimien, palvelujen ja muun toiminnan maksullisuuden sekä maksujen suuruuden yleisistä perusteista säädetään lailla. Liikenne- ja viestintäministeriö voi valtion maksuperustelain nojalla antaa asetuksen, jossa säädetään ko. maksuista. Oikeusministeriö pitää kuitenkin perusteltuna, että nyt lausuttavana olevassa laissa olisi säännös, jossa todettaisiin, että edellä viitatuista palveluista voidaan periä maksu.

6.

Lakiin luonnostellun 20 §:n 5 momentissa olevan säännöksen mukaan haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa ei saisi käsitellä sähköisten viestien sisältöä ilman viestinnän osapuolen suostumusta. Pykälän säännöskohtaisissa perusteluissa säännöstä ei mainita ja perustelut ovat säännöksen kanssa ristiriitaiset, kun niissä (s. 136) ykskantaan todetaan, että haavoittuvuuskartoituksessa tai kohdennetussa haavoittuvuuskartoituksessa ei saisi käsitellä tietoja sähköisten viestien sisällöstä. Myöskään esityksen suhdetta perustuslakiin ja säätämisjärjestystä koskevassa jaksossa osapuolen suostumuksen merkityksen arviointia ei suoriteta.

Kaavailtu sääntely on merkityksellinen perustuslain 10 §:n 2 momentissa turvatun luottamuksellisen viestin salaisuuden suojan kannalta. Kyseessä voi siis todeta olevan perusoikeuden rajoittamisen, vaikkakin se tässä tapauksessa ainakin osittain perustuisi perusoikeussuojaa nauttivan nimenomaiseen suostumukseen. Huomionarvoista on, että nyt kyseessä olevassa sähköisessä viestinnässä säännöksen tarkoittaman viestinnän osapuolia on vähintään kaksi, mutta usein myös useampia. Esitysluonnoksessa ei oteta erikseen kantaa siihen tilanteeseen, että suostumus tulisi hankkia mahdollisesti hyvinkin monelta eri ko. viestinnän osapuolelta, tai ylipäätään millä tavalla suostumus teknisesti pyydetäisiin (esim. suostumuslomakkeella). Viestinnän yhden osapuolen suostumus ei tarkoita sitä, että myös muut viestinnän osapuolet olisivat antaneet suostumuksensa.

Perustuslakivaliokunta on katsonut perusoikeusrajoituksen kohteeksi joutuvan henkilön suostumuksella voivan sinänsä olla merkitystä valtiosääntöoikeudellisessa arvioinnissa. Valiokunta on kuitenkin käytännössään pitänyt tällaista sääntelytapaa ongelmallisena ja korostanut suurta pidättyväisyyttä suostumuksen käyttämisessä perusoikeuksiin puuttumisen oikeutusperusteena. Valiokunnan mukaan tällainen sääntelytapa ei ole helposti sovitettavissa yhteen sen perustuslain 2 §:n 3 momentissa vahvistettuun oikeusvaltioperiaatteeseen sisältyvän vaatimuksen kanssa, jonka mukaan julkisen vallan käytön tulee perustua lakiin. Toimivallasta puuttua yksilön perusoikeuksiin on lisäksi aina säädettävä riittävän tarkkarajaisella ja soveltamisalaltaan täsmällisellä lailla. Valiokunta onkin pitänyt selvänä, että perusoikeussuoja ei voi oikeudellisenä kysymyksenä menettää aina merkitystään pelkästään siksi, että laissa säädetään jonkin toimenpiteen vaativan kohdehenkilön suostumusta. Perusoikeussuojaa ei voida millaisessa asiassa tahansa jättää riippumaan asianomaisen suostumuksesta. Valiokunta on pitänyt tässä suhteessa oleellisena sitä, mitä voidaan pitää oikeudellisesti relevanttina suostumuksena tietystä tilanteesta, ja edellyttänyt suostumuksenvaraisesti perusoikeussuojaan puuttuvalta lailta muun muassa tarkkuutta ja täsmällisyyttä, säännöksiä suostumuksen antamisen ja sen peruuttamisen tavasta, suostumuksen aitouden ja vapaaseen tahtoon perustuvuuden varmistamista sekä sääntelyn välttämättömyyttä. (ks. PeVL 1/2018 vp, s. 8)

Mainitun 20 §:n 5 momentin suostumussääntelyn kanssa ristiriitaiselta vaikuttaa saman pykälän 2 momentissa oleva säännös, jonka mukaan haavoittuvuuskartoituksella ei saisi hankkia tietoa yleisessä viestintäverkossa tai yleisesti saatavilla olevassa viestintäpalvelussa välitettävänä olevasta viestinnästä. Eli jos ei saisi hankkia tietoa viestinnästä, miten silloin säädettäisiin suostumuksen pyytämisestä sähköisten viestin sisällön käsittelemiseen?

Oikeusministeriö pitää välttämättömänä, että esityksen jatkovalmistelussa kaavailtu suostumussääntely perustellaan asianmukaisella tarkkuudella ja siihen liittyvät valtiosääntöiset näkökohdat arvioidaan esityksen säätämisyjärjestysperusteluissa. Ehdotettu sääntely ei myöskään saa muodostua siällöllisesti ristiriitaiseksi.

7.

Lain 22 §:ssä säädettäisiin kyberturvallisuustietojen vapaaehtoisista jakamisjärjestelyistä. Oikeusministeriö kiinnittää huomiota siihen, että pykälän 1 ja 3 momenteissa säädettäisiin ko. laissa säädettyjen toimijoiden ja CSIRT-yksikön ohella ”muista tahoista”, jotka voisivat muodostaa keskenään vapaaehtoisia jakamisjärjestelyjä ja voisivat käsitellä pykälän nojalla saamia tietoja. Pykälän säännöskohdainten perustelujen mukaan (s. 137) 22 §:llä täytäntöönpantaisiin NIS 2 –direktiivin 29 artikla. Mainitun artiklan 1 kohdan mukaan jäsenvaltioiden on varmistettava, että tämän direktiivin soveltamisalaan kuuluvat toimijat ja tapauksen mukaan muut toimijat, jotka eivät kuulu tämän direktiivin soveltamisalaan, voivat vapaaehtoisesti vaihtaa keskenään asiaankuuluvia kyberturvallisuustietoja, mukaan lukien tietoja kyberuhkista, läheltä piti -tilanteista, haavoittuvuuksista, tekniikoista ja menettelyistä, vaarantumisindikaattoreista, kyberhyökkäystaktiikoista, yksittäisistä uhkatoimijoista, kyberturvallisuushälytyksistä ja suosituksista.

Oikeusministeriön mielestä em. ”muut tahot” on säännösten erittäin epämääräinen ilmaisu sen suhteen, kuka tai mikä voisi osallistua vapaaehtoisin jakamisjärjestelyihin, joihin kuitenkin voisi sisältyä kriittistä tietoa esimerkiksi erilaisista uhkatekijöistä ja haavoittuvuuksista. Lisäksi ehdotetun 22 §:n 4 momentin nojalla jakamisjärjestelyn piiriin voisi kuulua myös tieto kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä. Pykälän perustelujen (s. 137) mukaan ”Kun CSIRT-yksikkö tukee jakamisjärjestelyä jakamalla kyberturvallisuustietoja jakamisjärjestelyyn osallistuville, olisi kyseiseen vapaaehtoiseen jakamisjärjestelyyn osallistuvalla taholla erikseen laissa säädetty tiedonsaantioikeus niihin tietoihin, joita kyberturvallisuustietojen vapaaehtoisessa jakamisjärjestelyssä jaetaan. Näin ollen kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn osallistuvat tahot voisivat saada kyseiset tiedot tiedonhallintalain 22 ja 24 §:ssä tarkoitetulla tavalla.”

Oikeusministeriön mielestä olisi välttämätöntä tarkentaa perustelut huomioon ottaen em. säännöksiä siten, että ”muiden tahojen” oikeus tiedonsaantiin nimenomaisesti säännösten kytkeäisiin erikseen laissa säädettyyn tiedonsaantioikeuteen (”muiden erikseen lailla tiedonsaantiin oikeutettujen tahojen” / ”muut erikseen lailla tiedonsaantiin oikeutetut tahot”).

Lisäksi 22 §:n ja 4 §:n 5 momentin suhteesta tulisi tehdä selkoa. Ehdotetun 4 §:n 5 momentin mukaan tässä laissa ei veloiteta sellaisen tiedon antamiseen, jonka luovuttaminen vaarantaisi maanpuolustusta tai kansallista turvallisuutta taikka olisi vastoin siihen liittyvää tärkeää etua. Epäselvää on, voisivatko 22 §:ssä tarkoitetut vapaaehtoiset jakamisjärjestelyt kuitenkin koskea tällaisia tietoja.

8.

Lain 25 §:ssä säädettäisiin valvovista viranomaisista, joita olisivat Liikenne- ja viestintävirasto, Energiavirasto, Turvallisuus- ja kemikaalivirasto, Sosiaali- ja terveysalan lupa- ja valvontavirasto, Etelä-Savon elinkeino-, liikenne-, ja ympäristökeskus, Ruokavirasto, sekä Lääkealan turvallisuus- ja kehittämiskeskus. Kukin valvova viranomainen valvoisi saman lainsäädännön noudattamista, mutta oman toimialansa toimijoita ja pykälässä valvontavastuut on jaettu viittaamalla lain liitteiden kohtiin. Pykälän 3 momentin mukaan, jos 1 momentin nojalla samaa toimijaa valvoisi useampi kuin yksi viranomainen, kukin valvova viranomainen valvoisi toimijaa vain 1 momentissa tarkoitetun toiminnan osalta. Valvovien viranomaisten olisi tehtävä yhteistyötä valvonnan toteuttamisessa.

Esitysluonnoksen perusteluissa (s. 97) usean valvojan malli nähdään perusteltuna mm. siitä syystä, että NIS 2 –sektoreilla on olemassa olevia valvontaviranomaisia, jotka valvovat niille sektorikohtaisessa lainsäädännössä määritettyjä kokonaisuuksia tai osa-alueita muun ohella turvallisuuden ja riskienhallinnan osalta. Mikäli viranomaistehtävät keskitettäisiin jatkossa vain yhdelle viranomaiselle, se voisi esitysluonnoksessa todetun mukaan aiheuttaa päällekkäisiä valvontatoimivaltuuksia sekä päällekkäisiä raportointivelvollisuuksia toimijoille. Valvonnan järjestämistä sektorikohtaisesti puoltaa esitysluonnoksessa todetun mukaan myös se, ettei kyberturvallisuus ole valvottavan toimijan muusta toiminnasta erillinen osa, vaan yhteiskunnan digitalisoituessa kyberturvallisuus hahmotetaan toiminnan kokonaisturvallisuuden osa-alueena. Valvontamallin osalta todetaan toisaalta myös (s. 96), että valvonnan keskittäminen Liikenne- ja viestintäviraston Kyberturvallisuuskeskukselle olisi haasteellista sen nykyisten tehtävien kannalta.

Keskitettyssä valvontamallissa nähdään esitysluonnoksessa ainoana vaihtoehtona kokonaan uuden valvontaviranomaisen tai jonkin viranomaisen yhteydessä olevan erillisen valvontayksikön perustami-

nen. Tällöin valvontaviranomaisen valvontakenttä muodostuisi laajaksi (s. 97). Esitysluonnoksen mukaan toimijoiden määrä ja laatu sekä toiminnan yhteiskunnallinen merkittävyys vaihtelevat toimialakohtaisesti, mikä puoltaa valvontamallia, jossa toimialakohtaiset erityispiirteet sekä toimialakohtaisen muuta kuin kyberturvallisuutta koskevan turvallisuuden ja riskienhallinnan sääntely voidaan yhteensovittaa mahdollisimman hyvin NIS 2 –valvontaan. Myös kustannustekijät puoltaisivat esitysluonnoksen mukaan hajautettua valvontaa. Toisaalta perustelujen mukaan nykyisistä viranomaisista yhdelläkään ei ole ehdotetun sääntelyn edellyttämää laaja-alaista osaamista eri toimialojen erityispiirteistä ja kyberturvallisuudesta.

Oikeusministeriö kiinnittää huomiota siihen, että vaihtoehtoisten toteuttamistapojen punninnassa viitataan Kyberturvallisuuskeskukseen, joka ei ole organisatorisesti itsenäinen viranomainen, vaan osa Liikenne- ja viestintävirastoa. Sen sijaan perusteluissa tulisi ennemmin arvioida vaihtoehtoisena toteutustapana mahdollisuutta keskittää valvontatehtävä Liikenne- ja viestintävirastolle. Se voisi edellyttää sinänsä valvontatehtävän rakentamista tai uuden yksikön luomista viranomaiseen, mutta kyseessä ei olisi uuden valvontaviranomaisen perustaminen. Liikenne- ja viestintävirastoon jouduttaneen joka tapauksessa luomaan tällainen tehtävä, kun viranomaisiin kohdistuva valvontatehtävä keskitettäisiin sille. Koska ehdotusta perustellaan mm. kustannustekijöillä, toteutustapojen punninnassa olisi syytä kiinnittää tarkemmin huomiota vaihtoehtoisten toteutustapojen kustannusten vertailuun. Esitysluonnoksen valossa usean viranomaisen resursseja jouduttaisiin joka tapauksessa lisäämään, huomioiden tarpeen varmistaa myös laaja-alainen osaaminen kyberturvallisuudesta, jolloin arviota hajautetun ratkaisun vähemmistä kustannuksista voitaneen kyseenalaistaa.

Oikeusministeriön mielestä esitysluonnoksessa esitetyistä perusteista huolimatta, kyberturvallisuuden valvonnan hajauttaminen usealle eri viranomaiselle on ongelmallista myös arvioitaessa esimerkiksi kyberturvallisuuden valvontatehtävän horisontaalista merkitystä (vrt. tietosuojalainsäädännön noudattamisen valvonta), oikeusturvan toteutumista ja esitysluonnoksessa kaavailtua viranomaisen normintovaltaa.

NIS 2 –direktiivin lähtökohtana on kyberturvallisuuden yhteisen korkean tason varmistaminen, joka tulee kansallisessa laissa panna täytäntöön. Lain toteutumisen valvonnan kannalta voi pitää perusteltuna, että kansallisesti on olemassa riittävillä voimavaroilla ja asiantuntemuksella varustettu valvontaviranomainen. Hajautettu valvontamalli ei mahdollistaisi kunkin valvontaviranomaisen kohdalla kovinkaan suuria resursseja (arviot resurssitarpeista s. 82-84), joka esityksen perusteella vaikuttaisi myös siihen, että valvontatoiminta olisi rajattu virka-ajan puitteisiin, eikä valmiutta päivystää viikonloppuisin, öisin tai arkipyhinä olisi (s. 130). Keskitetyn valvontamallin etuna voi pitää sitä, että valvontatoiminta olisi rutinoituneempaa, jolloin valmiudet poikkeuksellisiin tilanteisiin olisivat jo lähtökohtaisesti korkeammalla tasolla. Keskitetyn valvontamallin osalta tulisi perusteluissa myös huomioida osaamisen keskittyminen ja kehittyminen sekä valmiudet ratkaista myös harvemmin esiin nousevia erityiskysymyksiä.

Perustuslain näkökulmasta keskeistä on, että viranomaisen toimivalta perustuu lakiin ja toimivaltaisesta viranomaisesta ei ole epäselvyyttä. Viranomaisten toimivaltajärjestelyt eivät myöskään saa vaarantaa oikeusturvaa eikä hyvää hallintoa. Tämä merkitsee mm. sitä, että valvottaville tulee olla selvää, mikä viranomainen kulloinkin on toimivaltainen. Ehdotettu järjestely, jossa asetuksen velvoitteita valvoisi ja valvontaviranomaisen toimivaltaa käyttäisi seitsemän viranomaista on hyvin poikkeuksellinen, eikä vaikuta ongelmattomalta. On syytä huomata, että olemassa olevia viranomaisten laissa säädettyjä tehtävä- ja toimivaltarajoja on mahdollista muuttaa uudenlaisen sääntelyn tätä edellyttäessä.

Huomiota voidaan kiinnittää myös siihen, että nk. julkishallinnon toimialalla (2. lakiehdotus) valvovia viranomaisia olisi vain yksi eli Liikenne- ja viestintävirasto, vaikka myös julkishallinnon toimiala sisältää useita erilaisia toimijoita. Viimeksi mainitun osalta esitysluonnoksen perusteluissa (s. 100) todetaan, että valvontatehtävän jakaminen useammalle viranomaiselle ei olisi tarkoituksenmukaista.

Oikeusturvan osalta merkityksellistä on, että valvonnan hajautuessa ehdotetulla tavalla hyvin monelle eri viranomaiselle, lain valvontaan liittyvät soveltamiskäytännöt saattavat eriytyä tavalla, joka asettaa oikeusturvan tasoa erisuhtaiseksi. Kun valvontaviranomaisille ehdotetaan merkittäviä toimivaltuuksia, mm. johdon toiminnan rajoittaminen, elinkeinolupiin puuttuminen, rajat ylittävä yhteistyö, määräyksenantovaltuudet, valvontatoimivaltuudet sekä merkittävän suurien seuraamusmaksujen esittäminen lautakunnan päätettäväksi, näin merkittävät toimivaltuudet olisi perusteltua keskittää mm. osaamisen, valvonnan yhdenmukaisuuden ja tehokkuuden sekä oikeusturvan toteutumisen näkökulmasta yhdelle valvovalle viranomaiselle. Lisäksi tällainen järjestely vaikuttaa olevan myös omiaan aiheuttamaan toimivaltapaäselvyyksiä viranomaisten välille. Jatkovalmistelussa ehdotettua hajautettua valvovien viranomaisten järjestelmää on syytä tarkastella kriittisesti uudelleen tässä esitetty huomioiden.

Viranomaisten norminantovaltan osalta huomioon otettavaa on, että esitysluonnoksessa ehdotetaan norminantovaltuuksia valvontaviranomaisille. Ehdotetun 9 §:n 4 momentin nojalla valvova viranomainen voisi toimialallaan antaa tarkempia teknisiä määräyksiä: 1) kyberturvallisuuden riskienhallinnan

toimintamallissa huomioitavista osa-alueista ja riskienhallinnan ja viestintäverkkojen ja tietojärjestelmien tietoturvallisuuden hallinnan menettelyistä; 2) kehittämisen ja ylläpidon sekä haavoittuvuuksien käsittelyn menettelyistä; 3) omaisuudenhallinnasta ja toimintojen tärkeysluokittelun perusteista; 4) henkilöstöturvallisuuden, kyberturvallisuuskoulutuksen, poikkeamien havainnoinnin ja hallinnan sekä jatkuvuuden hallinnasta; 5) pääsynhallinnan, todentamisen ja salauksen menetelmistä; 6) perustason kyberhygieniakäytännöistä, joilla varmistetaan viestintäverkko- ja tietojärjestelmäturvallisuuden perusluonteiset hallintatoimenpiteet; 7) viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön, tilaturvallisuuden ja välttämättömien resurssien hallintatoimenpiteistä. Lakiehdotuksen 11 §:n 5 momentin nojalla valvova viranomainen voisi toimialallaan antaa tarkempia teknisiä määräyksiä: 1) siitä, milloin 1 momentissa tarkoitettu poikkeama on merkittävä; 2) 13 §:ssä tarkoitettussa loppuraportissa ilmoitettavista tiedoista; ja 3) merkittävien poikkeamien ja 12–13 §:n mukaisten tietojen ilmoittamismenettelyistä. Lakiehdotuksen 43 §:n 3 momentin nojalla valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä tietojen ilmoittamisesta.

Perustuslain 80 §:n 2 momentissa tarkoitettua norminantovallan delegoimista viranomaiselle on perusteltu esitysluonnoksessa (s. 200-201), tuomalla kuitenkin esiin myös sen käytön poikkeukselliseksi tarkoitettu luonne. Oikeusministeriö toteaa, että ehdotettu sääntely tarkoittaisi sitä, että seitsemän eri viranomaista voisi antaa määräyksiä samoista asioista. Tällainen viranomaisen norminantovaltuuden hajauttaminen vaikuttaa paitsi tavallisesta poikkeavalta, myös ongelmalliselta. Norminantovaltuudet vaikuttaisivat teknisyydestä huolimatta kuitenkin sisältävän siinä määrin yleisen luonteisiakin kaikki toimialat läpäiseviä tekijöitä, että perustuslain 80 §:n 2 momentin kannalta normiantovalta tulee – sen poikkeukselliseksi tarkoitettu käyttö huomioon ottaen – olla vain yhdellä viranomaisella. Norminantovaltuudet eivät vaikuta sisältävän vain toimialakohtaista ja teknistä sääntelyä. Jos perustuslain 80 §:n 2 momentissa tarkoitettua norminantovaltaa katsottaisiin perustelluksi antaa viranomaiselle, norminantovallan valtiosääntöiset lähtökohdat ja perustuslakivaliokunnan tulkintakäytäntö edellyttävät sen antamista vain yhdelle viranomaistaholle.

Viranomaiselle kaavaillun norminantovallan osalta on erikseen vielä syytä kiinnittää huomiota em. lakiehdotuksen 11 §:n 5 momentin 1 kohtaan, jonka nojalla valvova viranomainen voisi antaa tarkempia teknisiä määräyksiä siitä, milloin mainitun pykälän 1 momentissa tarkoitettu poikkeama on merkittävä. Oikeusministeriön käsityksen mukaan tällaista määrittelyvaltaa voi pitää keskeisenä sen kannalta, milloin toimijan on tehtävä viranomaiselle ilmoitus. Koska määräyksessä olisi kyse olennaisesti toimijoiden velvollisuuksien perusteisiin liittyvästä sääntelystä, viranomaisen määräyksen antovaltaa ei voida luonnehtia tekniseksi. Asiasta on säädettävä vähintään valtioneuvoston asetuksen tasoisella säädöksellä huomioiden asianmukaiset laintasoiset perussäännökset. Säädöstasoa arvioitaessa on lisäksi tehtävä selkoa laillisuusperiaatteen toteutumisesta, sillä 11 §:n mukaisen poikkeamailmoituksen tekemättä jättäminen olisi 37 §:n nojalla sanktioitu rangaistusluonteisin, merkittävän suurin seuraamusmaksuin.

9.

Lakiluonnoksen 27 §:ssä on säännöksiä valvovan viranomaisen tiedonsaantioikeuksista. Pykälän 1 momentin mukaan valvovalla viranomaisella olisi ko. lain mukaisia tehtäviä suorittaessaan oikeus saada salassapitosäännösten ja muiden tietojen luovuttamista koskevien rajoitusten estämättä tehtäviensä suorittamiseksi välttämättömät tiedot ko. laissa tarkoitetuilta toimijoilta. Oikeusministeriö toteaa, että vaikka tiedonsaantioikeus olisikin rajattu ko. lain mukaisten tehtävien suorittamiseen, jää tiedonsaantioikeuden määrittely säännöksessä kuitenkin hyvin väljäksi ja yksilöimättömäksi.

Perustuslakivaliokunta ei ole pitänyt hyvin väljiä ja yksilöimättömiä tietojensaantioikeuksia perustuslain kannalta mahdollisina edes silloin, kun ne on sidottu välttämättömyyskriteeriin. Perustuslakivaliokunta on painottanut, että erottelussa tietojen saamisen tai luovuttamisen tarpeellisuuden ja välttämättömyyden välillä on kyse tietosisältöjen laajuuden ohella myös siitä, että salassapitosäännösten edelle menevässä tietojensaantioikeudessa on viime kädessä kysymys siitä, että tietoihin oikeutettu viranomainen omine tarpeineen syrjäyttää ne perusteet ja intressit, joita tiedot omaavaan viranomaiseen kohdistuvan salassapidon avulla suojataan. Mitä yleisluonteisempi tietojensaantiin oikeuttava sääntely on, sitä suurempi on vaara, että tällaiset intressit voivat syrjäytyä hyvin automaattisesti. Mitä täydellisemmin tietojensaantioikeus kytketään säännöksissä asiallisiin edellytyksiin, sitä todennäköisemmin yksittäistä tietojensaantipyyntöä joudutaan käytännössä perustelemaan. Myös tietojen luovuttajan on tällöin mahdollista arvioida pyyntöä luovuttamisen laillisten edellytysten kannalta. Tietojen luovuttaja voi lisäksi kieltäytymällä tosiasiallisesti tietojen antamisesta saada aikaan tilanteen, jossa tietojen luovuttamisvelvollisuus eli säännösten tulkinta saattaa tulla ulkopuolisen viranomaisen tutkitavaksi. Tämä mahdollisuus on tärkeä tiedonsaannin ja salassapitointressin yhteensovittamiseksi. (PeVL 48/2018 vp, s. 4-5)

Vaikka kyse on valvontaviranomaisen valvontatoimivallan käyttämiseen liittyvästä tiedonsaantioikeudesta, jota on usein haastavaa täsmentää lainsäädännön tasolla, tulisi tiedonsaantioikeus oikeusministeriön mielestä pyrkiä kirjoittamaan tarkemmaksi ja yksilöivämmäksi. Esimerkiksi lakiluonnoksen

28 §:n 1 momentissa tiedonsaantioikeuden kannalta välttämättömät tiedot on ilmaistu tarkemmin ja yksilöivämmin. Lakiluonnoksen 27 §:n 1 momentin tiedonsaantioikeuden väljyydestä johtuen epäselväksi myös jää kyseisen tiedonsaantioikeussäännöksen suhde 28 §:n 1 momentissa säädettyyn tiedonsaantioikeuteen, ja se missä määrin 28 §:n 1 momentin tiedonsaantioikeus ei jo tulisi katetuksi väljemmällä 27 §:n 1 momentin mukaisella tiedonsaantioikeudella. Lisäksi ehdotetun pykälän 2 momentissa viitataan CER-direktiivin mukaisiin valvoviin viranomaisiin. Kyseisistä viranomaisista ei ole lainkaan mainintaa säännöskohtaisissa perusteluissa ja epäselväksi jää, mitkä viranomaiset olisivat kyseisen direktiivin mukaisia valvovia viranomaisia.

10.

Lain 29 §:ssä säädettäisiin tarkastusoikeudesta. Pykälän 1 momentissa olevan säännöksen nojalla valvova viranomainen voisi päätöksellään käyttää tarkastuksessa apuna tai pyytää tarkastuksen suorittajaksi toisen valvovan viranomaisen, tietoturvallisuuden arviointilaitoksen tai ulkopuolisen tietotekniikan asiantuntijan, jos se olisi tarkastuksen laadun tai laajuuden vuoksi tarpeellista. Säännöskohtaisissa perusteluissa (s. 145) todetaan, että mahdollisuus siirtää tarkastustehtävä toiselle valvovalle viranomaiselle tai ulkopuoliselle asiantuntijalle olisi tarpeen tilanteessa, jossa tarkastus edellyttäisi sellaista teknistä erityisosaamista, jota valvovalla viranomaisella ei olisi.

Perustuslain 124 §:n 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. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle.

Oikeusministeriö toteaa, että kyseessä oleva viranomaiselle kuuluvan valvontatehtävän antaminen muun tahon tehtäväksi vaikuttaa suhteellisen löyhästi perustellulta, tehtävään liittyessä kuitenkin kysymyksiä esimerkiksi ulkopuolisen tahon luotettavuuden toteamisesta. Sääntelyä ulkopuolisen asiantuntijan kelpoisuudesta tai siitä mitkä vaatimukset asiantuntijan tulee täyttää, tulisi myös tarkistaa, kun 29 §:n 1 momentin vaatimukset tarkastuksen suorittajan koulutuksesta ja kokemuksesta eivät vaikuta selkeästi koskevan myös ulkopuolista asiantuntijaa (lausejärjestys). Lisäksi voidaan kiinnittää huomiota siihen, että tarvetta tehtävän antamiseen ulkopuoliselle on esitysluonnoksen perusteluissa (s. 145) tehty säännökseen verraten eriävästi: perustelujen mukaan tehtävän antaminen liittyisi tekniseen erityisosaamiseen, säännöksessä puolestaan tarkastuksen laatuun ja laajuuteen.

Säännöksessä on myös ongelmallisella tavalla rinnastettu mahdollisuus käyttää tarkastuksen apuna muuta kuin viranomaista sekä mahdollisuus pyytää tarkastuksen suorittajaksi muu kuin viranomainen. Vaikuttaa perustellulta, että mahdollisuus ulkopuolisen tarkastajan käyttämiseen rajattaisiin ainoastaan viranomaista avustavaan tehtävään, etenkin, kun ehdotuksessa ei ole rajattu, mitä tarkastuksia muu kuin viranomainen voisi tehdä, ja kun huomioidaan, että itsenäisesti tarkastusta suorittavalla henkilöllä olisi merkittäviä toimivaltuuksia. Lisäksi on huomioitava, että tarkastuksissa ei olisi mistä tahansa valvontatyypisistä tarkastuksista kyse, vaan hyvin merkittäviin toimintoihin kohdistuvasta tarkastusoikeudesta. Perusteluissa todetaan: ”Tarkastuksessa voisi olla kyse satunnaistarkastuksesta, tarkastuksesta merkittävän poikkeaman jälkeen tai riskiarviointiin perustuvista säännöllisistä tarkastuksista yhteiskunnan toiminnan kannalta kriittisimmille toimijoille.” (s. 114) Oikeusministeriö pitää perusteltuna, että jatkovalmistelussa huolellisesti esitetään arvio siitä, mihin tarkastuksiin ulkopuolisia tarkastajia olisi mahdollista PL 124 §:n reunaehdoin käyttää ja millä edellytyksin, sekä tehdään asianmukaiset säännöskohtaiset rajaukset julkisen hallintotehtävän antamiselle.

Ulkopuolisen tarkastajan kelpoisuuteen liittyen tulisi jatkovalmistelussa arvioida myös tarve varmistua säännösperusteisesti henkilöturvallisuusselvityksen tekemisestä ottaen huomioon, että kyse olisi tehtäväkohtaisesta valtuutuksesta sekä merkittäviin toimintoihin kohdistuvasta tarkastusoikeudesta. Jatkovalmistelussa on lisäksi syytä arvioida huolellisesti PL 124 §:n asettamien edellytysten täyttymistä ja sitä, tulisiko turvallisuusjärjestelyjen tarkastusoikeus tehtävän luonteen ja merkityksen vuoksi säilyttää kuitenkin viranomaisella (ja sen nimissä virkamiestarkastajalla).

Esitysluonnoksen 2. lakiehdotuksen (laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta) 18 k §:ssä säädettäisiin Liikenne- ja viestintäviraston oikeudesta antaa tarkastustehtävään liittyvä avustava tehtävä tietoturvallisuuden arviointilaitoksista annetussa laissa (1405/2011) tarkoitetulle hyväksytylle tietoturvallisuuden arviointilaitokselle. Mainitussa 2. lakiehdotuksessa julkisen hallintotehtävän antaminen muulle kuin viranomaiselle on siis rajattu – sinänsä mainitusta laista (1405/2011) johtuen – huomattavasti tiukemmin kuin nyt kyseessä olevassa 1. lakiehdotuksessa.

Hajautetussa valvontamallissa verrattuna keskitettyyn, voi pitää oletettavana, että tarve ulkopuolisten asiantuntijoiden käyttöön tarkastuksissa on korostetumpaa. Tämä seikka tulisi perustuslain 124 §:ään liittyen ottaa huomioon ehdotettavan sääntelyn tarkoituksenmukaisuutta arvioitaessa. Myös se seikka,

että valvovat viranomaiset keskenään valtuuttavat toisiaan toimimaan tarkastuksissa apuna tai suorittamaan tarkastuksia toimivaltaisen viranomaisen puolesta ilmentää ehdotettuun usean valvovan viranomaisen järjestelmään liittyviä ongelmia.

11.

Lain 31 §:n 1 momentissa olevan säännöksen perusteella valvova viranomainen voisi velvoittaa toimijan julkistamaan sellaiset puutteet tai muut seikat, jotka liittyvät kyberturvallisuuden riskienhallinnasta annetun lain, sen nojalla annettujen määräysten tai NIS 2 –direktiivin nojalla annettujen säädösten rikkomiseen. Oikeusministeriö kiinnittää huomiota siihen, ettei säännöksessä eikä sen perusteissa tarkemmin todeta, millä tavoin toimijan tulisi julkistaa em. puutteet tai muut seikat. Säätelyä on tältä osin välttämätöntä täsmentää. Lisäksi tulisi tehdä selkoa siitä, missä määrin tieto kyberturvallisuudessa olevasta puutteesta olisi mahdollista velvoittaa julkistamaan ottaen huomioon, että sääntelyn tavoitteena on nimenomaan suojata kyberturvallisuutta ja kriittisiä turvallisuusjärjestelyjä.

Pykälän 2 momentin nojalla valvova viranomainen voisi antaa toimijalle huomautuksen tai varoituksen. Varoituksen voisi antaa, jos huomautusta ei asiasta ilmenevät seikat kokonaisuudessaan huomioiden voitaisi pitää riittävänä. Säännöskohtaisissa perusteluissa (s. 146) todetaan, että huomautus tai varoitus olisi seuraamus, joka voisi liittyä korjausvelvoitepäätökseen, mutta myös sellaiseen päätökseen, jolla päätetään valvontaprosessi ilman korjausvelvoitteita. Oikeusministeriö toteaa, että säännöksestä tulisi tarkemmin ilmetä, millä perusteella viranomainen voisi antaa toimijalle huomautuksen tai varoituksen. Huomautuksen ja varoituksen välistä eroa tulisi myös tarkemmin selostaa ja tuoda esiin lisäksi se, olisivatko toimijalle annetut huomautukset tai varoitukset missä määrin julkista tietoa.

12.

Lain 32 §:ssä olisi säännöksiä luvanvaraisen tai sertifioidun toiminnan rajoittamisesta ja luvan tai sertifiointin peruuttamisesta. Säännöksissä säänneltäisiin paitsi viranomaisen toimivallasta tehdä itsenäisiä päätöksiä rajoittamisesta ja peruuttamisesta, myös viranomaisen toimivallasta tehdä rajoittamis- tai peruuttamisasiassa päätösesityksiä toimivaltaiselle viranomaiselle. Oikeusministeriö pitää sääntelyn selkeyden kannalta parempana, että sääntely viranomaisen toimivallasta tehdä päätösesityksiä säänneltäisiin eri pykälässä.

Ehdotettu lupien ja sertifiointien rajoittamista ja peruuttamista koskeva sääntely näyttäytyy useilta osin ongelmallisena. Esityksessä tulisikin tehdä selkoa direktiivin jättämisestä kansallisesta liikkumavarasta ja siitä, miten sitä on käytetty perustuslain mukaisella tavalla huomioiden alla selostettu.

Säännös on muotoiltu hyvin väljästi ja epämääräisesti. Siitä ei käy ilmi, mitä lupia ja sertifiointeja toimivalta rajoittaa ja peruuttaa täsmällisesti ottaen koskee. Säännöksen ja sen perusteluiden valossa vaikuttaa siltä, että 32 §:ssä perustettaisiin toimivalta rajoittaa ja perua mitkä tahansa keskeisten toimijoiden muun lainsäädännön nojalla myönnettyt luvat. Oikeusministeriö pitää välttämättömänä täsmentää, mitä lupia ja sertifiointeja säännös koskee.

Asiallisesti ehdotetussa 32 §:ssä olisi kyse luvan ja sertifiointin rajoittamisen ja peruuttamisen uudesta perusteesta. Lähtökohtana tulee lisäksi pitää sitä, että kyseistä lupaa tai sertifiointia koskevassa laissa säädettäisiin luvan myöntämisen edellytyksistä ja toisaalta sen peruuttamisen ja rajoittamisen edellytyksistä, jotta toimija lupaa hakiessaan on tietoinen näistä seikoista. Edelleen vaikuttaa siltä, että 32 §:ssä mainitut luvan ja sertifiointin peruuttamisen perusteet tulisi olla vastaavasti luvan ja sertifiointin myöntämisen edellytyksenä. Luvan ja sertifiointin peruuttamisen uusien edellytysten osalta ongelmallista on, että luvan ja sertifiointin peruuttaminen ei vaikuta perustuvan suoraan lainsäädännön rikkomiseen ja tietyn laissa säädetyn velvoitteen rikkomiseen, vaan epämääräisempään toimijan oman mallin toteuttamiseen. Jatkovalmistelussa luvan ja sertifiointin rajoittaminen ja peruuttaminen tulisi kytkeä selkeämmin lain velvoitteiden rikkomiseen, mikäli mahdollista. Puolestaan 32 §:n 1 momentin 2 kohdan osalta oikeusministeriö viittaa edellä määräyksenantovaltuuksista todettuun.

Oikeusministeriö kiinnittää huomiota myös siihen, että pykälän säännöskohtaisissa perusteluissa (s. 146) todetaan, että valvova viranomainen voisi rajoittaa tai peruuttaa sellaisen luvan tai sertifiointin, jonka se on itse myöntänyt. Säännöstekstin perusteella ei voi yksiselitteisesti päätellä, että kyse olisi nimenomaisesti sellaisista luvista tai sertifiointeista, jotka peruuttava viranomainen on itse myöntänyt. Säännöstekstiä olisi näin ollen perusteltua muokata perusteluja vastaavaksi (”toimijalle myöntämänsä luvan”).

Pykälän 2 momentin mukaan valvovan viranomaisen olisi ennen 1 momentissa tarkoitettujen päätösten tekemistä annettava keskeiselle toimijalle huomautus tai varoitus sekä varattava kohtuullinen määräaika puutteen tai laiminlyönnin korjaamiseksi. Esitysluonnoksen perusteella ei selviä, mikä ero säännöksessä ehdotetuilla huomautuksella ja varoituksella olisi (miksi ylipäätään pitäisi olla käytettävissä

sekä huomautus että varoitus). Sääntely tulisi perustella asianmukaisesti, jotta käytössä olevan toimivallan perusteet olisivat selkeät ja lakia soveltavalla viranomaisella olisi myös tukea lain tulkintaan. Sama huomio voidaan kohdistaa myös lakiehdotuksen 33 §:n 1 momentissa olevaan sääntelyyn huomautuksen tai varoituksen antamisesta.

Ehdotetun 32 §:n nojalla valvovalla viranomaisella olisi toimivalta rajoittaa tai peruuttaa myöntämänsä luvan tai sertifiointin. Kun kyse on tilanteesta, jossa muu viranomainen on toimivaltainen lupa- tai sertifiointiviranomainen, valvova viranomainen voisi tehdä tälle päätösesityksen luvan tai sertifiointin rajoittamisesta tai peruuttamisesta. Päätösesitystä koskeva ehdotus merkitsisi siten sitä, että toinen viranomainen esittelee toiselle viranomaiselle päätöksen, jonka tämä ratkaisee. Tällainen mekanismi on kansallisesti täysin vieras. On lisäksi painotettava, että tällaisessa menettelyssä viranomaisten väliset toimivallat sekoittuvat merkittävästi. Edelleen esitysluonnoksen perusteella jää epäselväksi, miten toimivaltainen viranomainen käsittelee tällaisen päätösesityksen ja onko sillä laissa säädetty toimivalta päättää tällaisen esityksen mukaisesta luvan tai sertifiointin rajoittamisesta tai peruuttamisesta. Asianmukaisen toimivaltasääntelyn lisäksi esityksessä tulee tehdä selkoa siitä, mikä on tällaisen päätösesityksen luonne sekä sen suhde päätöksentekijän selvittämiselvöllisyyteen (hallintolaki 31 §). Jatkovalmistelussa tulee arvioida mahdollistaako asetuksen kansallinen liikkumavara sen, että kyse ei olisi toisen viranomaisen päätösesityksestä, vaan esimerkiksi sen velvollisuudesta ilmoittaa tällaisista tilanteista toimivaltaiselle viranomaiselle, joka viranomaisaloitteisesti ryhtyisi tutkimaan asiaa.

Lisäksi 32 §:n 3 momentissa käytetty passiivimuoto tulisi muuttaa aktiivimuotoon, jotta toimivaltainen viranomainen ilmenee säännöksestä selkeästi. Pykälässä käytettyä käsitettä ”keskeinen toimija” ei ole määritelty lain määritelmäpykälässä.

13.

Lain 35 §:ssä säädettäisiin valvovan viranomaisen toimivallasta asettaa päätöksen tehosteeksi uhkasakko, teettämishukka tai keskeyttämishukka. Säännöksessä viitattaisiin uhkasakkolakiin (1113/1990). Oikeusministeriö toteaa, että kun yleislaista ei poiketa, yleislakiin ei yleensä viitata ja nykyään viittaus uhkasakkolakiin suositellaan jätettäväksi pois (LAKO 12.7).

14.

Lakiluonnoksen 36 §:n 2 momentin mukaan valvova viranomainen voisi päätöksessään määrätä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää. Säännöstä ei esitysluonnoksessa erikseen perustella, jolloin jää epäselväksi, miksi viranomaisella tulisi olla rajoittamaton harkintavaltansa sen osalta määrääkö se päätöksen noudatettavaksi muutoksenhausta huolimatta, jollei valitusviranomainen toisin määrää. Esityksessä tulisi lisäksi esittää yleislain (HL 49 f § ja HOL 122 §) säännöksistä poikkeavalle sääntelylle erityiset painavat perusteet. Oikeusministeriön mielestä voidaan oikeusturvan toteutumisen yhtenäisyyden sekä oikeusvarmuuden kannalta pitää ongelmallisena sitä, että päätöksentekijä tapauskohtaisesti päättäisi päätöksen noudattamisesta muutoksenhausta huolimatta. Yleisesti käytetty sääntelytapa on säätää laissa siitä, että päätöstä on noudatettava muutoksenhausta huolimatta, jollei muutoksenhakuviranomainen toisin määrää.

15.

Lain 37-41 §:issä olisi säännökset seuraamusmaksusta. Lain 37 §:n osalta huomiota voidaan kiinnittää siihen, että hallinnollinen seuraamusmaksu voitaisiin määrätä *toimijalle*, kun direktiivissä (34 artikla) viitataan *keskeisiin ja tärkeisiin toimijoihin*. Vastaavasti lain 40 §:ssä seuraamusmaksun enimmäismäärän sääntelyn yhteydessä käytettäisiin termejä *keskeinen toimija* ja *tärkeä toimija*. Jatkovalmistelussa on tarkistettava 37 §:n sanamuoto toimijoihin viittaamisen osalta.

Luonnoksen perusteluissa todetaan, että 37 §:n sääntelyllä pantaisiin täytäntöön NIS 2 –direktiivin 34 artikla muiden 5 luvun säännösten kanssa. Esityksessä tulisi selkeästi ilmaista, miltä osin direktiivi edellyttää 37 §:ssä listattujen velvoitteiden rikkomisen sanktiointia vai liittyykö näihin kansallista liikkumavaraa ja miten sitä on perustuslain reunaehdoissa käytetty. Lisäksi säätämisyjärjestysperusteluissa tulisi arvioida, miten aineelliset velvoitteet ja seuraamusmaksusääntely täyttävät nyt ehdotetussa sääntelyssä laillisuusperiaatteen asettamat vaatimukset. Muutoinkin kansallisen liikkumavaran sisällyttäminen ja käytöstä tulisi ehdotuksessa tehdä paremmin selkoa (esim. ehdotetut 39-41 §).

Lakiluonnoksen 38 §:n mukaan seuraamusmaksun määräisi seuraamusmaksulautakunta. Säännöksen perusteella kyse olisi uuden valtioneuvoston toimielimen perustamisesta, minkä vuoksi ehdotusta on arvioitava PL 119 §:n 2 momentin valossa, joka edellyttää, että valtioneuvoston toimielimen yleisistä perusteista on säädettävä lailla, jos niiden tehtäviin kuuluu julkisen vallan käyttöä. Tällainen arviointi on lisättävä esityksen säätämisyjärjestysperusteluihin.

Oikeusministeriö kiinnittää lisäksi huomiota siihen, että liikenne- ja viestintäministeriön hallinnonalalla on vastikään ehdotettu säädettäväksi seuraamusmaksukollegio Liikenne- ja viestintäviraston yhteyteen määräämään erityisen suuria, EU-säätelyyn perustuvia seuraamusmaksuja (HE 70/2023 vp). Tällaisia erityisen suuria EU-säätelyyn perustuvia, NIS 2 –direktiivissäkin edellytettäviä, seuraamusmaksuja tuskin määrättäisiin vuosittain kovin montaa kappaletta. Lisäksi oikeusministeriön saamien tietojen mukaan tällaisia muita kollegiaalista päätöksentekoa edellyttäviä seuraamussäännöksiä on ilmeisesti tulossa LVM:n ja Liikenne- ja viestintäviraston toimialalla. Seuraamusmaksujen määrääminen on syytä organisoida tarkoituksenmukaisella ja kestäväällä tavalla sekä välttää tilannetta, jossa uuteen säätelyyn perustuva seuraamusmaksu edellyttää aina uuden kollegiaalisen päätöksentekolimen perustamista. Oikeusministeriöstä on esityksen valmisteluvaiheessa todettu, että seuraamusmaksukollegio/lautakuntasäätely kannattaa yhteensovittaa. Tässä säätelykokonaisuudessa tarkoituksenmukaisinta saattaisi olla, että merkittävien suurusten seuraamusmaksujen määrääminen keskitettäisiin yhteen viraston seuraamuslautakuntaan, johon jäsenet nimitettäisiin tarvittavan asiantuntemuksen mukaan ja kulloinenkin kokoonpano määrittäisi käsittelyssä olevan asian perusteella.

Sinänsä oikeusministeriö yhtyy esitettyyn arvioon siitä, että direktiivin tarkoittamat merkittävät suuret seuraamusmaksut, joihin sisältyy viranomaisen laaja harkintavalta, edellyttävät oikeusturvan vuoksi määräämistoimivallan osoittamista kollegiaaliseen päätöksentekoon. Samalla on kuitenkin korostettava, että mahdollisuus näin merkittäviin seuraamusmaksuihin asettaa oikeusturvan näkökulmasta erityisen vaatimuksen myös sille, miten lain mukainen viranomaisvalvonta järjestetään (keskitetty vai hajautettu malli).

Ehdotetun 38 §:n 4 momentin mukaan seuraamusmaksulautakunnalla olisi oikeus salassapitosäännösten estämättä saada maksutta tehtäviensä hoidon kannalta välttämättömät tiedot. Oikeusministeriön mielestä tiedonsaantioikeus on säännöksessä liian väljä ja sitä tulisi tarkentaa (vrt. 27 §:stä edellä lausuttu).

Lakiluonnoksen 41 §:n 5 momentin mukaan seuraamusmaksu vanhenisi viiden vuoden kuluttua lainvoiman saaneen päätöksen tekemisestä. Säännöksen perustelujen mukaan (s. 151) seuraamusmaksu vanhenisi viiden vuoden kuluttua siitä, kun sen määräämistä koskeva päätös on saanut lainvoiman. Oikeusministeriö toteaa, että säännös on perustelunsa kanssa ristiriitainen ja että seuraamusmaksun vanhenemista koskevan säännöksen osalta olisi perusteltua käyttää muotoa, jonka mukaan seuraamusmaksu vanhenee viiden vuoden kuluttua seuraamusmaksua koskevan lainvoiman saaneen ratkaisun antamispäivästä.

Muutoksenhakua (42 §) koskeva säännöskohtainen perustelu on virheellinen sen viitatessa ainoastaan hallinnollista seuraamusmaksua koskevaan päätökseen.

16.

Lakiluonnoksen 45 §:n 2 momentin mukaan kansallisen laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman tulisi sisältää NIS 2 –direktiivin 9 artiklan 3 ja 4 kohdassa tarkoitettujen tiedot. Edellä tässä lausunnossa on viitattu siihen, että perustuslakivaliokunta on pitänyt lähtökohtana, että kansallisia täytäntöönpanotoimia edellyttävät Euroopan unionin säädökset tulee pääsääntöisesti sisällyttää kansalliseen lainsäädäntöön EU-säädösten asiasisältöä vastaavilla kansallisilla säädöksillä. Perustuslakivaliokunta on pitänyt tietyn reunaehdoin mahdollisena säätelyä, jossa lain tasolla viitataan teknisluonteisten ja yksityiskohtaisten vaatimusten osalta suoraan direktiivin säännöksiin.

Oikeusministeriö pitää perusteltuna, että direktiivin edellyttämät tiedot säännellään laissa, eikä direktiivin täytäntöönpanoa jätetä direktiiviinvaraan.

17.

Lain 46 §:n 3 momentissa olisi säännös siitä, että valvovien viranomaisten olisi ilmoitettava CER-direktiivin mukaiselle toimivaltaiselle viranomaiselle, kun se käyttää 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimijaan. Lisäksi momentissa olisi säännös, jonka mukaan valvova viranomainen voi CER-direktiivin mukaisen toimivaltaisen viranomaisen perustellusta pyynnöstä kohdistaa 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimintaan.

Oikeusministeriön mielestä säätely valvovan viranomaisen velvollisuudesta tehdä ilmoituksia CER-direktiivin mukaiselle toimivaltaiselle viranomaiselle tulisi muuttaa sellaiseen muotoon, josta suoraan ilmenee se viranomainen, jolle ilmoitus on tehtävä. Samanlainen muutos (ko. viranomaisen nimenomainen nimeäminen direktiiviinvaraan) tulisi tehdä myös samassa momentissa olevaan säännökseen, jonka mukaan valvova viranomainen voisi CER-direktiivin mukaisen toimivaltaisen viranomaisen perustellusta pyynnöstä kohdistaa 4 luvussa säädettyjä toimivaltuuksia CER-direktiivin nojalla kriittiseksi tunnistettuun toimintaan.

18.

Lakiin tarkoitettujen liitteiden I ja II alussa voisi olla lyhyt informatiivinen johdanto, jolla liitteen sisältö kytkettäisiin lain sääntelyyn.

Laki julkisen hallinnon tiedonhallinnasta annetun lain muuttamisesta

1.

Lain soveltamisalaa koskevaan 3 §:ään lisättäisiin säännökset uuden 4 a luvun (jossa säänneltäisiin kyberturvallisuusvelvoitteista ja niiden noudattamisen valvonnasta) soveltamisesta. Ehdotetussa uudessa 3 §:n 2 momentissa on säännös, jonka mukaan lain 4 a luvun 18 h–18 l §:ää ei sovelleta tasavallan presidentin kansliaan, valtioneuvoston oikeuskanslerin toimintaan eikä Kansaneläkelaitokseen. Oikeusministeriö pitää perusteltuna, että em. säännöstä tarkistetaan sen osalta, että siinä mainittaisiin myös eduskunnan oikeusasiamies, joka mainitaan saman pykälän muissa soveltamisalarajauksissa.

2.

Lain 18 h §:n 1 momentissa säädettäisiin Liikenne- ja viestintäviraston toimivallasta valvontaviranomaisena. Oikeusministeriö toteaa, että säännöksessä olisi asianmukaista todeta viraston valvontatoiminnan riippumattomuus, kun sitä edellytetään direktiivin 31 artiklan 4 kohdassa (vrt. valvonnan riippumattomuudesta säätämistä tietosuojalain (1050/2018) 8 §).

Lain 18 h §:n 2 momentin säännöksen mukaan Liikenne- ja viestintäviraston olisi valvontatoimiaan suorittaessaan ja 18 l §:ssä tarkoitettua valvontapäätöstä tehdessään otettava huomioon NIS 2 –direktiivin 32 artiklan 7 kohdassa säädetyt seikat. Oikeusministeriö on edellä tässä lausunnossa tuonut esiin sen, että direktiivin täytäntöönpanossa tulisi välttää täytäntöönpanoa viittaamalla direktiiviin ja täytäntöönpano tulisi suorittaa kirjoittamalla direktiivissä edellytetty sääntely auki kansalliseen säädökseen. Oikeusministeriö toteaa, että direktiivin 32 artiklan 7 kohdassa säädetyt seikat olisi perusteltua kirjoittaa auki lakiin.

Ehdotetun 18 i §:n 3 momentissa säädettäisiin viranomaisen tiedonluovutusosoikeudesta julkisuuslain julkisuus- tai salassapito-olettan sisällävän salassapitosäännöksen osoittamissa rajoissa Liikenne- ja viestintävirastolle. Momentin toinen virke vaikuttaa tarpeettomalta, koska siinä säädettäisiin käytännössä vastaavasta tiedonluovutusosoikeudesta, josta säädetään jo julkisuuslaissa. Sääntelyn suhteesta julkisuuslaissa säädettyyn voitaisiin tehdä selkoa vain perusteluissa. Vastaava huomio koskee ehdotetun 3 momentin kolmatta virkettä. Momentin viimeinen virkkeen tarkoituksena vaikuttaisi perustelujen perusteella olevan viitata informatiivisesti kansainvälisistä tietoturva-velvoitteista annetussa laissa säädettyihin tietoaineistojen käsittelyä koskeviin säännöksiin. Jos viittauksen on tarkoitus olla informatiivinen, tulisi se muotoilla esimerkiksi muotoon ”erityissuojattavan tietoaineiston käsittelyssä noudatettavista velvoitteista säädetään kansainvälisistä tietoturva-velvoitteista annetussa laissa”.

3.

Lain 18 j §:n 3 momentissa olevan säännöksen mukaan tarkastusta suorittavalla olisi oikeus salassapitosäännösten estämättä saada tutkittavakseen tarkastustehtävän kannalta tarpeelliset tiedot. Huomioitavaa on, että tiedonsaantioikeus kohdistuisi viranomaistahoihin, mutta oikeusministeriö kiinnittää kuitenkin huomiota siihen, että 1. lakiehdotuksen 29 §:ssä tiedonsaantioikeus on sidottu tarkastuksen kannalta välttämättömiin tietoihin. Oikeusministeriö pitää perusteltuna, että myös 18 j §:n mainitussa säännöksessä tiedonsaantioikeus sidotaan tarkastuksen kannalta välttämättömiin tietoihin.

4.

Lain 18 l §:n 2 momentin nojalla Liikenne- ja viestintävirasto voisi antaa viranomaiselle huomautuksen tai varoituksen. Varoituksen voisi antaa, jos huomautusta ei asiasta ilmenevät seikat kokonaisuudessaan huomioiden voisi pitää riittävänä. Oikeusministeriö toteaa, että säännöksestä tulisi tarkemmin ilmetä, millä perusteella Liikenne- ja viestintävirasto voisi antaa viranomaiselle huomautuksen tai varoituksen. Huomautuksen ja varoituksen välistä eroa tulisi myös tarkemmin selostaa ja tuoda esiin lisäksi se, olisivatko viranomaiselle annetut huomautukset tai varoitukset missä määrin julkista tietoa.

Laki sähköisen viestinnän palveluista annetun lain muuttamisesta

Lain 167 §:ssä olevaa Liikenne- ja viestintäviraston määräyksenantovaltaa ehdotetaan laajennettavaksi siten, että virasto saisi antaa määräyksiä myös verkkotunnuksen käyttäjän tunnistamisesta ja verkkotunnuksen käyttäjän varmistamisesta. Esitysluonnoksen säännöskohtaisissa perusteluissa (s. 175) todetaan ko. määräyksenantovalan kohdistuvan sellaisten toimintaperiaatteiden ja menettelyjen sääntelyyn, joita verkkotunnusväliittäjien olisi otettava käyttöön, jotta ne voivat varmistua siitä että 167

§:n 1 momentissa tarkoitetut, verkkotunnuksen käyttäjän ilmoittamat tiedot olisivat oikeita ja ajantasaia. Esitysluonnoksen säätämisyjärjestysperusteluissa ko. määräyksenantovaltuutta ei mainita.

Oikeusministeriö toteaa, että ko. olevan määräyksenantovaltuuden sisältö vaikuttaa sellaisten luonteeltaan yleisten oikeussääntöjen antamiselta (verkkotunnusvälittäjälle asetettavia velvoitteita), joka tulisi sääntelyn merkityksen vuoksi toteuttaa lain tasoisella säädöksellä. Oikeusministeriö myös huomauttaa valmistelevalle ministeriölle siitä, että viranomaiselle esitettäisiin norminantovaltaa sitä juuriin perustelematta.

Samat huomiot ovat kohdistettavissa myös lain 170 §:n määräyksenantovaltuuksiin, joita laajennettaisiin siten, että Liikenne- ja viestintävirasto voisi antaa tarkempia määräyksiä myös tarkoitetuista julkisesti saataville asetettavista tiedoista, pääsyn antamisesta tietoihin sekä toimintaperiaatteista ja menettelyistä.

Suhde perustuslakiin ja säätämisyjärjestys –jakso

Oikeusministeriö arvioi, että ehdotettu sääntely muodostaa verrattain vaikeaselkoisen kokonaisuuden johtuen osin sääntelyn tekniluonteisuudesta, mutta myös siitä, että ehdotettu sääntely sisältää runsaasti viittauksia muuhun sääntelyyn kuten sähköisen viestinnän palveluista annetussa laissa säädettyyn. Tämä on omiaan vaikeuttamaan ehdotetun sääntelyn valtiosääntöistä arviointia.

1.

Esitysluonnoksen 1. lakiehdotuksen 28 §:n mukaan valvovalla viranomaisella olisi salassapitosääntöjen ja muiden tietojen luovuttamista koskevien rajoitusten estämättä oikeus saada toimijalta välitystieto, sijaintitieto tai haitallisen tietokoneohjelman tai käskyn sisältävä viesti, jos se on välttämätöntä kyberturvallisuuden riskienhallintavelvoitteiden valvomista varten tai merkittävien poikkeamien selvittämiseksi.

Esitysluonnoksen säätämisyjärjestysperusteluissa (s. 191) pohditaan kysymystä siitä, nauttiiko kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä viesti perustuslain 10 §:n 2 momentissa tarkoitettua luottamuksellisen viestin suojaa. Teknisesti kyse voi olla haittaohjelman luomasta viestistä, jota ei voi sinänsä pitää luonnollisen henkilön laatimana. Haitallisen tietokoneohjelman ja käskyn sisältävän viestin voidaan ajatella koskevan kuitenkin viestin sisältöä (s. 190).

Esitysluonnoksessa todetaan, että perustuslakivaliokunnan arvion varaan jää, missä määrin kuvatuun kaltainen haittaohjelmaviestintä nauttii viestinnän luottamuksellisuuden suojaa tai sijoittuu viestinnän luottamuksellisuuden suojan ydinalueelle esimerkiksi viestin teknisten haittaohjelmaominaisuuksien tai välitystietojen osalta (s. 191). Vaikka tulkintatilannetta voikin pitää haasteellisena, hallituksen esitysten laatimisohejeet edellyttävät, että lakiehdotukset on valmisteltava perustuslain mukaisiksi, jolloin hallituksen esityksessä on kerrottava, millä perusteilla sääntöjen katsotaan olevan sopusoinnussa perustuslain kanssa. Esityksen suhde perustuslakiin ja kansainvälisiin ihmisoikeusvelvoitteisiin sekä tarve perustuslakivaliokunnan käsittelyyn on arvioitava valmistelusta vastaavassa ministeriössä. Mainituilla perusteilla edellä viitatuun kaltaisia lausumia valiokunnan arvion varaan jättämisestä ei tulisi esittää.

Joka tapauksessa ehdotettu sääntely – vaikka katsottaisiin ettei kyberhyökkäyksen toteuttamiseksi luotu haitallisen tietokoneohjelman tai käskyn sisältävä viesti nauttisi perustuslain 10 §:n 2 momentissa tarkoitettua luottamuksellisen viestin suojaa – vaikuttaisi sen sisältöiseltä, että luottamuksellisen viestin salaisuuden suojaa nauttivaa viestintää saatettaisiin kuitenkin valvonnallisista syistä rajoittaa.

Perustuslain 10 §:n 4 momentin mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Vaikka kyseiset perusoikeuden erityiset rajoitusedellytykset mainitaankin esitysluonnoksessa (s. 187), niin luonnoksesta ei kuitenkaan vaikuta selkeästi ilmenevän, mihin em. rajoitusedellytyksistä kaavailtu lainsäädäntö olisi liitännäinen, ts. mikä olisi luottamuksellisen viestin salaisuuden rajoittamisen tarkka peruste perustuslain 10 §:n 4 momentin kannalta. Lakiehdotuksen 28 §:n säännöksessä perusteina mainitaan kyberturvallisuuden riskienhallintavelvoitteiden valvominen ja merkittävien poikkeamien selvittäminen, jotka eivät suoraan kohdistu tai ole yhtenevät perustuslain 10 §:n 4 momentin rajoitusedellytyksiin.

Esityksessä tulisi tarkentaa ja täsmentää perustuslain 10 §:n 4 momentin erityisten rajoitusedellytysten täytyminen. Esityksen säätämisyjärjestysperusteluissa olisi aiheellista viitata myös tuoreimpiin pe-

rustuslakivaliokunnan perustuslain 10 §:n 2 ja 4 momenttia koskeviin kannanottoihin. Lisäksi esitysluonnoksen pääasiallisessa sisällössä todetaan, että NIS 2 –direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen. Näin ollen säätämisyjärjestysperusteluissa olisi perusteltua kuvata myös sitä, missä määrin ehdotetun luottamuksellisen viestinnän rajoittamisen kannalta merkitykselliset säännösehdoitukset ovat sellaisia, että EU-sääntelyn täytäntöönpano nimenomaisesti edellyttää kyseisiä rajoituksia.

Perustuslakivaliokunnan mukaan perustuslain 10 §:n 4 momentin säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiin kuuluvasta välttämättömyysvaatimuksesta seuraa, että luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee olla mahdollisimman kohdennettua ja rajattua (PeVL 5/2023 vp, s. 4; PeVL 36/2018 vp, s. 12; PeVM 4/2018 vp, s. 7).

Esitysluonnoksen perustelujen mukaan (s. 189) kyse ei olisi kohdentamattomasta ja kaiken kattavasta tietoliikenteen valvonnasta. Ehdotetun 28 §:n säännöksen mukaan viranomaisella olisi oikeus saada välitystieto, sijaintitieto tai haitallisen tietokoneohjelman tai käskyn sisältävä viesti kyberturvallisuuden riskienhallintavelvoitteiden valvomista varten tai merkittävien poikkeamien selvittämiseksi. Säännöksen perusteella tiedonsaantioikeus nähtävästi koskisi sinänsä perustuslain 10 §:n 4 momentin kannalta yksilöimätöntä (esim. rikosepäily) tietoliikennettä, jolloin kohdentuminen vaikuttaisi tarkoittavan ainoastaan tiedonsaantioikeuden rajoittamista tiettyihin viestintäverkkoihin. Jos kyberhyökkäyksen toteuttamiseksi luodun haitallisen tietokoneohjelman tai käskyn sisältävän viestin ei katsottaisi nauttivan perusoikeussuojaa, niin luottamuksellisen viestin salaisuuden kannalta vaikuttaisi tällöin olennaiselta se, että viranomaisella olisi seuloa tai poimia haitallisen tietokoneohjelman tai käskyn sisältävät viestit tehokkaasti, jolloin perustellusti luottamuksellisen viestin salaisuutta nauttivaan viestintään ei tahattomasti kohdistettaisi viranomaistoimenpiteitä, eikä luottamuksellisen viestin salaisuuden suojaan niin ollen myöskään rajoitettaisi perusteettomasti (vrt. PeVL 5/2023 vp, s. 5 käytettävän teknologian kohdentamisesta).

Huomattavaa on, että 1. lakiehdotuksen 22 §:n 4 momentissa ja 24 §:n 1 momentissa olisi säännökset, joiden nojalla voitaisiin nk. vapaaehtoisissa jakamisjärjestelyissä luovuttaa tietoa kyberuhkaan tai poikkeamaan liittyvästä välitystiedosta tai haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä. Jos kyberhyökkäyksen toteuttamiseksi luodun haitallisen tietokoneohjelman tai käskyn sisältävän viestin ei katsottaisi nauttivan perusoikeussuojaa, ja tietoa sellaisesta luovutettaisiin, sääntely ei vaikuttaisi ongelmalliselta luottamuksellisen viestin salaisuuden suojan kannalta. Jos mainitunkaltaisen viestin puolestaan katsottaisiin nauttivan luottamuksellisen viestin salaisuuden suojaan, kysymyksenalaista on, voidaanko vapaaehtoisista jakamisjärjestelyä pitää mahdollisena, kun sitä ei ole pidettävä välttämättömänä, mikä on perusoikeuden rajoittamisen edellytys. Erityistä huomiota tulee kiinnittää myös siihen, että ko. viestin voisi ehdotetun sääntelyn nojalla luovuttaa nähtävästi esimerkiksi jakamisjärjestelyssä mukana oleva luonnollinen henkilö tai oikeushenkilö (toimija) toiselle luonnolliselle henkilölle tai oikeushenkilölle. Kaikkiaan tietojen luovuttaminen vaikuttaisi muodostuvan hyvin väljän sääntelyn varaan, jota ei siinä tapauksessa, että em. mainitunkaltaisen viestin katsottaisiin nauttivan luottamuksellisen viestin salaisuuden suojaan, voida oikeusministeriön käsityksen mukaan pitää perustuslain kannalta ongelmattomana.

Perusoikeusrajoituksen on täytettävä perusoikeuksien yleiset rajoitusedellytykset (PeVM 25/1994 vp, s. 5). Esitysluonnoksessa todetaan ehdotetun sääntelyn oikeasuhtaisuuteen liittyen (s. 188), että haavoittuvuuskartoituksella saavutetaan merkittäviä hyötyjä tietoturvaloukkausten ennalta ehkäisemisen kautta, joilla voi olla yksilöiden ja yhteiskunnan kannalta merkittäviäkin vaikutuksia esimerkiksi tietoturvojen tai toiminnan häiritsemisen muodossa. Oikeusministeriö toteaa, että perusoikeusrajoituksen oikeasuhtaisuuden kannalta vaikuttaisi esityksessä perustellulta vielä perustella sitä, missä määrin on arvioitavissa se, että viranomaistoimenpiteiden yhteydessä saatettaisiin rajoittaa luottamuksellisen viestin salaisuuden suojaan tahattomasti, jos ajatellaan etteivät kaikki viranomaistoimenpiteet välttämättä kohdistuisi tarkasti sellaiseen viestintään, jossa kyse olisi kyberhyökkäyksen toteuttamiseksi luodun haitallisen tietokoneohjelman tai käskyn sisältävästä viestistä.

Oikeusministeriö yhtyy esitysluonnoksessa (s. 202) olevaan toteamaan siitä, että haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan ehdotuksen johdosta esityksestä olisi tarpeen pyytää perustuslakivaliokunnan lausunto. Edellä tässä lausunnossa esiin tullessiin seikkoihin viitaten voi sinänsä todeta, että esitys sisältää myös muita sen laatuksia valtiosääntöoikeudellisia kysymyksiä, joiden perusteella esitys olisi perusteltua saattaa perustuslakivaliokunnan arvioitavaksi, minkä vuoksi mainitun kirjauksen olisi syytä olla laajempi ja kattaa muutkin kysymykset kuin haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevan ehdotuksen.

2.

Esitysluonnoksen 1. lakiehdotuksen 30 §:n 2 momentin mukaan valvovalla viranomaisella olisi oikeus saada tieto teetetyn turvallisuusauditoinnin tuloksista sekä päätöksellä velvoittaa toimija toteuttamaan turvallisuusauditoinnin suosittelemat kohtuulliset ja oikeasuhtaiset toimenpiteet kyberturvallisuuden

riskienhallinnan kehittämiseksi. Säännöskohtaisissa perusteluissa (s. 145) säännöstä ei erikseen perustella, vaan ainoastaan referoidaan säännöstä.

Oikeusministeriö toteaa, että säännöksen perusteella viranomaisella voisi velvoittaa toimijan suorittamaan toimenpiteitä kyberturvallisuuden riskienhallinnan kehittämiseksi. Oletettavaa on, että tuollaiset toimenpiteet aiheuttaisivat toimijalle kustannuksia. Sääntelyä tulisi tämän vuoksi arvioida siitä näkökulmasta, aiheutuisiko siitä toimijan omaisuuden suojan rajoittamista (perustuslain 15 §), ja täyttäisikö omaisuudensuojan rajoittaminen perusoikeuksien yleiset rajoitusedellytykset.

Oikeusministeriö kiinnittää huomiota myös yleisesti siihen, että kaavailtu lainsäädäntö tarkoittaisi esitysluonnoksessa olevan vaikutusarvioinninkin perusteella kustannuksia niille tahoille, joiden tulisi huolehtia laissa niille säädetyistä velvoitteista. Tässäkin suhteessa olisi esityksen säätämisyjärjestysperusteluissa asianmukaista esittää arvio esityksen suhteesta perustuslain 15 §:ään.

3.

Esitysluonnoksen 1. lakiehdotuksessa CSIRT –yksikkö tulisi arvioida säätämisyjärjestysperusteluissa perustuslain 119 §:n 2 momentin kannalta (vrt. esim. PeVL 51/2006 vp).

4.

Oikeusministeriö toteaa vielä, että edellä tässä lausunnossa on esitetty huomioita, joilla saattaa olla merkitystä esityksen säätämisyjärjestysperustelujen sisältöön.

Henkilötietojen suoja

Esitysluonnoksen perustelujen (s. 92) mukaan ”tietojärjestelmissä ja viestintäverkoissa käsiteltävien tietojen tietosuojaa edellyttää järjestelmien tietoturvaominaisuuksien kehittämistä. Toimenpiteet tietojärjestelmien ja viestintäverkkojen kyberturvallisuuden parantamiseksi vaikuttavat niissä käsiteltävien tietojen tietosuojaan sitä parantavasti.”

Ehdotetussa sääntelyssä on kyse eri asiasta kuin henkilötietojen suojassa. Oikeusministeriö kiinnittää huomiota siihen, että tietosuojalainsäädäntö koskee vain henkilötietojen suojaa, ei laajemmin tietojen suojaamista. Direktiivillä kuitenkin on liittymäkohtia henkilötietojen suojaan erityisesti siltä osin kuin on kyse henkilötietojen käsittelyn tietoturvasuojasta. Esitysluonnoksen 1. lakiehdotus sisältää myös säännökset, joissa on huomioitu suhde tietosuojalainsäädännön noudattamisen valvontaan sekä henkilötietojen tietoturvaloukkauksia koskeviin ilmoituksiin direktiivin mukaisesti. Lisäksi esitysluonnoksen perustelut sisältävät useita viittauksia tietosuojaan. Perustelutekstiä olisi hyvä täsmentää sen huomiomiseksi, mitä tietosuojalainsäädäntö koskee, sekä avata hieman enemmän tietosuojavaikutuksia. Oikeusministeriön näkemyksen mukaan ehdotetulla sääntelyllä olisi joka tapauksessa myönteisiä vaikutuksia tietoturvasuojan kohentumisen myötä myös henkilötietojen suojaan, kuten perustelutekstissä todetaan.

Viranomaisvaikutukset

Oikeusministeriön hallinnonalalla ehdotettavasta sääntelystä seuraisi vaikutuksia usealle viranomaiselle. Siltä osin kuin on kyse soveltamisalaan tulevista viranomaisista, oikeusministeriö pitää perusteltuna esitysluonnoksessa omaksuttua lähtökohtaa siitä, että pääosin pitäydytään NIS 2 –direktiivin edellyttämässä minimitäytäntöönpanossa, eikä hallinnollisia seurausmaksuja ehdoteta sovellettavaksi viranomaisiin. Tässä vaiheessa voidaan pitää riittävänä, että muut kuin soveltamisalaan kuuluvat viranomaiset voisivat soveltaa lakia joiltakin osin ilman lain asettamaa velvoitetta.

Hallituksen esityksen luonnoksessa arvioidaan (s. 90), että NIS 2 –direktiivin toimeenpanemiseksi tiedonhallintalakiin ehdotettavien muutosten ei katsota aiheuttavan kaikille viranomaisille merkittäviä lisäresurssitarpeita, jotka aiheutuisivat viranomaisille NIS 2 –direktiivin edellyttämien velvoitteiden kohteena olemisesta. Perustelujen mukaan osalla viranomaisista ehdotettu sääntely kuitenkin voisi edellyttää valmiustason nostamista sekä tietojärjestelmämuutoksia. Oikeusministeriö kiinnittää huomiota siihen, että ehdotetut tiedonhallintalain säännökset tarkoittaisivat viranomaisille uusia velvoitteita ja uusia tietoturvasuojan vähimmäisvaatimuksia. Uudet velvoitteet ja vaatimustenmukaisuus edellyttävät tarkempia tiedonhallintayksikkökohtaisia selvityksiä ja kehittämistä ainakin kyberturvallisuuden ja riskienhallinnan osalta sekä mahdollista valmiustason kohottamista. Lienee epätodennäköistä, että kaikki viranomaiset pystyisivät kattamaan kustannusvaikutuksia ainakaan kaikilta osin valtion talouden kehyspäätösten ja valtion talousarvion mukaisista määrärahoista ilman lisärahoitusta.

Esitysluonnoksessa on asianmukaisesti huomioitu tietosuojavaltuutetulle seuraavat lisätyövaikutukset. Oikeusministeriö kiinnittää huomiota siihen, että hallituksen esityksestä seuraisi myös hallinnol-

listen seuraamusmaksujen täytäntöönpanotehtävä Oikeusrekisterikeskukselle. Lain nojalla maksettavaksi määrätty seuraamusmaksu pantasiin täytäntöön siinä järjestyksessä kuin sakon täytäntöönpanosta annetussa laissa (672/2002) säädetään. Täytäntöönpanotehtävä olisi hyvä huomioida esitysluonnoksen viranomaisvaikutuksissa, vaikka vaikutukset jäisivätkin vähäisiksi. Koska hallinnollisia seuraamusmaksuja määrättäisiin oletettavasti harvoin, Oikeusrekisterikeskukselle aiheutuisi oikeusministeriön alustavan arvion mukaan vain vähäistä lisätyötä seuraamusmaksujen perintään liittyvästä tehtävästä. Tehtävästä ei myöskään aiheutuisi välitöntä lisärahoitustarvetta siinä tapauksessa, että sääntelyllä ei ole tietojärjestelmävaikutuksia ja lisätyö jää vähäiseksi. Valvontaviranomaiselle ehdotettu seuraamusten määräämistä koskeva toimivaltuus on kuitenkin uusi, joten tarkkoja vaikutuksia on mahdollista arvioida vasta, kun ehdotetun lainsäädäntöä on sovellettu jonkin aikaa.

Oikeusministeriö kiinnittää huomiota siihen, että hallituksen esityksestä seuraisi lisää muutoksenhakujen käsittelyä hallintotuomioistuimille. Muutoksenhakukäsittelyjen tarkkoja vaikutuksia on mahdollista arvioida vasta, kun ehdotettua lainsäädäntöä on sovellettu jonkin aikaa.

Esitysluonnoksen 1. lakiehdotuksen 11 §:n määritelmää merkittävästä poikkeamasta voisi tarkentaa taloudellisten vaikutusten osalta. Nykyisellä muotoilulla vähäisetkin taloudelliset tappiot johtaisivat merkittävään poikkeamaan, joten määritelmän tarkennusehdotuksena esim. "...tarkoitetaan poikkeamaa, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle merkittäviä taloudellisia tappioita..." sekä vastaavasti muualle esityksessä.

Ehdotus edellyttäisi kyberturvallisuusriskien hallitsemiseksi muutoksia sekä viranomaisten välisiin että viranomaisten ja palveluntarjoajien välisiin sopimuksiin. Sopimusjärjestelyillä tulee huomioida tarvittavat kyberturvallisuusriskien hallintatoimenpiteet. Sopimusjärjestelyistä syntynee lisäkustannuksia aiempaa nopeammasta reagointikyvystä ja valmiuden korottamisesta läpi toimitusketjujen, mutta tarkkoja kustannusvaikutuksia on vaikea ennakolta arvioida.

Johdon vastuu

Lakiehdotusten pääasiallisen sisällön kuvauksessa todetaan, että NIS 2 –direktiivin täytäntöönpano ehdotetaan tehtäväksi sen vähimmäistason mukaisesti ja kansallinen liikkumavara täysimääräisesti hyödyntäen.

Direktiivin 20 artiklan mukaan jäsenvaltioiden on varmistettava, että keskeisten ja tärkeiden toimijoiden hallintoelimet hyväksyvät direktiivissä tarkoitetut kyberturvallisuusriskien hallintatoimenpiteet ja valvovat mainitun artiklan täytäntöönpanoa ja että nämä hallintoelimet voidaan saattaa vastuuseen, jos toimijat rikkovat kyseistä artiklaa (1 kohta). Lisäksi artiklassa säädetään hallintoelinten jäsenten velvollisuudesta osallistua koulutukseen sekä keskeisten ja tärkeiden toimijoiden velvollisuudesta tarjota säännöllisesti vastaavaa koulutusta työntekijöilleen, jotta he voivat hankkia riittävät tiedot ja taidot kyetäkseen tunnistamaan riskejä ja arvioimaan kyberturvallisuusriskien hallintakäytäntöjä ja niiden vaikutusta toimijan tarjoamiin palveluihin (2 kohta). Direktiivissä ei ole erikseen määritelty, mitä hallintoelimellä tarkoitetaan, mutta erityisesti mainitun artiklan 2 kohdassa tarkoituksena näyttää olevan eron tekeminen toimijan varsinaisen "yhtiöoikeudellisen johdon" (ts. hallintoelimet) ja työntekijöiden (ml. mahdollisesti yhtiöoikeudellisen johdon alaisuudessa työsopimuksen perusteella johtavissa tehtävissä työskentelevät) välille.

Direktiivin 32 artiklan 5 kohdan b alakohdan mukaan jäsenvaltioiden on varmistettava, että toimivaltaisella viranomaisella on tietyn edellytyksin valtuudet pyytää asiaankuuluvia elimiä tai tuomioistuimia kieltämään väliaikaisesti kansallisen lainsäädännön mukaisesti ketä tahansa luonnollista henkilöä, joka hoitaa keskeisen toimijan johtotehtäviä toimitusjohtajan tai laillisen edustajan tasolla, hoitamasta kyseisen toimijan johtotehtäviä. Laillisella edustajalla tarkoitettaneen direktiivissä tahoja, joka voi yhtiöoikeudellisesti sitovalla tavalla edustaa yhtiötä. Suomessa tällaisia tahoja voinevat olla hallituksen jäsen tai muu nimetty henkilö, jonka edustamisoikeus perustuu yhtiöjärjestyksen määräykseen tai hallituksen yhtiöjärjestyksensä määrärauksen perusteella tekemään päätökseen (ks. OYL 6:26 §).

Mainittujen direktiivin artiklojen täytäntöönpanemiseksi esitetyissä 1. lakiehdotuksen säännöksissä johdon vastuuta (10 §) ja johdon toiminnan rajoittamista tarkoittavia toimenpiteitä (33 §) ehdotetaan sovellettavaksi toimijan varsinaisen yhtiöoikeudellisen johdon (ts. hallitus, hallintoneuvosto, toimitusjohtaja) lisäksi myös toimitusjohtajan välittömään alaisuuteen kuuluvissa tehtävissä toimiviin, jos nämä hoitavat keskeisen toimijan ylimpiä johtotehtäviä tai tosiasiaa johtavat sen toimintaa. Oikeusministeriön käsityksen mukaan ehdotukset menevät tältä osin direktiivin edellyttämää vähimmäistasoa pidemmälle. Ehdotus poikkeaa myös yleisestä sääntelytavasta, jossa yhtiöiden harjoittamaan toimintaan sovellettavassa lainsäädännössä on tapana osoittaa erityisiä tehtäviä ja niihin liittyvä vastuu yleensä, joskaan ei poikkeuksetta, yhtiöiden varsinaiselle yhtiöoikeudelliselle johdolle (esim. vakuutus- ja rahoitusalan erityissääntely). Perusteena tälle on, että myös sovellettavassa yhtiölainsäädännössä on otettu vastaavasti huomioon yhtiön hallinnon järjestämiseen liittyvä toimivallanjako sekä säädetty toimielinten vastuista.

Esityksen perusteluista ei käy ilmi, miksi mainittujen artiklojen osalta on päädytty direktiivin vähimmäisvaatimuksia pidemmälle menevään täytäntöönpanoon. Oikeusministeriön mukaan esityksen jatkovalmistelussa olisi syytä tarkastella, ja esityksessä tarpeen mukaan perustella, tarvetta ehdotetulle ratkaisulle. Arvioinnissa tulisi ottaa huomioon se, että varsinaisen yhtiöoikeudellisen johdon alaisuudessa toimiva johto voi eri yhtiöissä olla muodostettu hyvin erilaisilla tavoilla, mikä voi käytännössä vaikeuttaa sääntelyn soveltamista.

Oikeusministeriö kiinnittää lisäksi huomiota siihen, että 1. lakiehdotuksen 10 §:ssä ehdotetaan säädettäväksi johdon ”vastuusta” kyberturvallisuuden riskienhallinnan toteuttamisen ja valvonnan järjestämisestä. Yhtiöoikeudellisen johdon osalta ehdotetun tapainen vastuu toteutuu yleensä viime kädessä johdon erityisenä vahingonkorvausvastuuna (ks. esim. OYL 22:1.2 §). Yhtiöoikeudellisen johdon alaisuudessa toimivien työntekijöiden asemassa olevien vastuuseen sovelletaan vahingonkorvauslain 4 luvun säännöksiä. Käsillä olevassa ehdotuksessa säädetyin erityisen vastuun toteuttamistapana olisi ilmeisesti lähinnä 33 §:n mukainen johdon toiminnan rajoittaminen. Oikeusministeriö pitää perusteltuna, että lakiin perustuvaa, ja ilmeisesti myös direktiivin edellyttämää, johdon vastuuta selvennetään ehdotettua tarkemmin lakiehdotuksessa tai sen perusteluissa.

Osastopäällikkö, ylijohdaja

Johanna Suurpää

Lainsäädäntöneuvos

Veli-Pekka Hautamäki

Jakelu LVM Liikenne- ja viestintäministeriö

Tiedoksi Valtiosihteeri Teija Makkonen
Kansliapäällikkö Pekka Timonen
Lainsäädäntöjohtaja Susanna Siitonen
Ministerin erityisavustaja Maaria Wallin

VN/18157/2023-OM-22

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons: