Liikenne- ja viestintävaliokunta

Asia: HE 57/2024 vp Hallituksen esitys eduskunnalle kyberturvallisuusdirektiivin (NIS 2 -direktiivi) täytäntöönpanoa koskevaksi lainsäädännöksi (https://www.eduskunta.fi/pdf/HE+57/2024)

Liikenne- ja viestintävaliokunta / HE 57/2024 vp / asiantuntijalausunto

Sosiaali- ja terveysministeriö (STM) on osallistunut kyberturvallisuusdirektiivin (NIS2-direktiivi) kansallista toimeenpanoa tukevaan työryhmään, näin ollen STM:llä ei ole lausuttavaa tai lisättävää esitetyn kyberturvallisuuslain (HE 57/2024 vp) riskienhallintaan tai vähimmäistason yleisiin velvoitteisiin. Alla olevat kommentit koskevat lähinnä valvontavelvoitteiden hoitamista.

Ehdotettujen lakien vaikutukset apteekkien valvontaan ja Fimeaan sekä Valviraan

Lääkealan turvallisuus- ja kehittämiskeskuksella (Fimea) on esitetyssä kyberturvallisuuslaissa apteekkien valvontavelvoite (luku 4, 26 §), joka koskee mm. liitteen I kohdan 13 alakohtia c – f ja liitteen II kohtaa 9 ja 10 tarkoitettuja toimijoita. Tulkintamme mukaan kaikki apteekit kuuluvat lain soveltamisalaan.

Lisäksi kyberturvallisuuslakia koskevaan luonnokseen ei ole lisätty Fimean valvonnassa olevia lääkedirektiivin 2001/83/EY artiklassa 79 tarkoitettuja lääketukkukauppoja, joita ei ole mainittu myöskään kyberturvallisuusdirektiivin (EU) 2022/2555 liitteen I kohdassa 5. Terveys. Lääketukkukaupat kuuluvat kuitenkin CER-direktiivin (EU) 2022/2557 soveltamisalaan. Näiden direktiivien täytäntöönpanoon liittyvässä kansallisessa keskustelussa on todettu, että NIS2- ja CER-direktiivit olisi tarkoitus panna kansallisesti täytäntöön yhteensovitetusti ja että CER-direktiivin soveltamisalaan kuuluvat toimijatyypit kuuluisivat myös NIS2-direktiivin soveltamisalaan. Jos näin on tarkoitus, tämä olisi Fimean näkemyksen mukaan hyvä mainita kyberturvallisuuslaissa ja/tai sen esitöissä, jotta velvoitteet ja vastuut olisivat selkeitä niin toimijoille kuin valvoville viranomaisille.

Lakiluonnoksen 4 §:ssä säädetään soveltamisalan rajauksista muun muassa, että lakia ei sovelleta toimijaan, jonka harjoittama liitteessä I tai II tarkoitettu toiminta on satunnaista ja vähäistä.

Säännöskohtaisissa perusteluissa todetaan 4 §:n osalta seuraavaa:

”Pykälän 5 momentissa säädettäisiin poikkeus lain soveltamisesta silloin, kun liitteessä I tai II tarkoitettu toiminta on satunnaista ja vähäistä. Toiminnan satunnaisuutta ja vähäisyyttä tulisi arvioida suhteessa toiminnan ajalliseen kestoon, toiminnan pääasialliseen tarkoitukseen, toiminnan laajuuteen ja toiminnasta riippuvien henkilöiden tai asiakkaiden määrään. Satunnaisena ja vähäisenä toimintana olisi pidettävä esimerkiksi pääasiassa omaa käyttöä varten tapahtuvaa sähkön tuottamista aurinkopaneelin tai tuuligeneraattorin avulla, jossa sähköverkkoon syötetään ajoittain sähkön ylituotantoa, joka on määrällisesti vähäistä. Poikkeus olisi tarpeen, jotta lain soveltamisala ei laajenisi sen tarkoituksen vastaisesti kattamaan vähäisen tai satunnaisen liitteessä

I tai II tarkoitetun toiminnan johdosta kokonaisuudessaan sellaista oikeushenkilöä tai luonnollista henkilöä, jonka harjoittama toiminta muutoin täyttäisi tai ylittäisi keskisuuren toimijan määritelmän mutta ei muutoin kuuluisi lain soveltamisalaan.”

Edellä oleva linjaa toiminnan soveltamisalaan kuulumista satunnaiseksi ja vähäiseksi arvioidun toiminnan osalta. Fimean valvontaan tuleva lääkkeiden tutkimusta ja kehitystä harjoittavat toimijat -toimijatyyppi kattaa niin toimijoiden taustoilta kuin toiminnan laajuudelta hyvin erilaista tutkimus- ja kehitystoimintaa. Alemman tasoisiin säännöksiin (EU:n delegoidut säännökset, alemman tason kansalliset säädökset / säännökset / valtioneuvoston asetus) on tästä johtuen tarpeen saada tarkempia linjauksia, jotta sääntelyn piiriin kuuluvat toimijat tunnistettaisiin sääntelyn tarkoitus huomioon ottaen tarkoituksenmukaisesti.

Valmisteltavana olevan lain esitöissä (4 §, 5 mom.) olisi hyvä taustoittaa monipuolisemmin niitä liitteiden I ja II toimijatyyppejä, jotka tulevat lain soveltamisalaan niiden koosta riippumatta. Nyt hallituksen esityksen edellä kuvattu säännöskohtainen perustelu kuvaa vain varsin selkeää tyyppitapausta satunnaisesta ja vähäisestä toiminnasta.

Sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain (703/2023, asiakastietolaki) nojalla sosiaali- ja terveysalan lupa- ja valvontavirasto (Valvira) valvoo apteekkien tietojärjestelmien vaatimustenmukaisuutta. Valvira voi asiakastietolain 93 §:n mukaan antaa tietojärjestelmiin liittyviä määräyksiä, mutta Valvira ei anna määräyksiä apteekin muihin toimiin. Esitetyssä kyberturvallisuuslaissa valvova viranomainen Fimea ja Valvira voi antaa riskienhallinnan kehittämiseksi täsmentäviä ohjeita ja suosituksia sekä määräyksiä. Epäselväksi jää, minkä tyyppisiä ohjeita ja suosituksia Fimea voi antaa niin, että Valviran kanssa ei ole päällekkäisyyttä.

Lisäksi tietojärjestelmän poikkeamista ja käyttöympäristöihin ja tietoverkkoihin liittyvistä häiriöistä pitää tällä hetkellä tehdä ilmoitus Valviralle asiakastietolain perusteella. Käsiteltävänä olevan hallituksen esityksen 9. lain mukaan apteekin tulisi jatkossa ilmoittaa myös Fimealle, jos tietojärjestelmän poikkeama taikka käyttöympäristöihin tai tietoverkkoihin kohdistuva merkittävä tietoturvallisuuden häiriö voi aiheuttaa merkittävän riskin apteekin toiminnalle. Asiakastietolain sääntely täydentää kyberturvallisuuslain ehdotettua sääntelyä. Asiakastietolain ehdotetut muutokset ovat jatkumoa voimassa olevalle sosiaali- ja terveydenhuollon asiakastietojen käsittelyä koskevalle sääntelylle, jota NIS2–direktiivi ja kyberturvallisuuslaki täydentävät julkisten palvelunantajien sekä vähintään keskisuurten yksityisten toimijoiden osalta mahdollistaen tehokkaammat puuttumisen keinot kyseisten säädösten tarkoittamien merkittävien riskien osalta. Asiakastietolaki taas mahdollistaa asiakastietolain mukaisten tietojärjestelmien häiriötilanteisiin puuttumisen. Asiakastietojen käsittelystä annettu laki, NIS2-direktiivi, ja kyberturvallisuuslaki muodostavat kokonaisuuden, joka mahdollistaa asianmukaiset ja tarkoituksenmukaiset menettelyt eritasoisiin kyberturvallisuuden riskeihin puuttumiseen sosiaali- ja terveydenhuollon asiakastietojen osalta.

Esitetyn lain säännöskohtaisissa perusteluissa (s.191) todetaan valvovia viranomaisia koskevan 26 §:n kohdalla Fimean valvonnasta seuraavaa:

”Lääkealan turvallisuus- ja kehittämiskeskus olisi tässä laissa tarkoitettu valvova viranomainen muiden lääkinnällisten laitteiden valmistajien paitsi kansanterveysuhan aikana kriittisten lääkinnällisten laitteiden valmistajien osalta. Fimea olisi tässä laissa tarkoitettu valvova

viranomainen myös veripalveluiden, apteekkien sekä potilaiden oikeuksien soveltamisesta rajat ylittävässä terveydenhuollossa annetun EU-direktiivin (2011/24/EU) mukaisten lääkkeiden ja lääkinnällisten laitteiden tarjoajien osalta.”

Edellä oleva säännöskohtainen perustelu on vaikeasti avautuva Fimealle lakiluonnoksessa esitettyä valvontakokonaisuutta ajatellen. Perusteluteksti sulkee pois kansanterveysuhan aikana kriittisiksi arvioidut lääkinnällisten laitteiden valmistajat, jotka kuitenkin mainitaan liitteen I kohdan 13 alakohdassa e) Fimean valvontakohteina. Lääkinnällisten laitteiden valmistajat ovat myös kansanterveysuhan aikana Fimean valvontakohteina. Lisäksi säännöskohtaisessa perustelussa ei mainita liitteen I kohdan 13 alakohtaa d, joka koskee lääkeaineiden ja lääkkeiden valmistusta harjoittavia toimijoita eli lääketehtaita.

Valvontaviranomaisten resurssit ja valvonnan toimeenpano

Esitetyssä kyberturvallisuuslaissa valvovalla viranomaisilla Fimealla ja Valviralla on oikeus tehdä toimijaa koskevia ennakoivia tarkistuksia (29 §). Resurssitarpeet on kuvattu hallituksen esityksessä, mutta on epäselvää, saavatko valvontaviranomaiset niitä. Nykyisessä taloudellisessa tilanteessa tulisi määritellä tarkemmin, mikä on ennakoivan tarkastustoimen hyväksyttävä minimitaso. Jos lisäresursseja ei saada, tarkastusten käsittelyajat voivat kasvaa ja ruuhkauttaa valvontaviranomaisia. On hyvä huomata, että isojen toimijoiden ennakkovalvonta on haastava ja aikaa vievää. Lisäksi NIS2 tuo uutena kolmivaiheisen ilmoitusmenettelyn ja ilmoituksille on myös määräajat. Tämä lisää valvontaviranomaisille tulevia ilmoituksia ja lisää viranomaistyötä. Todennäköistä on myös, että sanktiot ilmoittamatta jättämisestä lisäävät ilmoitusten määrää.

Sote-sektorin omavalvonnan tarve tulee korostumaan entisestään. Kriittisimmät kohteet ovat hyvinvointialueet, jotka vastaavat aina ensisijaisesti järjestämisvastuulleen kuuluvista sosiaali- ja terveyspalveluista, niiden jatkuvuudesta ja häiriöttömyydestä. Osana sote-palveluiden järjestämistehtävää hyvinvointialueiden tulee varmistaa ja turvata palveluidensa jatkuvuus myös ostaessaan palveluita pienemmiltä, NIS2-velvoitteiden ulkopuolisilta yksityisiltä palveluntuottajilta ja niiden alihankkijoilta. Hyvinvointialueilla tuleekin olla riittävät resurssit ja tekninen kyvykkyys laajoja alueita ja ihmisryhmiä koskettavien kyberturvallisuusuhkien torjumiseksi sekä toteutuneiden riskien hallitsemiseksi ja korjaamiseksi. Näin ollen omavalvontaa tulisi korostaa kaikissa keskusteluissa.

Viranomaistehtävien lisääntymisen vuoksi valvontaviranomaisten hallinnollista taakkaa tulisi hillitä luomalla keskitetty asiointikanava (ilmoituslomake) poikkeamailmoituksille. Tämä asiointikanava tulisi toteuttaa toimivaltaisen viranomaisen (Kyberturvallisuuskeskus, KTK) toimesta niin, että valvontaviranomaiset saisivat poikkeamaraportit keskitetysti yhden pisteet kautta, ilman valvontaviranomaisille koituvia lisäkustannuksia. Tavoitteena on myös vähentää raportoinnista aiheutuvia päällekkäisyyksiä. Toisin sanoen Liikenne ja viestintäviraston Kyberturvallisuus-keskuksella on lakiluonnoksessa keskitetyn yhteyspisteen tehtävä. Jotta toimijat välttyisivät päällekkäisiltä ilmoitusmenettelyiltä ja sektorikohtaisten valvontaviranomaisten yhteyspisteen ilmoituskäsittelystä, olisi linjakasta, että kaikki kyberturvallisuuslainsäädäntöön liittyvät ilmoitukset keskitettäisiin Liikenne- ja viestintävirastolle. Tämä tukisi myös viraston CSIRT-yksikön edellytyksiä nopeaan tiedonvälitykseen mahdollisissa tietoturvaloukkauksissa. Vastaava toimintatapa on ollut myös NIS1-ilmoituksissa. Huomiona, että vakavissa ja laajoissa kyberturvallisuuspoikkeamissa voi

olla kyse useasta pienemmästä eri viranomaisten valvontavastuulle kuuluvista häiriöstä, joita ei pystytä alkuvaiheessa tunnistamaan tai erottamaan toisistaan, mistä syystä keskitetty ilmoittaminen KTK:lle on perusteltua. Keskitetyn viranomaiskanavan myötä KTK saisi suoraan myös kiireelliset NIS2-ilmoitukset, mikä auttaa viranomaistehtävien koordinoinnissa ja priorisoinnissa muiden valvovien viranomaisten kanssa, esimerkiksi KTK:lla on jatkuva päivystysvelvollisuus akuuteissa asioissa, mitä valvovilla viranomaisilla ei ole.

STM:n hallinnonalan valvovat viranomaiset ovat valmistautuneet esitetyn lain nojalla tehtäviin velvoitteisiin. On kuitenkin mahdollista, että valvontaviranomaiset tulevat tukeutumaan entistä enemmän toimivaltaisen viranomaisen (KTK) ohjeisiin ja tukeen omassa tarkastustoiminnassaan. Näin ollen toimivaltaisen viranomaisen resurssit tulisi varmistaa. Vaikka synergiaa ja yhteistyötä lisätään, riskinä on, että kaikkia kohteita ei voida valvoa ennakoidusti. Lisäksi valvontaviranomaisissa kyberturvallisuusasiantuntijoiden rekrytoinneissa ennakoidaan tulevan haasteita.

Kansallisessa toimeenpanossa tulisi tehdä priorisointeja. Yksi hyödyllinen työkalu on kyberturvallisuuskeskuksen tekemä 13 kohdan kyberhygienia (perustuu NIS2-direktiiviin) lista käytännöistä, joiden avulla hyvinvointialueet voisivat tämän lain toimeenpanossa toteuttaa vaaditut toimet kohteiden vaativuuden ja prioriteetin mukaisesti, eli valita painopisteitä. Näitä painopistevalintoja ja prioriteettien seuranta tulisi toteuttaa keskitetysti esimerkiksi liikenne- ja viestintäministeriön toimesta yhdessä muiden ministeriöiden kanssa. Kyberhygienia voisi olla myös yksi työkalu valvontaviranomaisten lakisääteisen valvonnan toteuttamista.

Yleisesti sanottuna esitetyn lain toimeenpanossa organisaation johdon tuki ja johdon osallistumisen merkitys tulee kasvamaan kyberturvallisuuden hallintajärjestelmän jalkauttamisessa ja ylläpidossa. Merkittävä tekijä on tässä yhteisöllisyys ja verkostoituminen. Toimeenpanossa koulutus ja tietoisuuden lisääminen sekä osaamisen kehittäminen ovat keskeistä.

Erityisasiantuntija, tietoturvapäällikkö Andrei Laurén