VALTIONEUVOSTON OIKEUSKANSLERI

Liikenne- ja viestintäministeriö

Viite:

Liikenne- ja viestintäministeriön lausuntopyyntö 3.10.2023 VN/18157/2023

Asia:

Hallituksen esitysluonnos kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Liikenne- ja viestintäministeriö on pyytänyt lausuntoani otsikkoasiassa. Totean lausuntonani seuraavan.

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

Yhteiskunnan perustoimintojen kannalta kriittisten toimijoiden viestintäverkkojen ja tietojärjestelmien turvallisuus on muuttunut yhä tärkeämmäksi ja keskeisemmäksi suojelun kohteeksi. Varautumisen ja kriisinkestävyyden kannalta on välttämätöntä, että näille toimijoille asetetaan yhdenmukaiset ja ajantasaiset vaatimukset kyberhyökkäyksiin varautumisesta ja niiden torjumisesta.

Ehdotettu uusi yleislaki kyberturvallisuuden riskienhallinnasta on mielestäni kannatettava sääntelyratkaisu aikaisempaan hajautettuun sääntelyyn verrattuna. Yleislain sisältämät yhteiset riskienhallintavelvoitteet ja raportointivelvoitteet yhdenmukaistavat kyberturvallisuuden ylläpitoa ja kiinnittävät organisaatioiden huomiota kyberturvallisuutta koskevista perusasioista huolehtimiseen. Uuden NIS2-direktiivin soveltamisala ulottuu merkittävästi laajemmalle kuin aikaisemman direktiivin, joka implementointiin erityislainsäädäntöön tehdyillä rajatuilla muutoksilla. Laajan soveltamisalankin vuoksi on perusteltua, että NIS2-direktiivin täytäntöönpano toteutetaan yleislailla.

Julkishallinnon toimijat tulevat nyt ensi kertaa kyberturvallisuussääntelyn piiriin. NIS2-direktiivin täytäntöönpano julkishallinnossa säädettäisiin julkisen hallinnon tiedonhallintalain (906/2019) muutoksella. Myös tämä on mielestäni perusteltu ja kannatettava ratkaisu.

Soveltamisalaa koskevat huomiot

Sääntelyn soveltamisala laajenee ehdotuksessa merkittävästi aikaisempaan verrattuna. Direktiivin ja uuden lainsäädännön velvoitteiden täytäntöönpanossa on keskeistä, että eri alojen toimijat ovat tietoisia uusista lakisääteisistä velvoitteista. Tämän huomioon ottaen on jossain määrin ongelmallista, että lain soveltamisala määrittyy varsin vaikeaselkoisella tavalla kyberturvallisuuden riskienhallinnasta annetun lain 3 §:n ja lain liitteiden I ja II, lain 2 §:n määritelmäsäännöksen (”keskisuuri toimija”, joka puolestaan määräytyy komission suosituksen perusteella) sekä lain 3 §:n 2 momentissa säädetyn valtuuden nojalla annetulla valtioneuvoston asetuksella. Kyse on sinänsä erityistoimialoista, kuten liikenteen, energian, viestinnän, vesihuollon, terveyden sekä kemikaali- ja elintarvikealojen toimijoista, mutta soveltamisalan piiriin voi lukeutua myös kooltaan pieniäkin henkilö- ja yhteisötoimijoita. Perustuslain 80 §:n 1 momentin ja 18 §:n sekä yleisemminkin yksilöiden ja yhteisöjen oikeusaseman kannalta olisi suositeltavaa, ettei lain soveltamisala jäisi näin monipolvisen määrittelyn varaan.

1. lakiehdotuksen 43 §:ssä asetetaan toimijoille velvoite itse tunnistaa asemansa soveltamisalaan kuuluvana ja ilmoittautua valvontaviranomaiselle toimijaluetteloon. Tämän velvoitteen laiminlyönnistä voisi lain 37 §:n mukaan seurata hallinnollinen seuraamusmaksu. Ottaen huomioon lain asettamat velvoitteet ja sanktiouhka on välttämätöntä, että asianomaiset valvontaviranomaiset huolehtivat riittävästä neuvonnasta ja ohjauksesta lain toimeenpanossa. Erityisesti pienten toimijoiden kohdalla viranomaisohjaus on välttämätöntä, sillä jo pelkästään toimijan oman aseman selvittäminen hankalasti avautuvan soveltamisalasääntelyn avulla voi olla vaikeaa.

Kyberturvallisuutta koskevat velvoitteet ulotettaisiin julkishallintoon julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) muutoksella. Lain 3 §:n mukaan uutta 4 a lukua kyberturvallisuusvelvoitteista ja niiden noudattamisen valvonnasta sovellettaisiin valtion virastoihin ja laitoksiin, valtion liikelaitoksiin, itsenäisiin julkisoikeudellisiin laitoksiin sekä hyvinvointialueisiin ja –yhtymiin. Valtion turvallisuusviranomaiset ja eräät muut laissa säädetyt viranomaiset jäisivät soveltamisalan ulkopuolelle. Myös kunnat, kuntayhtymät ja julkisia hallintotehtäviä hoitavat viranomaiskoneiston ulkopuoliset tahot jäisivät soveltamisalan ulkopuolelle, mutta soveltamisalan piiriin kuuluisivat kuitenkin CER-direktiivin täytäntöönpanolain mukaiset julkishallinnon toimialojen kriittiset toimijat.

Lain 3 §:n mukaan valtioneuvoston oikeuskanslerin toimintaan, tasavallan presidentin kansliaan ja Kansaneläkelaitokseen sovellettaisiin laissa säädettyjä riskienhallinta- ja raportointivelvoitteita, mutta niihin ei sovellettaisi lain 4 a luvun säännöksiä uusien velvoitteiden valvonnasta ja seuraamuksista. Totean, että valtioneuvoston oikeuskanslerin osalta sääntely vastaa nykyisin noudatettua sääntelytapaa (esim. tietosuojalain 14.2 §), jossa ylin laillisuusvalvoja suljetaan nimenomaisilla säännöksillä muun viranomaisvalvonnan ulkopuolelle.

Lain 3 §:n säännökset jättävät eduskunnan virastot, esim. valtiontalouden tarkastusviraston sekä eduskunnan oikeusasiamiehen, kokonaan lain 4 a luvun soveltamisen ulkopuolelle. Direktiivin 6 artiklan 35 kohta ei sinällään tätä edellyttäisi, sillä direktiivissä käytetyllä käsitteellä ”parlamentti” viitataan kansanedustuslaitoksen toimintaan, Suomessa eduskunnan valtiopäivätoimintaan. Eduskunnan virastot on yleensä kansallisessa lainsäädännössä säädetty yleislakien piiriin kuuluviksi. Jatkovalmistelussa on syytä vielä tarkistaa 3 §:n säännökset näiltä osin; lain 37 §:n 2 momentissa viitataan eduskunnan virastoihin, joten tarkoituksen ei ehkä olekaan ollut jättää niitä lain soveltamisalan ulkopuolelle.

Julkishallinnon toimijoita koskevia säännöksiä on sijoitettu hieman epäloogisella tavalla myös yleislakiin (33.2 §, 37.2 §), vaikka sääntelyn yleisenä lähtökohtana lienee se, että tiedonhallintalain säännökset ovat kattavia julkishallinnon toimijoiden osalta direktiivin implementoinnissa.

Riskienhallintavelvoitetta koskevat huomiot

—

Raportointivelvoitetta koskevat huomiot

—

Valvontaa koskevat huomiot

Esitysluonnoksen mukaan velvoitteiden noudattamisen valvonta olisi hajautettu eri toimialojen valvontaviranomaisille. Tämä on mielestäni oikeansuuntainen ratkaisu ottaen huomioon soveltamisalan laajuus ja heterogeenisuus. Lain täytäntöönpanossa on kuitenkin otettava huomioon se, että useimmilla eri sektorien valvontaviranomaisilla ei ole erityistä osaamista kyberturvallisuudessa. Tästä aiheutuu välttämätön tarve huolehtia näiden viranomaisten osaamisen syventämisestä, jotta valvontatehtäviä voidaan asianmukaisesti hoitaa.

Julkishallinnon osalta valvontaviranomaisena toimisi esitysluonnoksen mukaan keskitetysti Liikenne- ja viestintävirasto. Perusteluissa pohditaan viraston sopivuutta valvomaan ylempiä tahojaan, erityisesti ministeriöitä (s. 99-100). Tällaisia valvonta-asetelmia julkishallinnossa on jo nykyisinkin eri sektoreilla eivätkä ne ole lainsäädännön kannalta muodollisesti ongelmallisia. Tiedonhallintalain 3 §:ssä on otettu huomioon valtioneuvoston oikeuskanslerin asema ylimpänä laillisuusvalvojana asianmukaisella tavalla ja jätetty oikeuskansleri Liikenne- ja viestintäviraston valvonnan ja seuraamusten ulkopuolelle.

Kiinnitän huomiota myös siihen, että ehdotettu lainsäädäntö kuuluu aineelliselta sisällöltään osittain ilmoittajansuojelulain (1171/2022) soveltamisalaan, joten siinä asetettujen velvoitteiden laiminlyönti tai rikkominen voi johtaa myös ilmoittajansuojelujärjestelmän soveltamiseen. Tämä seikka on hyvä ottaa huomioon valvontajärjestelmää koskevissa perusteluissa.

Yleislain 36 §:n 1 momenttia on syytä sanamuodoltaan tarkentaa siten, että oikaisuvaatimusmenettelystä säädetään hallintolain 7 a luvussa (vrt. TiedonhallintaL 18 m §).

Seuraamusmaksua koskevat huomiot

NIS2-direktiivi sisältää säännökset hallinnollisesta seuraamusmaksusta lain velvoitteiden rikkomistilanteissa. Direktiivi jättää jäsenvaltioille kansallista liikkumavaraa hallinnollisen sanktion ulottamisessa julkishallinnon toimijoihin. Esitysluonnoksessa ehdotetaan, ettei julkishallinnon toimijoille voitaisi määrätä seuraamusmaksua. Tämä on mielestäni perusteltu ratkaisu ottaen huomioon kansallisessa lainsäädännössä noudatettu käytäntö (mm. TietosuojaL 24 §) ja se. että viranomaistoimintaan kohdistuu jo muutoinkin vahvemmat lain noudattamisen velvoitteet ja vastuu muihin toimijoihin verrattuna.

Seuraamusmaksun asettaisi monijäseninen toimielin, seuraamusmaksulautakunta, joka koostuisi eri sektorien valvontaviranomaisten edustajista. Lain 38 §:n 1 momentin mukaan lautakunta päättäisi seuraamusmaksusta valvovan viranomaisen esityksestä. Pykälän 3 momentissa todetaan kuitenkin, että seuraamusmaksun esittelijänä toimii sen valvovan viranomaisen virkamies, jonka valvontatoimivaltaan kohdistuva asia on ratkaistavana. Näiltä osin on tarkennettava, kumman tahon esityksestä —valvontaviranomaisen vai virkamiehen — on kyse: tekeekö valvontaviranomainen esityksestä ensin päätöksen ja onko esittelijänä toimiva

virkamies sidottu tähän päätökseen? Esittelijä kantaa esityksestä joka tapauksessa perustuslain 118 §:n mukaisen vastuun.

Hallinnollista seuraamusmaksua ja sen määräämistä koskevat perustelut ovat esitysluonnoksessa hyvin niukat. Esimerkiksi seuraamusmaksun määräämisessä huomioon otettavia seikkoja (39 ja 40 §) ei avata perusteluissa käytännössä lainkaan; millainen tulkintasisältö annetaan esim. toimijan halukkuudelle tehdä yhteistyötä valvovan viranomaisen kanssa? Kyse voi olla euromääräisesti erittäin merkittävästä seuraamusmaksusta, mikä edellyttäisi soveltamisen tueksi ohjaavaa perustelutekstiä.

Seuraamusmaksun määräämisessä on otettu 41 §:n 4 momentissa asianmukaisesti jo säännöstekstissä huomioon mahdollinen päällekkäisyys tietosuoja-asetuksen 83 artiklassa säädetyn seuraamusmaksun kanssa.

CSIRT-yksikön tehtäviä koskevat huomiot

—

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

Ks. edellä.

Verkkotunnusvälittäjiä koskevat huomiot

—

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

—

Vaikutustenarviointia koskevat huomiot

—

Muut huomiot ja avoin palaute esityksestä

Esitysluonnoksen säätämisjärjestysperusteluissa käsitellään laajasti luottamuksellisen viestin suojaa koskevia kysymyksiä. CSIRT-yksikön tekemää haavoittuvuuskartoitusta koskevien säännösten arvioinnissa käydään läpi tiedustelutoimintaa koskevia tulkintakannanottoja, mikä on hieman sekaannusta aiheuttavaa ja harhaanjohtavaa, sillä haavoittuvuuskartoitus ei tosiasiassa rinnastu miltään osin tiedustelutoimintaan liittyvään tiedonhankintaan tai tietoliikenteen seurantaan. Perusteluja olisi syytä kirkastaa näiltä osin. Haitallisen tietokoneohjelman tai käskyn sisältävän viestin käsittelyä koskevia perusteluja olisi myös aiheellista selkeyttää siten, ettei perusteluissa tukeuduttaisi (viestin välitystiedot s. 192) sellaiseen perustuslakivaliokunnan tulkintakäytäntöön, joka on sittemmin jo muuttunut toisen sisältöiseksi. On myös otettava huomioon, että haittaohjelmissa ja automatisoiduissa kalasteluviesteissä on itsessään kyse tietoliikenne- tai tietojärjestelmärikollisuudesta, minkä tulisi näkyä perustelutekstissä. Ehdotettu puuttuminen tällaiseen viestintään ja siitä tiedon jakaminen riskin kohteena

oleville toimijoille perustellaan lähtökohtaisesti perusoikeuksien yleisten rajoitusedellytysten kannalta. Perusteluissa olisi hyvä selventää, mikä on ehdotettujen säännösten suhde perustuslain 10 §:n 4 momentissa säädettyyn kvalifioituun lakivaraukseen.

Johdon toiminnan rajoittamista koskevissa säännöksissä (1. lakiehdotuksen 33 §) ja perusteluissa tulisi ottaa huomioon se, että säännökset voivat koskea myös henkilöyhtiöitä toisin kuin esitysluonnoksen perusteluissa todetaan. Keskeisiä toimijoita ovat 26 §:n mukaan esimerkiksi DNA-palveluntarjoajat ja luottamuspalvelujen tarjoajat niiden koosta riippumatta, joten johdon toiminnan rajoittamista koskevat säännökset voisivat kohdistua esim. mahdolliseen avoimen yhtiön tai kommandiittiyhtiön hallitukseen. Tämä on syytä arvioida myös perustuslain 18 §:n kannalta.

Esitysluonnoksessa jää osittain avoimeksi se, miten komission täytäntöönpanosäädöksiä ja standardointia koskevat NIS2-direktiivin 21 artiklan 5 kohdan, 23 artiklan 11 kohdan sekä 24 ja 25 artiklan säännökset on tarkoitus panna täytäntöön. Esitysluonnoksessa ei ole asiasta mahdollisesti tarvittavia asetuksenantovaltuuksia tai asiaa avaavia perusteluja. Esitysluonnokseen sisältyy säännökset valvontaviranomaisten määräystenantovallasta (1. lakiehdotuksen 9 §:n 4 mom.), joita olisi mahdollista käyttää ainakin osittain täytäntöönpanoon (perustelut s. 201).

Lakiehdotukset sisältävät paikoin terminologiaa, joka ei vastaa lakikielelle asetettuja yleiskielisyyden vaatimuksia (esim. 1. lakiehdotuksen 9 §:ssä ”kyberhygieniakäytännöt”, 20 §:ssä ”ei-intrusiivinen” ja ”konfiguroitu”, 2. lakiehdotuksen 18 c §:ssä ”kyberhygieniakäytännöt”). Näille termeille on tarpeen löytää asianmukaiset yleiskielen vastineet. Direktiivin käsite ”hallinnollinen sakko” on perustellusti muutettu täytäntöönpanolaissa ”hallinnolliseksi seuraamusmaksuksi”, joka on kansallisen lainsäädäntömme tuntema käsite.

Tämä asiakirja on allekirjoitettu sähköisesti.

Oikeuskansleri Tuomas Pöysti

Kansliapäällikkö Tuula Majuri

OKV/1898/21/2023-OKV-3

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons:

Majuri Tuula 91213735J	Pöysti Tuomas 912198006
2023-11-29	2023-11-30