Liikenteenohjausyhtiö Fintraffic Oy

Lausunto

29.11.2023

Asia: VN/18157/2023

Lausuntopyyntö: luonnos hallituksen esitykseksi kyberturvallisuusdirektiivin (NIS2-direktiivi) täytäntöönpanemiseksi

Lausunnonantajan lausunto

Yleiset huomiot NIS2-direktiivin tavoitteista ja tarkoituksesta

-

Soveltamisalaa koskevat huomiot

Liikenteenohjausyhtiö Fintraffic Oy (Fintraffic) lausuu esityksestä seuraavaa.

Tiedonhallintalain soveltamisala:

Tiedonhallintalain 3.2 § mukaan ” Lisäksi 4 a lukua sovelletaan [CER-lain] nojalla julkishallinnon toimialan kriittisiksi toimijoiksi määriteltyihin toimijoihin.” Fintrafficilla ei vielä tässä vaiheessa ole tarkkaa käsitystä siitä, katsotaanko liikenteenohjaus- ja hallintapalvelun tarjoajana toimivat julkiset ja yksityiset yritykset sellaisiksi julkishallinnon toimialan kriittisiksi toimijoiksi, joihin tullaan soveltamaan tiedonhallintalain 4 a luvun vaatimuksia (erityislaki) vai kuuluvatko liikenteenohjaus- ja hallintapalvelun tarjoajat kyberturvallisuuden riskienhallinnasta annetun lain soveltamisalaan (yleislaki). Soveltamisala määrittynee lopullisesti vasta CER-lain määritelmien täsmentyessä.

Kyberturvallisuuden riskienhallinnasta annetun lain soveltamisala:

Kyberturvallisuuden riskienhallinnasta annetussa laissa säädettäisiin mm. eräiden yhteiskunnan toiminnan kannalta kriittisten toimijoiden (toimijat) kyberturvallisuuden riskienhallinta- ja raportointivelvoitteista. Lain 3 §:n mukaan soveltamisalaan kuuluvalla toimijalla tarkoitetaan oikeushenkilöä tai luonnollista henkilöä, joka harjoittaa liitteessä I tai II tarkoitettua toimintaa.

Tieliikenne:

Liitteessä I on tieliikenteen osalta listattuna ainoastaan Komission delegoidun asetuksen (EU) 2015/962 2 artiklan 12 alakohdassa tarkoitetut liikenteenhallinnasta vastaavat tieviranomaiset sekä Liikenteen palveluista annetun lain (320/2017) 160 §:ssä tarkoitettujen älykkäiden liikennejärjestelmien ylläpitäjät. Lista ei sisällä tieliikenteen ohjaus- ja hallintapalvelun tarjoajia eikä myöskään esimerkiksi yksityisiä tunnelihallinnoijia. Fintraffic korostaa, että liikenteen palveluista annetun lain 137 §:n mukaista tieliikenteen ohjaus- ja hallintapalvelun tarjoajaa ei hallinnonalalla ole pidetty tieviranomaisena. Fintraffic kiinnittää huomiota, että vesiliikenteen osalta VTS-palveluntarjoajat ja raideliikenteen osalta liikenteenohjauspalvelua tarjoavat yhtiöt ovat listattuna liitteessä I.

Toki liikenteen palveluista annetun lain 140 § on ehdotettu jätettäväksi viittaus kyberturvallisuuden riskienhallinnasta annettuun lakiin. Tämä poikkeaa lakiehdotuksen taustalla olleesta systematiikasta, jonka mukaan erityislaeissa olevat velvoitteet kumottaisiin ja lain piiriin kuuluvat toimijat koottaisiin yhteen kyberturvallisuuden riskienhallinnasta annetun lain alle. Lisäksi Fintraffic korostaa, että liikenteen palveluista annetun lain 140 § on otsikoitu ”Tietoturva tieliikenteen ohjaus- ja hallintapalvelussa”, mutta lainkohta ei sisällä varsinaisesti tietoturvaa koskevia velvoitteita. Kuvattu ratkaisu jättää epäselväksi, sovelletaanko tieliikenteen ohjaus- ja hallintapalvelun tarjoajaan jatkossa tiedonhallintalain 4 luvun tietoturvallisuutta koskevia vaatimuksia (kts. myös TiHL 3.4 §) vai ohittaako erityislainsäädös yleislain tässä kohtaa. Fintraffic näkisi mahdollisena myös ratkaisun, jossa lain 140 § otsikko muutettaisiin koskemaan tietojen säilytystä ja tieliikenteen ohjaus- ja hallintapalvelun tarjoajat lisättäisiin suoraan Liitteeseen I.

Ilmaliikenne:

Liitteessä I on ilmaliikenteen osalta listattuna Yhtenäisen eurooppalaisen ilmatilan toteuttamisen puitteista annetun Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 549/2004 2 artiklan 1 alakohdassa määriteltyä lennonjohtopalvelua tarjoavat lennonjohtopalvelun tarjoajat.

Esityksen kohdassa 3.3.1 Ilmaliikenne on todettu, että ”ilmailu on kansainvälistä toimintaa, ja siviili-ilmailun sääntely perustuu pääosin kansainvälisiin sopimuksiin ja EU-lainsäädäntöön. EU on hiljattain hyväksynyt useita ilmailun kyberturvallisuutta koskevia säädöksiä. Ilmailun turvatoimiin liittyvät kyberturvallisuussäädökset ovat jo voimassa, mutta muilta osin kyberturvallisuutta koskevat säädökset (PART-IS) tulevat sovellettaviksi vasta lokakuussa 2025 tai helmikuussa 2026 eli vähintäänkin vuotta myöhemmin kuin NIS2-sääntely. Edelleen esityksessä on todettu, että ”ilmailun tietoturvallisuutta koskeva EU-sääntely soveltuu laajempaan toimijajoukkoon kuin NIS2-direktiivi, ja toimijoille asetettavat velvoitteet vastaavat pitkälti NIS2-vaatimuksia. Tätä ilmailun erityislainsäädäntöä voidaan pitää NIS2-direktiivin 4 artiklassa tarkoitettuina alakohtaisena unionin lainsäädäntönä.”

Lisäksi EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) N:o 376/2014 poikkeamien ilmoittamisesta, analysoinnista ja seurannasta siviili-ilmailun alalla koskee siviili-ilmailun turvallisuustietojen ilmoittamista, keräämistä, tallentamista, suojaamista, vaihtamista, jakamista ja analysointia. 1 artiklan 2. kohdan mukaan poikkeamien ilmoittamisen ainoana tarkoituksena on ehkäistä onnettomuuksia ja vaaratilanteita eikä osoittaa syyllisyyttä tai vahingonkorvausvelvollisuutta.

Poikkeama-asetuksen mukaan poikkeamatietojen vaihdon ensisijaisen tavoitteen olisi oltava ilmailuonnettomuuksien ja vaaratilanteiden ehkäiseminen. Sitä ei näin ollen olisi käytettävä syyllisyyden tai korvausvastuun osoittamiseen eikä turvallisuustason vertailuun (20). Tiedonsaantioikeutta koskevissa kansallisissa säädöksissä olisi otettava huomioon tällaisten tietojen tarvittava luottamuksellisuus. Kerätyt tiedot olisi suojattava asianmukaisella tavalla luvattomalta käytöltä ja luovuttamiselta. Niitä olisi käytettävä yksinomaan ilmailun turvallisuuden ylläpitämiseen ja parantamiseen, eikä niitä olisi käytettävä syyllisyyden tai vahingonkorvausvelvollisuuden osoittamiseen (33).

Ilmailulain 128 §:n mukaan viranomainen ei saa ryhtyä oikeudellisiin toimenpiteisiin suunnittelemattoman tai tahattoman rikkomuksen johdosta, joka tulee viranomaisen tietoon ainoastaan siksi, että siitä on tehty ilmoitus poikkeama-asetuksen nojalla, ellei kyse ole poikkeama-asetuksen 16 artiklan 10 kohdassa tarkoitetusta tilanteesta.

NIS2-direktiivin 4 artiklan kohdassa 1 taas on todettu, että ”jos alakohtaisissa unionin säädöksissä edellytetään, että keskeiset tai tärkeät toimijat ottavat käyttöön kyberturvallisuusriskien hallintatoimenpiteitä tai ilmoittavat merkittävistä poikkeamista, ja jos kyseiset vaatimukset ovat vaikutukseltaan vähintään tässä direktiivissä säädettyjä velvoitteita vastaavia, tällaisiin toimijoihin ei sovelleta tämän direktiivin asiaankuuluvia säännöksiä, myöskään VII luvun säännöksiä valvonnasta ja täytäntöönpanosta. Jos alakohtaiset unionin säädökset eivät kata tämän direktiivin soveltamisalaan kuuluvan toimialan kaikkia toimijoita, tämän direktiivin asiaankuuluvia säännöksiä sovelletaan edelleen niihin toimijoihin, joita kyseiset alakohtaiset unionin säädökset eivät kata.”

Fintrafficin näkemyksen mukaan ilmailun osalta noudatettavaa EU erityislainsäädäntöä voidaan pitää NIS2-direktiivin 4 artiklassa tarkoitettuina alakohtaisena unionin lainsäädäntönä, joten NIS2 direktiivin vaatimuksia ei tulisi ylipäänsä tulisi ulottaa koskemaan ilmailun toimijoita.

Lakiehdotuksen soveltamisalan piiriin on liitteessä I ilmaliikenteen osalta listattuna kohdassa c) ainoastaan Asetuksen (EY) 549/2004 2 artiklan kohdan 1 mukaiset lennonjohtopalvelun tarjoajat, mutta ei muita lennonvarmistuspalveluita (kts. myös EY 549/2004 2 artiklan kohdat 4, 7 ja 10) tarjoavia toimijoita, joita kaikkia tuleva PART-IS koskee. Fintraffic ei pidä perusteltuna, että ilmailun toimijakentässä juuri lennonjohtopalvelun tarjoajat asetettaisiin kaksoissääntelyn alaiseksi.

Välittömät toimittajat ja palveluntarjoajat (alihankkijat):

NIS2-direktiivin 21 artiklan 2 kohdan d alakohta ja 21 artiklan 3 kohta mukaan keskeisen toimijan on varmistuttava toimitusketjunsa turvallisuudesta välittömistä toimittajien ja palveluntarjoajien osalta.

Esityksen 9 §:n perusteluissa on todettu, että ”toimijat voisivat hallita toimitusketjujen kyberturvallisuusriskiä sisällyttämällä kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät ”välittömien toimittajiensa ja palveluntarjoajiensa” kanssa.” Kuitenkin ehdotetussa lakiluonnoksessa 9 § sanamuoto velvoittaa toimijan ulottamaan kyberturvallisuusriskien hallintatoimenpiteet lähtökohtaisesti koko toimintaketjuun, eikä direktiivin ja yksityiskohtaisiin perusteluihin kirjausten mukaisesti nimenomaisesti välittömiin toimittajiin ja palveluntarjoajiin. Mikäli toimija lailla asetetaan vastuuseen koko toimitusketjun kyberturvallisuusriskien hallintatoimenpiteistä, muodostuu toimitusketjujen hallinta sopimusoikeudellisesti hankalaksi, aikaa vieväksi ja potentiaalisesti todella kalliiksi. Lisäksi suomalaiset toimijat käytännössä asetetaan laajempaan vastuuseen kuin mitä direktiivi edellyttää vastaavilta eurooppalaisilta toimijoilta. Fintraffic näkee tärkeänä täsmentää lakiluonnoksen sanamuotoa, niin että se noudattelee direktiivin ja yksityiskohtaisiin perusteluihin kirjattua linjausta, jossa kyberturvallisuusriskien hallintatoimenpiteet kohdistetaan välittömiin toimittajiin ja palveluntarjoajiin.

Riskienhallintavelvoitetta koskevat huomiot

Välittömät toimittajat ja palveluntarjoajat (alihankkijat):

NIS2-direktiivin 21 artiklan 2 kohdan d alakohta ja 21 artiklan 3 kohta mukaan keskeisen toimijan on varmistuttava toimitusketjunsa turvallisuudesta välittömistä toimittajien ja palveluntarjoajien osalta.

Esityksen 9 §:n perusteluissa on todettu, että toimijat voisivat hallita toimitusketjujen kyberturvallisuusriskiä sisällyttämällä kyberturvallisuusriskien hallintatoimenpiteitä sopimusjärjestelyihin, joita ne tekevät ”välittömien toimittajiensa ja palveluntarjoajiensa” kanssa. Kuitenkin ehdotetussa lakiluonnoksessa 9 § sanamuoto velvoittaa toimijan ulottamaan kyberturvallisuusriskien hallintatoimenpiteet lähtökohtaisesti koko toimintaketjuun, eikä direktiivin ja yksityiskohtaisiin perusteluihin kirjausten mukaisesti nimenomaisesti välittömiin toimittajiin ja palveluntarjoajiin. Mikäli toimija lailla asetetaan vastuuseen koko toimitusketjun kyberturvallisuusriskien hallintatoimenpiteistä, muodostuu toimitusketjujen hallinta sopimusoikeudellisesti hankalaksi, aikaa vieväksi ja potentiaalisesti todella kalliiksi. Lisäksi suomalaiset toimijat käytännössä asetetaan laajempaan vastuuseen kuin mitä direktiivi edellyttää vastaavilta eurooppalaisilta toimijoilta. Fintraffic näkee tärkeänä täsmentää lakiluonnoksen sanamuotoa, niin että se noudattelee direktiivin ja yksityiskohtaisiin perusteluihin kirjattua linjausta, jossa kyberturvallisuusriskien hallintatoimenpiteet kohdistetaan välittömiin toimittajiin ja palveluntarjoajiin.

Raportointivelvoitetta koskevat huomiot

-

Valvontaa koskevat huomiot

-

Seuraamusmaksua koskevat huomiot

-

CSIRT-yksikön tehtäviä koskevat huomiot

-

Tiedonhallintalakia ja täytäntöönpanoa julkishallinnossa koskevat huomiot

-

Verkkotunnusvälittäjiä koskevat huomiot

-

Kumottavaksi ehdotettuja säännöksiä koskevat huomiot

Tieliikenne:

Liitteessä I on tieliikenteen osalta listattuna ainoastaan Komission delegoidun asetuksen (EU) 2015/962 2 artiklan 12 alakohdassa tarkoitetut liikenteenhallinnasta vastaavat tieviranomaiset sekä Liikenteen palveluista annetun lain (320/2017) 160 §:ssä tarkoitettujen älykkäiden liikennejärjestelmien ylläpitäjät. Lista ei sisällä tieliikenteen ohjaus- ja hallintapalvelun tarjoajia.

Vaikutustenarviointia koskevat huomiot

-

Muut huomiot ja avoin palaute esityksestä

-

Korvenoja Riikka