

Asia: VN/18947/2022-SM-46

Luonnos hallituksen esitykseksi laiksi yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta ja eräiksi muiksi laeiksi

1.

Yleiset huomiot CER-direktiivin kansallisesta toteuttamistavasta, kuten esimerkiksi viranomaistoiminnan järjestämisestä ja valvontamallista

-

2.

Soveltamisalaa koskevat huomiot, kuten esimerkiksi kriittisen toimijan määrittäminen ja kriteeristön kattavuus

Liikenteenohjausyhtiö Fintraffic Oy (Fintraffic) kiittää mahdollisuudesta lausua asiassa ja toteaa seuraavaa.

CER-lain ja kansallisen NIS2-lain välillä on tiivis yhteys, ja niiden täytäntöönpanoa ja soveltamisalaa tulee yhteensovittaa kansallisella tasolla. NIS2-lakia sovelletaan CER-lain nojalla kriittisiksi toimijoiksi määritettyihin toimijoihin riippumatta niiden koosta. Tämän lisäksi NIS2-lain soveltamisalaan voi kuulua myös laajempi joukko toimijoita, joita ei välttämättä ole määritelty kriittisiksi CER-lain mukaan.

Fintraffic pitää tärkeänä, että CER-direktiivin/lain liite: toimialat, alasektorit ja toimijaluokat sekä NIS2-lain liite 1 ovat linjassa keskenään niiden kriittisten toimijoiden osalta, jotka kuuluvat molempien lakien soveltamisalan piiriin. Aikaisemmin lausunnoilla olleen NIS2-lain soveltamisalaa koskeva liite on sisältänyt mm. lennonjohtopalveluntarjoajat (ATC), raideliikenteen liikenteenohjauspalvelua tarjoavat yhtiöt ja VTS-palveluntarjoajat. Tieliikenteen osalta NIS2-lain liite on sisältänyt liikenteenhallinnasta vastaavat tieviranomaiset sekä älykkäiden liikennejärjestelmien ylläpitäjät, mutta tieliikenteen ohjaus- ja hallintapalveluntarjoajaa koskeva säännös oli ehdotettu sisällytettäväksi liikenteen palveluista annetun lain 140 §:ään – mitä ratkaisua Fintraffic kritisoi omassa NIS2-lakia koskevassa lausunnossaan epä johdonmukaiseksi. Fintraffic korostaa, että CER-lain

liitteessä käytettyä 'tieviranomaisen' käsitettä ja soveltamisalaa tulee tarkentaa esitysluonnokseen/liitteeseen siten, että se tosiasiallisesti kattaa tieliikenteen liikenteenohjaus- ja hallintapalveluja tarjoavan organisaation. NIS2-lain liitteen 1 mukaista tarkempaa jaottelua ei ole nyt sisällytetty lausuttavana olevan CER-lain liitteeseen. Fintraffic pitää oikeusvarmuuden ja ennakoitavuuden näkökulmasta hankalana tilannetta, jossa CER-lain mukaisen kriittisen toimijan määrittämistä koskevan asian ratkaisee neljän vuoden välein se ministeriö, jonka toimialaan käsiteltävä toimija kuuluu.

Fintraffic pitää tärkeänä, että CER-kriittiseksi nimettäviä toimijoita olisi pidettävä NIS2-lain mukaisessa valvonnassa keskeisinä toimijoina. Tällöin kyseiset toimijat olisivat automaattisesti NIS2-lain mukaisen ennakkovalvonnan piirissä riippumatta niiden koosta.

Lähtökohtaisesti Fintraffic pitää CER-lain mukaista riskiarvioon perustuvaa toimintamallia hyvänä ratkaisuna. Kriittistä infrastruktuuria ja kriittisten toimijoiden häiriönsietokykyä koskevassa kansallisessa strategiassa ja riskiarvioinnissa sekä valvontaviranomaisten toiminnassa tulisi varmistaa, että vaatimukset ovat perusteltuja ja yhteismitallisia yli sektorirajojen ja etteivät kriittiset toimijat ryhdy toteuttamaan tai heiltä vaadita yli/alivarautumista. Kriittisen infrastruktuurin toimijoilta tulisi vaatia samantasoisia turvatoimia sikäli, kun turvattavat intressit ovat samantasoisia. Vähintäänkin olisi huolehdittava siitä, että uhka-arviot tehdään eri sektoreilla samoilla perusteilla samoja uhkia vastaan. Fintraffic näkee Huoltovarmuuskeskuksen merkitykseltään keskeisenä toimijana, jonka toimivaltuudet ja tehtävät tulisi kirjata lakiin yksiselitteisesti.

CER-lain puitteissa toimivien viranomaisten taloudelliset ja henkilöresurssit tulisi mitoittaa riittäviksi. Myös kriittisille toimijoille aiheutuvat hallinnolliset lisätyöt ja siitä aiheutuvat kustannukset tulisi pystyä arvioimaan. Kasuvat kustannukset tulisi ottaa huomioon myös tilanteissa, joissa kriittistä infrastruktuuria ylläpidetään julkisena hallintotehtävänä ja viranomainen/valtio maksaa korvauksen julkisen hallintotehtävän hoitamisesta.

Fintraffic korostaa, että organisaatiot toteuttavat ja tulevat jatkossa toteuttamaan CER- ja NIS2-lakien ohella useita erilaisia riskinarviointiin perustuvia prosesseja ja suojaustoimia erilaisissa viitekehyksissä, kuten erityislainsäädännön mukaiset turvallisuusjohtamisjärjestelmät ja toimintakäsikirjat, tiedonhallintalain mukainen tietoturvan riskinarviointi sekä tekoälyasetuksen mukainen korkean riskin järjestelmien riskinarviointi. Fintraffic pitää tärkeänä, etteivät eri viranomaisten edellyttämät riskinarviointiin liittyvät vaatimukset olisi ristiriitaisia silloin, kun organisaatioon kohdistuu vaatimuksia eri sääntelyn nojalla. Suotavaa olisi, että toteuttamalla esimerkiksi ISO27001 -standardin tai KATAKRI-vaatimusten mukaiset toimet, organisaation voitaisiin lähtökohtaisesti katsoa täyttävän uuden lainsäädännön vaatimukset. Pidemmällä aikavälillä voisi olla syytä tavoitella tilannetta, jossa turvallisuuteen ja riskinarviointiin liittyvät vaatimukset tulisivat "yhden luukun kautta" eli yksi vastuuviranomainen asettaisi sektori/toimialakohtaiset vaatimukset ja valvoisi niiden toteutumista.

Eri liikennemuotojen liikenteen ohjaus- ja hallintapalvelun tarjoajia koskee jo tällä hetkellä erityislainsäädännössä määritellyt varautumisvelvollisuudet (kts. laki liikenteen palveluista 139 §, alusliikennepalvelulaki 19 a §, raideliikennelaki 171 §, ilmailulaki 160 §). Kun tällainen liikenteen toimija tunnustetaan kriittiseksi toimijaksi, velvoitteita seuraisi sekä erityislainsäädännöstä että CER-laista. Esimerkiksi liikenteen erityislainsäädännössä edellytetään valmiussuunnitelmaa, joka sisällöltään vaikuttaa pitkälti samankaltaiselta kuin CER-lain 16 §:n mukainen häiriönsietokykyä koskeva suunnitelma. Lainvalmistelun yhteydessä olisi harkittava, tulisiko erityislain varautumista koskevat lainkohdat kumota siirryttäessä noudattamaan CER-lain mukaisia velvoitteita.

3.

Vaikutustenarviointia koskevat huomiot, kuten esimerkiksi yhteiskunnalliset vaikutukset, taloudelliset vaikutukset yrityksille, hallinnollinen taakka ja muut kustannukset sekä vaikutukset yritysten toimintaan

-

4.

Valvontaa koskevat huomiot

-

5.

Laiminlyöntimaksua koskevat huomiot

-

6.

Miten arvioitte turvallisuusselvityslakia koskevan esityksen tarpeellisuutta ja muotoilua? Millaisia turvallisuusvaikutuksia esityksellä olisi?

-

7.

Miten arvioitte satamien turvallisuusselvityksiä koskevan esityksen tarpeellisuutta ja muotoilua? Millaisia toiminnallisia ja taloudellisia vaikutuksia esityksellä olisi? Millaisia turvallisuusvaikutuksia esityksellä olisi?

-

8.

CER-yleislain 28 §:ään liittyen, miten arvioitte säännösehdotuksia, jotka koskevat muiden EU-jäsenvaltioiden rikosrekisteritietojen käyttämistä kriittisen toimijan työntekijästä tehtävässä turvallisuusselvityksessä (1. lakiesityksen 28§ sekä 3. ja 4. lakiesitys)?

-

9.

Muut huomiot

Kriittisen infrastruktuurin määritelmän osalta HE luonnoksen sivulla 69 esitetään vallitseva asiantila toteamalla, että "Lainsäädännön tasolla ei ole yhteistä menettelykehikkoa, joiden nojalla kriittinen infrastruktuuri määritettäisiin kansallisesti ja EU:n tasolla. Kriittisen infrastruktuurin määritelmän määrittämiseen tulisi kiinnittää erityistä huomiota viimeistään nyt CER-lakia säädettäessä. Myös kriittistä infrastruktuuria koskevan tiedon julkisuuteen ja riittävien salapitoperusteiden määrittämiseen tulisi kiinnittää huomiota julkisuuslain 24 §:n osalta - erityisesti kun julkisuuslain soveltamisalan laajentamista koskeva lainsäädäntöhanke on vireillä.

Fintraffic toteaa, että elintärkeän infrastuktuurin määrittämistä on ohjannut direktiivi (2008/114/EY) Euroopan elintärkeän infrastruktuurin määrittämisestä ja nimeämisestä sekä arvioinnista, joka koskee tarvetta parantaa sen suojaamista, on nyt kumottu CER-direktiivillä. Kumotun direktiivin 2 artiklan määritelmien mukaan 'elintärkeällä infrastruktuurilla' tarkoitetaan sellaisia jäsenvaltioissa sijaitsevia hyödykkeitä ja järjestelmiä tai niiden osia, jotka ovat keskeisiä yhteiskunnan välttämättömien toimintojen, terveydenhuollon, turvallisuuden, turvatoimien sekä väestön taloudellisen ja sosiaalisen hyvinvoinnin ylläpitämiseksi, ja joiden vahingoittumisella tai tuhoutumisella olisi merkittävä vaikutus jäsenvaltioon sen vuoksi, että näitä toimintoja ei kyetä ylläpitämään. 'Elintärkeän infrastruktuurin suojaamiseen liittyvillä arkaluonteisilla tiedoilla' tarkoitetaan elintärkeää infrastruktuuria koskevia tosiseikkoja, joita voitaisiin niiden paljastuttua käyttää sellaisten toimien suunnittelussa ja toteuttamisessa, joiden tarkoituksena on elintärkeiden infrastruktuurijärjestelmien vahingoittuminen tai tuhoutuminen. 'Suojaamisella' tarkoitetaan kaikkia toimia, joilla pyritään varmistamaan elintärkeän infrastruktuurin toimivuus, jatkuvuus ja eheys uhkatekijöiden, riskien tai haavoittuvuuden ehkäisemiseksi, vähentämiseksi ja poistamiseksi.

Myös avoimen datan direktiivissä (EU 2019/1024) on nimenomaisesti tunnistettu tarve elintärkeän infrastruktuurin suojaamiseen:

"(16) Avoimen datan ymmärretään käsitteenä yleensä tarkoittavan avoimissa tietomuodoissa olevaa dataa, jota kuka tahansa voi vapaasti käyttää, uudelleenkäyttää ja jakaa missä tahansa tarkoituksessa. Avoimen datan politiikka, jolla edistetään julkisen sektorin tiedon laajaa saatavuutta ja uudelleenkäyttöä yksityisiin tai kaupallisiin tarkoituksiin siten, että niihin liittyy vain vähän tai ei lainkaan oikeudellisia, teknisiä tai taloudellisia rajoitteita, ja jolla edistetään tiedonvälitystä taloudellisten toimijoiden lisäksi ensisijaisesti kansalaisille, voi merkittävästi edistää yhteiskunnallista osallistumista ja vauhdittaa merkittävästi kyseisen tiedon uudenlaiseen yhdistelyyn ja hyödyntämiseen perustuvien uusien palveluiden kehittämistä. Jäsenvaltioita kehoitetaan näin ollen edistämään tietojen luomista "sisäänrakennetun ja oletusarvoisen avoimuuden" periaatteella kaikkien tämän direktiivin soveltamisalaan kuuluvien asiakirjojen osalta. Näin toimiessaan niiden olisi varmistettava yleistä etua koskevien tavoitteiden, kuten yleisen turvallisuuden, johdonmukainen suojelutaso myös silloin, kun on kyse 'elintärkeän infrastruktuurin suojaamiseen' liittyvistä arkaluonteisista tiedoista. Niiden olisi myös varmistettava henkilötietojen suojeleminen, myös silloin, kun yksittäisessä tietoa-aineistossa oleva tieto ei aiheuta riskiä luonnollisen henkilön tunnistamisesta tai yksilöimisestä mutta kyseinen tieto saattaa yhdistettynä muihin käytettävissä oleviin tietoihin aiheuttaa tällaisen riskin.

(26) Tähän direktiiviin ei sisälly yleistä velvoitetta sallia 'julkisten yritysten' tuottamien asiakirjojen uudelleenkäyttö. Päätös uudelleenkäytön sallimisesta tai kieltämisestä olisi jätettävä asianomaisille julkisille yrityksille, ellei tässä direktiivissä tai unionin oikeudessa tai kansallisessa lainsäädännössä muuta edellytetä. Julkisen yrityksen olisi noudatettava tämän direktiivin III ja IV luvussa säädettyjä asiaa koskevia velvollisuuksia, etenkin esitysmuotojen, maksujen, avoimuuden, lisensien, syrjimättömyyden ja yksinoikeusjärjestelyjen kiellon osalta, vasta sitten, kun se on asettanut asiakirjan saataville uudelleenkäyttöä varten. Julkisten yritysten ei toisaalta pitäisi joutua noudattamaan II luvussa säädettyjä vaatimuksia, kuten pyyntöjen käsittelyyn sovellettavia sääntöjä. Kun asiakirjojen uudelleenkäyttö sallitaan, olisi kiinnitettävä erityistä huomiota neuvoston direktiivissä 2008/114/EY (14) määritellyn 'elintärkeän infrastruktuurin suojaamiseen liittyvien arkaluonteisten tietojen' ja Euroopan parlamentin ja neuvoston direktiivissä (EU) 2016/1148 (15) tarkoitettujen keskeisten palvelujen suojelemiseen."

Fintraffic korostaa myös, ettei julkisuuslain 24 § nykyisellään tunnista elintärkeän/kriittisen infrastruktuurin määritelmää eikä selkeää perustetta elintärkeän infrastruktuurin tai sen suojaamiseen liittyvien arkaluonteisten tietojen salassapidolle. Tämä on erityisen huolestuttavaa, kun samaan aikaan on vireillä lainsäädäntöhanke, joka olisi ulottamassa julkisuuslain soveltamisalaa julkista hallintotehtävää hoitaviin toimijoihin sekä julkisomisteisiin yhtiöihin, joista osa vastaa juuri kriittisen infrastruktuurin ylläpidosta sekä keskisten palveluiden tuottamisesta. Yhtäältä siis pyritään määrittämään toimenpiteitä yhteiskunnan kriittisen infrastruktuurin suojaamiseksi ja häiriönsietokyvyn parantamiseksi, mutta samaan aikaan pyritään lisäämään näiden samojen toimijoiden toiminnan ja asiakirjojen julkisuutta ilman, että kriittistä infrastruktuuria tai keskeisiä palveluita koskevan tiedon salassapidon perusteet varmistetaan.

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

-

Korvenoja Riikka
Liikenteenohjausyhtiö Fintraffic Oy