FiCom ry

Lausunto

03.07.2026

Asia: VN/11135/2026

Kyberturvallisuuslain seuranta ja arviointi

1. Taustatiedot

1.1 Organisaatiotyyppi

Etujärjestö / toimialaliitto / muu edunvalvontatoimija

1.2 Pääasiallinen toimialanne

Digitaalinen infrastruktuuri

1.3 KTL:n mukainen toimijatyyppi

Ei KTL:n soveltamisalaan kuuluva vastaaja

2. Lain soveltaminen ja velvoitteiden selkeys

2.1 Miten ymmärrettävästi riskienhallintaa ja raportointia koskevat velvoitteet on säädetty KTL-laissa?

3

2.2 Kuinka selkeinä pidätte lain velvoitteita organisaationne näkökulmasta?

3

2.3 Arvio viranomaisohjeistuksen riittävyydestä ja selkeydestä

Ohjeistus on riittävää joiltain osin

2.3 Avoin vastaus lain soveltamisesta ja velvoitteiden selkeydestä:

Riskienhallintavelvoitteet ovat pääosin ymmärrettäviä ja perustuvat pitkälti NIS2-direktiivin vähimmäistasoon, mitä FiCom pitää oikeana lähtökohtana. Raportointivelvoitteet ovat kuitenkin paikoin tulkinnanvaraisia, mikä alentaa kokonaisarviota ja lisää tarvetta täsmälliselle viranomaisohjeistukselle.

FiCom ei ole kyberturvallisuuslain mukainen keskeinen tai tärkeä toimija, vaan vastaa kyselyyn jäsenyritystensä ja toimialansa näkökulmasta. FiComin jäsenyrityksiin kuuluu digitaalisen infrastruktuurin ja ICT-palvelujen toimijoita, joilla on jo SVPL 275 §:ään sekä Liikenne- ja viestintäviraston määräykseen perustuvia häiriöilmoitusvelvoitteita. Kyberturvallisuuslain 11 §:n mukainen poikkeamailmoitusvelvoite limittyy näiden kanssa, ja samasta tapahtumasta eri sääntelykokonaisuuksien nojalla tehtävien ilmoitusten suhde on edelleen epäselvä.

Päällekkäisyys tulisi poistaa vähintään siten, että samaa tapahtumaa koskeva yksi ilmoitus täyttää sekä kyberturvallisuuslain että SVPL:n mukaiset ilmoitusvelvoitteet. Toimijan ei tule joutua arvioimaan rinnakkain useita osittain päällekkäisiä ilmoitusreittejä tai toimittamaan samoja tietoja useaan kertaan.

Ilmoitusvelvoitteiden tulkinnanvaraisuus koskee sekä viranomaiselle tehtäviä poikkeamailmoituksia että palvelujen vastaanottajille annettavia ilmoituksia merkittävistä poikkeamista ja merkittävistä kyberuhkista. Kyberturvallisuuskeskuksen ohjeistus ja valvoville viranomaisille laaditut suositukset ovat hyödyllisiä, mutta poikkeamien ja kynnysarvojen määrittelyä tulee edelleen täsmentää yhdessä säänneltyjen toimialojen kanssa.

3. Kyberturvallisuuslain vaikutukset organisaatioonne

3.1 Arvioikaa lain toimeenpanon vaikutuksia: Kyberturvallisuuden tason paraneminen organisaatiossanne

3

3.2 Arvioikaa lain toimeenpanon vaikutuksia: Riskienhallinnan kehittyminen organisaatiossanne

3

3.3 Arvioikaa lain toimeenpanon vaikutuksia: Toimintaan vaikuttavien häiriöiden väheneminen organisaatiossanne

2

3.4 Arvioikaa lain toimeenpanon vaikutuksia: Yhteistyön lisääntyminen viranomaisten kanssa riskienhallinnassa

3

3.5 Arvioikaa lain toimeenpanon vaikutuksia: Kumppanuus- ja toimitusketjuriskien hallinnan parantuminen organisaatiossanne

3

3.6 Kuvaus merkittävistä positiivisista vaikutuksista, joita olette havainneet lain toimeenpanosta

Lain toimeenpano on osaltaan yhdenmukaistanut kyberturvallisuuden perustasoa toimialojen välillä ja EU-tasolla, mikä on tärkeää erityisesti useassa jäsenvaltiossa toimiville yrityksille. Lisäksi riskienhallinta, johdon vastuu sekä toimitusketju- ja kumppanuusriskien tunnistaminen ovat systematisoituneet.

Digitaalisen infrastruktuurin toimijoilla kyberturvallisuuden taso oli kuitenkin jo ennestään korkea SVPL:n tietoturvavelvoitteiden vuoksi. Lain lisävaikutus on siksi suurin toimialoilla, joita aiempi sektorikohtainen sääntely ei kattanut.

3.7 Kuvaus merkittävimmistä haasteista tai kielteisistä vaikutuksista, joita olette havainneet lain toimeenpanosta

Merkittävimmät haasteet liittyvät päällekkäiseen sääntelyyn, raportointiin ja vaatimustenmukaisuuden osoittamiseen. FiComin jäsenyritysten näkökulmasta kyberturvallisuuslain velvoitteet limittyvät erityisesti SVPL:n häiriöilmoitusvelvoitteisiin ja osin muuhun kriittistä infrastruktuuria koskevaan sääntelyyn.

Raportointivelvoitteet ovat paikoin tulkinnanvaraisia ja kuormittavia, ja raportointi voi viedä aikaa poikkeaman tutkimiselta, torjumiselta ja vaikutusten korjaamiselta. Ilmoitusvelvoitteiden tulee olla selkeitä, oikeasuhtaisia ja teknisesti toteuttamiskelpoisia sekä soveltua myös pitkälti automatisoituihin prosesseihin.

3.8 Missä määrin arvioitte, että edellä kuvatut vaikutukset johtuvat nimenomaan KTL-laista?

2

3.8 Avoin vastaus kyberturvallisuuslain vaikutuksista organisaatiossanne

FiComin jäsenyrityksiin kuuluvien digitaalisen infrastruktuurin toimijoiden osalta havaitut vaikutukset johtuvat vain osittain kyberturvallisuuslaista, koska vastaavia tietoturva- ja häiriöilmoitusvelvoitteita on ollut jo SVPL:n nojalla. Aiemmin sääntelemättömillä toimialoilla kyberturvallisuuslain vaikutus voi olla selvästi suurempi.

4. Hallinnollinen taakka ja kustannukset

4.1 Hallinnollisen taakan määrän lisääntyminen organisaatiossanne

4

4.1 Avoin tarkennus:

Hallinnollinen taakka on kasvanut erityisesti päällekkäisten ilmoitus- ja vaatimustenmukaisuusvelvoitteiden vuoksi. Toimijoille on kertynyt raportointivelvoitteita NIS2-direktiivin, kriittistä infrastruktuuria koskevan sääntelyn, SVPL:n ja muun EU-sääntelyn myötä.

Hallitusohjelman tavoite yritysten hallinnollisen taakan kasvun välttämisestä tulee ottaa huomioon myös kyberturvallisuussääntelyn toimeenpanossa ja jatkokehittämisessä. Erityisesti on varmistettava, ettei sama tapahtuma tai vaatimustenmukaisuuden osoittaminen johda useisiin rinnakkaisiin prosesseihin.

4.2 Sääntelyn noudattamisesta aiheutuneiden kustannusten määrä

Merkittävät

4.2 Avoin tarkennus:

Kustannuksia aiheutuu muun muassa riskienhallinnan dokumentoinnista, raportointiprosesseista, auditoinneista ja päällekkäisestä vaatimustenmukaisuuden osoittamisesta. Tarkastuksissa tulisi hyödyntää sertifiointeja, auditointiraportteja ja muita vakiintuneita osoituskeinoja päällekkäisen hallinnollisen taakan välttämiseksi.

Sertifioinnista ei kuitenkaan tule muodostua tosiasiallisesti pakollista ilman vaikutusarviointia ja riskiperusteista tarveharkintaa. Vaatimustenmukaisuuden osoittamisen tulee olla oikeasuhtaista toimijan riskeihin, kokoon ja toiminnan luonteeseen nähden.

4.3 Miten arvioitte KTL-lain soveltamisen aikaista investointien tasoa kyberturvallisuuden kehittämiseen organisaatiossanne?

Kohtalaiset

4.3 Avoin tarkennus:

FiComin jäsenyrityksiin kuuluvat digitaalisen infrastruktuurin toimijat ovat investoineet kyberturvallisuuteen jo aiemmin SVPL:n velvoitteiden nojalla. Sen vuoksi kyberturvallisuuslain soveltamisen aikana tehdyt lisäinvestoinnit ovat näillä toimijoilla olleet pääosin kohtalaisia, vaikka aiemmin sääntelemättömillä toimialoilla investointien taso voi olla korkeampi.

5. Viranomaisyhteistyö ja raportointi

5.1 Poikkeamasta viranomaiselle ilmoittamiseen liittyvän prosessin sujuvuus

3

5.1 Avoin tarkennus:

Poikkeamailmoitusprosessi on pääosin toimiva, mutta päällekkäistä raportointia tulee vähentää. Kyberturvallisuuspoikkeamien ja infrastruktuurin häiriötilanteiden yhteinen sähköinen ilmoituskanava on kannatettava, koska se vähentää päällekkäistä raportointia ja parantaa viranomaisten yhteistä tilannekuvaa. Raportointi on voitava hoitaa yhden sähköisen ilmoituskanavan kautta siten, että toimijan kerran toimittamat tiedot välittyvät tarvittaessa toimivaltaisille viranomaisille myös rajat ylittävissä poikkeamissa ilman erillistä lisäraportointia.

5.2 Ilmoittamista koskevan velvoitteen selkeys ja merkittävän poikkeaman kynnyksen selkeys kyberturvallisuuslaissa

2

5.2 Avoin tarkennus:

Merkittävän poikkeaman kynnys jää edelleen tulkinnanvaraiseksi. Liian laajoja tai matalia kynnysarvoja tulee välttää, jotta raportointi ei vie huomiota poikkeamien torjunnasta. Esimerkiksi käyttäjätuntimittari ei aina kuvaa pilvipalvelun tilapäistä tason laskua tai latenssin kasvua; parempi

arviointitapa olisi painottaa palvelutason alenemista sekä vaikutuksen kohteena olevien asiakkaiden tai tilaajien osuutta.

Merkittävän poikkeaman kriteereissä tulee lisäksi ottaa huomioon komission täytäntöönpanoasetuksen (EU) 2024/2690 mukaiset täsmennykset eräiden toimijatyyppien osalta. Kriteeristö on laadittava tiiviissä yhteistyössä säänneltyjen toimialojen kanssa.

Ennakkovaroituksen 24 tunnin ja poikkeamailmoituksen 72 tunnin määräaikojen vuoksi ilmoituskynnyksen selkeydellä on suuri merkitys. Myös merkittävän kyberuhkan käsite on laaja, eikä siitä ilmene riittävän täsmällisesti, milloin palvelujen vastaanottajille on ilmoitettava ja miten velvoite suhteutuu viranomaiselle tehtäviin ilmoituksiin. Ilmoituskynnyksen epäselvyys voi johtaa varmuuden vuoksi tehtävään raportointiin, mikä heikentää ilmoitusten laatua ja kuormittaa sekä toimijoita että viranomaisia.

5.3 Viranomaisten tuen ja ohjeistuksen hyödyllisyys

4

5.3 Avoin tarkennus:

Kyberturvallisuuskeskuksen tuki ja CERT-toiminto ovat keskeisessä asemassa tilannekuvan ja varoitusten välittämisessä kriittisen infrastruktuurin toimijoille ja viranomaisille. Kyberturvallisuuskeskuksen 24/7-päivystys tulee säilyttää, jotta ympärivuorokautisiin ensi-ilmoituksiin voidaan reagoida ja muita toimijoita voidaan tarvittaessa varoittaa viipymättä.

6. Lain tavoitteiden toteutuminen

6.1 Arvio KTL-lain tavoitteiden toteutumisesta: Kyberturvallisuuden tason nousu organisaatiossanne

3

6.2 Arvio KTL-lain tavoitteiden toteutumisesta: Toimintaan vaikuttavien poikkeamien ennaltaehkäisy organisaatiossanne

3

6.3 Arvio KTL-lain tavoitteiden toteutumisesta: Organisaationne resilienssin paraneminen

3

6.4 Arvio KTL-lain tavoitteiden toteutumisesta: Riskienhallinnan kehitys organisaatiossanne

3

6.5 Arvio KTL-lain tavoitteiden toteutumisesta: Raportoinnin laadun parantuminen organisaatiossanne

3

6.6 Parhaiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumiselle

Parhaiten ovat toteutuneet kyberturvallisuuden perustason yhdenmukaistuminen sekä riskienhallinnan ja johdon vastuun systematisointi. Tämä perustuu NIS2-direktiivin kattavaan sääntelyyn ja siihen, ettei Suomi pääosin asettanut direktiiviä pidemmälle meneviä vaatimuksia. Yhteismitallisuus on erityisen tärkeää useassa jäsenvaltiossa toimiville yrityksille.

Myönteistä on myös se, että kyberturvallisuusvaatimukset ovat aiempaa selkeämmin osa yritysten yleistä riskienhallintaa ja johdon vastuuta, mikä vahvistaa kyberturvallisuuden asemaa liiketoiminnan jatkuvuuden ja resilienssin näkökulmasta.

6.7 Heikoiten toteutuneet tavoitteet ja perustelut tavoitteiden toteutumatta jäämiselle

Heikoiten ovat toteutuneet hallinnollisen taakan hallinta ja päällekkäisen sääntelyn purkaminen. Sektorikohtaista ja horisontaalista sääntelyä ei ole sovitettu yhteen riittävästi, eikä yhden luukun periaate vielä toteudu raportoinnissa kaikilta osin.

FiComin jäsenyritysten näkökulmasta ongelmallista on erityisesti kyberturvallisuuslain ja SVPL:n ilmoitusvelvoitteiden limittyminen. Tavoitteena tulee olla, että samaa tapahtumaa koskeva yksi ilmoitus riittää ja viranomaiset huolehtivat tietojen välittämisestä keskenään.

7. Kyberturvallisuuslain ajantasaisuus, oikeasuhtaisuus ja kehittämistarpeet

7.1 Vastaako laki nykyisiin kyberuhkiin ja teknologiseen kehitykseen?

3

7.2 Onko lainsäädäntöön tarpeen tehdä muutoksia?

Kyllä

7.2 Jos kyllä, miten kehittäisitte sääntelyä?

Sääntelyä tulisi kehittää ensisijaisesti vähentämällä päällekkäisiä ilmoitus- ja vaatimustenmukaisuuden osoittamisvelvoitteita. Kyberturvallisuuslain, SVPL:n häiriöilmoitussääntelyn ja mahdollisten kriittistä infrastruktuuria koskevasta sääntelystä seuraavien velvoitteiden yhteensovittaminen tulee varmistaa niin, ettei sama tapahtuma johda rinnakkaisiin ilmoitusprosesseihin.

Merkittävän poikkeaman ja merkittävän kyberuhkan kynnyksiä tulee täsmentää yhdessä toimialan kanssa. Raportointi tulee järjestää yhden luukun periaatteella myös rajat ylittävissä poikkeamissa, eikä kansallisesti tule asettaa NIS2-direktiiviä pidemmälle meneviä vaatimuksia ilman välttämättömyysperustetta ja vaikutusarviointia.

Lisäksi Liikenne- ja viestintäviraston resurssit sekä Kyberturvallisuuskeskuksen 24/7-päivystys tulee turvata. Tämä on välttämätöntä, jotta uudet valvontatehtävät, CERT-toiminto ja viranomaisten tilannekuvatehtävät voidaan hoitaa asianmukaisesti.

7.3 Minkälaisia KTL:n velvoitteet ovat suhteessa arvioonne toimialanne riskeistä ja organisaationne resursseista?

3

7.3 Avoin vastaus sääntelyn ajantasaisuudesta, oikeasuhtaisudesta ja kehittämistarpeista

Velvoitteet ovat pääosin oikeasuhtaisia, mutta päällekkäisyydet ja tulkinnanvaraisuus heikentävät niiden toteuttamiskelpoisuutta. Sääntelyn tulee olla riskiperusteista ja jättää toimijoille riittävä liikkumavara hallintatoimenpiteiden valinnassa.

Liian yksityiskohtaisia vaatimuksia tulee välttää. Nopeasti muuttuvassa kybertoimintaympäristössä sääntelyn tulisi asettaa tavoitteet ja vähimmäisvaatimukset, mutta jättää keinot mahdollisimman pitkälti toimijoiden riskiperusteisesti valittaviksi.

7.4 Näettekö vaihtoehtoisia sääntely- tai ohjauskeinoja, jotka voisivat toimia paremmin kuin nykyinen malli?

Nykyistä mallia paremmin voisivat toimia ohjauskeinot, joissa vahvistetaan riskiperusteisuutta ja painotetaan ohjeistusta sekä toimialayhteistyötä yksityiskohtaisen normituksen sijaan. Vaatimustenmukaisuuden osoittamisessa tulisi hyödyntää sertifiointeja, auditointiraportteja ja muita vakiintuneita osoituskeinoja ilman, että sertifioinnista muodostuu tosiasiallisesti pakollista.

Viranomaisten ja toimialojen ennakoiva yhteistyö voi vähentää tulkinnanvaraisuutta ja parantaa sääntelyn käytännön toimivuutta. Ohjeistusta tulisi valmistella yhdessä säänneltyjen toimijoiden kanssa, jotta se vastaa erilaisten palvelujen ja toimintaympäristöjen todellisia riskejä.

8. Muut huomiot ja avoin palaute

8.1 Avoin vastaus kyberturvallisuuslakia koskevista huomioista ja havainnoista

Liikenne- ja viestintäviraston ja Kyberturvallisuuskeskuksen resurssit tulee turvata, jotta uudet valvontatehtävät, CERT-toiminto ja muut viranomaistehtävät voidaan hoitaa asianmukaisesti. Erityisen tärkeää on säilyttää Kyberturvallisuuskeskuksen 24/7-päivystys, koska kyberpoikkeamat eivät noudata virka-aikoja.

Tulevat EU-tason muutokset, kuten NIS2-direktiivin mahdolliset muutokset ja kyberturvallisuusasetuksen uudistus, tulee toimeenpanna siten, että kansallinen liikkumavara säilyy eikä kustannuksia tai hallinnollista taakkaa tarpeettomasti lisätä.

EU-tason vaatimusten yhdenmukaisuus on tärkeää erityisesti useassa jäsenvaltiossa toimiville yrityksille, koska se vähentää päällekkäistä sääntelyä ja hallinnollista taakkaa. Sääntelyn kehittämisessä tulee siksi tavoitella EU-tason yhteentoimivuutta ja yhdenmukaisia raportointikäytäntöjä, mutta samalla välttää kansallisia lisävaatimuksia, jotka kasvattaisivat hallinnollista taakkaa ilman osoitettua turvallisuushyötyä.

Hälinen Janne
FiCom ry