

Eduskunnan liikenne- ja viestintävaliokunta

Viite: Asiantuntijalausuntopyyntönne hallituksen esityksestä kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi (HE 179/2025 vp)

1 Esitys

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt Lupa- ja valvontavirastolta lausuntoa hallituksen esityksestä niin kutsutun EU:n kyberkestävyysasetuksen ((EU) 2024/2847, Cyber Resilience Act, CRA) toimeenpanoa koskevaksi lainsäädännöksi.

Kyberkestävyysasetuksella asetetaan kyberturvallisuutta koskevat vähimmäisvaatimukset digitaalisen elementin sisältäville laitteille ja ohjelmistoille, jotka ovat suoraan tai epäsuorasti liitettävissä toiseen laitteeseen tai verkkoon. Asetuksen tavoitteena on varmistaa, että laitteet ja ohjelmistot saatetaan markkinoille nykyistä vähemmän haavoittuvuuksin, valmistajat suhtautuvat tietoturvaan vakavasti tuotteen koko elinkaaren ajan ja käyttäjät voivat ottaa kyberturvallisuutta koskevat ominaisuudet huomioon valitessaan ja käyttäessään tuotteita ja ohjelmistoja.

Kyberkestävyysasetus on suoraan sovellettavaa lainsäädäntöä ja se jättää jäsenvaltion kansalliseen liikkumavaraan vain vaatimustenmukaisuuden arviointilaitoksien ilmoittamista ja markkinavalvonnan järjestämistä koskevien viranomais tehtävien järjestämisen. Nyt käsillä olevan hallituksen esityksen (HE 179/2025 vp) 15 §:n mukaan Liikenne- ja viestintävirasto (Traficom) vastaisi keskitetysti kyberkestävyysasetuksen markkinavalvontaviranomaisen tehtävistä ja 16 §:ssä säädettäisiin, että suuririskisten tekoälyjärjestelmien osalta markkinavalvontaviranomaisena toimisi eräiden tekoälyjärjestelmien valvonnasta annetun lain nojalla toimivaltainen valvova viranomainen.

2 Lupa- ja valvontaviraston lausunto**2.1 Sote-sektorin erityispiirteet kyberkestävyysasetuksen soveltamisessa**

Lupa- ja valvontavirasto kiittää mahdollisuudesta lausua esitysluonnoksesta. Virasto pitää kyberkestävyysasetuksen tavoitteita tärkeinä ja korostaa, että Euroopan laajuisesti digitaalisten elementtien sisältävien laitteiden korkea kyberturvallisuuden tason ja käyttäjien riittävän laiteymmärryksen toteuttaminen edellyttävät markkinoille saatettujen tuotteiden vaatimustenmukaisuuden ohella sitä, että kansallinen tuotevalvonta on aidosti toimivaa ja riittävästi resursoitua.

Lupa- ja valvontavirasto toimii EU:n tekoälyasetuksen (EU 2024/1689) mukaisena julkisissa sosiaali- ja terveydenhuollon palveluissa ja Kansaneläkelaitoksen sosiaalietuuskäsittelyssä käytettävien suuririskisten tekoälyjärjestelmien markkinavalvontaviranomaisena. Tästä seuraa, että Lupa- ja valvontavirastosta on myös toimivaltainen näiden digitaalisten elementtien sisältävien laitteiden ja ohjelmistojen

kyberkestävyyttä koskevia vaatimuksien markkinavalvoja kyberkestävyyssasetuksen nojalla.

Sote-sektorilla markkinoilla jo olevien mutta erityisesti sinne tulossa olevien digitaalisten elementin sisältävien suuririskisten tekoälylaitteiden ja -ohjelmistojen määrä on merkittävä ja kasvaa nopeasti. Muun muassa tekoälyteknologiaa hyödyntävät asiakas- ja potilastietojärjestelmät ja niiden osajärjestelmät, muut tietohallinnon ohjelmistot ja tietoverkkojen komponentit, etähoidon ja digitaalisten palveluiden ratkaisut, sote-ammattilaisten tekoälytyökalut sekä erilaiset verkkoon kytkettävät älynsensoreita hyödyntävät seurantalaitteet muodostavat yhdessä hyvin laajan digitaalisen elementin sisältävän tuotejoukon sote-sektorilla. Näiden tuotteiden määrä ja monimuotoisuus tulevat jatkossa lisääntymään erityisesti hyvinvointialueiden voimakkaan talouden sopeuttamisen, palveluverkoston muutosten ja digitalisaation etenemisen myötä.

Tekoälyn hyödyt ja tavoiteltu käyttö sote-sektorilla perustuvat suurien asiakas- ja potilastietojen käsittelyyn, joka tyypillisesti tapahtuu osittain tai kokonaan rekisterinpitäjän IT-infrastruktuurin ulkopuolella, kuten pilvipalveluissa. Sote-sektorin kyberturvallisuushaavoittuvuuksilla on vakavia seuraamuksia, ja sote-infrastruktuurin häiriöt kohdistuvat usein myös yhteiskunnan haavoittuvimpiin ryhmiin. Yhden tekoälyavusteisen laitteen, ohjelmiston tai sen komponentin haavoittuvuus voi mahdollistaa pääsyn hyvin laajoihin asiakas- ja potilastietoihin. Tekoälyavusteiset diagnostiikka-, hoito- ja seurantajärjestelmät voivat aiheuttaa myös välittömän vaaran ihmishengille ja -terveydelle, jos ne eivät toimi halutulla tavalla. Erityisesti hyvinvointialueen tietoverkkoon ja järjestelmiin kohdistuvat tietoturvaloukkaukset rikkovat usein vakavasti ja hyvin monen asiakkaan- ja potilaan perusoikeuksia. Yhteiskunnallisesti kriittisen sote-sektorin kyberuhkien ja vakavien seuraamusten ehkäiseminen edellyttää reaktiivisten ilmiäntöjen käsittelyn lisäksi proaktiivista ja toimialaa syvällisesti ymmärtävää valvontaa, joka puolestaan edellyttää seuraavassa kappaleessa tarkemmin esitettäviä riittäviä viranomaisresursseja.

2.2 Lupa- ja valvontaviraston resurssitarpeet ja toimintaedellytysten varmistaminen

Kyberkestävyyssasetuksen mukainen markkinavalvonta on Lupa- ja valvontaviraston sote-toimialalla täysin uusi tehtäväkokonaisuus. Lupa- ja valvontaviraston ydinosaaminen on sosiaali- ja terveydenhuollon organisaatioiden ja ammattihenkilöiden lupahallinnossa ja valvonnassa, ei digitaalisten tuotteiden kyberturvallisuuden teknisessä tuotevalvonnassa. Uudet tehtävät vaativat muun muassa teknistä kyberturvallisuusasiantuntemusta, tekoälyjärjestelmien haavoittuvuuksia koskevaa osaamista, alan standardituntemusta, juridista kyberkestävyyssasetuksen osaamista sekä merkittäviä koulutusinvestointeja. Koska kyse on hyvin nopeasti kehittyvistä tekoälyteknologioista ja niiden kyberturvavaatimuksista, valvontaviranomaisen osaamista on jatkuvasti päivitettävä ja samalla ylläpidettävä vuoropuhelua ja yhteistyötä eri toimijoiden ja sidosviranomaisten kanssa. Osaamisen hankkiminen on pitkäkestoinen prosessi, joka on käynnistettävä hyvissä ajoin ennen valvontatehtävien alkamista.

Lupa- ja valvontavirasto arvioi, että kyberkestävyyssasetuksen mukaisten uusien tehtävien asianmukainen hoitaminen edellyttää vähintään 3 htv:n pysyvää lisäresurssia sekä erillisiä vuosittaisia kustannuksia. Tarkka arvio täsmentyy valvontatehtävien käynnistyttyä. Lupa- ja valvontavirasto katsoo, että rahoitus on turvattava valtion

talousarviossa viimeistään vuodesta 2027 alkaen, jolloin kyberkestävyysasetuksen tuotevaatimukset tulevat täysimääräisesti sovellettaviksi.

Resurssitarpeen arvioinnissa on otettava huomioon Lupa- ja valvontaviraston kokonaistilanne. Virastolle on viime vuosina tullut ja lähiaikoina on tulossa useita muita merkittäviä uusia lakisääteisiä tehtäviä (muun muassa EU:n kyberturvallisuusdirektiivi, tekoälyasetus ja eurooppalaista terveystietoaluetta koskeva asetus), joihin ei ole osoitettu lainkaan lisäresursseja. Ilman kyberkestävyysasetuksen vaatimia resursseja Lupa- ja valvontaviraston resurssivaje tuleville vuosille pelkästään sote-digitalisaatioon liittyvien uusien valvontatehtävien vuoksi on 15–20 htv. Lupa- ja valvontavirasto joutuu kattamaan nämä tehtävät nykyisillä vähenevillä resursseillaan, mikä on jo ennestään heikentänyt sen kykyä hoitaa lakisääteisiä tehtäviään.

Esitysluonnoksen mukaan hallitus ei esitä määrärahaa kyberkestävyysasetuksen toimeenpanoon valtion vuoden 2026 talousarviossa, minkä vuoksi asetuksen toimeenpano rahoitettaisiin viranomaisen olemassa olevia resursseja uudelleen kohdentamalla.

Lupa- ja valvontavirasto korostaa, ettei sen nykyisiä kyberturvallisuuslain, sosiaali- ja terveydenhuollon tietojärjestelmien valvonnan ja sosiaali- ja terveystietojen toissijaisesta käytöstä annetun lain mukaisen valvonnan henkilöstöresursseja (5 htv) ole mahdollista käyttää ehdotettavien tehtävien hoitamiseen, vaan ne tulee varata täysimääräisesti nykyisiin lakisääteisiin tehtäviin, jotka nekin tulevat lisääntymään edellä mainittujen EU-tehtävien myötä.

Kyberkestävyysasetuksen mukaisten tehtävien lisääminen Lupa- ja valvontaviraston nykytilanteeseen ilman erillistä rahoitusta ei ole tosiasiallisesti mahdollista tavalla, joka turvaisi sekä uusien että olemassa olevien tehtävien asianmukaisen hoidon. Ilman mitään lisäresursseja virasto joutuisi irrottamaan resursseja jo nykyisinkin kuormittuneesta sote-valvonnasta ja lupahallinnosta, ja kyberkestävyysasetuksen mukaisten vaatimusten valvonta tulisi priorisoida käytännössä vain reaktiiviseen kaikista vakavampien ilmiäntöjen käsittelyyn eli tilanteeseen, kun laitteen tai ohjelmiston haavoittuvuus on jo hyödynnetty ja isot vahingot mahdollisesti syntyneet. Tämän tyyppisellä pistemäisellä ja jälkikäteen tapahtuvalla valvonnalla ei todennäköisesti tule olemaan yksittäistä toimijaa laajempaa vaikuttavuutta tuotesektorilla. Ilman riittäviä resursseja toimialaosaaminen ja ennakollinen valvonta jäävät puuttumaan.

2.3 Puutteellisten viranomaisresurssien vaikutukset

Kyberkestävyysasetuksen tavoitteiden toteutuminen sote-sektorilla edellyttää, että valvontaviranomainen kykenee toimimaan proaktiivisesti ja asiantuntevasti. Tällä on merkittäviä positiivisia vaikutuksia talouden toimijoille.

Digitaalisen elementin sisältävien tuotteiden markkinoille tulo perustuu toimijan suorittamaan itsearviointiin ja vaatimusten toteuttamiseen, mikä edellyttää toimijalta investointeja. Lupa- ja valvontavirasto toteaa, että ilman riittävää valvontaviranomaisen näkyvyyttä, osaamista ja tuotemarkkinoita tehokkaasti läpileikkaavaa markkinavalvontaa on olemassa riski, etteivät kyberkestävyysasetuksen mukaiset tavoitteet, erityisesti turvallisuusnäkökohtien huomioiminen koko tuotteen elinkaaren ajan, toteudu.

Riittävästi resursoitu valvontaviranomainen pystyy tarjoamaan talouden toimijoille ohjausta ja neuvontaa jo ennen kuin tuote saatetaan markkinoille, mikä on erityisen tärkeää pienemmille laite- ja ohjelmistovalmistajille, startup-yrityksille ja pk-yrityksille. Kyberkestävyysasetuksen vaatimukset ovat uusia ja teknisesti monimutkaisia, eikä pienillä yrityksillä ole välttämättä resursseja hankkia kaikkea tarvittavaa juridista ja teknistä osaamista itsenäisesti. Ennakoiva ohjaus vähentää vaatimustenvastaisten tuotteiden riskiä ja siten korjaavista toimenpiteistä aiheutuvia kustannuksia. Toimiva valvonta myös tasoittaa kilpailua, sillä kun vaatimusten noudattamista valvotaan tehokkaasti markkinoilla, yritykset eivät voi saada kilpailuetua jättämällä kyberturvallisuusinvestoinnit tekemättä. Tämä suojaa lainmukaisesti toimivia yrityksiä epäreilulta kilpailulta.

Jos valvontaviranomainen ei saa riittäviä resursseja, vaikutukset talouden toimijoihin ovat merkittäviä ja osin päinvastaiset asetuksen tavoitteisiin nähden. Ilman riittävää ohjausta yritykset jäävät ilman selkeitä tulkintoja, mikä lisää oikeudellista epävarmuutta, hidastaa tuotekehitystä ja kasvattaa hallinnollista taakkaa erityisesti pk-yrityksillä. Heikko valvonta voi johtaa tilanteeseen, jossa osa toimijoista investoi kyberturvallisuuteen kyberkestävyysasetuksen vaatimusten mukaisesti ja osa ei. Tämä luo riskejä tuotteita käytettäessä ja asettaa yrityksiä eri asemaan. Markkinavalvonnan rajautuminen vain reaktiiviseen valvontaan voi johtaa isossa kuvassa siihen, että kyberturvallisuuspuutteita havaitaan vasta vakavien poikkeamien jälkeen. Tämä vahingoittaa sote-alan digitaalisten ratkaisujen mainetta laajemminkin ja heikentää asiakkaiden luottamusta julkisiin palveluihin.

2.4 Viranomaisten välinen yhteistyö

Digitaalisen elementin sisältävien ja verkkoon kytkettävien laitteiden määrä sote-sektorilla on valtava. Kyberkestävyysasetuksen soveltamisalaan kuuluviin talouden toimijoihin sovelletaan myös muita rinnakkaisia ja oletettavasti joiltakin osin päällekkäisiä kyber- ja tietoturvallisuutta koskevia säädöksiä ja vaatimuksia. Kyberkestävyysasetuksen mukaiset vaatimukset ovat vaarassa sekoittua sote-sektorin toimijoilla kyberturvallisuuslain mukaisiin tai sosiaali- ja terveydenhuollon asiakastietojen käsittelystä annetun lain mukaisiin tietojärjestelmien tietoturva vaatimuksiin.

Esitysluonnoksessa ehdotetaan keskitettyä markkinavalvonnan roolia Traficomille sekä hajautettua mallia suuririkisten tekoälyjärjestelmien markkinavalvontaviranomaisten osalta. Toimiva kyberkestävyysasetuksen vaatimusten valvonnan koordinaatio sote-sektorilla edellyttääkin edellä todettu huomioiden selkeitä viranomaisyhteistyön rakenteita erityisesti Traficom (tekninen asiantuntijatuki, haavoittuvuuskoordinaatio) ja tietosuojavaltuutetun (tietosuoja, henkilötietojen käsittely) kanssa, mikä vaatii jatkuvaa viranomaisyhteistyötä ja henkilöstöresursseja.

Lupa- ja valvontavirasto katsoo, että esitysluonnoksen 17 §:n mukainen Traficom harkinnanvarainen tuki ei täytä kyberkestävyysasetuksen 52 artiklan 8 kohdan mukaista vaatimusta riittävästä resursseista. Lupa- ja valvontaviraston näkemyksen mukaan lakiehdotuksen 17 §:n nojalla Traficom pyynnöstä antama asiantuntija-apu soveltuisi parhaiten pykälän yksityiskohtaisissa perusteluissa todetu tavoin vireillä olevassa valvonta-asiassa tarvittavaan teknisempään substanssiosaamiseen ja/tai yhtenäisten arviointiperusteiden noudattamisen varmistamiseen.

Yksittäisen valvonta-asian käsittely on kuitenkin vain osa markkinavalvontaviranomaiselle kuuluvaa laajaa vaatimustenmukaisuuden edistämisen ja valvontatehtäväkokonaisuutta edellä todetuin tavoin. Lupa- ja valvontavirasto pitää ehdotettavan lain 17 §:n mukaista asiantuntija-apua hyvänä lähtökohtana, mutta samalla toteaa, että sillä tulee olla valvonnasta itsenäisesti vastuussa olevana viranomaisena kyvykkyys nykyisessä hajautetussa markkinavalvonnan mallissa luoda, kehittää ja säilyttää oma kyberkestävyyden markkinavalvonnan asiantuntijaorganisaatio ja toimialankohtainen osaaminen.

3 Lisätietojen antaminen

Lisätietoja antaa tarvittaessa johtava asiantuntija Arttu Malava, puh. 0295 254 325.

Osastopäällikkö Satu Koskela

Johtava asiantuntija Arttu Malava

Tämä asiakirja on hyväksytty sähköisesti viimeiseltä sivulta ilmenevin tavoin.

Tämä asiakirja LVV-U/47504/2026 on hyväksytty sähköisesti / Detta dokument LVV-U/47504/2026 har godkänts elektroniskt

Esittelijä Malava Arttu 23.02.2026 09:12

Ratkaisija Koskela Satu 23.02.2026 09:19