

HALLITUKSEN ESITYS KYBERKESTÄVYYSASETUKSEN TOIMEENPANOJA KOSKEVAKSI LAIKSI

HE 179/2025 VP

Asiantuntijalausunto 25.2.2026

Teija Tiilikainen

Johtaja

Euroopan hybridiuhkien torjunnan osaamiskeskus

1. Yleistä

EU:n tasolla säädettyjen kyberturvallisuussäädösten tavoitteet ovat selkeät ja kannatettavat. Digitaaliset järjestelmät ovat mitä suurimmassa määrin rajat ylittäviä rakenteita, joihin sisältyviin haavoittuvuuksiin ja keskinäisriippuvuuksiin voi liittyä EU:n laajuisia turvallisuusriskejä. EU-tasosten standardien ja minimitasojen asettaminen kyberturvallisuudelle on perusteltua.

Kyberkestävyysasetuksen lähtökohtana on kyberturvallisuuteen liittyvä kehitys, jossa laitteet ja ohjelmistot joutuvat enenevässä määrin kyberhyökkäysten kohteeksi. Kyberhyökkäysten taustalla voi olla erilaisia toimijoita ja tarkoituksia, mutta nykyisessä geopoliittisessa ympäristössä niiden taustalta löytyy yhä useammin myös valtiollisia toimijoita. Kyberriskuilla länsimaaisia arvoja ja yhteiskuntajärjestelmiä haastavat valtiot pyrkivät lamauttamaan normaaleja yhteiskunnallisia toimintoja ja prosesseja sekä heikentämään kansalaisten luottamusta hallintoon tai poliittiseen johtoon. Digitaalisiin järjestelmiin kohdistuvilla hyökkäyksillä voidaan toisaalta myös horjuttaa valtioiden talouksia tai rahoitusjärjestelmiä. Ei myöskään ole poissuljettua, että järjestelmistä etsitään merkittäviä haavoittuvuuksia käytettäväksi vakavamman konfliktin tilanteessa. Erilaisia verkkoon kytkettyjä laitteita ja ohjelmistoja voidaan myös käyttää vihamieliseen tiedonkeruuseen ja vakoiluun.

Digitaalisten järjestelmien kattavuuden ja merkityksen huomioiden vaikuttaa perustellulta, että ohjelmistoihin tai järjestelmiin kohdistetaan horisontaalisia turvallisuusvaatimuksia jo ennen niiden tuloa markkinoille. Näillä pyritään vähentämään niihin liittyviä riskejä ja haavoittuvuuksia juuri kyberturvallisuuden näkökulmasta. Kyberkestävyysasetuksen tavoitteena onkin puuttua näihin haasteisiin ja varmistaa, että laitteisto- ja ohjelmistotuotteet 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. Asetuksen yleisenä tavoitteena olevaa digitaalisten järjestelmiin liittyvää turvallisuusriskien ja -haavoittuvuuksien parempaa ymmärrystä sekä siihen liittyvien vastuiden selkeyttämistä voi pitää erinomaisen kannatettavana.

Hallituksen esityksen tarkoituksena on antaa eräiden tuotteiden kyberkestävyyttä koskevan Euroopan unionin asetuksen eli niin kutsutun kyberkestävyyssäädöksen tai -asetuksen soveltamista täydentävät ja täsmentävät kansalliset säännökset. Kyberkestävyyasetus asettaa tietoturvaa koskevat horisontaaliset vähimmäisvaatimukset digitaalisen elementin sisältäville tuotteille eli laitteille ja ohjelmistoille, jotka ovat kytkettävissä internetiin tai toiseen laitteeseen. Ehdotetut säännökset koskevat kyberkestävyyasetuksen markkinavalvontaa, vaatimustenmukaisuuden arviointilaitoksien ilmoittamista ja valvontaa sekä hallinnollisia seuraamuksia. Esitys sisältää kansallista lainsäädäntöä täydentäviä säännöksiä myös kyberturvallisuuden sertifiointijärjestelmiä koskevan EU:n niin kutsutun kyberturvallisuusasetuksen soveltamiseksi. Ehdotetut säännökset koskevat kansallisen kyberturvallisuussertifiointin viranomaisen tehtäviä ja toimivaltuuksia sekä vaatimustenmukaisuuden arviointilaitoksia.

Hallituksen esitystä voidaan tavoitteiltaan - sekä kyberturvallisuuden vahvistamiseksi että eurooppalaisen säätelykehiksen tehokkaaksi kansalliseksi täytäntöönpanoksi - pitää kannatettavana ja esitettyjen lainmuutosten nopeaa voimaantumista toivottavana.

2. Yksityiskohtaisia huomioita

Kuten hallituksen esityksessä todetaan, kyberkestävyyasetusten mukaisten turvallisuusvaatimusten kohteena olevien laitteiden ja ohjelmistojen joukko on hyvin laaja, mikä luo Suomen oloissa uudenlaisen horisontaalisen säätelyn laitteiden valmistajille, maahantuojille tai välittäjille. Liikenne- ja viestintävirasto hoitaisi uutena tehtävänään tuotteiden markkinavalvontaa eli sitä, että markkinoille päässeet digitaaliset laitteet ja ohjelmat täyttävät niille asetetut kyberturvallisuusvaatimukset. Keskitetyn markkinavalvonnan malli on suomalaisissa olosuhteissa katsottu parhaaksi ja kustannustehokkaimmaksi vaihtoehdoksi. Samalle viranomaiselle kuuluisi kyberkestävyyasetuksen vaatima ilmoittavan viranomaisen rooli. Komissiolle annetaan kyberkestävyyasetuksella delegoitua säädösvaltaa pääasiassa tehdä lisäyksiä ja täydennyksiä asetuksen liitteisiin, jotka koskevat säädöksen kohteena olevia tuotteita, tuoteryhmiä tai niihin kohdistettujen vaatimusten yksityiskohtia.

Kyberkestävyysasetuksen tavoitteiden saavuttamisen näkökulmasta hallituksen esityksessä esitettyä kansallista täytäntöönpanotapaa voi pitää harkittuna ja sopivana Suomen olosuhteisiin.

Liikenne- ja viestintäviraston rooli keskeisenä kyberturvallisuuteen liittyvänä valvontaelimenä vahvistuu toisaalta myös sen myötä, että sille kuuluu EU:n kyberturvallisuusasetuksen mukaisen kyberturvallisuussertifiointin viranomaistehtävät. Kyberkestävyysasetuksen voimaantulo muuttaa myös aiemmin vapaaehtoisuuteen perustuvaa kybersertifiointia tekemällä siitä keskeisen välineen, jolla digitaalisten järjestelmien turvallisuusvaatimusten mukaisuus voidaan osoittaa.

Kyberturvallisuusasetuksen kansallisen täytäntöönpanon yhteydessä ei säädetty asetuksen mukaisten uusien kansallisen viranomaistehtävien hoidosta, minkä vuoksi hallituksen esityksessä esitetään näiden tehtävien hoitoon liittyvistä valtuuksista säädettäväksi tässä yhteydessä. Esitys vaikuttaa perustellulta ja tukee kyberkestävyysasetuksen kansallista täytäntöönpanoa.

Eurooppalaisen turvallisuuspoliittisen toimintaympäristön huomioiden digitaalisten järjestelmien turvallisuusriskien tehokkaampi huomioiminen yhtenäisten laatuvaatimusten ja haavoittuvuusarviointien pohjalta, samoin kuin tehokkailla valvontajärjestelmillä, muodostaa keskeisen ja tarkoituksenmukaisen resilienssivälineen. Hybridikeskuksen asiantuntemuksen pohjalta ei ole mahdollista yksityiskohtaisesti arvioida kaikkia kyberkestävyysasetuksen ja kyberturvallisuusasetuksen kansalliseen täytäntöönpanoon liittyviä yksityiskohtaisia ratkaisuja.