25.2.2026

Lausunto HE 179/2025 vp Hallituksen esitykseen eduskunnalle kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi

Kiitämme mahdollisuudesta lausua tästä hallituksen esityksestä eduskunnalle kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi.

Nykyisessä digitalisoituneessa maailmassa on ensiarvoisen tärkeää, että sääntelyä ulotetaan myös koskemaan digitaalisten laitteiden ja palveluiden kyberturvallisuutta. Tämä alue on jo pitkään ollut hyvin vapaa monista sellaisista vastuista, joita perinteisempien laitteiden ja palveluiden kohdalla on vaadittu. Koska yhteiskuntamme on enenevissä määrin riippuvainen digitaalisista palveluista ja laitteista, on näiden sääntely myös perusteltua.

EU:n kyberkestävyysasetus (CRA) on hyvä ensimmäinen askel tämän sääntelyn aloittamiseksi. Tämä hallituksen esitys on kokonaisuutena erittäin hyvin linjassa CRA:n kanssa ja näin ollen myös hyvä ensimmäinen askel kansallisessa sääntelyssä. Kuitenkin on syytä huomata muutamia tärkeitä seikkoja.

Ensinnäkin on tärkeä huomata, että digitaaliset palvelut ja laitteet kehittyvät nopealla tahdilla. Esityksessä ja itse CRA:ssakin mainittu seuranta ja vaikutusten tarkastelu on äärimmäisen tärkeää, mutta sen aikajänne (neljä vuotta) voi olla liian pitkä. Vaikka tällaisten asetusten vaikutuksia pitää arvioida pitkälläkin aikajänteellä, on myös nopeampi tarkastelu ja tarvittaessa reagointi tarpeen. Esimerkkinä voidaan mainita nyt viime aikoina valtavasti yleistynyt tekoälymenetelmien käyttäminen koodin tuottamisessa. Miten tämä esitetty asetus sekä CRA ylipäänsä vaikuttavat toimijoihin, jotka tuottavat avoimen lähdekoodin ohjelmistoja pääosin tekoälyavusteisesti koodaamaalla? Miten asetus suhtautuu tekoälyagentteihin, jotka voivat tällaista koodia tuottaa automaattisesti ja autonomisesti myös muokata kokonaisia avoimen lähdekoodin kirjastoja?

Yleisesti on myös syytä huomata erityisesti avoimen lähdekoodin käytön yleistyminen ja toisaalta tämän kentän suuri monimuotoisuus, jossa osa toimijoista tuottaa ohjelmistoja täysin ilman korvausta ja osa mahdollisesti kaupallisessa mielessä ja korvausta vastaan.

Esityksessä on hyvin huomioitu kyberturvallisuuteen ja haavoittuvuuksiin liittyvät ilmoitusvelvollisuudet ja se, että näitä ilmoituksia voi tulla Kyberturvallisuuskeskukselle useita eri reittejä pitkin. On tärkeää, että

Oulun yliopisto

PL 8000
90014 Oulun yliopisto

oulun.yliopisto @ oulu.fi
Puh 0294 480 000
Fax 08 344 064

www.oulu.fi

Kyberturvallisuuskeskuksella on kyvykkyys ottaa vastaan ilmoituksia myös tähän (tai mihinkään muuhunkaan) asetukseen liittymättömistä tapauksista ja lähteistä, joilla ei ole välttämättä ilmoitusvelvollisuutta. Näin saadaan parhaiten ylläpidettyä hyvää tilannekuvaa kansallisesta ja kansainvälisestä kyberturvallisuuden tilasta. Myös viranomaisten tiedonsaantioikeudet ja niihin tarvittavat muutokset on esityksessä huomioitu hyvin.

Merkittävänä muutoksena yksityisyyden suojaan liittyen on huomattava esityksessä annettavat uudet valtuudet ”kotietsintään” myös markkinavalvontaviranomaisten toimesta. Tämä on kuitenkin esityksessä hyvin perusteltu ja myös rajattu melko onnistuneesti. Pidämme tärkeänä, että esityksessä säilytetään rajaus siitä, että ulkopuolinen asiantuntija ei voi yksin, ilman viranomaista, toteuttaa tällaista etsintää. Ulkopuolisten asiantuntijoiden käyttämistä muissa yhteyksissä voidaan pitää perusteltuna ottaen huomioon CRA:n verrattaen laajan vaikutuspiirin sekä eri alojen kyberturvallisuuden erityispiirteiden huomioimisen tärkeyden.

Lopuksi on erittäin tärkeää pitää mielessä, että vaikka tämän asetuksen myötä useat aiemmin sertifioimattomat laitteet ja palvelut tulevat nyt jonkinasteisen sertifioinnin piiriin, niin 100% turvallisuutta ei tämäkään takaa. Kuitenkin on syytä seurata, että tämä esitetty asetus sekä CRA yleensä tuovat riittäviä kannustimia toimijoille todellisesti parantaa laitteiden ja palveluiden kyberturvallisuutta. Mikäli asetus mahdollistaa sen, että toimijoille riittää toteuttaa ”turvallisuutta” pelkästään paperilla, ilman konkreettisia toimia, jää valtaosa asetuksen hyödyistä saavuttamatta.

Tämän esityksen ehkä suurin heikkous on kuten niin usein, resursointi tai oikeammin sen puute. Esityksessä todetaan erityisesti Kyberturvallisuuskeskuksen vastuiden ja tehtävien kasvavan merkittävästi, mutta samalla todetaan, että nämä tullaan hoitamaan nykyisten budjettiraamien sisällä. On lyhytnäköistä ajatella, että näin merkittävästi uusia tehtäviä ja vastuita tuovaa asetusta voitaisiin valvoa hyvin ilman riittäviä lisäpanostuksia tähän valvontaan. Ja ilman kunnollista valvontaa jää myös suuri osa asetuksen hyödyistä saavuttamatta ja kyberturvallisuus kokonaisuutena ei saa tästä CRA:n tarkoittamaa parannusta. Toivomme siis lisäresursseja sekä tämän asetuksen toimeenpanoon ja valvontaan että kokonaisuutena CRA:n vaikutusten arviointiin.

Oulussa 25.2.2026

Kimmo Halunen

Digitally signed by Kimmo Halunen
DN: cn=Kimmo Halunen, c=FI, o=ITEE, ou=BISG, email=kimmo.halunen@oulu.fi
Reason: I am the author of this document
Date: 2026.02.26 08:54:38 +02'00'

Kimmo Halunen

Kyberturvallisuuden professori

Oulun yliopisto ja Maanpuolustuskorkeakoulu