Teknologiateollisuus

Eduskunta
Liikenne ja viestintävaliokunta
LIV@eduskunta.fi

9.2.2021

Asiantuntijapyyntönne 1.2.2021

Valtioneuvoston selvitys: EU-puheenjohtajamaan keskustelun avaus EU:n tasapainoisesta lähestymistavasta salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksiin saada pääsy salattuun tietoon yksittäistapauksissa toimivaltuuksien puitteissa (E 153/2020 vp)

Finnish Information Security Cluster – Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Kyberala ry kiittää mahdollisuudesta antaa asiantuntijalausuntonsa otsikossa mainitussa asiassa.

EU:n salausta koskeva päätöslauselma on sisällöltään varsin yleisellä tasolla, eikä se sisällä konkreettisia avauksia. Lisäksi se vaikuttaa olevan ristiriidassa muiden EU:n piirissä tehtävien tietoturvallisuutta koskevien aloitteiden kanssa. Päätöslauselmassa esitetty tavoite on kunnianhimoinen ja teknisesti tarkasteltuna hyvin haastava. Perusmuistiossa muotoiltu Suomen kanta asiaan on samansuuntainen. *Kyberala katsoo, että Suomen olisi digitalisaation ja turvallisuuden kärkimaana korostetun tärkeää puolustaa vahvan salausteknologian käyttöä ja mahdollisimman laajaa hyödyntämistä*.

Luotettava salausteknologia on keskeinen osa yhteiskunnan turvallisuutta

Lainvalvontaviranomaisilla tulee olla riittävät valmiudet rikosten torjuntaan ja ennalta ehkäisyyn digitaalisessa ympäristössä. Luotettava salausteknologia on kuitenkin rikostorjuntaa huomattavasti laajempi yhteiskuntaa koskeva turvallisuuskysymys. Koko digitaalisen yhteiskunnan sujuva ja turvallinen toiminta perustuu nykyisin vahvasti luotettavaan salausteknologiaan. Se suojelee kansalaisia kyberrikollisilta, turvaa demokratiaa, yhteiskunnan kriittistä infrastruktuuria ja yrityssalaisuuksia sekä on keskeinen osa kansallista turvallisuutta ja maanpuolustusta.

Tietoturvallisuutta heikentävien ominaisuuksien edellyttäminen on vaarallista

Mahdollinen vaatimus heikkouksien edellyttämisestä yhteiskunnan ja yksilöiden turvallisuutta ja tietosuojaa parantaviin ja suojaaviin järjestelmiin tai laitteisiin on hyvin vaarallinen. Heikkouksen olemassaolo tarkoittaisi, että aina on olemassa riski niiden paljastumiselle ulkomaisille tiedusteluviranomaisille, niiden väärinkäytölle tai tahattomille vahingoille. Joka tapauksessa samaan aikaan on mahdotonta estää rikollisia hyödyntämästä muuta sääntelyn ulottumattomissa olevaa salausteknologiaa.

Teknologiateollisuus ry

Eteläranta 10, PL 10, 00131 Helsinki
Puhelin 09 192 31
www.teknologiateollisuus.fi
Y-tunnus: 0215289-2

Taloudelliset vaikutukset huomattavia

Kyberturvallisuusala on tällä hetkellä globaali kasvuala ja sillä on merkittävä kasvu- ja työllistämispotentiaali Suomessa. *Kyberala korostaa, että tietoturvayrityksille ei tule asettaa vaatimuksia minkäänlaisten heikkouksien (esimerkiksi viranomaistakaporttien) tekemiseen tuotteisiinsa tai palveluihinsa.* Luotettavien tietoturvatuotteiden ja -palveluiden kannalta tällaiset velvoitteet käytännössä romuttaisivat luottamuksen yritysten tuotteisiin ja niiden kilpailukyky markkinoilla katoaisi. Kyberala katsoo, että tämä seikka tulisi huomioida myös Suomen kantaa määriteltäessä.

Tiedon määrän kasvu ja teknologia ovat edistäneet rikostorjunnan tehokkuutta

Tiedon määrän huomattava kasvu ja monet uudet teknologiset ratkaisut ovat viime vuosina parantaneet viranomaisten mahdollisuuksia rikostutkinnassa. Lisäksi viranomaisten kansainvälisen tiedonvaihdon sääntelyä ollaan parhaillaan kehittämässä erilaisin aloittein. Samoin viranomaisten ja yritysten yhteistyö rikostorjunnassa on ensiarvoisen tärkeää.

Rikostorjunnan tehokkuuden parantamiseen on mahdollista kehittää yhdessä ratkaisuja, jotka voidaan toteuttaa ilman muiden perusoikeuksien kohtuutonta vaarantamista ja vahvan salausteknologian käytön rajoittamista. Haasteet digitaalisen todistusaineiston hankkimisessa sekä rikostutkinnassa voidaan ratkaista kestävimmällä tavalla entistä paremmalla yhteistyöllä. Uuden teknologian keinoin voi olla mahdollista kehittää kontrolloituja ja hyväksyttäviä keinoja rikollisten tietoon pääsemiseen. Tehokkaimmin ratkaisua ongelmaan voidaan lähteä etsimään panostamalla aiempaa enemmän uusien rikostutkintakyvykkyyksien tutkimukseen ja kehittämiseen ilman vahvan salausteknologian vaarantamista.