FiCom ry | Asko Metsola
15.2.2021

Lausunto valtioneuvoston selvityksestä EU:n tasapainoisesta lähestymistavasta salaukseen

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt FiComilta lausuntoa valtioneuvoston selvityksestä EU-puheenjohtajamaan keskustelunavauksesta, joka koskee EU:n tasapainoista lähestymistapaa salaukseen sekä toimivaltaisten viranomaisten mahdollisuuksia saada yksittäistapauksissa pääsy salattuun tietoon toimivaltuuksiensa puitteissa. FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

Lokakuussa 2020 Yhdysvallat, Iso-Britannia, Australia, Uusi-Seelanti, Kanada, Intia ja Japani julkaisivat kansainvälisen lausunnon ”End-To-End-salaus ja yleinen turvallisuus”, jossa Intian ja Japanin tukemat Five Eyes -tiedusteluyhteistyöallianssin maat vaativat laillista pääsyä sisältöön luettavassa ja käyttökelpoisessa muodossa. Maat ilmoittivat tukevansa vahvaa salausta, koska sillä on elintärkeä rooli yksityisyydensuojan, tietoturvan, immateriaalioikeuksien, liikesalaisuuksien sekä kyberturvallisuuden varmistamisessa, samoin kuin journalistien, ihmisoikeuksien puolustajien ja haavoittuvassa asemassa olevien kansalaisten suojaamisessa sorretuissa maissa. Jälkimmäinen todetaan myös YK:n ihmisoikeusneuvoston päätöslauselmassa vuodelta 2017. Kaikesta tästä huolimatta maat vaativat samalla teknologiayrityksiä miettimään kanssaan keinoja, joilla mahdollistettaisiin pääsy salattuun sisältöön.

Loppuvuonna 2020 silloinen neuvoston puheenjohtajamaa Saksa peräänkuulutti omassa päätöslauselmassaan ”turvallisuutta salauksen avulla ja salauksesta huolimatta”. Päätöslauselman oksymoron viittaa siihen, että olisi löydettävä tasapaino vahvalla salauksella turvatun sähköisen viestinnän yksityisyyden ja turvallisuuden sekä toimivaltaisten viranomaisten tietoihin pääsyn välillä.

Saksan päätöslauselmassa korostetaan EU:n kannattavan tehokkaan salausteknologian käyttöä turvallisuuden sekä perus- ja ihmisoikeuksien toteutumiseksi, mutta samalla tuodaan esille lainvalvontaviranomaisten ongelmia saada tarvitsemansa tieto salausratkaisujen vuoksi. Päätöslauselman mukaan hallitusten, viranomaisten, teknologiateollisuuden, viestintäpalvelun tarjoajien, korkeakoulujen ja muiden asiaankuuluvien sidosryhmien olisi yhdessä etsittävä teknisiä ratkaisuja salattujen tietojen lailliseen saatavuuteen siten, että ratkaisut noudattaisivat laillisuuden, läpinäkyvyyden, välttämättömyyden ja suhteellisuuden periaatteita sekä ottaisivat oletusarvoisesti huomioon henkilötietojen suojaamisen. Koska asetettujen tavoitteiden saavuttamiseksi ei ole olemassa vain yhtä tapaa, yhteistyö teollisuuden kanssa olisi tarpeellista tasapainon löytämiseksi.

Päätöslauselman edistämiseksi ehdotetuista toimenpiteistä on luotu asiakirja, jonka mukaan eri sääntelykehysten vaikutuksia tulisi tarkastella ja pyrkiä johdonmukaiseen sääntelyyn, joka antaisi toimivaltaisille viranomaisille mahdollisuuden hoitaa operatiiviset tehtävänsä tehokkaasti. Asiakirjassa ei kuitenkaan tarkenneta, mitä sääntelykehykset tai kehitettävät uudet tekniset ratkaisut pitäisivät sisällään. Jatkuvaa tiedonvaihtoa edellä mainitun ”End-To-End-salaus ja yleinen turvallisuus” -lausunnon alullepanijamaiden sekä muiden relevanttien kansainvälisten toimijoiden kanssa pidetään tärkeänä.

FiComin jäsenyhtiöt tekevät jatkuvasti yhteistyötä lainvalvontaviranomaisten kanssa, jotta internet olisi turvallisempi niin yrityksille kuin yksityishenkilöille. Samalla FiCom kuitenkin tukee vahvaa salausta, jolla demokraattisessa yhteiskunnassa on keskeinen rooli kyberturvallisuuden ja käyttäjien yksityisyyden varmistamisessa.

Saksan päätöslauselmasta ei käy ilmi, mihin toimijoihin suunnitellut toimet kohdistuisivat. Suomen kannassa todetaan, että merkittävä osa viestinnästä tapahtuu teleyrityksistä riippumattomien toimijoiden alustoilla (ns. OTT-alustat), mutta tämä ei tarkoita, etteivätkö mahdolliset lainsäädäntöehdotukset voisi kohdistua myös teleyrityksiin.

Viestintäpalveluiden end-to-end-salaus sekä TLS:n (Transport Layer Security) ja HTTPS:n (Hypertext Transfer Protocol Secure) kaltaiset salausprotokollat ovat välttämättömiä, jotta internetiin voi luottaa. Nyt ehdotettujen toimien tarkoituksena on jättää salaukseen takaportti ja antaa lainvalvontaviranomaisille pääsy yksityiseen viestintään. Kansainväliset kokemukset ovat osoittaneet, että pahantahtoiset hakkerit käyttävät aina hyväkseen tällaisia toimenpiteitä, mikä heikentää sekä kyberturvallisuutta että käyttäjien ja yritysten yksityisyydensuojaa verkossa. Tämä puolestaan heikentäisi luottamusta internetiin ja voisi hidastaa verkkopalveluiden käyttöönottoa EU:ssa. Valtioneuvoston selvityksessä tai Saksan päätöslauselmassa ei ole tehty lainkaan elinkeinopoliittista vaikutusarviointia, vaan keskitytty ainoastaan viranomaistoimintaan kohdistuviin vaikutuksiin.

Operaattorit ovat valmiita tekemään yhteistyötä lainvalvontaviranomaisten kanssa jatkossakin, mutta verkkosisällön salauksen yhteiskunnallinen etu ja sen rikkomisen kielteiset vaikutukset ovat niin merkittäviä, että FiCom vastustaa pakollisten, unionin oikeuteen perustuvien viranomaistakaporttien käyttöönottoa. Mikäli sellaisia edes harkitaan, tulee palveluntarjoajien sijaintivaltioiden kansallisten viranomaisten arvioida riittävän tarkkarajaisten ja oikeasuhtaisten toimien lainmukaisuus. Lähestymistavan tulee olla tasapainoinen ja teknologianeutraali, ja siinä on otettava huomioon yksityisyydensuoja sekä tietosuoja. Viestinnän luottamuksellisuus on turvattava kaikissa olosuhteissa.