FiCom ry | Asko Metsola
22.4.2025

FiComin lausunto lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnan jatkokirjelmästä

Eduskunnan suuri valiokunta on pyytänyt FiComilta lausuntoa valtioneuvoston kirjelmään Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final) liittyvästä jatkokirjelmästä UJ 2/2025 vp. FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- Numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajien vapaaehtoiset toimet CSA-materiaalin tunnistamiseksi tulee kompromissitekstissä ehdotetun mukaisesti mahdollistaa.
- On hyvä, että tunnistamismääräyksistä on kompromissiehdotuksessa luovuttu, mutta tavoite viestintäsalaisuuden murtamiseksi sisältyy komission uuteen ProtectEU-strategiaan.

FiComin jäsenkunta ja koko ICT-ala on sitoutunut ehkäisemään ja torjumaan lapsiin kohdistuvaa seksuaalista väkivaltaa. Tämän osoittavat mm. teleyritysten lain 1068/2006 nojalla yhteistyössä Keskusrikospoliisin suorittamat aktiiviset, vapaaehtoiset toimet alaikäisiin kohdistuvan seksuaalisen väkivallan ehkäisemiseksi sekä toimialan yhteiset hankkeet lapsiin kohdistuvaa verkkorikollisuutta vastaan. Esimerkiksi verkkoalustojen käyttäjiä kannustetaan ilmoittamaan laittomaksi epäiltyjä verkkosisältöjä tai -toimintaa poliisille tai Pelastakaa Lapset -järjestön Nettivihje-palveluun. FiCom on mukana kansainvälisen Safer Internet Day -kampanjan osana järjestettävässä Mediataitoviikossa, tukee aktiivisesti Suojellaan Lapsia ry:n Turvallisesti digiliikenteessä -kampanjaa sekä kokoaa säännöllisesti yhteen jäsenyritystensä asiantuntijoita ratkomaan lasten verkkoturvallisuuteen liittyviä haasteita.

Kuten jatkokirjelmässäkin todetaan, asetusehdotus on kehittynyt monilta osin Suomen neuvottelutavoitteiden mukaiseen suuntaan. Aiempien esitysten kaltaisesta tunnistamismääräyksestä on luovuttu, ja siihen suoraan kytkeytyvät artiklat (7–11 artiklat) on poistettu. Tämä on erittäin tervetullut muutos. Puheenjohtajamaa Puolan kompromissitekstiehdotukseen on kuitenkin sisällytetty lauseke (85 artikla), jonka perusteella komissiota kehotetaan arvioimaan kolmen vuoden kuluessa asetuksen voimaantulosta, olisiko velvoittavalle tunnistamismääräykselle olemassa teknologiset ja oikeudelliset edellytykset.

FiCom pitää valtioneuvoston tavoin kannatettavana ehdotusta, jolla asetuksessa vakiinnutettaisiin numeroista riippumattomien viestintäpalvelun tarjoajien (esim. Facebook Messenger) vapaaehtoista tunnistamista koskeva, tällä hetkellä tilapäinen sääntely palveluissa välitetyn CSA-materiaalin tai siellä tapahtuvan groomingin havaitsemiseksi ja siitä ilmoittamiseksi ja kyseisen materiaalin poistamiseksi. Ehdotettu säännös tuo tarpeellista oikeusvarmuutta vakiintuneiden toimien jatkamiseksi, mutta siinä säädettäisiin samalla tilapäistä poikkeusasetusta tarkemmin yritysten vapaaehtoisista toimista CSA-materiaalin tunnistamiseksi. Palveluntarjoajien olisi esimerkiksi varmistettava, etteivät heidän vapaaehtoiset CSA-materiaalin tunnistustoimenpiteensä luo hallitsemattomia riskejä kyberturvallisuudelle, ja

palveluntarjoajien olisi mm. pidettävä yksityiskohtaisia lokitietoja toiminnoistaan sisäistä ja ulkoista tarkastelua varten sekä mahdollista rikosoikeudellista menettelyä varten. Ehdotetulla muotoiluilla vapaaehtoisista toimista asetuksella ei kielletä, kierretä tai muutoin heikennetä kyberturvallisuustoimenpiteitä eikä luoda velvoitteita purkaa päästä päähän -salausta tai rajoittaa sen käyttöä.

Jatkokirjelmän mukaan puheenjohtajamaa Puolan kompromissiehdotus sisältää sellaisia tilapäisestä asetuksesta siirrettyjä palveluntarjoajia koskevia raportointivelvoitteita, joilla voi olla lisätyövaikutusta tietosuojan valvontaviranomaisille. Merkittävimmät vaikutukset kuitenkin kohdistuvat niihin jäsenvaltioihin, joihin palveluntarjoajat ovat sijoittautuneet, ja alustavan arvion mukaan vaikutukset Suomessa olisivat vähäisiä. FiComin mielestä jatkoneuvotteluissa täytyy kuitenkin pitää huoli, että raportointivelvoitteet eivät paisu liiaksi ja että viranomaisille raportoidaan vain sellaista tietoa, jota myös aidosti käytetään johonkin.

Viestintäsalaisuuden murtaminen siirretty osaksi ProtectEU-strategiaa

Vaikka Puolan kompromissitekstistä ei suoraan seuraa velvoitteita, jotka voisivat tosiasiassa johtaa viestinnän päästä päähän -salauksen käytön tarkoituksen kiertämiseen, taustalla vaikuttaa lainvalvontaviranomaisten pitkäaikainen tavoite murtaa viestintäsalaisuus. Europol ja kaikkien jäsenmaiden lainvalvontaviranomaisten johtajat julkaisivat huhtikuussa 2024 yhteisen julistuksen, jonka mukaan tavoitteena on käytännössä murtaa salaus kaikelta viestinnältä kaikkea tutkintaa varten.

Tammikuussa 2023 EU:n epävirallinen oikeus- ja sisäministerikokous antoi tukensa tuolloisen puheenjohtajamaa Ruotsin esitykselle perustaa uusi foorumi, jossa jäsenvaltiot yhdessä eri intressitahojen kanssa selvittävät keinoja taata oikeus- ja lainvalvontaviranomaisten pääsy digitaalisessa ympäristössä olevaan tietoon. Aloitetta tukemaan perustettu korkean tason asiantuntijaryhmä käynnisti työnsä toteamalla suurimmaksi haasteeksi salauksen, joka estää pääsyn tallennettuun sisältöön ja digitaaliseen viestintädataan. Asiantuntijaryhmää on arvosteltu salailusta ja kokoonpanostaan, josta on jätetty osa sidosryhmistä kokonaan ulkopuolelle. Asiantuntijaryhmän loppuraportissa suositellaan useita toimia, jotka voivat heikentää salausta.

Euroopan komissio julkaisi 8.4.2025 uuden EU:n sisäisen turvallisuuden ProtectEU-strategian, joka pyrkii vahvistamaan jäsenvaltioiden kykyä turvata kansalaisiaan muuttuvassa turvallisuusympäristössä. Osana strategiaa komissio on kertonut esittävänsä vuoden 2025 ensimmäisellä puoliskolla tiekartan, jossa esitetään oikeudelliset ja käytännön toimenpiteet laillisen ja tehokkaan tietojen saannin varmistamiseksi. Tiekartan seurannassa komissio asettaa etusijalle tietojen säilyttämistä koskevien sääntöjen vaikutusten arvioinnin EU:n tasolla ja salaukseen liittyvän teknologiatiekartaston valmistelun, jotta voidaan tunnistaa ja arvioida teknologisia ratkaisuja, jotka mahdollistavat lainvalvontaviranomaisten pääsyn salattuihin tietoihin laillisesti, kyberturvallisuutta ja perusoikeuksia suojellen (”*In the follow-up to this Roadmap, the Commission will prioritise an assessment of the impact of data retention rules at EU level and the preparation of a Technology Roadmap on encryption, to identify and assess technological solutions that would enable law enforcement authorities to access encrypted data in a lawful manner, safeguarding cybersecurity and fundamental rights*”).

Suuren valiokunnan, eduskunnan sekä valtioneuvoston on hyvä seurata ProtectEU:n strategiaan sisältyvän salauksesta sekä tietojen säilyttämisestä laadittavan tiekartan valmistelua, pitäen mielessä salauksen murtamisesta aiemmin lausumansa.