FiCom ry | Janne Hälinen
8.9.2025

FiComin lausunto lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnan jatkokirjelmästä

Eduskunnan hallintovaliokunta 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 20/2025 vp. FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- **Tanskan kompromissiesitys palauttaa asetukseen aiemmin kritisoidun tunnistamismääräys-järjestelmän. Vaikka teksti sisältää uusia rajauksia ja suojatoimia, kokonaisuus on edelleen perusoikeuksien ja luottamuksellisen viestinnän kannalta ongelmallinen.**
- **FiCom yhtyy valtioneuvoston kantaan, jonka mukaan Suomi ei voi tukea ehdotettua kompromissia perustuslain kannalta ongelmalliseksi todetun tunnistamismääräyksen vuoksi.**
- **Kaikkiin kansalaisiin kohdistuvat tunnistamismääräykset johtaisivat käytännössä laajaan ennakkovalvontaan, rapauttaisivat viestinnän luottamuksellisuutta ja heikentäisivät tosiasiallisesti viestiliikenteen salausta.**
- **FiCom kannattaa edelleen mallia, jossa vapaaehtoinen tunnistaminen numeroista riippumattomissa viestintäpalveluissa tuodaan selkeään, pysyvään sääntelykehykseen ilman yleisvalvontaa ja ilman salauksen heikentämistä.**

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 kanssa 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. Lisäksi 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 paluu Puolan kompromissiehdotusta edeltävään Unkarin ehdotukseen. **Aiempien esitysten kaltaiseen tunnistamismääräykseen on siis palattu** ja siihen suoraan kytkeytyvät artiklat 7–11 palautettu. FiCom yhtyy valtioneuvoston kantaan, ettei Suomi voi tukea ehdotettua kompromissia edellä mainitun perustuslain kannalta ongelmalliseksi todetun tunnistamismääräyksen vuoksi.

FiCom pitää edelleen **kannatettavana aiempaa 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, siitä ilmoittamiseksi ja kyseisen materiaalin poistamiseksi. Puolan kompromissiesitykseen sisältynyt ehdotus säännökseksi toisi 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. Palveluntarjoajien olisi myös mm. pidettävä yksityiskohtaisia lokitietoja toiminnoistaan sisäistä ja ulkoista tarkastelua sekä mahdollista rikosoikeudellista menettelyä varten. Asetuksessa on todettava yksiselitteisesti, että vapaaehtoiset toimet eivät kiellä, kierrä tai heikennä kyberturvallisuustoimenpiteitä eivätkä luo velvoitetta purkaa tai rajoittaa päästä päähän -salauksen käyttöä.

Tarkentavat huomiot Tanskan kompromissiehdotuksesta

Tunnistamismääräysten soveltamisala kattaisi tunnetun ja uuden CSA-materiaalin; ns. grooming rajataan ulkopuolelle, ja sitä arvioidaan erikseen kolmen vuoden kuluessa. Tunnistaminen on rajattu visuaaliseen sisältöön ja URL-osoitteisiin. Teksti ja ääni jäävät rajauksen ulkopuolelle. Päästä päähän salatuissa palveluissa tunnistaminen tapahtuisi lähetystä edeltävästi käyttäjän suostumuksella. Tunnistamisteknologiat on ennakkovarmennettava ja hyväksyttävä täytäntöönpanosäädöksellä, ja palveluntarjoajille asetetaan lokitusvelvoite. Nämä täsmennykset eivät poista perusongelmaa: järjestely johtaisi tosiasiassa laajamittaiseen ennakkoskannaukseen ja loisi merkittäviä perusoikeus- ja kyberturvariskejä.

FiCom pyytää myös kiinnittämään huomiota siihen, että kompromissiesityksessä tunnistamismääräyksiä ei sovelleta valtion tileihin, joita käytetään kansallisen turvallisuuden, yleisen järjestyksen ylläpidon tai sotilaallisiin tarkoituksiin. Tämä ehdotettu poikkeus osoittaa, että vaadittuihin skannausratkaisuihin liittyy tunnistettuja turvallisuusriskejä juuri korkean suojaustason ympäristöissä. Samat riskit heijastuvat myös siviilikäyttöön, **mikä korostaa tarvetta välttää ratkaisuja, jotka tosiasiallisesti heikentävät salauksen luottamuksellisuutta tai johtavat massaskannaukseen.**

Puolan kompromissiehdotuksen tavoin Tanskan ehdotus 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.**

Lisäksi FiCom kiinnittää huomiota siihen, että ehdotus toisi osalle palveluntarjoajista velvollisuuden osallistua lapseen kohdistuvaa seksuaaliväkivaltaa todistavan uuden kuvamateriaalin ja groomingin havaitsemiseen tarkoitetun teknologian jatkokehittämiseen tekemällä yhteistyötä EU-keskuksen kanssa. Osallistumisen olisi oltava oikeassa suhteessa palveluntarjoajan taloudellisiin, teknisiin ja operatiivisiin valmiuksiin.

Tanskan ehdotuksen mukaan uutta asetusta sovelletaan 24 kuukauden kuluttua sen voimaantulosta, mutta havaitsemismääräykset vasta 48 kuukauden kuluttua. Tilapäisen asetuksen voimassaoloa jatketaan jopa 72 kuukauteen, jotta vapaaehtoinen havaitseminen voi jatkua siirtymäkautena. FiComin näkemyksen mukaan

tämä korostaa tarvetta yhtenäisille EU-tason teknisille määrittelyille ja raportointikaavoille, jotta päällekkäisiä velvoitteita tai ristiriitoja ei synny.

Viestintäsalaisuuden murtaminen siirretty osaksi ProtectEU-strategiaa

Vaikka Tanskan kompromissitekstistä ei suoraan seuraa velvoitteita, jotka voisivat tosiasiassa johtaa viestinnän päästä päähän -salauksen 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*”).

Hallintovaliokunnan, eduskunnan sekä valtioneuvoston on syytä seurata ProtectEU:n strategiaan sisältyvän salauksesta sekä tietojen säilyttämisestä laadittavan tiekartan valmistelua ja pitää mielessä salauksen murtamisesta aiemmin lausumansa.

FiCom ry

Janne Hälinen
juristi