

## FiComin lausunto lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnan jatkokirjelmästä

FiCom kiittää valiokuntaa mahdollisuudesta tulla kuulluksi ja pyynnöstä lausua 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 31/2025 vp.

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.

### FiComin keskeiset viestit

- **FiCom pitää hyvänä, että aiempiin kompromissiesityksiin sisältyneistä pakollisista tunnistamismääräyksistä on viimeisimmässä kompromissiesityksessä luovuttu. Ratkaisu, jossa vapaaehtoiset tunnistamistoimet vakinaistetaan, on oikea.**
- **Vaikka pakollisesta tunnistamismääräyksestä on luovuttu, jättää ehdotus oven auki sen palauttamiselle tulevaisuudessa. Suomen tulee linjata, ettei pakollisia tunnistamismääräyksiä tuoda takaisin missään muodossa.**
- **Vastuita sisällöistä ei tule siirtää teleoperaattoreille, eikä palveluntarjoajilta tule edellyttää päästä päähän -salauksen heikentäviä ratkaisuja tai keskeneräisten teknologioiden käyttöönottoa.**

### Tunnistamismääräykset ja vapaaehtoisuus

FiCom pitää valtioneuvoston tavoin hyvänä, että aiempien esitysten kaltaisesta tunnistamismääräyksestä on luovuttu ja siihen suoraan kytkeytyvät artikkelit 7–11 poistettu. FiCom yhtyy valtioneuvoston kantaan, jonka mukaan on kannatettavaa vakiinnuttaa sääntely, joka mahdollistaa numeroista riippumattomien viestintäpalvelujen (esimerkiksi Facebook Messengerin) vapaaehtoisen tunnistamisen palveluissa välitetyn CSA-materiaalin tai groomingin havaitsemiseksi, ilmoittamiseksi ja poistamiseksi.

Niin ikään FiCom korostaa valtioneuvoston tavoin, että jatkovalmistelussa on edelleen varmistettava, että vapaaehtoiselle tunnistamiselle asetetaan riittävät suojakeinot väärinkäytöksiä vastaan. Ehdotukseen sisältyy nimenomainen säännös, jonka mukaan asetus ei saa kieltää, tehdä mahdottomaksi, heikentää tai kiertää kyberturvallisuustoimenpiteitä eikä luoda velvoitetta purkaa tai rajoittaa päästä päähän -salauksen käyttöä; tämä linja on säilytettävä muuttumattomana.

FiCom pitää huolestuttavana, että ehdotukseen on edelleen sisällytetty mahdollisuus ottaa pakolliset tunnistamismääräykset takaisin. Ehdotuksen 85 artiklan mukaan komissio tekee viiden vuoden välein kokonaisarvion asetuksen toimivuudesta, ja lisäksi kolmen vuoden kuluessa laaditaan erillinen, näyttöön perustuva teknologia-arvio (johdantokappale 77 a), jossa tarkastellaan mm. käytettävissä olevien teknologioiden luotettavuutta. **Suomen tulee linjata, ettei pakollisia tunnistamismääräyksiä tuoda takaisin missään muodossa**, vaan pidättäytyä tiukasti vapaaehtoisuuteen pohjautuvassa mallissa ja varmistaa, että perusoikeudet ja kyberturvallisuus eivät vaarannu. Minkäänlaisia takaportteja tähän ei tule jättää auki.

## **Muut huomiot Tanskan ehdotuksesta**

Tanskan ehdotus sisältää sellaisia tilapäisestä asetuksesta siirrettyjä palveluntarjoajia koskevia raportointivelvoitteita, joilla voi olla lisäyövaikutusta tietosuojan valvontaviranomaisille. Merkittävimmät vaikutukset kuitenkin kohdistuvat niihin jäsenvaltioihin, joihin palveluntarjoajat ovat sijoittautuneet, ja alustavan arvion mukaan vaikutukset Suomessa olisivat vähäisiä. FiComin mielestä **jatkoneuvotteluissa on varmistettava, että raportointivelvoitteita ei laajenneta tarpeettomasti ja että viranomaisille raportoidaan vain sellaista tietoa, jota myös aidosti käytetään johonkin.**

Lisäksi FiCom kiinnittää huomiota siihen, että puheenjohtajamaan tekstissä korkean riskin palveluntarjoajille voidaan asettaa velvollisuus osallistua EU-keskuksen kanssa sellaisten tunnistusteknologioiden jatkokehittämiseen, joilla pienennetään jäljellä olevaa riskiä. Velvoitteen on oltava kohdennettu ja oikeasuhtainen sekä nimenomaisesti suhteessa palveluntarjoajan taloudellisiin, teknisiin ja operatiivisiin valmiuksiin. **Velvoitetta ei tule tulkita siten, että se siirtäisi vastuuta teleoperaattoreille, joilla ei ole mahdollista vaikuttaa sisältöihin, tai edellyttäisi päästä päähän -salauksen heikentäviä ratkaisuja tai keskeneräisten teknologioiden käyttöönottoa.**

Kokonaisuuteen sisältyvät poistomääräykset ja delisting-päätökset on sovitettava täsmällisesti yhteen DSA- ja TERREG-menettelyjen kanssa, jotta päällekkäisyys ja ristiriitaiset määräajat vältetään. FiCom pitää ongelmallisena mallia, jossa rajat ylittävien päätösten tuomioistuINVALVONTA tapahtuisi yksinomaan palveluntarjoajan sijoittautumisvaltiossa; oikeussuojan on oltava aidosti käytettävissä myös vahinkovaltion toimijoille. Päätösten on oltava tarkasti kohdennettuja, maantieteellisesti ja ajallisesti rajoitettuja, oikeassa suhteessa tavoiteltuun päämäärään nähden, ja niihin on liityttävä selkeät ilmoitus- ja muutoksenhakukeinot sekä palvelulle että sisällön alkuperäiselle julkaisijalle. Lisäksi tarvitaan yhdenmukaisia lomakkeita ja aikarajoja, jotta toimeenpano on ennakoitavaa eikä luo kohtuutonta hallinnollista taakkaa.

## **Viestintäsalaisuuden murtaminen siirretty osaksi ProtectEU-strategiaa**

Vaikka Tanskan viimeisimmässä kompromissitekstissä on luovuttu määräyksistä, jotka voisivat tosiasiallisesti 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 1.4.2025 uuden EU:n sisäisen turvallisuuden ProtectEU-strategian, joka pyrkii vahvistamaan jäsenvaltioiden kykyä turvata kansalaisiaan muuttuvassa turvallisuusympäristössä. Osana strategiaa komissio esitteli 24.6.2025 [tiekartan](#), jossa vuodelle 2025 asetetaan prioriteetiksi EU-tasoisien tietojen säilyttämistä koskevan sääntelyn vaikutustenarviointi sekä salauksen teknologiatiekartan valmistelu. Teknologiatiekartan on määrä valmistua vuoden 2026 toisella neljänneksellä, ja sen tarkoituksena on tunnistaa ja arvioida ratkaisuja, jotka mahdollistavat lainmukaisen pääsyn salattuihin tietoihin kyberturvallisuutta ja perusoikeuksia suojellen. **Eduskunnan ja valtioneuvoston on syytä seurata tiekartan toimeenpanoa ja pitää kiinni linjauksesta, ettei salauksen heikentämiseen tai yleisvalvontaan johtavia ratkaisuja hyväksytä.**

**FiCom ry**

Janne Hälinen  
juristi