15.10.2024

Liikenne- ja viestintävaliokunta

Elisa Oyj:n lausunto lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnasta

Viite: U 69/2022 vp / Lausuntopyyntö

Eduskunnan Liikenne- ja viestintävaliokunta on pyytänyt Elisa Oyj:ltä kirjallista lausuntoa valtioneuvoston kirjelmästä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final).

Elisa Oyj kiittää mahdollisuudesta tulla kuulluksi asiassa ja lausuu kunnioittaen seuraavaa

Elisa Oyj:n keskeiset viestit käsillä olevaan esitykseen liittyen

- Ehdotettu viestinnän seuranta ja CSA-materiaalin tunnistaminen kohdistuu laajaan, kohdentamattomaan joukkoon palveluiden käyttäjiä
- Ehdotettu tunnistamisteknologia on kierrettävissä
- CSA-materiaalin tunnistamiseen toteutettu järjestelmä mahdollistaa myös muun, esim. poliittisia kantoja kuvaavien viestien tunnistamisen
- Päätelaiteisiin ja viestintäsovelluksiin esitettyjä toimia ei tulisi vaatia
- Kansalaisten luottamus digitaalisten palveluiden turvallisuuteen ja luottamuksellisuuteen on varmistettava
- Elisa Oyj yhtyy Ficom ry:n lausuntoon kokonaisuudessaan.

Yleistä

Elisa Oyj, kuten muutkin toimialan yritykset ja järjestöt, on sitoutunut ehkäisemään ja torjumaan lapsiin kohdistuvaa seksuaalista välivaltaa. Elisa Oyj toimii mm. vapaaehtoisessa yhteistyössä Keskusrikospoliisin ja Pelastakaa Lapset ry:n kanssa lapsiin kohdistuvan seksuaalisen väkivallan ehkäisemiseksi. Asetuksen kohteena olevan seksuaalista hyväksikäyttöä koskevan CSA-materiaalin tuottaminen ja jakelu on ymmärtääksemme usein organisoitua ja ammattimaista rikollista toimintaa.

Lainsäädännön ja toiminnan kehittäminen lasten seksuaalisen hyväksikäytön ehkäisemiseksi ja lasten suojaamiseksi on hyvin tarpeellista. Kannatamme esitystä pois lukien tässä ja Ficom ry:n lausunnossa esitetyt CSA-materiaalin tunnistamiseen liittyvät haasteelliset toimet.

Olemme huolissamme käsillä olevan EU puheenjohtajamaa Unkarin ehdotuksen sisältämistä, suhteellisen helposti kierrettävistä ja viestinnän luottamuksellisuutta ja sananvapautta merkittävästi uhkaavista menettelyistä.

Näkemyksemme mukaan esitettyjä, ongelmallisia menettelyitä ei tulisi hyväksyä.

Esityksessä viestinnän seuranta ja CSA-materiaalin tunnistaminen kohdistuu laajaan, kohdentamattomaan joukkoon palveluiden käyttäjiä

Nyt käsillä olevassa esityksessä on, että kaikissa henkilöiden välisissä viestintäpalveluissa (”all interpersonal communications services”) tulisi ottaa käyttöön järjestelmä, joissa viestintäpalveluiden käyttäjät antavat suostumuksensa kaiken palveluihin lisäämänsä sisällön tarkistamiseen. Videoiden, kuvien tai linkkien lähettäminen palveluissa ei olisi mahdollista ilman em. seurannan hyväksyntää.

Ehdotus jättää avoimeksi seurannan toteutustavan. Lisäksi ehdotuksessa osin odotetaan tarvittavan teknologian synnyttämistä. Ainoa tällä hetkellä tunnettu menettely edellyttäisi yksityisyyttä loukkaavien teknologisten ratkaisujen, kuten asiakkaan puoleisen skannauksen tai palvelinpään skannauksen toteutuksen, jotta kohteena olevaa sisältöä voitaisiin ennen sen lähettämistä verrata tunnettuun CSA-materiaaliin. Vaikka esityksessä todetaan, ettei palveluntarjoajia pitäisi velvoittaa kieltämään päästä päähän -salausta tai tekemään siitä mahdotonta, sisällön skannaus tai tutkiminen ennen päästä päähän -salauksen soveltamista kumoaa salauksen tarkoituksen.

Sääntelyn kohteena oleviin sovelluksiin ja järjestelmiin lisättäisiin toiminnan vaatimat ominaisuudet riskiarvion perusteella, jolloin lähetettävien tietojen tarkastaminen kohdistuisi kaikkiin ko. palvelua käyttäviin henkilöihin. Suojellaan Lapsia ry:n tutkimuksessa lapsiin kohdistuvaa seksuaaliväkivaltaa todistavaa kuvamateriaalia käyttävät rikoksentekijät nimesivät sosiaalisen median alustoista suosituimpina laajasti käytetyt Instagramin, Facebookin sekä Discordin, ja viestintäsovelluksista Telegramin, WhatsAppin ja Signalin. Toiminnallisuus ja seuranta kohdistuisi käytännössä valtaosaan mobiilipalveluiden käyttäjiä. Materiaalia tuottavat ja levittävät rikolliset oletettavasti siirtyisivät käyttämään kanavia tai menetelmiä, joissa paljastumisen riski olisi pieni.

Ehdotettu tunnistamisteknologia on kierrettävissä

Päätelaitteessa toteutettava asiakaspään skannaus monimutkaistaisi päästä päähän -salauksen toteuttavia viestipalveluita. Tunnetun CSA-materiaalin tunnistaminen edellyttäisi tunnistettavaa materiaalia sisältävän tai ns. hash-tiivisteitä sisältävän tietokannan lataamista ja päivittämistä. Materiaalin tunnistaminen tapahtuisi tarkastamalla kaikki palvelussa lähetettävä materiaali tunnistamistietokannassa olevia tietoja vastaan. Tunnistetusta materiaalista tehtäisiin ilmoitus sitä niitä vastaanottavalla viranomaiselle. Ohjelmisto- tai konfiguraatiovirheet voivat altistaa palveluiden käyttäjät laajamittaisille rikollisten tai vihamielisten valtioiden toteuttamille hyökkäyksille, kuten laitteiden sisällön skannaukselle. Käyttäjien laitteisiin sovellusten mukana asennettavien tunnistusjärjestelmien ja niiden vaatimien laittoman materiaalin tunnistamistietojen käsittelyn vaikutuksia päätelaitteiden (ts. puhelinten) suorituskykyyn, mm. akunkestoon ei ole arvioitu.

Ehdotuksessa tunnistamismääräyksen olisi tarkoitus kohdistua vain tunnettuun CSA-materiaaliin. Matemaattisesti laskettavan hash-tiivisteen tarkoituksena on yksilöidä kohteena oleva kuva, video tai muu tiedosto. Pienikin muutos, esim. kuvan tarkkuudessa tai sen sisällössä, muuttaa tiivisteen, jolloin samalta näyttävä kuva ei ole enää laskennallisen tiivisteen kannalta identtinen ja jolloin kuvaa ei enää tunnistettaisi. Hyväksikäyttömateriaalin tuottaminen ja levittäminen on ammattimaista rikollisuutta, jossa

esimerkiksi generatiivisen tekoälyn käyttäminen kuvien muokkaamisessa mahdollistaa tiivisteitä hyödyntävän tunnistamisen vaivattoman kiertämisen.

Laittoman materiaalin tunnistaminen tiivisteiden laskemista varten synnyttää omat haasteensa. Oletettavan suuren volyymin edellyttämä automaattinen tunnistaminen on edelleen virhealtista. Automatisoidussa prosessissa on selvä riski vääristä tunnistuksista ja niiden kautta vääristä tunnistuksen jälkeisistä toimenpiteistä kansalaisille.

CSA-materiaalin tunnistamiseen toteutettu järjestelmä mahdollistaa myös muiden, esim. poliittisia kantoja kuvaavien viestien tunnistamisen

Toteutettava järjestelmä mahdollistaisi teknisesti helposti toteutettavan muun, ei-toivottavaksi todetun materiaalin, esimerkiksi meemien tai poliittisia kantoja ilmaisevien kuvien tunnistamiseen ja niistä edelleen ilmoittamisen.

Esitetyn järjestelmän väärinkäyttö synnyttäisi mahdollisuuden laajamittaiseen ja vakavaan sanan- ja ilmaisunvapauden rajoittamiseen.

Kansalaisten luottamus digitaalisten palveluiden turvallisuuteen ja luottamuksellisuuteen on varmistettava

Kaikkiin kansalaisiin kohdistuvilla tunnistamismääräyksillä ja -toiminnalla olisi mahdollisesti laajoja vaikutuksia kansalaisten digitaalisiin palveluihin kohdistuvaan luottamukseen ja sitä kautta pyrkimykseen saada laajemmin digitaalisten palveluiden avulla saatavia hyötyjä. Luottamuksellisen viestin salaisuuden suoja on keskeinen tekijä digitalisoituneessa yhteiskunnassa.

Näemme hyvin haastavana ehdotuksen mukaisessa, mahdollisesti hyvin läpinäkymättömässä, komissiolle ehdotetussa suorassa täytäntöönpanovallassa hyväksyä teknologiat, joita voidaan käyttää tunnistamismääräysten toteuttamisessa. Tässä ehdotetun kaltaiset muutokset, joilla Digitaalisten palveluiden perusteisiin tai kansalaisten palveluihin kohdistuvaan luottamukseen kajotaan, tulisi toteuttaa vain laajapohjaisen harkinnan, ei yksittäisin, kriittisenkin, tarpeen ajamana.

Tietoliikenteen ja tietotekniikan keskusliitto Ficom ry:n lausunto

Elisa Oyj yhtyy Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry:n lausuntoon kaikilta osin.

Allekirjoitus

Elisa Oyj:n puolesta

Jaakko Wallenius
turvallisuusjohtaja