Electronic Frontier Finland – Effi ry

Lausunto 19.9.2023

Asia: EU-asetus lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnasta

Electronic Frontier Finland - Effi ry pyytää kunnoittavasti eduskunnan liikenne- ja viestintävaliokuntaa ottamaan huomioon suraavat näkökohdat harkitessaan kantaansa valtioneuvoston U-jatkokirjeeseen, joka koskee Euroopan komission ehdotusta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final).

Lyhyt yhteenveto:

- **Viestinnän päästä-päähän salausta ei pidä rikkoa** eikä Suomen pidä hyväksyä mitään siihen epäsuorastikaan velvoittavaa muotoilua.
- **Ei massavalvontaa**: viestien seurantaa ilman kohdennettua epäilyä ei pidä sallia, saati edellyttää.
- **Ei pidä vaatia teknisesti mahdottomia** tai kuvitella tekoälyn pystyvän parempaan kuin se ennakoitavissa olevassa tulevaisuudessa voi pystyä.
- **Tunnistamismääräysten pitää olla kohdennettuja ja tarkkarajaisia** eikä perus- ja ihmisoikeusvelvoitteista pidä tinkiä.
- **Netin anonyymiä käyttöä ei pidä estää.** Mahdollisuus anonyymiin viestintään on kriittisen tärkeää ihmisoikeuksien puolustajille, toisinajattelijoille, väärinkäytösten paljastajille jne.

Lapsiin kohdistuvan seksuaalisen väkivallan torjunta on tärkeä asia. Silti tai oikeammin juuri siksi on tärkeää, että siihen käytettävät keinot ovat toimivia, kustannustehokkaita eivätkä ristiriidassa perus- ja ihmisoikeuksien kanssa. Ehdotetussa muodossa **asetus vaarantaisi kaikkien eurooppalaisten, erityisesti myös lasten yksityisyyden suojan** ja sananvapauden, sosiaali- ja terveysviranomaisten toiminnan, liiketoiminnan ja kansallisen turvallisuudenkin. Viimeisimmässä versiossa olevat maininnat siitä, ettei tällä tavoiteltaisi salauksesta luopumista, jäävät tyhjiksi sanoiksi, kun asetettuja vaatimuksia ei tosiasiallisesti muuten voisi toteuttaa.

Internetistä on tullut keskeisen tärkeä väline kaikilla elämän alueilla, niin henkilökohtaisessa viestinnässä kuin liike-elämässä ja viranomaistenkin, erityisesti myös sosiaali- ja terveydenhuollon toiminnassa. Sitä ei voi enää rinnastaa vain postiin tai puhelimeen, vaan se yltää myös kaikkein yksityisimpiin ja intiimeimpiin tilanteisiin. Jos tietokoneet ja puhelimet alkavat vakoilla kaikkea ihmisten viestintää ilman epäilyäkään mistään rikoksesta, se on verrattavissa lähinnä siihen, että koteihin pitäisi asentaa valvontakamerat, jotka ovat aina päällä. **Yhteiskunta ei voi olla vapaa, jos viattomienkin ihmisten kaikkea toimintaa valvotaan koko ajan.**

Sosiaali- ja terveydenhuollon kannalta viestien luottamuksellisuuden rikkominen toisi myös isoja ongelmia. Sosiaali- ja terveydenhuollon toimijoiden keskinäisten sekä asiakkaiden välisten videoyhteyksien, sähköpostien, puheluiden, etätapaamisten ja yhteydenottojen luottamuksellisuutta ei voitaisi taata. **Tämä vaarantaisi myös lasten turvallisuuden**, kun he eivät uskaltaisi ottaa lastensuojeluviranomaisiinkaan yhteyttä pelätessään viestiensä päätyvän vääriin käsiin.

Jos CSAM- tai grooming-viestien tunnistamistarkkuus on 90% kuten komission vaikutustenarviointiraportti antaa ymmärtää, se tarkoittaa, että joka kymmenes viaton viesti tulkitaan sellaiseksi. Siis täysin viatonkin - käytetyn tekoälytekniikan luonteesta johtuu, että se voisi tulkita viestejä epäilyttäviksi ilman mitään ilmeistä syytä. Virheiden määrä olisi myös suurempi harvinaisten kielten kuten suomen kanssa. **Järjestelmä tuottaisi vääjäämättä suunnattoman määrän vääriä positiivisia.** Vaikka esitys puhuukin niiden minimoimisesta, sitä ei ole mahdollista tehdä tehokkaasti, siinä törmätään matemaattiseen ongelmaan (ns. väärien positiivisten paradoksi tai base rate fallacy): kun etsittävien viestien suhteellinen osuus on pieni, vääriä positiivisia tulee vääjäämättä paljon vaikka testin tarkkuus yksittäisen viestin kohdalla olisi hyvinkin suuri. Jo muutaman viestin päivävauhdilla **viaton ihminen joutuisi turhaan epäillyksi keskimäärin kerran viikossa**.

Nämä tekoälyn mielestä epäilyttävät viestit joutuisivat sitten jonkun ihmisen tutkittaviksi. Eivätkä edes virkavastuulla toimivan poliisin, poliiseja ei siihen riitä, vaan ensimmäinen tarkistaja olisi todennäköisesti joku halvan työvoiman maassa automaattikääntäjän kanssa työskentelevä ylityöllistetty ja alipalkattu ihminen, jolle houkutus kohdalle osuvan arkaluontoisen viestin väärinkäytöstä helposti muodostuisi ylivoimaiseksi. **Esitys vaarantaa kaikkien viestien luottamuksellisuuden**, ei vain jotenkin "arveluttavien" tms.

Järjestelmä muodostaisi massiivisen tietoturvariskin. Eurooppalaisten kaikkiin viesteihin käsiksi pääsevä järjestelmä olisi vastustamaton houkutus pahantekijöille, erityisesti myös eri maiden tiedustelujärjestöille. Ilman tietoturva-aukkojakin potentiaali väärinkäytöksiin on ilmeinen: samaa mekanismia voisi käyttää eri tavoin “väärin ajattelevien” ihmisten etsimiseen, kaikkiin hallituksiinkaan ei voi tässä luottaa. Apple hylkäsi oman suunnitelmansa tällaisesta jo aikaisemmin todeten, ettei pysty toteuttamaan sitä turvallisesti, ja Britannian tekeillä olevasta vastaavasta laista vastaava ministeriö tiedotti äskettäin todenneensa sen teknisesti mahdottomaksi ja aikoo jättää sen laistaan pois.

Kaikkien viestien skannaaminen tulisi suunnattoman kalliiksi. Vaikka tekoäly selvittäisi 99% viesteistä, niiden kokonaismäärä on niin suuri, että ihmistyötä tarvittaisiin todella paljon. Lisäksi CSAM-aineiston levittäjät ovat jo lähes kokonaan kaikonneet puheenaolevista kaupallisista palveluista ns. pimeän verkon puolelle, **joten toimiessaankaan tästä järjestelmästä ei olisi suurta hyötyä.** Tällaisen kalliin viattomiinkin kansalaisiin kohdistuvan vakoilujärjestelmän asemesta **olisi parempi antaa enemmän resursseja poliisille ja lastensuojelujärjestöille**. Poliisihan ei nykyisin pysty tehokkaasti käyttämään edes nykyisten lakien mahdollistamia keinoja lasten suojeluun.

Koko asetus olisi tässä vaiheessa parasta palauttaa suunnittelupöydälle, mutta vähintään siitä pitää saada luottamuksellisen viestinnän täydellisesti rikkova salauksen murtopakko yksiselitteisesti pois.

Kunnioittavasti,

Electronic Frontier Finland – Effi ry

Tapani Tarvainen, toiminnanjohtaja