Electronic Frontier Finland – Effi ry

Lausunto 16.9.2025

Asia: Asia: U 69/2022 vp Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final).

Electronic Frontier Finland – Effi ry kiittää Liikenne- ja viestintävaliokuntaa mahdollisuudesta tulla kuulluksi otsikon asiassa.

Effi kannattaa vilpittömästi esityksen tavoitetta lapsiin kohdistuvan seksuaali-väkivallan ehkäisystä ja torjunnasta. Nykymuodossaan puheenjohtajamaa Tanskan ehdottama versio on räikeästi kaikkien ihmisten - myös lasten - perusoikeuksien vastainen, eikä sitä tällaisenaan tulisi missään nimessä hyväksyä.

Yhteenveto:

- **Järjestelmä muodostaisi massiivisen tietoturvariskin**. Niin rikolliset kuin valtiollisetkin toimijat, erityisesti erilaiset tiedustelupalvelut, pyrkisivät varmasti käyttämään sitä väärin, ja kyllin suurilla resursseilla se varmasti myös onnistuisi.
- **Esitys tosiasiallisesti rikkoisi päästä-päähän salauksen**: vaikka salausta ei murrettaisi vaan se kierrettäisiin tai sen käyttö estettäisiin, vaikutus olisi sama.
- **Kyseessä olisi Euroopan tuomioistuimen kieltämä massavalvonta**: määräyksen kohteeksi joutuneessa palvelussa kaikkien käyttäjien viestit pitäisi analysoida ilman kohdennettua epäilyä.
- **Netin anonyymiä käyttöä ei pidä estää**. Mahdollisuus anonyymiin viestintään on kriittisen tärkeää ihmisoikeuksien puolustajille, toisinajattelijoille, väärinkäytösten paljastajille jne.

Huomio lausuttavista asiakirjoista

Aluksi haluamme kiinnittää erityistä huomiota siihen, että valiokunta on pyytänyt lausuntoa vain aihetta koskevista Sisäministeriön perusmuistiosta ja Valtioneuvoston kirjelmästä koskien kyseistä aihetta, eikä valiokunnalla ole käytössään puheenjohtamaan ehdotusta varsinaiseksi asetustekstiksi. Effin näkemä puheenjohtajamaan ehdotus sisältää merkittäviä perusoikeusriskejä, jotka Sisäministeriö ja Valtioneuvosto ovat omassa käsittelyssään täysin ohittaneet. Demokratian toteutumisen vuoksi olisi välttämätöntä, että valiokuntakäsittely perustuisi kaikkiin asialle olennaisiin tietoihin, eikä jäisi pelkkien muiden tahojen kirjoittamien tiivistelmien varaan.

Effin lausunto pohjautuu yllä mainittujen kahden dokumentin lisäksi myös puheenjohtajamaan esitysluonnokseen numero 11596/25, joka on päivätty 24.7.2025.

Johdanto

Esityksessä ehdotetut toimet ovat suurelta osin kannatettavia. Toimenpiteet kuitenkin painottuvat velvoitteisiin, joita kohdistetaan palveluntarjoajiin ja ennaltaehkäisevät toimenpiteet ilmiön juurisyiden tunnistamiseen ja korjaamiseen ovat pääosin jääneet puuttumaan esityksestä.

Lisäksi esitys sisältää merkittäviä ihmisten perusoikeuksiin puuttuvia toimenpiteitä, joita on mahdoton hyväksyä. Näistä räikeimpinä nousevat esille pakollinen tunnistusmääräys ja ikärajoihin liittyvä käyttäjien

pakollinen tunnistaminen. Käsittelemme näitä ongelmakohtia erikseen seuraavaksi. Lopuksi käymme läpi ehdotuksia lisätoimenpiteiksi, joilla voitaisiin paremmin saavuttaa asetuksen julkilausutut tavoitteet.

Tunnistusmääräys

Perusoikeusvaikutukset

Puheenjohtajavaltion ehdotukseen sisältyvä mahdollisuus määrätä viestintäsovellukset suorittamaan automaattista tunnistamista käyttäjien välittämään kuvamateriaaliin on kiellettyä massavalvontaa. Määräys koskee kaikkia palvelun käyttäjiä - ei pelkästään niitä, joita epäillään rikoksesta. Skannauksen kohteena on kaikki käyttäjän välittämä kuvamateriaali sekä kaikki tekstisisältö, sillä URL -osoitteet ja niiden osat ovat tekstiä.

Nämä perusoikeuksien rajoitukset eivät ole tehokkaita, välttämättömiä tai oikeansuhtaisia.

Ehdotuksessa korostetaan tämän massavalvonnaksi luokiteltavan toimenpiteen olevan viimesijainen keino. Tunnistusmääräyksiä annettaisiin vain sovelluksille, joiden riski on luokiteltu korkeaksi.

Kuitenkin kun tarkastellaan keinoja, joiden ehdotuksessa katsotaan vähentävän riskiä, huomataan, että monet näistä itsessään edellyttävät massavalvontaa, eivätkä ole päästä-päähän salatuissa sovelluksissa mahdollisia toteuttaa. Lainsäätäjän ääneen lausumattomana tavoitteena on pakottaa automaattinen tunnistus käyttöön myös päästä-päähän salatuissa sovelluksissa.

Esimerkkejä tällaisista riskinhallintakeinoista, jotka eivät ole toteutettavissa sovelluksissa, joilla ei ole näkyvyyttä käyttäjien viesintään:

- sisällön moderointi
- palvelun toiminnan valvonta
- mitigaatiotoimien vaikutuksien staattinen analyysi

Ehdotuksessa myös esitetään vaihtoehtona, että mikäli käyttäjä ei hyväksy automaattisen tunnistuksen käyttöönottoa, hän ei voisi lähettää sovelluksessa kuvamateriaalia tai URL-osoitteita. Tällainen rajoitus tekee modernista viestintäsovelluksesta tosiasiallisesti käyttökelvottoman. Kuvamateriaalia kun voi sisältyä kuvien ja videoiden lisäksi esimerkiksi kaikkiin muihin kirjallisiin dokumentteihin: niin, Word, Excel kuin pdf-dokumentitkin voivat sisältää kuvamateriaalia. Samoin pakatut zip-tiedostot.

Salatun viestintävälineen käytön tosiasiallinen kielto olisi merkittävää puuttumista sananvapauden ydinalueelle.

Tunnistusmääräystä olisi myös mahdoton toteuttaa luotettavasti avoimia standardeja käyttävissä viestintäsovelluksissa, joissa käyttäjä voi itse valita haluamansa (avoimen lähdekoodin) asiakasohjelmiston palvelun käyttöön. Käyttäjä voi yksinkertaisesti itse poistaa tunnistustoiminnallisuuden käytöstä asiakasohjelmistossaan. Asetusta onkin ilmeisesti tulkittava niin, että avoimia standardeja käyttävien viestintäsovellusten tarjoaminen unionin alueella tulisi kielletyksi.

Lopuksi huomautamme pikanttina yksityiskohtana, että ehdotuksen 7 artiklassa erikseen annetaan mahdollisuus kansalliselle lainsäätäjälle halutessaan ohittaa vaatimus sille, että tunnistusmääräys pitäisi käsitellä tuomioistuimessa tai riippumattomassa viranomaisessa. Näin ollen edes vähäinen tasapaino perusoikeuksien toteutumisen kannalta jää asetuksesta puuttumaan.

Turvallisuus

Puheenjohtajanvaltion ehdotuksessa ehdotetaan, että mikäli päästä-päähän salauksen toteuttavalle viestintäsovellukselle annettaisiin määräys automaattisen tunnistamisen käyttöönotosta, tulisi tämä tunnistaminen suorittaa itse sovelluksessa, ennen kuin sen kohteena oleva kuvamateriaali salataan tiedonsiirtoa varten.

Tämä on merkittävä tietoturvariski.

Ehdotuksen mukaan tunnistaminen tehtäisiin käyttäen komission määrittelemiä tekniikoita - oleellisesti tämä tarkoittaisi komission toimittamaa sovelluskirjastoa, joka liitettäisiin osaksi kohdesovellusta. Tämä sovelluskirjasto käyttäisi EU-keskuksen tuottamia ja ajan tasalla pitämiä tunnisteita tunnistamaan salaista materiaalia.

Tällainen sovelluskirjasto, jonka toimintaperiaate on salainen, on loppukäyttäjän tai sovelluksen turvallisuutta arvioivan asiantuntijan näkökulmasta läpinäkymätön laatikko, jonka turvallisuudesta ei voida varmistua. Olennaisesti se siis olisi sovellukseen upotettava vakoiluohjelma.

Vaikutus on suurin kaikkein turvallisimmille päästä-päähän salatuille sovelluksille, joissa sovelluksen koko toiminta on varmennettu julkaisemalla lähdekoodi ja binäärikoodin tuottamismentelmä niin, että ne ovat läpinäkyvästi kaikkien varmennettavissa. Tällainen ylimääräinen lisäkomponentti romuttaisi oleellisesti tämän viestivälineen kaikkein tärkeimmän turvallisuustakeen.

Kolmannen osapuolen ei tarvitse olla pahantahtoinen, että tällainen ylimääräinen kirjasto muodostaisi tietoturvariskin. Nykyaikana yksinkertainenkin sovelluskomponentti koostuu niin monesta eri lähteestä tulevasta palasesta ja niiden kokoaminen toimivaksi sovellukseksi koostuu niin monesta eri vaiheesta, että koko prosessin varmistaminen turvalliseksi on merkittävä haaste. Tällaisista toimitusketjuhyökkäyksistä on lukemattomia esimerkkejä viime vuosilta.

Esimerkiksi Hollannin tiedustelu- ja turvallisuuspalvelu AIVD on ilmaissut pitävänsä tällaisen ylimääräisen ei-julkisen sovelluskomponentin aiheuttamaa hyökkäyspinta-alaa liian vaikeana turvattavaksi luotettavasti.

"Skannaussovelluksen asentaminen kaikkiin matkapuhelimiin ja siihen liittyvine infrastruktuuri- ja hallintaratkaisuuineen johtaa laajaan ja hyvin monimutkaiseen järjestelmään. Tällainen monimutkainen järjestelmä antaa pääsyn suureen määrään mobiililaitteita ja niissä olevia henkilötietoja. Syntyvä tilanne on AIVD:n mielestä liian suuri riski digitaaliselle resilienssillemme. [...] Tunnistamismääräysten soveltaminen päästä päähän -salatun viestinnän tarjoajiin sisältää liian suuren tietoturvariskin digitaaliselle kestävyydellemme."
- https://berthub.eu/articles/posts/dutch-intel-service-csam-update/

Mainittakoon myös, että Apple hylkäsi oman suunnitelmansa vastaavanlaisesta suodatuksesta jo aikaisemmin todeten, ettei pysty toteuttamaan sitä turvallisesti.

Pidämme erityisen huvittavana, että Valtioneuvosto on kirjelmässään, ilman sen kummempia perusteluita, väittänyt:
"Valtioneuvosto kiinnittää huomiota siihen, että sähköisen viestinnän vahvaan salaukseen ehdotetut rajoitukset eivät vaaranna kyberturvallisuutta tai viestintä- ja tietojärjestelmien turvallisuutta."

Lopuksi huomautamme, että ylikansallisen palveluntarjoajan toteuttaessa tunnistusmääräyksen edellyttämiä tunnistusmekanismeja, ei EU:lla ole tosiasiallista mahdollisuutta vaikuttaa siihen, etteivät EU:n ulkopuoliset kansalliset viranomaiset edellytä ylikansallista palveluntarjoajaa käyttämään samoja valvontamekanismeja ja

kerättyjä tietoja tavalla, jossa tässä esityksessä esitetyt oikeusturvatakuut jäävät toteutumatta. EU:lla on jo ennestään ongelmia taata kansalaistensa digitaalisten oikeuksien toteutuminen ylikansallisissa palveluissa. Tällaisten mekanismien toteuttaminen johtaisi väistämättä laaja-alaiseen käytännön massavalvontaan.

Käyttäjien pakollinen tunnistaminen

Ehdotuksessa käytännössä edellytetään niin viestintäpalveluiden tarjoajien kuin sovelluskauppojenkin toteuttavan pakollisen ikärajatarkastuksen, joka - riippuen kansallisesta lainsäädännöstä - enemmän tai vähemmän paljastaa käyttäjän identiteetin viranomaisille. Esimerkiksi Unkarin tapauksessa on vaikea kuvitella, että poliisivaltio käytännössä tarjoaisi kansalaisilleen mahdollisuutta anonyymiin ikärajatarkastukseen.

Ylipäätään, oikeus vastaanottaa tietoja myös anonymymisti on sananvapauden ydinaluetta. Tämä oikeus vastaanottaa tietoja sisältää myös oikeuden ladata haluansa viestintäsovelluksen tai sen lähdekoodin. Mahdollisuus anonyymiin viestintään on kriittisen tärkeää ihmisoikeuksien puolustajille, toisinajattelijoille, väärinkäytösten paljastajille jne.

Pakolliset ikärajatarkastukset puuttuvat voimakkaasti sananvapauteen ja ne tulisi poistaa ehdotuksesta.

Ikärajojen osalta haluamme vielä huomauttaa, että mahdollisuus luottamukselliseen viestintään on myös alaikäisen perusoikeus ja sen rajoittaminen, erityisesti koskien puhtaita viestintäsovelluksia, on hyvin kyseenalaista.

Lisäksi ikärajojen käytännön vaikutuksena tulee olemaan, että alaikäiset käyttäjät alkavat enenevissä määrin käyttämään hajautettuja palveluita, joita tämän asetuksen vaatimukset eivät koske ja joissa ei näin ollen myöskään ole ikärajavalvontaa. On asetuksen tavoitteiden vastaista, jos kaikkein haavoittuvimmassa asemassa olevat käyttäjät liiallisilla rajoituksilla ajetaan pois juuri niistä palveluista, joita asetuksella pyritään tekemään turvallisemmiksi. Tältä osin myös ikärajatarkastusten tehokkuus voidaan kyseenlaistaa.

Ehdotukset vaihtoehtoisiksi toimiksi

Haluamme korostaa esityksen sisältävän monia kannatettavia toimenpinteitä, joita verkkopalveluita velvoitetaan toteuttamaan näitä ovat esimerkiksi:

- käyttäjien informointi palvelun käytön riskeistä ja käyttäjien ohjaaminen luotettaviin apua tarjoaviin palveluihin
- käyttäjille tarkoitettu helppokäyttöinen ilmoitustoiminnallisuus CSA-materiaalin havaitsemisemisesta
- prosessit reagoida ilmoituksiin tehokkaasti
- lapsikäyttäjien turvallisuuden ja CSA-materiaalin levittämisen riskien huomioiminen osana palvelun kehitystä ja valvontaa
- käyttäjien yksityisyyttä kunnioittavat oletusasetukset

Haluaisimme tuoda lisäksi esille joitakin tarpeelliseksi katsomiamme toimenpiteitä, joita olisi syytä huomioida joko tässä asetuksessa tai osana jatkotoimenpiteitä:

- CSA-materiaaliin liittyvien ongelmien parempi tunnistaminen julkisisssa mielenterveyspalveluissa

ja näiden palveluiden rahoituksen lisääminen

- Hyväksikäytön uhreja avustavien palveluiden rahoituksen lisääminen ylipäätään
- Anonyymien mielenterveyspalveluiden tarjoaminen CSA-materiaalia katsoville henkilöille. Parhaimman tieteellisen tutkimuksen mukaan noin puolet näistä haluaisi lopettaa materiaalin käytön. Noin puolet heistä myös pelkää, että jatkuva materiaalin katselu saattaa johtaa lapsen oikeuksien loukkaamiseen. CSA-materiaali on heille addiktio. Heille ei kuitenkaan ole tarjolla ulkopuolisia resursseja addiktion hoitamiseen.
- Kansainvälisen esitutkintayhteistyön lisääminen lapsiin liittyvissä seksuaalirikostutkinnoissa. Anonyymiverkoissa epäiltyjen kanssallisuutta tai tekojen tapahtumapaikkaa on vaikea tunnistaa ja rikollinen toiminta on usein rajat ylittävää.
- Tieteellisen tutkimuksen kohdistaminen ilmiön parempaan ymmärtämiseen. Ilmiötä on tähän mennessä tutkittu hyvin vähän.

Erityisesti julkisten mielenterveyspalveluiden rahoituksen osalta huomautamme, että digitaalista nuorisotyötä ainoana suomalaisena organisaationa edistänyt Verke ajettiin vuonna 2024 alas rahoituksen loputtua. Ks. https://verke.hel.fi/