FiCom ry | Asko Metsola
15.10.2024

FiComin lausunto lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnasta

Eduskunnan hallintovaliokunta on pyytänyt FiComilta lausuntoa valtioneuvoston kirjelmästä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final). FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- Unkarin ehdotus ei ratkaisevasti eroa aiemmista kompromissiteksteistä, sillä taustalla on lainvalvontaviranomaisten pitkäaikainen tavoite murtaa salaus.
- Kaikkiin kansalaisiin kohdistuvilla tunnistamismääräyksillä olisi laajoja periaatteellisia vaikutuksia perusoikeuksien toteutumiseen verkossa, ja ne rapauttaisivat luottamuksellisen viestin salaisuuden suojaa.
- Ehdotus johtaisi toteutuessaan laajaan viestintäpalvelujen ennakkomonitorointiin. On olemassa huomattava riski myös sille, että ehdotus johtaisi monitoroinnin väärinkäyttöön.
- Hallitusohjelma ei edellytä nyt ehdotettujen menetelmien käyttöönottoa – jopa päinvastoin.
- Lukuisat eri asiantuntijat eri yhteiskunnan aloilta ovat esittäneet ehdotukseen liittyviä vakavia huolia.

FiComin jäsenet ja koko ICT-ala on sitoutunut ehkäisemään ja torjumaan lapsiin kohdistuvaa seksuaalista väkivaltaa. Tämän osoittaa mm. teleyritysten lain 1068/2006 nojalla yhteistyössä Keskusrikospoliisin 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.

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. Lisäksi FiCom on mukana alan eurooppalaisen yhteistyöjärjestön EuroISPA:n Online Content -työryhmässä, jossa jaetaan parhaita käytänteitä eri jäsenjärjestöjen kotimaista.

FiCom on jäsenineen kuitenkin erittäin huolissaan puheenjohtajamaa Unkarin komission asetusehdotukseen ehdottamista muotoiluista. Tuoreinkin, 7.10.2024 päivätty kompromissiteksti, on paikoin ristiriidassa ehdotetun sähköisen viestinnän tietosuoja-asetuksen (ePrivacy) ja voimassa olevan ePrivacy-direktiivin, EU:n kyberturvallisuusdirektiivin (NIS 2.0) sekä verkkoneutraliteettisääntöjen suojaamien perusperiaatteiden kanssa.

Taustalla pitkäaikainen tavoite murtaa viestintäsalaisuus

Käsiteltävänä on ehdotus lapsiin kohdistuvan seksuaaliväkivallan ehkäisemiseksi ja torjumiseksi, mutta taustalla vaikuttaa lainvalvontaviranomaisten pitkäaikainen tavoite murtaa viestintäsalaisuus kokonaan.

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 (ns. Going Dark –aloite). 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. Suomen eduskunnassa valtioneuvoston E-selvitys Going Dark -aloitteesta käsiteltiin huhtikuussa 2024 hyvin vähin äänin.

Samaan aikaan kun Going Dark -aloitetta käsiteltiin Suomessa, Europol ja kaikkien jäsenmaiden lainvalvontaviranomaisten johtajat julkaisivat huhtikuussa 2024 yhteisen julistuksen, jonka tavoitteena on käytännössä murtaa salaus kaikelta viestinnältä kaikkea tutkintaa varten.

Unkarin ehdotuksessa ei ratkaisevaa muutosta aikaisempaa

Puheenjohtajamaa Unkarin uusimmassa, 7.10.2024 päivätyssä tekstissä ehdotetaan, kuinka **kaikissa henkilöiden välisissä viestintäpalveluissa** (”*all interpersonal communications services*”, kohta 26a, s. 22) tulisi ottaa käyttöön järjestelmä, joissa viestintäpalveluiden käyttäjät antavat suostumuksensa kaiken palveluihin lisäämänsä sisällön tarkistamiseen. Tarkastus tapahtuisi ehdotuksen mukaan ennen päästä päähän -salauksen soveltamista. **Suostumuksesta kieltäytyvät käyttäjät eivät voisi lähettää videoita, kuvia tai linkkejä verkkopalvelun kautta lainkaan** (”*Users not giving their consent should still be able to use that part of the service that does not involve the sending of visual content and URLs.*”, kohta 26a, s. 22).

Ehdotus jättää avoimeksi, miten tarkastus tulisi toteuttaa. Ainoa tunnettu menettely edellyttäisi palveluntarjoajilta yksityisyyttä loukkaavien teknologisten ratkaisujen, kuten asiakkaan puoleisen skannauksen (CSS) tai palvelinpuolen skannauksen käyttöönottoa, jotta visuaalista sisältöä voitaisiin ennen sen lähettämistä verrata tunnettuun CSA-materiaaliin. Vaikka puheenjohtajamaa toteaa, ettei palveluntarjoajia pitäisi velvoittaa kieltämään päästä päähän -salausta tai tekemään siitä mahdotonta, sisällön skannaus ennen päästä päähän -salauksen soveltamista kumoaa täysin koko salauksen tarkoituksen. Väite olisi sama kuin tilanteessa, jossa posti velvoitettaisiin lukemaan kaikkien kansalaisten kirjeet ennen kirjekuoren sulkemista. Tällöin voitaisiin väittää, että ainoastaan kirjeen vastaanottaja saisi avata kirjekuoren, eikä kirjesalaisuutta olisi rikottu.

CSS monimutkaistaisi päästä päähän -salauksen toteuttavia järjestelmiä, sillä tunnetun CSA-materiaalin tietokannan tai hash-teknologian lataamista, päivittämistä, tarkistamista sekä raportointia varten järjestelmään tulisi lisätä rajapintoja ja koodia. Nämä järjestelmät ovat erittäin herkkiä ja edellyttävät vankkoja turvatoimia, joten mikä tahansa virhe voisi antaa hakkereille, rikollisille tai vihamielisille valtioille mahdollisuuden skannata laitteiden sisältöä kohdistetusti tai suuressa mittakaavassa. On myös olemassa huomattava riski, että tunnetun sisällön hash-tietokanta vuotaisi, mikä osaltaan voisi heikentää palveluiden

suojauksia. Kaiken kaikkiaan lisääntynyt monimutkaisuus johtaa todennäköisesti uusiin haavoittuvuuksiin, jotka heikentävät kaikkien käyttäjien turvallisuutta.

Ehdotettujen velvoitteiden soveltaminen perinteisiin, numeroihin perustuviin henkilöihin välisiin viestintäpalveluihin, kuten tekstiviesteihin tai puheluihin, on teknisesti mahdotonta. Palveluntarjoajilla ei ole pääsyä äänipuheluihin tai tekstiviesteihin niiden analysointia varten.

Unkarin ehdotus ei sinänsä ole uusi. Kuten sisäministeriökin 25.9.2024 päivätyssä perusmuistiossaan toteaa, jo aiempi puheenjohtajamaa Belgia oli esittänyt samaa keväällä 2024. Unkarin tekemät rajaukset aiempiin ehdotuksiin eivät poista sen ongelmia, joten on erikoista, että neuvostossa halutaan saada ratkaisu asetusehdotukseen nimenomaan nyt Unkarin puheenjohtajuuskaudella.

Tunnistamismääräyksen olisi tarkoitus kohdistua vain tunnettuun CSA-materiaaliin. Ehdotetun hash-teknologian heikkous on, että melko vähäisetkin muutokset alkuperäiseen kuvaan tai videoon muuttavat sen saamaa yksilöllistä tunnistetta, jolloin muokattu kuva voi läpäistä seulan. Hyväksikäyttömateriaalin tuottaminen ja levittäminen on ammattimaista rikollisuutta, jossa esimerkiksi generatiivisen tekoälyn käyttäminen mahdollistaa hash-teknologian kiertämisen. Toisaalta, kun otetaan huomioon analysoitavien kuvien määrä (kaikki lähetetyt kuvat ja videot kaikissa henkilöiden välisissä viestintäpalveluissa), jotkin nykyiset mallit aiheuttaisivat tutkijoiden mukaan erittäin suuren määrän vääriä positiivisia tuloksia. Jokainen näistä virheistä johtaisi siihen, että käyttäjiä epäiltäisiin aiheetta hirvittävistä rikoksista. Sekä väärien negatiivisten että väärien positiivisten tulosten määrän vähentämiseksi hajautusalgoritmit olisi konfiguroitava siten, että tietokanta väistämättä vuotaisi tietoja alkuperäisistä kuvista. Tämä voisi johtaa siihen, että estettäväksi tarkoitettua CSA-materiaalia olisi mahdollista saada tietokannasta ulos alkuperäisessä muodossaan.

Ehdotuksen hyväksyttävyyden kannalta on yhdentekevää, että tunnistamismääräys kohdistettaisiin vain sellaisiin verkkopalveluntarjoajiin tai niiden osiin, joissa on todettu korkea riski CSA-materiaalin levittämiselle. Suojellaan Lapsia ry:n tekemässä tutkimuksessa lapsiin kohdistuvaa seksuaaliväkivaltaa todistavaa kuvamateriaalia käyttävät rikoksentekijät nimesivät sosiaalisen median alustoista suosituimpina Instagramin, Facebookin sekä Discordin ja viestintäsovelluksista Telegramin, WhatsAppin ja Signalin.

Käytännössä korkean riskin verkkopalveluntarjoajia, joihin tunnistamismääräyksiä voitaisiin kohdistaa, olisivat siis nimenomaan suositut, kaikkien kansalaisten käyttämät alustat ja sovellukset. Ehdotettu ennakkomonitorointi kohdistuisi kaikkiin näitä suosittuja palveluita käyttäviin kansalaisiin eikä vain niihin, joita lainvalvontaviranomainen perustellusti epäilee CSA-materiaalin lähettämisestä. Oikeudellisesta näkökulmasta kaikkiin kansalaisiin kohdistuvilla tunnistamismääräyksillä olisi laajoja periaatteellisia vaikutuksia perusoikeuksien toteutumiseen verkossa, ja ne rapauttaisivat luottamuksellisen viestin salaisuuden suojaa.

Aivan yhtä yhdentekevää ehdotusten hyväksyttävyyden kannalta on, että tunnistamismääräys olisi kansallisen tuomioistuimen antama, ajallisesti rajattu viimesijainen keino, joka kohdistuisi vain visuaaliseen sisältöön ja pitäisi sisällään myös toimenpiteen valvonnan ja raportoinnin. **Kun asiakkaan puoleinen skannaus (CSS) on kerran otettu käyttöön kaikkien EU-kansalaisten käyttämissä palveluissa, olisi hyvin**

helppoa laajentaa skannaus kaikkiin laitteeseen tallennettuihin kuviin tai laajentaa hash-tietokantaa uudella, esimerkiksi terrorismiin tai järjestäytyneeseen rikollisuuteen liittyvällä sisällöllä ilman avointa demokraattista keskustelua. Unkarin muotoilussa komissiolle ehdotetaankin suoraa täytäntöönpanovaltaa hyväksyä teknologiat, joita voidaan käyttää tunnistamismääräysten toteuttamisessa.

Viestintäsalaisuus on ihmisoikeus

Euroopan ihmisoikeustuomioistuin julkaisi helmikuussa 2024 ratkaisunsa asiassa Podchasov v. Venäjä, jossa ihmisoikeustuomioistuin katsoi, että **päästä päähän ulottuvan salauksen kieltäminen, heikentäminen tai murtaminen rikkoo ihmisoikeuksia**. Tapauksessa Venäjän turvallisuuspalvelu FSB vaati viestipalvelu Telegramia luovuttamaan terrorismista epäiltyjen käyttäjien salattuja viestejä. Telegramin kieltäydyttyä luomasta kaikkien käyttäjien salausta heikentävää takaporttia, palvelu sai sakot ja kiellettiin Venäjällä.

Ihmisoikeustuomioistuimen ratkaisussa käydään ansiokkaasti läpi myös Yhdistyneiden kansakuntien, Euroopan unionin tuomioistuimen, Euroopan unionin kyberturvallisuusvirasto ENISA:n, Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun ulostulot aiheesta. Näistä esimerkiksi Yhdistyneiden kansakuntien mukaan vahva salaus on lasten suojelun tai rikosten selvittämisen tarvetta tärkeämpää.

Hallitusohjelma ei edellytä nyt ehdotettujen menetelmien käyttöönottoa – jopa päinvastoin.

Sisäministeriö on luetellut perusmuistioonsa muina asian käsittelyyn vaikuttavina tekijöinä eräitä hallitusohjelman kirjauksia. **Yksikään näistä hallitusohjelman kirjauksista ei edellytä nyt ehdotettujen menetelmien käyttöä. Puheenjohtajamaa Unkarin ehdotuksen hyväksyminen olisi paikoin jopa hallitusohjelman vastainen.**

Hallitusohjelman mukaan lapseen kohdistuvan seksuaaliväkivallan tapauksissa varmistetaan lapsen edun mukainen tutkinta ja monialainen tuki eri viranomaisten yhteistyönä (hallitusohjelman s. 195). **Oikeus viestinnän luottamuksellisuuteen on nimenomaan lapsen edun mukaista.** Esimerkiksi Euroopan tietosuojaneuvoston ja tietosuojavaltuutetun jo elokuussa 2022 antaman yhteisen lausunnon mukaan tunnistamismääräykset voisivat ”*jopa vahingoittaa ihmisiä, joita niillä pyritään suojelemaan. Ne voivat heikentää huomattavasti viestinnän luottamuksellisuutta, mikä altistaisi palveluja käyttävät lapset tarkkailulle tai salakuuntelulle*” (käännös tietosuojavaltuutetun toimiston).

Lukuisat seksuaaliväkivallasta selvinneet ovat kritisoineet alkuperäistä ehdotusta, samoin uhrien auttamiseen tähtäävät järjestöt Saksasta ja Espanjasta, Saksan ja Alankomaiden Nettivihjeet, Euroopan ammatillisten informatiikkayhdistysten neuvosto (CEPIS), 47 ihmisoikeusjärjestöä sekä saksalainen lastensuojelujärjestö. **Tuoreimpana käänteenä jo 379 tieteilijää kyberturvallisuuden ja tietosuojan alalta 36 maasta (tilanne 9.10.2024) on allekirjoittanut nimenomaan puheenjohtajamaa Unkarin uusinta ehdotusta vastustavan ulostulon.**

Hallitusohjelman mukaan hallitus selvittää tahallisten henkirikosten ja lapsiin kohdistuvien seksuaalirikosten syyteoikeuden vanhentumisajan pidentämistä tai syyteoikeuden vanhentumisesta luopumista ja ryhtyy

tarvittaviin toimenpiteisiin (hallitusohjelman s. 195). Lisäksi hallitus tiukentaa CAM- eli Child Abuse -materiaalia koskevaa sääntelyä vakavien rikosten uhreina olevien lasten suojelemiseksi. Väkivaltakuvauksen hallussapito kriminalisoidaan ja lasta seksuaalisesti esittävän kuvan hallussapidolle säädetään törkeä tekomuoto. Lisäksi huolehditaan, että muun raa'an väkivaltamateriaalin hallussapito on kriminalisoitu ihmisten ja eläinten suojelemiseksi (s. 196). **Ehdotetut keinot ovat kannatettavia, eikä niiden toteuttaminen liity mitenkään nyt käsiteltävänä olevaan ehdotukseen viestinnän ennakollisesta monitoroinnista.**

Hallitusohjelman mukaan kriminaalipolitiikan tavoitteena on rikosten ehkäiseminen, rikoksentekijöiden saattaminen vastuuseen teoistaan sekä uhrien auttaminen ja tukeminen (hallitusohjelman s. 195). Kaiken yksityisen viestinnän tarkistaminen jo olemassa olevan laittoman materiaalin esittämisen estämiseksi ei täytä mitään näistä tavoitteista. **CSA-materiaalia vastaan taistelemisen tulee perustua lapsiin kohdistuvan seksuaaliväkivallan, ei vain sitä kuvaavan materiaalin tai sen jakelun, poistamiseen.** Todistetusti tehokkaita menetelmiä, joita esimerkiksi YK suosittelee, ovat mm. koulutus, digitaalinen lukutaito, huoltajien valvonta ja erilaisten haitallisten havaintojen käyttäjäpohjainen turvallisuusraportointi palvelujen ylläpitäjille.