FiCom ry | Asko Metsola
28.9.2023

FiComin lausunto lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnasta

Eduskunnan suuren valiokunnan työjaosto on pyytänyt FiComilta lausuntoa valtioneuvoston U-jatkokirjeestä, joka koskee Euroopan komission ehdotusta 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

- Suomen ei tule hyväksyä muotoilua, joka käytännössä velvoittaisi viestinnän salauksen purkamiseen. Asetus ehdotetussa muodossaan vaarantaa kaikkien Euroopan kansalaisten perusoikeudet, itsemääräämisoikeudet sekä liikesalaisuuksien ja innovaatioiden suojan.
- Numeroihin perustuvien, henkilöiden välisten viestintäpalveluiden tarjoajat tulee jättää asetuksen velvoitteiden ulkopuolelle. Yksittäisten henkilöiden teksti- ja ääniviestinnän yleisluontoinen seuranta heikentäisi merkittävästi perusoikeuksien, kuten luottamuksellisen viestinnän, suojaa.
- Groomingiin ja CSAM:iin kohdistuvien tunnistamismääräysten edellytyksiä on tarkennettava. Suomen ei tule hyväksyä perus- ja ihmisoikeusvelvoitteiden vastaista sääntelyä tunnistamismääräyksestä.

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 Safer Internet -työryhmässä, jossa jaetaan parhaita käytänteitä eri jäsenjärjestöjen kotimaista.

FiCom on jäsenineen kuitenkin erittäin huolissaan komission ehdottaman asetuksen toimivuudesta ja tulevaisuudesta, varsinkin koska eräät asetuksessa ehdotetut velvoitteet ja toimenpiteet ovat teknisesti mahdottomia toteuttaa tai ne eivät sovellu palveluiden käyttötarkoitukseen. Lisäksi puheenjohtajamaa Espanjan tuoreinkin, 8.9.2023 päivätty kompromissiteksti, on paikoin ristiriidassa ehdotetun sähköisen viestinnän tietosuoja-asetuksen (ePrivacy) ja voimassa olevan ePrivacy-direktiivin, verkko- ja tietoturvadirektiivin päivityksen (NIS 2.0) sekä verkkoneutraliteettisääntöjen suojaamien perusperiaatteiden kanssa. Esitys johtaa käytännössä velvoitteeseen purkaa viestinnän salaus.

Viestinnän salausta ei tule purkaa

Kuten jatkokirjeessäkin tuodaan esille, **neuvoston oikeuspalvelun (NOP) lausunnossaan esittämän arvion mukaan salattuihin ympäristöihin ulottuva tunnistamismääräys tarkoittaisi, että palveluntarjoajien tulisi joko luopua tehokkaasta päästä päähän -salauksesta, luoda ns. takaovia päästäkseen salattuun sisältöön tai saada pääsy sisältöön käyttäjän päätelaitteella ennen sisällön salaamista.** NOP:n mukaan viestinnän yleinen käsittely CSA-materiaalin (Child Sexual Abuse Material, CSAM) tunnistamiseksi edellyttäisi de facto tietoturvatoimenpiteiden, erityisesti päästä päähän -salauksen, kieltämistä, heikentämistä tai muutoin kiertämistä, jotta kyseinen tunnistaminen olisi mahdollista. Tämä johtaisi vakavaan perus- ja ihmisoikeuksien rajoitukseen sekä rajoittaisi muiden oikeutettujen tavoitteiden, kuten tietoturvan, varmistamista.

Puheenjohtajamaa Espanjan tuoreimmassa, 8.9.2023 päivätyssä versiossa kompromissitekstin johdantokappaleisiin 26 ja 31 on lisätty maininnat siitä, ettei asetuksella tavoitella päästä päähän -salauksesta luopumista ja etteivät tunnistamismääräykset ole ristiriidassa digipalvelusäädöksen (Digital Services Act, DSA) yleisen valvontavelvollisuuden kiellon kanssa. Varsinaisen asetustekstin lisäysten mukaan tunnistamismääräykset olisi tarkoitettu vain CSAM:n havaitsemiseksi ja ne olisivat voimassa vain rajoitetun ajan (7 artikla) eikä niillä pitäisi voida päätellä viestinnän sisältöä tai tehdä päästä päähän -salausta mahdottomaksi (10 artikla). Lisäykset jäävät tyhjäksi kirjaukseksi. **Vaikka ehdotus teknologianeutraaliutta tavoitellen jättää yksityisten palveluntarjoajien päätettäväksi keinot tunnistamismääräyksen toteuttamiseksi, käytännössä asetuksessa säännellyt toimet edellyttävät tuoreimmassakin muotoilussa takaovien luomista tai käyttäjien sisältöön puuttumista.** Kuten U-jatkokirjeessäkin on todettu, tällä on laajakantoisia ja periaatteellisia vaikutuksia luottamuksellisen viestin salaisuuden suojaan sekä muiden perusoikeuksien toteutumiseen verkossa.

Viestintäpalveluiden päästä päähän -salaus sekä TLS:n (Transport Layer Security) ja HTTPS:n (Hypertext Transfer Protocol Secure) kaltaiset salausprotokollat ovat välttämättömiä, jotta internetiin voi luottaa. Ne takaavat kyberturvallisuuden ja tietosuojan internetissä, ja 16.1.2023 voimaan tullut ns. NIS 2.0 -direktiivi suosittelee ja paikoin jopa vaatii niitä. Salauksen murtuminen romahduttaisi internetin teknisen infrastruktuurin ja estäisi yritysten pyrkimykset edistää luottamusta, käyttäjien yksityisyyttä ja sananvapautta internetissä. Ilman salausta mikään järjestelmä maailmassa ei olisi enää turvallinen. **Asetus ehdotetussa muodossaan vaarantaa kaikkien Euroopan kansalaisten perusoikeudet, itsemääräämisoikeudet sekä liikesalaisuuksien ja innovaatioiden suojan.** Tällä taas olisi valtava vaikutus koko EU-alueen talouteen. **Suomen ei tule hyväksyä muotoilua, joka käytännössä velvoittaisi viestinnän salauksen purkamiseen.**

Euroopan unionin tuomioistuin on tehnyt ratkaisuissaan täysin selväksi, että sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohdassa suojattu viestinnän luottamuksellisuus on tulkinnassa pääsääntö. Viestinnän luottamuksellisuuteen tehtyjen poikkeuksien tulee säilyä poikkeuksena eikä muuttua säännöksi. Tätä periaatetta on noudatettava myös nyt ehdotetussa asetuksessa. Asetuksen tulee olla yhteensopiva myös digipalvelusäädöksen 7 artiklan kanssa, jonka mukaan ”*välittäjäpalvelujen tarjoajille ei saa asettaa yleistä velvoitetta valvoa siirtämiään tai tallentamiaan tietoja eikä velvoitetta pyrkiä aktiivisesti saamaan selville laitonta toimintaa osoittavia tosiasioita tai olosuhteita*”.

Soveltamisalaan vain palveluntarjoajat, joille velvoitteet ylipäätään mahdollisia

Kun lainsäätäjät ehdottavat yhdenmukaisia velvoitteita kaikille välittäjäpalveluille, niiden tulee ottaa huomioon verkkoekosysteemin monimuotoisuus. Asetuksen soveltamisalaan halutaan ymmärrettävästi sisällyttää kaikki mahdolliset palveluntarjoajat, mutta internet-palveluntarjoajilla on todellisuudessa hyvin

vaihtelevat tekniset mahdollisuudet puuttua CSAM:n tarjontaan. **Asetuksen soveltamisalan tulee kattaa vain sellaiset internet-palveluntarjoajat, jotka ovat CSAM:n leviämisen tai groomingin kannalta relevantteja ja joilla on mahdollisuus siihen puuttua.** Perinteisten numeroihin perustuvien, henkilöiden välisten viestintäpalvelujen tarjoajien osalta näin ei selvästikään ole, mikä on todettu jo Euroopan tietosuojavaltuutetun ja Euroopan tietosuojaneuvoston yhteisessä lausunnossa 4/2022. **Lausunnossaan em. viranomaiset totesivat, että yksittäisten henkilöiden teksti- ja ääniviestinnän yleisluontoisen seurannan kielteinen vaikutus on niin vakava, ettei sitä voida perustella EU:n perusoikeuskirjan puitteissa** (lausunnon kohdat 41, 56 ja 68–76).

Ehdotettujen velvoitteiden soveltaminen numeroihin perustuviin, henkilöihin välisiin viestintäpalveluihin, kuten tekstiviesteihin tai puheluihin, on myös teknisesti mahdotonta. Palveluntarjoajilla ei ole pääsyä äänipuheluihin tai tekstiviesteihin niiden analysointia varten. Yleinen säilytysvelvollisuus olisi suhteeton ja ristiriidassa Euroopan unionin tuomioistuimen ratkaisukäytännön kanssa. Samoista syistä näihin viestintäpalveluihin ei tule myöskään kohdistaa asetuksen 3 artiklan riskinarviointia tai 4 artiklan riskien pienentämistä koskevia velvoitteita. Asetuksen 3 artiklan 2 kohdassa ja 4 artiklan 3 kohdassa vaaditaan numeroista riippumattomien, henkilöiden välisten viestintäpalvelujen tarjoajia toteuttamaan tarvittavat iän varmistus- ja arviointitoimenpiteet, jotta lapsikäyttäjät tunnistetaan luotettavasti. Numeroihin perustuvissa viestintäpalveluissa tällainen iästä riippuvainen seuranta tai reagointi ei kuitenkaan ole tehokasta tai edes mahdollista, koska numeroihin perustuvien viestintäpalveluiden tarjoajat eivät tee sopimusta alaikäisten kanssa. Tällöin ne eivät myöskään tarjoa lapsille palveluita, jotka edellyttäisivät iän vahvistamista. Tämä koskee erityisesti yrityspalveluja, joissa sopimuspuolet ovat tyypillisesti yrityksiä, jotka hankkivat viestintäpalveluja täysi-ikäisten työntekijöiden puolesta pääsääntöisesti vain liiketoimintatarkoituksiin. **Numeroihin perustuvien, henkilöiden välisten viestintäpalvelujen tarjoajat tulee jättää asetuksen soveltamisalan ulkopuolelle.** Lisäksi internet-yhteyspalvelujen tarjoajia tulee pitää viimesijaisena keinona tunnistaa mahdollinen laiton sisältö tai estää pääsy siihen. Sen sijaan toimien tulee tapahtua mahdollisimman lähellä laittoman sisällön lähdettä, eli esimerkiksi ensisijaisesti sovelluksessa tai muulla alustalla, johon laiton sisältö on lisätty.

Soveltamisalan ulottamista palveluntarjoajiin, joilla ei ole teknistä mahdollisuutta toteuttaa asetuksen velvoitteita, on perusteltu käsittämättömästi muun muassa sillä, että asetus ottaisi huomioon tulevaisuuden kehityksen. Käytännössä tämä tarkoittaa sitä, että asetuksen soveltamisalaan sisällytettäisiin varmuuden vuoksi turhaan tuhansia yrityksiä eri puolilla Eurooppaa, jotta se kattaisi mahdollisesti tulevaisuudessa keksittävät uudet, CSAM:n leviämisen kannalta merkitykselliset palvelut. **Perusteettoman soveltamisalan laajentamisen sijaan komission tulee säännöllisesti arvioida asetusta, jotta soveltamisalaa voidaan tarvittaessa muuttaa.**

Groomingiin ja tuntemattomaan CSAM:iin kohdistuvat tunnistamismääräykset

Euroopan tietosuojavaltuutetun ja Euroopan tietosuojaneuvoston yhteisessä lausunnossa 4/2022 komissiota kehotettiin selkeyttämään edellytyksiä hyväksikäyttömateriaaliin ja lasten houkuttelemiseen (grooming) liittyvän tunnistamismääräyksen antamiselle. Tietosuojaneuvosto ja -valtuutettu olivat lausunnossaan erityisen huolissaan toimenpiteistä, joita suunnitellaan entuudestaan tuntemattoman CSAM:n ja groomingin havaitsemiseksi (lausunnon kohdat 68–76).

Suomessa lausunnosta tiedotti tietosuojavaltuutetun toimisto. Lausunnon mukaan ”*on selvää, että lasten seksuaalinen hyväksikäyttö on hirvittävä rikos, joka edellyttää nopeita ja tehokkaita toimia, mutta ehdotuksessa on nykyisessä muodossaan joitakin vakavia puutteita. Ehdotuksessa on epämääräisiä*

käsitteitä, jotka voivat johtaa erilaiseen täytäntöönpanoon eri puolilla EU:ta erityisesti tunnistamismääräysten osalta. Määräykset voivat tällaisenaan jopa vahingoittaa ihmisiä, joita niillä pyritään suojelemaan. Ne voivat heikentää huomattavasti viestinnän luottamuksellisuutta, mikä altistaisi palveluja käyttävät lapset tarkkailulle tai salakuuntelulle".

Esimerkiksi tekoälyn kaltaisen teknologian käyttö viestinnän skannaamiseen aiheuttaa todennäköisesti virheitä ja loukkaa yksityisyyttä. Tunnistusohjelmistojen virhealttius johtaa väistämättä sellaisenkin sisällön valvontaan, joka ei ole CSAM:ia. Lisäksi on huomioitava, että olemassa olevan CSAM:in levittäminen on tyypillisesti kuva- tai videopohjaista, kun taas grooming on tyypillisemmin teksti- tai puhepohjaista. Tällaisen sisällön tunnistamiseen ja analysointiin tarvittavat tekniset työkalut ovat väistämättä hyvin erilaisia, mikä asettaa lisähaasteita tunnistamiselle ja teknologioiden käytölle.

Komissio on jo aiemmin ilmoittanut olevansa tietoinen ongelmasta ja arvioinut vaikutustenarvioinnissaan nykyisten groomingia tunnistavien teknologioiden tarkkuudeksi 88 prosenttia. Arvioitu 12 prosentin virhemarginaali on kuitenkin aivan liikaa ja johtaisi siihen, että perustettava EU-keskus joutuisi käsittelemään lukuisia vääriä positiivisia tuloksia. Kun otetaan huomioon päivittäin internetissä jaettavan sisällön runsaus, kaikki muu paitsi täydellinen tarkkuus tarkoittaisi, että suuri määrä täydessä yhteisymmärryksessä täysi-ikäisten nuorten aikuisten kesken jaettua intiimiä sisältöä merkittäisiin CSAM:ksi. Lisäksi toimenpiteet, joissa viranomaisille annetaan yleinen oikeus päästä käsiksi kaikkeen sisältöön groomingin havaitsemiseksi, estävät Euroopan unionin perusoikeuskirjan 7 artiklassa (yksityiselämän suoja), 8 artiklassa (henkilötietojen suoja) ja 11 artiklassa (sananvapaus) taattujen oikeuksien toteutumisen.

Suomessa eduskunnan perustuslakivaliokunta on lausunnossaan PeVL 53/2022 vp todennut, ettei sääntely vaikuta ongelmattomalta perustuslain 10 §:n 4 momentin kannalta. Samoihin ongelmiin kiinnittivät huomiota myös liikenne- ja viestintäministeriö sekä Liikenne- ja viestintävirasto Traficom. Lisäksi eurooppalaiset toimialajärjestöt Alliance Française des Industries du Numérique, CISPE.cloud, CCIA Europe, CZ.NIC, Developers Alliance, DOT Europe, Eco, EuroISPA, FiCom, Freedom Internet, I2Coalition, ISPA Austria ja ITI ovat 6.9.2023 julkaisseet yhteisen lausunnon, jossa ne pyytävät Euroopan komissiota varmistamaan viestinnän salauksen sekä muuttamaan tunnistamismääräystä koskevia kohtia.

U-jatkokirjeen sekä FiComin saamien tietojen mukaan asetusehdotuksen neuvotteluissa ei ole toistaiseksi esitetty merkittäviä muutoksia tunnistamismääräystä koskevaan sääntelyyn. Kuten jatkokirjeessäkin on todettu, ehdotettu sääntely kohdistuisi myös viestinnän sisältötietoihin, eikä se kaikilta osin rajoittuisi rikollisen toiminnan havaitsemiseen. Sääntelyllä puututtaisiin rikoksesta epäillyn tai potentiaalisesti rikokseen syyllistyvän henkilön lisäksi niin lapsen kuin myös sivullisten henkilöiden yksityiselämään sekä henkilötietojen ja viestin salaisuuden suojaan. Tunnettuun CSAM:n kohdistuvat tunnistamismääräykset ovat ymmärrettäviä, mutta tuntemattoman CSAM:n havaitsemisen tulisi olla vapaaehtoista, ilman palveluntarjoajiin kohdistuvaa vastuuta. **Suomen ei tule hyväksyä perus- ja ihmisoikeusvelvoitteiden vastaista sääntelyä tunnistamismääräyksestä.**