Eduskunta
Liikenne- ja viestintävaliokunta

14.10.2024

# Lausunto asiaan U 69/2022 vp Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä

Kiitän kutsusta asiantuntijaksi ja mahdollisuudesta lausua Valtioneuvoston kirjelmään Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä. Asetuksen aihe on tärkeä ja lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa tulee parantaa nykyisestä merkittävästi. Valitettavasti nykyisessä muodossaan asetus ei tule onnistumaan tavoitteissaan.

Tässä lausunnossa keskityn erityisesti kokouksen liitteenä olevan sisäministeriön kokousmuistion asioihin, joilla Suomen kantaa otsikossa mainittuun Euroopan komission ehdotukseen perustellaan.

Muistiossa todetaan tunnistamismääräyksen rajauksesta seuraavaa *”Tunnistamismääräys on kohdennettu vain tunnettuun CSA-materiaaliin, jonka tunnistamisen osalta teknologiat ovat lähes täydellisiä.”* Tämä väite on hyvin erikoinen tunnetun tutkimustiedon valossa. On totta, että tunnetun materiaalin tunnistaminen oikein voi onnistua liki 100% todennäköisyydellä. Kuitenkin tämän esitetyn teknologian ongelmat eivät ole tässä, vaan virheellisissä tunnistuksissa (väärä positiivinen, false positive) eli tilanteissa, missä viaton materiaali tunnistetaan virheellisesti CSA-materiaaliksi. Jotkin tahot ovat esittäneet, että tähän olisi lähes virheettömiä menetelmiä, jotka kykenisivät jopa vain yhteen virheelliseen tunnistukseen triljoonasta (Microsoftin PhotoDNA). Kuitenkin tutkimus on osoittanut, että tätä väitettä PhotoDNA:han liittyen ei ole voitu varmentaa. Virhemarginaalit realistisilla parametrien arvoilla ovat edelleen tuhannesosien ja prosenttien luokkaa, mikä tekee niistä täysin käyttökelvottomia nykyisen viestinnän skaalalla (miljardeja viestejä päivittäin). [1]

Lisäksi on huomattava, että tunnetaan monia menetelmiä, joilla esimerkiksi kuvia voidaan muokata esitetyn kaltaisen tunnistamisjärjestelmän huijaamiseksi. Tämä tarkoittaa, että ihmissilmälle näkymättömillä muutoksilla voidaan tunnistamismenetelmä saada tekemään väärä tunnistus [2]. Tällaista ominaisuutta voidaan käyttää kahdella tavalla. Ensinnäkin kuvia voidaan muokata niin, että tunnistamisalgoritmi ei enää tunnista kuvaa CSA-

**Oulun yliopisto**

PL 8000
90014 Oulun yliopisto

oulun.yliopisto @ oulu.fi
Puh 0294 480 000
Fax 08 344 064

www.oulu.fi

materiaaliksi, vaikka se sitä olisikin. Ja toisaalta ihan tavallisista kuvista voidaan muokata sellaisia, jotka menetelmä tunnistaa virheellisesti CSA-materiaaliksi. Molemmissa tapauksissa luottamus järjestelmän toimintaan heikkenisi merkittävästi.

Toinen kohta muistiossa toteaa *”CSA-materiaalin tunnistusta voitaisiin tehdä ainoastaan visuaaliseen sisältöön”*. Tämä osoittaa todella huonoa ymmärrystä viestintäteknologioiden toiminnasta ja siitä, mitä tämä tarkoittaa esitetyn kaltaisen sisällön valvontamenetelmän kiertämiseksi. Lähtökohtaisesti kaikki viestintädata digitaalisissa laitteissa on ”vain” bittejä, ykkösiä ja nollia, ilman sen suurempaa merkitystä. Ohjelmistolle annettu ohjeistus näiden bittien tulkinnasta muodostaa sitten halutun lopputuloksen eli vaikkapa kuvan, äänen tai tekstitiedoston. On täysin triviaalia ottaa yhdellä tapaa tulkittu bittijono (esim. CSA-materiaalia sisältävä kuva) ja antaa sille ohjelmallisesti toinen tulkinta (äänitiedosto). Tällaisen tiedoston voi sitten lähettää vapaasti missä viestimessä tahansa, koska sisällön tarkistaminen ei koskisi tätä mediaa. Tämän jälkeen vastaanottaja voi tehdä vastaavan muutoksen äänestä kuvaksi.

Kuten muistiossa myös todetaan, tällä hetkellä tekstin ja äänen suhteen ei tunneta toimivia menetelmiä sisällön skannaamiseksi. Vaikka tällaiset menetelmät saataisiin luotua, ei skannauksen kiertämiseen edelleenkään tarvittaisi muuta kuin sopiva, paikallisesti viestintälaitteessa toimiva salausohjelmisto. Tällä salausohjelmistolla haluttu CSA-materiaali salattaisiin ja sen jälkeen se lähetettäisiin viestimellä eteenpäin. Skannaus ei voisi tunnistaa tätä viestiä miksikään tunnetuksi CSA-materiaaliksi, koska se olisi salattu jo ennen skannaamista. Eikä tämä riipu siitä, onko lähetettävä data kuvaa, tekstiä tai jotain muuta. Tämän tyyppisiä, esimerkiksi sähköpostien salaamiseen tarkoitettuja ohjelmia on ollut olemassa ja saatavilla jo ainakin 1990-luvulta saakka.

Teknologisen näkökulman lisäksi ehdotettuun asetukseen liittyy myös muita ongelmia.

Muistiossa todetaan ja asetuksessa esitetään, että tätä seulontaa tehtäisiin vain tiettyjen ehtojen täyttyessä ja että tähän täytyisi viestipalvelun loppukäyttäjän vielä itse suostua. Nykyisessä digitaalisessa yhteiskunnassa, jossa valtaosa kanssakäymisestä ja viestinnästä tapahtuu yksityisten viestipalvelujen kautta ja lisäksi sisältää kuva- ja videomateriaalia, tämä käytännössä tarkoittaa lähes kaikkien ihmisten asettamista epäilyksen alle. Mikäli joku jättää suostumuksensa antamatta tälle skannaukselle, hänen mahdollisuutensa osallistua yhteiskunnan toimintaan ja normaaliin sosiaaliseen kanssakäymiseen heikkenevät merkittävästi.

Mikäli asetuksen mukainen vaatimus sisällön etukäteisskannaamisesta asetetaan ja siihen kykenevä teknologia tulee osaksi keskeisiä viestintäpalveluita, ainoa este tämän kyvykkyyden käyttämisestä muihin tarkoituksiin on lainsäädännöllinen. Sisäministeriön muistiossakin todetaan, että skannaaminen halutaan laajentaa tekstiin ja ääneen heti kun teknologia sen mahdollistaa. Monissa muissa maissa EU-alueen ulkopuolella (ja ehkä jopa sisälläkin) odotetaan tällaista mahdollisuutta vesi kielellä. Autoritäärisissä maissa tullaan varmasti säätämään lakeja, jotka laajentavat tätä skannaamista kyseiselle hallinnolle epäedulliselle materiaalille [3] Tämä tulee johtamaan

sananvapauden heikkenemiseen entisestään sekä inhimilliseen kärsimykseen niille, jotka tällä tavoin saadaan kiinni noiden hallintojen toimesta.

Edelleen kyseessä on myös merkittävä arvovalinta. CSA-materiaalin levittämiseen ja käyttämiseen liittyen on tehty tutkimuksia ja ne eivät tue erityisesti asetuksessa esitettyä sisällön etukäteisskannaamista toimivana menetelmänä ehkäisemään tätä ongelmaa. Monet tutkimuksissa todetuista toimivista keinoista, kuten paremmat mielenterveyspalvelut sekä mahdollisuudet hakeutua ja päästä hoitoon matalalla kynnyksellä eivät ole lähtökohtaisesti teknologisia, vaikka voivat teknologiasta kyllä hyötyä [4]. Lisäksi iso osa jo nykyisillään raportoiduista tapauksista jää tutkimatta [3] oletettavasti poliisien ja muiden viranomaisten resurssien puutteen vuoksi. Koska nämä toimivat vaihtoehdot saattavat vaikuttaa vaikeilta toteuttaa ja ennen kaikkea kalliilta yhteiskunnalle, on houkuttelevaa ajatella, että teknologinen sääntely korjaisi nämä ongelmat ”helpommin” ja ”halvemmalla”. Kuten edellä on esitetty, asetuksessa esitetty teknologinen ratkaisu ei kuitenkaan ratkaise tätä ongelmaa. Näin ollen arvovalinta on tutkitusti toimivien, mutta vaikeiden ja kalliiden, ja tutkimustiedon valossa todennäköisesti toimimattomien, mutta halpojen ja helppojen, menetelmien välillä.

Vielä lopuksi on nostettava esiin myös esitetyn järjestelmän mahdolliset epätoivottavat kannustinvaikutukset CSA-materiaalia tuottavien rikollisten suuntaan. Mikäli järjestelmä voi tunnistaa vain jo tunnettua CSA-materiaalia, tämä luo kannustimen tuottaa mahdollisimman paljon uutta ja ennennäkemätöntä materiaalia. Tällaista materiaalia kun esitetyn kaltainen järjestelemä ei voi tunnistaa. Koska CSA-materiaaliin liittyy paljon ammattimaista rikollisuutta, tällaiset kannustimet vaikuttavat näiden rikollisten toimintaan tavalla, joka ei edistä asetuksen hyviä tarkoitusperiä.

Laajemmin koko asetusta kohtaan esitettyä kritiikkiä suosittelen katsomaan avoimesta kirjeestä, jonka on allekirjoittanut jo liki 400 tutkijaa ympäri maailman. Siinä tuodaan esille edellä mainittujen asioiden lisäksi myös muita näkökohtia, joiden perusteella esitettyä asetusta ei tule sellaisenaan hyväksyä. [5]

Oulussa 14.10.2024

Kimmo Halunen

Digitally signed by Kimmo Halunen
DN: cn=Kimmo Halunen, c=FI, o=ITEE, ou=BISG, email=kimmo.halunen@oulu.fi
Reason: I am the author of this document
Date: 2024.10.14 18:56:01 +03'00'

Kimmo Halunen

kyberturvallisuuden professori

Oulun yliopisto ja Maanpuolustuskorkeakoulu

Lähteet:

[1] Steinebach, Martin. "An analysis of photodna." *Proceedings of the 18th International Conference on Availability, Reliability and Security*. 2023.

[2] Hao, Qingying, et al. "It's not what it looks like: Manipulating perceptual hashing based applications." *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. 2021.

[3] Jussi Erosen kolumni: Whatsapp-viestisi syyniin? EU-komissio esittää poikkeuksellista massavalvontaa, https://yle.fi/a/74-20115616

[4] Nurmi, Juha, et al. "Investigating child sexual abuse material availability, searches, and users on the anonymous Tor network for a public health intervention strategy." *Scientific Reports* 14.1 (2024): 7849.

[5] Joint statement of scientists and researchers on the Proposal for the Child Sexual Abuse Regulation (9 September 2024), https://homes.esat.kuleuven.be/~preneel/Open_letter_CSAR_aug24_still_unacceptable.pdf