TIETOSUOJAVALTUUTETUN TOIMISTO

Lausunto

TSV/10200/2024

6.11.2024

Perustuslakivaliokunta
PeV@eduskunta.fi

U 69/2002 vp

Lausunto sisäministeriön lausunnosta 30.10.2024 asiaan U 69/2022 vp ja puheenjohtajamaa Unkarin tuoreimpaan kompromissiehdotukseen

Eduskunnan perustuslakivaliokunta on pyytänyt tietosuojavaltuutetun lisälausuntoa asiassa ”Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisystä ja torjunnasta (U 69/2022 vp)” koskien sisäministeriön lisäselvityksessä kerrotun vaikutuksesta tietosuojavaltuutetun aiemmin lausumaan.

Lausunto

Sisäministeriön tarkentava selvitys esittää, että CSAM-ehdotukseen sisältyvää tunnistamismääräystä voidaan käyttää kertaalleen rikolliseksi tunnistetun CSA-materiaalin tunnistamiseen lukematta läpivalaistavan kuvan merkityssisältöä sekä kuvailee voimassa olevan tilapäisen ePrivacy-poikkeussääntelyn oikeustilaa.

Sisäministeriön esitys ei tietosuojavaltuutetun näkemyksen mukaan tuo keskusteluun sellaista uutta tietoa, mikä edellyttäisi tietosuojavaltuutettua uudelleen arvioimaan aiemmin esittämäänsä. Tietosuojavaltuutettu esittää aiemmin lausumansa lisäksi seuraavat CSAM-asetusehdotusta koskevat huomiot.

Aluksi on todettava, että sisäministeriön lausunnossa esitetty ei koske yksinomaan tilanteita, joissa henkilötietoja käsitellään tunnistamismääräyksen antamista koskevassa tilanteessa. Asian arvioinnissa on keskeistä erottaa tilanteet, joissa kyse on viranomaisten toimivaltuuksien käyttämisestä niistä tilanteissa, joissa kyse kaupallisen toimijan tuotekehittelystä.

Sisäministeriön lausunnossa kertoma ei muuta sitä, että puheenjohtajamaa Unkarin kompromissiesitys rakentuu sen lähtökohdan varaan, että tunnistamismääräys koskee kohdentamatonta ja laajaa joukkoa palveluntarjoajan asiakkaita, eli esimerkiksi Signalin tai WhatsAppin käyttäjiä. Kyse näyttäisi olevan siitä, tuleeko skannattujen kuvien merkityssisällölle antaa merkitystä arvioitaessa sitä, koskeeko tunnistamismääräys kohdentamatonta ja laajaa joukkoa palveluntarjoajan asiakkaita.

Lähtökohtaisesti teknologianeutraalin ehdotuksen tunnistamismääräyksen antamista koskeva sääntely nojaa nykymuodossaan tiivistefunktioiden tuottamien tunnisteiden (”hash”) vertailuun. Tiivistefunktiota käytettäessä tiivistealgoritmi lukee kuvan läpikotaisin ja pyrkii tuottamaan siitä typistetyn, mahdollisimman täydellisesti lähtömateriaalia kuvaavan, sormenjälkeä vastaavan, tunnisteen siinä tarkoituksessa, että kuva voidaan tunnistaa CSA-materiaalia sisältäväksi kuvaksi. Tiivistefunktiot mielletään lähtökohtaisesti yksisuuntaisina toimenpiteinä, joita on hyvin vaikeaa kääntää, mutta on huomioitava että kuvasta muodostetusta hash-tunnisteesta voidaan palauttaa merkityksellistä tietoa alkuperäisen kuvan hahmoista ja asetelmista. Perustuslakivaliokunnalle annettu lisäselvitys esittää, että hash-arvojen vertailuun perustuvaa tunnistamismenettelyä voitaisiin käyttää lukematta kuvan merkityssisältöä.

Tietosuojavaltuutetun toimisto on usein kohdannut kysymyksen siitä, onko henkilötietoon kohdistuva toimenpide henkilötietojen käsittelyä, jos se toteutetaan hyvin nopeasti tai koneellisesti. Nämä seikat eivät kuitenkaan vaikuta arvioon siitä, onko kyse henkilötietojen käsittelystä. Tietosuojavaltuutettu toteaa, että vastaavasti kysymys siitä, kuinka paljon viestintäsalaisuutta loukataan, jos viesti avataan ja luetaan koneellisesti viranomaisen määräyksestä, ei eroa merkittävästi siitä, että viranomainen katsoo kuvan, muttei ilmaise tai käytä hyväksi näkemäänsä muuten kuin toteamalla onko kuva identtinen kielletyn kuvan kanssa. Viranomaisen toiminnan asianmukaisuuteen tulee voida lähtökohtaisesti luottaa. Näin ollen sanotulla seikalla ei tietosuojavaltuutetun näkemyksen mukaan ole ratkaisevaa merkitystä arvioitaessa, onko kyse toimenpiteestä, jota voidaan pitää oikeasuhtaisena ja tarkkarajaisena perustuslain perusoikeuksien rajoittamista koskevien vaatimusten[1] edellyttämällä tavalla.

Sisäministeriö on lausunnoissaan nostanut esiin PhotoDNA-nimisen teknologian, joka tietosuojavaltuutetun ymmärryksen mukaan ei ole julkinen eikä sen toimintaa ole ehdotuksessa esitelty tai arvioitu. Tietosuojavaltuutettu kiinnittää huomiota siihen, että PhotoDNA-teknologian julkisuuteen vuotaneen algoritmin tehokkuutta on tutkittu mm. arvostetussa Fraunhofer-instituutissa[2]. Tutkinnassa on havaittu, että CSA-kuva on helposti muokattavissa PhotoDNA-teknologialle tunnistamattomaksi pelkästään jokaisen modernin matkapuhelimen sisäänrakennettua kuvienkäsittelysovellusta käyttäen, ennen kuvan avaamista viestintäsovelluksessa sen lähettämistä ja läpivalaisua varten. Tietosuojavaltuutettu toteaa, että PhotoDNA:n soveltuminen käytettäväksi tunnistamismääräystä annettaessa edellyttäisi kattavampaa vaikutustenarviointia ottaen myös huomioon teknologioiden pakotetun käyttöönoton vaikutukset viestintäpalvelujen tietoturvallisuudelle. Kyse on merkittävästi digitaalisten yhteiskunnan perusrakenteisiin vaikuttavasta asetusehdotuksesta, joten teknistä asiantuntija-arvioita ei voida perustaa olettamiin, joiden paikkansapitävyyttä ei voida itsenäisesti tietopohjaisesti todentaa, tai odotuksiin tulevaisuudessa keksittävistä teknologioista.

[1] PeVM 25/1994 vp, s. 4–5. https://www.eduskunta.fi/FI/vaski/Mietinto/Documents/pevm_25+1994.pdf
[2] Steinebach, M. An Analysis of PhotoDNA, Fraunhofer SIT/ATHENE. https://doi.org/10.1145/3600160.3605048

TIETOSUOJAVALTUUTETUN TOIMISTO

PhotoDNA:lla tuotettuja hash-tunnisteita on myös rajoitetusti pystytty palauttamaan takaisin kuviksi koneoppimisen menetelmin[3][4]. Ehdotuksen mukaiset hash-tunnisteet sisältävät siis tietoa alkuperäisen kuvan ”merkityssisällöstä” ja tunnisteiden käsittely ja hallinnointi on näin ollen myös suojattava huolellisesti.

Tietosuojavaltuutettu painottaa, että yksityisten viestintäpalvelujen tarjoajien vapaaehtoista CSAM vastaista toimintaa ei voi rinnastaa toimintaan, jota viestintäpalvelu suorittaisi viranomaisen määräyksestä viranomaisen tarpeisiin. Viranomaisen toimivallan tulee aina perustua lakiin ja olla tarkkaan määritelty. Yksityisillä toimijoilla on sitä vastoin enemmän harkintamarginaalia sen kehittäessä omaa palveluaan. Lisäksi on otettava huomioon, että yksityisten toimijoiden tarpeisiin kehitetyt teknologiat voivat osoittautua viranomaistoimintaan sopimattomiksi.

Lisäksi on todettava, että esitetyt lisäselvitykset eivät vaikuta tietosuojavaltuutetun aiemmin lausumaan tunnistamismääräystä koskevasta suostumuksesta. Kuten asiassa on aiemmin todettu, tulisi käsittelystä säätää lailla nykyistä ehdotusta tarkkarajaisemmin.

Lopuksi tietosuojavaltuutettu vielä toteaa, että valiokuntakuulemisten yhteydessä on esitetty kysymys siitä, miten tunnistamismääräyksen yhteydessä käytettävä hash-arvojen vertailu eroaa virus- ja haittaohjelmien torjuntasovellusten tekemästä haitallisen ohjelmakoodin hash-arvojen vertailusta. Tietosuojavaltuutetun käsityksen mukaan ilmeisin eroavaisuus on virustorjuntatoimien todellisessa vapaaehtoisuudessa – käyttäjä haluaa ja päättää itse suojata tietojärjestelmiään ja on vapaa valitsemaan haluamansa toimittajan ja käyttämänsä teknologian omien mieltymystensä mukaisesti, ja siinä, että virustorjunnassa käytettävät tunnisteet ovat julkisia ja vapaasti asiantuntijoiden tarkasteltavissa, eivätkä ne sisällä tai ole muodostettu käyttäjän tiedoista. Koska rikolliseksi todetun CSA-materiaalin tunnisteita voidaan käyttää rikollisen aineiston levittämiseen ja levittämisen vastaisten läpivalaisutoimenpiteiden kiertämiseen, estetään käyttäjältä pääsy ja näkyvyys omassa tietojärjestelmässään käsiteltäviin CSAM-tunnisteisiin, toisin kuin virustunnisteiden kanssa toimitaan. Virustorjunnan käyttäjä voi myös itse päättää miten mahdollisiin virustorjuntaohjelmiston hälytyksiin reagoidaan ja halutessaan luopua virustorjunnasta.

Allekirjoitus

Anu Talus
Tietosuojavaltuutettu

Lauri Karppinen
IT-erityisasiantuntija

[3] Athalve, Anish. Inverting PhotoDNA. https://anishathalye.com/inverting-photodna/
[4] Prokos, Jonathan el al. Evaluating Perceptual Hashing with Machine Learning, Proceedings of the 32nd USENIX Conference on Security Symposium. https://eprint.iacr.org/2021/1531