Sisäministeriö
Inrikesministeriet

Lausunto 30.10.2024

Pekka Vasara
SM/PO

Perustuslakivaliokunta
Sisäministeriön lausunto asiaan U 69/2022 vp ja puheenjohtajamaa Unkarin tuoreimpaan kompromissiehdotukseen

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)

Perustuslakivaliokunta on pyytänyt sisäministeriöltä tarkentavaa selvitystä koskien asetusehdotusta lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (ns. CSAM-ehdotus). Valiokunta on pyytänyt erityisesti tietoa siitä, voidaanko CSAM-ehdotukseen sisältyvää toimenpidettä (tunnistamismääräys) käyttää kertaalleen rikolliseksi tunnistetun lapsiin kohdistuvan seksuaaliväkivaltamateriaalin tunnistamiseksi lukematta kuvan merkityssisältöä. Lisäksi valiokunta on pyytänyt selvitystä nykyisestä oikeustilasta (tilapäinen ePrivacy-poikkeusasetus, joka mahdollistaa viestintäpalvelujen vapaaehtoiset toimet ja mahdolliset viranomaisten toimivaltuudet).

Tilapäisen ePrivacy-poikkeusasetuksen ((EU) 2021/1232) tausta ja keskeinen sisältö

Tausta

Numeroista riippumattomien viestintäpalvelujen (kuten sähköposti- ja sanomanvälityspalvelut) tarjoajien sähköisen viestinnän vapaaehtoinen käsittely lasten seksuaalisen hyväksikäytön ehkäisemiseksi verkkoympäristössä on mahdollistettu EU:n laajuisesti vuonna 2021 voimaantulleella direktiivin 2002/58/EY tilapäisellä poikkeuksella (asetus (EU) 2021/1232, jäljempänä *tilapäinen poikkeusasetus*). Tilapäinen poikkeusasetus on sekä ajalliselta kestoltaan että soveltamisalaltaan rajattu, sillä kyseessä on tilapäinen poikkeus eräisiin sähköisen viestinnän tietosuojadirektiivin säännöksiin, joilla mahdollisestaan tiettyjen palveluntarjoajien vapaaehtoset toimet haitallisen materiaalin havaitsemiseksi ja poistamiseksi. Asetuksen soveltamisen oli määrä loppua viimeistään vuonna 2024, mutta pysyvää sääntelyä koskevien neuvottelujen venyessä tilapäisen poikkeusasetuksen soveltamisalaa päätettiin jatkaa huhtikuuhun 2026 asti.

Komissio antoi keväällä 2022 esityksen pysyväksi sääntelyksi eli CSAM-ehdotuksen. Komission esityksen mukaan tilapäinen poikkeusasetus on ollut tarkoitus kumota nyt neuvoteltavana olevalla asetusehdotuksella, mutta nykyisen puheenjohtajamaan kompromissiesityksen mukaisesti vapaaehtoista sääntelyä olisi tarkoitus osin jatkaa uuden CSA-materiaalin ja groomingin tunnistamiseksi. Tällä on tarkoituksena varmistaa, että nämä seksuaaliväkivallan muodot tulevat huomioiduksi, kun ne on uudessa CSAM-ehdotuksen kompromissitekstissä rajattu kokonaan ulos velvoittavan tunnistamismääräyksen piiristä. Näin yritykset voisivat samalla kehittää jatkossakin tunnistamiseen tarpeellisia teknologioita.

Valtioneuvoston kantaa tilapäiseen poikkeusasetukseen on käsitelty eduskunnalle toimitetussa U-kirjelmässä U 50/2020 vp. Perustuslakivaliokunta päätti kirjelmän käsittelyn yhteydessä, ettei asian johdosta ryhdytä toimenpiteisiin.

Sisältö

Tilapäisen poikkeusasetuksen 1 artiklan mukaan siinä vahvistetaan tilapäiset ja tiukasti rajatut säännöt eräistä direktiivissä 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi, ns. ePrivacy-direktiivi) säädetyistä velvoitteista poikkeamiselle. Asetus sallii tiettyjen numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajien käyttää erityisiä teknologioita, kuten esim. asetuksen johdanto-osan 7 kohdassa mainittua hash-tiivisteisiin perustuvaa teknologiaa, henkilötietojen ja muiden tietojen käsittelyyn siinä laajuudessa, kuin on ehdottoman välttämätöntä verkossa tapahtuvan lasten seksuaalisen hyväksikäytön havaitsemiseksi ja niiden palveluissa ja siitä ilmoittamiseksi ja kyseisen materiaalin poistamiseksi niiden palveluista. Asetuksen mukaan on mahdollista tunnistaa sekä ns. varmistettua eli tunnettua kuin myös uutta CSA-materiaalia, ja lasten houkuttelua (grooming).

Numeroista riippumattomat henkilöiden väliset viestintäpalvelut on määritelty direktiivissä (EU) 2018/1972. Sillä tarkoitetaan käytännössä esimerkiksi internetin kautta toimivia pikaviestipalveluita ja muita verkon yli toimivia ns. Over the Top –palveluita. Asetusta ei sovelleta ääniviestinnän seulomiseen. Asetuksen 25 johdanto-osan mukaan mitään tässä asetuksessa ei pitäisi tulkita niin, että sillä kiellettäisiin päästä päähän –salaus tai heikennettäisiin sitä. Vapaaehtoinen tunnistaminen ei käytännössä ole koskenut salattua viestisisältöä.

CSAM-ehdotuksessa yrityksiä velvoittava tunnistamismääräys voitaisiin kohdistaa myös päästä päähän salausta käyttäviin palveluihin. Menettelyn tarkoituksena on varmistaa, että yritykset ovat tasa-arvoisessa asemassa suhteessa lainsäädäntöön sekä varmistua, että joistain palveluista ei voisi muodostua turvasatamaa lapsiin kohdistuvan seksuaaliväkivallan välittämiselle. CSAM-ehdotuksen lähtökohta salauksen osalta on sama kuin tilapäisessä asetuksessa eli päästä päähän salausta ei kielletä. Laitteella tapahtuva seulonta – jonka teknologista toteutusta on kuvattu alempana – ei estä viestinnän päästä päähän salauksen käyttöä.

CSAM-ehdotuksen tapaan poikkeusasetuksessa on asetettu varsin tiukat edellytykset henkilötietojen ja muiden tietojen käsittelylle sekä vaatimuksia tällaiseen käsittelyyn käytettävälle teknologialle ja tähän poikkeusasetukseen nojautuville palveluntarjoajille. Suhteellisuus- ja välttämättömyysvaatimuksiin on kiinnitetty huomiota esimerkiksi vaatimalla, että käsittelyn on oltava oikeasuhtaista ja sen on rajoituttava ehdottoman välttämättömään asetuksen tarkoitukseen nähden.

Poikkeusasetuksen 3 artiklan 1 kohdan b alakohdan mukaan käytettävien teknologioiden tulee edustaa alan viimeisintä teknistä kehitystä ja niiden on oltava yksityisyyttä mahdollisimman vähän loukkaavia. Viestien tekstin seulomiseen käytettynä niillä ei tule voida päätellä viestien varisnaista sisältöä vaan ainoastaan havaita mahdolliseen verkossa tapahtuvaan lasten seksuaaliseen hyväksikäyttöön viittaavia toimintamalleja. Käytettyjen teknologioiden tulee olla riittävän luotettavia ja tunnistettaessa lasten seksuaalisiin tarkoituksiin houkuttelemista tulee käyttää vain keskeisiä indikaattoreita ja objektiivisesti määriteltyjä riskitekijöitä.

Poikkeusasetukseen sisältyy vaatimus palveluntarjoajille varmistaa ihmisen suorittama valvonta teknologioiden käytössä henkilötietojen ja muiden tietojen käsittelyyn, ottaa käyttöön menettelyt ja oikaisumekanismit sen varmistamiseksi, että yksittäiset henkilöt voivat tehdä valituksia ja ottaa käyttöön sisäiset menettelyt väärinkäytösten estämiseksi (3 artiklan 1 kohdan g alakohta). Erityisesti ihmisen suorittama valvonta ennen viranomaiselle ilmoittamista tulisi toteuttaa silloin, kun tunnistetaan ns. uutta materiaalia tai lasten houkuttelua.

Poikkeusasetuksen 6 artiklan mukaan EU:n yleisen tietosuoja-asetuksen (EU) 2016/679 mukaisesti nimetyt valvontaviranomaiset valvovat tilapäisen poikkeusasetuksen soveltamisalaan kuuluvaa tietojen käsittelyä. Lisäksi tilapäisessä poikkeusasetuksessa on sääntelyä koskien tietojen raportointia niin yritysten, jäsenvaltioiden kuin komissionkin toimesta.

Tilapäinen poikkeusasetus ei sisällä viranomaisia koskevaa toimivaltuussääntelyä, vaan toimivaltuus rikosten tutkimiseksi ja viranomaisen oikeus saada pääsy viestinnän tietoihin yksittäisen rikosepäilyn tilanteessa seuraa kansallisesta sääntelystä.

CSAM-ehdotukseen sisältyvän tunnistamismääräyksen teknologinen toteuttaminen

Tiedostojen tunnistuksessa käytettävien tiivistefunktioiden (hash, hash-arvo) luotettavuus on erittäin korkea käytettäessä tunnettuja tiivistefunktioita. Edellä kuvatun väliaikaisen sääntelyn mukaisesti palvelut hyödyntävät kyseistä teknologiaa jo nyt lapsiin kohdistuvan seksuaaliväkivallan ja siitä todistavan kuvamateriaalin tunnistamiseen. Samaa tekee myös kansalliset lainvalvontaviranomaiset sekä mm. Interpol.

Pelkästään tiedoston ominaisuuksiin perustuvalla hash-vertailulla on tunnetut heikkoutensa, mutta nykyään suurimpien palveluntarjoajien käyttämät teknologiat ovat aiempia tarkempia ja kykenevät luotettavasti ohittamaan kuviin tehdyt pienimmät muutokset vertailemalla teknisten tunnistetietojen samankaltaisuuksia. Osa suurimmista palveluntarjoajista käyttää Microsoftin vuonna 2009 kehittämää PhotoDNA -vertailua ja mm. sosiaalisen median yhtiö Meta on edelleen kehittänyt tätä

teknologiaa. Hash-arvojen vertailuun perustuvan tunnistustoimenpiteen luotettavuudesta ja toimivuudesta todistaa joidenkin yritysten jo nyt suorittama lapsiin kohdistuvan seksuaaliväkivallan torjunta, joka on perustunut edellä kuvattuun poikkeusasetukseen. Maailmanlaajuisesti vuonna 2023 ilmoitettiin 36 miljoonasta epäillystä lapsiin kohdistuvista verkkovälitteisistä seksuaalirikoksista.

Perustuslakivaliokunnan esittämään tekniseen kysymykseen voidaan todeta vastaukseksi, että hash-arvojen vertailuun perustuvaa tunnistamismenettelyä voidaan käyttää lukematta kuvan merkityssisältöä. Toimenpiteen pohjalta palveluntarjoaja saa tiedon, että sisältääkö kuva tunnistetietokannan mukaista sisältöä. Vastaus olisi siis joko kyllä (sisältää etsittävää materiaalia) tai ei (ei sisällä etsittävää materiaalia), eikä varsinaisesti viestin sisällöstä saada muuta tietoa.

Vain osumatilanteissa tarkastellaan semanttista sisältöä eikä semanttisen sisällön tarkastelu massavalvonnan luonteisesti ole tarpeellista tai edes mahdollista kaikkien palvelun kautta välitettävien visuaalisen sisällön osalta. Kun teknologia on todettu luotettavaksi, ja itse sisältö on lainvastaiseksi jo todettua, puuttumista on pidettävä oikeasuhtaisena. Toimintalogiikka CSAM-ehdotuksen tunnistamismääräyksessä on siis sama kuin nykyisissä käytänteissä (väliaikainen asetus), joita on avattu edellä.