Sisäministeriö
Inrikesministeriet

Lausunto 21.10.2024

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 sisäministeriön lausuntoa koskien asetusehdotusta lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (ns. CSAM-asetusedotus) ja eduskunnalle asetusehdotuksen neuvottelutilannetta koskevasta lisäselvityksestä. Lausunnossaan sisäministeriö tarkastelee ehdotettua kompromissia – ja erityisesti siihen sisältyvää tunnistamismääräystä – EU-oikeuden ja perustuslain näkökulmasta perustuslakivaliokunnan aiemman lausunnon valossa. (PeVL 5/2023 vp)

Sisäministeriö jakaa perustuslakivaliokunnan näkemyksen siitä, että asetusehdotus olisi uudenlaista EU-sääntelyä erityisesti siltä osin, että siitä voisi seurata palveluntarjoajille velvollisuus käsitellä henkilöiden välistä viestintää rikollisen materiaalin tunnistamiseksi ilman viranomaisen vahvistamaa tietyn henkilön liityntää selvitettävään tai ehkäistävään rikollisuuteen. Samalla sisäministeriö kiinnittää huomiota ehdotukseen tehtyihin muutoksiin ja katsoo, että luottamuksellisen viestin salaisuuden suojaan puuttumista on kohdennettu ja rajattu aiemmasta mm. seulottavaa sisällön kaventamisella sekä lisätyillä suojatakeilla, joita on esitelty yksityiskohtaisesti aiemmin toimitetussa lisäselvityksessä.

Tiettyjen perusoikeuksien rajoituksia (yksityiselämän suoja ja henkilötietojen suoja) tulisi arvioida vakiintuneen oikeuskäytännön mukaan suhteessa niiden tehtäviin yhteiskunnassa. Myös perustuslakivaliokunta on painottanut, että yksityiselämän ja henkilötietojen suoja tulee suhteuttaa toisiin perus- ja ihmisoikeuksiin sekä muihin painaviin yhteiskunnallisiin intresseihin, kuten esimerkiksi yleiseen turvallisuuteen liittyviin intresseihin, jotka voivat ääritapauksessa palautua henkilökohtaisen turvallisuuden perusoikeuteen (viittaus PeVL 5/1999 vp, s. 2/II). Lainsäätäjän tulee turvata yksityiselämän ja henkilötietojen suoja tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Valiokunta on painottanut, että yksityiselämän ja henkilötietojen suojalla ei ole etusijaa muihin perusoikeuksiin nähden.

Sisäministeriö katsoo, että ehdotettua sääntelyä arvioitaessa tulee ottaa huomioon laajasti tunnistamismääräykseen liittyvät olosuhteet alkaen erittäin painavista velvoitteista lasten tehokkaaksi suojelemiseksi. Sääntelyehdotuksen kannalta on oleellista huomioida, että kyseessä olevat erittäin vakavat rikokset ja niistä johtuvat yhtä vakavat lasten perusoikeuksien loukkaukset liittyvät luonnostaan rikoksentekijöiden verkossa harjoittamaan toimintaan. CSA-rikollisuuden kasvava määrä osoittaa, että nykyiset torjuntakeinot eivät ole olleet riittäviä. Tämän tyyppiseen rikollisuuteen voidaan puuttua tehokkaasti vain ottamalla mukaan verkkopalvelujen

tarjoajat, mukaan lukien henkilöiden väliset viestintäpalvelut. CSA-rikollisuuden ”piilevä” luonne eroaa verkon ulkopuolella voimakkaammin näkyvistä rikollisuudenaloista, joiden torjuntaan voi usein olla monia muitakin työkaluja. Lisäksi CSAM-rikokset eroavat myös muista verkossa tehtävistä laittomista toimista, kuten terroristisen propagandan tai tekijänoikeuksia rikkovan tiedostojen jakamisesta. Jälkimmäiset ovat jossain määrin enemmän julkisia pyrkimyksenä viestiä suuremmille henkilöryhmille. CSAM-rikollisuuden tilanteessa pelkkä kuva tai video on itsessään rikos.

Sisäministeriö kiinnittää huomiota lisäselvityksessä esiteltyihin kompromissitekstin muutoksiin ja lisättyihin suojatakeisiin, joiden avulla CSA-rikollisuutta on mahdollista torjua yksityisyyden suojaa kunnioittavalla tavalla välttäen kaiken mahdollisen viestiliikenteen jatkuvan seurannan. PJ-valtion kompromississa yksityisyyttä kunnioittava kohdentaminen tapahtuisi tunnistamismääräyksen moniportaisella prosessilla, riskikohdentamisella sekä teknologioiden toimivuudella.

Kuten toimitetussa lisäselvityksessä on todettu, tunnistamismääräyksessä olisi kyse räätälöidystä määräyksestä, johon sisältyy arvio mahdollisista perusoikeusvaikutuksista, sopivien tekniikoiden saatavuudesta ja toimivuudesta, mahdollisista lisätakeiden tarpeista. Kyse ei siis ole yleisesti ja kaikkiin palveluihin kollektiivisesti sellaisenaan sovellettavasta toimenpiteestä. Tunnistamismääräys voitaisiin kohdistaa vain palveluihin, jotka ovat ennalta määritelty korkean riskin palveluiksi ja silloinkin mahdollisuuksien mukaan palvelun yksilöitävissä olevaan osaan. Artiklassa 5 säädettäisiin mm. siitä, kuinka palvelu tai osa palvelusta voitaisiin luokitella korkean, keskitason tai matalan riskin kategoriaan. Palvelu pystyy arviointien aikana sekä lisäarvioinnin yhteydessä tekemään palveluunsa tai sen osiin muutoksia ja välttää joutumasta korkean riskin järjestelmäksi.

Tunnistaminen olisi ajallisesti rajattu, valvottu ja sisältäisi muutoksenhakua, valittamista ja tiedottamista koskevat määräykset. Tunnistamismääräys annettaisiin vain silloin, kun on mm. palveluntarjoajan toimesta osoitettu, että CSAM:n leviämiselle on merkittävä riski. Tunnistamismääräykset valmistellaan riippumattomien viranomaisten, EU-keskuksen ja kansallisten tietosuojaviranomaisten valvonnassa ja päätöksen antaisi tuomioistuin tai riippumaton hallintoviranomainen. Kaikki nämä viranomaiset ovat oikeudellisesti velvollisia varmistamaan toimien laillisuuden ja perusoikeuskirjan noudattamisen. Päätöksiin voidaan hakea muutosta.

Osa yrityksistä torjuu ja ennaltaehkäisee jo nyt CSA-rikollisuutta vapaaehtoisen sääntelyjärjestelmän puitteissa. Päästä päähän salaamattomissa palveluissa käytetään myös teknologioita erityisesti jo kertaalleen rikolliseksi määritellyn laittoman materiaalin löytämiseksi ja poistamiseksi alustoilta. Myös osa päästä päähän salausta käyttävistä palveluista arvioi alustojensa väärinkäytöksen riskejä ja poistavat niitä käyttäjätilejä, joiden epäillään jakaneen laitonta materiaalia palveluissaan. Tilien poistaminen tällaisissa tapauksissa perustuu monimutkaisiin algoritmeihin, käyttäjien ilmoituksiin, metatietoihin ja muihin saatavilla oleviin tietoihin, kuten profiilikuvien tai ryhmän tietojen analysointiin. Sisäministeriön tietojen mukaan palvelut pitävät usein torjuntakäytänteitään tehokkaina, sillä vain harvat poistettujen tilien toimenpiteistä johtaa käyttäjiltä tuleviin valituksiin ja vaateisiin käyttäjätilin palauttamisesta. Tällainen

palveluiden tekemä tärkeä torjuntatyö ei nykyisellään tarjoa rikostutkinnalle toivottavaa lisäarvoa, sillä tutkinnan kannalta tärkeään viestisisältöön ei päästä käsiksi. CSAM-asetuksessa tämä olisi kuitenkin osa tunnistamismääräyksen toimeenpanon edellyttämää merkittävän riskin määritelmää eli peruste, jonka avulla velvoite voitaisiin kohdistaa esimerkiksi tiettyyn palvelun osaan.

Tunnistamisen toteutusta päästä päähän salatussa verkkoympäristössä on kuvattu aiemmin toimiteussa lisäselvityksessä. Tunnistamisessa voitaisiin toteuttaa vain kertaalleen rikolliseksi määritellystä aineistosta ja ainoastaan EU-keskuksen laatimien ja tarkistaminen indikaattorein avulla. Hash-tunnistetietoihin kohdistuva toimenpide ei kerro henkilön yksityiselämästä, vaan ainoastaan osuma liputetaan. Tunnistamisessa ei ole tarvetta antaa pääsyä kaikkeen päätelaitteella olevaan tietoon tai edes kuvakirjastoon, vaan vain palveluympäristöön siirtyvä aineisto vertailtaisiin.

Sisäministeriö katsoo myös sääntelyn oikeasuhtaisuuden arvioinnin kannalta merkitykselliseksi pöydällä olevaan kompromissiesitykseen lisätyn käyttäjän suostumuksen periaatteen. Sen mukaan käyttäjän tulee antaa suostumuksensa sille, että tunnistamistoimintoa kertaalleen rikollisen materiaalin tunnistamiseksi voidaan käyttää. Vastaavasti jos käyttäjä ei antaisi lupaa kuvien hash-arvojen vertailuun, hän ei voisi lähettää kyseisellä sovelluksella kuvamuotoista materiaalia.

Tältä osin on kiinnitettävä huomiota siihen, olisiko silloin suostumus aidolla tapaa vapaasti annettu. Lisäksi suostumusta koskevan edellytyksen osalta olisi kiinnitettävä huomiota siihen, mikä sen suhde on EU:n yleisen tietosuoja-asetuksen mukaiseen suostumukseen henkilötietojen käsittelyperusteena. Tässä yhteydessä sisäministeriö kiinnittää huomiota Euroopan unionin tuomioistuimen asiassa C-252/21 antamaan ratkaisuun, jonka yhteydessä selvitettiin, voidaanko [Meta Platforms Irelandin] kaltaiselle määräävässä markkina-asemassa olevalle yritykselle antaa pätevällä tavalla, erityisesti yleisen tietoturva-asetuksen vapaaehtoinen suostumus? Euroopan unionin tuomioistuimen ratkaisussa todetaan, että *käyttäjillä on oltava sopimusmenettelyn yhteydessä vapaus kieltäytyä tapauskohtaisesti antamasta suostumustaan erityisiin tietojenkäsittelytoimiin, jotka eivät ole välttämättömiä sopimuksen täyttämiseksi, ilman että heidän on samalla luovuttava kokonaan verkkoyhteisöpalvelun ylläpitäjän tarjoaman palvelun käyttämisestä.* PJ-valtion kompromississa käyttäjä saisi jatka palvelun käyttöä muilta osin, vain kuvia ja videoita ei voisi lähettää. Merkityksellistä on myös, että henkilön ei ole pakko käyttää tunnistamismääräyksen saanutta palvelua, vaan se voi vaihtaa käyttämään muita palveluita.

Sisäministeriö toistaa kantansa, että ehdotusta ja sen yhtä velvoitetta (tunnistamismääräys) arvioitaessa on otettava huomioon tavoitteen yhteiskunnallinen painavuus ja erityisesti sovellettavat rajoitukset ja suojatoimien järjestelmä määräystä annettaessa. Kuten ylempänä todettiin näihin suojatakeisiin kuuluvat: tuomioistuimen tai riippumattoman hallintoviranomaisen tapauskohtaiseen harkintaan perustuvat määräykset; muiden riippumattomien viranomaisten osallistuminen ja valvonta kaikissa vaiheissa; riskien ennakkoarviointi ja lieventäminen; määräykset annetaan vain silloin, kun on objektiivisesti osoitettu, että lasten seksuaalisen hyväksikäytön riski on merkittävä; pakollinen kohdentaminen, tiukat aikarajat; säännöllinen raportointi ja

uudelleentarkastelu; tehokas muutoksenhaku ja valitusten käsittely; tiedottaminen käyttäjille; käytettävää teknologiaa koskevat erityisvaatimukset; käytettäviä indikaattoreita koskevat yksityiskohtaiset suojatakeet sekä komission ohjeista tulevat suojatakeet.

Muuta

Tämänhetkisten tietojen perusteella 27 jäsenmaasta 19 kannattaa PJ-valtion kompromissiehdotusta, ml. Pohjoismaista Ruotsi ja Tanska.