Sisäministeriö
Inrikesministeriet

Lausunto 15.10.2024

Pekka Vasara
SM/PO

Hallintovaliokunta
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)

Käsittely ja jatkokäsittelyn aikataulu

Euroopan komissio antoi 11.5.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ennaltaehkäisemiseksi ja torjumiseksi (jatkossa CSAM-ehdotus). Asetusehdotusta on käsitelty neuvoston lainvalvontatyöryhmän (LEWP) kokouksissa. Ehdotuksen teknisen luonteen sekä tietosuojaan ja luottamuksellisen viestin suojaan liittyvien kysymysten vuoksi sen käsittely on edennyt neuvostossa hitaasti.

Puheenjohtajavaltio Unkari on ilmoittanut tavoitteekseen hyväksyä neuvoston osittainen yleisnäkemys CSAM-ehdotuksesta puheenjohtajuuskaudellaan. Puheenjohtaja on luonnostellut kompromissiehdotuksen tavoitteensa saavuttamiseksi. Käytännössä tavoite osittaisesta yleisnäkemyksestä kattaisi lähes koko ehdotetun sääntelyn, pl. EU-keskuksen sijaintipaikkaa koskevan kokonaisuuden, johon on määrä palata keskusteluissa myöhemmin.

PJ-valtio tiedotti 7.10.2024 järjestettävässä Coreper II –kokouksessa jäsenmaita 10.10.20204 järjestettävän ministerineuvoston käsittelymuodon muutoksesta. PJ-valtion oli määrä järjestää ministerineuvostossa äänestys osittaisesta yleisnäkemyksestä, mutta nyt asiakohta käsitellään tilannekatsauksena. PJ-valtio jatkaa työtä osittaisen yleisnäkemyksen parissa, jatkokäsittelyn aikataulu ei toistaiseksi ole täsmentynyt.

Keskeisimmät muutokset suuren valiokunnan lausunnon (SuVL 7/2023 vp) valossa

Asetuksen keskeisimmät haasteet ovat liittyneet tunnistamismääräykseen (7 artikla), jonka nojalla verkkopalveluntarjoajia velvoitettaisiin tunnistamaan ja torjumaan CSA-materiaalia (CSA, child sexual abuse) alustoillaan, ja erityisesti sen suhteeseen luottamuksellisen viestinnän suojaan. Myös suuren valiokunnan lausunnossa (SuVL 7/2023 vp) on kiinnitetty huomiota tunnistamismääräykseen liittyviin herkkyyksiin ja todettukin, että tunnistamismääräys ei tuolloisessa muodossaan olisi ollut hyväksyttävissä. Eduskunnalle esitelty ratkaisu perustui tuolloisen puheenjohtajamaa Espanjan (syksyllä 2023) pöytäämään ratkaisuun.

PJ-valtio Unkarin pöytäämä – vaikkakin pitkälti Belgian kevään 2024 puheenjohtajuuskauden tuotokseen perustuva – kompromissiteksti on sisällöltään muuttunut eduskunnan valtioneuvostolle lokakuussa 2023 esittämien neuvottelutavoitteita koskevien reunaehtojen mukaisesti.

Tunnistamismääräyksestä on viimeisimpien puheenjohtajavaltioiden, Belgian ja Unkarin, toimesta tehty hyväksyttävämpi rajaamalla sen sovellusalaa mm. seuraavilla tavoilla, joiden voidaan katsoa vastaavan suuren valiokunnan lausunnossaan esille tuomiin huomioihin ja reunaehtoihin.

1) **Tunnistamismääräyksellä voitaisiin tunnistaa vain jo kertaalleen rikolliseksi todettuja kuvia ja videoita sekä URL-osoitteita**. Tunnistamismääräyksen sovellusalasta on siis rajattu pois teksti- tai ääniperustainen grooming ja uusi CSA-materiaali. Kertaalleen rikolliseksi todetun kuva ja videomateriaalin tunnistamista pidetään teknologisesti luotettavana; esimerkiksi komission mukaan tiedossa olevien kuvien ja videoiden tunnistamiseen käytetyn PhotoDNA -ohjelman virhemarginaali on olematon: ohjelma antaa tutkimusten mukaan väärän positiivisen kerran 50 miljardista kerrasta.

Nyt pöydällä olevalla kompromissin pohjalta ei siis voitaisi tunnistaa uutta CSA-materiaalia tai groomingia, Näiden osalta vuonna 2021 voimaantullutta ja vuonna 2024 jatkettua tilapäistä poikkeusta sähköisen viestinnän tietosuojadirektiivin tiettyihin säännöksiin **esitetään kompromissitekstissä jatkettavaksi**, jotta **palveluntarjoajat voisivat jatkaa ko. materiaalin vapaaehtoista tunnistamista ja raportoimista**. Tällä toimenpiteellä pyritään minimoimaan lastensuojelun kannalta negatiiviset vaikutukset groomingin ja uuden CSA-materiaalin jäätyä ulos velvoittavan sääntelyn sovellusalan piiristä. Nämä tunnistamismenetelmät voitaisiin kompromissin pohjalta tehdä velvoittavaksi esimerkiksi kokonaan uudella lainsäädäntöehdotuksella edellyttäen, että teknologinen kehitys tarjoaa riittävän tehokkaita ja perusoikeuksia kunnioittavia tunnistamismenetelmiä. Tähän mahdolliseen uuteen lainsäädäntäehdotukseen otettaisiin kantaa, mikäli sellainen annetaan. Pöydällä olevassa kompromissin mukaan palveluntarjoajat osallistuisivat komission ja EU-keskuksen teknologisen komitean eri tunnistamisteknologioiden kehittämiseen. Tilapäinen poikkeus on lähtökohtaisesti tarkoitettu olemaan voimassa vain määräajan, minkä jälkeen palveluntarjoajilla ei olisi enää mahdollisuutta toteuttaa vapaaehtoisuuteen perustuvia toimenpiteitään verkossa tapahtuvan lasten seksuaaliväkivallan paljastamiseksi, tällaisen aineiston poistamiseksi ja siitä ilmoittamiseksi.

2) Lapsiin kohdistuvaa seksuaaliväkivaltaa sisältävien kuvien ja videoiden **tunnistaminen ei vaatisi pöydällä olevassa kompromississa salausteknologian purkamista eikä heikentäisi ns.**

päästä päähän -salauksessa käytettyä teknologiaa. Kompromississa ei myöskään tehtäisi salauksen käyttöä mahdottomaksi. Pöydällä olevassa kompromississa päästä päähän salattua viestintää käyttävät palveluntarjoajat (esim.WhatsApp, Snapchat, TikTok) olisivat tosiasiallisesti sääntelyn osalta tasa-arvoisemmassa asemassa sellaisiin palveluihin nähden, jotka eivät käytä päästä päähän salausta (esim. Microsoftin peruspalvelut). Tavoitteena on, että lapsiin kohdistuvaa seksuaaliväkivaltamateriaalia ei voisi varauksetta ja vailla kiinnijäämisen riskiä välittää millään alustoilla.

Puheenjohtajan kompromississa hyödynnettäisiin ns. hash-lukuja vertailevia teknologioita. Vertailu perustuisi siihen, että käytettävä palvelu laskee kuvalle tai muulle tiedostolle ns. hash-luvun silloin kun käyttäjä valitsee lähetettävän kuvan puhelimensa galleriasta. Tätä hash-lukua verrattaisiin listaan tunnetusta CSAM:sta. Jos tiedoston hash-luku on tunnetun CSAM-aineiston luku, tulee tästä palveluntarjoajalle ns. osumailmoitus. Palveluntarjoajan tulee raportoida osumasta asetuksessa perustettavalle EU-keskukselle.

Toisin sanoen puheenjohtajavaltion kompromissin mukaisesti tunnistamismääräyksen kohdentuessa päästä päähän salattua viestintää hyödyntävään palveluntarjoajaan, hyödynnettäisiin hash-lukuja vertaavia teknologioita ainoastaan siinä hetkessä, jolloin kuvia tai videoita ladataan laitteelta, esim. kuvagalleriasta, lähetettäväksi – **eli ennen kuin viestin sisältö salautuu**. Hash-lukua käytetään useissa tietokoneiden ja älylaitteiden prosesseissa, ja esimerkiksi virustorjuntaohjelmistot voivat toimia osin samalla perusteella. Huomionarvoista on, että virustorjuntaohjelmistoilla on pääsy usein kaikkeen tietoon laitteilla jatkuvasti toisin kuin yllä kuvatussa tapauksessa, jossa pääsy olisi vain siihen tietoon, jota ollaan lähettämässä.

3) Ehdotettu menetelmä ei myöskään edellytä palvelun käyttöjärjestelmään tehtäviä muutoksia tai vakoiluohjelman tai muiden seurantalaitteiden asentamista esimerkiksi puhelimiin. Tunnistamismääräykseen liittyvät teknologiset ratkaisut toteutettaisiin puhelimessa jo olevan käyttöjärjestelmän kautta. Kun tuomioistuin määräisi palveluntarjoajalle tunnistamismääräyksen, olisi palveluntarjoajan mahdollistettava yllä kuvattu tunnistaminen.

4) Pöydällä olevan kompromissiesityksen mukaan edellä kuvattu **tunnistamismääräyksen toteuttaminen olisi mahdollista vain sillä edellytyksellä, että jokainen käyttäjä antaa palveluntarjoajan ehtojen mukaisesti nimenomaisen suostumuksensa siihen, että ko. tunnistamistoimintoa voidaan palvelussa käyttää.** Jos käyttäjä ei anna lupaa kuvien hash-arvojen vertailuun, hän ei voi lähettää ko. sovelluksella kuvamuotoista materiaalia. Tekstimuotoista materiaalia voisi edelleen lähettää.

5) Lisäksi **tunnistamismääräys kohdennettaisiin vain sellaisiin verkkopalveluntarjoajiin tai niiden osiin, joissa on todettu korkea riski CSA-materiaalin leviämiselle.** Riskin toteaminen perustuisi viranomaisten toimesta tehtävään riskiluokitukseen. Tämän mahdollistamiseksi palveluntarjoajat olisivat velvollisia arvioimaan ja raportoimaan alustansa CSA-materiaaliin liittyvistä riskeistä palveluissaan. Riskiluokitusta on mahdollista tarkistaa.

6) **Tunnistamismääräyksen antaminen** kansallisen tuomioistuimen tai riippumattoman hallintoviranomaisen toimesta **on ehdotetussa kompromissitekstissä viimesijainen keino**, sillä palveluntarjoajille annetaan mahdollisuus torjua CSA-materiaalia alustoillaan, ennen kuin edetään tunnistamismääräyksen antamiseen. Tunnistamismääräys olisi myös rajattu ajallisesti ja pitää sisällään toimenpiteen valvonnan ja raportoinnin. Tunnistamismääräys voidaan antaa kohdennettuna vain palvelun tiettyyn osaan ja se koskee vain ennalta CSA-materiaaliksi vahvistetun materiaalin tunnistamista. Tunnistaminen ei siis olisi yleistä saatikka erottelematonta toimintaa.

Esitetyillä rajausehdotuksilla –säilyttäen samalla kaikki palvelut soveltamisalan piirissä – on varmistettu suuren valiokunnan lausunnossaan edellyttämä asetelma, jossa säädettävien toimenpiteiden tulee olla riittävän tehokkaita ja samalla ennakoitavia oikeassa suhteessa ja välttämättömiä ehdotuksen tavoitteen toteutumiseksi. Suuri valiokunta on valtioneuvoston tavoin painottanut lausunnossaan lapsen edun merkitystä, kun punnitaan ehdotuksen eri artiklojen suhdetta perustuslakiin ja perus- ja ihmisoikeuksiin. Ehdotuksen tavoitteena on suojata lapsia seksuaaliväkivallalta.

Edellä kuvatussa mallissa toteutuu myös suuren valiokunnan edellyttämällä tavalla se, että ehdotetut toimenpiteet eivät johda päästä päähän salauksen tai muiden vastaavien tietoturvatoimenpiteiden yleiseen heikentämiseen tai niiden purkamisen taikka niiden käytön rajoittamiseen ja tätä kautta viestinnän sekä viestintään liittyvien palvelujen tietoturvan ja kyberturvallisuuden tason heikkenemiseen.

Valtioneuvosto jakaa suuren valiokunnan 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. CSAM-asetuksen kohdentaminen päästä päähän salatuissa palveluissa perustuisi palveluiden jo nyt tekemään riskiperustaiseen työhön. Suurimmat tällaisista yrityksistä sulkevat kuukausittain satojatuhansia käyttäjätilejä epäillyn CSA-materiaalin jakamisen vuoksi. Tilien poistaminen tällaisissa tapauksissa perustuu monimutkaisiin algoritmeihin, käyttäjien ilmoituksiin, metatietoihin ja

muihin saatavilla oleviin tietoihin, kuten profiilikuvien tai ryhmän tietojen analysointiin. Palvelut pitävät usein torjuntakäytänteitään tehokkaina, sillä vain harvat poistettujen tilien toimenpiteistä johtaa käyttäjiltä tuleviin valituksiin ja vaateisiin käyttäjätilin palauttamisesta. On tärkeä huomioida, että tällainen palveluiden tekemä tärkeä ennaltaehkäisevä työ ei nykyisellään tarjoa rikostutkinnalle toivottavaa lisäarvoa, sillä viestisisältöön ei päästä käsiksi. CSAM-asetuksessa tämä olisi kuitenkin osa tunnistamismääräyksen toimeenpanon edellyttämää merkittävän riskin määritelmää, jonka avulla velvoite voitaisiin kohdistaa tiettyyn palvelun osaan.

Muuta

Tämänhetkisten tietojen perusteella 27 jäsenmaasta 8 vastustaa ehdotusta – näiden joukossa suuria jäsenvaltioita, joilla suuri painoarvo neuvoston äänestyksissä. Suomen Pohjoismaiset kumppanit Ruotsi ja Tanska tukevat pöydällä olevaa kompromissia.