Sisäministeriö
Inrikesministeriet

Lausunto 26.5.2025

Pekka Vasara
SM/PO

Perustuslakivaliokunta

Sisäministeriön lisäselvitys asiaan UJ 2/2025 vp - 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 lisäselvitystä koskien asetusehdotusta lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (ns. CSAM-ehdotus). Valiokunta on pyytänyt erityisesti tietoa siitä, miten nyt käsillä olevassa kompromissiehdotuksessa viestintään kohdistuvat käsittelytoimenpiteet poikkeavat niistä käsittelytoimista, joita viestintään olisi kohdistettu aikaisemmin ehdotuksessa olleen tunnistamismääräyksen perusteella (ts. onko viesteihin puuttuminen erilaista kuin se olisi aikaisemman ehdotuksen mukaan ollut).

Sisäministeriö vastaa kunnioittavasti seuraavaa:

Viestinnän käsittelytoimenpiteet poikkeavat näissä kahdessa eri asetusehdotus versiossa toisistaan mm. teknisten reunaehtojen, velvoitteiden laajuuden sekä valvontarakenteiden osalta. Nyt käsiteltävänä olevan kompromissitekstin mukainen tunnistaminen perustuisi yritysten omaehtoiseen toimintaan. Aikaisemmissa kompromissiteksteissä taas kyse olisi ollut viranomaisen antaman määräyksen jälkeen seuratusta prosessista ja palveluun lisättävästä ominaisuudesta. Aikaisemmissa kompromissiteksteissä olisi säädetty siitä, missä tilanteissa tunnistamismääräyksen antamisen edellytykset täyttyvät. Sen sijaan nykyisessä kompromississa kyse on nykyisten käytäntöjen jatkamisen mahdollistavasta sääntelystä, jossa keskeistä on asettaa reunaehdot sille, miten viestinnän tietoja olisi mahdollista käsitellä CSA-materiaalin ja groomingin tunnistamiseksi. Molemmissa malleissa tavoitteena on ollut turvata lasten oikeudet siten, että viestinnän luottamuksellisuuteen puuttuminen on suhteellisuus- ja välttämättömyysperiaatteiden mukaista /oikeasuhtaista tavoiteltuun päämäärään nähden.

Sisäministeriö huomioi, että CSAM-asetusehdotuksen eri kompromissiversioissa ei ole säännelty *teknologisesti* sitä, miten luottamukselliseen viestintään puuttuminen tulisi käytännössä palveluntarjoajien toimesta toteuttaa. Menettelyn taustalla on ollut pyrkimys pitää sääntely teknologianeutraalina ja tulevaisuuden vaatimukset huomioon ottavana, sillä palveluiden joukko on rakenteiltaan moninaista ja tunnistamiseen käytettävä teknologia kehittyy. Poikkeuksen muodostaa kuitenkin edelliseen kompromissiin sisältynyt Belgian puheenjohtajakaudella laadittu ehdotus teknisestä toiminnosta eli ns. *upload moderation*, jota voidaan pitää yksityiskohtaisena ja osittain myös teknologiaa koskevana sääntelynä. Ehdotetulla toiminnolla olisi säädetty CSA-materiaalin tunnistamisesta päästä päähän salatussa viestintäympäristössä hash-skannaustekniikkaa hyödyntäen siinä hetkessä, jolloin kuva tai video ladataan laitteelta lähetettäväksi – eli ennen kuin viestin sisältö salataan viestin välittämistä varten. Eduskunta piti upload moderation -toimintoa ongelmallisena. Upload moderation -toiminto ole enää tuoreimmassa kompromissitekstissä mukana. Tunnistamismääräyksen poiston myötä poistuu myös asetusehdotukseen aikaisemmin liittynyt mahdollinen velvollisuus purkaa viestinnän salaus tunnistamismääräyksen noudattamiseksi.

Palveluntarjoajat voivat nykyisessäkin kompromississa nojata käytettävien teknologioiden osalta asetuksella luotavaan EU-keskukseen ja sen tarjoamaan tukeen. Kyseinen asiantuntijakeskus ylläpitää luetteloita saatavilla olevista teknologioista, joita yritykset voivat hankkia, asentaa ja ottaa käyttöön maksutta, jotta voitaisiin vähentää tai estää CSA-materiaalin leviämistä ja lasten houkuttelua. Eduskunnan aiemmin arvioiman kompromissin mukaan yritys olisi tunnistamismääräyksen yhteydessä ollut velvoitettu laatimaan yksityiskohtaisen täytäntöönpanosuunnitelman, jossa olisi esitetty toimenpiteet, jotka se aikoo toteuttaa suunnitellun tunnistamismääräyksen täytäntöön panemiseksi, mukaan lukien yksityiskohtaiset tiedot suunnitelluista teknologioista ja suojatoimista. Tällaista velvoitettua teknologista arviointia ei ole puheenjohtajamaan uusimmassa kompromissiversiossa, joka perustuu tunnistamisen osalta yritysten vapaaehtoiseen toimintaan. Sen sijaan yritysten vapaaehtoisten tunnistamistoimenpiteiden olisi täytettävä tekstissä määritellyt varsin tiukat ehdot (mm. suhteellisuus- ja välttämättömyysvaatimus). Joiltakin osin näitä ehtoja on lisätty verrattuna esimerkiksi tällä hetkellä voimassa olevaan tilapäiseen poikkeusasteukseen ((EU) 2021/1232); esimerkiksi palveluntarjoajien olisi varmistettava, etteivät heidän vapaaehtoiset CSA-materiaalin tunnistustoimenpiteensä loisi hallitsemattomia riskejä kyberturvallisuudelle ja palveluntarjoajien olisi mm. pidettävä yksityiskohtaisia lokitietoja toiminnoistaan sisäistä ja ulkoista tarkastelua varten sekä mahdollista rikosoikeudellista menettelyä varten.

Nyt käsiteltävä kompromissiehdotus eroaa myös aiemmasta tunnistamismääräykseen perustuvasta versiosta siltä osin, että tunnistamisessa on lisätty metatietojen merkitystä ja käsittelyä on joiltain osin rajattu. Vapaaehtoisessa tunnistamisessa käytettäviä teknologioita ei saisi käyttää viestien tekstin järjestelmälliseen suodattamiseen ja seulomiseen muuten kuin yksinomaan sellaisten toimintamallien (patterns) havaitsemiseksi, jotka viittaavat mahdollisiin konkreettisiin perusteisiin epäillä verkossa tapahtuvaa lasten seksuaalista hyväksikäyttöä, eikä niillä pitäisi voida päätellä viestien varsinaista sisältöä. Kun kyse olisi groomingin tunnistamiseen käytettävästä teknologiasta, tällaisten epäilyä koskevien konkreettisten perusteiden olisi perustuttava objektiivisesti määritettyihin riskitekijöihin, kuten ikäeroon ja siihen, että seulottavan viestinnän osapuolena on todennäköisesti lapsi.

Edelleen tuoreimpaan kompromissitekstiin on lisätty ihmisen suorittamaa valvontaa koskevia kirjauksia. Palveluntarjoajat varmistavat ihmisen suorittaman valvonnan ja tarvittaessa ihmisen toteuttamat toimet sellaisessa henkilötietojen ja muiden tietojen käsittelyssä, jossa käytetään tämän asetuksen soveltamisalaan kuuluvia teknologioita. Muun kuin aikaisemmin CSA-materiaaliksi varmistetun sisällön osalta ihmisen tulee varmistaa sisältö ennen sen raportoimista viranomaisille.

Merkitystä on myös sillä, että nykyisen puheenjohtajamaan kompromissitekstissä soveltamisalaan kuuluvien palveluntarjoajien joukko on aiempaa rajatumpi. Kun tunnistamismääräys olisi voitu antaa säilytyspalveluiden tarjoajille tai henkilöiden välisten viestintäpalveluiden tarjoajille, niin yritysten vapaaehtoiset tunnistustoimet olisi sallittu ainoastaan numeroista riippumattomien henkilöiden välisten viestintäpalveluiden tarjoajille (esim. Facebook Messenger). Toisaalta tunnistamismääräystä oli tarkoitus kohdentaa vain erillisellä määräyksellä vain niihin palveluntarjoajiin, joiden palvelussa tai palvelunosassa oli havaittu korkea riski CSA-materiaalin leviämiselle.