Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

5.5.2025

Eduskunta
Suuri valiokunta

Viite: U 69/2022 vp

Lausunto: Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final)

Teknologiateollisuus sekä Kyberala kiittävät mahdollisuudesta lausua asiasta (yhteinen lausunto). Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka vastaavat puolesta Suomen viennistä, tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa.

Tiivistelmä

Ehdotuksella on hyväksyttävä ja erittäin painava tavoite suojata lapsia verkkovälitteiseltä seksuaaliväkivallalta. Pyrkimys vakivallattoman lapsuuden turvaamiseksi ja vakavien rikosten uhreina olevien lasten suojelemiseksi on kannatettava. Puheenjohtaja Puola on onnistunut laatimaan useista syistä kannatettavan kompromissiehdotuksen. Ehdotuksen tavoitteet ovat aiempiin ehdotuksiin verrattuna oikeammassa suhteessa tavoiteltuun päämäärään verrattuna ja tarjoavat tehokkaita torjua lapsiin kohdistuvaa seksuaalista hyväksikäyttöä kaikkien verkon käyttäjien yksityisyyttä ja perusoikeuksia kunnioittaen.

Kannatettavaa on, että viestinnän luottamuksellisuuden suojaan sekä muihin perusoikeuksiin puuttumista on rajoitettu perustellusti ja selvästi. Koska varsinaisen lakiehdotuksen tekstiä ei ole ollut saatavilla, ei ole mahdollista lausua onko näihin puuttumista rajoitettu kuitenkaan ehdottoman välttämättömään. Erityisen kannatettavaa joka tapauksessa on, että sääntely ei ole enää johtamassa laajaan ja yksilöimättömään viestinnän sisällön tarkkailuun ja tunnistamiseen viranomaisten toimesta. Tiivistäen voidaan todeta, että:

- Ehdotuksen avulla voidaan suojata lapsia seksuaaliselta hyväksikäytöltä, myös hallitusohjelman tavoitteiden valossa
- Ehdotus on paremmin perusoikeuksien rajoittamisedellytysten tarpeellisuus- ja suhteellisuusperiaatteen mukainen ja edistää vähemmän haitallisia, mutta tehokkaita ratkaisuja lasten suojelemiseen
- Ehdotus mahdollistaa yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten sekä huoltovarmuuden turvaamisen aiempaa paremmin
- Valitettavasti tavoite viestintäsalaisuuden murtamisesta on siirretty komission uuteen ProtectEU-strategiaan, josta syystä jäsenvaltioiden parlamentaariselle valvonnalle on tarvetta jatkossakin

Viestinnän luottamuksellisuuden suojan ja muihin perusoikeuksiin puuttumisen rajoittaminen

Ehdotuksen keskeinen muutos aiempaan on pakollisen tunnistamismääräyksen (artiklat 7–11), poistaminen ja vapaaehtoisten havaitsemistoimenpiteiden käyttöönotto palveluntarjoajille, joiden nojalla palveluntarjoajia olisi voitu viranomaismääräyksellä velvoittaa tunnistamaan lapsiin kohdistuvaa seksuaalista väkivaltaa esittävää materiaalia. Muutos on oikea ja varmistaa, että sääntely ei johda laajaan ja yksilöimättömään viestinnän sisällön valvontaan viranomaisten toimesta.

Eteläranta 10, PL 10, 00131 Helsinki

Päästä-päähän-salaus tarkoittaa, että kukaan muu kuin viestin lähettäjä ja tarkoitetut vastaanottajat eivät voi lukea viestejä tai muuten analysoida niitä päätelläkseen viestin sisältöä. Näin ollen myöskään viestejä välittävä palveluntarjoaja tai muu taho ei tällöin voi saada viestin sisältöä tietoonsa, vaikka viestit kulkevat sen tietojärjestelmien kautta. Sisäministeriö korostaa perusmuistiossaan (1.4.2025), että asetusehdotuksessa ei ole velvoitteita, jotka voivat tosiasiassa johtaa viestinnän päästä päähän -salauksen käytön tarkoituksen kiertämiseen.

Puheenjohtajan ehdottamaan tekstiin on säilytetty aikaisemmissa kompromissiteksteissäkin ollut lauseke siitä, ettei asetuksella kielletä, kierretä tai muutoin heikennetä kyberturvallisuustoimenpiteitä, joiden ydinaluetta on digitaalisen tiedon salaaminen. Onkin välttämätöntä, että asia on laissa erikseen säännökseksi muotoiltuna (ei ainoastaan ns. resitaalina), jotta tulkintaepäselvyyksiltä ja raskailta tuomioistuinkäsittelyiltä voidaan välttyä myöhemmin. Viestintäpalveluiden tarjoajien on voitava valita käyttämänsä salausteknologiat ja sovittava niiden soveltamisesta asiakkaidensa kanssa, sillä päästä päähän -salauksen perimmäinen tarkoitus on palvelun tarjoajan (asiakkaan omistaman) tiedon luottamuksellisuuden ja eheyden varmistaminen. Tämä on myös Suomen kokonaisturvallisuuden kannalta keskeinen yhteiskunnan taloudellisten edellytysten sekä huoltovarmuuden turvaamisen lähtökohta.

Ehdotuksessa korostetaan, että viestinnän luottamuksellisuuden suojaan ja muihin perusoikeuksiin puuttuminen tulee rajoittua vain välttämättömään. Ehdotuksessa on otettu paremmin huomioon EU:n tietosuojalainsäädäntö ja luottamuksellisten viestien suojaaminen. Vapaaehtoisiksi tarkoitetuille havaitsemistoimenpiteille on asetettu tiukkoja suojatoimia väärinkäytösten estämiseksi ja sen turvaamiksi, että ne nojautuvat automaatioon ja kehittyneen (ja edelleen kehittyvään) teknologian käyttämiseen.

Sisäministeriön perusmuistiosta jää kuitenkin epäselväksi, perustuisiko kompromissiehdotuksen viestien sisältöön kohdistuva, palveluntarjoajien vapaaehtoinen tekninen valvonta edelleen viestintäpalveluiden käyttäjien suostumukseen (esim. käyttäjäehdoissa). Edelleen on epäselvää, olisiko käytännössä pakollinen suostumus (palvelun käyttämisen mahdollistamiseksi) voimassa olevan EU:n yleisen tietosuoja-asetuksen vastainen. Yleisen tietosuoja-asetuksen mukaan, jotta suostumus olisi pätevä, sen on oltava yksilöity, tietoinen ja aidosti vapaaehtoinen, josta on oltava mahdollisuus myös kieltäytyä ilman haitallisia seurauksia.

Numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajien vapaaehtoiset toimet CSA-materiaalin tunnistamiseksi

Ehdotuksessa on lisätty tietyille palveluntarjoajille mahdollistettujen vapaaehtoisten käsittelytoimenpiteiden tuominen pysyvän sääntelyn piiriin (uusi artikla 4a) mahdollistaen sen, että numeroista riippumattomat henkilöiden välisten viestintäpalvelujen tarjoajat voivat käyttää soveltuvia teknologioita henkilötietojen ja muiden tietojen käsittelyyn siinä laajuudessa, kuin on välttämätöntä CSA-materiaalin tai groomingin havaitsemiseksi ja siitä ilmoittamiseksi. Ehdotuksessa viranomaiset voisivat suositella palveluntarjoajalle riskien arviointia sekä riskiä vähentävien toimenpiteiden käyttöönottoa varmisten, että palveluntarjoajat voivat toteuttaa tehokkaita toimenpiteitä CSA-materiaalin leviämisen estämiseksi. Ehdotuksessa korkean riskin palveluntarjoajilla olisi lisäksi velvollisuus tarjota tehokkaita vaihtoehtoisia ilmoitusmekanismeja palvelun käyttäjille CSA-materiaaliin kytkeytyvissä tapauksissa (12 artikla). Tämä mahdollistaa, että käyttäjät voivat helposti ilmoittaa havaitsemastaan laittomasta sisällöstä.

On kuitenkin tarpeen, että ehdotuksessa laittoman sisällön tunnistamiseen käytettävän teknologian käyttämisessä epäilyä koskevien konkreettisten perusteiden on perustuttava objektiivisesti määritettyihin riskitekijöihin. Laittoman sisällön tunnistamisen tarkoituksena eikä

seurauksena tule olla viestinnän sisällön päätteleminen, vaan käsittelyn tarkoituksena tulisi olla sellaisten käyttäytymis- ja toimintamallien (patterns) tunnistaminen, jotka viittaavat mahdolliseen lasten hyväksikäyttöön. Tällaisilla keinoilla on hyvä mahdollisuus puuttua myös ns. grooming-toimintaan (seksuaalinen houkuttelu).

Lapsiin kohdistuvan seksuaaliväkivallan torjunnan tuleekin perustua lasten välittömästi uhriksi joutumisen estämiseen, ei pelkästään sitä kuvaavan materiaalin tai sen jakelun poistamiseen. Tästä näkökulmasta niin EU-lainsäädännön vaatimukset, kansainväliset sopimukset, hallitusohjelman tavoitteet sekä erityisesti lapsen etuun sisältyvä viestinnän luottamuksellisuus tulisivat kompromissiehdotuksen avulla paremmin saavutetuiksi.

Sähköisen viestinnän luottamuksellisuuden ja yksityisyyden ydinalueen murentamisen ensimmäinen vaihe

Europol ja jäsenmaiden lainvalvontaviranomaisten johtajat julkaisivat keväällä 2024 yhteisen julistuksen, jonka tavoitteena on käytännössä murtaa salaus eli yksityisyyden suoja kaikelta viestinnältä. Tällä kertaa ehdotettiin viestiliikenteen valvontaa ja tarkistamista lasten seksuaalisen hyväksikäytön torjunnan näkökulmasta.

Nyt ehdotus on laajennettu 8.4.2025 julkaistussa EU:n sisäisen turvallisuuden strategiassa (ProtectEU) koskemaan turvallisuusviranomaisten pääsyä kaikkeen sähköiseen informaatioon. Päämäärä koskettaa selvästi ja suoraan myös päästä päähän -salausta sekä muutakin salatussa muodossa olevaa digitaalista tietoa, kuten yrityssalaisuuksia, jotka ovat yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten turvaamisen perusta. Poliittisille päättäjille perustellaan turvallisuuden nimissä osin harhaanjohtavasti yksittäisten toimien tarpeellisuutta rikostorjunnassa. Turvallisuuden ”edistämisen” houkutus usein osoittautunut suureksi, mutta digitaalisessa maailmassa turvallisuuden edistäminen on usein kaksiteräinen miekka. Salausteknologian heikentäminen, käytön rajoittaminen tai niitä valmistavien yhtiöiden pakottaminen yhteistyöhön ”laillisen pääsyn” tarkoituksissa on johtanut käytännössä tilanteisiin, jossa turvallisuus on heikentynyt entisestään ja vahingot koskettaneet rikollisten toimijoiden sijasta nimenomaan sivullisia.

On kuitenkin huomattava, että komissio korostaa samalla, että teknologisten ratkaisujen, jotka mahdollistavat lainvalvontaviranomaisten pääsyn salattuihin tietoihin laillisesti, on suojattava myös kyberturvallisuutta ja perusoikeuksia. Tämä tullee olemaan keskeinen parlamentaarista harkintaa ja valvontaa edellyttävä aihekokonaisuus komission jatkotyössä. Toivommekin, että valtioneuvosto, eduskunta sekä eritoten Suuri valiokunta seuraavat tarkasti strategiaan liittyvien ehdotusten valmistelua.

Teknologiateollisuus ry

Helena Soimakallio
Johtaja, Toimialat ja liiketoiminnan jatkuvuus

Kyberala ry

Peter Sund
Toimitusjohtaja

Lisätiedot:

Peter Sund, 050 565 0621
peter.sund@teknlogiateollisuus.fi