Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

15.9.2025

Eduskunta
Liikenne- ja viestintävaliokunta

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 ja Kyberala kiittävät mahdollisuudesta lausua asiasta. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa. Teknologiateollisuuden jäsenet vastaavat puolesta Suomen viennistä, tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Lausunto on edellä mainittujen yhteinen.

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. Edellisen puheenjohtaja Puolan ehdotuksesta poiketen puheenjohtaja Tanska on jättänyt keskeisiä kannatettavia ehdotuksia huomiotta kompromissiehdotuksesta ja palannut ns. Unkarin ehdotuksen tielle. Ehdotukseen sisällytetyt keinot ovatkin selvässä epäsuhteessa hyväksyttävään päämäärään verrattuna sisältäen kaikkien verkon käyttäjien yksityisyyttä ja perusoikeuksia loukkaavan lähestymistavan. Erityisen haitallista on, että sääntely olisi jälleen johtamassa laajaan ja yksilöimättömään viestinnän sisällön tarkkailuun ja tunnistamiseen viranomaisten toimesta. Ehdotus olisi myös heijastusvaikutuksiltaan ennakoimaton. Tiivistäen voidaan todeta, että:

- Ehdotuksen avulla lasten seksuaaliselta hyväksikäytöltä suojaaminen olisi tehotonta ja epätarkoituksenmukaista
- Ehdotus ei ole perusoikeuksien rajoittamisedellytysten tarpeellisuus- ja suhteellisuusperiaatteen mukainen eikä edistäisi vähemmän haitallisia ja tehokkaita ratkaisuja lasten suojelemiseen
- Ehdotus vahingoittaa yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten sekä huoltovarmuuden turvaamista
- Tavoite viestintäsalaisuuden murtamisesta on sisällytetty myös komission ProtectEU-strategiaan, josta syystä jäsenvaltioiden parlamentaariselle valvonnalle on tarvetta jatkossakin

Ehdotus ei ole tehokas lasten suojaamiseksi

Verkkovälitteinen seksuaaliväkivalta voidaan jakaa kahdenlaiseen toimintaan: seksuaaliväkivaltaa todistavan materiaalin levittämiseen verkossa sekä ”groomingiin” eli verkkohoukutteluun. Verkkohoukuttelussa on kyse manipulatiivisesta menettelystä, jossa aikuinen luo alaikäiseen luottamussuhteen tarkoituksenaan valmistella heitä seksuaaliseen hyväksikäyttöön. Keskeisin kohde lasten suojelemiseen väkivallalta on aikuisten suorittama hyväksikäyttömateriaalin tuottaminen, jossa alaikäinen on välittömästi rikollisen teon kohde. Ehdotuksesta on rajattu pois sekä verkkohoukuttelun torjunta.

Ehdotetut keinot eivät olisi edelleenkään tehokkaita. Lapsin kohdistetun seksuaaliväkivalan tekijät käyttävät samoja viestintäpalveluja, kuin laillisesti toimivat tahotkin. Viestintäpalveluiden vaihtaminen on vaivatonta, josta syystä mm. epäselvään palveluntarjoajariskin arviointia ei voi

Eteläranta 10, PL 10, 00131 Helsinki

pitää harkittuna menettelynä. Aiemmissa Teknologiateollisuuden ja Kyberalan esille nostamat seikat tunnistamismääräyksen teknishallinnolliseen toteuttamiseen ovat edelleen päteviä.

Viestinnän luottamuksellisuuden suojan ja muihin perusoikeuksiin puuttumisen rajoittaminen

Ehdotuksen keskeinen muutos Puolan ehdotukseen on pakollisen tunnistamismääräyksen käyttöönotto. Ehdotuksessa palautetaan pakollinen, epätarkoituksenmukaisesti eri palveluntarjoajille kohdennetun, viestintä- ja säilytyspalvelujen käyttäjien luottamuksellisen sähköisen viestinnän läpivalaisun. Lisäksi ehdotukseen on palautettu ns. palvelujen käyttäjien pakotettu suostumus, jota ei voida pitää EU-oikeuden sallimana keinona.

Muutos johtaa laajaan ja yksilöimättömään viestinnän sisällön valvontaan viranomaisten toimesta. Perustuslakivaliokunnan lausuntokäytännön mukaisesti valvonnan edellytyksenä tulee olla konkreettinen ja yksilöity rikosepäily, mitä ehdotettu tunnistamismääräys ei edellytyksenä täytä. Olennaista on, että 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. Sillä ei ole merkitystä, tehtäisiinkö viestinnän sisällön valvontaa ennen tai jälkeen tiedon teknistä salaamista. Kyse olisi edelleen salauksen käytön ja oikeuden yksityiseen viestintään tarkoituksen kiertämisestä.

On leimaavaa, että turvallisuus- ja puolustusviranomaiset on rajattu ehdotuksen ulkopuolelle, sillä läpivaisumekanismin sisällyttämisen riskit viestintäpalveluissa ovat hyvin ymmärretyt. 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. Liikesalaisuudet, kuten asiakas- ja tuotekehitystiedot ovat päivittäisen vakoilu- ja sabotaasiriskin kohteena, jolloin myös taloudellinen turvallisuus sekä huoltovarmuus ovat uhattuna.

Viestinnän luottamuksellisuuden suojaan ja muihin perusoikeuksiin puuttuminen tulee rajoittua vain välttämättömään. Lähtökohdaksi onkin asetettava unionin perusoikeussuojaan kuuluvien yksilöitä ja yhteisöjä koskevan yksityisyyden suojan lisäksi se, että jokaisella on oikeus vastaanottaa tietoja ja muita viestejä kenenkään (viranomaisen) ennakolta estämättä (ks. PL 12 §). Vastaavan tulkintakäytännön on omaksunut myös Euroopan ihmisoikeustuomioistuin.

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

Ehdotuksessa on lisätty määräaikaiset siirtymäsäännökset tietyille palveluntarjoajille mahdollistettujen vapaaehtoisten käsittelytoimenpiteiden (numeroista riippumattomat henkilöiden välisten viestintäpalvelujen tarjoajat) voivat jatkaa soveltuvien teknologioiden henkilötietojen ja muiden tietojen käsittelemiseksi lasten suojaamiseksi. Menettely on kuitenkin määräaikainen eikä sisällä luotettavaa kuvausta siitä, mikä tai millainen ns. pysyvistä järjestelyistä tulisi. Näiltä osin ehdotus poikkeaa olennaisesti Puolan kompromissiehdotuksesta.

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. Viitaten Perustuslakivaliokunnan lausuntokäytäntöön (mm. PeVL 2/2024 vp) on tärkeä huomioida, että mm. Perustuslain tai EU:n perusoikeuskirjaan sisältyvien perusoikeuksien käsitteitä ei tule määritellä tavallisen tai sekundaarisen (EU) lain tasolla. Tämä asia tullee olemaan keskeinen parlamentaarista harkintaa ja valvontaa edellyttävä aihekokonaisuus komission jatkotyössä. Toivommekin, että valtioneuvosto sekä eduskunta seuraavat tarkasti strategiaan liittyvien ehdotusten valmistelua.

Kiinnitämme lopuksi huomiota Yhdistyneiden kuningaskuntien (UK) tapahtumaketjuun, jossa Investigatory Powers Act -säädöksen perusteella viranomaisten vaatima päästä-päähän salauksen (E2EE) murtaminen johti siihen, että mm. yleisesti hyvin turvallisena pidetty säilytys- ja viestintäpalvelujen tarjoaja Apple -konserni poisti vahvan salauksen saatavilta kaikilta UK:ssa sijaitsevilta käyttäjiltään. Tämä kehityskulku johtaa ilmeiseen kokonaisturvallisuuden heikentymiseen. Saatamme myös myös valiokunnan tietoon, että aiemmin Yhdysvaltojen (US) Kyberturvallisuuden ja infrastruktuurin turvallisuusviraston (CISA) ja Liittovaltion rikostorjuntaviraston (FBI) lisäksi nyttemmin US kauppakomissio (FTC) on varsin selkeäsanaisesti varoittanut yhdysvaltalaisia teknologiapalvelujen tarjoajia heikentämästä palveluidensa yhdysvaltalaisten käyttäjien tietoturvallisuutta edellä mainituista ilmeisistä syistä.

Kyberala ry
Peter Sund
Toimitusjohtaja

Teknologiateollisuus ry
Helena Soimakallio
Johtaja, Toimialat ja liiketoiminnan jatkuvuus

Lisätiedot:

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