Lausunto
Asianumero: U 69/2022 vp
Päivämäärä: 15.10.2024

Pauliina Penttilä
TIO / TTU

Hallintovaliokunta

U 69/2022 vp ehdotuksesta asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (ns. CSAM-asetusehdotus)

Liikenne- ja viestintäministeriön asiantuntijalausunto

Hallintovaliokunta on pyytänyt liikenne- ja viestintäministeriön lausuntoa koskien asetusehdotusta lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (ns. CSAM-asetusedotus). Liikenne- ja viestintäministeriö kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan kunnioittavasti seuraavaa:

Asetusehdotuksen tavoite lasten suojelemisesta on äärimmäisen tärkeä, ja liikenne- ja viestintäministeriö tukee vahvasti ajatusta EU-tasolla luotavasta oikeasuhtaisesta ja kestävästä sääntelystä, jolla tähän tavoitteeseen voidaan päästä. Liikenne- ja viestintäministeriö on valmistelussa tuonut esille sitä, että erittäin kannatettavasta tavoitteesta huolimatta ehdotetuilla toimilla on erittäin merkittävää vaikutusta perusoikeuksina turvattuihin viestinnän luottamuksellisuuteen ja sähköisen viestinnän tietosuojaan. Valmistelussa tuleekin varmistua siitä, että perusoikeuksien rajoitusedellytysten on täytyttävä.

Komission alkuperäinen esitys sisältää monia eri toimenpiteitä, joilla jatkossa voidaan parantaa lasten suojelua seksuaaliselta väkivallalta ja estää sitä esittävän materiaalin välittämistä verkossa. Liikenne- ja viestintäministeriön käsityksen mukaan kaikki muut komission ehdottamat toimenpiteet ovat työryhmässä olleet riidattomia paitsi niin kutsuttu tunnistamismääräys. Kyseinen toimenpide on erityisen ongelmallinen siltä osin kuin sillä velvoitetaan palveluntarjoaja käymään ennakollisesti läpi henkilöiden välistä luottamuksellista viestintää ja heikennetään päästä päähän -salausta.

Luottamuksellisen viestin suoja

Liikenne- ja viestintäministeriö korostaa U-jatkokirjelmässä UJ 19/2023 vp ilmaistua kantaa, jonka mukaan tunnistamismääräyksen on oltava kohdennettu ja sen käyttöönoton ei tule johtaa koko väestön ja kaikkien viestintäpalveluiden ja tietoliikenteen yleiseen ja erotuksettomaan valvontaan. Tavoitteena tulee olla, että tunnistamismääräys on mahdollisimman kohdennettu henkilöihin, jotka liittyvät lapsiin kohdistuvien seksuaalirikosten selvittämiseen tai joiden voidaan epäillä olleen osallisina tällaisiin rikoksiin. Tältä osin liikenne- ja viestintäministeriö viittaa perustuslain 10 §:n 4 momentin mukaisiin rajoituksiin. Perustuslain 10 §:n 4 momentin säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiin kuuluvasta välttämättömyysvaatimuksesta seuraa, että luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee olla mahdollisimman kohdennettua ja rajattua (PeVL 35/2018 vp, s. 12). Lisäksi ministeriö korostaa, että viestinnän luottamuksellisuuden suoja ei ole vastakkainen lasten oikeuksien ja niiden toteutumisen kannalta,

vaan myös lapsilla on oikeus viestiä ja oikeus viestinnän luottamuksellisuuteen. Digitaaliset viestintäkanavat ovat tärkeitä nykylasten elämässä (ks. CRC/C/GC/25).

Liikenne- ja viestintäministeriö pitää sisäministeriön tavoin tunnistamismääräyksen soveltamisalaan neuvotteluissa tehtyjä rajoituksia kannatettavina, ja ne lisäävät toimenpiteen hyväksyttävyyttä. Esimerkiksi sisäministeriön lisäselvityksessä esiin tuodusti tunnistamismääräystä ei voitaisi kohdistaa ns. uuteen CSA-materiaaliin, vaan ainoastaan laittomaksi vahvistettu sisältö olisi tunnistamistoimenpiteen kohteena. Myöskään teksti- tai ääniviestien tunnistamista ei edellytettäisi, eikä lasten houkuttelu eli ns. grooming olisi tunnistamismääräyksen kohteena. Näiltä osin liikenne- ja viestintäministeriö jakaa asiantuntijoiden arvion, että teknologia tällaiseen tunnistamiseen on keskeneräistä ja epätarkkaa.[1] Näin ollen näiden kaikkein ongelmallisimpien aineistojen rajaaminen tunnistamismääräyksen soveltamisalan ulkopuolelle on ollut myönteinen kehitysaskel.

Käsiteltävää asetusehdotusta koskevassa perustuslakivaliokunnan lausunnossa PeVL 5/2023 vp todetusti ehdotukseen liittyy runsaasti oikeudellista epävarmuutta siitä, pystyttäisiinkö tunnistamismääräyksen perusteella käytettävä teknologia kohdentamaan siten, että erilaisten palveluiden piirissä tapahtuva viestiliikenteen käsittely olisi riittävän kohdennettua perustuslain ja EU:n perusoikeuskirjan tulkintakäytännössä edellytetyllä tavalla (PeVL 5/2023 vp, kappale 6).

Liikenne- ja viestintäministeriö kiinnittää huomiota siihen, että Euroopan parlamentin vahvistetun neuvottelukannan mukaan tunnistamismääräys tulisi rajoittua tiettyihin henkilöihin tai henkilöryhmiin, joihin liittyy perusteltu syy epäillä heidän liittyvän CSA-materiaalin välittämiseen.[2] Puheenjohtajamaan kompromissiesityksessä vastaavaa lisäystä ei ole.

Lopuksi liikenne- ja viestintäministeriö tuo sisäministeriön lisäselvitystä täydentävästi esiin, että tunnistamismääräys olisi nykyisessä kompromississa rajattu viestien sisällöissä olevien kuvien lisäksi myös URL-osoitteisiin. On käytännössä epäselvää, millaisella teknologialla viestien sisällöissä olevia URL-osoitteita olisi mahdollista käsitellä ilman puuttumista muuhun viestin sisältöön, mukaan lukien tekstimuotoiseen ja henkilökohtaisesti vain vastaanottajalle tarkoitettuun sisältöön.

Vaikutukset viestinnän salaukseen ja viestintäpalveluiden turvallisuuteen

U-jatkokirjelmän UJ 19/2023 vp mukaisesti valtioneuvosto pitää tärkeänä, että ehdotetut toimet eivät vaaranna kyberturvallisuutta tai viestintä- ja tietojärjestelmien turvallisuutta. Asiantuntijakuulemisissa on tuotu esiin, että salauksen heikentäminen huonontaa palvelujen turvallisuutta yleisesti ja mahdollistaa siten myös pahantahtoisille toimijoille aiempaa helpommin erilaiset väärinkäytökset. Esimerkiksi mahdolliset takaportit voisivat olla myös ulkopuolisten valtiollisten toimijoiden ja rikollisten tahojen hyödynnettävissä.

Kuten sisäministeriön lisäselvityksessä tuodaan esiin, kompromissiesityksen mukaan tunnistamismääräyksen kohdentuessa päästä päähän -salausta käyttävään palveluntarjoajaan, tulisi palveluntarjoajan tunnistaa käyttäjän välittämä kuva ns. hash- eli tiivistetietokantaa vasten ennen viestin salaamista sen välittämistä varten. Kompromissiesityksen mukaan visuaalisen

[1] Ks. esim. EPRS European Parliamentary Research Service: Proposal for a regulation laying down the rules to prevent and combat child sexual abuse - Complementary impact assessment, julkaistu huhtikuussa 2023.
[2] REPORT on the proposal for a regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, hyväksytty 16.11.2023, lisäys 24.

aineiston lisäksi viestin tekstisisällöstä olisi myös tunnistettava URL-osoitteet. Liikenne- ja viestintäministeriön saaman käsityksen mukaan tämä käytännössä edellyttäisi, että palveluntarjoajalla tai sen toimittamalla sovelluksella olisi oltava kyky analysoida palvelussa jaettua kuva- ja tekstimuotoista sisältöä, jota käyttäjä pyrkii lähettämään sovelluksella. Tämä tarkoittaisi käytännössä velvoitetta kiertää päästä päähän –salaus. Asiantuntijakuulemisten yhteydessä tietoturva-asiantuntijat ovat ilmaisseet tällaiseen ratkaisuun liittyvän erittäin vakavia huolia kyberturvallisuudesta sekä perusoikeuksien toteutumisesta.

Salauksen merkitys perusoikeuksien toteutumisen turvaajana on viime vuosina korostunut. Esimerkiksi perustuslakivaliokunnan mukaan välillisesti salauksen purkaminen voisi johtaa myös perustuslain 12 §:ssä turvatun sananvapauden kannalta ongelmalliseen tilanteeseen. (PeVL 5/2023 vp) Myös Euroopan ihmisoikeustuomioistuin on viimeaikaisessa ratkaisussaan ottanut kantaa salauksen merkitykseen perusoikeussuojan näkökulmasta. Digitaalisella aikakaudella tekniset ratkaisut sähköisen viestinnän yksityisyyden turvaamiseksi ja suojaamiseksi, mukaan lukien salaustoimenpiteet, osaltaan varmistavat muiden perusoikeuksien, kuten sananvapauden, toteutumisen. Salaus lisäksi auttaa kansalaisia ja yrityksiä puolustautumaan tietotekniikan väärinkäytöksiä, kuten hakkerointia, identiteetti- ja henkilötietojen varkauksia, petoksia ja luottamuksellisten tietojen epäasianmukaista paljastamista vastaan. Tämä on otettava asianmukaisesti huomioon arvioitaessa toimenpiteitä, jotka voivat heikentää salausta. (Podchasov v. Venäjä, 2024, §§ 76)

Toimien oikeasuhtaisuutta arvioitaessa olisi myös otettava huomioon se, että tietoturvatoimenpiteiden kiertämisellä tai niitä heikentämällä sen negatiiviset vaikutukset kohdistuisivat kaikkiin palvelun käyttäjiin. Toisaalta käyttäjät voivat myös itse salata viestinsä ennen sen lähettämistä tai välittää sen salattuun kansioon tallennettuna, jolloin palvelun salausta heikentävillä toimilla ei voitaisi taata rikollisen toiminnan tunnistamista.