

Liikenne- ja viestintävaliokunta

Viite

Liikenne- ja viestintävaliokunnan asiantuntijapyyntö asiassa U 69/2022 vp, UJ 19/2023 vp

Asiantuntijalausunto valtioneuvoston kirjelmästä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä ja sitä koskevista jatkokirjelmästä

Liikenne- ja viestintävirasto kiittää mahdollisuudesta lausua valtioneuvoston kirjelmästä ja jatkokirjelmästä. Liikenne- ja viestintävirasto pitää asetusehdotuksen tavoitteita lasten suojelemisesta erittäin kannatettavina ja tukee valtioneuvoston kantaa. Liikenne- ja viestintävirasto korostaa edelleen sen tärkeyttä, että puuttuminen viestinnän luottamuksellisuuteen asetusehdotuksen mukaisilla tunnistamismääräyksillä¹ rajoitetaan valtioneuvoston kannan mukaisesti vain välttämättömään.

Lisäksi Liikenne- ja viestintävirasto pitää ehdottoman tärkeänä, ettei asetusehdotus heikennä viestintäpalvelujen tietoturvaa tai rajoita sen kehittämistä. Asetusehdotuksen tavoite on kiistämättömän tärkeä, mutta oikeasuhtaisten keinojen valinta on kriittisessä asemassa, jotta asetuksella puututa perusoikeutena turvatus luottamuksellisen viestin suojan ytimeen eikä vaaranneta kyberturvallisuutta.

Tunnistamismääräysten vaikutuksista viestinnän luottamuksellisuuteen

Liikenne- ja viestintäviraston asiantuntijalausunnossa 26.9.2022 tehdyt huomiot tunnistamismääräyksestä ovat edelleen pääosin ajankohtaisia, vaikka asetusehdotukseen onkin tehty muutoksia, jotka korostavat mahdollista tunnistamismääräystä edeltävää riskien lieventämistä ensisijaisena keinona. Riskien lieventämisen menettelyt ja muut keinot, joilla parannettaisiin käyttäjien mahdollisuuksia ilmoittaa mahdollisesta lapsiin kohdistuvasta seksuaaliväkivaltaa todistavasta kuvamateriaalista tai lasten houkuttelusta sekä saada apua, ovat erittäin kannatettavia.

Sen sijaan asetusehdotuksen mukaiseen tunnistamismääräysten käyttöalaa ja aineellisiin edellytyksiin ei ole tiettävästi neuvotteluissa tehty olennaisia muutoksia lukuun ottamatta puheluiden rajaamista pois. Näin ollen edelleen ongelmallinen on asetusehdotuksen erittäin laaja soveltamisala, joka kattaisi myös perinteiset viestimet, kuten tekstiviestit ja sähköpostin. Ehdotus voi potentiaalisesti koskea kaikkia henkilöiden välisen viestinnän palveluiden käyttäjiä, mikä asettaa ehdotuksen ongelmalliseen suhteeseen EU-tuomioistuimen oikeuskäytännön kanssa eritoten, koska kyse on myös viestinnän sisällön käsittelystä.

Asetusehdotuksessa on nähtävissä riski siitä, että tunnistamismääräysten antaminen voisi lopulta johtaa käytännössä kattavaan ja pysyvään viestinnän valvontaan. Asetusehdotukseen ei näytä sisältyvän aineellisia takeita, jotka estäisivät viestinnän valvonnan muodostumisen lopulta pääsäännöksi. Valtioneuvosto korostaakin asianmukaisesti jatkokirjelmässä, että tunnistamismääräyksen olisi oltava kohdennettu ja että niiden käyttöönoton ei tule johtaa koko väestön ja kaikkien viestintäpalvel-

¹ Asetusehdotuksen mukaisilla tunnistamismääräyksillä veloitetaan palveluntarjoaja valvomaan automatisoidusti viestintää. Tunnistamismääräykset voisivat koskea tiedossa olevan tai uuden lapsiin kohdistuvan seksuaaliväkivallasta todistavan kuvamateriaalin taikka lapsen houkuttelun (grooming) tunnistamista. Tunnistamismääräys voitaisiin kohdistaa hosting-palveluntarjoajaan tai henkilöiden välisen viestintäpalvelun, kuten pikaviesti-, tekstiviesti- tai sähköpostipalvelun, tarjoajaan.

luiden ja tietoliikenteen yleiseen ja erotuksettomaan valvontaan. Kuten valtioneuvosto toteaa, ehdotettu sääntely ei kuitenkaan ole tältä osin ongelmaton.

Ongelmallista tunnistamismääräyksissä on myös niiden oikeudellisten kriteerien avoimuus, joiden perusteella tunnistamismääräyksen antaminen ratkaistaisiin. Vakava ongelma on myös ns. väärin positiivisten tapausten eli esimerkiksi virheellisesti houkutteluksi tunnistettujen tapausten mahdollisuus, joka liittyy etenkin uuden kuvamateriaalin ja erityisesti houkuttelun tunnistamiseen. Tämä aiheuttaa huomattavan uhan niin lasten kuin aikuistenkin yksityisyyden suojan ja muiden perusoikeuksien toteutumiselle.

Tunnistamismääräysten vaikutuksista tietoturvaan ja salauksen käyttöön

Jatkokirjelmässä tuodaan asianmukaisesti esiin viestinnän salauksen keskeisyys kyberturvallisuuden kannalta ja todetaan valtioneuvoston kannaksi, että tulee huolehtia siitä, ettei asetusehdotuksesta seuraa yleistä velvoitetta palveluntarjoajille purkaa viestinnän vahvaa salausta tai luopua vahvan salauksen käytöstä.

Liikenne- ja viestintävirasto katsoo, että tunnistamismääräykset eivät saa johtaa salauksen heikentämiseen eivätkä päästä päähän -salauksen² käytön estymiseen tai rajoittamiseen. Kuten jatkokirjelmässä todetaan, salauksen heikentäminen heikentää palveluiden tietoturvaa. Salaus on keskeinen keino huolehtia palveluiden tietoturvasta ja ehkäistä tietoturvaloukkauksia. Asetusehdotuksen varsinaiseen säädöstekstiin ei kuitenkaan sisälly takeita siitä, että tunnistamismääräykset eivät voisi tällä tavoin heikentää salausta tai vaarantaa muutoin tietoturvaa.

Tunnistamismääräysten antaminen ei saa rajoittaa palveluntarjoajien mahdollisuuksia käyttää erilaisia salaukseen perustuvia tietoturvatyökaluja. Asetusehdotus ei saa johtaa ristiriitaan palveluntarjoajiin kohdistuvien tietoturva-vaatimusten kanssa eikä estää valvontaviranomaista edellyttämästä tarvittaessa myös päästä päähän -salauksen käyttämisestä. Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY), teledirektiivi ((EU) 2018/1972) ja jatkossa NIS2-direktiivi ((EU) 2022/2555) sekä niiden kansallinen voimaantulolainsäädäntö edellyttävät viestintäpalveluiden tarjoajia huolehtimaan palveluidensa tietoturvasta. Päästä päähän -salauksen käyttöä pyritään erityisesti edistämään teledirektiivillä ja NIS2-direktiivillä³, eikä asetusehdotus saa olla tämän tavoitteen kanssa ristiriidassa. Teleyritysten tietoturvatyökalujen riittävyyden arviointi kuuluu Suomessa Liikenne- ja viestintäviraston toimivaltaan. Voimassa oleva lainsäädäntö voi tapauskohtaisen riski- ja kustannusarvion perusteella periaatteessa jopa edellyttää päästä päähän -salauksen käyttöä, minkä lisäksi valvontaviranomaisella voi olla mahdollisuus erikseen määrätä tietyissä tilanteissa päästä päähän -salauksen käytöstä, kun se on perusteltua. Tulisi myös ottaa huomioon, että vaatimukset palveluiden tietoturvallisuuden heikentämiseksi voisivat johtaa siihen, että palveluntarjoajia vetäytyy EU:n markkinoilta.

Tyypillisesti tunnistamismääräyksen toteuttaminen tapahtuisi tietyllä teknisesti tavalla, jossa palveluntarjoajalla olisi palvelimellaan pääsy kaikkeen käyttäjän palveluun lähettämään teksti-, kuva- ja ääniviestipohjaiseen sisältöön. Mikäli palveluntarjoaja joutuisi tietomurron tai sisäisen väärinkäytöksen kohteeksi, voisi tekijällä olla vastaavasti mahdollista saada pääsy kaikkien käyttäjien viestisisältöihin.

² Päästä päähän -salauksella tarkoitetaan välitettävän viestinnän salaamista päätelaitteiden välillä eli käyttäjältä käyttäjälle. Tällöin viestintää käyttäjien välillä välittävä taho ei pysty tarkastelemaan välitettävää sisältöä selkokielisenä eikä näin ollen pysty myöskään tunnistamaan siitä tiettyä sisältöä.

³ Teledirektiivin johdanto-osan kohta 97 ja NIS2-direktiivin johdanto-osan kohta 98. Vaikka tämä tulisi direktiivien mukaan sovittaa yhteen jäsenvaltioiden toimivaltaan kuuluvan rikosten ennalta estämisen, tutkimisen, paljastamisen ja rikoksiin liittyvät syytetoimien kanssa, käsittää tämä totunnaisesti esimerkiksi telekommunikaation erotuksena asetusehdotuksen uusista tunnistamismääräyksistä. NIS2-direktiivin mukaan tällaisissa tapauksissa toimenpiteet eivät saisi "heikentää päästä päähän -salausta, joka on tehokas tietosuojan, yksityisyyden suojan ja viestinnän turvallisuuden kannalta kriittinen teknologia".

Viestinnän skannaamiseen käytettävien ohjelmistokomponenttien tietoturvasta voi olla erittäin hankala varmistua. On myös epäselvää, miten voitaisiin teknisesti varmistua siitä, että järjestelmiä ei voitaisi väärinkäyttää muun halutun viestinnän tunnistamiseen.

Asetusehdotus ei saa myöskään johtaa siihen, että palveluntarjoajan olisi saatava päästä päähän -salausta käytettäessä pääsy laitteelle tallennettuihin tietoihin salauksen kiertämiseksi. Tässä tapauksessa tunnistamismääräyksen edellyttämän viestinnän analysointi tapahtuisi päätelaitteen avulla viestintää välittävän tahon palvelimien sijaan. Myös tällaiseen päätelaitteella tapahtuvaan valvontaan liittyy kuitenkin erittäin vakavia huolia kyberturvallisuudesta sekä perusoikeuksien toteutumisesta. Se edellyttäisi päätelaitteella käsiteltävien tietojen analysointia ja palveluntarjoajan pääsyä analysoituihin tietoihin, mihin liittyy samoja riskejä kuin yllä on kuvattu.

Yhteenveto

Asetusehdotuksen tavoitteet ovat kiistämättömän tärkeitä. Viestinnän luottamuksellisuutta ei kuitenkaan voida rajoittaa enempää kuin on välttämätöntä ja oikeasuhtaista lasten oikeuksien turvaamiseksi. Asetusehdotuksen mahdollistamien tunnistamismääräysten oikeasuhtaisuudesta ja välttämättömyydestä tulee varmistua. Velvoitteiden tulee olla riittävästi kohdennettuja. Asetusehdotus ei saa heikentää tietoturvaa esimerkiksi rajoittamalla päästä päähän -salauksen käyttöä.

Marko Priiki
johtava asiantuntija
Liikenne- ja viestintävirasto