Liikenne- ja viestintävaliokunta

Viite
Liikenne- ja viestintävaliokunnan asiantuntijapyyntö asiassa U 69/2022 vp

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

Liikenne- ja viestintävaliokunta on pyytänyt Liikenne- ja viestintäviraston lausuntoa koskien asetusehdotusta lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (ns. CSAM-asetusehdotus) ja eduskunnalle asetusehdotuksen neuvottelutilannetta koskevaa sisäministeriön lisäselvitystä. Liikenne- ja viestintävirasto kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan kunnioittavasti seuraavaa:

Liikenne- ja viestintävirasto pitää asetusehdotuksen tavoitteita lasten suojelemisesta erittäin kannatettavina. Asetusehdotuksen tavoite on kiistämättömän tärkeä, mutta oikeasuhtaisten keinojen valinta on kriittisessä asemassa, jottei asetuksella puututa perusoikeutena turvatun luottamuksellisen viestin suojan ytimeen eikä vaaranneta kyberturvallisuutta. Liikenne- ja viestintävirasto korostaa edelleen sen tärkeyttä, että puuttuminen viestinnän luottamuksellisuuteen asetusehdotuksen mukaisilla tunnistamismääräyksillä[1] ja muilla toimenpiteillä rajoitetaan vain välttämättömään. Sen sijaan useat asetusehdotukseen sisältyvät 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.

Suuri valiokunta on liikenne- ja viestintävaliokunnan tavoin katsonut olevan erityisen tärkeätä varmistaa, etteivät tunnistamismääräykset edes tosiasiassa johda päästä päähän salauksen tai muiden vastaavien tietoturvatoimenpiteiden yleiseen heikentämiseen tai niiden purkamisen taikka niiden käytön rajoittamiseen ja tätä kautta viestinnän sekä viestintään liittyvien palvelujen tietoturvan ja kyberturvallisuuden tason heikkenemiseen (SuVL 7/2023 vp, kohta 6). Liikenne- ja viestintävirasto katsoo erityisesti päästä päähän -salauksen[2] käytön olevan tavanomainen, keskeinen ja tehokas keino edistää palveluiden tietoturvallisuutta ja ehkäistä tietoturvaloukkauksia.

Vaikka asetusehdotukseen onkin tehty muutoksia, jotka kaventavat tunnistamismääräyksen soveltamisalaa ja korostavat mahdollista tunnistamismääräystä edeltävää riskien lieventämistä ensisijaisena keinona, rajoittaa asetusehdotus edelleen huomattavasti palveluntarjoajien mahdollisuuksia tarjota tietoturvallisia viestintäpalveluita unionissa. Keskeisimmät haasteet liittyvät keskeisten tietosuojaperiaatteiden noudattamisen ja viestinnän luottamuksellisuuden tehokaan suojaamisen pitämiseen merkkinä asetusehdotuksen

[1] Asetusehdotuksen mukaisilla tunnistamismääräyksillä velvoitetaan palveluntarjoaja valvomaan automatisoidusti viestintää tiedossa olevan lapsiin kohdistuvan seksuaaliväkivaltaa todistavan kuvamateriaalin tunnistamiseksi.
[2] Päästä päähän -salauksella pyritään takaamaan, että lähettäjän ja vastaanottajan välinen viestintä pysyy salassa kaikilta muilta kuin viestinnän osapuolilta. Tällöin edes viestintää käyttäjien välillä välittävä taho ei pysty tarkastelemaan välitettävää sisältöä selkokielisenä eikä näin ollen pysty myöskään tunnistamaan siitä tiettyä sisältöä.

mukaisesta kohonneesta riskistä palvelussa sekä tunnistamismääräyksen ulottumiseen päästä päähän salattuun viestintään.

Asetusehdotukseen ei tehdyistä muutoksista huolimatta sisälly riittäviä takeita siitä, että tunnistamismääräykset eivät heikentäisi salausta tai vaarantaisi muutoin tietoturvaa. On erityisesti huomattava, että ehdotuksen 10 artiklan vaatimukset johtavat tosiasiassa väistämättä päästä päähän salauksen heikentämiseen ja kiertämiseen 1(5) artiklan estämättä.

Ehdotuksen perusteella päästä päähän-salatuissa palveluissa tunnistamismääräyksen edellyttämän viestinnän analysointi tapahtuisi päätelaitteen avulla viestintää välittävän tahon palvelimien sijaan. On kuitenkin huomattava, että myös tällaiseen päätelaitteella tapahtuvaan valvontaan liittyy erittäin vakavia huolia kyberturvallisuudesta sekä perusoikeuksien toteutumisesta. Se edellyttäisi päätelaitteella käsiteltävien tietojen analysointia ja palveluntarjoajan pääsyä analysoituihin tietoihin.[3] Tämän vuoksi on myös epäselvää, miten voitaisiin teknisesti varmistua siitä, että järjestelmiä ei voitaisi väärinkäyttää muun halutun viestinnän tunnistamiseen.

Vaikka sinällään on myönteistä, että tunnistamismääräys perustuu riskiluokitukseen, on huomattava, että tällöin asetusehdotuksen II osan ja liitteen XIV mukaiset arviointikriteerit ovat keskeisessä asemassa puuttumisen oikeasuhtaisuuden arvioinnissa. On selvää, että riskin arvioinnissa käytettävät mittarit vaikuttavat myös niiden palveluntarjoajien ja palveluiden toimintaan, joille ei anneta tunnistamismääräystä. Tältä osin on todettava olevan viestinnän luottamuksellisuuden ja tietoturvallisuuden kannalta erittäin kielteistä, että kyseisiin riski-indikaattoreihin kuuluu tavallisia ja keskeisiä viestinnän tietoturvallisuutta lisääviä toimenpiteitä, kuten oletusarvoisen päästä päähän -salauksen käyttö. Samoin alhaisen riskiluokituksen saaminen edellyttäisi palvelun käyttäjien tarpeetonta profiloimista. Asetusehdotuksessa on edelleen nähtävissä riski siitä, että tunnistamismääräysten antaminen voisi lopulta johtaa käytännössä varsin kattavaan ja pysyvään viestinnän luottamuksellisuuden ja tietoturvallisuuden heikentämiseen.

Tunnistamismääräykseen ja palvelun riskitason arviointiin liittyvät haasteet voivat johtaa ristiriitaan palveluntarjoajiin kohdistuvien tietoturvavaatimusten kanssa. Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY), teledirektiivi ((EU) 2018/1972) ja NIS2-direktiivi ((EU) 2022/2555) sekä niiden kansallinen voimaanpanolainsäädäntö edellyttävät viestintäpalveluiden tarjoajia huolehtimaan palveluidensa tietoturvasta. Päästä päähän -salauksen käyttöä pyritään erityisesti edistämään teledirektiivillä ja NIS2-direktiivillä[4], eikä asetusehdotuksen tulisi olla tämän tavoitteen kanssa ristiriidassa. 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. Ehdotus vaikuttaa kielteisesti

[3] Käytännössä päätelaitteella visuaalisesta aineistosta muodostettujen tunnisteiden vertailu tietokantaan tallennettuihin tunnisteisiin tapahtuisi muualla kuin käyttäjän päätelaitteella. Lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevalla kuvamateriaalin tunnistamiseen käytettävän URL- ja tiivistetietokannan sisällön pitämisen luottamuksellisena ehdotuksen 46 artiklan mukaisesti käytännössä edellyttää päätelaitteella muodostettujen tunnisteiden vertailua tietokantaan muualla kuin käyttäjän päätelaitteella.
[4] 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 telekuuntelun erotuksena asetusehdotuksen uusista tunnistamismääräyksistä. NIS2-direktiivin mukaan tällaisetkaan toimenpiteet eivät saisi "heikentää päästä päähän -salausta, joka on tehokkaan tietosuojan, yksityisyyden suojan ja viestinnän turvallisuuden kannalta kriittinen teknologia".

tietoturvatoimenpiteiden toteuttamiseen ja voi johtaa siihen, että tietoturvallisia palveluita tarjoavia palveluntarjoajia vetäytyy EU:n markkinoilta.

Näin ollen jo palvelun riskitason määrittämisessä käytettävät kriteerit ja pelkkä mahdollisuus tunnistamismääräyksen antamisesta heikentävät yleisesti ja erotuksettomasti palveluntarjoajien mahdollisuuksia varmistua palveluiden tietoturvallisuudesta. Tältä osin ehdotuksen 86 artiklan mukaista komissiolle delegoitavaa toimivaltaa päivittää kyseistä liitettä voidaan pitää sen erittäin keskeisen vaikutuksen vuoksi haastavana. Samoin riskiarvioinnissa käytettävien kriteerien määrityksen ongelmat ja tunnistamismääräyksen olemassaoloon liittyvät kielteiset tietoturvavaikutukset pahentavat edelleen ikärajavalvontaan liittyviä riskejä.

Estomääräysten toteuttamiseen liittyvien teknisten haasteiden osalta Liikenne- ja viestintävirasto viittaa valiokunnalle 26.9.2022 antamaansa asiantuntijalausuntoon.

Asetusehdotuksen tavoitteet ovat kiistämättömän tärkeitä, mutta toimien oikeasuhtaisuutta arvioitaessa on huomioitava ehdotetun sääntelyn negatiivisten vaikutusten kohdistuminen yleisesti ja erotuksetta kaikkiin asetuksen soveltamisalaan kuuluvien tietoyhteiskunnan palveluiden käyttäjiin, mukaan lukien palveluita käyttäviin lapsiin. On lisäksi huomattava käyttäjien voivan myös itse salata viestinsä ennen sen lähettämistä, jolloin palvelun salausta heikentävillä toimilla ei voitaisi tehokkaasti taata rikollisen toiminnan tunnistamista. Näiltä osin toimenpiteellä tosiasiassa saavutettava hyöty jää epäselväksi suhteessa siitä aiheutuviin perusoikeuksien rajoituksiin ja tietoturvavaikutuksiin.

Tuure Ilmarinen
lakimies
Liikenne- ja viestintävirasto