Penttilä
TIO / TTI

Lausunto
3.10.2023

Suuren valiokunnan työjaosto

U 69/2022 vp Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä ja sitä koskeva jatkokirjelmä UJ 19/2023 vp

Liikenne- ja viestintäministeriön asiantuntijalausunto

Suuren valiokunnan työjaosto on pyytänyt liikenne- ja viestintäministeriön lausuntoa koskien valtioneuvoston kirjelmää Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä ja sitä täydentävää jatkokirjelmää UJ 19/2023 vp. Liikenne- ja viestintäministeriö kiittää mahdollisuudesta lausua asiassa ja esittää lausuntonaan kunnioittavasti seuraavaa:

Liikenne- ja viestintäministeriötä on kuultu U-jatkokirjelmän valmistelussa, ja ministeriö voi yhtyä U-jatkokirjelmässä esitettyihin kantoihin. Pääministeri Petteri Orpon hallituksen ohjelman mukaan hallitus tiukentaa CAM- eli Child Abuse –materiaalia koskevaa sääntelyä vakavien rikosten uhreina olevien lasten suojelemiseksi (s. 196). Niin ikään hallitus määrittelee ja tunnistaa yhteiskunnan kannalta kriittiset tietovarannot, -palvelut ja -järjestelmät ja varmistaa näiden toimintavarmuuden sekä turvallisuuden. Myös tietosuojan ja kyberturvallisuuden osaaminen tulevat oleman aikaisempaa tärkeämpiä digitalisoituvissa ympäristöissä (s. 114).

Liikenne- ja viestintäministeriö pitää asetusehdotuksen tavoitetta lasten suojelemisesta erittäin kannatettavana ja tärkeänä. Julkisella vallalla on velvollisuus turvata lapsen oikeuksien toteutuminen myös digitaalisessa ympäristössä (ks. esim. YK:n lapsen oikeuksien komitean vuoden 2021 yleiskommentti nro 25 (CRC/C/GC/25)). YK:n lapsen oikeuksien komitea on osana Suomen määräaikaistarkastelua kesäkuussa 2023 suositellut tehostamaan puuttumista verkossa olevaan lapsen seksuaalista hyväksikäyttöä koskevaan materiaaliin (CRC/C/OPSC/FIN/CO/1, 24(e) kohta).

Liikenne- ja viestintäministeriön toimialan kannalta asetusehdotuksessa on erityisesti keskeistä sen laajakantoiset ja periaatteelliset vaikutukset viestinnän luottamuksellisuuden suojaan ja viestinnän salaukseen ja siten myös viestintäpalveluiden ja –järjestelmien turvallisuuteen. Nämä oikeudet eivät ole pelkästään vastakkaisia 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 painottaa valtioneuvoston kannassa ilmaistua ehdotuksen tavoitteiden ja perustuslain, EU:n perusoikeuskirjan ja Euroopan ihmisoikeussopimuksen asettamien reunaehtojen yhteensovittamista. Tältä osin jatkokirjelmässä eritellään myös ministeriön näkemyksen mukaan perustuslakivaliokunnan verrattain kriittistä lausuntoa (PeVL 53/2022 vp). Lisäksi kannanmuodostuksessa merkityksellistä on muu perustuslakivaliokunnan käytäntö. Perustuslakivaliokunta on katsonut, että perustuslain 1 §:n 3 momentti yhdessä perustuslain 22 §:ssä säädetyn perus- ja ihmisoikeuksien turvaamisvelvollisuuden kanssa merkitsee, että valtioneuvoston tulee osallistua EU-säädösehdotusten valmisteluun tavalla, joka turvaa perus- ja ihmisoikeuksia Suomen lisäksi koko Euroopan unionissa (ks. PeVL 31/2022 vp, s. 5-6). Perustuslakivaliokunta on myös tuonut esille, että valtioneuvosto on perustuslain 2 §:n 3 momentissa julkisen vallan käytön lakiperustaisuuden ja julkisen toiminnan lakisidonnaisuudesta säädetyn johdosta sidottu perustuslakiin myös EU-sääntelyn valmistelussa. Perustuslain 74 §:ssä perustuslakivaliokunnalle säädetystä valtiosääntöisestä tehtävästä johtuu, että mikäli perustuslakivaliokunta on perustellusti asettunut tietylle kannalle perustuslain tulkinnassa, ei vastakkaista kantaa voida pitää ainakaan selvänä ja riidattomana. Valtioneuvosto ei siten voi toimia EU-lainsäädännön valmistelussa vastoin perustuslakivaliokunnan ilmaisemaa selvää ja ehdotonta valtiosääntöoikeudellista kantaa. Velvollisuus ottaa valiokunnan kannanmuodostus asianmukaisesti huomioon on luonteeltaan oikeudellinen velvollisuus. Perustuslakivaliokunta on perustuslainmukaisuuden ensisijainen tulkitsija, ja perustuslainmukaisuutta koskevat kannanotot sitovat niin eduskunnan muita valiokuntia kuin valtioneuvostoa. (PeVL 16/2020 vp, s. 10).

Viestinnän luottamuksellisuuden suoja

Asetusehdotuksella luotaisiin sitova kehys ja luotaisiin uusia työkaluja, joilla lapsiin kohdistuvaan seksuaaliväkivaltaan ja tällaista väkivaltaa todistavan materiaalin levittämiseen voidaan puuttua. Ministeriö kiinnittää huomiota siihen, että suurimmasta osasta näistä asetusehdotuksella luotavista velvoitteista ei ole jäljellä merkittäviä neuvottelukysymyksiä. Liikenne- ja viestintäministeriö yhtyy U-jatkokirjelmässä esitettyyn positiiviseen arvioon siitä, että neuvotteluissa on saatu tehtyä muutoksia, joilla on lisätty viestintä- ja säilytyspalveluiden käyttöön liittyvien riskien arvioinnin ja riskiä vähentävien toimenpiteiden painoarvoa. Kyseisillä keinoilla puututaan viestintäalan yritysten omaisuudensuojaan ja elinkeinovapauteen, mutta ministeriö korostaa, että tällaisten ennakollisten ja kaikkien henkilöiden viestintään liittyviä perusoikeuksia vähemmän rajoittavien toimenpiteiden tulisi olla ensisijainen keino ongelmaan puuttumiseksi.

U-jatkokirjelmässä todetusti liikenne- ja viestintäministeriö kiinnittää huomiota siihen, että tunnistamismääräystä koskevaan sääntelyyn ei ole tehty neuvotteluissa merkittäviä muutoksia. Tätä kirjausta taustoittaa se, että neuvottelujen aikana ei ole saatu yhteisesti jaettua käsitystä siitä, missä laajuudessa tunnistamismääräyksen toteuttamisella puututtaisiin viestinnän sisältöön. Siten myös perusoikeutena taattuun viestinnän luottamuksellisuuden suojaan kohdistuvan loukkauksen laajuudesta on kuultu erilaisia arvioita. Tunnistamismääräyksellä palveluntarjoajat voitaisiin velvoittaa ennakollisesti käsittelemään palvelussaan jaettujen viestien

sisältöä mahdollisesti rikollisen aineiston tunnistamiseksi. Tunnistamismääräys kohdistuisi sekä julkisesti saatavilla olevaan materiaaliin että henkilöiden väliseen luottamukselliseen viestintään. Toistaiseksi vastaamattomia kysymyksiä liittyy esimerkiksi siihen, mikä olisi tunnistamismääräyksen maantieteellinen ulottuvuus ja siis yhden jäsenvaltion viranomaisten antaman tunnistamismääräyksen vaikutus toisessa jäsenvaltiossa sijaitseviin käyttäjiin. Yhdessä jäsenmaassa rikolliseksi arvioitu toiminta ei välttämättä täytä tunnusmerkistöä toisessa jäsenmaassa. Neuvottelujen aikana on esitetty myös huolia siitä, ovatko asetusehdotuksen suojatoimet riittävät estämään tunnistamisteknologian väärinkäytöksiä. Toinen kysymys on erityisesti groomingin tunnistamiseen käytettävien teknologioiden kehitystaso. Euroopan parlamentin tilaaman täydentävän vaikutustenarvioinnin[1] mukaan muun kuin englanninkielisen viestinnän tunnistamiseen käytettävät teknologiat eivät toistaiseksi ole riittävän kehittyneitä. Ehdotuksen tavoitteena on teknologianeutraalisuus, mikä jättää palveluntarjoajille paljon harkintaa tunnistamismääräyksen toteuttamiseen.

U-jatkokirjelmässä viitataan neuvoston oikeuspalvelun lausuntoon. Oikeuspalvelun lausuntoon on perusteltua kiinnittää erityisesti huomiota, sillä sen mukaan tunnistamismääräys on erityisen vakava yksityiselämän suojan ja henkilötietojen suojan rajoitus eikä ehdotettu sääntely vaikuta täyttävän perusoikeuksien rajoitusedellytyksiä, kuten lailla säätämisen vaatimusta, ydinalueen suojaa ja suhteellisuusperiaatetta. Neuvoston oikeuspalvelun arvion mukaan asetusehdotukseen sisältyy merkittävä riski siihen, että ehdotetut toimet eivät ole oikeassa suhteessa tavoiteltuun päämäärään eli kannatettavasta tavoitteestaan huolimatta toimenpiteet komission ehdottamassa laajuudessa ylittävät välttämättömän rajat. EU-oikeuden tuomien rajoitusten lisäksi myös U-jatkokirjelmässä on huomioitu, että ehdotettu sääntely ei nykyisessä muodossaan ole täysin ongelmatonta suhteessa perustuslaissa taattuun viestin salaisuuden suojaan.

Perusoikeuden rajoitusedellytysten mukaisesti liikenne- ja viestintäministeriö korostaa valtioneuvoston kannan mukaisia kirjauksia siitä, että tunnistamismääräyksen tulee olla kohdennettu ja sen tulee olla mahdollisimman kohdennettu henkilöihin, jotka liittyvät lapsiin kohdistuvien seksuaalirikosten selvittämiseen tai joiden voidaan epäillä olleen osallisina tällaisiin rikoksiin. EU-tuomioistuin on viestinnän luottamuksellisuutta koskevassa oikeuskäytännössään edellyttänyt, että lainsäädännön on täytettävä objektiiviset kriteerit, joilla luodaan yhteys säilytettävien tietojen ja tavoitellun päämäärän välille. Näiden edellytysten on erityisesti oltava käytännössä sellaisia, että niissä rajataan tehokkaasti toimenpiteen laajuus ja tätä kautta asianomainen yleisö. (Tele2 ja Watson –ratkaisu, yhdistetyt asiat C-203/15 ja C-698/15, ECLI:EU:C:2016:970, kohta 110). Näissä ratkaisuissa unionin tuomioistuin on usein pitänyt jäsenvaltioiden sääntelyä yleisenä ja erotuksettomana, vaikka jäsenvaltiot ovat pitäneet toimiansa kohdennettuina.

Liikenne- ja viestintäministeriö toistaa myös ensimmäisessä U-kirjelmässä todetun siitä, että asetusehdotus olisi uudenlaista sääntelyä erityisesti siltä

[1] 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.

osin, että siitä voisi seurata palveluntarjoajille velvollisuus käsitellä henkilöiden välistä viestintää rikollisen materiaalin tunnistamiseksi. Nykyisin viestinnän sisällön kuin myös viestinnän välitystietojen käsittelyn tarkoitukset on laissa rajattu, eivätkä palveluntarjoajat saa käsitellä viestin sisältöä esimerkiksi kaupallisia tai markkinointitarkoituksia varten. EU-tasolla hyväksyttiin tilapäinen poikkeusasetus ((EU) 2021/1232), jolla palveluntarjoajille on tarkkaan määritellyin suojakeinoin ja rajoituksin sekä salausta heikentämättä sallittu vapaaehtoinen viestinnän tietojen käsittely lapsiin kohdistuvan seksuaaliväkivallan torjumiseksi ja viranomaisille ilmoittamiseksi. Nyt käsiteltävänä olevalla asetusehdotuksella tämä tilapäinen poikkeus ja vapaaehtoisuuteen perustuva tunnistaminen kumottaisiin.

Viestinnän salaus ja viestintäpalveluiden ja –järjestelmien turvallisuus

Liikenne- ja viestintäministeriö painottaa valtioneuvoston kannan kirjausta siitä, että valtioneuvosto pitää tärkeänä, että ehdotetut toimet eivät vaaranna kyberturvallisuutta tai viestintä- ja tietojärjestelmien turvallisuutta. Ehdotettujen toimien tehokkuuden lisäksi tulee huolehtia siitä, ettei asetusehdotuksesta seuraa yleistä velvoitetta palveluntarjoajille purkaa viestinnän vahvaa salausta tai luopua vahvan salauksen käytöstä. Tätä kirjausta taustoittavasti ministeriö tuo seuraavan esille.

Suomi on tuonut EU-asioiden käsittelyssä vuosien ajan johdonmukaisesti esille, että sähköisten viestintäpalveluiden käyttäjillä tulee olla halutessaan oikeus ja mahdollisuus salata viestintänsä omien tarpeidensa mukaisesti. (U 58/2017 vp, UJ 29/2017 vp, LiVL 27/2017) Tässä yhteydessä on myös asiantuntijakuulemisiin perustuen todettu, että vahvaan salaukseen tehtäviä rajoituksia on teknisesti haastavaa toteuttaa ilman, että tällä samalla lisätään riskejä viestinnän ja järjestelmien turvallisuuden kannalta (LiVP 4/2021 vp, 9 § (LiV:n kannanotto asiaan E 153/2020 vp); viimeisimpänä salauksen heikentämisen vaikutuksista palvelun turvallisuuteen LiVL 5/2023 vp).

Ehdotuksen vaikutus viestinnän salaukseen on erittäin merkityksellistä sen arvioinnissa, miten laajakantoisia ja periaatteellisia vaikutuksia ehdotetulla sääntelyllä on mm. luottamuksellisen viestin salaisuuden suojaan verkossa. Ministeriö korostaa vahvan salauksen merkitystä digitaalisessa maailmassa toisaalta digitalisten järjestelmien ja toisaalta käyttäjien perusoikeuksien turvaamisessa. Salaus on tunnistettu esimerkiksi verkkoturvallisuutta koskevassa ns. NIS2-direktiivissä keskeisenä viestintäjärjestelmien turvallisuuden kannalta, ja erityisesti päästä päähän –salaus on tehokkaan tietosuojan, yksityisyydensuojan ja viestinnän turvallisuuden kannalta kriittinen teknologia. Liikenne- ja viestintäministeriö kiinnittää huomiota siihen, että salauksen heikentäminen heikentää aina palvelun tietoturvaa, ja sen negatiiviset vaikutukset kohdistuisivat kaikkiin käyttäjiin.

Viestinnän vahvan salauksen tärkeä merkitys perusoikeuksien suojaajana on tunnistettu YK:n yleiskokouksen ja ihmisoikeusneuvoston päätöslauselmissa, joissa jäsenvaltioilta on peräänkuulutettu salausteknologioiden käyttöön puuttumisesta pidättäytymistä. Myös YK:n lasten oikeuksien komitea on korostanut, että CSA-materiaalin tunnistaminen salatussa viestinnässä tulee olla tiukasti rajattua laillisuus-, välttämättömyys ja suhteellisuusperiaatteen mukaisesti. (CRCC/GC/25,

kappale 70; ks. myös kappale 59). YK:n ihmisoikeusvaltuutetun toimisto on 4.4.2022 päivätyssä raportissaan (A/HRC/51/17 The right to privacy in the digital age) suositellut valtioita välttämään kaikkia suoria tai epäsuoria yleisiä ja erotuksettomia rajoituksia salauksen käyttöön.

Valtioneuvoston kannassa todetusti asetusehdotuksesta ei tule seurata yleistä velvoitetta palveluntarjoajille purkaa viestinnän vahvaa salausta tai luopua vahvan salauksen käytöstä. Ottaen huomioon yllä olevan, liikenne- ja viestintäministeriön arvion mukaan sähköisen viestinnän salauksen heikennyksiä ei tulisi hyväksyä ennen kuin on luotettavasti osoitettu, etteivät ne tosiasiallisesti heikennä viestintä- ja tietojärjestelmien ja yleisemminkin sähköisen viestinnän turvallisuutta ja siten kansalaisten perusoikeuksia. Mikäli ehdotuksesta seuraisi velvoite purkaa viestinnän salausta, olisi sillä laajakantoisia ja periaatteellisia vaikutuksia luottamuksellisen viestin salaisuuden suojaan sekä muiden perusoikeuksien toteutumiseen verkossa. Ministeriö korostaa, että näin periaatteellisesti merkittävää ratkaisua ei tulisi jättää asetuksessa epäselväksi. Ministeriön arvion mukaan asetusehdotus viimeisimmän kompromissitekstin mukaisessa laajuudessa tarkoittaisi neuvoston oikeuspalvelun lausunnon mukaisesti, että palveluntarjoajien tulisi joko luopua tehokkaasta päästä päähän -salauksesta, luoda ns. takaovia päästäkseen salattuun sisältöön tai saada pääsy sisältöön käyttäjän päätelaitteella ennen sisällön salaamista. U-jatkokirjelmässäkin todetusti neuvoston oikeuspalvelu arvioi, että viestinnän yleinen käsittely CSA-materiaalin tunnistamiseksi edellyttäisi *de facto* tietoturvatoimenpiteiden, erityisesti päästä päähän -salauksen, kieltämistä, heikentämistä tai muutoin kiertämistä, jotta kyseinen tunnistaminen olisi mahdollista.

Ministeriö korostaa, että neuvotteluissa tarvitaan vielä ponnekasta vaikuttamistyötä, jotta tämä näkökulma tulee riittävällä varmuudella katetuksi neuvoston kannassa. Samalla käsittelyssä tulee erottaa palveluntarjoajille asetettavat yleiset ja erotuksettomat velvoitteet ja niiden kaikkiin käyttäjiin kohdistuvat vaikutukset, sekä toimivaltaisten viranomaisten mahdollisuudet saada tarkkarajainen ja oikeasuhtainen pääsy salattuun tietoon yksittäistapauksissa toimivaltuuksiensa puitteissa. Ministeriö korostaa, että asetusehdotuksessa ei säännellä viranomaisten toimivaltuuksista ja mahdollisuuksista kohdistaa esimerkiksi telekuuntelua rikoksesta epäiltyihin, vaan asetusehdotuksessa säännellään pääasiassa palveluntarjoajiin kohdistettavia velvoitteita, joka tunnistamismääräyksen nykyisessä muodossa tarkoittaisi palveluntarjoajalle kohdistettavaa määräystä käsitellä ennakollisesti viestinnän sisältöä ilman viranomaisen vahvistamaa tietyn henkilön liityntää selvitettävään tai ehkäistävään rikollisuuteen.

Lopuksi liikenne- ja viestintäministeriö kiinnittää huomiota U-kirjelmässä 69/2022 vp esitettyyn kantaan, että palveluntarjoajia ei tule vaatia valvomaan (monitoroimaan) sisältöjen laillisuutta yleisesti. Tämä on merkityksellinen myös U-jatkokirjelmän mukaisen kannan kannalta, että sääntelyä olisi pyrittävä edelleen täsmentämään sen varmistamiseksi, että se täyttää sääntelyn selkeyttä, ennakoitavuutta, välttämättömyyttä, oikeasuhtaisuutta, perusoikeuden ydinalueen suojaa ja oikeussuojaa koskevat vaatimukset.

Pauliina Penttilä

Ylitarkastaja
Tietoliiketoimintayksikkö
Tieto- ja turvallisuusosasto