Eduskunnan perustuslakivaliokunnalle

Asia: Jatkokirjelmä UJ 2/2025 vp - U 69/2022 vp Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final)

Tausta

Komission mukaan lapsiin kohdistuva seksuaaliväkivalta on kasvanut viime vuosina räjähdysmäisesti. Se käsittää sekä lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan kuvamateriaalin jakamisen että lasten houkuttelemisen seksuaalitekoihin (”grooming”) ja jopa väkivallantekijöiden tapaamiseen verkon ulkopuolella.

Euroopan komissio antoi 11.5.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ennaltaehkäisemiseksi ja torjumiseksi (ns. CSAM-ehdotus; COM (2022) 209 final). Vaikka yksimielisyys vallitsee siitä, että asetusehdotuksella tavoitellaan tärkeää ja hyväksyttävää päämäärää, ehdotuksen käsittely on ollut hidasta, koska päämäärään on pyritty sellaisin keinoin, joiden on nähty muodostavan uhkia mm. tietosujalle, yksityiselämän suojalle, luottamuksellisen viestin suojalle ja sananvapaudelle.

Kysymys on PL 96 §:ssä tarkoitetusta asiasta, joten se käsitellään U-kirjelmänä.

Perustuslakivaliokunta on lausunnossaan PeVL 20/2021 katsonut, että Suomen perustuslaissa turvatut perusoikeudet ovat merkityksellisiä myös EU-sääntelyn valmistelussa.[1] Suomen perustuslain tulee siten ohjata valtioneuvoston kannanmuodostusta EU-lainsäädännön

[1] Esim. PeVL 15/2017 vp, s. 4 ja PeVL 9/2017 vp, s. 5—6 ja niissä viitatut lausunnot.

valmistelussa.[2] Lisäksi perustuslakivaliokunnan mielestä 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.[3]

Eduskunnan perustuslakivaliokunta on antanut CSAM-asiaa käsiteltäessä lausunnot PeVL 53/2022 vp (U 69/2022 vp), PeVL 5/2023 vp (jatkokirjelmä UJ 19/2023 vp — U 69/2022 vp) ja PeVL 47/2024 vp ─ U 69/2022 vp. Edellisellä kerralla asian käsittelyn pohjana olivat suuren valiokunnan perustuslakivaliokunnalle lähettämät asiakirjat eli Sisäministeriön perusmuistio 25.9.2024 EU/88/2022-SM-52, sisäministeriön lausunto 8.10.2024 EUN 78/2024 vp ja tuorein CSAM-ehdotus per 7.10.2024. Tällä kertaa lausuntopyyntöön on oheistettu U 69/2022 kirjelmän lisäksi Sisäministeriön 1.4.2025 päivätty perusmuistio EU/88/2022-SM-63. Arvioinnin kohteena ovat edellä mainitussa perusmuistiossa esitetyt näkökohdat.

Lähtökohdat

Perustuslakivaliokunta on katsonut lausunnoissaan 53/2022 vp, 5/2023 vp ja 47/2024 vp, että asetusehdotuksella on selvästi hyväksyttävä ja erittäin painava tavoite suojata lapsia verkkovälitteiseltä seksuaaliväkivallalta. Tavoite on yhteydessä useisiin perustuslaissa ja kansainvälisissä ihmisoikeussopimuksissa turvattuihin perus- ja ihmisoikeuksiin. Perustuslakivaliokunta on pitänyt valtioneuvoston tavoin erittäin tärkeänä, että verkossa tapahtuvaan lapsiin kohdistuvaan seksuaaliväkivaltaan pystytään puuttumaan tehokkaasti. Kuten perustuslakivaliokunta on todennut, myös YK:n lapsen oikeuksien sopimus sekä lasten suojelemisesta seksuaalista riistoa ja seksuaalista hyväksikäyttöä vastaan tehty Euroopan neuvoston yleissopimus (ns. Lanzaroten sopimus) ja naisiin kohdistuvan väkivallan ja perheväkivallan ehkäisemisestä ja torjumisesta tehty Euroopan neuvoston yleissopimus (ns. Istanbulin sopimus) velvoittavat ryhtymään tehokkaisiin toimiin lasten suojaamiseksi väkivallalta. Tätä edellyttää myös perustuslain 22 pykälässä säädetty perus- ja ihmisoikeuksien turvaamisvelvollisuus, joka koskee myös oikeuksien toteutumista yksitysten välisissä suhteissa.

Asetusehdotuksen keskeisimmät haasteet ovat liittyneet tunnistamismääräykseen (artikla 7), jonka nojalla soveltamisalaan kuuluvia palveluntarjoajia eli säilytyspalvelun ja henkilöiden välisen viestintäpalvelun tarjoajia olisi voitu viranomaismääräyksellä velvoittaa tunnistamaan lapsiin kohdistuvaa seksuaalista väkivaltaa esittävää materiaalia (CSA-materiaalia) sekä lasten houkuttelemista seksuaalisiin tarkoituksiin (ns. grooming) alustoillaan ja ilmoittamaan siitä viranomaisille, ja erityisesti tunnistamismääräyksen suhteeseen luottamuksellisen viestinnän suojaan sekä viestinnän salaukseen.

[2] PeVL 20/ 2017 vp, s. 6.
[3] PeVL 20/2017 vp, s. 6, PeVL 53/2017 vp, s. 5.

Perustuslakivalioikunta katsoi edellisessä asiaa koskeavassa lausunnossaan PeVL 47/2022, että tehdyistä parannuksista huolimatta ehdotettu tunnistamismääräystä koskeva sääntely ei ollut valtiosääntöoikeudellisesti ongelmatonta erityisesti perustuslain 10 §:n 2 ja 4 momentissa turvatun luottamuksellisen viestin salaisuuden kannalta. Pelkkä riskiarvio ja tunnistamismääräyksen kohdentumisen yleisyys merkitsivät "hyvin selvää etääntymistä siitä perustuslain 10 §:n 4 momenttiin liittyvästä vaatimuksesta, jonka mukaan rikosperusteinen puuttuminen luottamuksellisen viestin salaisuuteen edellyttää konkreettista ja yksilöityä rikosepäilyä." Lisäksi pidettiin ongelmallisena sitä, että tunnistamimääräys olisi kohdistunut edelleen palveluntarjoajiin ja heidän osaltaan lähtökohtaisesti kaikkien palveluja käyttävien viestintään, jolloin sen soveltaminen olisi saattanut muodostua varsin laajaksi ja yksilöimättömäksi.[4]

Perustuslakivaliokunta kiinnitti huomiota myös siihen, oliko tunnistamismääräystä koskeva sääntely tosiasiassa soveltuvaa valiokunnan sinänsä hyväksyttävänä ja erittäin painavana pitämään sääntelyn tavoitteeseen pääsemiseksi. Kanta liittynee siihen, että useat asiantuntijat olivat katsoneet, että ehdotettu perus- ja ihmisoikeuksiin puuttuva menettely ei tosiasiassa olisi ollut kovin tehokas keino CSA-materiaalin levittämisen ehkäisemiseen.

Sisäministeriön perusmuistion (1.4.2025) mukaan tuorein asetusehdotus perustuu puheenjohtajamaan Puolan 28.1.2025 jakamaan kompromissiehdotukseen. Ehdotuksen soveltamisalasta on poistettu kokonaan tunnistamismääräys ja siihen suoraan kytkeytyvät artiklat (7-11 artiklat). Tekstistä on siten poistettu esimerkiksi aiempaan ehdotukseen sisältynyt toiminto, jolla laitonta sisältöä olisi voitu tunnistaa salattua ympäristöä käyttävissä palveluissa ns. hash-lukuja vertaamalla ennen viestin salaamista ja lähettämistä.

Tunnistamismääräystä koskeva kompromissiehdotus

Tunnistamismääräyksen sijaan puheenjohtajamaa on ehdottanut niin sanotulla poikkeusasetuksella[5] tietyille palveluntarjoajille mahdollistettujen vapaaehtoisten käsittelytoimenpiteiden tuomista pysyvän sääntelyn piiriin (uusi artikla 4a). Toisin sanoen CSAM-asetuksella ehdotettaisiin vakiinnutettavaksi tilapäisen poikkeusasetuksen nojalla sovellettu menettely, joka mahdollistaisi sen, että numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajat voisivat käyttää erityisiä teknologioita henkilötietojen ja muiden tietojen käsittelyyn siinä laajuudessa kuin on ehdottoman välttämätöntä niiden

[4] PeVL 53/2022 vp, kappale 10, PeVL 5/2023 vp, kappale 4, PeVL 47/2024, kappale 8.
[5] EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2021/1232, annettu 14 päivänä heinäkuuta 2021, tilapäisestä poikkeuksesta direktiivin 2002/58/EY tiettyihin säännöksiin siltä osin kuin on kyse teknologioista, joita numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajat käyttävät henkilötietojen ja muiden tietojen käsittelyyn verkossa tapahtuvan lasten seksuaalisen hyväksikäytön torjumiseksi (tilapäinen poikkeusasetus). Asetuksen voimassaoloa on jatkettu 3.4.2026 saakka.

palveluissa välitetyn CSA-materiaalin tai siellä tapahtuvan groomingin havaitsemiseksi ja siitä ilmoittamiseksi ja kyseisen materiaalin poistamiseksi.

Numeroista riippumattomalla henkilöiden välisellä viestintäpalvelulla tarkoitetaan henkilöiden välisen viestinnän palvelua, joka ei yhdisty kansallisessa tai kansainvälisessä numerointisuunnitelmassa olevan numeron tai olevien numeroiden avulla. Tällaisia ovat Sisäministeriön perusmuistion mukaan esimerkiksi pikaviestintään tarkoitetut, internetin välityksellä toimivat puhe-, video-, videoneuvottelu- ja pikaviestipalvelut kuten WhatsApp tai Facebook Messenger.

Puheenjohtajan kompromissitekstin pohjalta olisi mahdollista tunnistaa sekä tunnettua että uutta CSA-materiaalia, ja lasten houkuttelua (grooming). Sähköisen viestinnän käsittely tapahtuisi teknologisin menetelmin ja sen olisi täytettävä asetusehdotuksessa määritellyt varsin tiukat ehdot, kuten mm. suhteellisuus- ja välttämättömyysvaatimus. Käytettävien teknologioiden olisi puututtava yksityisyyteen mahdollisimman vähän. Tekstin käsittelyn osalta edellytyksenä olisi, ettei teknologialla voitaisi päätellä viestinnän sisältöä vaan ainoastaan tunnistaa sellaisia toimintamalleja, jotka viittaavat mahdolliseen lasten hyväksikäyttöön.

Kyse olisi viestintäpalvelun tarjoajien osalta vapaaehtoisesta toiminnasta. Asetuksella ei kiellettäisi, kierrettäisi tai heikennettäisi kyberturvallisuustoimenpiteitä eikä luotaisi velvoitteita purkaa päästä päähän -salausta tai rajoittaa sen käyttöä. Sisäministeriön muistion mukaan tunnistamismääräyksen poistamisen myötä myös salattuihin viestisisältöihin liittyvä ja asian käsittelyssä ongelmalliseksi tunnistettu (SuVL 10/2024 vp, 8. kappale) epäselvyys poistuisi. Muistiossa viitatussa Suuren valiokunnan lausunnon kohdassa oli kyse viestinnän massavalvonnasta sekä siitä, että ehdotettu malli olisi tosiasiassa kiertänyt viestinnän päästä päähän -salauksen tarkoituksen.

Toisin kuin edellisessä ehdotuksessa, uusimmassa kompromissiehdotuksessa palveluntarjoajia ei velvoitettaisi toimeenpanemaan CSA-materiaalin levittämiseen liittyviä riskejä lieventäviä toimenpiteitä. Palveluntarjoajia koskevat riskinarviointi- tai ennaltaehkäisymenetelmät tulisi toteuttaa vain suositusperusteisesti. Lisäksi korkean riskin palveluntarjoajilla olisi velvollisuus tarjota tehokkaita vaihtoehtoisia ilmoitusmekanismeja palvelun käyttäjille CSA-materiaaliin kytkeytyvissä tapauksissa (12 artikla).

Ehdotuksessa säädettäisiin tilapäistä poikkeusasetusta tarkemmin yritysten vapaaehtoisista toimista CSA-materiaalin tunnistamiseksi. Ehdotukseen on sisällytetty seuraavia suojakeinoja:

- palveluntarjoajien olisi varmistettava, etteivät heidän vapaaehtoiset CSA-materiaalin tunnistustoimenpiteensä luo hallitsemattomia riskejä kyberturvallisuudelle
- palveluntarjoajien olisi pidettävä yksityiskohtaisia lokitietoja toiminnoistaan sisäistä ja ulkoista tarkastelua sekä mahdollista rikosoikeudellista menettelyä varten

Arviointi

Lähtökohdat

Tilapäistä poikkeusasetusta ei sen säätämisvaiheessa arvioitu perustuslakivaliokunnassa eikä sen suhteesta Euroopan unionin perusoikeuskirjaan ole EU-tuomioistuimen oikeuskäytäntöä. Aikaisemmin hyväksyttyä ns. poikkeusasetusta koskevassa Valtioneuvoston kirjelmässä U 50/2020 on tarkasteltu sääntelyn suhdetta perustuslakiin sekä perus- ja ihmisoikeusvelvoitteisiin hyvin ylimalkaisesti ja asetusta on pidetty EU:n perusoikeuskirjan 7 artiklan mukaisena.[6] Ongelmia ei ole esitetty olevan myöskään viestin luottamuksellisuuden, sananvapauden tai henkilötietojen suojan osalta.[7]

Perusoikeuksia voidaan rajoittaa, kun rajoitukset ovat lailla säädettyjä, täsmällisiä ja tarkkarajaisia, rajoitus on hyväksyttävä ja oikeassa suhteessa hyväksyttävään päämäärään, perusoikeuden ydintä ei rajoiteta, oikeusturvajärjestelyistä on huolehdittu ja ihmisoikeusvelvoitteita on noudatettu.[8]

Euroopan neuvoston ihmisoikeussopimus (EIS) asettaa yksityiselämän suojan (ml. henkilötietojen suoja) ja sananvapauden rajoittamisen edellytykseksi sen, että rajoituksista on säädetty lailla tietyn kyseissä artiklassa (8 ja 10 artiklat) säädetyn oikeushyvän turvaamiseksi ja että rajoitus on välttämätön demokraattisessa yhteiskunnassa.

EU:n perusoikeuskirjan (POK) 7 artiklassa turvataan yksityis- ja perhe-elämän suoja ja 8 artiklassa henkilötietojen suoja. POK 52(1) artiklan mukaan "Tässä perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia."

Suhteellisuusperiaatetta on arvioitu EUT:ssa, jonka mukaan "rajoituksia voidaan tehdä ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. Rajoitukset on toteutettava täysin välttämättömän rajoissa, ja kyseessä olevat rajoitukset sisältävässä säännöstössä on säädettävä selvistä ja täsmällisistä näiden rajoitusten laajuutta ja soveltamista koskevista säännöistä.[9] Suhteellisuusperiaatetta koskeva vaatimus "ei täyty, jos asetettu yleisen edun mukainen tavoite voidaan kohtuudella saavuttaa yhtä tehokkaasti muilla rekisteröityjen perusoikeuksia vähemmän rajoittavilla keinoilla".[10] Perusoikeuksien

[6] U 50/2020 s. 4-
[7] U 50/2020 s. 4-5.
[8] PeVM 25/1994 ja useat sen jälkeiset lausunnot.
[9] Tuomio 30.1.2024, *Direktor na Glavna direktsia "Natsionalna politsia" pri MVR – Sofia*, C-118/22, 39 kohta oikeuskäytäntöviittauksineen.
[10] C-118/22, 40 kohta oikeuskäytäntöviittauksineen sekä *CG v. vastaan Bezirkshauptmannschaft Landeck*, C-548/21, kohta 87.

rajoittamisen oikeasuhtaisuuden arviointi edellyttää kaikkien yksittäistapauksen merkityksellisten seikkojen punnintaa.[11] Kannabista koskevan huumausainerikoksen ja siihen liittyvien matkapuhelimessa olevien tietojen tutkintaa koskevassa tapauksessa tuoreessa tapauksessa C-548/21näitä olivat muun muassa perusoikeuksien käyttämiselle asetetun rajoituksen vakavuus, joka riippui niiden tietojen luonteesta ja arkaluonteisuudesta, joihin toimivaltaiset poliisiviranomaiset saattoivat saada pääsyn; rajoituksella tavoitellun yleisen edun mukaisen tavoitteen merkitys; matkapuhelimen omistajan yhteys kyseessä olevaan rikokseen ja kyseisten tietojen merkityksellisyys tosiseikkojen toteamisen kannalta (kohta 90). Tuomion mukaan tutkinnan kohteena olevan rikoksen vakavuus on yksi keskeisistä tekijöistä silloin, kun tutkitaan sen vakavan puuttumisen oikeasuhteisuutta, joka aiheutuu pääsystä matkapuhelimen sisältämiin henkilötietoihin, joiden perusteella voidaan tehdä täsmällisiä päätelmiä rekisteröidyn yksityiselämästä (kohta 96). Merkitystä ei kuitenkaan voida antaa pelkästään sille, koska muutoin rajoitettaisiin toimivaltaisten viranomaisten direktiivin 2016/680 mukaisia valtuuksia tutkia rikoksia yleisesti (kohta 97).

Lailla säätämisen vaatimus edellyttää, että lain säännökset ovat riittävän yksityiskohtaiset ja selkeät siten, että yksilöt pystyvät ennakoimaan toimintansa seuraukset. EUT on ratkaisussa C-548/21 katsonut, että rajoituksen ulottuvuus on määriteltävä riittävän selvästi ja täsmällisesti (kohta 98 oikeuskäytäntöviittauksineen).

EUT on edellä mainitussa matkapuhelimen sisältämien tietojen tutkimista huumausainerikoksen selvittämiseksi koskevassa tuomiossa C-548/21 katsonut, että kun “kyse on erityisesti pääsystä rikostutkinnan kohteena olevan henkilön matkapuhelimen sisältämiin tietoihin, on tärkeää, että perusteltua epäilyä siitä, että kyseinen henkilö on tehnyt, tekee tai suunnittelee tekevänsä rikoksen tai on tavalla tai toisella osallisena rikoksessa, tuetaan objektiivisilla ja riittävillä seikoilla.” (kohta 101). Suhteellisuusperiaatteen noudattamisen varmistamiseksi EUT piti olennaisen tärkeänä, että “kun toimivaltaisten kansallisten viranomaisten pääsy henkilötietoihin aiheuttaa vaaran vakavasta tai jopa erityisen vakavasta puutumisesta rekisteröidyn perusoikeuksiin, tämä pääsy edellyttää joko tuomioistuimen tai riippumattoman hallintoelimen suorittamaa etukäteisvalvontaa.” (kohta 102) “Erityisesti rikostutkinnan osalta tällainen valvonta edellyttää, että kyseinen tuomioistuin tai elin pystyy varmistamaan oikeudenmukaisen tasapainon yhtäältä rikollisuuden torjunnan yhteydessä suoritettavan tutkinnan tarpeisiin liittyvien oikeutettujen intressien ja toisaalta henkilöiden, joiden tietoihin pääsy koskee, yksityiselämän kunnioittamista ja henkilötietojen suojaa koskevien perusoikeuksien välillä.” (kohta 103) Tuomion mukaan toimivaltaisten poliisiviranomaisten pääsy matkapuhelimen sisältämiin tietoihin on “evättävä tai sitä on rajoitettava, jos pääsy viestinnän sisältöön tai arkaluonteisiin tietoihin ei vaikuta oikeutetulta ottaen huomioon rikoksen vakavuus ja tutkinnan tarpeet.”

Tuomion C-548/21 mukaan “direktiivin 2016/680 4 artiklan 1 kohdan c alakohtaa, luettuna perusoikeuskirjan 7 ja 8 artiklan sekä 52 artiklan 1 kohdan valossa, on tulkittava siten, että se ei ole esteenä kansalliselle lainsäädännölle, jossa annetaan toimivaltaisille viranomaisille

[11] C-118/22, 62 ja 63 kohta oikeuskäytäntöviittauksineen ja C-548/21, kohta 89.

mahdollisuus saada yleisesti pääsy matkapuhelimen sisältämiin tietoihin rikosten torjuntaa, tutkintaa, selvittämistä ja syyteharkintaa varten, jos kyseisessä lainsäädännössä

- määritellään riittävän täsmällisesti kyseisten rikosten luonne tai niiden ryhmät,
- taataan suhteellisuusperiaatteen noudattaminen ja
- asetetaan asianmukaisesti perusteltuja kiireellisiä tapauksia lukuun ottamatta tämän mahdollisuuden käyttämisen edellytykseksi tuomioistuimen tai riippumattoman hallintoelimen suorittama etukäteisvalvonta."

Direktiivin 2016/680 13 ja 54 artiklaa, luettuina perusoikeuskirjan 47 artiklan ja 52 artiklan 1 kohdan valossa, oli tulkittava siten, että

- ne ovat esteenä kansalliselle lainsäädännölle, jonka mukaan toimivaltaiset viranomaiset voivat yrittää saada pääsyn matkapuhelimen sisältämiin tietoihin ilmoittamatta rekisteröidylle sovellettavien kansallisten menettelyjen yhteydessä syitä, joihin tuomioistuimen tai riippumattoman hallintoelimen antama lupa saada pääsy tällaisiin tietoihin perustuu, heti kun näiden tietojen ilmoittaminen ei voi enää vaarantaa näille viranomaisille kyseisen direktiivin nojalla kuuluvia tehtäviä.

CSA-materiaalia koskevassa asiassa tarkastelu kaiketi kohdistuisi muihinkin kuin lainvastaisiin viesteihin ja muihinkin henkilöihin kuin rikoksesta epäiltyihin, mutta tarkastelu ei kaiketi ulottuisi yhtä syvälle yksityisyyteen kuin matkapuhelintietojen tarkastelu. Tarkempaa tietoa siitä, miten palveluntarjoaja päättelisi viestien sisältävän CSA-materiaalia tai ns. groomingia ei Sisäministeriön perusmuistiossa ole annettu. Matkapuhelimesta puolestaan voidaan löytää mm. sijaintitietoja, verkkoselailuhistoriaa, viestejä, kuvia ja muistiinpanoja, jotka voivat kertoa sen käyttäjästä hyvin henkilökohtaisia ja ns. arkaluonteisia tietoja (tietosuoja-asetus käyttää termiä erityisiin henkilötietoryhmiin kuuluvat tiedot). Tilanteet eivät siis ole samanlaisia. Samankaltaisia periaatteita kuitenkin sovelletaan molemmissa tapauksissa.

Rajoitustoimenpiteistä säädettäisiin EU:n asetuksessa ja sääntelyllä on hyväksyttävä tavoite, lasten suojeleminen verkkovälitteiseltä seksuaaliväkivallalta. Näin ollen lailla säätämisen vaatimus toteutuisi, jos sääntely olisi tarpeeksi täsmällistä. Täsmällisyyttä ei kuitenkaan Sisäministeriön perusmuistion perusteella pysty arvioimaan.

Lisäksi on otettava huomioon, että POK 24 artiklan mukaan kaikissa lasta koskevissa viranomaisten tai yksityisten laitosten toimissa on ensisijaisesti otettava huomioon lapsen etu. Tämä saattaa joissakin tapauksissa puoltaa hieman pidemmälle meneviä perusoikeuden rajoituksia lasten oikeuksien suojelemiseksi kuin jos kysymyksessä olisi muunlainen suojattava intressi.

Yksityiselämän, henkilötietojen ja luottamuksellisen viestin suoja

Viestinnnän tapa

Sisäministeriön perusmuistiosta ei ilmene, miksi ehdotettu menettely rajattaisiin (ja on jo poikkeusasetuksessa rajattu) koskemaan vain numeroista riippumattomia viestintäpalveluita. Direktiivin (EU) 2018/1972[12] 2 artiklan 7 kohdan mukaan numeroista riippumattomalla henkilöiden välisellä viestintäpalvelulla tarkoitetaan "henkilöiden välistä viestintäpalvelua, joka ei yhdisty yleiseen käyttöön osoitettujen numerovarojen eli kansallisessa tai kansainvälisessä numerointisuunnitelmassa olevan numeron tai olevien numeroiden avulla tai mahdollistamalla viestinnän kansallisessa tai kansainvälisessä numerointisuunnitelmassa olevan numeron tai olevien numeroiden kanssa".

Vaikka tämänkaltainen sääntely rajaisi sen soveltamiasalan piiristä numeroon sidotut viestintätavat, olisi sen soveltamisala edelleen laaja. Sisäministeriön muistion mukaan sääntelyn piirissä olisivat "internetin välityksellä toimivat puhe-, video-, videoneuvottelu- ja pikaviestipalvelut kuten WhatsApp tai Facebook Messenger." Tästä päätellen sääntely soveltuisi myös sähköpostiviestintään sekä esimerkiksi Teamsin ja Zoomin avulla tapahtuvaan viestintään. Esimerkiksi videoneuvotteluun tai sähköpostiviestien lähettämiseen kohdistuvia rajoituksia ei voitane pitää yhtään lievempinä kuin jos valvonta kohdistuisi Teamsin kautta otetun videopuhelun sijaan puhelimen kautta toimitettuun videopuheluun tai puheluun taikka sähköpostiviestien sijaan puhelimella lähetettyihin tekstiviesteihin.

Viestien lähettäjille tai vastaanottajille ei välttämättä ole selvää, sovelletaanko heidän viestintäänsä poikkeusasetusta ja sovellettaisiinko siihen nyt ehdotettua sääntelyä vai ei. Esimerkiksi Sisäministeriön mukaan WhatsApp on numerosta riippumaton, mutta tiedotusvälineiden mukaan se ei vielä lokakuussa 2024 ollut numerosta riippumaton.[13] Käytännössä WhatsAppilla viestitään juuri puhelinnumeron avulla.

Sisäministeriön perusmuistiossa ei mainita, lähetetäänkö CSA-materiaalia enemmän juuri poikkeusasetuksessa kuvatuilla numeroista riippumattomilla viestintäpalveluilla verrattuna asetusehdotuksen ulkopuolelle jääviin viestintätapoihin. Näin ollen ehdotetun sääntelyn tehokkuus voidaan kyseenalaistaa sillä perusteella, että onko sen avulla mahdollista torjua lapsiin kohdistuvaa seksuaaliväkivaltaa niin tehokkaasti, että esitetty puuttuminen yksityiselämän ja henkilötietojen suojaan sekä luottamukselliseen viestintään olisi oikeasuhtaista. Kun sääntely ei ulottuisi numeroihin sidottuihin viestintätapoihin, niin eikö olisi oletettavaa, että CSA-materiaalia lähetettäisiin kiinni jäämisen ehkäisemiseksi juuri näillä sääntelyn ulottumattomissa olevilla numeroon perustuvilla viestintätavoilla? Toki numeropalveluiden käyttämistä lainvastaisiin tarkoituksiin hillinnee se, että rikoksentekijä on

[12] EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI (EU) 2018/1972, annettu 11 päivänä joulukuuta 2018, eurooppalaisesta sähköisen viestinnän säännöstöstä (uudelleenlaadittu) (ETA:n kannalta merkityksellinen teksti).

[13] Henrik Kärkkäinen: WhatsAppiin tärkeä päivitys – enteilee perustavanlaista muutosta sovelluksessa, Ilta Sanomat 23.10.2024, https://www.is.fi/digitoday/mobiili/art-2000010781890.html (luettu 11.5.2025).

monesti helpommin selvitettävissä kuin eräiden numerosta riipppumattomien verkkopalveluiden osalta. Toki kiinijäämisriskiä voidaan vähentää käyttämällä prepaid-liittymiä.

Viestinnän kohdentuminen

Aikaisemmin ehdotettu tunnistamismääräys olisi kohdistunut lähtökohtaisesti kaikkien palveluja käyttävien viestintään, jolloin sen soveltaminen olisi saattanut muodostua varsin laajaksi ja yksilöimättömäksi.[14] Perustusvaliokunta ei tämän vuoksi pitänyt ehdotettua tunnistamismääräystä koskevaa sääntelyä valtiosääntöoikeudellisesti ongelmattomana erityisesti perustuslain 10 §:n 2 ja 4 momentissa turvatun luottamuksellisen viestin salaisuuden kannalta. Luottamuksellisen viestinnän suojaa arvioitaessa on huomattava, että se ulottuu paitsi viestin lähettäjään myös sen vastaanottajaan.[15] Viestin sisällön lisäksi perustuslain säännöksillä suojataan myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle. Viestin tunnistamistiedot eivät kuitenkaan kuulu luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueelle.[16]

Esitettyjen tietojen valossa jäi epäselväksi, millaisia toimenpiteitä palveluntarjoajat voisivat tehdä CSA-materiaalin levittämisen ja groomingin estämiseksi, miten viestinnän osapuolia informoitaisiin tällaisesta mahdollisuudesta ja millaisia oikeusturvakeinoja viestinnän osapuolilla olisi. Toimenpiteet voisivat kohdistua lähtökohtaisesti kaikkien palveluja käyttävien viestintään, jolloin niiden soveltaminen voisi muodostua varsin laajaksi ja yksilöimättömäksi.[17] Tähän liittyvä ongelma ei nähdäkseni ratkea sillä, että tunnistamismääräyksen sijaan palveluntarjoajille annettaisiin mahdollisuus suorittaa näitä "valvontatoimia" vapaaehtoisesti. Pikemminkin näen sananvapauden, yksityiselämän suojan, henkilötietojen suojan ja luottamuksellisen viestinnän suojan kannalta arveluttavalta, että viestintäpalveluntarjoaja voisi vapaehtoisesti ryhtyä tai olla ryhtymättä "valvomaan" viestinnän sisältöä. Se, että palveluntarjoaja tekisi nämä toimeet vapaaehtoisesti ei nähdäkseni tee puuttumisesta viestinnän osapuolten kannalta yhtään lievempää.

Yksityinen taho ei myöskään toimi samanlaisen virkavastuun nojalla kuin poliisit tai muut virkahenkilöt rikoksia tai muita lainvastaisuuksia selvittäessään, joten viestinnän osapuolten oikeusturva ja asema voisi jäädä heikoksi. Jos tällaiseen malliin päädyttäisiin, tulisi palveluntarjoajien toimien lainmukaisuutta ja asianmukaisuutta valvoa tehokkaasti.

[14] Ks. PeVL 53/2022 vp, kappale 10, PeVL 5/2023 vp, kappale 4, PeVl 47/2024, kappale 8.
[15] HE 309/1993 vp, s. 53–54, ks. esim. PeVL 33/2013 vp, s. 3/I, PeVL 32/2013 vp, s. 3/I, PeVL 19/2008 vp, s. 3, PeVL 59/2006 vp, s. 2, PeVL 16/2004 vp, s. 6, PeVL 10/2004 vp, s. 4–5.
[16] Esim. PeVL 33/2013 vp, s. 3, PeVL 32/2013 vp, s. 3, PeVL 6/2012 vp, s. 3–4, PeVL 67/2010 vp, s. 4, PeVL 66/2010 vp, s. 7, PeVL 62/2010 vp, s. 4.
[17] Ks. PeVL 53/2022 vp, kappale 10, PeVL 5/2023 vp, kappale 4 ja PeVL 47/2024, kappale 8.

Lopuksi

Jos päädyttäisiin vapaaehtoiseen tunnistamiseen, olisi jatkovalmistelussa neuvoteltava menettelyn edellytyksistä ja sisällöstä tarkemmin sekä varmistettava, että menettelylle asetetaan riittävät suojakeinot väärinkäytöksiä vastaan. Sääntelyn tulisi myös olla EU:n tietosuojalainsäädännön mukaista. Lisäksi olisi ennen etenemistä selvitettävä, mitkä olisivat tiettyjen palveluntarjoajien vapaaehtoisten tunnistamistoimien tosiasialliset vaikutukset mm. käyttäjien henkilötietojen ja yksityiselämän suojaan sekä sananvapauteen ja luottamuksellisen viestin suojaan. Huomiota olisi kiinnitettävä myös sääntelyn selkeyteen viestinnän osapuolten ja palveluntarjoajien kannalta.

Edellä esitetyillä perusteilla katson, että ehdotettu vapaaehtoiseen tunnistamiseen perustuva menettely on ongelmallinen perus- ja ihmisoikeuksina turvattujen yksityiselämän suojan ja henkilötietojen suojan, luottamuksellisen viestin suojan ja sananvapauden kannalta. Samalla painotan, että sääntelyn tarkoitus eli lasten suojaaminen verkkovälitteiseltä seksuaaliväkivallalta on hyväksyttävä ja erittäin painava.

Espoossa, toukokuun 11. päivänä 2025

Päivi Korpisaari

Viestintäoikeuden professori

Varatuomari