Eduskunnan perustuslakivaliokunnalle

Asia: 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 tapaamisen 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 valmistelussa.[2] Lisäksi perustuslaki-

[1] Esim. PeVL 15/2017 vp, s. 4 ja PeVL 9/2017 vp, s. 5—6 ja niissä viitatut lausunnot).
[2] PeVL 20/ 2017 vp, s. 6.

valiokunnan 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 asiaa käsiteltäessä lausunnot 53/2022 vp (U 69/2022 vp) ja 5/2023 vp (jatkokirjelmä UJ 19/2023 vp — U 69/2022 vp). Asian käsittelyn pohjana valiokunnassa ovat tällä kertaa asetusehdotuksen käsittelyn tämänhetkistä vaihetta kuvaavat 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.

Lähtökohdat

Perustuslakivaliokunta on katsonut lausunnoissaan 53/2022 vp ja 5/2023 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.

Asetusehdotuksen ongelmallisimmaksi kohdaksi on muodostunut tunnistamismääräystä koskeva 7 artikla, jonka mukaan verkkopalveluntarjoajia velvoitettaisiin tunnistamaan ja torjumaan CSA-materiaalia (child sexual abuse -aineistoa). Säännösehdotus on herättänyt kysymyksiä erityisesti luottamuksellisen viestin suojan, mutta myös yksityiselämän suojan, tietosuojan ja sananvapauden kannalta.

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

Aikaisemman asetusehdotuksen pohjalta laaditussa suuren valiokunnan lausunnossa (SuVL 7/2023) katsottiin, ettei tuolloisen ehdotuksen mukainen ratkaisu olisi ollut hyväksyttävissä. Myös perustuslakivaliokunta piti lausunnoissaan PeVL 53/2022 vp sekä PeVL 5/2023 vp asetusehdotusta ongelmallisena luottamuksellista viestintää koskevan PL 10 §:n 4 momentin kannalta.

Asetusehdotuksen nykytila

Asetusehdotuksen 7 artiklaa on aikaisempien perustuslakivaliokunnan lausuntojen jälkeen muutettu siten, että tunnistamismääräystä on kohdennettu tarkemmin ja se kohdistuisi vain jo kertaalleen tunnistettuun CSA-materiaaliin. Niin kutsuttu grooming ja uuden CSA-materiaalin tunnistaminen on jätetty tunnistamismääräyksen soveltamisalan ulkopuolelle. Lisäksi vuonna 2021 voimaantullutta ja vuonna 2024 jatkettua tilapäistä poikkeusta sähköisen viestinnän tietosuojadirektiivin tiettyihin säännöksiin esitetään jatkettavaksi. Sen nojalla palveluntarjoajat voivat tunnistaa ja raportoida vapaaehtoisesti havaitsemastaan uudesta CSA-materiaalista sekä groomingista.

Sisäministeriön lausunnon 8.10.2024 EUN 78/2024 vp mukaan aikaisempaan ehdotukseen verrattuna uusimpaan ehdotukseen on tehty seuraavat muutokset:

1) Tunnistamismääräys kohdennettaisiin vain tunnettuun CSA-materiaaliin. Se kohdistuisi siten vain jo kertaalleen rikolliseksi todettuihin kuviin ja videoihin. Tunnistamismääräyksen soveltamisalasta on lisäksi rajattu pois teksti- tai ääniperustainen grooming ja uusi CSA-materiaali.
2) Lapsiin kohdistuvaa seksuaaliväkivaltaa sisältävien kuvien ja videoiden tunnistaminen ei edellyttäisi salausteknologian purkamista eikä heikentäisi ns. päästä päähän -salauksessa käytettyä teknologiaa. CSA-materiaalin jäljittämisessä hyödynnettäisiin ns. hash-lukuja vertailevia teknologioita siten, että käytettävä palvelu laskee kuvalle tai muulle tiedostolle ns. hash-luvun silloin kun käyttäjä valitsee lähetettävän kuvan puhelimensa galleriasta. Tätä hash-lukua verrattaisiin listaan tunnetusta CSA-materiaalista. Jos tiedoston hash-luku on tunnetun CSA-aineiston luku, tulee tästä palveluntarjoajalle ns. osumailmoitus, ja palveluntarjoajan tulee raportoida osumasta asetuksessa perustettavalle EU-keskukselle. Tunnistamismääräyksen kohdentuessa päästä päähän salattua viestintää hyödyntävään palveluntarjoajaan, hyödynnettäisiin hash-lukuja vertaavia teknologioita ainoastaan siinä hetkessä, jolloin kuvia tai videoita ladataan laitteelta, esim. kuvagalleriasta, lähetettäväksi – eli ennen kuin viestin sisältö salautuu.

3) Ehdotettu menetelmä ei edellytä palvelun käyttöjärjestelmään tehtäviä muutoksia tai vakoiluohjelman tai muiden seurantalaitteiden asentamista esimerkiksi puhelimiin. Tunnistamismääräykseen liittyvät teknologiset ratkaisut toteutettaisiin puhelimessa jo olevan käyttöjärjestelmän kautta.
4) Tunnistamismääräyksen toteuttaminen olisi mahdollista vain sillä edellytyksellä, että jokainen käyttäjä antaa palveluntarjoajan ehtojen mukaisesti nimenomaisen suostumuksensa siihen, että ko. tunnistamistoimintoa voidaan palvelussa käyttää. Jos käyttäjä ei anna lupaa kuvien hash-arvojen vertailuun, hän ei voi lähettää ko. sovelluksella kuvamuotoista materiaalia. Tekstimuotoista materiaalia voisi edelleen lähettää.
5) Tunnistamismääräys kohdennettaisiin vain sellaisiin verkkopalveluntarjoajiin tai niiden osiin, joissa on todettu korkea riski CSA-materiaalin levittämiselle. Riskin toteaminen perustuisi viranomaisten toimesta tehtävään riskiluokitukseen. Tämän mahdollistamiseksi palveluntarjoajat olisivat velvollisia arvioimaan ja raportoimaan alustansa CSA-materiaaliin liittyvistä riskeistä palveluissaan.
6) Tunnistamismääräyksen antaminen kansallisen tuomioistuimen tai riippumattoman hallintoviranomaisen toimesta on ehdotetussa kompromissitekstissä viimesijainen keino, sillä palveluntarjoajille annetaan mahdollisuus torjua CSA-materiaalia alustoillaan ennen kuin edetään tunnistamismääräyksen antamiseen. Tunnistamismääräys olisi myös rajattu ajallisesti ja pitäisi sisällään toimenpiteen valvonnan ja raportoinnin. Tunnistaminen ei siis olisi yleistä saatikka erottelematonta toimintaa.

Sisäministeriön lausunnon 8.10.2024 EUN 78/2024 vp mukaan "Valtioneuvosto jakaa suuren valiokunnan näkemyksen siitä, että asetusehdotus olisi uudenlaista EU-sääntelyä erityisesti siltä osin, että siitä voisi seurata palveluntarjoajille velvollisuus käsitellä henkilöiden välistä viestintää rikollisen materiaalin tunnistamiseksi ilman viranomaisen vahvistamaa tietyn henkilön liityntää selvitettävään tai ehkäistävään rikollisuuteen."

Arvioinnin lähtökohdat

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.[4] Euroopan neuvoston ihmisoikeussopimus (EIS) asettaa yksityiselämän suojan (ml. henkilötietojen suoja) ja sananvapauden rajoittamisen edellytykseksi sen, että rajoituksista on säädetty lailla tietyn kyseissä

[4] PeVM 25/1994 ja useat sen jälkeiset lausunnot.

artiklassa (8 ja 10 artiklat) säädetyn oikeushyvän turvaamiseksi ja että rajoitus on välttämätön demokraattisessa yhteiskunnassa. EU:n perusoikeuskirjan (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."

Tunnistamismääräys

Asetusehdotuksen 7 artiklassa säädetään tunnistamismääräyksen antamisesta. Tässä ei toisteta asian aikaisemmissa käsittelyvaiheissa esitettyä, vaan arvioidaan asiaa etenkin asetusehdotukseen edellisten perustuslakivaliokunnan lausuntojen jälkeen tehtyjä muutoksia ja pohditaan, onko tunnistamismääräystä koskeva ehdotettu sääntely muutoksista huolimatta edelleen ongelmallinen perus- ja ihmisoikeuksien kannalta.

Perustuslain 10 §:n 1 momentin mukaan "Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla."

Saman pykälän 4 momentin (817/2018) mukaan "Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta." PL 10 §:n 4 momentissa turvatun luottamuksellisen viestinnän perusoikeussuojan tavoitteena on turvata jokaiselle oikeus luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Kyseessä on molempien viestinnän osapuolten perusoikeus.[5]

Perustuslakivaliokunta on 4 momenttia koskevassa mietinnössään 4/2018 katsonut, että "rajoituslausekkeen on edelleen turvattava riittävästi luottamuksellisen viestin salaisuutta ja asetettava riittävän tiukat valtiosääntöiset rajat siihen puuttumiselle." Valiokunta ei pitänyt oikeana luottamuksellisen viestin rajoittamista rikosten torjunnassa, kuten hallitus ehdotti, vaan esitti puuttumismahdollisuutta vain rikosten tutkintaan liittyen. Vakiintuneen tulkinnan mukaan "rikoksen tutkintana pidetään sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn

[5] HE 309/1993 vp s. 53.

johdosta, vaikka rikos ei olisi vielä edennyt toteutuneen teon asteelle. Tältä osin tulkinta on vakiintunut eikä siitä ole epäselvyyttä."[6]

Perustuslakivaliokunta on perustuslain 10 §:n 4 momentin ja tiedustelulainsäädännön säätämisen yhteydessä todennut, että 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.[7] Valiokunta totesi erikseen, että perustuslain 10 §:n 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa.[8] Siltä osin kuin on kyse yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnasta, perustuslain 10 §:n 4 momenttiin sisältyvää rajoituslauseketta on jo ennen perustuslain voimaantuloa[9] tulkittu varsin johdonmukaisesti siten, että rikoksen tutkintana pidetään sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei olisi vielä edennyt toteutuneen teon asteelle.[10] Perustuslakivaliokunnan käytännössä edellä mainittuihin rikoksiin on rinnastettu myös törkeä lapsen seksuaalinen hyväksikäyttö.[11] Samoin perustuslakivaliokunta on pitänyt mahdollisena, että luottamuksellisen viestin salaisuutta rajoitetaan henkilön henkeä tai terveyttä uhkaavan välittömän vaaran torjumiseksi, kunhan rajoitukset ovat välttämättömiä ja oikeasuhtaisia.[12]

Yksityiselämä ja henkilötietojen suoja osana sitä turvataan myös EIS 8 artiklassa. Yksityiselämän suoja ja henkilötietojen suoja turvataan omina perusoikeuksinaan POK 7 ja 8 artikloissa. Yksityiselämän suojaa koskevassa POK 7 artiklassa mainitaan nimenomaisesti, että "Jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan."

Sananvapaus turvataan PL 12 §:ssä. Sen 1 momentin kahden ensimmäisen virkkeen mukaan "Jokaisella on sananvapaus. Sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Tarkempia säännöksiä sananvapauden käyttämisestä annetaan lailla." Sananvapaus turvataan myös EIS 10 artiklassa sekä POK 11 artiklassa.

Erilaisten sovellusten kautta tapahtuva kahdenkeskinen tai useamman ihmisen välinen viestintä on perus- ja ihmisoikeutena turvatun sananvapauden käyttämistä. Tällainen viestintä kuuluu myös yksityiselämän suojan piiriin paitsi osana luottamuksellista

[6] PeVL 2/1996 s. 1–3, PeVL 5/1999 s. 2-3 ja PeVM 4/2018 s. 5-6.
[7] PeVL 35/2018 vp, s. 12.
[8] PeVM 4/2018 vp, s. 7— 8.
[9] Esim. PeVL 2/1996 vp, PeVL 5/1999 vp.
[10] PeVM 4/2018 vp, s. 5.
[11] PeVL 26/2014 vp.
[12] PeVL 6/2018 vp.

viestintää myös sen vuoksi, että yksityiselämän piiriin kuuluu oikeus luoda ja ylläpitää ihmissuhteita, jota toteutetaan keskeisesti myös erilaisia viestintätapoja hyödyntämällä.

Seuraavassa arvioidaan asetusehdotuksen tehtyjä muutoksia edellä mainittujen oikeuksien toteutumisen ja turvaamisen kannalta, ottaen huomioon, että perus- ja ihmisoikeuksien turvaamisvelvollisuudesta voidaan johtaa myös velvollisuus suojata lapsia asetusehdotuksessa kuvatulta seksuaaliväkivallalta. Asetusehdotuksella onkin erittäin painava tavoite tehokkaasti ennaltaehkäistä ja torjua lapsiin kohdistuvaa verkkovälitteistä seksuaaliväkivaltaa EU-tason toimin.

Suuri valiokunta on aikaisemmassa asiaa koskevassa lausunnossaan SuVL 7/2023 s. 3 katsonut, että asetuksessa säädettävien toimenpiteiden tulee olla riittävän tehokkaita ja samalla ennakoitavia, oikeassa suhteessa ja välttämättömiä ehdotuksen tavoitteen toteutumiseksi.

Perustuslakivaliokunta on lausunnossaan 5/2023 katsonut, että

> "*(8)* Perustuslakivaliokunta pitää siten valtioneuvoston tavoin tärkeänä, että asetusehdotuksen hyväksyttävään ja erittäin painavaan tavoitteeseen pyrittäisiin keinoilla, jotka ovat tehokkaita ja oikeassa suhteessa tavoiteltuun päämäärään. Viestinnän luottamuksellisuuden suojaan ja muihin perusoikeuksiin puuttuminen tulee rajata vain välttämättömään, ja sen tulee olla oikeasuhtaista. Valiokunta korostaa myös valtioneuvoston tavoin, että ehdotetun sääntelyn tulee olla riittävän selkeää, ennakoitavaa ja kohdennettua ja että tunnistamismääräyksen on oltava kohdennettu."

Esitetyssä tunnistamisessa olisi kysymys yksityiselämän suojaan, luottamukselliseen viestintään, henkilötietojen suojaan sekä sananvapauteen puuttumisesta, joten jotta puuttumista voitaisiin pitää oikeutettuna, tulisi sen olla oikeasuhtaista ja välttämätöntä demokraattisessa yhteiskunnassa sekä välttämätöntä ehdotuksen tavoitteiden toteutumiseksi. Jotta puuttuminen olisi oikeutettua, tulisi sen avulla myös pystyä tehokkaasti ehkäisemään epätoivottua rikollista käyttäytymistä.

Ehdotuksen sananvapauteen ja yksityisyyteen puuttuvaa luonnetta rajoittaisi se, että sisältöä ei tarkasteltaisin sellaisenaan, vaan kyse olisi kuvatiedoston eräiden teknisten ominaisuuksien vertaamisesta tunnistettujen CSA-materiaalia sisältävien kuvien vastaavaan tekniseen ominaisuuteen. Vaikka sisältöää ei tarkasteltaisi sellaisenaan, kyse on kuitenkin merkittävästä puuttumisesta, koska käytännössä se saattaisi merkitä sitä, että kaikki lähetetyt kuvatiedostot joutuvat kyseisen tarkastelun alaisiksi. Asetusehdotuksen mukaan tarkastelu ulottuisi lisäksi myös linkkeihin.

Näkemykseni mukaan ehdotettu säännös, jonka mukaan tunnistamismääräyksellä voitaisiin tunnistaa vain jo kertaalleen rikolliseksi todettuja kuvia ja videoita ei tehokkaasti ehkäisisi lapsiin kohdistuvaa seksuaaliväkivaltaa tai auttaisi saamaan tähän syyllistyviä rikoksentekijöitä kiinni. Syitä tähän on useita. Ensinnäkin säännös ei koskisi lainkaan uutta CSA-materiaalia eikä groomingia. Toisekseen tietyn, sisällöltään rikollisen aineiston toteaminen rikolliseksi tapahtuisi käsitykseni mukaan oikeudenkäynnissä, ja ottaen huomioon esitutkinnan ja oikeuskäsittelyn vaatima aika tällaista sisällöltään rikollista materiaalia voitaisiin lähettää verkossa useamman vuoden ajan ennen kuin se todettaisiin rikolliseksi ja se voitaisiin tallentaa vertailutietokantaan ja antaa hälyytyksen, jos joku muu lähettää juuri samaa aineistoa. Kolmanneksi, kiinnijäämisriski tällaisista rikoksista lienee kaikesta huolimatta melko pieni, joten materiaalia todennäköisesti levitettäisiin jatkuvasti paljon enemmän kuin sitä olisi vertailutietokannassa ja vain murto-osa rikollisesta aineistosta päätyisi vertailutietokantaan. Tämä johtuu esimerkiksi siitä, että viestien lähettäjiä ja vastaanottajia voi olla vaikea selvittää, kun viestejä voidaan lähettää ja vastaanottaa myös anonyymisti, eivätkä tällaiset tapaukset etene oikeuteen saakka. Toki en ole varma, olisiko käytössä myös jokin muunlainen mekanismi kuin oikeudenkäynti rikollisen aineiston toteamiseksi. Neljänneksi todettakoon, että tunnistamisen tapahtuminen asetusehdotuksessa esitetyllä tavalla hash-teknologialla merkitsisi sitä, että tunnistamista olisi varsin helppo kiertää rajaamalla kuvaa hiukan tai lyhentämällä videota vaikka sekunnilla, jolloin vertailutietokanta ei enää tunnistaisi aineistoa. On oletettavaa, että asetuksessa tarkoitettuihin rikoksiin syyllistyvät keksisivät tapoja kiertää hash-lukuun perustuva tunnistaminen.

Esitetyllä tavalla ei siten nähdäkseni pystytä kovin tehokkaasti ehkäisemään lapsiin kohdistuvaa seksuaaliväkivaltaa ja suojelemaan heidän yksityisyyttään, joten merkittävää perus- ja ihmisoikeuksiin kajoamista ei oikein voi perustella lasten edulla, kun hyöty tästä laajamittaisesta kajoamisesta olisi varsin marginaalinen.

Käsitykseni mukaan asetusehdotus olisi muutetussakin muodossa uudenlaista EU-sääntelyä siltä osin kuin siitä voisi seurata palveluntarjoajille velvollisuus käsitellä henkilöiden välistä viestintää rikollisen materiaalin tunnistamiseksi ilman viranomaisen vahvistamaa tietyn henkilön liityntää selvitettävään tai ehkäistävään rikollisuuteen. Nähdäkseni lähetetyn kuvamateriaalin “tunnistaminen” nyt esitetyssä laajuudessa ilman konkreettista rikosepäilyä muodostaa merkittävän puuttumisen yksityisyyden ja henkilötietojen suojaan, luottamuksellisen viestin suojaan sekä sananvapauteen. Lisäksi esimerkiksi tutkivaa journalismia harjoitettaessa voi olla tarpeen lähettää ja käsitellä lapsiin kohdistuvaa seksuaaliväkivaltamateriaalia epäkohtien paljastamiseksi ja ehdotus merkitsisi sitä, että journalisti saattaisi itsensä syytteen vaaraan tai ainakin hankaluuksiin, jos käyttäisi tavanomaisia journalistisia salattuja viestintäteknologioita ja materiaali sattuisi löytymään tunnistustietokannasta. Myös jo pelko tunnistamistietokannan osumasta voisi hankaloittaa journalistista toimintaa.

Siltä osin kuin tunnistaminen ei vaatisi salausteknologian purkamista tai ns. päästä päähän -salauksen heikentämistä totean, että ehdotuksessa kuvattu menettely, jonka mukaan tunnistamisteknologiaa käytettäisiin vain silloin, kun kuva tai video latautuu laitteelta lähetettäväksi – eli ennen kuin viestin sisältö salautuu – ei olennaisesti muuta sitä tosiasiaa, että ehdotuksella puututtaisiin hyvin laajamittaisesti ihmisten ja organisaatioiden väliseen luottamukselliseen viestintään.

Uuteen asetusehdotukseen on lisätty edellytys siitä, että jokainen käyttäjä antaa palveluntarjoajalle nimenomaisen suostumuksen siihen, että palvelussa voidaan käyttää edellä kuvattua tunnistamistoimintoa. Jos suostumusta hash-arvojen vertailuun ei anneta, ei palvelun kautta ole mahdollista lähettää kuvamuotoista materiaalia tai linkkejä. Tekstimuotoisia viestejä voisi lähettää.

Ehdotettu suostumusmalli ei nähdäkseni perustu aitoon vapaaehtoisuuteen. Ihminen voi toki jossan määrin suostua perus- ja ihmisoikeuksiensa rajoittamiseen, mutta tässä säännösehdotuksessa kuvien, videoiden tai linkkien lähettäminen ei olisi mahdollista ilman suostumusta hash-lukujen vertailuun. Perus- ja ihmisoikeuden käyttäminen eli kuvaviestien ja linkkien lähettäminen edellyttäisi siis suostumusta näiden hash-arvojen vertailuun. Vanhan sanonnan mukaan kuva kertoo enemmän kuin 1000 sanaa. Kuva on keskeinen itsensä ilmaisun muoto ja kuvaviestien lähettämismahdollisuuden poistuminen olisi olennainen yksityiselämän suojaa ja sananvapautta rajoittava seikka. Monet sovellukset, kuten Snapchat ja TikTok on jopa tehty nimenomaan ja etupäässä kuvamateriaalin lähettämistä varten. Suostumusta ei näissä olosuhteissa voitaisi pitää aitona, koska se olisi käytännössä pakko antaa voidakseen lähettää kuvaviestejä tai linkkejä – varsinkin kun on mahdollista, että kaikki suosituimmat viestikanavat tulisivat tunnistamismääräysten piiriin.

EU:n yleisellä tietosuoja-asetuksella (2016/679; TSA) ei sinällään olisi etusijaa ehdotettuun asetukseen verrattuna, mutta todettakoon, että TSA 7 artiklassa säädetään suostumuksesta henkilötietojen käsittelyyn. Asetuksen johdannon 32. kohdan mukaan “Suostumus olisi annettava selkeästi suostumusta ilmaisevalla toimella, kuten kirjallisella, mukaan lukien sähköisellä, tai suullisella lausumalla, josta käy ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn.” Johdannon 42. kohdan mukaan “Suostumusta ei voida pitää vapaaehtoisesti annettuna, jos rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta ja jos hän ei voi myöhemmin kieltäytyä suostumuksen antamisesta tai peruuttaa sitä ilman, että siitä aiheutuu hänelle haittaa.” Näkisin, että asetusehdotuksen mukaisessa tilanteessa kuvamateriaalin tai linkin lähettäjän antama suostumus ei ole aito, koska hänellä ei ole todellista vapaan valinnan mahdollisuutta, jos hän haluaa lähettää kuvia. Suostumuksen antamatta jäämisestä seuraisi merkittävää haittaa. Koska kysymys on perus- ja ihmisoikeuden rajoittamisesta, on suostumuksen pätevyydellä nähdäkseni vielä tavanomaistakin suurempi merkitys.

Asetusehdotuksen mukaan tunnistamismääräys kohdennettaisiin vain sellaisiin verkkopalveluntarjoajiin tai niiden osiin, joissa on todettu korkea riski CSA-materiaalin leviämiselle. Epämääräiseksi jää se, miten tämä riski todettaisiin. Käytännössä saattaisi käydä niin, että tunnistamismääräys kohdennettaisiin kaikkiin tavanomaisiin viestintäkanaviin. Toisaalta on oletettavissa, että CSA-materiaalia pyrittäisiin levittämään niissä kanavissa, joihin tunnistamismääräystä ei ole kohdennettu, joten epäilyksen alaiseksi jää, voitaisiinko tunnistamismääräyksellä tehokkaasti ehkäistä CSA-materiaalin leviämistä, jollei sitä kohdenneta kaikkiin mahdollisiin viestintäkanaviin (ja tällöinkin sen leviämisen ehkäisemistä heikentäisivät aikaisemmin mainitut tosiasiat kuten se, että kuvaa on helppo manipuloida siten, että ns. hash-luku eroaa rikolliseksi todetun kuvamateriaalin hash-luvusta jne.).

Tiedossani ei ole, mitä tarkoitetaan palveluntarjoajien mahdollisuudella torjua CSA-materiaalia aloustoillaan ennen tunnistamismääräyksen antamista. Näin ollen tämän keinon tehokkuutta on vaikea arvioida. Asialla on merkitystä sikäli, että tunnistamismääräystä pidetään tähän nähden toissijaisena keinona.

Sisäministeriön lisäselvityksessä viitataan myös siihen, että tunnistamismääräys olisi rajattu ajallisesti ja pitäisi sisällään toimenpiteen valvonnan ja raportoinnin. Ymmärtääkseni tunnistamismääräys voisi olla enintään 24 kuukautta. Uutta tunnistamismääräystä lienee kuitenkin mahdollista hakea edellisen tunnistamismääräyksen päätyttyä, joten määräajan merkitys jäänee vähäiseksi. Käytännössä tunnistamistoimintaa olisi todennäköisesti pakko jatkaa koko ajan, jos lapsiin kohdistuvien seksuaalirikosten tekijät halutaan saada kiinni tai näitä rikoksia pyritään estämään. Näin ollen ehdotettu sääntely merkitsisi sitä, että tunnistamismääräyksen voimassaolo olisi pääsääntö ja siitä “vapaa viestintä” olisi poikkeus, mikä olisi periaatteellisesti ja käytännöllisesti todella suuri muutos nykytilanteeseen verrattuna. Lisäksi tunnistamismenettely kohdistuisi valtaosin ihmisiin, joilla ole koskaan ollut mitään tekemistä lapsiin kohdistuvan seksuaaliväkivallan kanssa.

Jo asetusehdotuksen aikaisemmissa käsittelyissa on esitetty huoli siitä, että tunnistamismääräyksen soveltamisalaa ei ole rajattu tiettyihin henkilöihin, vaan se koskisi myös sellaisia tilanteita, joissa ei ole kyse konkreettisesta ja yksilöidystä rikosepäilystä, jolloin se käytännössä voisi johtaa yleiseen ja erittelemättömään viestien valvontaan. Esimerkiksi perustuslakivaliounnan mietinnässä 53/2022 vp todetaan, että

> (10) Perustuslain 10 §:n 4 momenttiin nykyisin sisältyvää rajoituslauseketta on jo ennen perustuslain voimaantuloa (ks. esim. PeVL 2/1996 vp, PeVL 5/1999 vp) tulkittu varsin johdonmukaisesti siten, että rikoksen tutkintana pidetään sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei olisi vielä edennyt toteutuneen teon asteelle (PeVM

4/2018 vp, s. 5). Perustuslakivaliokunnan käsityksen mukaan nyt ehdotettu sääntely koskee kuitenkin myös sellaisia tilanteita, joissa ei ole kyse konkreettisesta ja yksilöidystä rikosepäilystä.

(11) Perustuslakivaliokunta on perustuslain nykyisen 10 §:n 4 momentin ja tiedustelulainsäädännön säätämisen yhteydessä todennut, että 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). Valiokunta totesi erikseen, että perustuslain 10 §:n 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa (PeVM 4/2018 vp, s. 7—8).”

Nähdäkseni uusi ehdotus on edelleen ongelmallinen tässä suhteessa. Valvonta kohdistuisi käytännössä kaikkiin tunnistamismääräyksen alaista viestintäteknologiaa käyttäviin ihmisiin ja organisaatiohin, vaikka kysymys ei olisi minkäänlaisesta konkreettisesta rikosepäilystä. Pakotettu suostumusmekanismi ei nähdäksen muuta asiaa muuksi.

Lopuksi

Ehdotetun sääntelyn tarkoituksena on turvata lasten väkivallatonta lapsuutta sekä lasten yksityisyyttä sikäli kuin kysymys on lapsiin kohdistuvaa seksuaaliväkivaltaa tms. sisältävän aineiston levittämisestä. Tarkoitusperä on äärimmäisen hyvä. Nähdäkseni ehdotulla sääntelyllä puututtaisiin monien muiden perus- ja ihmisoikeuksien käyttämiseen ja jotta tällainen puuttuminen olisi oikeutettua, tulisi sille olla välttämättömät ja hyväksyttävät perusteet ja rajoitusten tulisi olla oikeassa suhteessa hvyäksyttävään päämäärään. Tässä ehdotuksessa ei käsittääkseni näin ole. Valtaosa ihmisistä ei koskaan hallusssapidä tai lähetä minkäänlaista lapsiin kohdistuvaa seksuaaliväkivaltaa käsittävää kuva- tai muuta materiaalia, ja silti asetusehdotus mahdollistaisi myös tällaisten tavallisten ihmisten luottamukselliseen viestintään puuttumisen ilman minkäänlaista konkreettista rikosepäilyä.

Kuvamateriaalilla on nykyaikaisessa viestinnässä keskeinen merkitys, joten rajoitusten kohdistuminen kuvamateriaaliin ei merkitse vähäistä rajoitusta. Toki puuttumista vähentää se, että aineistovertailu tehtäisiin ns. hash-luvun perusteella eikä autenttinen kuvamateriaali tallentamalla.

Niin tärkeää kuin lapsiin kohdistuvan rikollisuuden estäminen ja selvittäminen onkin, niin tällaista mekanismia ei tiettävästi ole säädetty minkään muiden rikosten osalta, joten senkin vuoksi on syytä suhtautua pidättyvästi ehdotettuihin perus- ja ihmisoikeuspuuttumisiin. On arvioitava myös tasapuolisuutta eri oikeushyvien kesken – ehdotettaisiinko vastaavaa mekanismia seuraavaksi esimerkiksi henkeen ja terveyten kohdistuvien rikosten ehkäisemiseksi.

Espoossa, lokakuun 21. päivänä 2024

Päivi Korpisaari

Viestintäoikeuden professori, varatuomari

Espoo