Sisäministeriö
Inrikesministeriet

Lausunto 20.5.2025

Pekka Vasara
SM/PO

Hallintovaliokunta

Sisäministeriön lausunto asiaan 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)

Eduskunnan hallintovaliokunta on pyytänyt sisäministeriöltä lausuntoa asetusehdotuksesta lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (jäljempänä CSAM-asetusedotus). Vastuuministeriönä sisäministeriö toteaa kunnioittavasti seuraavaa:

Tausta:

Euroopan komissio antoi 11.5.2022 CSAM-asetusehdotuksen, jonka käsittely on edennyt neuvostossa hitaasti sen teknisen luonteen sekä tietosuojaan ja luottamuksellisen viestin suojaan liittyvien kysymysten vuoksi. Unkari tavoitteli asiassa neuvoston yleisnäkemystä oikeus- ja sisäasioiden neuvostossa 12.-13.12.2024, mutta puheenjohtajan esittämän kompromissiteksti ei saavuttanut riittävää määräenemmistöä tuekseen.

Puheenjohtaja Puolan johdolla jatketaan yli kaksi ja puolivuotta kestäneitä neuvotteluja neuvoston yleisnäkemyksen saavuttamiseksi. Tämänhetkisten tietojen mukaan Puola tavoittelee puheenjohtajuuskaudellaan neuvoston osittaista yleisnäkemystä kesäkuun oikeus- ja sisäasioiden neuvoston yhteydessä.

Ehdotuksen keskeisimmät muutokset

Puheenjohtajan laatiman uuden kompromissiehdotuksen tavoitteena on tehostaa lapsiin kohdistuvan seksuaaliväkivallan torjuntaa, rajoittamatta suhteettomasti käyttäjien perusoikeuksia ja huomioiden korkea tietosuojan taso. Tavoitteen taustalla on eri havaintoihin perustuvat arviot siitä, että verkkovälitteisesti tapahtuvan lapsiin kohdistuvan seksuaaliväkivaltamateriaalin välittäminen on kasvanut merkittävästi.

Puheenjohtajan valmisteleman kompromissiehdotuksen soveltamisalasta on poistettu kokonaan tunnistamismääräys ja siihen suoraan kytkeytyvät artiklat (7-11 artiklat). Siten tekstistä on poistettu esimerkiksi aiempaan ehdotukseen sisältynyt tekninen toiminto (ns. *upload moderation*), jolla laitonta sisältöä olisi voitu tunnistaa salattua ympäristöä käyttävissä palveluissa ns. hash-lukuja vertaamalla ennen viestin salaamista lähettämistä varten.

Ehdotukseen on kuitenkin sisällytetty lauseke (85 artikla), jonka perusteella komissiota kehotetaan arvioimaan kolmen vuoden kuluessa asetuksen voimaantulosta, olisiko velvoittavalle tunnistamismääräykselle olemassa teknologiset ja oikeudelliset edellytykset.

Tunnistamismääräyksen sijaan puheenjohtaja ehdottaa vuonna 2021 voimaantulleella – ja vuonna 2024 jatketulla – direktiivin 2002/58/EY tilapäisellä poikkeuksella (asetus

(EU) 2021/1232*)* tietyille palveluntarjoajille mahdollistettujen vapaaehtoisten käsittelytoimenpiteiden tuomista pysyvän sääntelyn piiriin. Toisin sanoen CSAM-asetuksella ehdotettaisiin vakiinnutettavaksi tilapäisen poikkeusasetuksen nojalla sovellettu menettely, joka mahdollistaa sen, että numeroista riippumattomat henkilöiden välisten viestintäpalvelujen tarjoajat (esim. Facebook Messenger) voivat käyttää erityisiä teknologioita henkilötietojen ja muiden tietojen käsittelyyn siinä laajuudessa, kuin on ehdottoman välttämätöntä niiden palveluissa välitetyn CSA-materiaalin tai siellä tapahtuvan groomingin havaitsemiseksi ja siitä ilmoittamiseksi ja kyseisen materiaalin poistamiseksi.

Puheenjohtajan kompromissitekstin pohjalta olisi mahdollista tunnistaa sekä ns. varmistettua eli tunnettua kuin myös uutta CSA-materiaalia, ja lasten houkuttelua (grooming). Tilapäisen poikkeusasetuksen tapaan puheenjohtajan ehdottamassa mallissa sähköisen viestinnän käsittely tapahtuisi teknologisin menetelmin ja sen olisi täytettävä asetusehdotuksessa määritellyt varsin tiukat ehdot (mm. suhteellisuus- ja välttämättömyysvaatimus). Kompromissin mukaan käsittelyyn käytettävien teknologioiden olisi muun muassa oltava mahdollisimman vähän yksityisyyteen puuttuvia alan viimeisimmän kehityksen mukaisesti. Tekstin käsittelyn osalta edellytyksenä on, että teknologialla ei tule voida päätellä viestinnän sisältöä vaan käsittelyn tarkoituksena tulisi olla sellaisten toimintamallien (*patterns*) tunnistaminen, jotka viittaavat mahdolliseen lasten hyväksikäyttöön. Kyse olisi viestintäpalvelun tarjoajille vapaaehtoisesta toiminnasta.

Puheenjohtajan ehdottamassa mallissa säädettäisiin tilapäistä poikkeusasetusta tarkemmin yritysten vapaaehtoisista toimista CSA-materiaalin tunnistamiseksi. Esimerkiksi seuraavia suojakeinoja on sisällytetty mukaan: palveluntarjoajien olisi varmistettava, etteivät heidän vapaaehtoiset CSA-materiaalin tunnistustoimenpiteensä luo hallitsemattomia riskejä kyberturvallisuudelle ja palveluntarjoajien olisi mm. pidettävä yksityiskohtaisia lokitietoja toiminnoistaan sisäistä ja ulkoista tarkastelua varten sekä mahdollista rikosoikeudellista menettelyä varten.

Puheenjohtajan ehdottamassa tekstissä on säilytetty aikaisemmissa kompromissiteksteissäkin ollut lauseke siitä, ettei asetuksella kielletä, kierretä tai muutoin heikennetä kyberturvallisuustoimenpiteitä. Lisäksi asetuksella ei luoda velvoitteita purkaa päästä päähän -salausta tai rajoittaa sen käyttöä. Tunnistamismääräyksen poistamisen myötä myös salattuihin viestisisältöihin liittyvä ja asian käsittelyssä ongelmalliseksi tunnistettu (SuVL 10/2024 vp, 8. kappale) epäselvyys poistuisi.

Kompromissiehdotuksen arviointia suhteessa perustuslakiin ja perus- ja ihmisoikeusvelvoitteisiin

Tilapäistä poikkeusasetusta ei sen säätämisvaiheessa arvioitu perustuslakivaliokunnassa eikä sääntelyn suhteesta Euroopan unionin perusoikeuskirjaan ole myöskään EU-tuomioistuimen oikeuskäytäntöä.

Perusoikeuksien rajoittamisen edellytyksiä arvioitaessa, merkitystä on sillä, että rajoitustoimenpiteistä säädettäisiin yksityiskohtaisesti EU:n jäsenvaltioissa suoraan sovellettavassa asetuksessa. Lisäksi ehdotuksella 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 CSAM-asetusehdotuksen yhteydessä aiemmin kiinnittänyt huomiota siihen, että sääntelyyn sisältynyttä tunnistamismääräystä ei ollut rajattu tiettyihin henkilöihin, ja siten sääntelyn soveltaminen olisi voinut muodostua varsin laajaksi ja yksilöimättömäksi (PeVL 47/2024 vp). Uuteen ehdotukseen ei sisälly enää velvoittavaa tunnistamismääräystä. Sen sijaan palveluntarjoaja voisi omalla päätöksellään tehdä viesteille tunnistamista asetuksessa säädettyjen edellytysten täyttyessä. U-kirjelmässä U 50/2020 vp on käsitelty ehdotuksen suhdetta Euroopan unionin perusoikeuskirjan 7 ja 24 artikloihin vuonna 2021 tulleessa tilapäisessä poikkeusasetuksessa. Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. Komissio on katsonut vapaaehtoisen tunnistamisen olevan tältä osin perusoikeuskirjan mukainen. Lisäksi kompromissiehdotus ottaa huomioon perusoikeuskirjan 24 artiklan, jonka mukaan kaikissa lasta koskevissa viranomaisten tai yksityisten laitosten toimissa on ensisijaisesti otettava huomioon lapsen etu.

Perustuslakivaliokunta on arvioinut yksityiselle toimijalle annettavaa oikeutta käsitellä tietyin edellytyksin tunnistamistietoja toisen yksityisen ja kolmannen tahon välisestä sähköisestä viestinnästä ensinnäkin sellaisen hallituksen esityksen yhteydessä, jossa esitettiin yhteisötilaajalle sallittavan tietyin edellytyksin käsitellä sähköisen viestinnän tunnistamistietoja maksullisen tietoyhteiskunnan palvelun tai viestintäverkon luvattoman käytön, viestintäpalvelun ohjeen vastaisen käytön sekä yrityssalaisuuksien paljastamisen selvittämiseksi (HE 48/2008 vp, PeVL 29/2008 vp). Perustuslakivaliokunnan mukaan esimerkiksi yritysvarallisuuden arvon ja elinkeinotoiminnan taloudellisten edellytysten turvaamiseen liittyvät seikat ovat hyväksyttäviä ja painavia perusteita tietoverkoissa harjoitettavaan viestintään kohdistuville rajoituksille (PeVL 29/2008 vp, s. 3).

Perustuslakivaliokunta ei ehdotetun sääntelyn kaltaisessa asetelmassa arvioinut sääntelyä suoraan suhteessa perustuslain 10 §:n 3 momentissa (nyk. 4 momentissa) sallittuihin rajoitusperusteisiin, jotka ainakin ensisijaisesti koskevat julkisen vallan taholta tulevia puuttumisia (PeVL 47/1996 vp, s. 4; PeVL 29/2008 vp, s. 2). Kirjallisuudessa on katsottu, että ”esitetty tulkintakannanotto tarkoittaa, että perusoikeuksien horisontaalivaikutus jäisi näin lain säätämisvaiheessa arvioitavaksi vain perusoikeuksien yleisten rajoitusedellytysten mukaisesti.[1] . Lausunnon mukaan tietojensaantioikeuden antaminen yksityiselle olisi edellyttänyt perustuslain 10 §:n silloisen 3 momentin säännösten huomioon ottamista ”tätä laajemman” tietojensaantioikeuden tapauksessa, mutta tarkoitettu viittaussuhde on epäselvä sikäli, tarkoittiko perustuslakivaliokunta yllä mainitun tulkinnan koskevan vain

[1]Teuvo Pohjolainen, Viestinnän tietosuoja ja tunnistamistietojen käsittelyn oikeus. Juhlajulkaisu Mikael Hidén 1939–7/12–2009, s. 425–433, 429.

tunnistamistietojen tai muutoin ei-täydellisten tietojen käsittelyä (PeVL 29/2008 vp, s. 3).

Edellä mainitussa yhteydessä perustuslakivaliokunta piti sääntelyn oikeasuhtaisuuden näkökulmasta olennaisena, että sääntely edellytti ensisijaisina keinoja, joilla ei puututa käyttäjien luottamukselliseen viestintään. Valiokunta myös korosti, että käsittely on lain vaatimusten vuoksi sallittua ainoastaan sen tarkoituksen vaatimassa laajuudessa eikä käsittelyllä voida rajoittaa luottamuksellisen viestin suojaa enempää kuin on välttämätöntä (PeVL 29/2008 vp, s. 3).

Voimassa oleva sähköisen viestinnän luottamuksellisuutta koskeva lainsäädäntö sisältää sääntelyä, jolla sallitaan viestinnän välittäjän käsitellä viestinnän sisältöä tietoturvasta huolehtimiseksi (laki sähköisen viestinnän palveluista 272 §). Sääntely on alun perin sisältynyt kumottuun sähköisen viestinnän tietosuojalakiin. Perustuslakivaliokunta on kyseistä sääntelyä arvioidessaan katsonut, että perusoikeuksien käyttämiseen ja niiden toteutumisen edistämiseen tällä tavoin liittyvät seikat ovat hyväksyttäviä ja painavia perusteita tietoverkoissa harjoitettavaan viestintään kohdistuville rajoituksille. Lisäksi valiokunta on pitänyt tärkeänä, että viestin sisältöön puuttuminen on kytketty rikosepäilyyn (PeVL 9/2004 vp, s. 4). Sittemmin myös viestin sisällön puuttumisen edellytyksenä ollut kytkös rikostunnusmerkistöön on kuitenkin poistettu säännöksestä perustuslakivaliokunnan myötävaikutuksella (HE 48/2008 vp, s. 30 ja PeVL 29/2008 vp, jossa sanottua muutosta ei kuitenkaan käsitellä). Sittemmin vastaava sääntely otettiin perustuslakivaliokunnan myötävaikutuksella säädettyyn tietoyhteiskuntakaareen (nyk. nimike laki sähköisen viestinnän palveluista) (PeVL 18/2014 vp). Kyseinen sääntely mahdollistaa myös viestin sisällön käsittelyn, jonka tulee lähtökohtaisesti olla automaattista, mutta joka voi olla eräin edellytyksin myös manuaalista.

Perustuslakivaliokunnan myötävaikutuksella säädetyllä sähköisen viestinnän palveluista annetun lain 272 §:llä on monia rakenteellisia samankaltaisuuksia tilapäisen asetuksen mahdollistamaan vapaaehtoiseen tunnistamiseen nähden. Sääntely on luonteeltaan mahdollistavaa eikä velvoittavaa. Mainittu pykälä mahdollistaa muun ohella viestin sisältöä koskevan automaattisen selvittämisen viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Siten myös havaitusta rikosepäilystä voidaan ilmoittaa poliisille. Säännös ei ole kuitenkaan kytketty rikostunnusmerkistöön, vaan esimerkiksi myös tahattomasti aiheutuvia tietoturvauhkia voidaan pyrkiä tunnistamaan (HE 48/2008 vp, s. 30). Tietoturvalle haittaa aiheuttavia seikkoja voidaan havaita periaatteesta kaikesta viestinnästä, mikäli toimenpidettä voidaan pitää välttämättömänä tietoturvasta huolehtimiseksi.

Kuten edellä todettiin, pykälän soveltamista ei ole kytketty yksilöidyn rikosepäilyn olemassaoloon. Vain pykälän 1 momentin 3 kohdassa tarkoitetun maksuvälinepetosten valmistelun ehkäisyn tavoitteen osalta sääntely on kytketty rikostunnusmerkistöön, mutta tältäkään osin käsittely ei edellytä yksilöidyn rikosepäilyn olemassaoloa, vaan maksuvälinepetoksen valmistelua merkitseviä viestejä voidaan seuloa kaikesta soveltuvasta viestinnästä pykälän edellytysten

täyttyessä. Tietoturvahäiriöiden ja roskapostin torjumisen osalta pykälä ei ole kytketty rikostunnusmerkistöihin.

Siten vaikuttaa siltä, että perustuslakivaliokunnan lausuntokäytännön mukaan sellainen sääntely, jossa yksityiselle toimijalle annetaan oikeus käsitellä välitystietoja sekä viestin sisältöä, on ollut mahdollista myös muissa kuin PL 10 §:n 4 momentin rajoituslausekkeen mukaisissa tilanteissa. Perustuslakivaliokunta ei kuitenkaan ole ottanut yksityisten väliseen asetelmaan kantaa viime vuosina, vaan uudempi lausuntokäytäntö PL 10 §:n 4 kohdasta koskee viranomaisten tiedonsaantioikeuksia. Perustuslakivaliokunnan myötävaikutuksella on kuitenkin vastikään säädetty nimenomaisesti SVPL 272 §:n soveltamiseen perustuvasta tietoturvaloukkausten havainnointipalvelusta (kyberturvallisuuslain 24 §, PeVL 62/2024 vp, HE 57/2024 vp). Näin ollen perustuslakivaliokunta ei ole uudemmassakaan käytännössään pitänyt SVPL 272 §:ään perustuvaa viestinnän tietojen käsittelyä valtiosääntöisesti ongelmallisena.

Nyt ehdotettu sääntely eroaa aikaisemmin käsitellystä tunnistamismääräyksestä (esim. PeVL 47/2024 vp) siinä, että kyse ei olisi viranomaisen määräyksen perusteella toteutettavasta toimenpiteestä. Perustuslain 10 §:n 4 momentissa sallitut rajoitusperusteet koskevat ensisijaisesti julkisen vallan taholta tulevia puuttumisia (PeVL 47/1996 vp). Toisaalta vapaaehtoisellakin viestien tunnistamisella toteutetaan pääasiassa julkista, rikosten ennaltaehkäisyyn liittyvää intressiä.

Julkiselle vallalle perustuslain 22 §:ssä säädetty perus- ja ihmisoikeuksien turvaamisvelvollisuus koskee oikeuksien toteutumista myös yksityisten keskinäisissä suhteissa. Velvollisuus kohdistuu säännöksen esitöiden mukaan käytännössä lähinnä lainsäätäjään, jonka tehtävänä on täsmentää perustuslaissa yleisellä tasolla ilmaistuja perusoikeuksia niin, että niiden vaikutus ulottuu myös yksityisiin suhteisiin (HE 309/1993 vp, s. 75). Yksityiselämän suojan takaamiseksi valtiolta on perinteisesti edellytetty sen ohella, että se itse pidättäytyy loukkaamasta kansalaisten yksityiselämää, myös aktiivisia toimenpiteitä yksityiselämän suojaamiseksi toisten yksilöiden loukkauksia vastaan. Yksityiselämän suojaa koskeva säännös yhdessä perusoikeuksien turvaamista koskevan perustuslain 22 §:n kanssa edellyttää lainsäätäjän ylläpitävän tehokasta perustuslain 10 §:ssä turvattujen oikeushyvien suojaa (HE 309/1993 vp, s. 53).

Vapaaehtoisuuteen perustuvan tunnistamisen laajuuden arvioinnissa keskeistä on sääntelyn välttämättömyyden ja oikeasuhtaisuuden arvioiminen. Tässä suhteessa merkityksellistä on, koskeeko oikeus viestintäsalaisuuden rajoittamiseen CSA-materiaalin tunnistamiseksi vain tunnettua CSA:ta vai myös uutta CSA:ta tai groomingia. Erityisen merkittävää välttämättömyys- ja oikeasuhtaisuusarvioinnin kannalta on, puututtaisiinko tunnistamisessa myös viestien sisältöön.

Käsillä olevassa ehdotuksessa pyrittäisiin mahdollistamaan sähköisen viestinnän käsittely lasten suojelemiseksi seksuaaliselta hyväksikäytöltä siten, että puuttuminen luottamukselliseen viestintään ja muihin perusoikeuksiin olisi mahdollisimman vähäistä ja oikeasuhtaista. Ehdotus sisältää useita, varsin yksityiskohtaisia edellytyksiä, jotka käsittelyn olisi täytettävä ollakseen lain mukaista. Keskeistä on, että

perusoikeuteen puuttumisen taustalla on erittäin painava yhteiskunnallinen intressi eli lasten suojeleminen vakavalta rikollisuudelta. Lasten seksuaalinen hyväksikäyttö loukkaa vakavasti perusoikeuksia ja erityisesti lasten oikeutta heidän hyvinvointinsa kannalta tarpeelliseen suojeluun ja hoivaan, ja kyse onkin laajasti kriminalisoidusta toiminnasta. Lisäksi EU-lainsäädäntö sekä useat kansainväliset sopimukset kuten esim. YK:n lapsen oikeuksien sopimuksen ja lapsen oikeuksien komitean työ sekä Euroopan neuvoston lapsen seksuaalisen väkivallan vastaisen ihmisoikeussopimus (nk. Lanzaroten sopimus), joihin Suomi on sitoutunut, edellyttävät sopimusvaltioilta toimia, joilla suojellaan lapsia kaikenlaiselta hyväksikäytöltä. YK:n lapsen oikeuksien komitea antoi Suomelle kesäkuussa 2023 uudet suositukset, joissa lasten suojaaminen väkivallalta on yksi keskeinen suosituksen aihe (CRC/C/FIN/CO/5-6). Komitea kiinnitti Suomen huomiota mm. turvaamaan tehokkaat toimet lasten suojaamiseksi verkossa tapahtuvalta (online) väkivallalta.

Sääntelyn välttämättömyyden ja oikeasuhtaisuuden kannalta merkityksellisiä voivat olla sääntelyyn liitetyt suojakeinot, joilla pyritään torjumaan sääntelyn muodostuminen liian laajaksi ja yksilöimättömäksi viestinnän sisällön tunnistamiseen. Esimerkiksi kompromissiehdotuksessa edellytetään, että kun on kyse groomingin tunnistamiseen käytettävästä teknologiasta, tällaisten epäilyä koskevien konkreettisten perusteiden olisi perustuttava objektiivisesti määritettyihin riskitekijöihin, kuten ikäeroon ja siihen, että seulottavan viestinnän osapuolena on todennäköisesti lapsi. Erityisesti groomingin havaitseminen aikaisessa vaiheessa voisi ennaltaehkäistä tehokkaasti lapsiin kohdistuvaa seksuaalirikollisuutta, millä voidaan katsoa olevan myönteisiä vaikutuksia paitsi lasten oikeuksien toteutumiselle myös koko yhteiskunnalle.

Sisäministeriön saamien tietojen mukaan tilapäisen poikkeusasetuksen voimassaoloaikana palveluntarjoajien teknologioiden käyttö ei ole herättänyt merkittävää julkista kritiikkiä tai sellaisia huolia tietosuojan tai tietoturvan vaarantumisesta, jotka olisivat johtaneet esimerkiksi komission tai kansallisten tietosuojaviranomaisten puuttumiseen niiden käyttöön.

Oikeusturva

Perustuslain 21 §:n 1 momentti sisältää yleissäännöksen jokaisen oikeudesta saada itseään koskeva asia lain mukaan toimivaltaisen tuomioistuimen tai muun viranomaisen ratkaistavaksi. Lähtökohtana on yksilön oikeus omasta aloitteestaan saada asiansa käsitellyksi. Käsittelyn tuomioistuimessa ja muussa viranomaisessa on lisäksi aina tapahduttava asianmukaisesti ja ilman aiheetonta viivytystä

Asetuksessa taataan oikeussuojakeinot myös uuden vapaaehtoiseen tunnistamiseen liittyvän toiminnon osalta. Kompromissiehdotuksessa säädetään asianmukaisista menettelyistä ja oikaisumekanismeista, joiden perusteella käyttäjät voivat valittaa heitä koskevista päätöksistä.

Viestinnän salaus perusoikeuksien toteutumisen kannalta

Viestinnän salausta perusoikeuksien toteutumisen kannalta on käsitelty yksityiskohtaisemmin U-jatkokirjelmässä UJ 19/2023 vp. Tältä osin asetusehdotus on

muuttunut hyväksyttävämpään suuntaan, sillä asetusehdotuksen aikaisemmissa esityksissä mukana ollut velvoite tunnistaa viestinnän sisältöä myös salatussa viestiympäristössä on poistunut tunnistamismääräyksen poiston myötä.

Valtioneuvoston kanta tiivistetysti

Valtioneuvosto pitää lapsiin kohdistuvan seksuaaliväkivallan torjumista ensisijaisen tärkeänä ja katsoo, että tavoitteeseen tulee pyrkiä keinoilla, jotka ovat tehokkaita ja oikeassa suhteessa tavoiteltuun päämäärään. Viestinnän luottamuksellisuuden suojaan ja muihin perusoikeuksiin puuttumisen tulee rajoittua vain välttämättömään ja sen tulee olla oikeasuhtaista. Sääntelyn ei tule johtaa laajaan ja yksilöimättömään viestinnän sisällön tunnistamiseen.

Valtioneuvosto katsoo, että asetusehdotus on kehittynyt monilta osin Suomen neuvottelutavoitteiden mukaiseen suuntaan. On hyvä, että aiempien esitysten kaltaisesta tunnistamismääräyksestä on luovuttu.

Valtioneuvosto pitää kannatettavana ehdotusta, jolla asetuksessa vakiinnutettaisiin numeroista riippumattomien viestintäpalvelun tarjoajien (esim. Facebook Messenger) vapaaehtoista tunnistamista koskeva tällä hetkellä tilapäinen sääntely palveluissa välitetyn CSA-materiaalin tai siellä tapahtuvan groomingin havaitsemiseksi ja siitä ilmoittamiseksi ja kyseisen materiaalin poistamiseksi. Jatkovalmistelussa on edelleen varmistettava, että vapaaehtoiselle tunnistamiselle asetetaan riittävät suojakeinot väärinkäytöksiä vastaan.

Ehdotettujen keinojen on oltava toteutettavissa ja tehokkaita, ja sääntelyn tulee olla mahdollisimman teknologianeutraalia, jotta varmistetaan ehdotuksen tulevaisuuskestävyys. Valtioneuvosto pitää hyvänä, että asetusehdotuksesta ei seuraa velvoitteita, jotka voivat tosiasiassa johtaa viestinnän päästä päähän -salauksen käytön tarkoituksen kiertämiseen.