

Euroopan komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaali-väkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final)

Eduskuntatunnus

U 69/2022 vp

Käsittelyvaihe ja jatkokäsittelyn aikataulu

Euroopan komissio antoi 11.5.2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ennaltaehkäisemiseksi ja torjumiseksi (jatkossa CSAM-asetusehdotus, COM (2022) 209 final). CSAM-asetusehdotuksen käsittely aloitettiin Tšekin puheenjohtajuuskaudella 2022. Ehdotuksen teknisen luonteen sekä tietosuojan ja luottamuksellisen viestin suojaan liittyvien kysymysten vuoksi sen käsittely on edennyt neuvostossa hitaasti. Unkari tavoitteli asiassa neuvoston yleisnäkemyistä oikeus- ja sisäasioiden neuvostossa 12.-13.12.2024, mutta puheenjohtajan esittämän kompromissiteksti ei saavuttanut riittävää määränemmistöstä tuekseen.

Puheenjohtaja Puolan johdolla jatketaan yli kaksi ja puolivuotta kestäneitä neuvotteluja neuvoston yleisnäkemyksen saavuttamiseksi. Tämä kirjelmä perustuu puheenjohtajan 28.1.2025 jakamaan kompromissiehdotukseen. Tämänhetkisten tietojen mukaan Puola tavoittelee puheenjohtajuuskaudellaan neuvoston osittaista yleisnäkemyistä kesäkuun oikeus- ja sisäasioiden neuvoston yhteydessä.

Suomen kanta

Valtioneuvosto täydentää aikaisempia, U 69/2022 vp:n yhteydessä muodostettuja, kantojaan seuraavasti osallistuakseen asetusehdotuksen käsittelyyn neuvostossa.

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 tosiasiaassa johtaa viestinnän päästä päähän -salauksen käytön tarkoituksen kiertämiseen.

Valtioneuvosto pitää edelleen tärkeänä sitä, että sääntelyn tulee olla EU:n tietosuojalainsäädännön mukaista.

Valtioneuvosto muodostaa asiassa lopullisen kantansa kokonaisarviointin pohjalta. Valtioneuvosto painottaa lapsen oikeuksien merkitystä, kun punnitaan ehdotuksen eri artiklojen suhdetta perustuslakiin ja perus- ja ihmisoikeuksiin.

Pääasiallinen sisältö

Lähtökohdan Puolan puheenjohtajuuskauden työlle on muodostanut edellisen puheenjohtajan Unkarin laatima kompromissiteksti. Puheenjohtajan laatiman uuden kompromissiehdotuksen tavoitteena on tehostaa lapsiin kohdistuvan seksuaaliväkivallan torjuntaa, rajoittamatta suhteettomasti käyttäjien perusoikeuksia ja huomioiden korkea tietosuojan taso.

Puheenjohtajan kompromissiehdotus perustuu komission alkuperäiseen ehdotukseen, neuvotteluprosessin myötä syntyneisiin ratkaisuihin sekä tuoreisiin – tarkemmin alla lueteltuihin – muutoksiin. Alkuperäisen ehdotuksen sisältöä on käsitelty tarkemmin asiaa koskevassa U-kirjelmässä (U 69/2022 vp) ja U-jatkokirjelmässä (UJ 19/2023 vp), sekä eduskunnalle toimitetussa erillisselvityksessä asian EUN 78/2024 vp yhteydessä.

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 (jatkossa CSA-materiaalia) sekä lasten houkuttelemista seksuaalisiin tarkoituksiin (ns. grooming) alustoillaan ja ilmoittamaan siitä viranomaisille, ja erityisesti tunnistamismääräyksen suhteeseen luottamuksellisen viestinnän suojaan sekä viestinnän salaukseen.

Asetusehdotukseen tehdyt keskeisimmät muutokset Puolan puheenjohtajuuskaudella

Puheenjohtajan valmisteleman kompromissiehdotuksen soveltamisalasta on poistettu kokonaan tunnistamismääräys ja siihen suoraan kytkeytyvät artikkelit (7-11 artikkelit). 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 kehoitetaan arvioimaan kolmen vuoden kuluessa asetuksen voimaantulosta, olisiko velvoittavalle tunnistamismääräykselle olemassa teknologiset ja oikeudelliset edellytykset.

Tunnistamismääräyksen sijaan puheenjohtaja ehdottaa vuonna 2021 voimaantulleella – ja vuonna 2024 jatkettulla – direktiivin 2002/58/EY tilapäisellä poikkeuksella (asetus (EU) 2021/1232 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, jäljempänä *tilapäinen poikkeusasetus*) tietyille palveluntarjoajille mahdollistettujen vapaaehtoisten käsittelytoimenpiteiden tuomista pysyvän sääntelyn piiriin (uusi artikla 4a). Toisin sanoen CSAM-asetuksella ehdotettaisiin vakiinnutettavaksi tilapäisen poikkeusasetuksen nojalla sovellettu menettely, joka mahdollistaa sen, että numeroista riippumattomat henkilöiden välisten viestintäpalvelujen tarjoajat 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. 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 esimerkiksi pikaviestintään tarkoitetut, internetin välityksellä toimivat puhe-, video-, videoneuvottelu- ja pikaviestipalvelut kuten WhatsApp tai Facebook Messenger.

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 päähen -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.

Puheenjohtajan kompromissiehdotuksessa palveluntarjoajia ei veloitettaisi aiemman ehdotuksen tapaan toimeenpanemaan CSA-materiaalin levittämiseen liittyviä riskejä lieventäviä toimenpiteitä, Sen sijaan viranomaiset voisivat suositella palveluntarjoajalle, jonka palveluun on tunnistettu liittyvän korkea riski CSA-materiaalin leviämiseen tai groomingiin, tiettyjen riskiä vähentävien toimenpiteiden käyttöönottoa.

Puheenjohtajan kompromissitekstissä on mukana ehdotusluonnokseen Belgian puheenjohtajuuskaudella (kevät 2024) lisätty palveluiden riskiluokittelujärjestelmä, joka pohjaisi viranomaisille välitettävään itsearviointiin. Säädöksiä on muutettu niin, että palveluntarjoajia koskevat riskinarviointi- tai ennaltaehkäisymenetelmät tulisi toteuttaa vain suositusperusteisesti, eikä velvoittavana toimina (5a artikla). Puheenjohtajan ehdotukseen on lisätty käyttäjälähtöiseen raportointiin painoarvoa, kun ehdotuksen mukaan korkean riskin palveluntarjoajilla olisi velvollisuus tarjota tehokkaita vaihtoehtoisia ilmoitusmekanismeja palvelun käyttäjille CSA-materiaaliin kytkeytyvissä tapauksissa (12 artikla).

Vaikuttaminen neuvoston lainvalvontatyöryhmässä (LEWP)

CSAM-asetusehdotus sisältää lukuisia eri velvollisuuksia, jotka parantaisivat lasten suojaamista verkkovälitteiseltä seksuaaliväkivallalta (riskien arviointi ja lieventäminen ja mm. poistamis-, esto- ja hakutuloksista poistamismääräykset, joilla poistettaisiin lasten seksuaalista väkivaltaa esittävä materiaali tai estettäisiin pääsy tällaiseen materiaaliin). Suomi on vaikuttanut neuvotteluissa pyrkimyksenä luoda tehokas lainsäädäntö lasten suojelemiseksi verkossa ja sen ulkopuolella.

Suomi on vaikuttanut neuvotteluissa kirjelmien U 69/2022 vp ja UJ 19/2023 vp kantojen, sekä suuren valiokunnan lausunnon SuVL 10/2024 vp mukaisesti. Valtioneuvosto on neuvotteluissa tuonut esille alustavaa positiivista suhtautumistaan puheenjohtajan ratkaisuun siinä, että aiempien esitysten kaltaisesta tunnistamismääräyksestä luovuttaisiin, ja että palveluntarjoajien mahdollisuudesta jatkaa CSA-materiaalin vapaaehtoista tunnistamista ja siitä raportointia turvattaisiin.

Samalla neuvotteluissa on pyritty selvittämään, mitkä olisivat tiettyjen palveluntarjoajien vapaaehtoisten tunnistamistoimien tosiasialliset vaikutukset mm. käyttäjien henkilötietojen ja yksityiselämän suojaan, erityisesti luottamuksellisen viestin salaisuuden suojaan korostaen samalla, että EU:n perusoikeuskirja tulee ottaa sääntelyssä asianmukaisesti huomioon. Lisäksi Suomi on neuvotteluissa pyrkinyt vaikuttamaan myös muilta osin sääntelyn selkeyteen suhteessa EU:n yleiseen tietosuojasetukseen.

Tilapäisen poikkeusasetuksen soveltamisajan jatkaminen

Tilapäinen poikkeusasetus tuli voimaan vuonna 2021, jolloin numeroista riippumattomille viestintäpalveluille mahdollistettiin sähköisen viestinnän tietosuojadirektiivin eli direktiivin 2002/58/EY tietyistä artikloista poikkeaminen silloin, kun viestinnän tietojen käsittely on tarpeen lasten seksuaalisen hyväksikäytön ja CSA-materiaalin havaitsemiseksi, poistamiseksi ja viranomaisten tietoon saattamiseksi. Asetuksen taustalla on eurooppalaisen sähköisen viestinnän säännösten (ns. teledirektiivi) (EU) 2018/1972 voimaantulo vuonna 2020, jolloin numeroista riippumattomat henkilöiden välisten viestintäpalvelut tulivat osaksi sähköisen viestinnän tietosuojadirektiivin soveltamisalaa. Valtioneuvoston kanta tilapäiseen poikkeusasetukseen on muodostettu U-kirjelmällä U 50/2020 vp.

Nimensä mukaisesti tilapäinen poikkeusasetus oli tarkoitettu ajalliselta soveltamiseltaan rajatuksi siihen asti, kunnes komissio antaa ehdotuksen pysyväksi lasten seksuaalista

hyväksikäyttöä torjuvaksi asetusehdotukseksi. Tilapäinen poikkeusasetus oli tarkoitettu olevan voimassa 3.8.2024 asti. CSAM-asetusehdotuksen neuvotteluiden venyessä loppuvuodesta 2023 tuli kuitenkin selväksi, että pysyvä sääntely ei ehtisi tulla voimaan ennen tilapäisen poikkeusasetuksen päättymispäivää. Oikeudellisesti epävarman välitilan välttämiseksi komissio antoi joulukuussa 2023 ehdotuksen, jolla pidennettiin tilapäisen poikkeusasetuksen soveltamista. Tilapäisen poikkeusasetuksen soveltamisaikaa pidennettiin 3.4.2026 asti. Lisäksi kolmikantaneuvotteluissa parlamentin kanssa yhdenmukaistettiin asetukseen sisältyviä raportointivelvoitteita.

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, mukaan lukien Euroopan ihmisoikeussopimuksen 8 artiklan sekä EU:n perusoikeuskirjan 7 ja 8 artiklan rajoittamisen on perustuttava lakiin, sillä on oltava hyväksyttävä tavoite ja sen tulee olla välttämätön ja oikeasuhteinen toimenpide tavoitteen saavuttamiseksi. Lisäksi riittävistä oikeusturvajärjestelyistä niille, joiden perusoikeuksia rajoitetaan, on varmistuttava. Jotta laissa säätämisen vaatimus täyttyy, toimenpiteen tulee paitsi perustua lakiin, lain säännösten tulee myös olla riittävän yksityiskohtaiset ja selkeät siten, että yksilöt pystyvät ennakoimaan toimintansa seuraukset.

Sen arvioinnissa, täyttääkö ehdotettu sääntely yleiset perusoikeuksien rajoittamisen edellytykset, merkitystä on ensinnäkin sillä, että rajoitustoimenpiteistä säädettäisiin yksityiskohtaisesti EU:n jäsenvaltioissa suoraan sovellettavassa asetuksessa. Toiseksi ehdotuksella on selvästi hyväksyttävä ja erittäin painava tavoite suojata lapsia verkkovälitteistä seksuaaliväkivallalta. Tavoite on yhteydessä useisiin perustuslaissa ja kansainvälisissä ihmisoikeussopimuksissa turvattuihin perus- ja ihmisoikeuksiin.

Perustuslakivaliokunta on CSAM-asetusehdotuksen yhteydessä aiemmin kiinnittänyt huomiota siihen, että sääntelyyn sisällynyttä 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 täytyessä. U-kirjelmässä U 50/2020 vp on käsitelty ehdotuksen suhdetta Euroopan unionin perusoikeuskirjan 7 ja 24 artikloihin vuonna 2021 tullessa tilapäisessä poikkeusasetuksessa. Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämänsä, 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.

Perustuslain 10 §:n ensisijaisena tarkoituksena on perusoikeusuudistuksen esitöiden mukaan (HE 309/1993 vp, s. 53/II) suojata luottamukselliseksi tarkoitettujen viestien sisältö ulkopuolisilta. Tämä merkitsee esimerkiksi suojaa kirjeiden ja muiden luottamukselliseksi tarkoitettujen viestien avaamista ja hävittämistä vastaan (PeVL 30/2001 vp, s. 2/I).

Perustuslakivaliokunta on arvioinut yksityiselle toimijalle annettavaa oikeutta käsitellä tiettyin edellytyksin tunnistamistietoja toisen yksityisen ja kolmannen tahon välisestä sähköisestä viestinnästä ensinnäkin sellaisen hallituksen esityksen yhteydessä, jossa esitettiin yhteisötilaajalle sallittavan tiettyin 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 laajemmin” tietojensaantioikeuden tapauksessa, mutta tarkoitettu viittaussuhde on epäselvä sikäli, tarkoittiko perustuslakivaliokunta yllä mainitun tulkinnan koskevan vain 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

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

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 tältäkin osin käsittely ei edellytä yksilöidyn rikosepäilyn olemassaoloa, vaan maksuvälinepetoksen valmistelua merkitseviä viestejä voidaan seuloa kaikesta soveltuvasta viestinnästä pykälän edellytysten täytyessä. 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 väliin asetelmaan kantaa viime vuosina, vaan uudempi lausuntokäytäntö PL 10 §:n 4 kohdasta koskee viranomaisen 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 uudemmasakaan 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 merkitsevää 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.

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 käsiteltyksi. Käsitellyn tuomioistuimessa ja muussa viranomaisessa on lisäksi aina tapahduttava asianmukaisesti ja ilman aiheutonta 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. Jos asetusehdotuksesta seuraisi velvoite purkaa viestinnän salausta, olisi sillä jatkokirjelmän mukaan laajakantoisia ja periaatteellisia vaikutuksia luottamuksellisen viestin salaisuuden suojaan sekä muiden perusoikeuksien toteutumiseen verkossa. Tämän lisäksi perustuslakivaliokunta kiinnitti huomiota siihen, että välillisesti salauksen purkaminen voisi johtaa myös perustuslain 12 §:ssä turvatun sananvapauden kannalta ongelmalliseen tilanteeseen. Asetusehdotuksen jatkovalmistelussa tulisi siten perustuslakivaliokunnan mukaan valtiosääntöoikeudellistakin syistä riittävästi varmistua siitä, ettei ehdotettu sääntely johda tietoturvallisuuden yleiseen heikentymiseen tietoverkoissa (PeVL 5/2023 vp, 10. kappale).

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.

EU:n oikeuden mukainen oikeusperusta/päätöksentekomenettely

Asetusehdotuksen oikeusperusta on Euroopan unionin toiminnasta tehdyn sopimuksen 114 artikla.

Lisäksi puheenjohtajan ehdottama tiettyjen verkkopalveluntarjoajien vapaaehtoiisiin CSA-materiaalin tunnistamistoimiin perustuva malli pohjautuu henkilötietojen käsittelyä koskevan sääntelyn osalta 16 artiklaan (SEUT), joka tarjoaa oikeusperustan säännöille, joka koskee unionin toimielinten, elinten ja laitosten sekä jäsenvaltioiden, silloin kun viimeksi mainitut toteuttavat unionin oikeuden soveltamisalaan kuuluvaa toimintaa, suorittamaa henkilötietojen käsittelyä, sekä säännöille, jotka koskevat näiden tietojen vapaata liikkuvuutta.

Ehdotus käsitellään yhdessä Euroopan parlamentin kanssa tavallisessa lainsäätämisyjärjestyksessä ja neuvosto tekee ratkaisunsa määräenemmistöllä. Valtioneuvoston arvion mukaan oikeusperustat on asianmukaisesti valittu ja niiden yhdistäminen on mahdollista.

Käsittely Euroopan parlamentissa

Parlamentti on jo muodostanut kantaansa CSAM-ehdotukseen.

Kansallinen valmistelu

U-jatkokirjettä on käsitelty kirjallisessa menettelyssä EU7 ja EU19 -jaostoissa 25.-31.3.2025

Eduskuntakäsittely

U 69/2022 vp, UJ 19/2023 vp

Kansallinen lainsäädäntö, ml. Ahvenanmaan asema

Asetusehdotuksen suhdetta Suomen lainsäädäntöön ja Ahvenanmaan asemaa on selvitetty U-kirjelmässä U 69/2022 vp.

Taloudelliset vaikutukset

Asetusehdotuksen taloudellisia vaikutuksia on selvitetty U-kirjelmässä U 69/2022 vp. Puheenjohtajan kompromissiehdotus sisältää kuitenkin sellaisia tilapäisestä asetuksesta siirrettyjä palveluntarjoajia koskevia raportointivelvoitteita, joilla voi olla lisätyövaikutusta tietosuojan valvontaviranomaisille. Merkittävimmät vaikutukset kuitenkin kohdistuvat niihin jäsenvaltioihin, joihin palveluntarjoajat ovat sijoittautuneet, ja alustavan arvion mukaan vaikutukset Suomessa olisivat vähäisiä.

Muut asian käsittelyyn vaikuttavat tekijät

-

Asiakirjat

-

Laatijan ja muiden käsittelijöiden yhteystiedot

Pekka Vasara, SM, pekka.vasara@gov.fi
Pauliina Penttilä, LVM, pauliina.penttila@gov.fi
Niklas Vainio, OM, niklas.vainio@gov.fi
Virpi Koivu, OM, virpi.koivu@gov.fi

VAHVA-tunnus

EU/88/2022

Napsauta tähän ja kirjoita kukin tunnus omalle rivilleen

Liitteet -

Viite -