Anu Mutanen, apulaisprofessori 21.10.2024

LAUSUNTO EDUSKUNNAN PERUSTUSLAKIVALIOKUNNALLE VALTIONEUVOSTON KIRJELMÄSTÄ (U 69/2022 VP) EUROOPAN KOMISSION EHDOTUKSESTA EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI LAPSIIN KOHDISTUVAN SEKSUAALIVÄKIVALLAN EHKÄISYÄ JA TORJUNTAA KOSKEVISTA SÄÄNNÖISTÄ (COM(2022) 209 FINAL)

Eduskunnan perustuslakivaliokunnan pyytämänä lausuntona otsikossa mainitusta valtioneuvoston kirjelmästä esitän kunnioittavasti seuraavan.

Yleistä

Valtioneuvoston kirjelmä (U 69/2022 vp) koskee ehdotusta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (CSAM-ehdotus). Asiasta on annettu myös valtioneuvoston jatkokirjelmä (UJ 19/2023 vp). Perustuslakivaliokunta on antanut asetusehdotusta koskevista valtioneuvoston kirjelmistä lausunnot PeVL 53/2022 vp ja PeVL 5/2023 vp. Tämän jälkeen suuri valiokunta on antanut asiassa lausunnon SuVL 7/2023 vp.

Nyt asian käsittelyn pohjana perustuslakivaliokunnassa ovat asetusehdotuksen käsittelyn tämänhetkistä vaihetta kuvaavat suuren valiokunnan perustuslakivaliokunnalle lähettämät seuraavat asiakirjat: Perusmuistio, sisäministeriö, EUN 78/2024 vp, 25.9.2024; sisäministeriön lausunto asiaan U 69/2022 vp ja puheenjohtajamaa Unkarin tuoreimpaan kompromissiehdotukseen, EUN 78/2024 vp, 8.10.2024; Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse – State of play, Council of the European Union, 2022/0155(COD), 12406/24, 7.10.2024.

Viimeksi mainituista asiakirjoista ilmenee, että puheenjohtajavaltio Unkari on tehnyt asiassa kompromissiehdotuksen osittaiseksi yleisnäkemykseksi asetusehdotuksesta. Asetusehdotusta on sen käsittelyn edetessä muutettu siten, että tunnistamismääräystä on kohdennettu aiempaan nähden. Tunnistamismääräys on kohdennettu vain jo kertaalleen tunnettuun CSA-materiaaliin, jonka tunnistamista pidetään teknologisesti lähes täydellisenä. Teknologisesti epätarkemmat menetelmät (groomingin ja uuden CSA-materiaalin tunnistaminen) rajattaisiin soveltamisalasta pois. Tunnistamismääräys kohdennettaisiin vain sellaisiin verkkopalveluntarjoajiin tai niiden osiin, joissa on todettu korkea riski CSA-materiaalin leviämiselle. Riskin toteamineen perustuisi viranomaisten toimesta tehtävään riskiluokitukseen. CSA-materiaalin tunnistusta voitaisiin tehdä ainoastaan visuaaliseen sisältöön {käytännössä kuvat ja videot), jonka osalta on jo olemassa luotettavia ja hyvin toimivia tunnistamisteknologioita. Teksti- tai ääniperustainen viestisisältö ei siis kuuluisi tunnistamismääräyksen soveltamisalaan. Tunnistamismääräyksen antaminen olisi kansallisen tuomioistuimen antama on viimesijainen keino. Tunnistamismääräys olisi myös rajattu ajallisesti ja pitäisi sisällään toimenpiteen valvonnan ja raportoinnin. Kompromissiehdotuksen pohjalta ei puretaisi viestin päästä päähän salausta, eikä tällaisen salauksen käyttöä kiellettäisi tai tehtäisi

mahdottomaksi. Tunnistamismääräyksen kohdentuessa päästä päähän salattua viestintää hyödyntävään palveluntarjoajaan hyödynnettäisiin hash-skannaustekniikoita ennen kuin viestin sisältö salautuu. Tämä toimenpide olisi mahdollista vain sillä edellytyksellä, että käyttäjät antavat palveluntarjoajan ehtojen mukaisesti nimenomaisen suostumuksensa siihen, että kyseistä tunnistamistoimintoa voidaan palvelussa käyttää.

Asiakirjojen mukaan Suomi voi tukea tätä esitystä, koska siinä vastataan riittävällä tavalla valtioneuvoston kannassa ja suuren valiokunnan lausunnossa esiin nostettuihin huomioihin ja reunaehtoihin. Esitetyillä rajausehdotuksilla – säilyttäen samalla kaikki palvelut soveltamisalan piirissä – on varmistettu suuren valiokunnan lausunnossaan edellyttämä asetelma, jossa säädettävien toimenpiteiden tulee olla riittävän tehokkaita ja samalla ennakoitavia oikeassa suhteessa ja välttämättömiä ehdotuksen tavoitteen toteutumiseksi. Suuri valiokunta on valtioneuvoston tavoin painottanut lapsen edun merkitystä, kun punnitaan ehdotuksen eri artiklojen suhdetta perustuslakiin ja perus- ja ihmisoikeuksiin. Ehdotetussa mallissa toteutuu myös suuren valiokunnan edellyttämällä tavalla se, että ehdotetut toimenpiteet eivät johda päästä päähän salauksen tai muiden vastaavien tietoturvatoimenpiteiden yleiseen heikentämiseen tai niiden purkamisen taikka niiden käytön rajoittamiseen ja tätä kautta viestinnän sekä viestintään liittyvien palvelujen tietoturvan ja kyberturvallisuuden tason heikkenemiseen. 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.

Olen antanut perustuslakivaliokunnalle 9.10.2023 lausunnon valtioneuvoston kirjelmästä (U 69/2022 vp) ja valtioneuvoston jatkokirjeestä (UJ 19/2023 vp) eduskunnalle Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä. Viittaan asian valtiosääntöoikeudellisen arvioinnin lähtökohtien osalta mainittuun aiempaan lausuntooni, jossa myös otin huomioon perustuslakivaliokunnan lausunnon PeVL 53/2022 vp. Esitän tässä lausunnossa arviointia mainitun lausunnon jälkeisen kehityksen valossa, etenkin asetusehdotuksen käsittelyn tämänhetkistä vaihetta kuvaavien asiakirjojen ja perustuslakivaliokunnan lausunnon PeVL 5/2023 vp muodostamalta perustalta.

Arviointi

CSAM-ehdotuksen keskeisimmät ongelmat ovat kytkeytyneet tunnistamismääräykseen (artikla 7), jonka nojalla verkkopalveluntarjoajia velvoitettaisiin tunnistamaan ja torjumaan CSA-materiaalia (CSA, child sexual abuse) alustoillaan, ja erityisesti sen suhteeseen luottamuksellisen viestinnän salaisuuden suojaan. Asian käsittelyn pohjana olevissa asetusehdotuksen käsittelyn tämänhetkistä vaihetta kuvaavissa asiakirjoissa on asianmukaisesti kuvattu asetusehdotukseen tehdyt keskeisimmät muutokset, jotka nähdäkseni keskeisesti kytkeytyvät etenkin luottamuksellisen viestinnän salaisuuden suojan aiempaa parempaan huomioon ottamiseen asetusehdotuksessa. Merkille pantavaa on, että asiakirjoissa ei esitetä varsinaista uutta valtiosääntöoikeudellista arviointia. Samalla voi kuitenkin todeta, että valtioneuvoston kirjelmässä ja jatkokirjeessä on käyty läpi keskeiset valtiosääntöoikeudellisesti merkitykselliset seikat luottamuksellisen viestin salaisuuden suojaa koskevan perustuslain 10 §:n 2 ja 4 momentin näkökulmasta. Pidän valtioneuvoston esittämää valtiosääntöoikeudellista arviointipohjaa

tältä osin sinänsä asianmukaisena enkä näe tarpeelliseksi toistaa sitä tässä. Tätä valtiosääntöoikeudellista arviointiperustaa kuitenkin täydentää perustuslakivaliokunnan lausunto PeVL 5/2023 vp, joka on vielä syytä ottaa huomioon.

Asian valtiosääntöoikeudellisessa arvioinnissa on yhtäältä tarpeen korostaa ehdotetun sääntelyn tavoitetta puuttua tietoverkon välityksellä tapahtuvaan lapsen fyysiseen ja henkiseen seksuaaliseen hyväksikäyttöön sekä lapsen houkutteluun. Perustuslakivaliokunta katsoi aiemmissa lausunnoissaan, 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 piti valtioneuvoston tavoin erittäin tärkeänä, että verkossa tapahtuvaan lapsiin kohdistuvaan seksuaaliväkivaltaan pystytään puuttumaan tehokkaasti (PeVL 5/2023 vp, kappale 1 ja 2, PeVL 53/2022 vp, kappale 2). Käsiteltävänä olevan ehdotuksen tavoitteet ovat siten epäilyksittä valtiosääntöoikeudellisesti kannatettavia ja voivat sinänsä osaltaan perustella niiden saavuttamiseksi tarvittavia perusoikeusrajoituksia.

Toisaalta arvioinnissa on syytä painottaa perustuslakivaliokunnan näkemysten mukaisesti sitä, että asetusehdotus muodostaa varsin laajan ja monimutkaisen sääntelykokonaisuuden, ja se on merkittävä useiden perustuslaissa turvattujen perusoikeuksien kannalta (PeVL 5/2023 vp, kappale 3). Lisäksi on tarpeen korostaa, että asetusehdotuksen periaatteellinen merkitys on paitsi huomattava myös ongelmallinen erityisesti luottamuksellisen viestin salaisuuden suojan kannalta. Erityisesti palveluntarjoajille asettavaksi ehdotetun tunnistamisvelvoitteen voi arvioida olevan luonteeltaan hyvin perusoikeusherkkä. Nyt arvioitavana olevat muutosehdotukset eivät muuta mainittuja lähtökohtia.

Perustuslakivaliokunta kiinnitti aikaisemmissa lausunnoissaan huomiota siihen, että ehdotuksen mukaisia tunnistamismääräyksiä ei ollut rajattu tiettyihin henkilöihin. Sääntelyn soveltaminen voi siten muodostua varsin laajaksi ja yksilöimättömäksi. Valiokunta kiinnitti huomiota myös siihen, että ehdotettu sääntely koski myös tilanteita, joissa ei ole kyse konkreettisesta ja yksilöidystä rikosepäilystä. (PeVL 5/2023 vp, kappale 4, PeVL 53/2022 vp, kappale 9 ja 10.) Perustuslain 10 §:n 4 momentissa mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiin kuuluvasta välttämättömyysvaatimuksesta seuraa, että luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee olla mahdollisimman kohdennettua ja rajattua. Perustuslain 10 §:n 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa. Perustuslakivaliokunnan käsityksen mukaan asetusehdotuksen sääntely ei vaikuttanut ongelmattomalta perustuslain 10 §:n 4 momentin kannalta. (PeVL 5/2023 vp, kappale 5 ja 6, PeVL 53/2022 vp, kappale 12, ja niissä viitatut lausunnot.)

Havaintojeni mukaan tunnistamismääräystä koskevaan sääntelyyn asetusehdotuksessa ei ole toistaiseksi esitetty mainittuihin perustuslakivaliokunnan ongelmallisina pitämiin seikkoihin kohdistuvia muutoksia. Sääntelyä ei olisi edelleenkään rajattu tiettyihin henkilöihin ja sääntely koski myös tilanteita, joissa ei ole kyse konkreettisesta ja yksilöidystä rikosepäilystä. Tältä osin perustuslakivaliokunnan aiemmat asiaa koskevat kannat ovat siten edelleen merkityksellisiä. Asiassa voi yhtyä valtioneuvoston ja suuren valiokunnan arvioon siitä, että ehdotettu sääntely 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. Näin ollen asetusehdotuksen sääntely ei vaikutta näiltä osin edelleenkään ongelmattomalta perustuslain 10 §:n 4 momentin kannalta. Etenkään mahdollisuus puuttua viestintäsisältöihin jopa ilman konkreettista rikosepäilyä ei ole yhteensopiva perustuslain 10 §:n 4 momentissa säädettyjen luottamuksellisen viestin salaisuuden rajoitusedellytysten kannalta.

Samalla on syytä kiinnittää jälleen huomiota siihen, että perustuslakivaliokunta on perustuslain 10 §:n muuttamisen yhteydessä pitänyt perusteltuna, että hallitus käynnistää selvitystyön, joka kattaisi laajemminkin perustuslain kotirauhan suojaa ja luottamuksellisen viestin salaisuutta koskevien rajoituslausekkeiden muutostarpeen (PeVM 4/2018 vp, s. 6). Valiokunta on sittemmin kiirehtinyt selvitystyön aloittamista (mm. PeVL 12/2019 vp, s. 6, PeVL 6/2019 vp, s. 5) ja pitänyt perustuslain 10 §:n rajoituslausekkeiden muutostarpeiden selvitystyötä välttämättömänä. Muutostarpeita tulee arvioida ottaen huomioon muun muassa vakavan rikollisuuden uudet muodot ja tapahtunut teknologinen kehitys (PeVL 5/2023 vp, kappale 9, PeVL 30/2010 vp, s. 6).

Perustuslakivaliokunta kiinnitti CSAM-ehdotuksesta antamissaan aiemmissa lausunnoissa lisäksi huomiota siihen, että ehdotettu sääntely kohdistuisi myös viestinnän sisältötietoihin ja jättäisi epäselviksi erityisesti tunnistamismääräyksen perusteella käytettävän teknologian käytön vähimmäiskriteerit. Lisäksi ehdotukseen nähtiin liittyvän runsaasti oikeudellista epävarmuutta siitä, pystyttäisiinkö tunnistamismääräyksen perusteella käytettävä teknologia kohdentamaan siten, että erilaisten palveluiden piirissä tapahtuva viestiliikenteen käsittely olisi riittävän kohdennettua perustuslain ja perusoikeuskirjan tulkintakäytännössä edellytetyllä tavalla. (PeVL 5/2023 vp, kappale 6.)

Mainittuihin seikkoihin tunnistamismääräyksen kohdentumisesta ja sen perusteella käytettävästä teknologiasta on havaintojeni mukaan esitetty merkittäviä muutoksia. Tällaisia olisivat etenkin tunnistamismääräyksen kohdentaminen vain jo kertaalleen tunnettuun CSA-materiaaliin ja vain sellaisiin verkkopalveluntarjoajiin tai niiden osiin, joissa on todettu korkea riski CSA-materiaalin leviämiselle sekä se, että CSA-materiaalin tunnistusta voitaisiin tehdä ainoastaan visuaaliseen sisältöön. Tunnistamismääräys olisi ajallisesti rajattu kansallisen tuomioistuimenantama viimesijainen keino, johon liittyisi myös raportointi- ja valvontamenettely. Kaikkiaan on myönteistä, että muutoksilla on pyritty teknologisesti aiempaa tarkempien ja luotettavimpien menetelmien käyttöön. Samalla on kuitenkin todettava, vaikka teksti- tai ääniperustainen viestisisältö ei kuuluisi tunnistamismääräyksen soveltamisalaan, kohdistuisi sääntely kuitenkin visuaalisiin sisältöihin ja siten edelleen osaan viestinnän sisältötiedoista.

Perustuslakivaliokunta tarkasteli lisäksi tässä asiayhteydessä kysymystä viestinnän salauksesta perusoikeuksien toteutumisen kannalta (etenkin perustuslain 10 §:n mukainen luottamuksellisen viestin salaisuuden suoja ja 12 §:ssä turvattu sananvapaus) ja totesi, että asetusehdotuksen jatkovalmistelussa tulisi riittävästi varmistua siitä, ettei ehdotettu sääntely johda tietoturvallisuuden yleiseen heikentymiseen tietoverkoissa (PeVL 5/2023 vp, kappale 10). Kompromissiehdotuksen pohjalta ei purettaisi viestin päästä päähän salausta, eikä tällaisen salauksen käyttöä kielletä tai tehdä mahdottomaksi. Tunnistamismääräys voisi kuitenkin kohdentua päästä päähän salattua viestintää hyödyntävään palveluntarjoajaan, ja tällöin hyödynnettäisiin hash-skannaustekniikoita ennen kuin viestin sisältö salautuu. Tämä

toimenpide olisi mahdollista vain, jos käyttäjät antavat palveluntarjoajan ehtojen mukaisesti nimenomaisen suostumuksensa tunnistamistoiminnon käyttämiselle palvelussa. Ehdotetuissa muutoksissa vaikutetaan otettavan huomioon tietoturvallisuuden yleiseen heikentymiseen tietoverkoissa kytkeytyviä valtiosääntöisestikin merkityksellisiä huolia.

Kaikkiaan voi todeta, että asetusehdotukseen ehdotetut muutokset ovat sinänsä merkittäviä myös valtiosääntöoikeudellisesti esimerkiksi siinä, että tunnistamisvelvoite kohdistuisi vain viestintään, jossa on jo tunnistettu lapsen hyväksikäyttöä tarkoittavaa materiaalia. Tältä osin voi yhtyä kantaan siitä, että tunnistamismääräyksestä on tehty aiempaa hyväksyttävämpi, myös valtiosääntöisesti. Ehdotetussa sääntelyssä on pyritty etsimään keinoja parantaa ja tehostaa verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa perusoikeuksiin aiempia ehdotusmuotoiluja vähemmän puuttuvilla ja aiempaa tarkemmin kohdistetuilla toimenpiteillä.

Samalla on kuitenkin syytä korostaa, että asetusehdotus on näkemykseni mukaan edelleen osin ongelmallinen perustuslain 10 §:n 2 ja 4 momentin suojaaman luottamuksellisen viestin salaisuuden suojan kannalta. Tällaisina ongelmakohtina näyttäytyvät etenkin viestisisältöihin puuttuminen, henkilöllinen kohdentamattomuus, rajautumattomuus rikoksen tutkintaan ja konkreettiseen ja yksilöityyn rikosepäilyyn. Näiltäkin osin on siten syytä toistaa perustuslakivaliokunnan aiemmat kannat asetusehdotukseen oikeasuhteisuudesta ja välttämättömyydestä sekä täsmällisyydestä ja tarkkarajaisuudesta suhteessa sääntelyn tarkoittamiin viestinnän luottamuksellisuuden suojan rajoituksiin (PeVL 5/2023 vp, kappale 8). Mainittujen valtiosääntöoikeudellisten ongelmakohtien asianmukaista huomioon ottamista asian jatkokäsittelyssä on syytä korostaa viitaten siihen, että perustuslakivaliokunta on painottanut yleisesti sen varmistamista, että EU-oikeuden asetusehdotukset pysyvät olemassa olevien perus- ja ihmisoikeusperiaatteiden puitteissa (PeVL 5/2023 vp, kappale 7 ja siinä viitatut lausunnot).

Helsingissä 21.10.2024

Anu Mutanen, apulaisprofessori