

14.09.2023

POL-2022-118237

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)

1 Lausuntopyynnöstä

Eduskunnan liikenne- ja viestintävaliokunta on 5.9.2023 pyytänyt Poliisihallituksen lausuntoa asiasta *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)* sekä ilmoittamaan Poliisihallituksen asiantuntijan valiokunnan järjestämään kuulemiseen.

2 Valtioneuvoston kirjelmästä

2.1 Yleistä asetusehdotuksesta

Yllä mainitun valtioneuvoston kirjelmän sisältö on kannatettava. Prosessi eurooppalaisen lainsäädännön luomiseksi, jonka pyrkimyksenä on suojella lapsia verkkovälitteisen seksuaaliväkivallalta, on ollut pitkä. Lapsiin kohdistuva seksuaaliväkivalta ja siihen liittyvä kuvallisen aineiston välittäminen ja hallussapito on laajasti kriminalisoitu ja valtiot kannattavat toimenpiteitä, jolla voidaan tehostaa lapsiin kohdistuvan seksuaalisen väkivallan torjuntaa, vaikka kaikilta osin ei ole yksimielisyyttä toimenpiteiden laadusta. Komission esitys asetukseksi on ollut lähtökohdiltaan kunnianhimoinen ja sen tavoitteena on ollut osallistaa internetin säilytys- ja välityspalveluita tarjoavat yritykset lapsiin kohdistuvan seksuaalisen väkivallan torjuntaan. Pelkästään kansalliset lainsäädännölliset tai viranomaistoimet eivät johda kyseisen vakavan rikollisuuden torjunnan kannalta toivottuun lopputulokseen.

Keskusrikospoliisilta saadun tiedon mukaan sen lapsiin kohdistuvan seksuaalisen väkivallan torjunnan ryhmä käsitteli viime vuonna noin 10 000 kyseiseen rikollisuuteen liittyvää tietoa. Tieto tulee pääosin ulkomailta ja saatua tietoa käytetään arvioitaessa, onko Suomessa asiassa syytä epäillä rikosta ja aloitetaanko esitutkinta. Vaikka saapuvan tiedon määrä on valtava ja se kasvaa koko ajan on tiedossa, että kyseessä on vain jäävuoren huippu internetin palveluissa olevasta tiedosta, joka koskee lapsiin kohdistuvaa seksuaalista väkivaltaa.

Suomi on sitoutunut kansainvälisiin sopimuksiin, joiden tavoitteena on taata turvallinen lapsuus. Edellä mainittuja sopimuksia ovat mm. YK:n lapsen oikeuksien sopimuksen sekä Euroopan neuvoston ihmisoikeussopimuksen lasten suojaamiseksi seksuaaliväkivallalta (nk. Lanzaroten sopimus), mukainen.

Lapsiin kohdistuvan seksuaalisen väkivallan torjunnan keinojen on oltava, kuten muunkin lainsäädännön, tarkkarajaista ja oikeasuhtaista. Keinojen oikeasuhtaisuutta arvioitaessa on annettava riittävä paino lasten turvallisuudelle ja seksuaaliselle itsemääräämisoikeudelle suhteessa muihin oikeuksiin eikä arvioida lainsäädännön vaikutuksia pelkästään muihin perusoikeuksiin.

2.2 Tunnistamismääräyksestä ja sen toteuttamisesta

Komission antamassa asetusehdotuksessa säädettäisiin toimista, joiden tavoitteena olisi vähentää riskiä internetin eri palveluissa tapahtuvalle lapsiin kohdistuvan seksuaalisen väkivallan kuva-aineiston jakamiselle sekä lasten houkuttelua seksuaalisiin tekoihin (grooming). Lähtökohta toiminnalle on uusi ja sisältäisi internetin palveluntarjoajille asetettavia velvollisuuksia tunnistaa edellä kuvattua sisältöä. Pieni osa palveluntarjoajista toimii tällä hetkellä viranomaisten ja kolmannen sektorin kanssa yhteistyössä riskien vähentämiseksi, mutta toimet eivät ole olleet komission arvioiden mukaan riittäviä ja sen vuoksi on tarpeen säätää toimista, joilla voidaan vähentää lasten ja nuorten riskiä joutua seksuaalisen väkivallan kohteeksi erilaisissa internetin palveluissa.

Tunnistamismääräykseen liittyen olennaista on se, että tunnistamismääräys kohdennettaisiin tuomioistuimen tai hallintoviranomaisen määräyksellä sellaisiin palveluntarjoajiin, joissa olisi kohonnut riski lasten seksuaalisen väkivallan aineiston levittämiseksi tai groomingille, joten se ei kohdistuisi kaikkiin tai kaikkeen viestintään. Ennen tunnistamismääräyksen antamista palveluntarjoajaa olisi myös kuultava. Tunnistamismääräys rajattaisiin ajallisesti ja palveluntarjoajalla olisi asetuksen perusteella velvollisuus tiedottaa käyttäjiään niistä toimista, joihin se on ryhtynyt riskien vähentämiseksi. Tunnistamismääräys ei siis kohdentuisi kaikkiin viestinnän palveluita tarjoaviin toimijoihin, eikä olisi siten yleistä ja erottelematonta toimintaa. Teknologiat, joita käytettäisiin edellä mainitun aineiston tunnistamiseksi olisivat palveluntarjoajan päätettävissä ja EU-keskus tarjoaisi maksutta näitä teknologioita palveluntarjoajien käyttöön. Teknologinen kehitys on nopeaa ja on varmistettava, että palveluntarjoajilla on mahdollisuus hyödyntää uusinta teknologiaa tunnistamismääräysten toteuttamisessa. Tunnistamismääräys tarkoittaisi käytännössä sitä, että viestin sisältö skannattaisiin ja mikäli sieltä tunnistettaisiin asetuksessa määriteltä aineistoa, niin viesti otettaisiin lähempään tarkasteluun.

Esitettyä tunnistamismääräystä on kritisoitu mm. siksi, että rikolliset siirtyisivät palveluihin, joihin ei olisi kohdistettu tunnistamismääräystä tai palvelut kieltäytyisivät sitä toteuttamasta. Olennaista on kuitenkin se, että asetuksella vaikutettaisiin sellaisiin palveluihin, joissa on paljon käyttäjiä ml. lapsia ja nuoria. On selvää, ettei millään lainsäädännöllisillä toimilla voidaan estää tällaista vakavaa rikollisuutta kokonaisuudessaan, mutta haittoja voidaan vähentää merkittävästi ja tehdä rikollisesta toiminnasta nykyistä hankalampaa, jolloin riski joutua lapsiin kohdistuvan seksuaalisen väkivallan uhriksi pienenee.

Tunnistamismääräystä vastaavaa eurooppalaista lainsäädäntöä ei ole käytettävissä vertailupohjaksi, mutta kansallisesti laki sähköisen viestinnän palveluista (917/2014) 272 §:ssä säädetään viestinnän välittäjän ja lisäarvopalveluiden tarjoajan oikeudesta viestinnän sisältötietojen automaattiseen selvittämiseen. Tämä toimi on verrattavissa esitettyyn tunnistamismääräykseen automaattisen skannauksen sekä pykälän 1 momentin 1. kohdan mukaisesti asian esitutkintaan saattamiseksi. Kyseisen lainkohdan osalta ei ole esitetty laajaa kritiikkiä siitä, että se vaarantaisi tieto- tai kyberturvallisuutta. Kyseistä lainkohtaa on perusteltu hallituksen esityksessä HE 48/2008 vp muun muassa roskapostituksen torjumisella.

2.3 Salauksesta

Tunnistamismääräyksen toteuttamisen kannalta on tärkeää, että suurin osa tunnistamismääräyksen kohteena olevan palveluntarjoajan tarjoamasta sisällöstä voidaan seuloa siten, että sieltä voidaan tunnistaa lapsiin kohdistuvan seksuaaliseen väkivaltaan liittyvää aineistoa. Internetissä tapahtuva liikenne on pääosin tavalla tai toisella salattua ja salauksen kannalta on tärkeää ymmärtää salauksen ja päästä päähän tapahtuvan salauksen ero. Tieto voi olla salattu siten, että sen välittäminen on turvallista, mutta eri viranomaiset voivat päästä lain sallimissa tapauksissa sisältöön. Rikosten torjumiseksi esitutkintaviranomaisilla on lain säätämässä tapauksissa ja tuomioistuimen päättämässä yksittäistapauksissa oikeus telekuunteluun. Olennaista rikosten torjumiseksi käytettävien pakkokeinojen suhteessa salaukseen on se, että teleoperaattoreille on Suomessa ja kansainvälisesti asetettu lainsäädännössä velvoitteet toteuttaa heidän tarjoamat palvelut siten, että telekuuntelu voidaan suorittaa. Teknologinen kehitys on edennyt säätelyä nopeammin ja siksi esimerkiksi pikaviestinpalveluita tarjoaville yrityksille ei ole asetettu samanlaisia velvoitteita kuin teleoperaattoreille. Edellä mainittu mahdollistaa sen, että pikaviestintää käyttävät yritykset hyödyntävät viestien välityksessä päästä päähän salattua viestiliikennettä, jolloin viestien sisältötiedon saaminen ei ole mahdollista välittävänä olevasta viestistä. Tähän ongelmaan tulisi etsiä ratkaisua palveluntarjoajien kanssa tehtävällä yhteistyöllä.

Toinen vaihtoehto sisällön skannauksen osalta olisi toteuttaa se käyttäjän laitteilla sen palveluntarjoajan ohjelmistolla, johon tunnistamismääräys kohdentuu. Nykyisinkin laitteilla oleva tieto, joka tarvitaan ohjelman tai pika-viestinnän käyttämiseen on sellaista tietoa, johon on annettava pääsy tai sovellusta ei voi muutoin käyttää.

Tietoon pääsy ei edellytä myöskään takaovien luomista järjestelmään. Telekuuntelussa televiestinnän sisältöön pääsy on mahdollista operattoreiden käytössä olevien järjestelmien ansiosta ja siinä yhteydessä ei puhuta takaovesta ja tätä termiä ei tulisi käyttää myöskään tietoon pääsystä muiden viestinnän palveluita tarjoavien tahojen kanssa. Kun tietoon pääsy on palveluntarjoajan kontrollissa, toimintatapa EU-keskuksen tiedossa ja käyttäjiä tiedotettu riskien vähentämiseen tähtäävistä toimenpiteistä ei voida puhua takaovesta. Takaovi on kyberturvallisuuden terminä käytössä sellaisissa tilanteissa, jossa järjestelmään saadaan pääsy salaa ja tavalla, joka ei ole ulkopuolisten tiedossa. Asetusehdotuksen tavoitteena on julkinen ja kuvattu prosessi, jota valvovat palveluntarjoajien lisäksi myös mm. EU-keskus. Oikeampaa olisi puhua etuovesta, koska tunnistamismääräyksen prosessi on läpinäkyvä ja avoin.

3 Ilmoittamisvelvollisuudet

Asetuksella palveluntarjoajille asetettavat ilmoitusvelvollisuudet eivät saa haitata lapsiin kohdistuvien seksuaalirikosten syylistyneiden henkilöiden tunnistamista, tutkimista ja syytetoimia jäsenvaltioissa.

4 Resurssivaikutukset poliisiin

Kuten lausunnon alussa on todettu, niin poliisi vastaanottaa jo nykyisin mit-tavan määrän lapsiin kohdistuvaan seksuaaliseen väkivaltaan liittyvää tie-toa. Mikäli tiedon määrä ja poliisille tehtävät ilmoitukset kasvavat on välttä-mätöntä varmistaa poliisin riittävät resurssit sekä ilmoitusten käsittelyyn että rikosten tutkintaan. Tässä vaiheessa arviona voidaan esittää, että pel-kästään ilmoitusten käsittelyyn on tarvetta osoittaa viisi henkilötyövuotta. Mikäli poliisille tehtävien ilmoitusten määrä kasvaa huomattavasti olisi ky-seisten rikosten tutkintaan poliisille osoitettava vähintään kymmenen henki-lötyövuotta lisää.