FiCom ry | Asko Metsola
28.9.2022

FiComin lausunto lapsiin kohdistuvan verkkovälitteisen seksuaaliväkivallan torjunnasta

Eduskunnan hallintovaliokunta on pyytänyt FiComilta lausuntoa valtioneuvoston kirjelmästä, joka koskee Euroopan komission ehdotusta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä. FiCom kiittää mahdollisuudesta tulla kuulluksi ja esittää kunnioittavasti seuraavaa:

FiComin keskeiset viestit

- Asetusehdotuksen tulee olla yhteensopiva muun EU-sääntelyn kanssa.
- Soveltamiselle tulee varata pidempi aika lukuisten uusien velvoitteiden takia.
- Numeroihin perustuvien henkilöiden välisten viestintäpalveluiden tarjoajat tulee jättää asetuksen velvoitteiden ulkopuolelle, ja asetuksen määritelmiä on muutenkin tarkistettava.
- Groomingiin ja CSAM:iin kohdistuvien tunnistamismääräysten edellytyksiä on tarkennettava.
- Estomääräyksiä koskeviin artikloihin on tehtävä lukuisia korjauksia tietosuojan ja verkkoturvallisuuden varmistamiseksi.
- Usealle eri taholle raportointia on vältettävä, ja palveluntarjoajilla tulee olla vastuuvapauden suojaama mahdollisuus kehittää ja ottaa käyttöön uusia teknologioita CSAM:n torjumiseksi, myös vapaaehtoisesti.

FiComin jäsenet ja koko ICT-ala on sitoutunut ehkäisemään ja torjumaan lapsiin kohdistuvaa seksuaalista väkivaltaa. Tämän osoittaa mm. teleyritysten lain 1068/2006 nojalla yhteistyössä Keskusrikospoliisin suorittamat aktiiviset, vapaaehtoiset toimet alaikäisiin kohdistuvan seksuaalisen väkivallan ehkäisemiseksi sekä toimialan yhteiset hankkeet lapsiin kohdistuvaa verkkorikollisuutta vastaan. Esimerkiksi verkkoalustojen käyttäjiä kannustetaan ilmoittamaan laittomaksi epäiltyjä verkkosisältöjä tai -toimintaa poliisille tai Pelastakaa Lapset -järjestön Nettivihje-palveluun.

FiCom on mukana kansainvälisen Safer Internet Day -kampanjan osana järjestettävässä Mediataitoviikossa, tukee aktiivisesti Suojellaan Lapsia ry:n Turvallisesti digiliikenteessä -kampanjaa sekä kokoaa säännöllisesti yhteen jäsenyritystensä asiantuntijoita ratkomaan lasten verkkoturvallisuuteen liittyviä haasteita. Lisäksi FiCom on puheenjohtajana alan eurooppalaisen yhteistyöjärjestön EuroISPA:n Safer Internet -työryhmässä, jossa jaetaan parhaita käytänteitä eri jäsenjärjestöjen kotimaista.

Tästä huolimatta FiCom on jäsenineen huolissaan komission nyt ehdottaman asetuksen toimivuudesta ja tulevaisuudesta, varsinkin koska eräät asetukseen ehdotetut velvoitteet ja toimenpiteet ovat teknisesti mahdottomia toteuttaa tai ne eivät sovellu palveluiden käyttötarkoitukseen. Lisäksi nyt ehdotettu asetusteksti on ristiriidassa ehdotetun sähköisen viestinnän tietosuoja-asetuksen (ePrivacy) ja voimassa olevan ePrivacy-direktiivin, verkko- ja tietoturvadirektiivin päivityksen (NIS 2.0), yleisen tietosuoja-asetuksen (GDPR) sekä verkkoneutraliteettisääntöjen suojaamien perusperiaatteiden kanssa.

Asetusehdotuksen tulee olla yhteensopiva muun EU-sääntelyn kanssa

Euroopan unionin tuomioistuin on tehnyt ratkaisuissaan täysin selväksi, että sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohdassa suojattu viestinnän luottamuksellisuus on tulkinnassa pääsääntö. Viestinnän luottamuksellisuuteen tehtyjen poikkeuksien tulee säilyä poikkeuksena eikä muuttua säännöksi. Tätä periaatetta on noudatettava myös nyt ehdotetussa asetuksessa.

Viestintäpalveluiden end-to-end-salaus sekä TLS:n (Transport Layer Security) ja HTTPS:n (Hypertext Transfer Protocol Secure) kaltaiset salausprotokollat ovat välttämättömiä, jotta internetiin voi luottaa. Ne takaavat kyberturvallisuuden ja tietosuojan internetissä, ja vielä tänä vuonna voimaan tuleva NIS 2.0 -direktiivi suosittelee ja paikoin jopa vaatii niitä. Salauksen murtuminen romahduttaisi internetin teknisen infrastruktuurin ja estäisi yritysten pyrkimyksiä edistää luottamusta, käyttäjien yksityisyyttä ja sananvapautta internetissä. Ilman salausta mikään järjestelmä maailmassa ei olisi enää turvallinen. Asetus ehdotetussa muodossaan vaarantaa kaikkien Euroopan kansalaisten perusoikeudet, itsemääräämisoikeudet sekä liikesalaisuuksien ja innovaatioiden suojan. Tällä taas olisi valtava vaikutus koko EU-alueen talouteen.

Asetusehdotus on erityisesti lapsen seksuaalisiin tarkoituksiin houkuttelun (grooming) osalta ristiriidassa yleisen tietosuoja-asetuksen (GDPR) kanssa. Ehdotettu kansallisen koordinoivan viranomaisen pakollinen rooli tilanteessa, jossa yritys ilmoittaa epäilyttävästä sisällöstä johtaa siihen, että viranomainen voi päästä käsiksi sisältöön, joka ei ole asetusehdotuksessa tarkoitettua lapsiin kohdistuvaa seksuaaliväkivaltaa todistavaa kuvamateriaalia (Child Sexual Abuse Material, CSAM) tai edes muutenkaan laitonta. Tämä vaarantaa asianomaisten henkilöiden yksityisyyden.

Kansallisten tietosuojaviranomaisten ja kansallisten koordinoivien viranomaisten yhteistyö on olennaista sääntelyjen vastavuoroisuuden kannalta. Jos tietosuojaa koskevassa vaikutustenarvioinnissa päädytään siihen lopputulokseen, että tietty toimenpide ei ole GDPR:n mukaan sallittu ja tietosuojaviranomainen tämän vahvistaa, on asetusehdotuksen mukaisen koordinoivan viranomaisen noudatettava tätä lopputulosta. Se ei saa vaatia palveluntarjoajalta toimenpiteitä, jotka ovat ristiriidassa tietosuojavelvoitteiden kanssa.

Asetusehdotus vaarantaa verkkoneutraliteetin periaatteen vaatimalla URL-osoitteisiin kohdistuvaa estomääräystä, sillä tällainen estomääräys edellyttää palveluntarjoajalta yksityiskohtaista analyysiä kaikista verkkojensa kautta lähetetyistä datapaketeista (DPI, Deep Packet Inspection). Asetusehdotuksen 1 artiklan 3 kohtaan tulee lisätä kohta ”*e) Asetus (EU) 2015/2120*” sen varmistamiseksi, että estomääräyksissä huomioidaan myös verkkoneutraliteetti. Vastaava lisäys tulee tehdä myös johdantolauseeseen 7.

Asetuksen tulee olla yhteensopiva myös piakkoin voimaantulevan digipalvelusäädöksen (Digital Services Act, DSA) 7 artiklan kanssa, jonka mukaan ”*välittäjäpalvelujen tarjoajille ei saa asettaa yleistä velvoitetta valvoa siirtämiään tai tallentamiaan tietoja eikä velvoitetta pyrkiä aktiivisesti saamaan selville laitonta toimintaa osoittavia tosiasioita tai olosuhteita*”. Yleisen valvontavelvollisuuden kielto sisältyy myös vielä voimassa olevaan sähköisestä kaupankäynnistä annettuun direktiiviin (sähkökauppadirektiivi).

Asetusta olisi tarkoitus soveltaa jo kuuden kuukauden kuluttua sen voimaantulosta. Kuten U-kirjelmässäkin on todettu, ehdotuksesta voidaan arvioida aiheutuvan palveluntarjoajille uudenlaisia tehtäviä, merkittäviä kustannuksia ja hallinnollista taakkaa uusien velvoitteiden myötä. Asetuksen velvoitteiden soveltamiselle varattu lyhyt, vain kuuden kuukauden aika on erittäin ongelmallinen lukuisten uusien velvoitteiden takia. Soveltamiselle tulee varata ehdotettua pidempi aika, vähintään 12 kuukautta.

Soveltamisalaan vain palveluntarjoajat, joille velvoitteet ylipäätään mahdollisia

Kun lainsäätäjät ehdottavat yhdenmukaisia velvoitteita kaikille välittäjäpalveluille, niiden tulee ottaa huomioon verkkoekosysteemin monimuotoisuus. Asetuksen soveltamisalaan halutaan ymmärrettävästi sisällyttää kaikki mahdolliset palveluntarjoajat, mutta internet-palveluntarjoajilla on todellisuudessa hyvin vaihtelevat tekniset mahdollisuudet puuttua CSAM:n tarjontaan. Asetuksen soveltamisalan tulee kattaa vain sellaiset internet-palveluntarjoajat, jotka ovat CSAM:n leviämisen tai groomingin kannalta relevantteja ja joilla on mahdollisuus siihen puuttua. Perinteisten, numeroihin perustuvien henkilöiden välisten viestintäpalvelujen tarjoajien osalta näin ei selvästikään ole, mikä on todettu jo Euroopan tietosuojavaltuutetun ja Euroopan tietosuojaneuvoston yhteisessä lausunnossa 4/2022. Lausunnossaan em. viranomaiset totesivat, että yksittäisten henkilöiden teksti- ja ääniviestinnän yleisluontoisen seurannan kielteinen vaikutus on niin vakava, ettei sitä voida perustella EU:n perusoikeuskirjan puitteissa (lausunnon kohdat 41, 56 ja 68–76).

Ehdotettujen velvoitteiden soveltaminen numeroihin perustuviin henkilöihin välisiin viestintäpalveluihin, kuten tekstiviesteihin tai puheluihin, on myös teknisesti mahdotonta. Palveluntarjoajilla ei ole pääsyä äänipuheluihin tai tekstiviesteihin niiden analysointia varten. Yleinen säilytysvelvollisuus olisi suhteeton ja ristiriidassa Euroopan unionin tuomioistuimen ratkaisukäytännön kanssa. Samoista syistä näihin viestintäpalveluihin ei tule myöskään kohdistaa asetuksen 3 artiklan riskinarviointia tai 4 artiklan riskien pienentämistä koskevia velvoitteita. Asetuksen 3 artiklan 2 kohdassa ja 4 artiklan 3 kohdassa vaaditaan numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajia toteuttamaan tarvittavat iän varmistus- ja arviointitoimenpiteet, jotta lapsikäyttäjät tunnistetaan luotettavasti. Numeroihin perustuvissa viestintäpalveluissa tällainen iästä riippuvainen seuranta tai reagointi ei kuitenkaan ole tehokasta tai edes mahdollista, koska numeroihin perustuvien viestintäpalveluiden tarjoajat eivät tee sopimusta alaikäisten kanssa. Tällöin ne eivät myöskään tarjoa lapsille palveluita, jotka edellyttäisivät iän vahvistamista. Tämä koskee erityisesti yrityspalveluja, joissa sopimuspuolet ovat tyypillisesti yrityksiä, jotka hankkivat viestintäpalveluja täysi-ikäisten työntekijöiden puolesta pääsääntöisesti vain liiketoimintatarkoituksiin. Numeroihin perustuvien henkilöiden välisten viestintäpalvelujen tarjoajat tulee jättää asetuksen soveltamisalan ulkopuolelle.

Soveltamisalan ulottamista palveluntarjoajiin, joilla ei ole teknistä mahdollisuutta toteuttaa asetuksen velvoitteita, on perusteltu käsittämättömästi muun muassa sillä, että asetus ottaisi huomioon tulevaisuuden kehityksen. Käytännössä tämä tarkoittaa sitä, että asetuksen soveltamisalaan sisällytettäisiin varmuuden vuoksi turhaan tuhansia yrityksiä eri puolilla Eurooppaa, jotta se kattaisi mahdollisesti tulevaisuudessa keksittävät uudet, CSAM:n leviämisen kannalta merkitykselliset palvelut. Perusteettoman soveltamisalan laajentamisen sijaan komission tulee säännöllisesti arvioida asetusta, jotta soveltamisalaa voidaan tarvittaessa muuttaa.

Säilytyspalvelun määritelmää tulee kaventaa

Asetusehdotuksen määritelmä säilytyspalvelulle viittaa digipalvelusäädöksen 2 artiklan f kohdan kolmannen luetelmakohdan määritelmään, jossa välittäjäpalvelulla tarkoitetaan muun muassa ”*säilytyspalvelua, joka käsittää palvelun vastaanottajan toimittamien tietojen tallentamisen palvelun vastaanottajan pyynnöstä*”. Tähän digipalvelusäädöksen määritelmään sisältyvät kuitenkin myös sellaiset IT-infrastruktuurin toimijat, mukaan lukien pilvi-infrastruktuuri, joiden palveluiden pohjalle palveluntarjoajien asiakkaat voivat rakentaa, käyttää ja kontrolloida omia, itse suunnittelemiaan pilvipohjaisia IT-järjestelmiään. Tällaisten

välittäjäpalveluiden asiakkailla on paras pääsy ja kyky vaikuttaa loppukäyttäjien sisältöön, ja siten ne pystyvät myös parhaiten toteuttamaan asetukseen ehdotettujen määräysten velvoitteita.

Asetuksen säilytyspalvelun määritelmää tulee kaventaa sen varmistamiseksi, että havaitsemis- tai poistamismääräyksiä ei kohdisteta syvemmällä internet-infrastruktuurissa sijaitseviin välittäjäpalveluihin. Asetuksessa tulee ottaa huomioon tekniset erot erilaisten palveluntarjoajien välillä. Sähköistä todistusaineistoa rikosasioissa koskevista eurooppalaisesta esittämismääräyksestä ja säilyttämismääräyksestä annettavan asetuksen (e-Evidence-asetus) 5 artiklan 6 kohdan mukaisesti jotkut toimijat ovat vain osa palveluntarjoajan yritykselle tai muulle yhteisölle kuin luonnollisille henkilöille tarjoamaa infrastruktuuria. Havaitsemis- ja poistamismääräysten tulee kohdistua vain palveluntarjoajiin, joilla on suora pääsy ja hallinta käyttäjiensä sisältöön.

Lisäksi B2B-palvelut tulee sulkea kokonaan soveltamisalan ulkopuolelle, koska niitä ei käytetä CSAM:in levittämiseen.

Groomingiin ja tuntemattomaan CSAM:iin kohdistuvat tunnistamismääräykset

Euroopan tietosuojavaltuutetun ja Euroopan tietosuojaneuvoston yhteisessä lausunnossa 4/2022 komissiota kehotetaan selkeyttämään edellytyksiä hyväksikäyttömateriaaliin ja lasten houkuttelemiseen (grooming) liittyvän tunnistamismääräyksen antamiselle. Tietosuojaneuvosto ja -valtuutettu ovat lausunnossaan erityisen huolissaan toimenpiteistä, joita suunnitellaan entuudestaan tuntemattoman CSAM:n ja groomingin havaitsemiseksi (lausunnon kohdat 68–76). Esimerkiksi tekoälyn kaltaisen teknologian käyttö viestinnän skannaamiseen aiheuttaa todennäköisesti virheitä ja loukkaa yksityisyyttä. Tunnistusohjelmistojen virhealttius johtaa väistämättä sellaisenkin sisällön valvontaan, joka ei ole CSAM:ia. Lisäksi on huomioitava, että olemassa olevan CSAM:in levittäminen on tyypillisesti kuva- tai videopohjaista, kun taas grooming on tyypillisemmin teksti- tai puhepohjaista. Tällaisen sisällön tunnistamiseen ja analysointiin tarvittavat tekniset työkalut ovat väistämättä hyvin erilaisia, mikä asettaa lisähaasteita tunnistamiselle ja teknologioiden käytölle.

Komissio on ilmoittanut olevansa tietoinen ongelmasta ja arvioinut vaikutustenarvioinnissaan nykyisten groomingia tunnistavien teknologioiden tarkkuudeksi 88 prosenttia. Arvioitu 12 prosentin virhemarginaali on kuitenkin aivan liikaa ja johtaisi siihen, että perustettava EU-keskus joutuisi käsittelemään lukuisia vääriä positiivisia tuloksia. Kun otetaan huomioon päivittäin internetissä jaettavan sisällön määrä, kaikki muu paitsi täydellinen tarkkuus tarkoittaisi, että suuri määrä täydessä yhteisymmärryksessä täysi-ikäisten nuorten aikuisten kesken jaettua intiimiä sisältöä merkittäisiin CSAM:ksi. Lisäksi toimenpiteet, joissa viranomaisille annetaan yleinen oikeus päästä käsiksi kaikkeen sisältöön groomingin havaitsemiseksi estävät, että Euroopan unionin perusoikeuskirjan 7 ja 8 artikloissa taatut oikeudet vapauteen ja turvallisuuteen sekä yksityis- ja perhe-elämän kunnioittamiseen toteutuvat.

Tunnettuun CSAM:n kohdistuvat tunnistamismääräykset ovat ymmärrettäviä, mutta tuntemattoman CSAM:n havaitsemisen tulisi olla vapaaehtoista, ilman palveluntarjoajiin kohdistuvaa vastuuta.

Estomääräyksiin tehtävä lukuisia korjauksia

Verkkosivuestot eivät tarjoa konkreettista ratkaisua ongelmaan, ja ne on helppo kiertää

Verkkosivujen estäminen ei ole tehokkain keino torjua CSAM:ia. Estomääräykset vain siirtävät laittoman sisällön pois suuren yleisön näkyviltä. Toimet pitää sen sijaan kohdistaa laittoman sisällön lähteelle. Laitonta sisältöä aktiivisesti etsivillä henkilöillä on useita tapoja päästä siihen käsiksi, koska kaikki estotoimenpiteet voidaan kiertää. Domain-nimet ja palvelimet ovat helposti vaihdettavissa, minkä lisäksi esimerkiksi virtuaaliset erillisverkot (VPN, virtual private network) ja muut vastaavat palvelut ovat helppokäyttöisiä ja kaikkien tiedossa olevia tapoja kiertää estot.

EU:n toimielinten virkamiehet ovat todenneet, että estomääräykset ovat viimesijainen keino CSAM:n torjumiseksi. Tämä ei kuitenkaan käy mitenkään ilmi asetusehdotuksen estomääräyksiä koskevan 16 artiklan tekstistä, joten artiklaan tulee lisätä selkeästi estomääräysten viimesijaisuus. Asetusehdotuksen johdantokappaleesta 32 voidaan tulkita, että ennen estomääräyksen antamista viranomaisten on täytynyt pyytää säilytyspalvelun tarjoajaa poistamaan tai estämään pääsy sisältöön, tarvittaessa yhteistyössä sen kolmannen maan toimivaltaisten viranomaisten kanssa, johon säilytyspalveluntarjoaja on sijoittautunut. Tämä toissijaisuusperiaate tulee selkeästi ilmaista asetustekstissä.

URL-osoitteiden esto on erityisen haitallinen tietosuojan ja verkkoturvallisuuden kannalta

Asetuksessa edellytettyjen tiettyjen URL-osoitteiden estäminen vaatii palveluntarjoajalta yksityiskohtaista analyysiä kaikista verkkojensa kautta lähetetyistä datapaketeista (DPI, Deep Packet Inspection). Asetusehdotuksen 16 artiklan 2 kohdan b alakohdan vaatimus toimittaa koordinoivalle viranomaiselle "*tiedot, jotka koskevat erityisesti käyttäjien pääsyä tai yritystä päästä URL-osoitteiden osoittamaan lapsiin kohdistuvaa seksuaaliväkivaltaa todistavaan kuvamateriaaliin*" yhdessä saman artiklan 4 kohdan a alakohdan muotoilun "*näyttöä siitä, että palvelua on viimeisten 12 kuukauden aikana käytetty huomattavassa määrin URL-osoitteiden osoittamaan lapsiin kohdistuvaa seksuaaliväkivaltaa todistavaan kuvamateriaaliin pääsyyn tai pääsyn yrittämiseen kyseiseen materiaaliin*" kanssa vaikuttaa edellyttävän, että palveluntarjoajien on arvioitava, ovatko heidän asiakkaansa yrittäneet päästä käsiksi johonkin luetteloitujen URL-osoitteiden osoittamaan CSAM:iin tai käyttäneet sitä. Tämä onnistuu ainoastaan DPI:n avulla.

Tällaisia nyt vaadittavia toimia on aiemmin pidetty laittomina sekä verkkoneutraliteetin että tietosuojan vuoksi. Lisäksi suurin osa tietoliikenteestä on nykyään suojattu HTTPS-protokollalla, joten palveluntarjoajien tulisi purkaa datapakettien suojaus väliintulohyökkäyksen (man-in-the-middle attack) avulla, mikä olisi selkeästi Euroopan unionin tuomioistuimen ratkaisukäytännön sekä NIS 2.0 -direktiivin velvoitteiden vastaista. Myös Euroopan tietosuojavaltuutettu ja Euroopan tietosuojaneuvosto pitivät yhteisessä lausunnossaan 4/2022 tällaisia toimia suhteettomina (lausunnon kohta 80).

Euroopan unionin tuomioistuimen vakiintuneen ratkaisukäytännön mukaisesti palveluntarjoajan tulee saada itse määrittää "*toimenpiteet, jotka vastaavat parhaiten sen käytettävissä olevia resursseja ja kapasiteettia ja jotka ovat yhteensoveltuvia sellaisten muiden velvollisuuksien ja haasteiden kanssa, joista sen on huolehdittava harjoittaessaan toimintaansa*" (kts. C-314/12 UPC Telekabel, kappale 52). Jonkun tietyn konkreettisen toimenpiteen, kuten esimerkiksi URL-eston, määrääminen loukkaa palveluntarjoajien elinkeinonvapautta.

Määräysten suhteellisuus ja suojatoimet edellyttävät tarkennuksia

Asetusehdotuksen 16 artiklan 5 kohdan a alakohta edellyttää, että viranomaiset määrittävät ”*tehokkaat ja oikeasuhteiset rajoitukset ja suojatoimet*” silloin, kun ne pyytävät estomääräyksen antamista tai antavat sellaisen, jotta estomääräyksen kielteiset seuraukset rajoittuvat siihen, mikä on ehdottoman välttämätöntä. Tältä osin on tärkeää määrittää, mihin rajoituksiin ja suojatoimiin viitataan. Vastaavasti 16 artiklan 7 kohdan lopussa todetaan, että ”[*t]ällaisiin pyyntöihin sovelletaan tämän jakson säännöksiä soveltuvin osin*”. Kohta on epäselvä ja tulee poistaa.

Oikeussuojakeinoja, tiedottamista ja estomääräyksistä raportointia koskevan 18 artiklan 3 kohta edellyttää, että palveluntarjoaja perustaa valitusmekanismin, jotta käyttäjät voivat toimittaa sille kanteluja estovelvoitteita koskevan asetuksen 5 jakson mukaisten velvoitteiden väitetyistä rikkomisista. Valitukset artiklojen 16–18 väitetyistä rikkomisista tulee asetuksen johdonmukaisen soveltamisen vuoksi tehdä toimivaltaiselle viranomaiselle eikä internetyhteyspalvelun tarjoajille.

Asetustekstissä tulee korostaa paremmin määräysten suhteellisuutta. Lisäksi tulee varmistaa, että yrityksillä on aina oikeus täysimääräiseen korvaukseen kaikista viranomaisten avustamisesta aiheutuneista kustannuksista, myös henkilötyön osalta.

Raportointia usealle eri taholle vältettävä

Kun otetaan huomioon eri yritysten, kansallisten tai kansainvälisten, toiminnan laajuus sekä se, että lapsiin kohdistuvaan seksuaaliväkivaltaan liittyvät rikokset voivat vaikuttaa yhdessä tai useammassa maassa, asetustekstissä tulee antaa internet-palveluntarjoajille mahdollisuus valita, ilmoittavatko ne havainnoistaan EU-keskukselle vai paikallisille viranomaisille sen mukaan, mikä on niille ja niiden liiketoiminnalle luontevinta. Edelleen kansallisilla viranomaisilla on oltava mahdollisuus raportoida EU-keskukselle, mikä lievittäisi eri viranomaisten taakkaa. Monissa maissa on tällä hetkellä vakiintuneet ja toimivat raportointijärjestelmät, eikä ehdotettu menettely vaarantaisi kansallisesti toimivien yritysten käytäntöjä. Vastaavasti monikansallisilla yrityksillä olisi mahdollisuus raportoida vain yhdelle viranomaiselle usean eri viranomaisen sijaan.

Yhdysvaltojen palveluntarjoajien raportointivelvollisuutta koskevan lainsäädännön perusteella (Title 18, osa 1, kappale 110, osio § 2258A) kaikilla Yhdysvalloissa toimivilla palveluntarjoajilla on velvollisuus ilmoittaa sekä ilmeisistä lasten hyväksikäyttöä koskevista rikkomuksista että niiden uhasta Kansallisen kadonneiden ja hyväksikäytettyjen lasten keskuksen (National Center for Missing & Exploited Children, NCMEC) CyberTipline-vinkkipalveluun. Asetuksessa tulee selventää, miten palveluntarjoajat voivat välttää kaksinkertaisen raportoinnin EU-keskukselle, NCMEC:lle ja paikallisille lainvalvontaviranomaisille. Mainittujen viranomaisten välinen yhteistyö on olennaisen tärkeää tietokantojen ajan tasalla pitämiseksi sekä CSAM:n vastaisten toimien pirstoutumisen estämiseksi.

Palveluntarjoajille vastuuvapauden suojaama mahdollisuus kehittää ja ottaa käyttöön uusia teknologioita CSAM:n torjumiseen

On hyvä, että perustettava EU-keskus tarjoaa työkaluja maksutta niitä tarvitseville. On kuitenkin huomioitava, ettei integrointi olemassa olevaan tekniseen ympäristöön ole aina mahdollista, erityisesti PK-yrityksille, ja että NIS 2.0 -direktiivi estää palveluntarjoajia sallimasta ulkoista teknologiaa infrastruktuuriinsa. Asetukseen ehdotettujen velvoitteiden täyttäminen edellyttää joka tapauksessa säännöllisiä, merkittäviä investointeja sekä uuteen teknologiaan että henkilötyöhön. Näitä suurin osa PK-yrityksistä ei välttämättä

pysty toteuttamaan. Sääntelyssä pelkästään verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan tunnistamiseen käytettyjen teknologioiden virhetasoihin keskittyminen on harhaanjohtavaa ja todennäköisesti rajoittaisi palveluntarjoajien toimintaa sekä kykyä innovoida uutta. Teknologioiden virhetasot riippuvat useista tekijöistä, ja on tärkeää erottaa toisistaan tunnetun CSAM:in, tuntemattoman CSAM:in ja groomingin tunnistamiseen käytetyt työkalut.

Asetukseen tulee lisätä digipalvelusäädöksen 6 artiklan mukainen mahdollisuus suorittaa vilpittömässä mielessä ja huolellisesti vapaaehtoisia, oma-aloitteisia tutkimuksia tai toteuttaa muita toimenpiteitä, joiden tarkoituksena on havaita, tunnistaa ja poistaa laitonta sisältöä tai estää pääsy siihen.

Ehdotettu asetus korvaisi tällä hetkellä voimassa olevan väliaikaisen asetuksen, minkä jälkeen palveluntarjoajat eivät voisi enää vapaaehtoisesti ehkäistä CSAM:n levittämistä alustoillaan siihen suunniteltujen tekniikoiden tai työkalujen avulla. Pakollisten havaitsemisvelvoitteiden tulisi toimia vapaaehtoisuuteen perustuvan havaitsemisen rinnalla.