



**Euroopan
tietosuojaneuvoston ja
Euroopan
tietosuojavaltuutetun
yhteinen lausunto 4/2022
Euroopan parlamentin ja
neuvoston ehdotuksesta
asetukseksi lapsiin
kohdistuvan
seksuaaliväkivallan ehkäisyä
ja torjuntaa koskevista
säännöistä**

Annettu 28. heinäkuuta 2022

Translations proofread by EDPB Members.

This language version has not yet been proofread.

SISÄLLYS

1.	Taustaa.....	7
2.	Lausunnon soveltamisala.....	9
3.	Yleisiä huomioita oikeuksista viestinnän luottamuksellisuuteen ja henkilötietojen suojaan	9
4.	Erityisiä huomioita.....	12
4.1	Suhde voimassa olevaan lainsäädäntöön	12
4.1.1	Suhde yleiseen tietosuojasetukseen ja sähköisen viestinnän tietosuojadirektiiviin .	12
4.1.2	Suhde asetukseen (EU) 2021/1232 ja vaikutus verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan vapaaehtoiseen tunnistamiseen	12
4.2	Yleisen tietosuojasetuksen mukainen lakisääteinen perusta	13
4.3	Riskinarviointi ja lieventämisvelvoitteet.....	13
4.4	Tunnistamismääräysten antamisen ehdot.....	15
4.5	Suunniteltujen toimenpiteiden tarpeellisuuden ja oikeasuhteisuuden analyysi	17
4.5.1	Tunnistamisen tehokkuus.....	18
4.5.2	Ei vähemmän yksityisyyttä loukkaava toimenpide	19
4.5.3	Oikeasuhteisuus suppeimmassa merkityksessä.....	20
4.5.4	Lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevan kuvamateriaalin tunnistaminen	22
4.5.5	Lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan muun kuin aiemmin tiedossa olevan kuvamateriaalin tunnistaminen	22
4.5.6	Lapsen houkuttelun seksuaalisiin tarkoituksiin (ns. grooming) tunnistaminen	23
4.5.7	Päätelmä suunniteltujen toimenpiteiden tarpeellisuudesta ja oikeasuhteisuudesta ..	24
4.6	Ilmoitusvelvoitteet	25
4.7	Poistamis- ja estovelvoitteet.....	25
4.8	Asiaankuuluvat teknologiat ja takeet	26
4.8.1	Sisäänrakennettu ja oletusarvoinen tietosuoja	26
4.8.2	Teknologioiden luotettavuus	26
4.8.3	Ääniviestinnän seulominen.....	28
4.8.4	län tarkistaminen.....	28
4.9	Tietojen säilyttäminen	29
4.10	Vaikutus salaukseen	29
4.11	Valvonta, täytäntöönpano ja yhteistyö	31
4.11.1	Yleisen tietosuojasetuksen mukainen kansallisten valvontaviranomaisten rooli	31

4.11.2	Euroopan tietosuojaneuvoston tehtävä.....	32
4.11.3	Lapsiin kohdistuvan seksuaaliväkivallan EU-keskuksen rooli	33
4.11.4	Europolin rooli.....	35
5.	Päätelmät	40

Tiivistelmä

Euroopan komissio antoi 11. toukokuuta 2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä.

Ehdotuksessa säilytyspalvelujen, henkilöiden välisten viestintäpalvelujen ja muiden palvelujen tarjoajille asetettaisiin ehdollisia velvoitteita, jotka koskevat lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevan ja uuden kuvamateriaalin sekä seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamista, siitä ilmoittamista, sen poistamista ja sen estämistä. Ehdotuksessa säädetään myös EU:n uuden erillisviraston, jäljempänä 'EU-keskus', ja lapsiin kohdistuvaan seksuaaliväkivaltaan liittyviä kysymyksiä koordinoivien kansallisten viranomaisten verkoston perustamisesta, jotta ehdotettu asetusta voidaan panna täytäntöön. Kuten ehdotuksen perusteluissa tunnustetaan, ehdotukseen sisältyvät toimenpiteet vaikuttaisivat kyseessä olevien palvelujen käyttäjien perusoikeuksien toteuttamiseen.

Lapsiin kohdistuva seksuaaliväkivalta on erityisen vakava ja katala rikos. Unioni on tunnustanut sen tehokasta torjumista koskevan tavoitteen yleisen edun mukaiseksi tavoitteeksi, jolla pyritään suojelemaan uhrien oikeuksia ja vapauksia. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu muistuttavat kuitenkin, että kaikissa perusoikeuksien rajoituksissa, kuten ehdotuksessa esitetyissä, on noudatettava Euroopan unionin perusoikeuskirjan 52 artiklan 1 kohdassa asetettuja vaatimuksia.

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu korostavat, että ehdotus aiheuttaa vakavaa huolta siitä, ovatko suunniteltu puuttuminen ja perusoikeuksien suojelun rajoitukset oikeasuhteisia yksityisyyden ja henkilötietojen suojan kannalta. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat tämän osalta, että menettelytakeilla ei voida koskaan täysin korvata aineellisia takeita. Monimutkaisella järjestelmällä, jossa riskinarviointi- ja -hallintatoimenpiteet laajenevat tunnistamismääräyksiksi, ei voida korvata aineellisilta velvoitteilta vaadittua selkeyttä.

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että ehdotuksen keskeiset osatekijät eivät ole selkeitä. Tämä koskee muun muassa "merkittävän riskin" käsitettä. Lisäksi näiden takeiden soveltamisesta vastaavilla tahoilla on erittäin laaja harkintavaltaa, joka aiheuttaa oikeudellista epävarmuutta siitä, miten kussakin yksittäisessä tapauksessa varmistetaan kyseessä olevien oikeuksien tasapaino. Nämä tahot vaihtelevat yksityisistä toimijoista hallinto- ja/tai oikeusviranomaisiin. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu korostavat, että kun lainsäätävä sallii erityisen vakavat puuttumiset perusoikeuksiin, sen on taattava oikeusvarmuus siitä, milloin ja missä puuttumiset sallitaan. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu tunnustavat, että lainsäädäntö ei saa olla liian ohjailevaa ja että sen käytännön soveltamiseen on jätettävä jonkin verran joustavuutta. Ne katsovat kuitenkin, että ehdotuksessa jää liian paljon mahdollisuuksia mahdolliseen väärinkäyttöön, koska selkeitä aineellisia normeja ei ole.

Suunniteltujen tunnistamistoimenpiteiden tarpeellisuuden ja oikeasuhteisuuden osalta Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat erityisen huolissaan toimenpiteistä, joita suunnitellaan muun kuin tiedossa olevan lapsiin kohdistuvan seksuaaliväkivaltaa todistavan kuvamateriaalin (CSAM) ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun (ns. grooming) osalta henkilöiden välisissä viestintäpalveluissa. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että näillä toimenpiteillä toteutettava puuttuminen ylittää sen, mikä on tarpeen ja oikeasuhteista niissä käytettäviin teknologioihin liittyvän yksityisyyden loukkaamisen, todennäköisyyteen perustuvan luonteen ja virhetasojen vuoksi. Lisäksi toimenpiteet, joilla viranomaiset pääsevät yleisesti käyttämään viestinnän

sisältöä tunnistaakseen seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun, vaikuttavat todennäköisemmin perusoikeuskirjan 7 ja 8 artiklassa tunnustettujen oikeuksien keskeiseen sisältöön. Siksi seksuaalisiin tarkoituksiin tapahtuvaan lapsen houkutteluun liittyvät asiaankuuluvat säännökset olisi poistettava ehdotuksesta. Ehdotuksen soveltamisalasta ei myöskään suljeta pois ääniviestinnän seulontaa. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että ääniviestinnän seulonta on erityisen yksityisyyttä loukkaavaa ja että se on siksi jätettävä pois ehdotetussa asetuksessa esitetystä tunnistamisvelvoitteiden soveltamisalasta. Tämä koskee sekä ääniviestejä että suoraa viestintää.

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ilmaisevat epäilynsä myös estotoimenpiteiden tehokkuudesta ja katsovat, että olisi kohtuutonta vaatia internetpalvelujen tarjoajia avaamaan verkkoviestien salausta, jotta CSAM-materiaalia koskevat viestit voitaisiin estää.

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat myös, että salausteknologiat myötävaikuttavat perustavanlaatuisesti yksityiselämän ja viestinnän luottamuksellisuuden kunnioittamiseen, sananvapauteen sekä innovointiin ja digitaalitalouden kasvuun. Digitaalitalous onkin riippuvaista näiden teknologioiden tarjoamasta korkeatasoisesta luottamuksesta ja luottamuksellisuudesta. Ehdotuksen johdanto-osan 26 kappaleessa sekä tunnistamisteknologioiden että viestinnän luottamuksellisuutta suojaavien teknisten toimenpiteiden, kuten salauksen, valintaan liitetään edellytys siitä, että valittujen teknologioiden on täytettävä asetetun ehdotuksen vaatimukset. Tunnistamisen on siis oltava mahdollista niiden avulla. Tämä tukee ehdotuksen 8 artiklan 3 kohdasta ja 10 artiklan 2 kohdasta saatua käsitystä siitä, että palveluntarjoaja ei voi kieltäytyä tunnistamismääräyksen täytäntöönpanosta siksi, että se olisi teknisesti mahdotonta. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että suojattuja ja yksityisiä viestintäkanavia ja niiden väärinkäytön torjuntaa koskevien yhteiskunnallisten tarpeiden välistä tasapainoa olisi parannettava. Ehdotuksessa olisi todettava selkeästi, että mitään ehdotetussa asetuksessa ei pitäisi tulkita niin, että sillä kiellettäisiin salausta tai heikennettäisiin sitä.

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suhtautuvat myönteisesti ehdotuksen toteutumukseen siitä, että ehdotus ei vaikuta tietosuojaviranomaisten yleisen tietosuoja-asetuksen mukaisiin valtuuksiin ja toimivaltaan. Ne katsovat kuitenkin, että koordinoivien viranomaisten ja tietosuojaviranomaisten tehtävien välistä suhdetta olisi säänneltävä paremmin. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu arvostavat tämän osalta roolia, joka ehdotuksessa annetaan tietosuojaneuvostolle vaatimalla sen osallistumista ehdotuksen käytännön täytäntöönpanoon. Tietosuojaneuvoston olisi erityisesti annettava lausunto teknologioista, joita EU-keskus antaisi saataville tunnistamismääräysten täytäntöönpanoa varten. Olisi kuitenkin selvennettävä, mikä tarkoitus lausunnolla prosessissa olisi ja miten EU-keskus toimisi saatuaan tietosuojaneuvoston lausunnon.

Lopuksi Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu panevat merkille, että ehdotuksessa säädetään EU-keskuksen ja Europolin tiiviistä yhteistyöstä, jossa ne antavat toisilleen ”mahdollisimman laajan pääsyn asiaankuuluviin [...] tietojärjestelmiin”. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu tukevat periaatteessa näiden kahden viraston yhteistyötä, mutta koska EU-keskus ei ole lainvalvontaviranomainen, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu tekevät kuitenkin useita suosituksia asiaankuuluvien säännösten parantamiseksi. Suositukset koskevat muun muassa sitä, että EU-keskuksen ja Europolin välillä siirretään henkilötietoja vain tapauskohtaisesti, huolellisesti arvioidun pyynnön perusteella ja suojatun tietojenvaihtotyökalun, kuten SIENA-verkon, kautta.

Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu, jotka

ottavat huomioon yksilöiden suojelusta unionin toimielinten, elinten ja laitosten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta sekä asetuksen (EY) N:o 45/2001 ja päätöksen N:o 1247/2002/EY kumoamisesta 23 päivänä lokakuuta 2018 annetun asetuksen 2018/1725 42 artiklan 2 kohdan, jäljempänä 'unionin tietosuoja-asetus'¹,

ottavat huomioon ETA-sopimuksen sekä erityisesti sen liitteen XI ja pöytäkirjan 37, sellaisina kuin ne ovat muutettuina 6 päivänä heinäkuuta 2018 annetulla ETA:n sekakomitean päätöksellä N:o 154/2018²,

ottavat huomioon Euroopan komission pyynnön Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteisestä lausunnosta, joka koskee 12 päivänä toukokuuta 2022 annettua ehdotusta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä³,

ANTAVAT SEURAAVAN YHTEISEN LAUSUNNON:

1. TAUSTAA

1. Euroopan komissio antoi 11. toukokuuta 2022 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä, jäljempänä 'ehdotus' tai 'ehdotettuasetus'⁴.
2. Ehdotus annettiin 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 annetun asetuksen (EU) 2021/1232, jäljempänä 'väliaikainen asetust'⁵, hyväksymisen jälkeen. Väliaikaisessa asetuksessa ei vaadita asiaankuuluvia palveluntarjoajia ottamaan käyttöön toimenpiteitä lapsiin kohdistuvan seksuaaliväkivaltaa todistavan kuvamateriaalin (jäljempänä 'CSAM-materiaali') (esim. kuvien ja videoiden) ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun (ns. grooming) tunnistamiseksi

¹ EUVL L 295, 21.11.2018, s. 39.

² Viittauksilla 'jäsenvaltioihin' tarkoitetaan koko tässä asiakirjassa ETA:n jäsenvaltioita.

³ Ehdotus Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä, COM(2022) 209 final.

⁴ Ks. edellinen alaviite

⁵ Euroopan parlamentin ja neuvoston asetust (EU) 2021/1232, annettu 14 päivänä heinäkuuta 2021, 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 EUVL [2021] L 274/41.

niiden palveluissa, mutta palveluntarjoajat voivat tehdä niin vapaaehtoisesti kyseisessä asetuksessa esitettyjen ehtojen mukaisesti⁶.

3. Ehdotus koostuu kahdesta pääosasta. Ensinnäkin siinä asetetaan säilytyspalvelujen, henkilöiden välisten viestintäpalvelujen ja muiden palvelujen tarjoajille ehdollisia velvoitteita, jotka koskevat lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevan ja uuden kuvamateriaalin sekä seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamista, siitä ilmoittamista, sen poistamista ja sen estämistä. Toiseksi ehdotuksessa säädetään EU:n uuden erillisviraston, jäljempänä 'lapsiin kohdistuvan seksuaaliväkivallan EU-torjuntakeskus' tai 'EU-keskus', ja lapsiin kohdistuvaan seksuaaliväkivaltaan liittyviä kysymyksiä koordinoivien kansallisten viranomaisten verkoston perustamisesta, jotta ehdotettu asetetus voidaan panna täytäntöön⁷.
4. Kuten ehdotuksen perusteluissa tunnustetaan, ehdotukseen sisältyvät toimenpiteet vaikuttaisivat kyseessä olevien palvelujen käyttäjien perusoikeuksien toteuttamiseen. Näihin oikeuksiin kuuluvat erityisesti perusoikeudet, jotka liittyvät yksityisyyden kunnioittamiseen (mukaan lukien viestinnän luottamuksellisuus osana laajempaa oikeutta yksityis- ja perhe-elämän kunnioittamiseen), henkilötietojen suojaan sekä sananvapauteen ja tiedonvälityksen vapauteen⁸.
5. Ehdotettujen toimenpiteiden on määrä perustua voimassa olevaan EU:n tietosuojaa ja yksityisyydensuojaa koskevaan lainsäädäntöön ja jossain määrin täydentää sitä. Tämän osalta perusteluissa todetaan seuraavaa:

”Ehdotus perustuu yleiseen tietosuojasetukseen (GDPR). Käytännössä palveluntarjoajat vetoavat usein erilaisiin yleisessä tietosuojasetuksessa säädettyihin käsittelyperusteisiin sellaisten henkilötietojen käsittelyssä, jotka liittyvät verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan vapaaehtoiseen tunnistamiseen ja siitä ilmoittamiseen. Ehdotuksessa esitetään kohdennettujen tunnistamismääräysten järjestelmä ja määrittää tunnistamisen edellytykset, mikä parantaa kyseisten toimien oikeusvarmuutta. Henkilötietojen käsittelyyn liittyvien pakollisten tunnistamistoimien osalta ehdotuksessa ja erityisesti sen perusteella annetuissa tunnistamismääräyksissä vahvistetaan näin ollen tällaisen käsittelyn perusteet, joihin viitataan yleisen tietosuojasetuksen 6 artiklan 1 kohdan c alakohdassa. Siinä säädetään henkilötietojen käsittelystä, joka on tarpeen rekisterinpitäjälle unionin oikeuden tai kansallisen lainsäädännön nojalla kuuluvan lakisääteisen veloitteen noudattamiseksi.

Ehdotus kattaa muun muassa palveluntarjoajat, jotka tarjoavat henkilöiden välisiä sähköisiä viestintäpalveluja ja joihin näin ollen sovelletaan sähköistä kaupankäyntiä koskevan direktiivin ja sen parhaillaan neuvoteltavana olevan tarkistusehdotuksen kansallisia täytäntöönpanosäännöksiä. Ehdotuksessa esitetyt toimenpiteet rajoittavat joiltakin osin mainitun direktiivin asiaa koskevien säännösten mukaisten oikeuksien ja velvoitteiden soveltamisalaa, erityisesti sellaisten toimien osalta, jotka ovat ehdottoman välttämättömiä tunnistamismääräysten täytäntöönpanemiseksi. Tältä osin ehdotus edellyttää mainitun direktiivin 15 artiklan 1 kohdan analogista soveltamista.”⁹

⁶ Ks. myös Euroopan tietosuojavaltuutetun lausunto 7/2020, joka koskee ehdotusta tilapäisistä poikkeuksista direktiivistä 2002/58/EY verkossa tapahtuvan lasten seksuaalisen hyväksikäytön torjumiseksi (10.11.2020).

⁷ COM(2022)209 final, s. 17.

⁸ COM(2022)209 final, s. 12.

⁹ COM(2022)209 final, s. 4–5.

6. Koska suunnitellut perusoikeuksiin puuttumiset ovat vakavia, ehdotus on erityisen tärkeä ihmisten oikeuksien ja vapauksien suojelulle henkilötietojen käsittelyssä. Siksi komissio päätti 12. toukokuuta 2022 kuulla Euroopan tietosuojaneuvostoa ja Euroopan tietosuojavaltuutettua EU:n tietosuoja-asetuksen 42 artiklan 2 kohdan mukaisesti.

2. LAUSUNNON SOVELTAMISALA

7. Tässä yhteisessä lausunnossa esitetään Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteisiä näkemyksiä ehdotuksesta. Se rajoitetaan yksityisyyden ja henkilötietojen suojaan liittyviin ehdotuksen näkökohtiin. Yhteisessä lausunnossa tuodaan erityisesti esiin alueita, joilla ehdotuksella ei pystytä varmistamaan yksityisyyttä ja tietosuoja koskevien perusoikeuksien riittävää suojaa, tai vaaditaan yhdenmukaistamaan ehdotusta lisää yksityisyyden ja henkilötietojen suoja koskevan EU:n oikeudellisen kehyksen kanssa.
8. Kuten tässä lausunnossa jäljempänä selitetään, ehdotus herättää vakavaa huolta siitä, ovatko suunnitellut puuttumiset ja perusoikeuksien suojelun rajoitukset tarpeellisia ja oikeasuhteisia yksityisyyden ja henkilötietojen suojan kannalta. Yhteisen lausunnon tarkoituksena ei ole kuitenkaan esittää tyhjentävää luettelo kaikista kysymyksistä, joita ehdotus herättää yksityisyydestä ja tietosuojasta, eikä antaa nimenomaisia ehdotuksia ehdotuksen sanamuodon parantamiseksi. Sen sijaan yhteisessä lausunnossa esitetään yleisellä tasolla huomautuksia tärkeimmistä ehdotuksen herättämistä kysymyksistä, joita Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat havainneet. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu voivat kuitenkin edelleen antaa molemmille lainsäätäjille lisähuomautuksia ja -suosituksia ehdotusta koskevan lainsäädäntöprosessin aikana.

3. YLEISIÄ HUOMIOITA OIKEUKSISTA VIESTINNÄN LUOTTAMUKSELLISUUTEEN JA HENKILÖTIETOJEN SUOJAAN

9. Viestinnän luottamuksellisuus on olennainen osa Euroopan unionin perusoikeuskirjan, jäljempänä 'perusoikeuskirja', 7 artiklassa tunnustettua perusoikeutta yksityis- ja perhe-elämän kunnioittamiseen¹⁰. Lisäksi perusoikeuskirjan 8 artiklassa tunnustetaan perusoikeus henkilötietojen suojaan. Myös oikeudet viestinnän luottamuksellisuuteen ja oikeus yksityis- ja perhe-elämän taataan Euroopan ihmisoikeussopimuksen 8 artiklassa, ja ne ovat osa jäsenvaltioiden yhteisiä perustuslaillisia perinteitä¹¹.
10. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu muistuttavat, että perusoikeuskirjan 7 ja 8 artiklassa tunnustetut oikeudet eivät ole ehdottomia, vaan ne on suhteutettava siihen tehtävään, joka niillä on yhteiskunnassa¹². Lapsiin kohdistuva seksuaaliväkivalta on erityisen vakava ja

¹⁰ Ks. esim. Euroopan tietosuojaneuvoston lausunto sähköisen viestinnän tietosuoja-asetuksen tarkistuksesta ja sen vaikutuksesta henkilöiden yksityisyyden suojaan ja heidän viestintänsä luottamuksellisuuteen (25.5.2018).

¹¹ Lähes kaikkien Euroopan maiden perustuslait sisältävät viestinnän luottamuksellisuuden suoja koskevan oikeuden. Ks. esim. Italian tasavallan perustuslain 15 §, Saksan liittotasavallan perustuslain 10 §, Belgian perustuslain 22 § ja Alankomaiden kuningaskunnan perustuslain 13 §.

¹² Ks. mm. EUT:n tuomio asiassa C-311/18, *Facebook Ireland ja Schrems*, 172 kohta oikeuskäytäntöviittauksineen. Ks. myös yleisen tietosuoja-asetuksen johdanto-osan 4 kappale.

katala rikos. Unioni on tunnustanut sen tehokasta torjumista koskevan tavoitteen yleisen edun mukaiseksi tavoitteeksi, jolla pyritään suojelemaan uhrien oikeuksia ja vapauksia. Siltä osin kuin on kyse erityisesti sellaisten rikosten, joiden uhreja ovat etenkin alaikäiset ja muut heikossa asemassa olevat henkilöt, tehokkaasta torjunnasta, Euroopan unionin tuomioistuin (EUT) on huomauttanut, että perusoikeuskirjan 7 artiklasta voi seurata viranomaisia koskevia toimintavelvollisuuksia sellaisten oikeudellisten toimenpiteiden toteuttamiseksi, joilla suojataan yksityis- ja perhe-elämää, kotia ja viestejä. Tällaiset velvollisuudet voivat perustua myös perusoikeuskirjan 3 ja 4 artiklaan jokaisen ruumiillisen ja henkisen koskemattomuuden suojaamisen osalta sekä kidutuksen sekä epäinhimillisen tai halventavan kohtelun kiellon osalta.¹³

11. Kaikissa perusoikeuskirjalla tunnustettujen oikeuksien rajoituksissa, kuten ehdotuksessa suunnitelluissa¹⁴, on kuitenkin noudatettava Euroopan unionin perusoikeuskirjan 52 artiklan 1 kohdassa asetettuja vaatimuksia. Kaikissa viestinnän luottamuksellisuutta koskeviin oikeuksiin ja yksityis- ja perhe-elämää koskevaan oikeuteen puuttumisessa on ennen kaikkea noudatettava kyseisten oikeuksien olennaista sisältöä¹⁵. Oikeuden olennaiseen sisältöön vaikutetaan, jos oikeuden perussisältö tehdään tyhjäksi ja henkilö ei voi käyttää oikeutta¹⁶. Oikeuteen ei saa puuttua tavoitellun päämäärän kannalta suhteettomasti eikä tavalla, jota ei voida hyväksyä ja jolla loukattaisiin näin suojatun oikeuden keskeistä sisältöä¹⁷. Tämä tarkoittaa, että vaikka perusoikeus, kuten oikeus viestinnän luottamuksellisuuteen ja oikeus henkilötietojen suojaan, ei olisi luonteeltaan ehdoton, siinä on joitakin olennaisia osia, joita ei voida rajoittaa.
12. Euroopan unionin tuomioistuin on useaan otteeseen soveltanut niin sanottua oikeuden olennaisen sisällön testausta sähköisen viestinnän yksityisyyden alalla. Asiassa *Tele2 Sverige ja Watson* tuomioistuin totesi, että lainsäädännöllä, jossa ei sallita viestin sisällön säilyttämistä, ei niin ollen vahingoiteta yksityisyyttä ja henkilötietojen suojaa koskevien oikeuksien keskeistä sisältöä¹⁸. Asiassa *Schrems* tuomioistuin totesi, että säännöstöstä, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön, on erityisesti katsottava, että sillä loukataan yksityiselämän kunnioitusta koskevan perusoikeuden, sellaisena kuin se taataan perusoikeuskirjan 7 artiklassa, keskeistä sisältöä¹⁹. Asiassa *Digital Rights Ireland ja Seitlinger ym.* tuomioistuin totesi, että vaikka tietojen säilyttäminen, johon direktiivissä 2006/24 velvoitetaan, merkitsee erityisen vakavaa puuttumista yksityisyyttä koskevaan perusoikeuteen ja muihin perusoikeuskirjan 7 artiklassa tarkoitettuihin oikeuksiin, se ei ole omiaan aiheuttamaan haittaa mainittujen oikeuksien keskeiselle sisällölle, koska direktiivissä ei sallita tiedon saamista sähköisen viestinnän sisällöstä sellaisenaan²⁰. Tästä oikeuskäytännöstä voidaan päätellä, että toimenpiteet, joiden nojalla viranomaiset pääsevät yleisesti viestinnän sisältöön, vaikuttavat todennäköisemmin perusoikeuskirjan 7 ja 8 artiklassa tunnustettujen oikeuksien keskeiseen sisältöön. Nämä näkökohdat ovat yhtä merkityksellisiä myös

¹³ EUT, yhdistetyt asiat C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net ym.*, 126–128 kohta. Ks. myös Euroopan tietosuojavaltuutetun lausunto 7/2020, joka koskee ehdotusta tilapäisistä poikkeuksista direktiivistä 2002/58/EY verkossa tapahtuvan lasten seksuaalisen hyväksikäytön torjumiseksi (10.11.2020), 12 kohta.

¹⁴ Ks. COM(2022)209 final, s. 12–13.

¹⁵ Perusoikeuskirjan 52 artiklan 1 kohta.

¹⁶ Ks. Euroopan tietosuojavaltuutettu, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19.12.2019), s. 8, saatavilla osoitteessa https://edps.europa.eu/sites/default/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

¹⁷ EUT, asia C-393/19, *OM*, 53 kohta.

¹⁸ EUT, yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige ja Watson*, 101 kohta.

¹⁹ EUT, asia C-362/14, *Schrems*, 94 kohta.

²⁰ EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland ja Seitlinger ym.*, 39 kohta.

CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamistoimenpiteissä, joita ehdotuksessa suunnitellaan.

13. Euroopan unionin tuomioistuin on lisäksi todennut, että tietosuojatoimenpiteillä on keskeinen rooli sen varmistamisessa, että ei aiheuteta haittaa perusoikeuskirjan 8 artiklassa vahvistetun henkilötietojen suojaa koskevan perusoikeuden keskeiselle sisällölle²¹. Digiajalla tekniset ratkaisut, joilla varmistetaan sähköisen viestinnän luottamuksellisuus ja suojellaan sitä, ovat keskeisiä kaikkien perusoikeuksien käyttämisen varmistamisessa. Näitä toimenpiteitä ovat muun muassa salaustoimenpiteet.²² Tämä olisi otettava asianmukaisesti huomioon, kun arvioidaan CSAM-materiaalin tai seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun pakollista tunnistamista koskevia toimenpiteitä erityisesti, jos ne heikentäisivät tai huonontaisivat salausta²³.
14. Perusoikeuskirjan 52 artiklan 1 kohdassa säädetään myös, että perusoikeuskirjassa tunnustettujen perusoikeuksien käyttämistä voidaan rajoittaa ainoastaan lailla. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia²⁴. Suhteellisuusperiaatteen noudattamiseksi lainsäädännössä on esitettävä selkeät ja täsmälliset säännöt kyseessä olevien toimenpiteiden laajuudesta ja soveltamisesta sekä säädettävä vähimmäistakeista, jotta henkilöillä, joiden henkilötietoja asia koskee, on riittävät takuut siitä, että tietoja suojataan tehokkaasti väärinkäytön riskiltä²⁵. Lainsäädännössä on erityisesti mainittava, missä olosuhteissa ja millä edellytyksillä tällaisten tietojen käsittelyä koskeva toimenpide voidaan toteuttaa, jotta taataan, että puuttuminen rajoittuu ehdottoman välttämättömään²⁶. Kuten Euroopan unionin tuomioistuin on selventänyt, tarve tällaisista takeista on tärkeä varsinkin silloin, kun henkilötietoja käsitellään automaattisesti ja kun on suojattava kyseistä henkilötietojen erityisryhmää eli arkaluonteisia tietoja²⁷.
15. Ehdotuksessa rajoitettaisiin direktiivin 2002/58/EY, jäljempänä 'sähköisen viestinnän tietosuojadirektiivi'²⁸, 5 artiklan 1 ja 3 kohdassa ja 6 artiklan 1 kohdassa säädettyjen oikeuksien ja velvollisuuksien käyttöä siinä määrin kuin se on tarpeen ehdotuksen 1 luvun 2 jakson mukaisesti annettujen tunnistamismääräysten täytäntöön panemiseksi. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että siksi ehdotusta on arvioitava peruskirjan ja yleisen tietosuojasetuksen lisäksi myös sähköisen viestinnän tietosuojadirektiivin 5 ja 6 artiklan sekä 15 artiklan 1 kohdan perusteella.

²¹ Ks. edellinen alaviite., 40 kohta.

²² Ks. YK:n ihmisoikeusneuvosto, päätöslauselma 47/16 ihmisoikeuksien edistämisestä, suojelusta ja käyttämisestä verkossa, YK:n asiakirja A/HRC/RES/47/16 (26.7.2021).

²³ Ks. myös väliaikaisen asetuksen johdanto-osan 25 kappale.

²⁴ Ks. "Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit", 11.4.2019, saatavilla osoitteessa https://edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²⁵ EUT, yhdistetyt asiat C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net ym.*, 132 kohta.

²⁶ Ks. edellinen alaviite.

²⁷ Ks. edellinen alaviite.

²⁸ Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi), sellaisena kuin se on muutettuna direktiivillä 2006/24/EY ja direktiivillä 2009/136/EY.

4. ERITYISIÄ HUOMIOITA

4.1 Suhde voimassa olevaan lainsäädäntöön

4.1.1 Suhde yleiseen tietosuoja-asetukseen ja sähköisen viestinnän tietosuojadirektiiviin

16. Ehdotuksessa todetaan, että se ei vaikuta säännöksiin, jotka johtuvat muista unionin säädöksistä, erityisesti yleisestä tietosuoja-asetuksesta²⁹ ja sähköisen viestinnän tietosuojadirektiivistä. Toisin kuin väliaikaisessa asetuksessa, ehdotuksessa ei säädetä yksiselitteisestä tilapäisestä poikkeuksesta sähköisen viestinnän tietosuojadirektiivin 5 artiklan 1 ja 3 kohtaan ja 6 artiklan 1 kohtaan vaan niissä tarkoitettujen oikeuksien ja velvollisuuksien käytön rajoittamisesta. Olisi myös huomattava, että väliaikaisessa asetuksessa säädetään poikkeuksesta yksinomaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 1 kohdan ja 6 artiklan 1 kohdan säännöksiin eikä 5 artiklan 3 kohdan säännöksiin.
17. Ehdotuksessa viitataan lisäksi sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohtaan, jonka nojalla jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla rajoitetaan direktiivin 5 ja 6 artiklassa säädettyjen oikeuksien ja velvollisuuksien soveltamisalaa, jos tällaiset rajoitukset ovat välttämättömiä, asianmukaisia ja oikeasuhteisia demokraattisessa yhteiskunnassa, muun muassa rikosten torjunnan, tutkinnan, selvittämisen ja syyteharkinnan varmistamiseksi. Ehdotuksen mukaan sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohtaa sovelletaan analogisesti, jos ehdotuksessa rajoitetaan sähköisen viestinnän tietosuojadirektiivin 5 artiklan 1 ja 3 kohdassa ja 6 artiklan 1 kohdassa säädettyjen oikeuksien ja velvoitteiden käyttöä.
18. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu muistuttavat, että unionin tuomioistuin on tehnyt selväksi, että sähköisen viestinnän tietosuojadirektiivi 15 artiklan 1 kohtaa on tulkittava suppeasti. Se tarkoittaa, että 15 artiklan 1 kohdassa sallitun poikkeuksen viestinnän luottamuksellisuutta koskevaan periaatteeseen on pysyttävä poikkeuksena eikä siitä saa tulla sääntöä³⁰. Kuten tässä yhteisessä lausunnossa myöhemmin esitetään, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että ehdotus ei täytä (tiukkoja) vaatimuksia välttämättömydestä, vaikuttavuudesta ja oikeasuhteisuudesta. Lisäksi ne toteavat ehdotuksen tarkoittavan, että puuttumisesta viestinnän luottamuksellisuuteen voi itse asiassa pikemminkin tulla sääntö sen sijaan, että se pysyisi poikkeuksena.

4.1.2 Suhde asetukseen (EU) 2021/1232 ja vaikutus verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan vapaaehtoiseen tunnistamiseen

19. Ehdotuksen 88 artiklan mukaan ehdotuksella kumottaisiin väliaikainen asetus, jossa säädetään tilapäisestä poikkeuksesta sähköisen viestinnän tietosuojadirektiivin tiettyihin säännöksiin, jotta numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajat voivat käyttää vapaaehtoisesti teknologioita CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamiseksi. Näin siis ehdotetun asetuksen soveltamispäivästä lähtien sähköisen viestinnän tietosuojadirektiivistä ei voisi tehdä poikkeusta, jonka perusteella kyseiset

²⁹ Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (ETA:n kannalta merkityksellinen teksti) (EUVL L 119, 4.5.2016, s. 1–88).

³⁰ Tuomio, annettu 21.12.2016, yhdistetyt asiat C-203/15 ja C-698/15 *Tele2 Sverige AB ja Watson*, 89 kohta.

palveluntarjoajat voisivat tunnistaa vapaaehtoisesti verkkovälitteistä lapsiin kohdistuvaa seksuaaliväkivaltaa.

20. Koska ehdotuksella käyttöön otettavat tunnistamisvelvoitteet koskisivat vain tunnistamismääräysten saajia, ehdotetun asetuksen tekstissä olisi tärkeää selventää, että teknologioiden vapaaehtoinen käyttö CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamiseen pysyy sallittuna vain, jos se on sallittu sähköisen viestinnän tietosuojadirektiivissä ja yleisessä tietosuoja-asetuksessa. Tämä tarkoittaisi esimerkiksi, että numeroista riippumattomien henkilöiden välisten viestintäpalvelujen tarjoajia estettäisiin käyttämästä kyseisiä teknologioita vapaaehtoisesti, ellei sitä olisi sallittu kansallisissa laeissa, joilla sähköisen viestinnän tietosuojadirektiivi saatetaan osaksi kansallista lainsäädäntöä, sähköisen viestinnän tietosuojadirektiivin 15 artiklan 1 kohdan ja perusoikeuskirjan mukaisesti.
21. Yleisesti ottaen ehdotetussa asetuksessa kannattaisi selventää lisää verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan vapaaehtoisesta tunnistamisen tilaa ehdotetun asetuksen soveltamispäivän jälkeen ja siirryttäessä väliaikaisessa asetuksessa esitetystä vapaaehtoisesta tunnistamisjärjestelmästä ehdotetussa asetuksessa esitettyihin tunnistamisvelvoitteisiin. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu esimerkiksi suosittelivat tekemään selväksi, että ehdotetusta asetuksesta ei saada lakisääteistä perustaa henkilötietojen käsittelylle ainoastaan verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan vapaaehtoisesta tunnistamista varten.

4.2 Yleisen tietosuoja-asetuksen mukainen lakisääteinen perusta

22. Ehdotuksella pyritään vahvistamaan yleisessä tietosuoja-asetuksessa tarkoitettu lakisääteinen perusta henkilötietojen käsittelylle CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamista varten. Perusteluissa siis todetaan seuraavasti: ”Henkilötietojen käsittelyyn liittyvien pakollisten tunnistamistoimien osalta ehdotuksessa ja erityisesti sen perusteella annetuissa tunnistamismääräyksissä vahvistetaan näin ollen tällaisen käsittelyn perusteet, joihin viitataan yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohdassa. Siinä säädetään henkilötietojen käsittelystä, joka on tarpeen rekisterinpitäjälle unionin oikeuden tai kansallisen lainsäädännön nojalla kuuluvan lakisääteisen velvoitteen noudattamiseksi³¹.”
23. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suhtautuvat myönteisesti komission päätökseen poistaa henkilötietojen käsittelyn oikeusperustaa koskeva oikeudellinen epävarmuus, joka syntyi väliaikaisen asetuksen myötä. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat myös samaa mieltä komission näkemyksestä, jonka mukaan tunnistamistoimenpiteiden käyttöönoton seuraukset ovat liian kauaskantoisia ja vakavia, jotta palveluntarjoajien voitaisiin antaa päättää, toteuttavatko ne näitä toimenpiteitä³². Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu panevat kuitenkin merkille, että kaikki oikeusperustat, joiden perusteella palveluntarjoajien on puututtava tietosuoja- ja yksityisyyttä koskeviin perusoikeuksiin, ovat päteviä vain, jos niissä noudatetaan perusoikeuskirjan 52 artiklan 1 kohdassa esitettyjä ehtoja, kuten seuraavissa osissa analysoidaan.

4.3 Riskinarviointi ja lieventämisvelvoitteet

24. Ehdotuksen II luvun 1 jakson mukaan säilytyspalvelujen tarjoajien ja henkilöiden välisten viestintäpalvelujen tarjoajien on yksilöitävä, analysoitava ja arvioitava kunkin tarjoamansa palvelun

³¹ Ks. edellinen alaviite, s. 4.

³² Ks. ehdotus, COM(2022)209 final, s. 14.

osalta riski, että palvelua käytetään verkkovälitteiseen lapsiin kohdistuvaan seksuaaliväkivaltaan, ja pyrittävä sitten minimoimaan yksilöidyt riskit toteuttamalla ”kohtuullisia riskinhallintatoimenpiteitä, jotka on räätälöity [...] määritetyn riskin mukaan”.

25. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että riskinarviointia tehdessään palveluntarjoajan olisi otettava erityisesti huomioon ehdotuksen 3 artiklan 2 kohdan a–e alakohdassa luetellut seikat, muun muassa palveluntarjoajan ehdoissa esitetyt kiellot ja rajoitukset, tapa, jolla käyttäjät käyttävät palvelua, ja sen vaikutus kyseiseen riskiin, tapa, jolla palveluntarjoaja on suunnitellut palvelun ja ylläpitää sitä, mukaan lukien liiketoimintamalli, hallintotapa ja asiaankuuluvat järjestelmät ja prosessit, ja sen vaikutus kyseiseen riskiin. Lapsen houkuttelua seksuaalisiin tarkoituksiin koskevan riskin huomioon ottamiseksi ehdotetaan seuraavia seikkoja: missä määrin lapset käyttävät tai todennäköisesti käyttävät palvelua, käyttäjien eri ikäryhmät ja lapsen houkuttelua seksuaalisiin tarkoituksiin koskeva riski ikäryhmittäin, sellaisten toimintojen saatavuus, joilla käyttäjät voivat etsiä muita käyttäjiä ja olla suoraan yhteydessä muihin käyttäjiin, erityisesti yksityisen viestinnän kautta, sekä toiminnot, joilla käyttäjät voivat jakaa kuvia tai videoita muiden käyttäjien kanssa.
26. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu tunnustavat, että nämä perusteet vaikuttavat merkityksellisiltä. Huolta aiheuttaa joka tapauksessa se, että perusteet jättävät melko paljon varaa tulkinnalle ja arvioinnille. Useita perusteita kuvaillaan erittäin yleisluontoisesti (esim. ”tapa, jolla käyttäjät käyttävät palvelua, ja sen vaikutus kyseiseen riskiin”), tai ne liittyvät perustoimintoihin, jotka ovat yleisiä useissa verkkopalveluissa (esim. ”käyttäjien mahdollisuus jakaa kuvia tai videoita muiden käyttäjien kanssa”). Tällaisenaan perusteet näyttävät olevan enemmän kallellaan subjektiiviseen (kuin objektiiviseen) arviointiin.
27. Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun mielestä sama pätee ehdotuksen 4 artiklan mukaisesti toteutettaviin riskinhallintatoimenpiteisiin. Sellaiset toimenpiteet kuin palveluntarjoajan sisällön moderointi- tai suosittelujärjestelmien mukauttaminen asianmukaisilla teknisillä ja operatiivisilla toimenpiteillä ja henkilöstöllä näyttävät olevan merkityksellisiä määritetyn riskin vähentämisen kannalta. Jos näitä perusteita kuitenkin sovelletaan monimutkaisessa riskinarviointiprosessissa ja yhdistetään abstrakteihin ja epämääräisiin käsitteisiin, joilla kuvataan riskin hyväksyttävä määrä (esim. ”merkittävässä määrin”), ne eivät täytä oikeusvarmuuden ja ennakoitavuuden vaatimuksia, jotka tarvitaan perustelemaan puuttuminen yksityishenkilöiden välisen viestinnän luottamuksellisuuteen. Siten ne ovat selkeää puuttumista yksityisyyttä ja sananvapautta koskeviin perusoikeuksiin.
28. Vaikka palveluntarjoajat eivät saa puuttua viestinnän luottamuksellisuuteen riskinarviointi- ja lieventämisstrategioissaan ennen tunnistamismääräyksen saamista, riskinarviointi- ja lieventämisvelvoitteiden ja niistä johtuvien tunnistamisvelvoitteiden välillä on suora yhteys. Ehdotuksen 7 artiklan 4 kohdassa tunnistamismääräyksen antamisesta tehdään riippuvaista siitä, että on näyttöä merkittävästä riskistä, että kyseistä palvelua voitaisiin käyttää verkkovälitteiseen lapsiin kohdistuvaan seksuaaliväkivaltaan. Ennen kuin tunnistamismääräys annetaan, on suoritettava monimutkainen prosessi, jossa ovat mukana palveluntarjoajat, koordinoiva viranomainen ja oikeusviranomainen tai muu riippumaton hallintoviranomainen, joka on vastuussa määräyksen antamisesta. Ensin palveluntarjoajien on arvioitava riski siitä, että niiden palveluja käytetään verkkovälitteiseen lapsiin kohdistuvaan seksuaaliväkivaltaan (ehdotuksen 3 artikla), ja määritettävä mahdolliset riskinhallintatoimenpiteet (ehdotuksen 4 artikla), joilla riskiä voidaan vähentää. Tämän toimenpiteet tulokset on sitten raportoitava toimivaltaiselle koordinoivalle viranomaiselle (ehdotuksen 5 artikla). Jos riskinarvioinnista käy ilmi, että lieventämistoimenpiteistä huolimatta riski on edelleen merkittävä, koordinoiva viranomainen kuulee palveluntarjoajaa tunnistamismääräyksen

antamista koskevan pyynnön luonnoksesta ja antaa palveluntarjoajalle mahdollisuuden esittää huomautuksia. Palveluntarjoajan on sitten esitettävä täytäntöönpanosuunnitelma, myös lausunto toimivaltaiselta tietosuojaviranomaiselta, jos kyseessä on seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistaminen. Jos koordinoiva viranomaisena päättää edetä asiassa, tuomioistuimien tai muu riippumaton hallintoviranomaisena laatii ja lopuksi antaa tunnistamismääräyksen. Näin ollen alustava riskinarviointi ja määritetyn riskin vähentämiseksi valitut toimenpiteet ovat ratkaiseva perusta koordinoivan viranomaisen sekä toimivaltaisen oikeus- tai hallintoviranomaisen arvioinnille siitä, onko tunnistamismääräystarpeen.

29. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu panevat merkille tunnistamismääräyksen antamiseen johtavat monimutkaiset vaiheet. Niihin kuuluu palveluntarjoajan tekemä alustava riskinarviointi ja palveluntarjoajan ehdotus riskinhallintatoimenpiteistä sekä palveluntarjoajan myöhempi vuorovaikutus toimivaltaisen koordinoivan viranomaisen kanssa. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että palveluntarjoajalla on huomattavat mahdollisuudet vaikuttaa prosessin lopputulokseen. Ne panevat tämän osalta merkille, että ehdotuksen johdanto-osan 17 kappaleessa todetaan, että palveluntarjoajien pitäisi pystyä osana riskiraportointia ilmaisemaan ”halukkuutensa ja valmiutensa” siinä tapauksessa, että niille annetaan tunnistamismääräys. Näin ollen ei voida olettaa, että joka ikinen palveluntarjoaja pyrkii välttämään tunnistamismääräyksen antamisen, jotta sen käyttäjien viestinnän luottamuksellisuus voidaan säilyttää, soveltamalla tehokkaimpia mutta mahdollisimman vähän yksityisyyttä loukkaavia lieventämistoimenpiteitä. Tämä koskee erityisesti sitä, kun kyseisillä lieventämistoimenpiteillä puututaan palveluntarjoajan perusoikeuskirjan 16 artiklan mukaiseen elinkeinovapauteen.
30. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu haluavat korostaa, että menettelytakeilla ei voida koskaan täysin korvata aineellisia takeita. Siksi edellä kuvattuun tunnistamismääräyksen mahdolliseen antamiseen johtavaan monimutkaiseen prosessiin pitäisi liittää selkeät aineelliset velvoitteet. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että ehdotus on epäselvä useissa keskeisissä seikoissa (esim. käsitteet ”merkittävä riski” ja ”merkittävässä määrin”), mitä ei voida korjata sillä, että menettelytakeissa on useita kerroksia. Tämä on vieläkin tärkeämpää siksi, että kyseisten takeiden soveltamisesta vastuussa olevilla tahoilla (esim. palveluntarjoajilla ja oikeusviranomaisilla) on laaja harkintavaltaa siinä, miten kunkin yksittäisen tapauksen kyseessä olevat oikeudet saadaan tasapainoon. Koska ehdotuksen hyväksymisestä seuraisi laajoja puuttumisia perusoikeuksiin, lainsäätäjän olisi varmistettava, että ehdotuksessa esitetään selkeämmin, milloin ja missä kyseiset puuttumiset sallitaan. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu tunnustavat, että lainsäädäntötoimenpiteet eivät saa olla liian ohjailevia ja että niiden käytännön soveltamiseen on jätettävä jonkin verran joustavuutta. Ne katsovat kuitenkin, että ehdotuksen nykyisessä tekstissä jätetään liian paljon mahdollisuuksia mahdolliseen väärinkäyttöön, koska selkeitä aineellisia normeja ei ole.
31. Asetuksella voi olla huomattava vaikutus erittäin moneen rekisteröityyn (eli mahdollisesti kaikkiin henkilöiden välisten viestintäpalvelujen käyttäjiin). Siksi Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu korostavat, että lainsäädäntöön tarvitaan enemmän oikeusvarmuutta, selkeyttä ja ennakoitavuutta sen varmistamiseksi, että ehdotetut toimenpiteet ovat aidosti tehokkaita niiden tavoitteiden saavuttamisessa ja että samalla ne haittaavat mahdollisimman vähän kyseessä olevia perusoikeuksia.

4.4 Tunnistamismääräysten antamisen ehdot

32. Ehdotuksen 7 artiklassa säädetään, että sijoittautumispaikan koordinoivalla viranomaisella on valtuudet pyytää jäsenvaltion toimivaltaista oikeusviranomaista tai kyseisen jäsenvaltion muuta

riippumatonta hallintoviranomaista antamaan tunnistamismääräys, jossa säilytyspalvelujen tarjoajaa tai henkilöiden välisten viestintäpalvelujen tarjoajaa vaaditaan toteuttamaan 10 artiklassa tarkoitetut toimenpiteet verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan tunnistamiseksi tietyssä palvelussa.

33. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ottavat asianmukaisesti huomioon seuraavat edellytykset, jotka on täytettävä ennen tunnistamismääräyksen antamista:
 - a. näyttöä on merkittävästä riskistä, että palvelua käytetään tapauksen mukaan 7 artiklan 5, 6 ja 7 kohdassa tarkoitettuun verkkovälitteiseen lapsiin kohdistuvaan seksuaaliväkivaltaan
 - b. tunnistamismääräyksen antamisen syyt ovat painavimmat kuin kielteiset vaikutukset kaikkien asianomaisten osapuolten oikeuksiin ja oikeutettuihin etuihin, kun otetaan erityisesti huomioon tarve varmistaa oikeudenmukainen tasapaino kyseisten osapuolten perusoikeuksien välillä.
34. Merkittävä riski määritellään 5 kohdassa ja 7 artiklan perusteella käsiteltävänä olevan tunnistamismääräyksen tyyppin mukaan. Tiedossa olevan CSAM-materiaalin tunnistamista koskevien tunnistamismääräysten osalta merkittävän riskin katsotaan olevan olemassa, jos
 - a. palveluntarjoajan mahdollisesti jo toteuttamista tai tulevaisuudessa toteuttamista lieventävistä toimenpiteistä huolimatta on todennäköistä, että palvelua käytetään merkittävässä määrin tiedossa olevan lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan kuvamateriaalin levittämiseen, ja
 - b. on näyttöä siitä, että kyseistä palvelua tai vastaavaa palvelua, jos sitä ei ole vielä tarjottu unionissa tunnistamismääräyksen antamista koskevan pyynnön esittämispäivänä, on käytetty viimeksi kuluneiden 12 kuukauden aikana merkittävässä määrin lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevan kuvamateriaalin levittämiseen.
35. Kun tunnistamismääräys annetaan muusta kuin tiedossa olevasta CSAM-materiaalista, todennäköisyydessä ja tosiasiallisessa näytössä on viitattava muuhun kuin tiedossa olevaan CSAM-materiaalin. Lisäksi tiedossa olevasta CSAM-materiaalista on pitänyt antaa aiemmin tunnistamismääräys, jonka perusteella palveluntarjoajan on pitänyt toimittaa merkittävä määrä ilmoituksia CSAM-materiaalista (ehdotuksen 7 artiklan 6 kohta). Lapsen houkuttelua seksuaalisiin tarkoituksiin koskevan tunnistamismääräyksen osalta merkittävän riskin katsotaan olevan olemassa, jos palveluntarjoajaa voidaan pitää henkilöiden välisten viestintäpalvelujen tarjoajana, on todennäköistä, että palvelua käytetään merkittävässä määrin lapsen houkutteluun seksuaalisiin tarkoituksiin, ja on näyttöä siitä, että palvelua on käytetty huomattavassa määrin lapsen houkutteluun seksuaalisiin tarkoituksiin (ehdotuksen 7 artiklan 7 kohta).
36. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että vaikka ehdotuksen 7 artiklan 5–7 kohdassa esitetään tarkennuksia, tunnistamismääräyksen antamishdoissa käytetään pääosien epämääräisiä oikeudellisia käsitteitä, kuten ”merkittävässä määrin”, ”huomattavassa määrin” ja ”merkittävä määrä”. Ne myös toistavat osittain itseään, koska näyttö aiemmasta hyväksikäytöstä vaikuttaa usein tulevan hyväksikäytön todennäköisyyden vahvistamiseen.
37. Ehdotuksessa suunnitellaan järjestelmää, jossa tunnistamismääräyksen tarpeellisuudesta päätettäessä on tehtävä ennakoiva päätös palvelun tulevasta käytöstä verkkovälitteiseen lapsiin kohdistuvaan seksuaaliväkivaltaan. Siksi on ymmärrettävää, että 7 artiklassa esitetyt edellytykset ovat luonteeltaan ennustavia. Koska ehdotuksessa kuitenkin turvaututaan epämääräisiin käsitteisiin, palveluntarjoajien sekä toimivaltaisten oikeusviranomaisten tai muiden riippumattomien

valtuutettujen hallintoviranomaisten on vaikeaa soveltaa ehdotuksessa käyttöön otettuja lakisäätöisiä vaatimuksia ennakoivasti ja niin, ettei se ole mielivaltaista. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat huolissaan siitä, että nämä laajat ja epämääräiset käsitteet aiheuttavat oikeusvarmuuden puutetta sekä huomattavia eroja ehdotuksen käytännön täytäntöönpanossa unionissa. Eroja voi olla esimerkiksi siinä, miten jäsenvaltioiden oikeusviranomaiset tai muut riippumattomat hallintoviranomaiset tulkitsevat käsitteitä ”todennäköisyys” ja ”merkittävässä määrin”. Tällaista lopputulosta ei voitaisi hyväksyä, koska henkilöiden välisten viestintäpalvelujen tarjoajien tunnistamismääräyksiä koskevat säännökset ovat sähköisen viestinnän tietosuojadirektiivin 5 artiklassa tarkoitettuja luottamuksellisuuden periaatteen soveltamisen rajoituksia. Niiden selkeys ja ennakoitavuus ovat siksi erittäin tärkeitä sen varmistamiseksi, että rajoituksia sovelletaan yhtenäisesti koko unionissa.

4.5 Suunniteltujen toimenpiteiden tarpeellisuuden ja oikeasuhteisuuden analyysi³³

38. Kuten edellä todetaan, annettavissa tunnistamismääräyksissä on kolme tyyppiä: lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevan kuvamateriaalin levittämistä koskevat tunnistamismääräykset (ehdotuksen 7 artiklan 5 kohta), lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan uuden kuvamateriaalin levittämistä koskevat tunnistamismääräykset (ehdotuksen 7 artiklan 6 kohta) ja lapsen houkuttelua seksuaalisiin tarkoituksiin koskevat tunnistamismääräykset (ehdotuksen 7 artiklan 7 kohta). Kunkin tunnistamismääräyksen käytännön täytäntöönpano edellyttäisi yleensä erilaista teknologiaa. Siksi niiden puuttumisen tasot ovat erilaisia, ja siten ne myös vaikuttavat eri tavoin yksityisyyttä ja henkilötietojen suojaa koskeviin oikeuksiin.
39. Lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevan kuvamateriaalin tunnistamisessa käytetään tavallisesti täsmäytysteknologiaa. Siinä siis hyödynnetään tiedossa olevan CSAM-materiaalin olemassa olevia tietokantoja, joihin kuvia (myös videoiden pysäytyskuvia) voidaan verrata. Jotta täsmäytys onnistuu, palveluntarjoajan käsittelemät kuvat sekä tietokannan kuvat digitoitava. Se tehdään tavallisesti muuntamalla ne hash-arvoiksi eli tiivisteiksi. Tällaisen tiivistämisteknologian väärin positiivisten tulosten määräksi on arvioitu enintään yksi viidestäkymmenestä miljardista (eli väärin positiivisten tulosten osuus on 0,000000002 prosenttia).³⁴
40. Uuden CSAM-materiaalin tunnistamisessa käytetään tavallisesti erilaista teknologiaa, muun muassa luokittimia ja tekoälyä³⁵. Niiden virhetasot ovat kuitenkin yleisesti paljon korkeampia. Vaikutustenarviointikertomuksen mukaan esimerkiksi uuden CSAM-materiaalin tunnistamiseen on teknologioita, joiden tarkkuustasoksi voidaan asettaa 99,9 prosenttia (eli väärin positiivisten tulosten osuus on 0,1 prosenttia), mutta tällä tarkkuustasolla ne pystyvät tunnistamaan asianomaisesta tietojoukosta vain 80 prosenttia kaikesta CSAM-materiaalista³⁶.

³³ Ks. myös Euroopan tietosuojavaltuutetun pikaopas tarpeellisuudesta ja oikeasuhteisuudesta ”The EDPS quick guide to necessity and proportionality”, saatavilla osoitteessa https://edps.europa.eu/sites/default/files/publication/20-01-28_edps_quickguide_en.pdf.

³⁴ Ks. Euroopan komissio, komission yksiköiden valmisteluasiakirja, Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse, SWD(2022) 209 final, jäljempänä vaikutustenarviointikertomus’ tai ’SWD(2022) 209 final’, s. 281, alaviite 511.

³⁵ Vaikutustenarviointikertomus, s. 281.

³⁶ Ks. edellinen alaviite, s. 282.

41. Vaikutustenarviointikertomuksessa selitetään, että kirjallisessa viestinnässä tapahtuva lapsen houkuttelu seksuaalisiin tarkoituksiin tunnistetaan tavallisesti viestinnän mallien perusteella. Vaikutustenarviointikertomuksessa huomautetaan, että joidenkin nykyisten seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamisteknologioiden tarkkuusaste on 88 prosenttia³⁷. Komission mukaan se tarkoittaa, että sadasta keskustelusta, joiden on mahdollisesti ilmoitettu sisältävän lasten rikollista houkuttelua, 12 voidaan sulkea pois [ehdotuksen mukaan EU-keskuksen tekemän] arvioinnin perusteella eikä niistä ilmoiteta lainvalvontaan³⁸. Vaikka ehdotusta sovellettaisiin myös ääniviestintään – toisin kuin väliaikaista asetusta – vaikutustenarviointikertomuksessa ei kuitenkaan käsitellä yksityiskohtaisemmin teknisiä ratkaisuja, joita voitaisiin käyttää seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamiseen sellaisessa ympäristössä.

4.5.1 Tunnistamisen tehokkuus

42. Tarpeellisuuteen kuuluu, että on tehtävä tosiasioihin perustuva arviointi suunniteltujen toimenpiteiden tehokkuudesta niiden tavoitteen saavuttamisessa sekä siitä, onko se vähemmän yksityisyyttä loukkaava kuin muut vaihtoehdot saman tavoitteen saavuttamisessa³⁹. Toinen ehdotetun toimenpiteen oikeasuhteisuutta koskevassa arvioinnissa huomioon otettava tekijä on nykyisten toimenpiteiden tehokkuus verrattuna ehdotettuun⁴⁰. Jos samaa tai samankaltaista tarkoitusta varten on jo toimenpiteitä, niiden tehokkuus olisi arvioitava oikeasuhteisuuden arvioinnin osana. Jos samaan tai samankaltaiseen tarkoitukseen tähtäävien nykyisten toimenpiteiden tehokkuutta ei arvioida, uuden toimenpiteen oikeasuhteisuustestiä ei voida katsoa asianmukaisesti suoritetuksi.
43. Säilytyspalvelujen ja henkilöiden välisten viestintäpalvelujen tarjoajat voivat CSAM-materiaalin tai seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamalla edistää yleistä tavoitetta lapsiin kohdistuvan seksuaalisen väkivallan ja lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan kuvamateriaalin verkossa tapahtuvan levittämisen ehkäisystä ja torjunnasta. Se, että ehdotuksessa esitettyjen toimenpiteiden tehokkuus on arvioitava, herättää kuitenkin kolme keskeistä kysymystä:
- Onko verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan tunnistamistoimet helppo kiertää?
 - Mikä vaikutus tunnistamistoimilla on lainvalvontaviranomaisten toimintaan?⁴¹
 - Miten ehdotus vähentäisi oikeudellista epävarmuutta?
44. Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun tehtävänä ei ole vastata yksityiskohtaisesti näihin kysymyksiin. Ne huomauttavat kuitenkin, että kysymyksiä ei käsitellä kokonaisvaltaisesti vaikutustenarviointikertomuksessa eikä ehdotuksessa.

³⁷ Ks. edellinen alaviite, s. 283.

³⁸ Ehdotus, COM(2022)209 final, s. 14, alaviite 32.

³⁹ Euroopan tietosuojavaltuutettu, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11.4.2017, s. 5; Euroopan tietosuojavaltuutettu, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019), s. 8.

⁴⁰ Euroopan tietosuojavaltuutettu, Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data (19.12.2019), s. 11.

⁴¹ Vaikutustenarviointikertomuksen liitteen II (s. 132) mukaan 85,71 prosenttia lainvalvontakyselyyn vastanneista esitti huolensa lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan kuvamateriaalin määrän kasvusta viime vuosikymmenenä ja resurssien (esim. henkilöstön, tekniikan) puutteesta.

45. CSAM-materiaalin tunnistamisen kiertämismahdollisuuden osalta on huomautettava, että tällä hetkellä ei näytä olevan teknistä ratkaisua salattuna jaetun CSAM-materiaalin tunnistamiseen. Siksi kaikki tunnistamistoimet – myös asiakaspuolen seulonta, jossa tarkoituksena on kiertää palveluntarjoajan tarjoama päästä päähän -salaus⁴² – voidaan kiertää helposti salaamalla sisältö erillisen sovelluksen avulla ennen sen lähettämistä tai lataamista. Näin ollen ehdotuksessa suunnitelluilla tunnistamistoimilla voi olla CSAM-materiaalin levittämiseen verkossa toivottua pienempi vaikutus.
46. Komissio odottaa myös, että lainvalvontaviranomaisille lapsiin kohdistuvasta seksuaaliväkivallasta toimitettujen ilmoitusten määrä kasvaa, kun ehdotuksessa käyttöön otetut tunnistamisveloitteet hyväksytään⁴³. Ehdotuksessa tai vaikutustenarviointikertomuksessa ei kuitenkaan selitetä, miten sillä puututaan nykyisen asiantilan puutteisiin. Koska lainvalvontaviranomaisten resurssit ovat rajallisia, näyttää olevan tarpeen ymmärtää paremmin, olisiko ilmoitusten määrän kasvulla merkityksellistä vaikutusta lainvalvontatoimiin, joilla torjutaan lapsiin kohdistuvaa seksuaaliväkivaltaa. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu haluavat joka tapauksessa korostaa, että kyseiset ilmoitukset olisi arvioitava ajoissa, jotta päätös ilmoitetun materiaalin merkityksestä rikoksen kannalta voitaisiin tehdä mahdollisimman pian ja vähentää merkityksettömien tietojen säilyttämistä mahdollisimman paljon.

4.5.2 Ei vähemmän yksityisyyttä loukkaava toimenpide

47. Vaikka myönteiset vaikutukset komission suunnittelemasta CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamisesta pystyttäisiinkin konkretisoimaan, tunnistamisen on oltava vähiten yksityisyyttä loukkaava toimenpide verrattuna yhtä tehokkaisiin toimenpiteisiin. Ehdotuksen 4 artiklassa säädetään, että ensiksi palveluntarjoajien pitäisi harkita sellaisten lieventävien toimenpiteiden käyttöönottoa, joilla riskiä niiden palvelujen käyttämisestä verkkovälitteiseen lapsiin kohdistuvaan seksuaaliväkivaltaan pienennetään niin, että se alittaa rajan, jonka ylityessä tunnistamismääräys voidaan antaa. Lieventävät toimenpiteet, joilla voitaisiin vähentää huomattavasti kyseisessä palvelussa tehdyn seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tai siinä vaihdetun CSAM-materiaalin määrää, olisivat usein vähemmän yksityisyyttä loukkaavia toimenpiteitä verrattuna tunnistamismääräykseen⁴⁴. Jos siis asianomainen palveluntarjoaja ei ota tällaisia toimenpiteitä käyttöön vapaaehtoisesti, toimivaltaisen riippumattoman hallintoviranomaisen tai oikeusviranomaisen pitäisi voida tehdä lieventävien toimenpiteiden täytäntöönpanosta pakollista ja täytäntöönpanokelpoista sen sijaan, että se antaisi tunnistamismääräyksen. Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun mielestä se, että ehdotuksen 5 artiklan 4 kohdan nojalla koordinoiva viranomainen voi ”vaatia” palveluntarjoajaa ottamaan käyttöön, tarkistamaan, lakkauttamaan tai laajentamaan lieventäviä toimenpiteitä, ei riitä, koska tällainen vaatimus ei olisi yksinään täytäntöönpanokelpoinen. Sen noudattamatta jättämisestä ”rangaistaisiin” vain tunnistamismääräyksen antamisella.
48. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat siksi, että koordinoivalle viranomaiselle tai toimivaltaiselle riippumattomalle hallinto- tai oikeusviranomaiselle olisi

⁴² Ks. lisätietoja jäljempänä kohdasta 4.10.

⁴³ Ks. mm. vaikutustenarviointikertomus, liite 3, SWD(2022)209 final, s. 176.

⁴⁴ Voitaisiin harkita esimerkiksi sellaisia toimenpiteitä kuin CSAM-materiaalin välittämisen estäminen asiakaspuolella estämällä sähköisen viestinnän sisällön lataaminen ja lähettäminen, koska ne voivat tietyissä tilanteissa auttaa estämään tiedossa olevan CSAM-materiaalin kiertämistä.

yksiselitteisesti annettava valtuudet määrätä vähemmän yksityisyyttä loukkaavista lieventävistä toimenpiteistä ennen tunnistamismääräyksen antamista tai sen sijasta.

4.5.3 Oikeasuhteisuus suppeimmassa merkityksessä

49. Jotta toimenpide noudattaisi perusoikeuskirjan 52 artiklan 1 kohdassa vahvistettua suhteellisuusperiaatetta, toimenpiteestä johtuvat edut eivät saisi olla pienempiä kuin haitat, joita toimenpide aiheuttaa perusoikeuksien käyttämiselle. Suhteellisuusperiaatteella siis rajoitetaan viranomaisten valtuuksien käyttöä edellyttämällä, että käytettyjen keinojen ja niiden tavoitteen (tai niillä saavutettavan tuloksen) on oltava tasapainossa⁴⁵.
50. Jotta toimenpiteen vaikutusta yksityisyyttä ja henkilötietojen suojaa koskeviin perusoikeuksiin voidaan arvioida, on erityisen tärkeää määrittää täsmällisesti⁴⁶
- **toimenpiteen soveltamisala**, muun muassa niiden ihmisten määrä, joihin se vaikuttaa, sekä se, aiheuttaako toimenpide sivuvaikutuksia (eli puuttumista muiden henkilöiden kuin toimenpiteen kohteiden yksityisyyteen)
 - **toimenpiteen laajuus**, muun muassa kerättävien tietojen määrä, toimenpiteen kesto, se, edellyttääkö tarkastettava toimenpide erityisten tietoryhmien keräämistä ja käsittelyä
 - **yksityisyyden loukkaamisen taso**, jossa otetaan huomioon toimenpiteeseen kuuluvan toiminnan luonne (vaikuttaako se salassapitovelvollisuuden piiriin kuuluviin toimiin, asianajajan ja asiakkaan väliseen suhteeseen, terveydenhoitotoimiin), tilanne, se, profiloidaanko toimenpiteessä asianomaisia henkilöitä, ja käytetäänkö käsittelyssä (osittain tai kokonaan) automaattista päätöksentekojärjestelmää, jossa on virhemahdollisuus
 - se, koskeeko toimenpide **haavoittuvassa asemassa olevia henkilöitä**
 - se, vaikuttaako toimenpide myös **muihin perusoikeuksiin** (esim. sananvapautta koskevaan oikeuteen, kuten asioissa *Digital Rights Ireland ja Seitlinger ym. ja Tele2 Sverige ja Watson*)⁴⁷.
51. Tässä yhteydessä on myös tärkeää panna merkille, että vaikutus voi olla vähäinen asianomaisen henkilön kannalta mutta merkittävä tai erittäin merkittävä yhteisesti / yhteiskunnalle kokonaisuudessaan⁴⁸.
52. Kaikissa kolmessa tunnistamismääräyksen tyypissä (tiedossa olevan CSAM-materiaalin, uuden CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistaminen) tällä hetkellä käytävissä olevissa teknologioissa käytetään kaikkien asianomaisten käyttäjien sisältötietojen

⁴⁵ Ks. asia C-343/09, *Afton Chemical*, 45 kohta; yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke ja Hartmut Eifert*, 74 kohta; asiat C-581/10 ja C-629/10, *Nelson ym.*, 71 kohta; asia C-283/11, *Sky Österreich*, 50 kohta; ja asia C-101/12, *Schaible*, 29 kohta. Ks. lisäksi Euroopan tietosuojavaltuutettu, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit* (11.4.2017).

⁴⁶ Euroopan tietosuojavaltuutettu, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19.12.2019), s. 23.

⁴⁷ Ks. myös Euroopan tietosuojavaltuutetun lausunto 7/2020, joka koskee ehdotusta tilapäisistä poikkeuksista direktiivistä 2002/58/EY verkossa tapahtuvan lasten seksuaalisen hyväksikäytön torjumiseksi (10.11.2020), sivulta 9 eteenpäin.

⁴⁸ Euroopan tietosuojavaltuutettu, *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data* (19.12.2019), s. 20.

automaattista käsittelyä. Sisällön analysointiin käytettävät teknologiat ovat usein monimutkaisia, ja niihin liittyy usein tekoälyn käyttöä. Palvelun käyttäjä ei siksi ehkä täysin ymmärrä, miten teknologia käyttäytyy. Lisäksi tällä hetkellä käytössä olevien teknologioiden, erityisesti uuden CSAM-materiaalin tai seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamiseen käytettävien teknologioiden virhetasojen tiedetään olevan melko korkeita⁴⁹. Vaarana on lisäksi se, että EU-keskukselle tehdään ehdotuksen 12 artiklan 1 kohdan ja 48 artiklan 1 kohdan mukaisesti ilmoitus ”mahdollisen” CSAM-materiaalien tunnistamisen perusteella.

53. Lisäksi ehdotuksen mukaiset tunnistamismääräyksen antamista koskevat yleiset ehdot, joita sovelletaan koko palveluun eikä vain valittuihin viesteihin⁵⁰, uuden tai tiedossa olevan CSAM-materiaalin levittämistä koskevien tunnistamismääräysten enintään 24 kuukauden soveltamisaika ja lapsen houkuttelua seksuaalisiin tarkoituksiin koskevien tunnistamismääräysten enintään 12 kuukauden soveltamisaika⁵¹ jne. voivat tehdä määräyksen käytännön soveltamisalasta erittäin laajan. Seuranta olisi siksi itse asiassa yleistä ja summittaista eikä käytännössä kohdennettua.
54. Edellä kerrotun perusteella Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat huolissaan myös mahdollisista lamaannuttavista vaikutuksista sananvapauden harjoittamiselle. Ne muistuttavat, että tällainen lamaannuttava vaikutus katsotaan sitä todennäköisemmäksi, mitä epäselvempi laki on.
55. Ehdotus ei ole riittävän yksilöity, täsmällinen ja selvä, jotta täytettäisiin oikeusvarmuutta koskeva edellytys⁵², ja sen soveltamisala on laaja eli se koskee kaikkia kyseisiä palveluja tarjoavia tietoyhteiskunnan palveluntarjoajia unionissa⁵³. Näin ollen ehdotuksella ei varmisteta, että CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamisessa käytetään tosiasiallisesti vain kohdennettua lähestymistapaa. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat siksi, että ehdotuksesta voisi käytännössä tulla tosiasiallinen perusta kaikkien EU:n/ETA:n käyttäjien kaikenlaisen sähköisen viestinnän yleisluontoiselle ja summittaiselle sisällön tarkastamiselle. Lainsäädäntö voi näin ollen saada ihmiset pidättäytymään jakamasta lakisääteistä sisältöä sen pelossa, että he voisivat toimiensa vuoksi joutua kohteeksi.
56. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu tiedostavat kuitenkin, että yksityisyyteen puuttumisen taso voi olla erilainen eri toimissa, joilla torjutaan verkossa tapahtuvaa lasten seksuaalista hyväksikäyttöä. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat yleisesti, että puheen tai tekstin automaattinen analyysi mahdollisen seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamiseksi on todennäköisesti merkittävämpää puuttumista kuin kuvien tai videon vertaaminen aiemmin vahvistettuihin CSAM-materiaalia koskeviin tapauksiin CSAM-materiaalin levittämisen tunnistamiseksi. Lisäksi olisi tehtävä ero ”tiedossa olevan CSAM-materiaalin” ja ”uuden CSAM-materiaalin” tunnistamisen välillä. Myös säilytyspalvelujen tarjoajiin ja henkilöiden välisten viestintäpalvelujen tarjoajiin kohdennetut toimenpiteet olisi erotettava toisistaan.

⁴⁹ Ks. tarkemmin edellä 4.5 kohta ja jäljempänä 4.8.2 alakohta.

⁵⁰ Ks. ehdotuksen 7 artiklan 1 kohta.

⁵¹ Ks. ehdotuksen 7 artiklan 9 kohdan kolmas alakohta.

⁵² Ks. EUT, asia C-197/96, *Euroopan yhteisöjen komissio vastaan Ranskan tasavalta*, 15 kohta.

⁵³ Ks. ehdotuksen 1 artiklan 2 kohta.

4.5.4 Lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan tiedossa olevan kuvamateriaalin tunnistaminen

57. Vaikka johdanto-osan 4 kappaleen mukaan ehdotus olisi ”teknologianeutraali”, sekä ehdotettujen tunnistamistoimenpiteiden tehokkuus että niiden vaikutus ihmisiin riippuvat hyvin paljon käytettävän teknologian valinnasta ja valituista indikaattoreista. Tämä tiedostetaan komission vaikutustenarviointikertomuksen liitteessä 8⁵⁴ ja vahvistetaan muissa tutkimuksissa, muun muassa Euroopan parlamentin tutkimuspalvelujen kohdennetussa korvaavassa vaikutustenarvioinnissa, joka koskee komission ehdotusta tilapäisestä poikkeuksesta sähköisen viestinnän tietosuojadirektiiviin verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan torjunnan osalta helmikuusta 2021 lähtien⁵⁵.
58. Ehdotuksen 10 artiklassa esitetään useita vaatimuksia tunnistamiseen käytettäville teknologioille. Ne koskevat erityisesti teknologioiden tehokkuutta, luotettavuutta ja sitä, että ne loukkaavat mahdollisimman vähän käyttäjien oikeuksia yksityis- ja perhe-elämään, myös viestinnän luottamuksellisuuteen, ja henkilötietojen suojaan.
59. Tämän osalta Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että nykyisellään ainoat teknologiat, jotka näyttävät täyttävän yleisesti nämä vaatimukset, ovat tiedossa olevan CSAM-materiaalin tunnistamisessa käytettävät eli täsmäytysteknologiat, joissa tehdään vertailuja tiivistetietokantoihin.

4.5.5 Lapsiin kohdistuvaa seksuaaliväkivaltaa todistavan muun kuin aiemmin tiedossa olevan kuvamateriaalin tunnistaminen

60. Aiemmin tuntemattoman (uuden) CSAM-materiaalin tunnistamiseen tähtäävien toimenpiteiden arviointi johtaa erilaisiin päätelmiin niiden tehokkuudesta, luotettavuudesta ja yksityisyyttä ja tietosuojaa koskeviin perusoikeuksiin kohdistuvan vaikutuksen rajoittamisesta.
61. Ensinnäkin, kuten ehdotuksen vaikutustenarviointikertomuksessa selitetään, aiemmin tuntemattoman CSAM-materiaalin tunnistamiseen tällä hetkellä käytettäviin teknologioihin kuuluu luokittimia ja tekoälyä. Luokitin on mikä tahansa algoritmi, jolla lajitellaan tietoa merkittyihin tietoluokkiin tai -ryhmiin, tietomallien tunnistamisen avulla⁵⁶. Näin ollen näiden teknologioiden tulokset ja vaikutus vaihtelevat täsmällisyyden, tehokkuuden ja yksityisyyteen puuttumisen tason osalta. Samalla ne ovat myös alttiimpia virheille.
62. Aiemmin tuntemattoman CSAM-materiaalien tunnistamisessa käytettävät tekniikat ovat samankaltaisia kuin seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamisessa käytettävät, koska kummatkaan eivät perustu yksinkertaisiin täsmäytysteknologioihin vaan ennakoiviin malleihin, joissa käytetään tekoälyteknologioita. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että aiemmin tuntemattoman CSAM-materiaalin tunnistamisessa olisi oltava erittäin huolellinen, koska järjestelmän virheellä olisi vakavat vaikutukset

⁵⁴ Ks. tiedot väärrien positiivisten tulosten tasosta vaikutustenarviointikertomuksen liitteessä 8, sivulta 279 eteenpäin.

⁵⁵ Ks. Commission proposal on the temporary derogation from the e-Privacy Directive for the purpose of fighting online child sexual abuse: Targeted substitute impact assessment (Euroopan parlamentin tutkimuspalvelut, helmikuu 2021), sivulta 14 eteenpäin.

⁵⁶ Vaikutustenarviointikertomus, liite 8, s. 281.

rekisteröityihin, joiden automaattisesti merkittäisiin mahdollisesti tehneen erittäin vakavan rikoksen ja joiden henkilötiedot ja viestinnän yksityiskohdat ilmoitettaisiin.

63. Toiseksi kirjallisuudesta löydetystä suorituskykyindikaattoreista saadaan hyvin vähän tietoa niiden laskemiseen käytetyistä ehdoista sekä niiden vastaavuudesta tosielämän ehtojen kanssa. Tämä tarkoittaa, että niiden suorituskyky voisi tosielämässä olla odotettua heikompi, joten ne olisivat epätarkempia ja tuottaisivat enemmän vääriä positiivisia tuloksia. Joitakin näistä indikaattoreista käsitellään ehdotukseen liitettyssä vaikutustenarviointikertomuksessa⁵⁷.
64. Kolmanneksi suorituskykyindikaattoreita pitäisi käsitellä asiaankuuluvien tunnistamistyökalujen nimenomaisessa käyttötilanteessa, jolloin saadaan kattava näkemys tunnistamistyökalujen käyttäytymisestä. Kun tekoälyalgoritmeja käytetään kuviin tai tekstiin, voi esiintyä vinoumia tai syrjintää, koska tietyt väestöryhmät eivät ole kunnolla edustettuina algoritmin kouluttamiseen käytetyissä tiedoissa. Tämä ilmiö on dokumentoitu hyvin. Nämä vinoumat olisi tunnistettava ja mitattava ja ne olisi vähennettävä hyväksyttävälle tasolle, jotta tunnistamisjärjestelmistä olisi todellista hyötyä koko yhteiskunnalle.
65. Vaikka tunnistamiseen käytettävistä teknologioista on tehty tutkimus⁵⁸, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että nykyisten työkalujen luotettavuuden arvioimiseksi tarvitaan lisäanalyysia. Tässä analyysissa pitäisi hyödyntää kattavia suorituskykyindikaattoreita ja arvioida mahdollisten virheiden vaikutusta tosielämän oloissa ja kaikkien niiden rekisteröityjen osalta, joita ehdotus koskee.
66. Kuten edellä todetaan, Euroopan tietosuojaneuvostolla ja Euroopan tietosuojavaltuutetulla on vakavia epäilyksiä siitä, missä määrin ehdotuksen 7 artiklan 6 kohdassa säädetyillä menettelytakeilla pystytään tasapainottamaan näitä riskejä. Lisäksi, kuten edellä huomautettiin, ne panevat merkille, että ehdotuksessa käytetään melko abstrakteja ja epämääräisiä käsitteitä kuvaamaan riskin hyväksyttävää määrää (esim. ”merkittävässä määrin”).
67. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat huolissaan siitä, että nämä laajat ja epämääräiset käsitteet aiheuttavat oikeusvarmuuden puutetta ja saavat aikaan huomattavia eroja ehdotuksen käytännön täytäntöönpanossa unionissa. Eroja voi olla esimerkiksi siinä, miten jäsenvaltioiden oikeusviranomaiset tai muut riippumattomat hallintoviranomaiset tulkitsevat esimerkiksi käsitteitä ”todennäköisyys” ja ”merkittävässä määrin”. Tämä on huolestuttavaa myös siksi, että tunnistamismääräyksiä koskevat säännökset ovat sähköisen viestinnän tietosuojadirektiivin 5 artiklassa tarkoitettuja luottamuksellisuuden periaatteen rajoituksia. Ehdotetussa asetuksessa on siis parannettava niiden selkeyttä ja ennakoitavuutta.

4.5.6 Lapsen houkuttelun seksuaalisiin tarkoituksiin (ns. grooming) tunnistaminen

68. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että lapsen houkuttelun seksuaalisiin tarkoituksiin (ns. grooming) tunnistamista varten ehdotetuilla toimenpiteillä, joihin kuuluu puheen tai tekstin automaattista analyysia, puututaan todennäköisesti mitä huomattavimmin käyttäjien yksityis- ja perhe-elämää koskeviin oikeuksiin, myös viestinnän luottamuksellisuuteen, sekä henkilötietojen suojaan koskevaan oikeuteen.

⁵⁷ Vaikutustenarviointikertomus, liite 8, s. 281–283.

⁵⁸ Vaikutustenarviointikertomus, sivulta 279 eteenpäin.

69. Tiedossa olevan ja jopa uuden CSAM-materiaalin tunnistamisen soveltamisala voidaan rajoittaa kuvien ja videoiden analyysiin, mutta seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistaminen laajennettaisiin määritelmän mukaisesti kaikkeen tekstipohjaiseen viestintään (ja mahdollisesti ääniviestintään), joka kuuluu tunnistamismääräyksen soveltamisalaan. Näin kyseessä olevan viestinnän luottamuksellisuuteen puututaan paljon enemmän.
70. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että henkilöiden välisten viestintäpalvelujen kautta välitetyn tekstipohjaisen viestinnän mahdollisesta käytöstä seksuaalisiin tarkoituksiin tapahtuvaan lapsen houkutteluun tehtävä yleinen ja summittainen automaattinen analyysi ei tosiasiallisesti ole tarpeellisuuden ja oikeasuhteisuuden vaatimusten mukainen. Vaikka käytetty teknologia rajoitetaan indikaattorien käyttöön, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että tällaisen yleisen ja summittaisen analyysin käyttöönotto on liiallista ja voi jopa vaikuttaa perusoikeuskirjan 7 artiklassa tunnustetun yksityisyyttä koskevan perusoikeuden olennaiseen sisältöön.
71. Kuten on jo todettu, aineellisten takeiden puuttumista seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamistoimenpiteistä ei voida korvata pelkästään menettelytakeilla. Lisäksi riittävän oikeudellisen selkeyden ja oikeusvarmuuden puuttumista (eli epämääräisen lakikielen käyttöä, esim. ”merkittävässä määrin”) koskeva ongelma on vielä vakavampi tekstipohjaisen henkilökohtaisen viestinnän automaattisessa analyysissä kuin tiivistämisteknologiaan perustuvassa kuvien vertailussa.
72. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat lisäksi, että sananvapauteen kohdistuva ”lamaannuttava vaikutus” on erityisen merkittävä, kun ihmisten tekstiviestejä (tai ääniviestejä) tarkastetaan ja analysoidaan laajassa mittakaavassa. Ne muistuttavat, että tällainen lamaannuttava vaikutus on sitä vakavampaa, mitä epäselvempi laki on.
73. Lisäksi, kuten vaikutustenarviointikertomuksessa⁵⁹ ja Euroopan parlamentin tutkimuspalvelun tutkimuksessa⁶⁰ todetaan, tekstipohjaisen seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamisteknologioiden tarkkuustaso on paljon matalampi kuin tiedossa olevan CSAM-materiaalin tunnistamisteknologioiden⁶¹. Seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamistekniikoissa on tarkoitus analysoida keskustelun jokaista näkökohtaa ja antaa niille todennäköisyysluokitus. Siksi Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu myös katsovat niiden olevan alttiita virheille ja väärinkäytölle.

4.5.7 Pöytäkirja suositeltujen toimenpiteiden tarpeellisuudesta ja oikeasuhteisuudesta

74. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat suositeltujen tunnistamistoimenpiteiden tarpeellisuuden ja oikeasuhteisuuden osalta erityisen huolissaan aiemmin tuntemattoman CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun (ns. grooming) tunnistamiseen suunnitelluista toimenpiteistä. Tämä johtuu siitä, että näissä teknologioissa loukataan yksityisyyttä, koska niissä voidaan myöntää yleisluonteinen pääsy viestinnän sisältöön ja ne perustuvat todennäköisyyteen. Se johtuu myös niiden virhetasoista.
75. Unionin tuomioistuimen oikeuskäytännöstä voidaan lisäksi päätellä, että toimenpiteet, joiden nojalla viranomaiset pääsevät yleisesti viestinnän sisältöön, vaikuttavat todennäköisemmin perusoikeuskirjan 7 ja 8 artiklassa tunnustettujen oikeuksien keskeiseen sisältöön. Nämä näkökohdat

⁵⁹ Vaikutustenarviointikertomus, liite 8, s. 281–283.

⁶⁰ S. 15–18.

⁶¹ Ks. edellä, 40 kohta.

ovat erityisen merkityksellisiä myös seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamistoimenpiteissä, joita ehdotuksessa suunnitellaan.

76. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat joka tapauksessa, että erityisesti seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamista koskevien toimenpiteiden aiheuttama puuttuminen ylittää sen, mikä on ehdottoman välttämätöntä ja oikeasuhteista. Nämä toimenpiteet pitäisi siksi poistaa ehdotuksesta.

4.6 [Ilmoitusvelvoitteet](#)

77. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelevat, että ehdotuksen 13 artiklan luettelo ilmoituksista koskevista erityisvaatimuksista täydennetään vaatimuksella siitä, että ilmoitukseen sisällytetään tiedot nimenomaisesta teknologiasta, jonka avulla palveluntarjoaja on saanut tiedon asiaankuuluvasta väkivaltaisesta sisällöstä, mikäli palveluntarjoaja sai mahdollisen lapsiin kohdistuvan seksuaaliväkivallan tietoonsa toimenpiteillä, jotka on toteutettu ehdotuksen 7 artiklan mukaisesti annetun tunnistamismääräyksen täytäntöönpanoa varten.

4.7 [Poistamis- ja estovelvoitteet](#)

78. Yksi toimenpiteistä, joita ehdotuksessa suunnitellaan CSAM-materiaalin levittämisen riskien vähentämiseksi, on sellaisten poistamis- ja estomääräysten antaminen, joilla palveluntarjoajat veloitetaan poistamaan verkkovälitteinen lapsiin kohdistuvaa seksuaaliväkivaltaa todistava kuvamateriaali tai estämään sen käyttäminen tai estämään pääsy siihen⁶².
79. Vaikka poistamismääräysten vaikutus tietosuojaan ja viestinnän yksityisyyteen on melko vähäinen, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu muistuttavat yleisesti kokonaisvaltaisesta periaatteesta, jota on noudatettava, eli siitä, että kaikkien tällaisten toimenpiteiden on oltava mahdollisimman kohdennettuja.
80. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu kiinnittävät kuitenkin huomiota siihen, että internetpalvelujen tarjoajilla on pääsy vain sisällön täsmälliseen URL-osoitteeseen, jos sisältö annetaan saataville selkotekstinä. Aina, kun sisältö annetaan saataville https-yhteyshäytännön kautta, internetpalvelujen tarjoajilla ei ole pääsyä täsmälliseen URL-osoitteeseen, ellei se riko viestinnän salausta. Siksi Euroopan tietosuojaneuvostolla ja Euroopan tietosuojavaltuutetulla on epäilyksiä estotoimenpiteiden tehokkuudesta, ja ne katsovat, että olisi kohtuutonta vaatia internetpalvelujen tarjoajia avaamaan verkkoviestien salausta, jotta CSAM-materiaalia koskevat viestit voitaisiin estää.
81. Lisäksi ja yleisemmin ottaen olisi pantava merkille, että pääsyn estäminen digitaaliseen tuotteeseen (tai sen käytön estäminen) on verkon tasolla tehtävä toimi, jonka toteuttaminen voi osoittautua tehottomaksi, jos samasta tuotteesta on useita (mahdollisesti samankaltaisia mutta ei samanlaisia) kopioita. Tällainen toimi voi myös osoittautua suhteettomaksi, jos estäminen vaikuttaa muihin digitaalisiin tuotteisiin, jotka eivät ole lainvastaisia, kun ne on tallennettu samalle palvelimelle, jonka käyttö estetään käyttämällä verkkokäskyjä (esim. IP-osoite tai lisääminen nimipalvelun mustalle listalle). Kaikki verkkotason toimintamallit eivät myöskään ole

⁶² Ehdotus, 14 ja 16 artikla.

estämisessä yhtä tehokkaita, ja joitakin voi olla helppo kiertää melko perustason teknisillä taidoilla.

82. Ehdotetussa asetuksessa pitäisi myös selkeyttää koordinoivien viranomaisten valtuuksia estomääräysten antamisessa. Esimerkiksi 16 artiklan 1 kohdan ja 17 artiklan 1 kohdan nykyisestä sanamuodosta ei käy selväksi, onko koordinoivilla viranomaisilla valtuudet antaa estomääräyksiä vai vain pyytää niiden antamista⁶³.

4.8 Asiaankuuluvat teknologiat ja takeet

4.8.1 Sisäänrakennettu ja oletusarvoinen tietosuojaja

83. Ehdotuksen vaatimukset, joita sovelletaan CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamiseksi käyttöön otettaviin teknologioihin, eivät vaikuta riittävän tiukoilta. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat erityisesti panneet merkille, että ehdotuksessa ei – toisin kuin väliaikaisen asetuksen⁶⁴ vastaavissa säännöksissä – viitata yksiselitteisesti sisäänrakennettua ja oletusarvoista tietosuojaa koskevaan periaatteeseen eikä säädetä, että viestien tekstin seulomiseen käytettäessä teknologioilla ei pidä voida päätellä viestien varsinaista sisältöä. Ehdotuksen 10 artiklan 3 kohdan balakohdassa säädetään vain, että teknologioilla ei pidä voida ”poimia” asiaankuuluvasta viestinnästä muita tietoja kuin ne, jotka ovat ehdottoman välttämättömiä tunnistamista varten. Tämä vaatimus ei kuitenkaan vaikuta riittävän tiukalta, koska muita tietoja voi olla mahdollista *päätellä* viestinnän varsinaisesta sisällöstä *poimimatta* niitä itse viestinnästä.
84. Siksi Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelevat sisällyttämään ehdotuksen johdanto-osan kappaleen, jonka mukaan asetuksen (EU) 2016/679 25 artiklassa tarkoitettua sisäänrakennettua ja oletusarvoista tietosuojaa sovelletaan ehdotuksen 10 artiklan nojalla säänneltyihin teknologioihin lain nojalla. Sitä ei siksi tarvitse toistaa säädösoosassa. Myös 10 artiklan 3 kohdan b alakohtaa pitäisi muuttaa, jotta voidaan varmistaa, että sen lisäksi, että muita tietoja ei poimita, niitä ei myöskään päätellä, kuten tällä hetkellä säädetään väliaikaisen asetuksen 3 artiklan 1 kohdan b alakohdassa.

4.8.2 Teknologioiden luotettavuus

85. Ehdotuksessa oletetaan, että palveluntarjoajat voivat käyttää useita eri teknologiaratkaisuja tunnistamismääräysten täytäntöönpanoon. Ehdotuksessa oletetaan erityisesti, että muun kuin tiedossa olevan CSAM-materiaalin ja seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamiseen on saatavilla ja käytettävissä tekoälyjärjestelmiä⁶⁵ ja että jotkin koordinoivat viranomaiset voisivat pitää niitä parhaana käytettävissä olevana tekniikkana. Vaikka ehdotuksen tehokkuus perustuu näiden teknisten ratkaisujen luotettavuuteen, tekniikoiden yleisestä ja

⁶³ Ehdotuksen 16 artiklan 1 kohdassa lukee: ”Sijoittautumispaikan koordinoivalla viranomaisella on oltava valtuudet pyytää sen nimenneen jäsenvaltion toimivaltaista oikeusviranomaista tai kyseisen jäsenvaltion riippumatonta hallintoviranomaista antamaan estomääräys”, kun taas 17 artiklan 1 kohdassa lukee: ”Sijoittautumispaikan koordinoivan viranomaisen on annettava 16 artiklassa tarkoitettujen estomääräykset [...]” (alleviivaukset lisätty).

⁶⁴ Väliaikainen asetus, 3 artiklan 1 kohdan b alakohta.

⁶⁵ Ks. vaikutustenarviointikertomus, s. 281–282

järjestelmällisestä käytöstä on hyvin vähän tietoa saatavilla, minkä vuoksi sitä on pohdittava huolellisesti.

86. Lisäksi, vaikka Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun piti käyttää ehdotukseen liitettyssä vaikutustenarviointikertomuksessa mainittuja tunnistamisteknologioiden suorituskykyindikaattoreita oikeasuhteisuuden arvioinnissa, koska vaihtoehtoja ei ollut, on pantava merkille, että kertomuksesta saadaan hyvin vähän tietoa siitä, miten niitä on arvioitu ja kertovatko ne asiaankuuluvien teknologioiden todellisesta suorituskyvystä. Testeistä tai vertailukohtista, joita teknologian myyjät ovat käyttäneet suorituskyvyn mittaamisessa, ei ole tietoja. Ilman tällaisia tietoja testejä ei voida toistaa eikä arvioida suorituskyvystä annettujen lausuntojen pätevyyttä. Tämän osalta olisi pantava merkille, että vaikka suorituskykyindikaattoreita voitaisiinkin tulkita niin, että niiden mukaan jotkin tunnistamistyökalut ovat erittäin tarkkoja (esimerkiksi tiettyjen seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamistyökalujen tarkkuus on 88 prosenttia)⁶⁶, näitä indikaattoreita olisi arvioitava sen perusteella, miten tunnistamistyökaluja on tarkoitus hyödyntää käytännössä, ja sen mukaan, miten vakavia riskejä kyseisen materiaalin virheellinen arviointi aiheuttaisi asianomaisille rekisteröidyille. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat lisäksi, että tällaisessa suuririskisessä käsittelyssä 12 prosentin virheosuus on suuri riski rekisteröidyille, jotka voivat saada vääriä positiivisia tuloksia, siitäkin huolimatta, että käytössä on takeita, joilla estetään vääriä ilmoitukset lainvalvontaan. On erittäin epätodennäköistä, että palveluntarjoajat pystyisivät sitomaan riittävästi resursseja niin monien väärin positiivisten tulosten tarkastamiseen.
87. Kuten edellä mainitaan ⁶⁷, suorituskykyindikaattoreista pitäisi saada tyhjentävä näkemys tunnistamistyökalujen käyttäytymisestä. Kun tekoälyalgoritmeja käytetään kuviin tai tekstiin, voi esiintyä vinoumia tai syrjintää, koska tietyt väestöryhmät eivät ole kunnolla edustettuina algoritmin kouluttamiseen käytetyissä tiedoissa. Tämä ilmiö on dokumentoitu hyvin. Nämä vinoumat olisi tunnistettava ja mitattava ja ne olisi vähennettävä hyväksyttävälle tasolle, jotta tunnistamisjärjestelmistä olisi todellista hyötyä koko yhteiskunnalle.
88. Vaikka tunnistamiseen käytettävistä teknologioista on tehty tutkimus⁶⁸, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että nykyisten työkalujen luotettavuuden arvioimiseksi riippumattomasti ja tosielämän käyttötapauksissa tarvitaan lisäanalyysia. Tässä analyysissa pitäisi hyödyntää kattavia suorituskykyindikaattoreita ja arvioida mahdollisten virheiden vaikutusta tosielämän oloissa ja kaikkien niiden rekisteröityjen osalta, joita ehdotus koskee. Koska nämä teknologiat ovat perusta, jolle ehdotus on laadittu, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että analyysi on erittäin tärkeää ehdotuksen asianmukaisuuden arvioimiseksi.
89. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat myös, että ehdotuksessa ei määritellä teknologiakohtaisia vaatimuksia virhetasoille, luokittimien käytölle ja niiden vahventamiselle tai muille rajoituksille. Näin tällaisten vaatimusten laatiminen jää tehtäväksi käytännössä, kun arvioidaan tietyn teknologian käytön oikeasuhteisuutta. Se puolestaan vähentää entisestään täsmällisyyttä ja selkeyttä.
90. Koska väärin positiivisten tulosten seuraukset rekisteröidyille ovat merkittäviä, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että väärin positiivisten tulosten

⁶⁶ Ks. edellinen alaviite, s. 283.

⁶⁷ Ks. edellä 63 ja 64 kohta.

⁶⁸ Ks. vaikutustenarviointi kertomus, sivulta 279 eteenpäin.

osuutta on pienennettävä minimiin ja että kyseisten järjestelmien suunnittelussa on pidettävä mielessä, että valtavaan enemmistöön sähköisestä viestinnästä ei sisälly mitään CSAM-materiaalia eikä seksuaalisiin tarkoituksiin tapahtuvaa lapsen houkuttelua. Siinä on pidettävä mielessä myös se, että hyvinkin pieni väärin positiivisten tulosten osuus voi tarkoittaa erittäin monia vääriä positiivisia tuloksia tunnistettavien tietojen määrän mukaan. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu ovat yleisemmin ottaen huolissaan myös siitä, että vaikutustenarviointikertomuksessa mainittujen käytettävissä olevien työkalujen suorituskyky ei perustu täsmällisiin ja vertailukelpoiin indikaattoreihin väärin positiivisten ja väärin negatiivisten tulosten osuuksista. Ne katsovat myös, että kyseisille teknologioille olisi laadittava vertailukelpoisia ja tarkoituksenmukaisia suorituskykyindikaattoreita, ennen kuin niiden voidaan katsoa olevan saatavilla ja tehokkaita.

4.8.3 Ääniviestinnän seulominen

91. Toisin kuin väliaikaisessa asetuksessa⁶⁹, ehdotuksen soveltamisalasta ei suljeta pois ääniviestinnän seulomista seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamisen yhteydessä⁷⁰. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että ääniviestinnän seulominen on erityisen yksityisyyttä loukkaavaa, koska se tavallisesti edellyttää aktiivista, jatkuvaa ja ”suoraa” kuuntelua. Joissakin jäsenvaltioissa myös suojellaan erityisesti puheen yksityisyyttä⁷¹. Lisäksi siksi, että periaatteessa kaikki ääniviestinnän sisältö olisi analysoitava, tämä toimenpide vaikuttaa todennäköisesti perusoikeuskirjan 7 ja 8 artiklassa tunnustettujen oikeuksien keskeiseen sisältöön. Tämä tunnistamisenmenetelmä pitäisi siis jättää pois ehdotetussa asetuksessa esitetystä tunnistamiselvöitteiden soveltamisalasta sekä ääniviestien että suoran viestinnän osalta etenkin siksi, että ehdotukseen liitettyssä vaikutustenarviointikertomuksessa ei määritelty mitään tiettyjä riskejä tai uhkaympäristön muutoksia, joilla sen käyttö voitaisiin perustella.⁷²

4.8.4 Iän tarkistaminen

92. Ehdotuksessa kannustetaan palveluntarjoajia käyttämään iän tarkistusta ja arviointia koskevia toimenpiteitä palvelujensa lapsikäyttäjien tunnistamista varten⁷³. Tämän osalta Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että tällä hetkellä ei ole olemassa teknistä ratkaisua, jonka avulla voitaisiin arvioida varmasti verkkosivustojen käyttäjän ikä, jos ei hyödynnetä virallista digitaalista henkilöllisyyttä, joka ei ole vielä tässä vaiheessa kaikkien EU:n kansalaisten käytettävissä⁷⁴. Näin ollen ehdotuksessa suunniteltu iän tarkistamista koskevien toimenpiteiden käyttö voisi johtaa siihen, että verkkopalvelujen käytön ulkopuolelle suljetaan esimerkiksi nuorelta näyttävät aikuiset tai että otetaan käyttöön yksityisyyttä huomattavasti loukkaavia iäntarkistamistyökaluja, mikä voisi estää asianomaisten palvelujen lainmukaisen käytön tai vähentää sitä.
93. Vaikka ehdotuksen johdanto-osan 16 kappaleessa viitataan vanhempien käyttöön tarkoitettuihin valvontavälineisiin mahdollisina lieventävinä toimenpiteinä, Euroopan tietosuojaneuvosto ja

⁶⁹ Ks. väliaikainen asetus, 1 artiklan 2 kohta.

⁷⁰ Ks. ehdotus, 1 artikla.

⁷¹ Ks. esim. Saksan rikoslaki, 201 §.

⁷² Ks. vaikutustenarviointikertomus.

⁷³ Ks. ehdotus, 4 artiklan 3 kohta, 6 artiklan 1 kohdan c alakohta ja johdanto-osan 16 kappale.

⁷⁴ Ks. esim. CNIL, lapsen iän ja vanhemman suostumuksen tarkistamista lapsen yksityisyys huomioiden koskeva suositus 7: Check the age of the child and parental consent while respecting the child's privacy (9.8.2021).

Euroopan tietosuojavaltuutettu suosittelevat tämän vuoksi, että ehdotettua asetusta muutetaan niin, että siinä annetaan palveluntarjoajien nimenomaan hyödyntää vanhempien käyttöön tarkoitettuja valvontavälineitä täydentämään iän tarkistamista tai sen vaihtoehtona.

4.9 Tietojen säilyttäminen

94. Ehdotuksen 22 artiklassa rajoitetaan tarkoituksia, joita varten ehdotuksen soveltamisalaan kuuluvat palveluntarjoajat voivat säilyttää asetuksessa esitettyjen veloitteiden noudattamiseksi toteutettujen toimenpiteiden yhteydessä käsiteltyjä sisältötietoja ja muita tietoja. Ehdotuksessa kuitenkin todetaan, että palveluntarjoajat voivat säilyttää näitä tietoja myös verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan tunnistamisteknologioiden tehokkuuden ja täsmällisyyden parantamiseksi tunnistamismääräyksen täytäntöönpanoa varten, mutta ne eivät saa tallentaa henkilötietoja sitä varten.⁷⁵
95. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että vain niiden palveluntarjoajien, jotka käyttävät omia tunnistamisteknologioitaan, pitäisi voida säilyttää tietoja teknologioiden tehokkuuden ja täsmällisyyden parantamiseksi, kun taas niiden, jotka käyttävät EU-keskuksen tarjoamia teknologioita, ei pitäisi voida käyttää tätä mahdollisuutta. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat lisäksi, että käytännössä voisi olla vaikeaa varmistaa, että mitään henkilötietoja ei tallenneta tätä tarkoitusta varten, koska valtaosa sisältötiedoista ja muista tunnistamistarkoituksia varten käsitellyistä tiedoista katsotaan todennäköiseksi henkilötiedoiksi.

4.10 Vaikutus salaukseen

96. Euroopan tietosuojaviranomaiset ovat jatkuvasti puhuneet vahvojen salaustyökalujen laajan saatavuuden puolesta ja vastustaneet kaikenlaisia takaportteja⁷⁶. Tämä johtuu siitä, että salaus on tärkeää sen varmistamisessa, että kaikkia ihmisoikeuksia voidaan käyttää verkossa ja verkon ulkopuolella⁷⁷. Salausteknologiat myötävaikuttavat myös perustavanlaatuisesti sekä yksityiselämän ja viestinnän luottamuksellisuuden kunnioittamiseen että innovointiin ja digitaalitalouden kasvuun. Digitaalitalous onkin riippuvaista näiden teknologioiden tarjoamasta korkeatasoisesta luottamuksesta ja luottamuksellisuudesta.
97. Henkilöiden välisessä viestinnässä päästä päähän -salaus on ratkaisevan tärkeä työkalu sähköisen viestinnän luottamuksellisuuden varmistamisessa, koska siinä estetään voimakkain teknisin suojoitimin kaikkien muiden kuin lähettäjän ja vastaanottajan (vastaanottajien), myös palveluntarjoajan, pääsy viestinnän sisältöön. Mikäli päästä päähän -salauksen käyttöä pyritään jollakin tavalla estämään tai vähentämään, palveluntarjoajille määrätään velvoite käsitellä sähköisen viestinnän tietoja muuta tarkoitusta varten kuin niiden palvelujen tarjoamiseksi tai niille määrätään velvoite välittää sähköistä viestintää ennakoivasti kolmansille osapuolille, se aiheuttaisi riskin siitä, että palveluntarjoajat tarjoavat vähemmän salattuja palveluja, jotta ne voivat noudattaa veloitteitaan paremmin. Tämä heikentäisi salauksen roolia yleisesti ja rapauttaisi EU:n kansalaisten perusoikeuksia kohtaan tuntemaa kunnioitusta. Olisi pantava merkille, että päästä päähän -salaus on yksi yleisimmin käytetyistä turvallisuustoimenpiteistä sähköisen viestinnän alalla, mutta muutkin

⁷⁵ Ehdotus, 22 artiklan 1 kohta.

⁷⁶ Ks. tietosuojatyöryhmän salausta koskeva lausunto Statement of the WP29 on encryption and their impact on the protection of individuals with regard to the processing of their personal data in the EU (11.4.2018).

⁷⁷ Ks. YK:n ihmisoikeusneuvosto, päätöslauselma 47/16 ihmisoikeuksien edistämisestä, suojelusta ja käyttämisestä verkossa, YK:n asiakirja A/HRC/RES/47/16 (26.7.2021).

tekniset ratkaisut (esim. muiden salausratkaisujen käyttö) voivat olla tai niistä voi tulla yhtä tärkeitä digitaalisen viestinnän luottamuksellisuuden varmistamisessa ja suojelussa. Niiden käyttöä ei siksi pitäisi estää tai vähentää.

98. Henkilöiden välisen sähköisen viestinnän kuunteluun ja analysointiin tarkoitettujen työkalujen käyttöönotto on perustavanlaatuisesti vastoin päästä päähän -salausta, jossa pyritään teknisesti takaamaan, että lähettäjän ja vastaanottajan välinen viestintä pysyy salassa.
99. Vaikka ehdotuksessa ei vahvistetakaan järjestelmällistä kuunteluelvoitetta palveluntarjoajille, pelkkä mahdollisuus siihen, että tunnistamismääräys voitaisiin antaa, vaikuttaa näin ollen luultavasti huomattavasti palveluntarjoajien tekemiin teknisiin valintoihin erityisesti, koska määräyksen noudattamisen määräaika on lyhyt ja sen noudattamatta jättämisestä koituu raskaita seuraamuksia⁷⁸. Käytännössä tämä voi johtaa siihen, että tietyt palveluntarjoajat lopettavat päästä päähän -salauksen käytön.
100. Ehdotuksesta mahdollisesti johtuva päästä päähän -salauksen käyttöä heikentävä tai estävä vaikutus on arvioitava huolellisesti. Kaikki päästä päähän -salauksen yksityisyyttä suojelevan luonteen kiertämiseen tarkoitetut tekniikat, jotka esitettiin ehdotukseen liitettyssä vaikutustenenarviointikertomuksessa, saivat aikaan turvallisuutta koskevia porsaanreikiä⁷⁹. Esimerkiksi asiakaspuolen seulonta⁸⁰ johtaisi luultavasti siihen, että salaamatonta sisältöä käytettäisiin ja käsiteltäisiin loppukäyttäjän laitteilla huomattavasti ja kohdentamattomasti. Tällainen luottamuksellisuuden huomattava heikkeneminen vaikuttaisi erityisesti lapsiin, koska tunnistamismääräykset koskevat todennäköisemmin heidän käyttämiään palveluja. Näin he joutuisivat alttiiksi seurannalle ja salakuuntelulle. Palvelinpuolen seulonta on sekin kuitenkin perustavanlaatuisesti yhteensopimaton päästä päähän -salauksen mallin kanssa, koska vertaisalattu viestintäkanava olisi rikottava, mikä johtaisi henkilötietojen massakäsittelyyn palveluntarjoajien palvelimilla.
101. Vaikka asetuksessa todetaan, että siinä ”jätetään asianomaisen palveluntarjoajan valittavaksi teknologiat, joita on käytettävä tunnistamismääräysten noudattamiseksi tehokkaasti, eikä tätä pitäisi tulkita niin, että se kannustaisi jonkin tietyn teknologian käyttöön tai estäisi sen”⁸¹, joidenkin tunnistamismääräysten rakenteellinen yhteensopimattomuus päästä päähän -salauksen kanssa on itse asiassa suuri jarru päästä päähän -salauksen käyttämiselle. Kykenemättömyydellä käyttää päästä päähän -salausta (joka edustaa tällä hetkellä viimeisintä kehitystä luottamuksellisuuden teknisessä takaamisessa) käyttäviä palveluja ja päästä niihin voisi olla lannistava vaikutus sananvapauteen ja sähköisten viestintäpalvelujen oikeutettuun yksityiseen käyttöön. Myös komissio tiedostaa CSAM-materiaalin tai seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamisen ja päästä päähän -salauksen haitallisen suhteen, kun se panee vaikutustenenarviointikertomuksessa⁸² merkille todennäköisyyden siihen, että päästä päähän -salauksen toteuttaminen Facebookissa vuonna 2023 lopettaisi Facebookin tekemän vapaaehtoisen seulonnan.

⁷⁸ Ks. ehdotus, 35 artikla.

⁷⁹ Ks. osa 4.2 julkaisussa Abelson, Harold, Ross J. Anderson, Steven M. Bellare, Josh Benaloh, Matt Blaze, John L. Callas, Whitfield Diffie, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Vanessa Teague and Carmela Troncoso, ”Bugs in our Pockets: The Risks of Client-Side Scanning”, *ArXiv abs/2110.07450* (2021).

⁸⁰ Asiakaspuolen seulonnalla tarkoitetaan laajasti ottaen järjestelmiä, jotka voivat seuloa viestien sisällöistä osuvia vastenmielisen sisällön tietokantaan ennen kuin viesti lähetetään aiottulle vastaanottajalle.

⁸¹ Ehdotus, johdanto-osan 26 kappale.

⁸² Vaikutustenenarviointikertomus, s. 27.

102. Sen varmistamiseksi, että ehdotetulla asetuksella ei heikennetä EU:n kansalaisten sähköisen viestinnän turvallisuutta tai luottamuksellisuutta, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että ehdotuksen täytäntöönpanoehtoissa olisi selkeästi todettava, että mitään ehdotetussa asetuksessa ei pitäisi tulkita niin, että sillä kiellettäisiin salaus tai heikennettäisiin sitä, väliaikaisen asetuksen johdanto-osan 25 kappaleen mukaisesti.

4.11 Valvonta, täytäntöönpano ja yhteistyö

4.11.1 Yleisen tietosuojasetuksen mukainen kansallisten valvontaviranomaisten rooli

103. Ehdotuksessa säädetään kansallisten koordinoivien viranomaisten verkoston perustamisesta. Se vastaisi ehdotetun asetuksen soveltamisesta ja täytäntöönpanon valvonnasta.⁸³ Vaikka ehdotuksen johdanto-osan 54 kappaleessa todetaan, että "[t]ämän asetuksen valvontaa ja täytäntöönpanoa koskevien sääntöjen ei pitäisi katsoa vaikuttavan tietosuojaviranomaisille asetuksen (EU) 2016/679 nojalla kuuluviin valtuuksiin ja toimivaltaan", Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että koordinoivien viranomaisten tehtävien ja tietosuojaviranomaisten tehtävien välistä suhdetta pitäisi säännellä paremmin ja että tietosuojaviranomaisille pitäisi antaa ehdotetussa asetuksessa näkyvämpi rooli.
104. Palveluntarjoajia pitäisi erityisesti vaatia kuulemaan tietosuojaviranomaisia yleisen tietosuojasetuksen 36 artiklassa tarkoitetussa ennakkokuulemismenettelyssä ennen minkään CSAM-materiaalin tai seksuaalisiin tarkoituksiin tapahtuvan lapsen houkuttelun tunnistamistoimenpiteiden käyttöönottoa, eikä vain sellaisten tunnistamistoimenpiteidellöin käytön yhteydessä, jotka liittyvät lapsen houkutteluun seksuaalisiin tarkoituksiin, kuten ehdotuksessa tällä hetkellä suunnitellaan⁸⁴. Kaikkien tunnistamistoimenpiteiden pitäisi katsoa aiheuttavan oletusarvoisesti suuren riskin, ja niille on siksi tehtävä ennakkokuulemismenettely riippumatta siitä, koskevatko ne lapsen houkuttelua seksuaalisiin tarkoituksiin vai CSAM-materiaalia, kuten on jo väliaikaisessa asetuksessa⁸⁵. Lisäksi yleisen tietosuojasetuksen nojalla nimetyillä toimivaltaisilla tietosuojaviranomaisilla pitäisi olla valtuudet esittää näkemyksensä suunnitelluista tunnistamistoimenpiteistä aina eikä vain erityisolosuhteissa⁸⁶.
105. Ehdotetussa asetuksessa olisi myös vahvistettava järjestelmä toimivaltaisten viranomaisten ja tietosuojaviranomaisten tunnistamismääräyksiä koskevien erimielisyyksien käsittelyä ja ratkaisemista varten. Tietosuojaviranomaisille pitäisi erityisesti antaa oikeus riitauttaa tunnistamismääräys sen antaneen toimivaltaisten oikeusviranomaisten tai riippumattomien hallintoviranomaisten jäsenvaltion tuomioistuimessa. Tämän osalta Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu panevat merkille, miten ehdotuksen nykyisessä versiossa toimivaltainen viranomainen voi tunnistamismääräystä antaessaan sivuuttaa toimivaltaisten tietosuojaviranomaisten lausunnon. Tämä voi johtaa ristiriitaisiin päätöksiin, koska tietosuojaviranomaisilla säilyvät yleisen tietosuojasetuksen 36 artiklan 2 kohdassa vahvistetun mukaisesti kaikki yleisen tietosuojasetuksen 68 artiklan mukaiset korjaavat toimivaltuudet, myös valtuudet määrätä käsittelykielto.

⁸³ Ehdotus, 25 artikla.

⁸⁴ Ehdotus, 7 artiklan 3 kohdan toisen alakohdan b alakohta.

⁸⁵ Väliaikainen asetus, 3 artiklan 1 kohdan c alakohta.

⁸⁶ Ks. ehdotus, 7 artiklan 3 kohdan toisen alakohdan c alakohta.

4.11.2 Euroopan tietosuojaneuvoston tehtävä

106. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu panevat merkille, että ehdotuksen 50 artiklan 1 kohdan kolmannen virkkeen mukaan ”EU-keskus pyytää teknologiakomitealtaan ja Euroopan tietosuojaneuvostolta lausunnon” ennen kuin se lisää tietyn teknologian luetteloon teknologioista, joita säilyttämispalvelujen ja henkilöiden välisten viestintäpalvelujen tarjoajat voivat harkita käyttävänsä tunnistamismääräysten täytäntöönpanoon. Siinä säädetään lisäksi, että Euroopan tietosuojaneuvoston on annettava lausuntonsa kahdeksan viikon kuluessa ja että määräaika voidaan tarvittaessa pidentää kuudella viikolla ottaen huomioon aiheen monimutkaisuus. Lopuksi siinä edellytetään, että Euroopan tietosuojaneuvoston on ilmoitettava EU-keskukselle tällaisesta pidennyksestä kuukauden kuluessa kuulemispyynnön vastaanottamisesta sekä viivästyksen syyt.
107. Tietosuojaneuvoston nykyisistä tehtävistä säädetään yleisen tietosuoja-asetuksen 70 artiklassa ja direktiivin (EU) 2016/680 51 artiklassa, jäljempänä ’rikosasioiden tietosuojadirektiivi’⁸⁷. Näiden tehtävien osalta todetaan, että Euroopan tietosuojaneuvosto antaa neuvontaa komissiolle sekä antaa lausuntoja komission, kansallisen valvontaviranomaisten tai puheenjohtajansa pyynnöstä. Vaikka ehdotuksen 1 artiklan 3 kohdan d alakohdassa todetaan, että ehdotus ei vaikuta yleisessä tietosuoja-asetuksessa ja rikosasioiden tietosuojadirektiivissä esitettyihin sääntöihin, EU-keskuksen valtuuttaminen pyytämään lausuntoja Euroopan tietosuojaneuvostolta ylittää Euroopan tietosuojaneuvostolle yleisessä tietosuoja-asetuksessa ja rikosasioiden tietosuojadirektiivissä osoitetut tehtävät. Siksi ehdotetussa asetuksessa – vähintään johdanto-osassa – olisi tehtävä selväksi, että ehdotuksella laajennetaan Euroopan tietosuojaneuvoston tehtäviä. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu arvostavat tämän osalta merkittävää roolia, joka ehdotuksessa osoitetaan tietosuojaneuvostolle, kun sitä pyydetään osallistumaan ehdotetun asetuksen käytännön täytäntöönpanoon. Käytännössä Euroopan tietosuojaneuvoston sihteeristöllä on olennainen rooli tietosuojaneuvoston lausuntojen antamiseen tarvittavan analyyttisen, hallinnollisen ja logistisen tuen antamisessa. Siksi on ratkaisevan tärkeää osoittaa Euroopan tietosuojaneuvostolle riittävät määrärahat ja henkilöstö, jotta voidaan varmistaa, että tietosuojaneuvosto ja sen jäsenet pystyvät täyttämään tehtävänsä. Valitettavasti ehdotuksen säädökseen liittyvässä rahoitus selvityksessä ei kuitenkaan ilmoiteta lisävaroista Euroopan tietosuojaneuvostolle ehdotuksessa osoitettujen lisätehtävien suorittamiseen⁸⁸.
108. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat myös, että ehdotuksen 50 artiklassa ei selitetä, miten EU-keskus etenee saatuaan tietosuojaneuvoston lausunnon⁸⁹. Ehdotuksen johdanto-osan 27 kappaleessa todetaan vain, että EU-keskuksen ja Euroopan komission olisi otettava Euroopan tietosuojaneuvoston neuvot huomioon. Siksi olisi selvennettävä, mikä tarkoitus pyydetävällä lausunnolla olisi ehdotuksen 50 artiklassa tarkoitettussa prosessissa ja miten EU-keskuksen on määrä toimia saatuaan tietosuojaneuvoston lausunnon.
109. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat lisäksi, että vaikka kaikissa Euroopan tietosuojaneuvoston ohjeissa tai mahdollisissa lausunnoissa tunnistamisteknologioiden käytöstä arvioidaan kyseisten teknologioiden käyttöä yleisellä tasolla, yleisen tietosuoja-asetuksen 36

⁸⁷ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston päätöksen 2008/977/YOS kumoamisesta (EUVL L 119, 4.5.2016, s. 89–131).

⁸⁸ Ks. ehdotus, sivulta 105 eteenpäin.

⁸⁹ Ks. vertailun vuoksi rikosasioiden tietosuojadirektiivin 51 artiklan 4 kohta.

artiklan mukaista ennakkokuulemista varten kansallisen valvontaviranomaisten on otettava huomioon erityiset olosuhteet ja tehtävä tapauskohtainen arviointi asiaankuuluvan rekisterinpitäjän tekemästä aiotusta käsittelystä. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että valvontaviranomaiset soveltavat ja niiden pitäisi soveltaa yleisen tietosuoja-asetuksen 36 artiklassa esitettyjä kriteereitä päättäessään, onko tarpeen jatkaa yleisessä tietosuoja-asetuksessa asetettua määräaika ennakkokuulemisen vuoksi annettavien lausuntojen antamiseen. Myöskään ei ole tarpeen soveltaa eri vaatimuksia, kun ennakkokuuleminen koskee tunnistamisteknologian käyttöä.⁹⁰

110. Tunnistamisvelvoitteita koskevia ohjeita koskevan 11 artiklan soveltamiseksi ehdotuksessa todetaan, että komissio voi antaa ohjeita ehdotuksen 7–10 artiklan soveltamisesta. Ehdotuksen 11 artiklaa olisi muutettava, jotta voidaan tehdä selväksi, että komission olisi koordinoivien viranomaisten ja EU-keskuksen lisäksi kuultava Euroopan tietosuojaneuvostoa ohjeluonnoksista, jotka eivät kuulu säädettyyn julkista kuulemista koskevaan prosessiin, ennen tunnistamisvelvoitteita koskevien ohjeiden antamista.
111. Lainsäätäjien on siksi arvioitava enemmän tätä Euroopan tietosuojaneuvoston tehtävää sekä sen roolia ehdotuksen nojalla käyttöön otettavassa oikeudellisessa kehyksessä.

4.11.3 Lapsiin kohdistuvan seksuaaliväkivallan EU-keskuksen rooli

112. Ehdotuksen IV luvun nojalla perustettaisiin EU-keskus, uusi erillisvirasto, jonka avulla ehdotus pantaisiin täytäntöön. Muiden tehtävien ohella EU-keskuksen olisi helpotettava luotettavien tunnistamisteknologioiden saatavuutta palveluntarjoajille, asetettava saataville indikaattoreita, jotka perustuvat jäsenvaltioiden tuomioistuinten tai riippumattomien hallintoviranomaisten todentamaan verkkovälitteiseen lapsiin kohdistuvaan seksuaaliväkivaltaan sen tunnistamista varten, antaa pyynnöstä tietynlaista apua riskinarviointien suorittamisessa ja tukea viestintää asiaankuuluvien kansallisten viranomaisten kanssa⁹¹.
113. Tämän osalta Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suhtautuvat myönteisesti ehdotuksen 77 artiklan 2 kohtaan, jossa vahvistetaan, että EU-keskuksen suorittamaan henkilötietojen käsittelyyn sovelletaan EU:n tietosuoja-asetusta, sekä säädetään, että toimenpiteet, joiden mukaisesti EU-keskus soveltaa kyseistä asetusta, mukaan lukien EU-keskuksen tietosuojavastaavan nimittämistä koskevat toimenpiteet, vahvistetaan Euroopan tietosuojavaltuutetun kuulemisen jälkeen. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat kuitenkin, että useita tämän luvun säännöksiä on syytä tarkastella lähemmin.
114. Ensinnäkin Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että ehdotuksen 48 artiklassa vaaditaan toimittamaan kaikki ilmoitukset, jotka eivät ole ”ilmeisen perusteettomia”⁹², kansallisille lainvalvontaviranomaisille ja Euroopan unionin lainvalvontayhteistyövirastolle (Europol). Tämä kynnysarvo sille, että EU-keskuksen on toimitettava ilmoitukset kansallisille lainvalvontaviranomaisille ja Europolille (”ei ilmeisen perusteettomia”),

⁹⁰ Ks. ehdotus, johdanto-osan 24 kappale.

⁹¹ Ks. COM(2022) 209 final, s. 7.

⁹² Käsite ”ilmeisen perusteeton” kuvataan ehdotuksen johdanto-osan 65 kappaleessa tapauksiksi, ”joissa on ilman perusteellista oikeudellista tai tosiasiallista analyysiäkin välittömästi ilmeistä, että ilmoitetut toimet eivät ole verkkovälitteistä lapsiin kohdistuvaa seksuaaliväkivaltaa”.

vaikuttaa liian matalalta erityisesti siksi, että EU-keskuksen perustamisen tarkoitus, kuten komission vaikutustenarviointikertomuksessa⁹³ todetaan, on lieventää lainvalvontaviranomaisten ja Europolin taakkaa virheellisesti CSAM-materiaaliksi merkityn sisällön suodattamisessa. Tämän kannalta on epäselvää, miksi EU-keskus, joka on asiantuntemuskeskus, ei voisi tehdä perusteellisempaa oikeudellista ja tosiasiallista arviointia, jotta voidaan vähentää riskiä siitä, että syyttömien ihmisten tiedot toimitetaan lainvalvontaan.

115. Toiseksi säännös siitä, miten kauan henkilötietoja pidetään tallessa EU-keskuksessa, vaikuttaa melko avoimelta kyseisten tietojen arkaluonteisuus huomioon ottaen. Vaikka ei olisi mahdollista asettaa enimmäissäilytysaikaa kyseisten tietojen tallentamiselle, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelivat, että ehdotuksessa asetetaan vähintään enimmäismääräaika tietojen tallentamisen säilyttämisen tarpeellisuuden arvioinnille ja vaaditaan perusteluja säilyttämisen jatkamiselle sen jälkeen.
116. Koska EU-keskuksessa käsiteltävät henkilötiedot ovat lisäksi erittäin arkaluonteisia, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu katsovat, että käsittelyyn pitäisi soveltaa lisätakeita, erityisesti tehokkaan valvonnan varmistamiseksi. Tätä varten EU-keskus voitaisiin velvoittaa pitämään lokia tietoja koskevista automaattisten käsittelyjärjestelmien käsittelytoimista (eli toistettaisiin EU:n tietosuoja-asetuksen IX luvun mukainen operatiivisia henkilötietojen koskeva vaatimus), muun muassa kirjaamalla henkilötietojen syöttäminen, muuttaminen, käyttö, hakeminen, luovuttaminen, yhdistäminen ja poistaminen. Hakuja ja luovutuksia koskevista lokeista on pystyttävä todentamaan kyseisten toimien perusteet sekä toteutuspäivä ja -aika, operatiivisia henkilötietoja hakeneen tai luovuttaneen henkilön tiedot ja mahdollisuuksien mukaan vastaanottajien henkilöllisyys. Lokeja käytettäisiin käsittelyn lainmukaisuuden todentamiseen, omavalvontaan ja käsittelyn eheyden ja turvallisuuden varmistamiseen. Lokit olisivat EU-keskuksen tietosuojavastaavan ja Euroopan tietosuojavaltuutetun saatavilla pyynnöstä.
117. Ehdotuksessa viitataan lisäksi palveluntarjoajien velvollisuuteen ilmoittaa käyttäjille CSAM-materiaalin tunnistamisesta tunnistamismääräyksen avulla sekä oikeudesta tehdä kantelu koordinoivalle viranomaiselle⁹⁴. Ehdotuksessa ei kuitenkaan säädetä menettelyistä, jotka koskevat rekisteröityjen oikeuksien käyttämistä niin, että siinä otetaan myös huomioon useat paikat, joihin henkilötietoja voidaan ehdotuksen mukaan toimittaa ja joissa niitä voidaan säilyttää (EU-keskus, Europol, kansalliset lainvalvontavirastot). Vaatimukseen käyttäjille ilmoittamisesta pitäisi kuulua velvoite ilmoittaa henkilölle, että heidän tietonsa on toimitettu eteenpäin ja, soveltuvin osin, että niitä käsittelevät eri tahot (esim. kansalliset lainvalvontaviranomaiset tai Europol). Käytössä pitäisi lisäksi olla keskitetty menettely käyttöoikeuksia, oikaisua ja poistamista koskevien pyyntöjen vastaanottamista ja koordinoitua varten tai vaihtoehtoisesti velvoite siitä, että rekisteröidyn pyynnön saanut taho vastaa koordinoinnista muiden asianomaisten tahojen kanssa.
118. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu panevat merkille, että ehdotuksen 50 artiklan mukaan EU-keskuksen tehtävänä on laatia luettelo teknologioista, joita voidaan käyttää tunnistamismääräysten täytäntöönpanoon. Ehdotuksen 12 artiklan 1 kohdan mukaan palveluntarjoajien on kuitenkin ilmoitettava kaikki tiedot, jotka osoittavat sen palveluissa olevan mahdollista verkkovälitteistä lapsiin kohdistuvaa seksuaaliväkivaltaa, eikä vain tunnistamismääräyksen täytäntöönpanosta johtuvia tietoja. On erittäin luultavaa, että tällaisia tietoja

⁹³ Ks. esimerkiksi vaikutustenarviointikertomuksen sivu 349.

⁹⁴ Ks. ehdotuksen 10 artiklan 6 kohta ja sen jälkeen, kun ilmoitus on toimitettu EU-keskukselle, ehdotuksen 12 artiklan 2 kohta.

tulisi huomattava määrä palveluntarjoajien ehdotuksen 4 artiklassa tarkoitettujen lieventävien toimenpiteiden käytöstä. Siksi vaikuttaa olevan ratkaisevan tärkeää määrittää se, mitä nämä toimenpiteet voisivat olla, niiden tehokkuus, niiden virhetaso mahdollisesta lapsiin kohdistuvasta seksuaaliväkivallasta ilmoittamisesta sekä se, miten ne vaikuttavat ihmisten oikeuksiin ja vapauksiin. Huolimatta siitä, että ehdotuksen 4 artiklan 5 kohdassa todetaan, että komissio voi yhteistyössä koordinoivien viranomaisten ja EU-keskuksen kanssa ja julkisen kuulemisen jälkeen antaa asiaankuuluvia ohjeita, Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun mielestä on tärkeää, että lainsäätäjä sisällyttää 50 artiklaan EU-keskuksen tehtäväksi laatia myös luettelon suositeltavista lieventävistä toimenpiteistä ja asiaankuuluvista parhaista käytännöistä, jotka ovat erityisen tehokkaita mahdollisen lapsiin kohdistuvan seksuaaliväkivallan tunnistamisessa. Koska tällaisilla toimenpiteillä voidaan puuttua tietosuoja ja yksityisyyttä koskeviin perusoikeuksiin, suositellaan myös, että EU-keskus pyytää Euroopan tietosuojaneuvostolta lausuntoa ennen tällaisen luettelon laatimista.

119. Myös ehdotuksen 51 artiklan 4 kohdassa esitettyjen turvallisuusvaatimusten tulisi olla täsmällisempiä. Siinä voidaan ottaa esimerkkiä turvallisuusvaatimuksista, joista on säädetty muissa asetuksissa, jotka koskevat laaja-alaisia järjestelmiä, joihin liittyy suuririskistä käsittelyä. Niitä ovat muun muassa asetus 767/2008⁹⁵ (ks. 32 artikla), asetus 1987/2006⁹⁶ (ks. 16 artikla), asetus 2018/1862⁹⁷ (ks. 16 artikla) ja asetus 603/2013⁹⁸ (ks. 34 artikla).

4.11.4 Europolin rooli

120. Ehdotuksessa säädetään EU-keskuksen ja Europolin tiiviistä yhteistyöstä. Ehdotuksen IV luvun mukaan, kun EU-keskus on saanut palveluntarjoajilta ilmoituksia epäilyistä CSAM-materiaalista, se tarkastaa ne ja arvioi, mitkä ilmoitukset ovat täytäntöönpanokelpoisia (eivät ilmeisen perusteettomia), ja toimittaa ne eteenpäin Europolille sekä kansallisille lainvalvontaviranomaisille⁹⁹. EU-keskus antaa Europolille pääsyn indikaattori- ja ilmoitustietokantoihinsa tarkoituksena tukea

⁹⁵ Euroopan parlamentin ja neuvoston asetus (EY) N:o 767/2008, annettu 9 päivänä heinäkuuta 2008, viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta (EUVL L 218, 13.8.2008, s. 60–81).

⁹⁶ Euroopan parlamentin ja neuvoston asetus (EY) N:o 1987/2006, annettu 20 päivänä joulukuuta 2006, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä (EUVL L 381, 28.12.2006, s. 4–23).

⁹⁷ Euroopan parlamentin ja neuvoston asetus (EU) 2018/1862, annettu 28 päivänä marraskuuta 2018, Schengenin tietojärjestelmän (SIS) perustamisesta, toiminnasta ja käytöstä poliisiyhteistyössä ja rikosasioissa tehtävässä oikeudellisessa yhteistyössä, neuvoston päätöksen 2007/533/YOS muuttamisesta ja kumoamisesta sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 1986/2006 ja komission päätöksen 2010/261/EU kumoamisesta (EUVL L 312, 7.12.2018, s. 56–106).

⁹⁸ Euroopan parlamentin ja neuvoston asetus (EU) N:o 603/2013, annettu 26 päivänä kesäkuuta 2013, Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta annetun asetuksen (EU) N:o 604/2013 tehokkaaksi soveltamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksessa tehtäviä vertailuja koskevista pyynnöistä sekä vapauden, turvallisuuden ja oikeuden alueen laaja-alaisen tietojärjestelmien operatiivisesta hallinnoinnista vastaavan eurooppalaisen viraston perustamisesta annetun asetuksen (EU) N:o 1077/2011 muuttamisesta (EUVL L 180, 29.6.2013, s. 1–30).

⁹⁹ Ks. ehdotuksen 48 artikla.

Europolia epäiltyjen lapsiin kohdistuvien seksuaalirikosten tutkinnassa¹⁰⁰. EU-keskus antaa lisäksi Europolille ”mahdollisimman laajan pääsyn” tietojärjestelmiinsä¹⁰¹. Virastot jakavat keskenään myös tiloja ja joitakin (muuta kuin operatiivisia) infrastruktuureita¹⁰².

121. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat, että useat näkökohdat ehdotetun EU-keskuksen ja Europolin välisessä yhteistyössä herättävät huolta ja edellyttävät tarkennuksia.

Ilmoitusten toimittaminen EU-keskuksesta Europolille (48 artikla)

122. Ehdotetun asetuksen 48 artiklassa vaaditaan EU-keskusta toimittamaan ilmoitukset, jotka eivät ole ilmeisen perusteettomia, ja kaikki merkitykselliset lisätiedot Europolille ja sen jäsenvaltion toimivaltaiselle lainvalvontaviranomaiselle tai toimivaltaisille lainvalvontaviranomaisille, joka todennäköisesti on toimivaltainen tutkimaan mahdollista lapsiin kohdistuvaa seksuaaliväkivaltaa tai nostamaan siitä syytteen. Vaikka tässä artiklassa annetaan Europolille tehtäväksi määrittää asiaankuuluva lainvalvontaviranomainen, jos asianomainen jäsenvaltio ei ole selvillä, säännöksellä itse asiassa tarkoitetaan, että kaikki ilmoitukset on toimitettava Europolille riippumatta siitä, onko kansallista viranomaista määritetty ja onko EU-keskus jo toimittanut ilmoituksen.
123. Ehdotuksessa ei kuitenkaan selvennetä, mitä lisäarvoa saataisiin Europolin osallistumisesta tai sen odotetusta roolista, kun ilmoitukset on otettu vastaan. Tämä koskee erityisesti tapauksia, joissa kansallinen lainvalvontaviranomainen on määritetty ja sille on ilmoitettu samaan aikaan.¹⁰³
124. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu muistuttavat, että Europolin toimeksianto rajoittuu jäsenvaltioiden toimivaltaisten viranomaisten toimien tukemiseen ja niiden keskinäiseen yhteistyöhön kahteen tai useampaan jäsenvaltioon vaikuttavien vakavien rikosten ehkäisyssä ja torjumisessa¹⁰⁴. Asetuksen (EU) 2016/794¹⁰⁵, sellaisena kuin se on muutettuna asetuksella (EU) 2022/991¹⁰⁶, jäljempänä ’muutettu Europol-asetus’, 19 artiklassa säädetään, että unionin elimen, joka toimittaa tietoja Europolille, on määritettävä niiden käsittelytarkoitus Europolissa sekä käsittelyn ehdot. Se vastaa myös siirrettyjen henkilötietojen paikkansapitävyydestä¹⁰⁷.

¹⁰⁰ Ks. ehdotuksen 46 artiklan 4 ja 5 kohta.

¹⁰¹ Ks. ehdotuksen 53 artiklan 2 kohta.

¹⁰² Erityisesti henkilöstöhallintoon, tietotekniikkaan, muun muassa kyberturvallisuuteen, rakennuksiin ja viestintään liittyviä.

¹⁰³ Ehdotuksen johdanto-osan 71 kappaleessa viitataan vain yleisesti Europolin kokemukseen toimivaltaisten kansallisten viranomaisten määrittämisestä epäselvissä tilanteissa ja sen rikostiedustelutietojen tietokantaan, joka voi auttaa tunnistamaan yhteyksiä muissa jäsenvaltioissa tehtäviin tutkimuksiin.

¹⁰⁴ Ks. muutetun Europol-asetuksen 3 artikla.

¹⁰⁵ Euroopan parlamentin ja neuvoston asetus (EU) 2016/794, annettu 11 päivänä toukokuuta 2016, Euroopan unionin lainvalvontayhteistyövirastosta (Europol) sekä neuvoston päätösten 2009/371/YOS, 2009/934/YOS, 2009/935/YOS, 2009/936/YOS ja 2009/968/YOS korvaamisesta ja kumoamisesta (EUVL L 135, 24.5.2016, s. 53–114).

¹⁰⁶ Euroopan parlamentin ja neuvoston asetus (EU) 2022/991, annettu 8 päivänä kesäkuuta 2022, asetuksen (EU) 2016/794 muuttamisesta siltä osin kuin on kyse Europolin yhteistyöstä yksityisten osapuolten kanssa, Europolin suorittamasta henkilötietojen käsittelystä rikostutkimusten tukemiseksi sekä Europolin roolista tutkimuksessa ja innovoinnissa (EUVL L 169, 27.6.2022, s. 1–42).

¹⁰⁷ Ks. muutetun Europol-asetuksen 38 artiklan 2 kohdan a alakohta.

125. Ilmoitusten kattava toimittaminen Europolille olisi siksi ristiriidassa muutetun Europol-asetuksen kanssa ja aiheuttaisi useita tietosuojariskejä. Henkilötietojen käsittelyn kaksinkertaistaminen voisi johtaa siihen, että samaan aikaan tallennetaan useita kopioita samoista erittäin arkaluonteisista henkilötiedoista (esim. EU-keskuksessa, Europolissa, kansallisessa lainvalvontaviranomaisessa). Se aiheuttaisi riskejä tietojen paikkansapitävyydestä, koska tietokantoja ei ehkä ole synkronoitu, sekä rekisteröityjen oikeuksien käytölle. Lisäksi ehdotuksen matala kynnyisarvo (ei ilmeisen perusteettomien) ilmoitusten jakamiselle lainvalvontaviranomaisten kanssa merkitsee, että Europolin tietojärjestelmiin tallennetaan erittäin todennäköisesti vääriä positiivisia tuloksia (esim. virheellisesti lapsiin kohdistuvaksi seksuaaliväkivallaksi merkittyä sisältöä) mahdollisesti pitkiksi ajoiksi.¹⁰⁸
126. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelevat siksi, että ehdotuksessa täsmennetään ja rajoitetaan olosuhteita, joissa EU-keskus voisi toimittaa ilmoitukset Europolille muutetun Europol-asetuksen mukaisesti, ja tarkoituksia, joita varten niitä voitaisiin toimittaa. Siitä pitäisi yksiselitteisesti jättää pois olosuhteet, joissa ilmoitukset on toimitettu asiaankuuluvalla jäsenvaltion valvontaviranomaiselle, sillä siitä käy ilmi, että rajatylittävää ulottuvuutta ei ole. Ehdotukseen pitäisi lisäksi sisällyttää vaatimus siitä, että EU-keskus siirtää henkilötietoja Europolille vain, kun se on asianmukaista, merkityksellistä ja rajoitettu siihen, mikä on ehdottoman välttämätöntä. Lisäksi on säädettävä erityistakeista tietojen laadun ja luotettavuuden varmistamiseksi.

¹⁰⁸ Komission vaikutustenarviointikertomuksen mukaan Europol on pystynyt tutkimaan vain 20 prosenttia tietokannassaan olevasta 50 miljoonasta yksittäisestä CSAM-kuvasta ja -videosta, mikä kertoo siitä, että sillä ei resursseja käsitellä tällä hetkellä saamaansa CSAM-aineistoa. Ks. Impact Assessment Report accompanying the Proposal for a Regulation laying down rules to prevent and combat child sexual abuse, SWD(2022)209, s. 47–48.

Ehdotuksen 53 artiklan 2 kohta EU-keskuksen ja Europolin välisestä yhteistyöstä

127. Ehdotuksen 53 artiklan 2 kohdassa edellytetään, että Europol ja EU-keskus antavat toisilleen ”mahdollisimman laajan pääsyn asiaankuuluviin tietoihin ja tietojärjestelmiin, jos se on tarpeen niiden tehtävien suorittamiseksi ja tällaista pääsyä koskevien unionin säädösten mukaista”.
128. Ehdotuksen 46 artiklan 4 ja 5 kohdassa täsmennetään lisäksi, että Europolilla on pääsy EU-keskuksen indikaattori- ja ilmoitustietokantoihin, ja 46 artiklan 6 kohdassa säädetään menettelystä, jolla pääsy myönnetään. Europol toimittaa pyynnön, jossa täsmennetään pyydetyn pääsyn tarkoitus ja se, missä määrin pääsy on tarpeen tämän tarkoituksen täyttämiseksi. EU-keskus arvioi pyynnön huolellisesti.
129. Europolin pääsystä EU-keskuksen tietojärjestelmiin ja niistä saatujen tietojen myöhemmältä käytöltä edellytetyt kriteerit ja takeita ei ole selvennetty. Vaille selitystä jää myös se, miksi Europolille on tarpeen myöntää suora pääsy muun kuin lainvalvontaviraston tietojärjestelmiin, joissa on erittäin arkaluonteisia henkilötietoja, joiden yhteyttä rikolliseen toimintaan ja rikosten ehkäisyyn ei ehkä ole vahvistettu. Jotta voidaan varmistaa korkeatasoinen tietosuojajärjestelmä ja käyttötarkoituksen rajoittamisen periaatteen noudattaminen, Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelevat, että henkilötietoja siirretään EU-keskuksesta Europoliin vain tapauskohtaisesti huolellisesti arvioitun pyynnön perusteella SIENAn¹⁰⁹ kaltaisen suojatun tiedonvaihtoverkkosovelluksen kautta.
130. Ehdotuksen 53 artiklan 2 kohdassa on ehdotuksen ainoa viittaus EU-keskuksen pääsyyn Europolin tietojärjestelmiin. Siksi on epäselvää, mitä tarkoituksia varten ja minkä nimenomaisten takeiden mukaisesti tällainen pääsy toteutuisi.
131. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu muistuttavat, että Europol on EU:n perussopimuksilla perustettu lainvalvontavirasto, jonka ydintehtävänä on vakavien rikosten ehkäisy ja torjunta. Europolin käsittelemiin operatiivisiin henkilötietoihin sovelletaan siksi tiukkoja tietojenkäsittelysääntöjä ja -takeita. Ehdotettu EU-keskus ei ole lainvalvontaelin, eikä sille pitäisi missään olosuhteissa myöntää suoraa pääsyä Europolin tietojärjestelmiin.
132. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu huomauttavat lisäksi, että suuri osa molempien virastojen kannalta merkittävistä tiedoista koskevat väitetyjen rikosten uhreihin liittyviä henkilötietoja, alaikäisten henkilötietoja ja sukupuolielämää koskevia henkilötietoja, jotka kuuluvat muutetun Europol-asetuksen mukaan erityisiin henkilötietoryhmiin. Muutetussa Europol-asetuksessa säädetään tiukat ehdot erityisiin henkilötietoryhmiin pääsulle. Muutetun Europol-asetuksen 30 artiklan 3 kohdassa säädetään, että ainoastaan Europolilla saa olla suora pääsy kyseisiin henkilötietoihin. Tarkemmin pääsy on pääjohtajan valtuuttamalla rajoitetulla joukolla Europolin virkamiehiä.¹¹⁰
133. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelevat siksi, että ehdotuksen 53 artiklan 2 kohdan sanamuotoa selkeytetään, jotta siinä otetaan asianmukaisesti huomioon muutetun Europol-asetuksen nojalla voimassa olevat rajoitukset, ja täsmennetään EU-keskukseen pääsyä koskevia ehtoja. Erityisesti kaikki pääsy Europolin tietojärjestelmissä käsiteltäviin henkilötietoihin olisi, kun se katsotaan ehdottoman välttämättömäksi EU-keskuksen tehtävien suorittamiselle, myönnettävä vain tapauskohtaisesti nimenomaisten tarkoituksen ja perustelut

¹⁰⁹ Suojattu tiedonvaihtoverkkosovellus (SIENA).

¹¹⁰ Muutetussa Europol-asetuksessa tähän kieltoon tehdään poikkeuksia SEUT-sopimuksen V osaston nojalla perustetuille unionin virastoille. Ehdotuksen oikeusperusta (SEUT-sopimuksen 114 artikla sisämarkkinoiden yhdenmukaistamisesta) huomioon ottaen tämä poikkeus ei kuitenkaan sisältäisi ehdotettua EU-keskusta.

esittävän yksiselitteisen pyynnön perusteella. Europolin pitäisi arvioida kyseiset pyynnot huolellisesti ja toimittaa EU-keskukselle henkilötietoja ainoastaan, kun se on ehdottoman välttämätöntä ja oikeassa suhteessa pyydettyyn tarkoitukseen nähden.

Ehdotuksen 10 artiklan 6 kohta Europolin roolista käyttäjille ilmoittamisessa tunnistamismääräyksen täytäntöönpanon jälkeen

134. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suhtautuvat myönteisesti ehdotuksen 10 artiklan 6 kohdassa esitettyyn vaatimukseen siitä, että palveluntarjoajien on ilmoitettava tunnistamismääräyksen täytäntöönpanosta käyttäjille, joiden henkilötietoja se voi koskea. Nämä tiedot on annettava käyttäjille vasta sen jälkeen, kun Europolilta tai 48 artiklassa tarkoitetun ilmoituksen vastaanottaneen jäsenvaltion kansalliselta lainvalvontaviranomaiselta on saatu vahvistus, että tietojen antaminen käyttäjille ei haittaa lapsiin kohdistuvien seksuaalirikosten ehkäisemistä, tunnistamista ja tutkimista koskevia toimia tai niihin liittyviä syytöksiä.
135. Säännöksen käytännön täytäntöönpanosta on kuitenkin epäselvyyttä. Jos ilmoitukset toimitetaan sekä Europolille että jäsenvaltion lainvalvontaviranomaiselle, ehdotuksessa ei kerrota, tarvitaanko vahvistus yhdeltä vastaanottajalta vai molemmilta. Ehdotuksessa ei myöskään esitetä menettelyjä/ehtoja tämän vahvistuksen saamiseksi (esim. onko vahvistukset kanavoitava EU-keskuksen kautta). Koska Europolin ja kansallisten lainvalvontaviranomaisten on mahdollisesti käsiteltävä suuria määriä CSAM-materiaalia ja koska vahvistuksen antamiselle ei ole tarkkaa määräaikaakaan ("ilman aiheutonta viivytystä"), Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelivat, että sovellettavia menettelyjä selvennetään, jotta tämän takeen toteutuminen käytännössä voidaan varmistaa. Lisäksi veloitteeseen käyttäjille ilmoittamisesta pitäisi sisältyä tiedot kyseisten henkilötietojen vastaanottajista.

Tietojen kerääminen ja läpinäkyvyysraportointi (83) artikla

136. Ehdotuksen 83 artiklan 3 kohdassa säädetään, että EU-keskus kerää tietoja ja laatii tilastoja ehdotetun asetuksen mukaisten tehtäviensä lukumäärästä. Valvontaa varten Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suosittelivat, että tähän tilastoluetteloon lisätään Europolille 48 artiklan mukaisesti toimitettujen ilmoitusten lukumäärä sekä Europolin 46 artiklan 4 ja 5 kohdan mukaisesti saamien pääsyyntöjen lukumäärä, mukaan lukien niiden pyyntöjen lukumäärä, joissa EU-keskus myönsi tai epäsi pääsyn.

5. PÄÄTELMÄT

137. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu suhtautuvat myönteisesti komission pyrkimykseen varmistaa tehokkaat toimet verkkovälitteisen lapsiin kohdistuvan seksuaaliväkivallan torjumiseksi, mutta ne katsovat, että ehdotus herättää useita vakavia huolenaiheita tietosuojasta ja yksityisyydestä. Siksi Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu kehottavat lainsäätäjiä muuttamaan ehdotettua asetusta erityisesti sen varmistamiseksi, että suunnitellut tunnistamisveloitteet täyttävät sovellettavat tarpeellisuutta ja oikeasuhteisuutta koskevat vaatimukset eivätkä heikennä tai huononna salausta yleisesti. Euroopan tietosuojaneuvosto ja Euroopan tietosuojavaltuutettu voivat edelleen antaa tukeaan lainsäädäntöprosessin aikana, jos tässä yhteisessä lausunnossa esiin tuotujen huolenaiheiden käsittelyssä tarvitaan niiden apua.

Euroopan tietosuojavaltuutetun puolesta

Euroopan tietosuojaneuvosto

Euroopan tietosuojavaltuutettu

Puheenjohtaja

(Wojciech Wiewiorowski)

(Andrea Jelinek)