Teknologiateollisuus

Finnish Information Security Cluster
Kyberala

17.10.2024

Eduskunta
Hallintovaliokunta

Viite: U 69/2022 vp

Lausunto: Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final)

Kiitämme mahdollisuudesta lausua asiasta. Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka tekevät puolet Suomen viennistä ja tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyber- ja tietoturvallisuusalaa. Haluamme kiinnittää huomiota seuraaviin seikkoihin:

Tiivistelmä

Ehdotuksella on hyväksyttävä ja erittäin painava tavoite suojata lapsia verkkovälitteiseltä seksuaaliväkivallalta. Hallituksen pyrkimys vakivallattoman lapsuuden turvaamiseksi ja vakavien rikosten uhreina olevien lasten suojelemiseksi on kannatettava. Eduskunta on edellyttänyt, että asetuksessa säädettävien toimenpiteiden tulee olla riittävän tehokkaita ja samalla ennakoitavia, oikeassa suhteessa ja välttämättömiä ehdotuksen tavoitteen toteutumiseksi. Nyt ehdotettu toteutustapa tavoitteiden saavuttamiseksi olisi kuitenkin edelleen hyvin haitallinen muiden perusoikeuksien suojaamiselle, olisi seurauksiltaan ennakoimaton sisältäen suuria yleisen tietoturvan heikennyksiä sekä rikollista toimintaa harjoittavien järjestelmän kiertämispyrkimyksiä. Erityisen ongelmallisen asiasta tekee se, että ehdotus olisi tehoton asetettujen tavoitteiden saavuttamiselle:

- Ehdotus ei suojaa lapsia seksuaaliselta hyväksikäytöltä
- Ehdotus perusoikeuksien rajoittamisesta ei ole tarpeellisuus- ja suhteellisuusperiaatteen mukainen
- Ehdotus ei mahdollista poliittisten tavoitteiden saavuttamista
- Ehdotus on ensimmäinen vaihe sähköisen viestinnän luottamuksellisuuden ja yksityisyyden ydinalueen murentamiselle
- Ehdotus uhkaa yhteiskunnan kokonaisturvallisuutta
- Ehdotus on voimassa olevan EU-oikeuden vastainen
- Suomen tulisi edistää vähemmän haitallisia ja tehokkaita ratkaisuja lasten suojelemiseen

Ehdotus ei suojaa lapsia seksuaaliselta hyväksikäytöltä

Verkkovälitteinen seksuaaliväkivalta voidaan jakaa kahdenlaiseen toimintaan: seksuaaliväkivaltaa todistavan materiaalin levittämiseen verkossa sekä ”groomingiin” eli verkkohoukutteluun. Verkkohoukuttelussa on kyse manipulatiivisesta menettelystä, jossa aikuinen luo alaikäiseen luottamussuhteen tarkoituksenaan valmistella heitä seksuaaliseen hyväksikäyttöön.

Keskeisin kohde lasten suojelemiseen väkivallalta on aikuisten suorittama hyväksikäyttömateriaalin tuottaminen, jossa alaikäinen on välittömästi rikollisen teon kohde. Unkarin ehdotuksesta on rajattu pois sekä verkkohoukuttelun torjunta, että uuden seksuaaliväkivaltaa todistavan materiaalin tunnistaminen (res. 23a–28, art. 7). Ehdotus ei siis estäisi uusien kuvien tai muun materiaalin tuottamista. Ainoa soveltamisalaan sisällytetty tekotapa on jo olemassa olevan materiaalin edelleen jakaminen käyttäjältä toiselle. Materiaalin

Eteläranta 10, PL 10, 00131 Helsinki

edelleen jakamiseen liittyen ei voida puhua uhrien välittömästä suojelemisesta. Lakiehdotuksen edellisen käsittelykierroksen aikana Perustuslakivaliokunta kiinnitti huomiota siihen, että houkuttelun torjunnalla olisi kaikkein myönteisin vaikutus mahdollisten uhrien perusoikeuksiin, koska se edistäisi parhaiten hyväksikäytön ehkäisemistä.

Lisäksi on tärkeä huomata, että tekijät jakavat materiaaliaan pääsääntöisesti pimeän verkon kautta ja yleisten viestintäsovellusten tai alustojen kautta jaettava materiaali on vain pieni osa kokonaisuutta. Tämä tosiasia on laajasti tunnettu sekä verkkoturvallisuuden edistäjien että lainvalvontaviranomaisten keskuudessa. Ehdotus ei myöskään ulottuisi samalla tavalla tavanomaisiin tietokoneisiin (kuten läppäreitä ja pöytäkoneita), joita käytetään yleisesti hyväksikäyttöaineiston laittomaan käsittelyyn sekä myös viestintäpalveluiden hyödyntämiseen (esim. Messenger, verkkopelialustat, Discord, Microsoft Teams sekä WhatsApp/WhatApp for Business).

Kielletyn materiaalin tunnistamiseen käytettäisiin ns. hashing-teknologiaa, eli kuva- tai videotiedostoista lasketaan kiinteän pituinen merkkijono, ns. yksilöllinen tunniste (ts. tiiviste). Teknologian tehokkuus on kuitenkin edelleen kyseenalainen, sillä tiedoston muokkaus muuttaa sen tunnistetta ja siten heikentää tekniikan luotettavuutta merkittävästi. Tunnisteen muuttuminen johtaa sekä siihen, että laitonta sisältöä ei tunnisteta. Tehokkaiden tekoälyjärjestelmien saatavuus tarjoaa ennennäkemättömiä mahdollisuuksia etsiä tunnistuksen kiertämiseen soveltuvia tekniikoita. Esimerkiksi vaikka komission viittaaman kuvien ja videoiden tunnistamiseen käytetyn PhotoDNA -ohjelman virhemarginaali olisikin pieni on osoitettu, että vähäinenkin kuvan muuttaminen muuttaa myös sen tunnistetta niin, että tunnistus voidaan kiertää. Myös Applen vastaava algoritmi, jota kehitettiin usean vuoden ajan, osoitettiin tutkijoiden toimesta kierrettäväksi vain kahdessa viikossa.

Ehdotus perusoikeuksien rajoittamisesta ei ole tarpeellisuus- ja suhteellisuusperiaatteen mukainen

Hyvin tunnettuun ns. posti- ja kirjemaailmaan verrattuna ehdotus tarkoittaisi käytännössä, että Suomessa Posti tarkastaisi lähetettävien kirjeiden sisällön postilaatikkoon jätettäessä ja lähettäisi tarvittaessa kopion lainvalvontaviranomaiselle. Tässä mallissa kirjesalaisuutta turvaavilla toimilla eli kirjekuoreen sulkemisella ei olisi enää merkitystä. Näin ollen yksityiselämän suojaa ja viestintäsalaisuutta (ml. kirjesalaisuus) heikennettäisiin perustavanlaatuisesti, mikäli ehdotus hyväksyttäisiin esitetyssä muodossa. Kuvien ja videoiden tutkiminen ennen salausta heikentää yksityisen viestinnän tarkoitusta ja kiertäisi tosiasiallisesti oikeutta salauksen käyttöön yksityisyyden suojan sekä viestinnän yksityisyyden turvaajana (perustuslaki 10 §:n 4 momentti). Tämä koskisi myös yritysten välistä ja työelämässä käytävää luottamuksellista viestintää.

Ehdotetusta sääntelystä ei ole annettu olennaista tietoa Euroopan unionin perusoikeuskirjan ja kansainvälisten ihmisoikeussopimusten, kuten Euroopan ihmisoikeussopimuksen valossa. Euroopan ihmisoikeustuomioistuin julkaisi helmikuussa 2024 ratkaisunsa asiassa Podchasov v. Venäjä, jossa tuomioistuin katsoi, että päästä-päähän ulottuvan salauksen (E2EE) kieltäminen, heikentäminen tai murtaminen rikkoo ihmisoikeuksia. Tapauksessa Venäjän turvallisuuspalvelu FSB vaati viestipalvelu Telegramia luovuttamaan rikoksesta epäiltyjen käyttäjien salattuja viestejä. Ratkaisussa käsitellään laajasti Yhdistyneiden kansakuntien (YK), EU:n tuomioistuimen, EU:n kyberturvallisuusvirasto ENISA:n, Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun kannanotot ja päätökset aiheesta. Näistä esimerkiksi YK:n mukaan vahva oikeus yksityiseen (salattuun) viestintään ylittää punnintatilanteessa lasten suojelun tai rikosten selvittämisen tarpeen. Vaikka YK:n lapsen oikeuksien sopimusta sekä lasten suojelemisesta seksuaalista riistoa ja seksuaalista hyväksikäyttöä vastaan tehtyä Euroopan neuvoston yleissopimusta (ns. Lanzaroten sopimus) on pidettävä hyvin tärkeinä, niidenkin ydinvelvoite ovat

tehokkaat toimet lasten suojaamiseksi väkivallalta. Ehdotus alittaa sekä tehokkuuden edellytyksen, että ylittää muiden perusoikeuksien rajoitusedellytykset.

Perustusvaliokunta on edellyttänyt, että perustuslain 10 §:n 4 momentin säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiin kuuluvasta välttämättömyysvaatimuksesta seuraa, että luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee olla mahdollisimman kohdennettua ja rajattua (PeVL 35/2018 vp, s. 12). Valiokunta on erikseen todennut, että perustuslain 10 §:n 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa (PeVM 4/2018 vp, s. 7—8).

Lisäksi valiokunta kiinnitti käsillä olevan ehdotuksen edellisellä käsittelykerralla huomiota siihen, että ehdotuksen mukaisia tunnistamismääräyksiä ei ole rajattu tiettyihin henkilöihin, jolloin sääntelyn soveltaminen voi siten muodostua varsin laajaksi ja yksilöimättömäksi. Lisäksi valiokunta on pitänyt vakiintuneena jo vuosikymmeniä varsin johdonmukaisesti sitä, että rikoksen tutkintana pidetään sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn takia, vaikka rikos ei olisi vielä edennyt toteutuneen teon asteelle. Näiltä osin ehdotus ei tosiasiallisesti ole muuttunut aiemmasta. Vaikka ehdotus olisikin laittoman materiaalin tunnistamisessa tarkempi (rajaus ns. ”korkeariskisiin” palveluntarjoajiin sekä visuaaliseen sisältöön ja linkkeihin, tunnistamismääräys viimesijaisena keinona sekä ajallisen keston rajaaminen) se olisi silti poikkeuksellisen laajaa ja yksilöimätöntä eikä perustuisi konkreettiseen ja yksilöityyn rikosepäilyyn.

On erittäin tärkeää havaita, että viestintäpalveluissa välitettävien viestien määrä on valtava. Yksistään WhatsApp-palvelu välittää maailmanlaajuisesti n. 100 miljardia viestiä päivässä. Kun lasketaan muut palvelut mukaan, kuten iMessage (n. 1 mrd, Microsoft Teams (n. 300 milj.), Discord (n. 4 mrd), Telegram (150 mrd, joista kuvia ja videoita 1,7 mrd) jne. voidaan todeta, että yksityisten viestien päivittäinen määrä on vähintään n. 260 miljardia. Tämä tarkoittaa sitä, että kuva- ja videotiedostoja olisi arviolta ainakin 1% kaikissa viesteissä eli 2,6 miljardissa, päivittäin. Kaikista viesteistä pelkästään 1 promilleen kohdistettu tunnistamismääräys tarkoittaisi silti 260 miljoonan viestin tutkimista päivittäin. Lienee selvää, että kyseessä ei voi olla rajattu ja yksilöity valvonnan kohdistaminen. Myös Tietosuojavaltuutettu on pitänyt käytännössä kaikkien palvelun käyttäjien kuva- ja videomateriaalin tutkimista kohdentamattomana.

Päästä-päähän-salaus tarkoittaa, että kukaan muu kuin viestin lähettäjä ja tarkoitetut vastaanottajat eivät voi lukea viestejä tai muuten analysoida niitä päätelläkseen viestin sisältöä. Näin ollen myöskään viestejä välittävä palveluntarjoaja tai muu taho ei voi tietää viestin sisältöä, vaikka viestit kulkevat sen tietojärjestelmien kautta. Eduskunta on aiemmassa asiaa koskevassa johtopäätöksissä edellyttänyt, ettei valvonta edes ”*tosiasiassa johda päästä päähän salauksen tai muiden vastaavien tietoturvatoimenpiteiden yleiseen heikentämiseen tai niiden purkamisen taikka niiden käytön rajoittamiseen ja tätä kautta viestinnän sekä viestintään liittyvien palvelujen tietoturvan ja kyberturvallisuuden tason heikkenemiseen*”. Mikäli palveluntarjoajilla tai muilla tahoilla on mahdollisuus tutkia merkittävä osa viesteistä ja niiden sisällöstä, kyseessä ei ole päästä päähän salaus.

Lisäksi on tärkeää huomioida, että suhteellisuusperiaatteen kannalta on merkityksetöntä, että tunnistamismääräys kohdistettaisiin vain verkkopalveluntarjoajiin, joissa on todettu korkea riski laittoman materiaalin levittämiselle. Suojellaan Lapsia ry:n toteuttamassa tutkimuksessa[1] lapsiin kohdistuvaa seksuaaliväkivaltaa todistavaa kuvamateriaalia hyödyntävät rikoksentekijät nimesivät suosituimpina palveluina Instagramin, Facebookin, WhatsAppin, Signalin, Discordin

[1] https://www.suojellaanlapsia.fi, 20.2.2024.

sekä Telegramin. Käytännössä korkean riskin verkkopalveluntarjoajia, joihin tunnistamismääräyksiä kohdistettaisiin suosittuihin kaikkien kansalaisten työ- ja vapaa-ajan tarkoituksiin käyttämiin alustoihin ja sovelluksiin.

Vastaavasti suhteellisuusperiaatteen kannalta merkityksetöntä on, että tunnistamismääräys olisi kansallisen tuomioistuimen antama, ajallisesti rajattu viimesijainen keino, joka kohdistuisi vain visuaaliseen sisältöön ja pitäisi sisällään myös toimenpiteen valvonnan ja raportoinnin. Ensinnäkin tuomioistuimen antama määräys olisi edelleen sekä kohdentamatonta että yksilöimätöntä ja kohdistuisi väistämättä valtavaan määrään henkilöitä ja viestejä. Viimesijaisuuden vaatimusta voidaan pitää lähinnä toiveajatteluna ja käytännössä menettelystä tulisi ensisijainen. Tuomioistuimella ei olisi mitään muuta keinoa valvoa menettelyn asianmukaisuutta, kuin tiedustella poliisiviranomaiselta mitä muuta ilmiön suhteen on jo tehty, jolloin vastauksena annettaisiin vakiomuotoisesti, että muut keinot eivät ole olleet tehokkaita (koska lähes kaikki viestintäpalvelut ovat korkean riskin kohteita ja niissä epäillään harjoitettavan edelleen laitonta toimintaa).

Olennaista on myös havaita, että vastoin Sisäministeriön asiakirjoista syntyvää vaikutelmaa, viestinnän valvonta ei kohdistu vain kuviin ja videoihin, vaan myös verkkolinkkeihin (URL). Verkkolinkit ovat viestien tekstisisältöön kuuluvia merkkijonoja, joiden yhdistelmä muodostaa tietokoneelle ohjeen siirtyä tiettyyn verkko-osoitteeseen (internet-sivu tms.). Näin ollen voidaan perustellusti todeta, että viestien valvonta kohdistuu myös itse viestin sisältöön eikä yksinomaan ns. kuva- tai videotiedostoihin.

Välttämättömyysperiaate edellyttää, että perusoikeuksiin kohdistuvat rajoitukset ovat sallittuja vain, jos ne ovat välttämättömiä tavoitteen saavuttamiseksi. Rajoituksia voidaan käyttää vain, jos tavoitetta ei voida saavuttaa vähemmän puuttuvin keinoin. Yllä on osoitettu, että ehdotus ei ole tehokas lasten hyväksikäytön torjumiseksi verkkoympäristössä. Lisäksi laajamittainen viestinnän valvonta aiheuttaisi tutkijoiden[2] mukaan erittäin suuren määrän vääriä tuloksia, jossa jokainen näistä johtaisi viestin lähettäjään kohdistuvaan vakavaan rikosepäilyyn. Tutkijat ja tieteenharjoittajat sekä kyberturvallisuuden ja tietosuojan asiantuntijat ovat ehdottaneet lukuisia vähemmän haitallisia keinoja hyväksikäytön rajoittamiseksi. Vastaavasti viestintäpalveluiden tarjoajat ovat ottaneet käyttöön monia toimiviksi osoittautuneita menetelmiä, joista lisää alla.

Näin ollen ehdotus ei täytä perusoikeuksien rajoitusedellytyksiä. Ehdotus jää parhaimmillaankin hyvin rajalliseksi lapsen edun näkökulmasta. Vastapainona punninnassa oleva lähes kaikkiin viestintäpalveluihin ja -sovelluksiin kohdistetun laajamittaisen valvonnan ei voida hyvällä tahdollakaan ajatella olevan ehdottoman tarpeellista eikä suhteellisuusperiaatteen mukaista.

Ehdotus ei mahdollista Suomen poliittisten tavoitteiden saavuttamista

Lakiehdotuksessa on kyse rikosilmiön oireiden hoitamisesta tehottomin keinoin ja samalla vahingollisten seurausten syntymisestä muualla. Ehdotus ei ole hallitusohjelman suuntaviivojen mukainen. Ehdotuksella on toki hyväksyttävä ja tärkeä pyrkimys suojata lapsia verkkovälitteiseltä seksuaaliväkivallalta. Tavoitetta ei tule kuitenkaan toteuttaa niin, että luottamuksellisuuden ja yksityisyyden tason heikentämisen lisäksi vaarantuvat myös lapsen oikeudet.

Hallitusohjelman mukaan kriminaalipolitiikan tavoitteena on rikosten ehkäiseminen, rikoksentekijöiden saattaminen vastuuseen teoistaan sekä uhrien auttaminen ja tukeminen

[2] Open letter on the position of scientists and researchers on the updated version of the EU's proposed Child Sexual Abuse Regulation https://homes.esat.kuleuven.be/~preneel/Open_letter_CSAR_aug24_still_unacceptable.pdf

(hallitusohjelman s. 195). Viestinnän yksityisyyden perustavanlaatuinen heikentäminen ei täytä mitään näistä tavoitteista. Lapsiin kohdistuvan seksuaaliväkivallan torjunnan tulee perustua lasten välittömästi uhriksi joutumisen estämiseen, ei vain sitä kuvaavan materiaalin tai sen jakelun poistamiseen. Tehokkaita menetelmiä, joita esimerkiksi YK suosittelee ja jotka voisivat olla käsittelyssä olevan asetuksen piirissä ovat mm. alustoille asetettavat velvoitteet haitallisten havaintojen käyttäjäpohjaisen turvallisuusraportoinnin esille tuontiin sekä turvallisuuslähtöisten design-periaatteiden noudattamiseen.

Suomi yhdessä EU:n ja Yhdysvaltojen ehdottivat viime vuonna korkean tason periaatteita lasten ja nuorten suojelusta ja vaikutusmahdollisuuksien lisäämisestä digitaalisessa ympäristössä. Ne vaativat hallituksia noudattamaan kansainvälisen oikeuden asettamia ihmisoikeusvelvoitteita, mukaan lukien verkkoympäristöön liittyvät toimet ja käytännöt sekä yksityisyyteen liittyvät lailliset velvoitteet.

Hallitusohjelman mukaan ”Oikeusvaltion ytimessä on kansalaisten luottamus oikeudenmukaisesti toimivaan yhteiskuntaan ja oikeusjärjestelmään.” (s. 175). Näin ollen rikosprosessia tulisi kehittää siihen suuntaan, että rikoksiin syyllistyneet myös tuomittaisiin tehokkaasti. Tämä tarkoittaa sitä, että rikoksentekijöiden vastuuseen saattamiseksi tulisi kohdentaa jo annettuja esitutkintatoimivaltuuksia ja -resursseja. Käytännössä syyttäjät ja tuomioistuimet tarvitsevat myös lisäresursseja vaikeita ja kansainvälisiä ulottuvuuksia (monikansalliset viestintäpalveluyhtiöt sekä käyttäjien sijainti eri valtioiden alueella) sisältävien juttujen huolelliseen käsittelyyn sekä rikosprosessin hallinnolliseen tehostamiseen. Nyt käsillä oleva ehdotus ei tue näitä tavoitteita, vaan aiheuttaa päinvastaisen seurauksen lainvalvontaresurssien kohdistamisesta laajan verkkovalvonnan tuloksena syntyvän virhetietoa sisältävän tietomassan käsittelyyn.

Hallitusohjelman mukaan lapseen kohdistuvan seksuaaliväkivallan tapauksissa varmistetaan lapsen edun mukainen tutkinta ja monialainen tuki eri viranomaisten yhteistyönä (hallitusohjelman s. 195). Oikeus viestinnän luottamuksellisuuteen on lapsen edun mukaista. Esimerkiksi Euroopan tietosuojaneuvoston ja tietosuojavaltuutetun jo elokuussa 2022 antaman yhteisen lausunnon mukaan tunnistamismääräykset voisivat ”jopa vahingoittaa ihmisiä, joita niillä pyritään suojelemaan. Ne voivat heikentää huomattavasti viestinnän luottamuksellisuutta, koska ne altistaisivat palveluja käyttävät alaikäiset tarkkailulle tai salakuuntelulle”.

Ehdotus on ensimmäinen vaihe sähköisen viestinnän luottamuksellisuuden ja yksityisyyden ydinalueen murentamiselle

Europol ja kaikkien jäsenmaiden lainvalvontaviranomaisten johtajat julkaisivat keväällä 2024 yhteisen julistuksen, jonka tavoitteena on käytännössä murtaa salaus eli yksityisyyden suoja kaikelta viestinnältä. Tämä julistus nojaa Ruotsin puheenjohtajakaudella laadittuihin tavoitteisiin ja nyt käsillä onkin Ruotsin nimeämän komissaarin ehdotus, joka on päälinjoiltaan muiden EU:n digitaalisen turvallisuuden politiikkatoimien kanssa ristiriitainen.

Nyt ehdotetaan viestiliikenteen valvontaa ja tarkistamista lasten seksuaalisen hyväksikäytön torjunnan näkökulmasta, myöhemmin jonkin muun rikoslajin tai vaikkapa Venäjän uhan perusteella. Poliittisille päättäjille on turvallisuuden nimissä harhaanjohtavasti perusteltu yksittäisten toimien tarpeellisuutta viestinnän valvonnan laajentamiseksi. Turvallisuuden ”edistämisen” houkutus usein osoittautunut suureksi. Esimerkkeinä tästä ovat mm. Suomen poliisin pyrkimykset päästä käyttämään biometrisen tunnistamisen (passirekisteri) tietoja rikosten selvittämiseen, vaikka alun perin valmistelussa oli edellytetty yksinomaan, että tiedot kansalaisista kerätään vain henkilöllisyystodistuksiin liittyvää tunnistamista varten. Vastaavasti hiljakkoin tiedustelulakien arvioinnin yhteydessä Sisäministeriö esitti tiedustelukeinojen käytön

avulla kerättyjen tietojen käyttämistä myös rikostorjuntaan. Sisäministeriö esitti muutosta, vaikka Eduskunta hyväksyi perustuslain muutoksen sekä tiedustelulait sillä ehdolla, että tietoja kerätään yksinomaan valtion turvallisuustiedustelun tarpeisiin, koska laajan tarkkailun ja tietojen keräämisen taustalla ei ole rikosepäilyä.

Unkarin ehdotus vaarantaakin myös Suomen maineen korkean digitaalisen luottamuksen ja perusoikeudet takaavana maana, mikä väistämättä heikentää yksityistä omistajuutta, liiketoimintaa ja investointihalukuutta, sillä myös elinkeinotoiminta nojaa vahvasti oikeussubjektien oikeuteen viestiä ja siirtää tietoa luottamuksellisesti osapuolten välillä.

Kun viestinnän valvonta on kerran otettu käyttöön kaikkien viestintäpalveluissa, olisi hyvin houkuttelevaa ja helppoa laajentaa valvonta kaikkiin laitteeseen tallennettuihin kuviin tai laajentaa tunnistetietokantaa uudella, esimerkiksi muiden rikoslakien liittyvällä sisällöllä ilman avointa demokraattista arviointia. Unkarin muotoilussa komissiolle ehdotetaankin suoraa täytäntöönpanovaltaa hyväksyä teknologiat, joita voidaan käyttää tunnistamismääräysten toteuttamisessa. Saksa, Hollanti ja moni muu EU-jäsenvaltio on todennutkin selvästi, että lakiehdotuksella ei ole paikkaa demokraattisessa oikeusvaltiossa.

Ehdotus uhkaa yhteiskunnan kokonaisturvallisuutta

Viestien sisällön tekninen valvonta ja tunnistus edellyttämällä päästä päähän salausta käyttäviä viestintäpalveluita mahdollistamaan välitettävien viestien läpivalaisu jo viestijän päätelaitteessa aiheuttaa merkittävän ja ratkaisemattoman riskin Suomelle kahdella tavalla: ensinnäkin järjestelmä mahdollistaisi valtioiden välisen tiedustelun laajentamisen toisten valtioiden oikeudenkäyttöpiiriin sekä laajamittaisen laittoman vakoilun pahantahtoisille valtioille, kuten Venäjä ja Kiina. Liikenne- ja viestintävaliokunta on aiemmassa lausunnossaan (LiVL 5/2023 vp, 5.3.2024) ilmaissut, että tietoturvan tason heikentämistä ei voi toteuttaa vain kotimaan turvallisuusviranomaisten tarpeita varten. Väärinkäyttömahdollisuuksien luominen huonontaa palvelujen turvallisuutta yleisesti ja mahdollistaa siten myös pahantahtoisille toimijoille aiempaa helpommin erilaiset väärinkäytökset aiheuttaen suoria vaikutuksia myös luottamuksellisen viestin suojan ja muiden perusoikeuksien toteutumiseen.

Viestien tutkiminen viestijän päätelaitteessa ennen viestin salaamista ja lähettämistä tarkoittaa, että järjestelmän täytyy tarkistaa se tunnettua laitonta materiaalia (esim. kuvia, videoita tai linkkejä) sisältävää tietokantaa vastaan. Tavanomainen tapa toteuttaa vaatimus on sisällyttää viestintäsovellukseen ns. yksilöllinen tunnistetietokanta, joka olisi paikallisesti jokaisessa laitteessa tai etäpalvelimella. Viestin läpivalaistavista elementeistä luotaisiin tunniste samalla algoritmilla, jolla tunnetusta laittomasta materiaalista (esim. kuvat) on luotu tunnisteet, jonka jälkeen järjestelmä tarkistaa, onko tämä tunniste tietokannassa. Järjestelmässä on tällöin mekanismi valvoa mitä tahansa sisältöä. Koska tietokanta sisältää vain tunnisteita tahoilla, joilla on kyky laillisesti tai laittomasti lisätä jokin kohde tunnistetietokantaan, voi lisätä tunnisteita siten, että tunnisteista ei voi millään keinoilla päätellä, onko tunniste luotu asianmukaisesti (esim. lasten seksuaalista hyväksikäyttöä todistavasta kuvasta) vai mistä tahansa muusta viestin osasta. Tämä johtuu siitä, että tunnisteista ei ole teknisesti mahdollista palauttaa alkuperäistä tiedostoa tai muutoinkaan rajoittaa koskemaan vain esim. hyväksikäyttöä koskevaa kuvastoa.

Valvonnan kohteiden eli kansalaisten on mahdotonta tarkistaa, onko järjestelmää laajennettu alkuperäisestä valvontakohteesta myös muihin kohteisiin, vaikka tunnistetietokanta olisikin saatavilla. Koska hyväksikäyttömateriaalia on laitonta pitää hallussaan, tietokannan tunnisteita ei voida verrata teknisesti alkuperäisten tiedostojen tunnisteisiin. Tämän seurauksena tietokannan sisältö on todellisuudessa ulottumattomissa kansalaisyhteiskunnan valvojille kuten toimittajille, akateemikoille, poliitikoille tai ylipäätään kenellekään, jolla ei ole pääsyä koko

alkuperäiseen aineistoon. Lisäksi on syytä huomioida, että suuressa osassa EU:n jäsenvaltioita on olemassa kansallista tiedustelulainsäädäntöä, joka mahdollistaa mm. teknisen laitetarkkailun tai muun tietoliikennetiedustelun muiden valtioiden alueella ja kansalaisiin kohdistuen, ja jonka avulla mm. palveluntarjoajia voidaan pakottaa lain nojalla avustamaan toiseen valtioon kohdistuvan tiedustelun toimeenpanossa viestien valvonnan avulla. Tämä tarkoittaa sitä, että järjestelmää voidaan käyttää myös kolmasien valtioiden intressien edistämiseen tiedustelun kohteena olevien ihmisten perusoikeuksien vastaisesti.

Lisäksi järjestelmä olisi äärimmäisen kiinnostava ja altis pahantahtoisille laajamittaista vakoilua harjoittaville kolmansille valtioille kuten Venäjälle ja Kiinalle, sillä haavoittuvuuksia hyväksikäyttäen (joita löydetään kaikista tietojärjestelmistä) järjestelmää voitaisiin käyttää myös viestien tekstin täydelliseen purkamiseen. Järjestelmälle itselleen on teknisesti merkityksetöntä, onko yksilöllinen tunniste tekstiä vai esim. kuvia. Järjestelmään voitaisiin syöttää myös keskeisiä sanoja tunnisteina ja siten pystyä päättelemään mikä tahansa sanojen kokoelma, jonka käyttäjät lähettävät viestissä. Käyttäjillä ei olisi mitään mahdollisuutta havaita, että heidän viestejään puretaan salaa. Esimerkiksi Alankomaiden turvallisuuspalvelu on todennut julkisesti, että tällaisen järjestelmän käyttöönotto viestintäpalveluissa muodostaa riskin, jota ei yksinkertaisesti voida ottaa.

Ehdotus on voimassa olevan EU-oikeuden vastainen

Viestien sisältöön kohdistuva tekninen valvonta edellyttämällä viestintäpalveluiden käyttäjiä suostumaan välitettävien viestien tutkimiseen jo viestijän päätelaitteessa on käsityksemme mukaan voimassa olevan EU:n yleisen tietosuoja-asetuksen vastainen. Jotta viestintäpalvelua voisi käyttää kuvia videoita tai linkkejä sisältävien viestien lähettämiseen käyttäjän olisi suostuttava viestien tutkimiseen. Yleisen tietosuoja-asetuksen mukaan, jotta suostumus olisi pätevä, sen on oltava yksilöity, tietoinen ja aidosti vapaaehtoinen, josta on oltava mahdollisuus myös kieltäytyä ilman haitallisia seurauksia. Käsillä olevan ehdotus kuitenkin rajoittaisi palvelun täysimääräisen käytön, mikäli viestien tutkimisella ei antaisi suostumista. Suostumuksen edellyttämistä olisi pidettävä vapaaehtoisuuteen perustumattomana sekä seurauksiltaan käyttäjälle haitallisena ja siten ehdotus ei täyttäisi yleisen tietosuoja-asetuksen edellytyksiä.

Kuten yllä on todettu, kansalaisten tai niitä edustavien tahojen ei olisi mahdollista valvoa oikeusturvaansa tehokkaasti ehdotuksen moninaisten tietoturvallisuuteen sekä tietosuojaan liittyvien riskien vuoksi. Esimerkiksi salassa pidettävän tunnistetietokannan eheys, rinnakkaisten tietokantojen olemassaolo, valvontaan käytettävien ohjelmistomoduulien luottamuksellisuus ja eheys ja saatavuus (toimivuus), kolmansiin valtioihin päätyvien henkilötietojen käsittely, tunnistusalgoritmien tarkkuus sekä luotettavuus olisivat kaikki käytännössä mahdottomia oikeudenloukkauksen kohteena oleville valvoa asianmukaisesti.

Suomen tulisi edistää vähemmän haitallisia ja tehokkaita ratkaisuja lasten suojelemiseen

Oireiden sijaan olennaista on juurisyyhyn vaikuttaminen. Ainakin 47 ihmisoikeusjärjestöä on vastustanut ehdotuksen haitallisia seurauksia aiheuttavia kohtia. 9.10.2024 mennessä 379 tieteilijää kyberturvallisuuden ja tietosuojan alalta 36 maasta on allekirjoittanut Unkarin uusinta ehdotusta perustellusti vastustavan kannanoton.

Kuten yllä on todettu, samaan aikaan on olemassa lasten suojelun kannalta tehokkaita ja samalla perusoikeuksia suojaavia keinoja, joita voidaan tukea valmisteilla olevalla asetuksella ilman, että siihen sisällytetään viestien valvonnan ja tutkimisen elementtejä:

- Haitallisten havaintojen käyttäjäpohjainen turvallisuusraportointi palvelujen ylläpitäjille
- Mikäli palvelu on suunnattu nuorille tai lapsille, palveluntarjoajien tulisi perehdyttää käyttäjiä verkkohoukuttelun riskeistä
- Verkkohoukuttelun torjunnan osalta vuonna 2024 jatkettua tilapäistäpoikkeusta sähköisen viestinnän tietosuojadirektiivin tiettyihin säännöksiin tulee jatkaa pysyvästi, jotta palveluntarjoajat voivat jatkaa ko. materiaalin vapaaehtoista tunnistamista ja raportoimista
- Alustojen turvallisuusraportointitieto tulisi olla suoraviivaisesti käytettävissä kansallisten neuvontapalveluiden ja sekä viranomaistyön prosesseissa hyväksikäytön vähentämiseksi ja uhrien auttamiseksi
- Velvoittavien suunnitteluperiaatteiden asettaminen alustoille. Komissio on jo laatinut strategian (European strategy for a Better Internet for Kids, BIK+) ikätasolle sopivan palvelusuunnittelun periaatteiksi ja laatinut pyynnön eurooppalaiselle standardille verkkoikävarmennukselle vuoteen 2024 mennessä. Tähän tarkoitukseen soveltuva käyttäjien tunnistaminen tulee myös mahdolliseksi EU:n digitaalisen identiteetin (eIDAS 2.0) avulla vuoden aikana.
- Lisäksi viestintäpalveluiden tarjoajat hyödyntävät muita ikään sopivan suunnittelun periaatteita ja oletusasetuksia, jotka minimoivat tietojen keräämisen käyttäjiltä, tukevat turvallista vuorovaikutusta alustoilla ja suojaavat haitalliselta sisällöltä ja vuorovaikutukselta, seksuaaliselta hyväksikäytöltä ja manipuloinnilta.

Asetuksen vaikutuspiirin ulkopuolisia keskeisiä keinoja ovat:

- Käyttäjäkoulutus, digitaalisen lukutaiton kehittäminen sekä huoltajien valvonta
- Rikoksentekijöiden vastuuseen saattaminen edellyttää jo olemassa olevien esitutkintatoimivaltuuksien ja -resurssien asianmukaista kohdentamista sekä syyttäjien ja tuomioistuimien kyvykkyyksien vahvistamista hankalien ja kansainvälisiä ulottuvuuksia sisältävien rikosasioiden huolelliseen käsittelyyn sekä rikosprosessin hallinnolliseen tehostamiseen
- Lapsen lähestymistä seksuaalisessa tarkoituksessa koskevan rikos- ja poliisilain muuttaminen siten, että poliisilla olisi oikeus lähestyä henkilöä väärän identiteetin keinoin eikä tilannetta pidettäisi todellisen uhrin (lapsen) puuttuessa sellaisena, että tekijä ei olisi syyllistynyt mihinkään rikokseen (toisin kuin Virossa, jossa poliisi on päässyt tehokkaasti valeidentiteetin avulla internetissä rikoksentekijöiden jäljille)

Teknologiateollisuus ry

Matti Mannonen
Johtaja, Uudistuva teollisuus

Kyberala ry

Peter Sund
Toimitusjohtaja

Lisätiedot:

Peter Sund, 050 565 0621
peter.sund@teknlogiateollisuus.fi

Antti Poikola, 044 337 5439
antti.poikola@teknologiateollisuus.fi