U 68/2022 vp Lausunto

Liikenne- ja viestintävaliokunta

2024-10-16

WITH secure | Consulting

Lausunnon antaja

Päivämäärä	Tekijä	Muutos	Versio
2024-10-16	Antti Laatikainen, Johtava tietoturvakonsultti	Lopullinen versio	1.0

Dokumentin jakelu

Päivämäärä	Vastaanottaja	Organisaatio
2024-10-16	Liikenne- ja viestintävaliokunta	Eduskunta

Toimeksianto

Asia: U 69/2022 vp Valtioneuvoston kirjelmä Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (COM(2022) 209 final).

WithSecure perustaa seuraavan lausuntonsa omaan teollisuudenalan erityisosaamiseensa, sekä valiokunnan esityslistan liitteeseen U_69_2022_EUN_78_2024_vp_pdf sekä U_69_2022_Proposal_for_a_Regulation_12406_24_pdf jotka toimitettiin WithSecurelle pohjamateriaaliksi.

Lähtökohta lausunnolle

Sosiaalinen media ja ihmisiä yhdistävät verkkopalvelut ovat olennainen osa nykyaikaisen tietoyhteiskunnan toimintaa. Niiden luonteeseen kuuluu valitettavasti myös erilaisten rikollisten toimintojen mahdollistaminen, joihin kuuluu lasten seksuaalinen hyväksikäyttö. Rikosten torjumiseksi palveluntarjoajien on toimittava vastuullisesti ja ryhdyttävä toimenpiteisiin väärinkäytön estämiseksi. Toimenpiteiden tulee olla kohdennettuja ja suhteellisia, jotta laillisten käyttäjien perusoikeuksia ei loukata eikä palveluntarjoajille aseteta liiallisia rasitteita.

Toimenpiteiden tulee ennen kaikkea olla oikeamittaisia suhteutettuna uhreille aiheutuneisiin kärsimyksiin ja vahinkoihin.

Nyt ehdotettu toimintatapa ja malli lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä vaikuttavat WithSecuren mielestä teknisesti haastavilta toteuttaa. Ne edellyttävät riskialttiita toimintatapoja, joita WithSecuren osaamisen perusteella on vaikea nähdä tarkoituksenmukaisina.

Ehdotetun lähestymistavan tehokkuus on parhaimmillaankin tavoitteeksi asetetun rikollisuuden muodon torjumisen suhteen kyseenalainen.

WithSecure lähestyy annettua lausuntopyyntöä riskienhallinnan, yksityisyydensuojalainsäädännön sekä teknisten tietoturvan hallintakeinojen suunnittelun ja toteutuksen haasteiden näkökulmasta.

LAUSUNTO

WithSecuren näkemyksen mukaan ehdotettu lakiesitys on vaarallinen EU-kansalaisten perusoikeuksille, teknisesti erittäin haastava toteuttaa ja teholtaan sekä kattavuudeltaan kyseenalainen.

Tämä herättää huolta sekä yksityisyydestä että käytännön toteutettavuudesta.

WithSecuren kanta on että Suomen ei pidä tukea tämänhetkistä kompromissiesitystä seuraaviin asioihin vedoten:

Tiedon käsittely uhkaa eurooppalaisten perusoikeuksia

Ehdotetussa asetuksessa valvonnan piiriin määrättäisiin vain korkean riskin keskustelualustat ja ohjelmistot. WithSecuren tulkinta asetuksessa esitetyn palveluiden riskien arvioinnin kuvauksesta[1] on, että käytännössä kaikki nykyisin käytössä olevat sosiaalisen median alustat ja erilaiset yhteisölliset verkkopalvelut kuuluvat korkean riskin palveluiden piiriin. Suuri osa näistä palveluista toimii EU:n ulkopuolelta käsin.

Verkkopalveluiden ja viestintäalustojen toimittajille annetaan ehdotetussa asetuksessa tehtäväksi kerätä erittäin arkaluontoista tietoa käyttäjistä. Heitä sitovat ainoastaan heidän omat, yrityksen sisäiset riskienhallintavelvoitteet, jotka määrittävät, miten minimoida pääsy tietoihin, vähentää kerätyn tiedon määrää ja suojata tiedot asianmukaisesti. Ensivaiheessa luotava järjestelmä tunnistaa verkko- ja viestintäpalveluista ainoastaan aiemmin tunnistettuja lapsiin kohdistuvaa seksuaalista hyväksikäyttöä sisältäviä materiaaleja (eng. child sexual abuse material, CSAM) kuva- ja videotallenteina.Tulevaisuudessa järjestelmään on tarkoitus lisätä kehittyneempiä toiminnallisuuksia, joilla pystytään tunnistamaan myös aiemmin tuntemattomia CSAM materiaaleja, myös mahdollisesti puheesta ja tekstistä[2].

Kerätty data on palveluntarjoajan sijaintimaassa paikallisen lainsäädännön alaista, ja siihen voidaan kohdentaa paikallisia viranomaispyyntöjä. Käsittelyssä oleva säädös ei sisällä vaatimusta ilmoittaa tällaisista tietopyynnöistä EU:n viranomaisille tai palvelun käyttäjille.

Kun tekninen valmius tällaisen tiedon keräämiseen on saatu käytettäviin palveluihin käyttöön, sitä on helppo konfiguroida keräämään mitä tahansa tietoa. Säädöksen kuvaus ja toiminnan rajaus ei sisällä palveluissa käytettävän tekstimuotoisen viestinnän sisältöä, mutta tämän rajauksen valvonta sekä toteutus perustuu täysin toimittavien yritysten riskienhallintaan sekä paikalliseen lainsäädäntöön ja toimintakulttuuriin. Mikään ei estä valvonnan laajentamista muihin aihealueisiin ja tunnisteisiin, kuten ei-toivottuun poliittiseen mielipideilmaisuun.

Palveluntarjoaja voi säilyttää tapahtumalokeja ja niiden pohjana käytettävää tapahtumien raakadataa viiden vuoden ajan, jolloin niiden poistaminen tapahtuu palveluntarjoajan ja paikallisen lainsäädännön mukaisesti.

WithSecuren mielestä tällaisen tiedonkeruun toteuttamiseen ja tiedon suunnitellun asetuksen mukaisen käyttön valvontaan liittyy huolta, erityisesti kun asetustekstissä useaan kertaan mainitaan, että valvontaa ei saa suorittaa kansalliseen turvallisuuteen liittyviin henkilöihin[3]. Tämä osoittaa WitSecurelle selkeästi, että viranomaiset olettavat tämän teknologian voivan, ja mahdollisesti tulevankin, käyttöön tavoilla, jotka poikkeavat tässä asetuksessa määritellyistä.

Tämä herättää vakavia huolenaiheita yksityisyyden suojasta ja teknologian väärinkäytön mahdollisuuksista.

[1] 2022/0155(COD) Article 3
[2] 2022/0155(COD) Recital 77a
[3] 2022/0155(COD) Recital 12a, Article 7(8d), Main elements of the presidency compromise text (9c),

Aikaansaatava valvontaprosessi tehoton

Ehdotetussa asetuksessa esitetyt palveluntarjojilta edellytetyt riskienhallinnan kontrollikeinot[4], kuten pakolliset vanhempien valvonta- ja rajaamistyökalut ja käyttäjien helpon ilmoituskanavan edellyttäminen palvelussa, ovat hyviä asioita. On myös positiivista, ettei ehdotetussa esityksessä tiedon siirron suojaamisen kryptausta ehdoteta heikennettävän.

Ehdotettu valvontavaatimus perustuu selkeästi käyttäjille ilmoitettavaan valvontaan[5] määritellyissä palveluissa. Lapsiin kohdistuva seksuaalinen halu luokitellaan Euroopassa sairaudeksi. Onkin kysymyksiä herättävää, että käyttääkö tästä sairaudesta kärsivä ihminen keskustelualustoja, joissa tietää valvonnan olevan käytössä.

Ehdotettu asetus määrittelee valvonnan rajoittuvan mediaformaatteina kuviin ja videotallenteisiin, sekä perustuvan vain EU:n valvontakeskuksen hallussa oleviin tunnettuihin CSAM materiaaleihin[6] ja niiden tunnistetietoihin. Kuvatunlainen rajattu valvonta kartoittaa käytännössä, mitkä eri alustojen käyttäjätilit ovat keskenään jakaneet tunnettuja CSAM kuvia tai videoita. Tämä jättää suuren osan ehdotetun asetuksen perustelussa määritellystä, tätä valvontaa oikeuttavasta toiminnasta, kuten verkkoviettelystä (eng. grooming), käytännössä kokonaan valvonnan ulkopuolelle. Verkkoviettely ja suoraan lapsiin kohdistuvat yhteydenotot sekä erilaiset heidän manipulointiin käytettävät viestit ovat käynnissä olevaan keskusteluun liittyviä, reaktiivisia, reaaliaikaisia ja useimmiten uniikkeja tekstejä ja kuvia. Tähän uhkakuvaan nyt luotava rakenne ei tuo minkäänlaista suojaa.

Erilaisissa sosiaalisen median alustoissa jaettava materiaali hajautuu käytännössä käyttäjien päätelaitteille, eri ohjelmistojen tietokantoihin ja mobiililaitteen tai kannettavan tietokoneen kuvakansioihin. Ehdotetussa asetuksessa kuvatun CSAM materiaalin poistomääräyksen käsittelyaika on WithSecuren käytännön arvion mukaan vähintäänkin päiviä, todennäköisesti viikkoja, mahdollisesti kuukausia. Annetun poistovaatimuksen jälkeen palveluntarjoajalle annetaan mahdollisuus kuitata poistomääräys “teknisesti liian haastavana tai mahdottomana toteuttaa”. WithSecure arvioi omaan tekniseen järjestelmätuntemukseensa perustuen, että tätä kuittausprosessia tullaan käyttämään paljon. Käytännön haasteeksi muodostuu prosessin tekniset yksityiskohdat, kuten että keskusteluun käytettävän mobiililaitteen sosiaalisen median ohjelmiston toimittaja ei käytännössä omaa ohjelmistoaan konfiguroimalla pysty poistamaan mobiililaitteelta kuvakansioon siirrettyjä kuvia.

Esitetyssä asetuksessa tunnettua CSAM-materiaalia sisältävien verkkopalveluiden estomääräyksen kontrolli kohdistuu palvelun verkko-osoitteisiin. Palvelun ylläpito voi kuitenkin helposti luoda palvelulle useita samaan aikaan voimassa olevia verkko-osoitteita, keksiä uusia tai ohjeistaa palvelun käyttäjiä ottamaan suoraan yhteyttä palvelun IP-osoitteella. Tämä tekee estomääräysten valvonnasta haastavaa ja mahdollistaa sen kiertämisen.

IT projektina yrityksille haastava

Sosiaalisen median ja erilaisten verkkopalveluiden rakentamiseen käytetään monia eri ohjelmointikieliä ja ohjelmointitapoja, ja niiden ohjelmallinen toimintalogiikka ja rakenne vaihtelevat suuresti. Ehdotetun asetuksen mukaisen valvontamääräyksen antamisen jälkeen EU:n valvontakeskus määrittää ja/tai toimittaa tarvittavan koodin tai ohjelmistomoduulit palveluntarjoajalle[7], joilla valvonta tulee toteuttaa.

Nämä ohjelmistomoduulit ja toiminnallisuudet täytyy integroida ohjelmiston sisäiseen arkkitehtuuriin sellaiseen tiedon käsittelyn (eng. data flow) vaiheeseen, jossa niillä pystytään tehokkaasti lukemaan esimerkiksi mobiililaitteen avoimeen keskusteluun liitettävän kuvan datan ja muodostamaan siitä tiivisteen tai tunnisteen. Toinen vaihtoehto valvonnalle käytännössä on, että moduulille annetaan oikeudet lukea kaikki mobiililaitteella tallessa olevat kuvat ja videot ja raportoida niiden tunnisteet palveluntarjoajalle.

---

[4] 2022/0155(COD) Article 3, 4, ANNEX XIV
[5] 2022/0155(COD) Recital 26a, Article 10
[6] 2022/0155(COD) Recital 77a
[7] 2022/0155(COD) Article 7, 10

Palveluntarjoajan tulee ehdotetun asetuksen mukaan pitää kirjaa siitä, mistä laitteesta tunnistetiedot ovat peräisin, ja toimittaa ne muuttumattomina EU:n valvontakeskukselle. Tämän siirron kuvausta ei ole esitetty ehdotuksessa, mutta oletettavasti se tapahtuu jonkinlaisen ohjelmistorajapinnan kautta.

Edellä kuvattujen toiminnallisuuksien aikaansaaminen ohjelmistokokonaisuudessa edellyttää valvontaan käytettävien ohjelmistomodulien ja ohjelmistokirjastojen yhteensopivuutta kaikkien käytössä olevien ohjelmointikielien, mobiililaitteiden käyttöjärjestelmien, versioiden ja vaikkapa ohjelmistojen sisäisten kryptografisten toteutusten kanssa.

Tekninen toteutus tietokoneen nettiselaimella käytettävien palveluiden suhteen on taas täysin erilainen, eikä välttämättä teknisiltä ominaisuuksiltaan mahdollista toteuttaa samalla tavalla kuin mobiililaitteissa. Nettiselaimet on rakennettu nykyään hyvin tietoturvallisiksi, eikä niissä ole samalla tavalla mahdollista asentaa lisäosia tai toiminnallisuuksia kuin mobiililaitteiden ohjelmistoihin. Nettiselaimilla ei esimerkiksi ole vakiona lupaa lukea kovalevylle tai käyttöjärjestelmän muihin osiin tallennettuja kuvatiedostoja.

WithSecuren kokemukseen perustuva arvio on, että edellä mainittujen teknisten toiminnallisuuksien käyttöönotto olemassa olevaan ohjelmistoon vaatii ohjelmistoa tuottavalta taholta kuukausien suunnittelua, testausta ja asteittaista levitystä julkaistuihin versioihin. Ohjelmistokehityksen henkilöstölle tarvittavat resurssit ovat mittavat.

Vastuiden ja seuraamusten jakautuminen epäselvää

Ehdotetussa asetuksessa palveluntarjoajien edellytetään määrittelemään toimintaansa ja tuotettuun palveluun liittyvät riskit ja raportoimaan ne EU:n valvontakeskukselle. Heidän on myös noudatettava EU:n valvontakeskuksen vaatimuksia valvontaan käytettävien teknologioiden implementoinnista, ja maksettava valvontakeskukselle suorittamistaan CSAM materiaalin verifiointihauista.

Kaikki toiminnan kustannukset lankeavat palveluita tuottavien yritysten itsensä maksettavaksi, poislukien mikro- ja pienet yritykset[8].

EU valvontakeskus ja toimintaa valvovat viranomaiset voivat suorittaa valvontatoimia palveluita tuottaviin yrityksiin.

Verkko- ja viestintäpalveluita ylläpitävillä yrityksillä on mahdollisuus valittaa, tai ilmoittaa viivästyksistä suunnitellun asetuksen valvontaprosessin jokaisesta vaiheesta ja näin kyseenalaistaa kaikki heihin kohdistuvat pyynnöt ja vaatimukset.

WithSecurelle muodostuu asetuksesta epäselvä kuva, mikä on EU valvontakeskuksen todellinen vaikutusvalta verkko- ja viestintäpalveluita tuottavaan yritykseen, jos heillä on mahdollisuus vedota teknisiin haasteisiin tai pyydetyn tehtävän kustannuksiin.

Annex XIV:n kuvaama palvelun riskiarvioinnin itsearviointilomakke on hyvin ylätasoinen, subjektiivinen eikä WithSecuren näkemyksen mukaan mene tarpeeksi syvälle palvelun toteutuksen tapoihin tai toimintamalleihin että sen tulosten perusteella voitaisiin arvioida EU valvontakeskuksessa valvottavan yrityksen tietoturvan tai riskienhallinnan todellista tilaa.

Vaatimustenmäärittely epäselvää

Ehdotetussa asetuksessa ja sen määrittelyssä WithSecure näkee vaarallisen paljon tulkinnanvaraisia määrityksiä, sekä erilaisissa asetuksen kohdissa ehdotettuja hallintakeinoja joiden käytännön toteutusta ei avata. Tämä tekee ehdotetun asetuksen tietoturvallisuuden- tai toteutettavuuden arvioinnista haastavaa.

[8] 2022/0155(COD) Article 3 (3)

Miten esimerkiksi käytännössä tunnistetaan käyttäjät, jotka työskentelevät kansallisen turvallisuuden parissa? Perustuuko tämä käyttäjien itse tekemään ilmoitukseen ja miten valvotaan että annettu ilmoitus on paikkansapitävä? Entä miten tulee suhtautua kansallisessa turvallisuudessa työskentelevän henkilön omassa henkilökohtaisessa käytössä oleviin laitteisiin, ohjelmistoihin ja tileihin?

Mistä EU-EUvalvontakeskuksella käytössä oleva tunnettu CSAM-materiaali tulee ja kuinka ajanmukaista tai kattavaa se on, jos ehdotetussa asetuksessa luotava valvontajärjestelmä ei ensi vaiheessa luo uusia tunnistetietoja eikä raportoi niitä? Onko kuukausia vanhan, esimerkiksi poliisitutkimusten kautta saadun video- ja kuvamateriaalin tunnistaminen verkkopalveluissa niin tehokasta suojaa lapsille ja nuorille, että se oikeuttaa edellä kuvatut haasteet palvelun asianmukaisen laillisen käytön, tietoturvallisen rakentamisen ja palveluntarjoajille koituvien kustannusten suhteen?

WithSecure näkee myös haastavana, miten tullaan suhtautumaan tilanteisiin, joissa verkko- tai viestintäpalvelun tarjoaja toteaa yrityksen sisäiseen riskienhallintapäätökseen perustuen, että he tekevät jo tarpeeksi määriteltyjä riskienhallinnan kontrolleja ja EU-valvontakeskuksen heiltä edellyttämä riskien hallintakeinojan käyttöönoton lisätyö on heille taloudellisesti ylitsepääsemättömän kallista.

Entä miten toimitaan, jos verkko- tai viestintäpalvelu on rakennettu käyttäen teknisiä ratkaisuja joihin EU:n valvontakeskus ei pysty toimittamaan valvontamääräyksen edellyttämää teknisen toteutuksen ohjelmointimoduleita tai kirjastoja?

Nämä kysymykset herättävät huolta siitä, kuinka tehokas ja käytännössä toteuttamiskelpoinen ehdotettu säädös on, ja miten se vaikuttaa sekä palveluntarjoajiin että käyttäjiin. On tärkeää, että tällaiset epäselvyydet ja avoimet vastuut määritellään huolellisesti ennen säädöksen voimaantuloa, jotta voidaan varmistaa sen toimivuus ja oikeudenmukaisuus kaikille osapuolille.

Yleisiä kommentteja ja havaintoja.

Julkisuudessa esillä olleisiin kiinniottotapauksiin ja tehtyihin tutkimuksiin perustuen on oletettavaa, että lasten seksuaalisen hyväksikäytön vähentämiseen on olemassa myös tietoverkkojen puolella paljon esitettyä rakennetta tehokkaampia toimia. Nämä toimet perustuvat perinteiseen lainvalvonnan toimintaan sekä sille annettaviin laajempiin toimivaltuuksiin ja työkaluihin.

WithSecure suosittelee, että tämän aihepiirin arvioinnissa otetaan huomioon myös nuorille suunnatun opetuksen ja kasvatuksen merkitys, vanhempien roolin vahvistaminen nuorten kasvun tukemisessa sekä lapsiin seksuaalisesti suuntautuneiden ihmisten tuen ja hoidon tarve.

Nyt ehdotettu asetus ja toimintamalli ei kata tämän monimutkaisen ongelmakentän haasteista kuin pienen osan, tuoden samalla keskusteluun valtavan määrän uusia, siihen aiemmin kuulumattomia haasteita.

Lausunnon antaja:

Helsingissä, 16.10.2024

Antti Laatikainen

Johtava tietoturvakonsultti

WithSecure Consulting

antti.laatikainen@withsecure.com

+358406372163

Liitteet:

1) Kokoava PowerPoint-esitys, esitetty valiokunnan tilaisuudessa 16.10.2024