



10.09.2025

AV24869
290/00.04.02/2024

Eduskunnan liikenne- ja viestintävaliokunta

LAUSUNTO 4: U 69/2022 VP VALTIONEUVOSTON KIRJELMÄ EUROOPAN KOMISSION EHDOTUKSESTA EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUKSEKSI LAPSIIN KOHDISTUVAN SEKSUAALIVÄKIVALLAN EHKÄISYÄ JA TORJUNTAA KOSKEVISTA SÄÄNNÖISTÄ

Tausta

Liikenne- ja viestintävaliokunta on pyytänyt Puolustusvoimien lausuntoa koskien valtioneuvoston kirjelmää Euroopan komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi lapsiin kohdistuvan seksuaaliväkivallan ehkäisyä ja torjuntaa koskevista säännöistä (U 69/2022 vp). Puolustusvoimat on lausunut aikaisemmin asiaan liittyen 13.9.2023 (AT22141), 14.10.2024 (AU26246) ja 21.4.2025 (AV11773) tältä osin uudistaa lausunnossaan tuodut näkökannat.

Puolustusvoimat ei tunnista itseään toimijana, johon nyt kyseistä komission asetusehdotusta voitaisiin soveltaa suoraan. Puolustusvoimat on tuonut aikaisemmissa lausunnoissaan esiin sen, miten Puolustusvoimat käsittelee henkilötietoja. Lisäksi on lausuttu siitä, miten Puolustusvoimat voisi toimia, jos Puolustusvoimat havaitsee mm. verkossa aineistoa, joka liittyy rikolliseen toimintaan.

Nykyisestä ehdotuksesta

Puolustusvoimat pitää asetusehdotuksen tavoitteita lasten suojelemisesta erittäin kannatettavina. Puolustusvoimien näkemyksen mukaan on tarpeellista muodostaa selkeä ja sitova oikeudellinen kehys, jonka avulla voidaan torjua ja ennaltaehkäistä lapsiin kohdistuvaa seksuaaliväkivaltaa. Lainsäädännön tulee turvata viranomaisille ja muille toimijoille riittävät keinot lasten suojelemiseksi verkkoympäristössä tavalla, joka on myös yhteensopiva perustuslain turvaaman luottamuksellisen viestin salaisuuden ja henkilötietojen suojan kanssa.

Tavoite ei kuitenkaan voi syrjäyttää kaikkien verkon käyttäjien perusoikeuksia viestinnän luottamuksellisuuteen ja yksityisyyden suojaan muuten kuin sen osalta, mikä on ehdottoman välttämätöntä.

Sisäministeriön 22.8.2025 päivätyn perusmuistion EU/88/2022-SM-72 mukaan valtioneuvosto huomioi, että myös uusiin kompromissiehdotus sisältää useita velvoitteita, jotka vahvistavat lasten suojaa verkkovälikiteiseltä seksuaaliväkivallalta. Valtioneuvosto ei kuitenkaan voi tukea ehdotettua kompromissia, sillä ehdotukseen on palautettu aiempien kompromissiehdotusten mukainen, perustuslain kannalta ongelmalliseksi todettu tunnistamismääräys.

Asetusehdotuksen keskeisimmät haasteet ovat liittyneet tunnistamismääräykseen (artikla 7), jonka nojalla soveltamisalaan kuuluvia palveluntarjoajia eli säilytyspalvelun ja henkilöiden välisen viestintäpalvelun tarjoajia voitaisiin **viranomaismääräyksellä velvoittaa** tunnistamaan lapsiin kohdistuvaa seksuaalista väkivaltaa esittävää materiaalia (jatkossa CSA-materiaalia) sekä lasten houkuttelemista seksuaalisiin tarkoituksiin (ns. grooming) alustoillaan ja ilmoittamaan siitä viranomaisille, ja erityisesti tunnistamismääräyksen suhteeseen luottamuksellisen viestinnän suojaan sekä viestinnän salaukseen.

Asetusehdotukseen tehty keskeisimmät muutokset Tanskan puheenjohtajuuskaudella

Muistion mukaan Tanskan laatima kompromissiteksti merkitsee käytännössä kokonaan paluuta Belgian ja Unkarin puheenjohtajakausilla neuvoteltuun versioon, jota käsiteltiin eduskunnalle toimitetussa erilliselvityksessä asian EUN 78/2024 vp yhteydessä. Yksinomaan palveluntarjoajien vapaaehtoisuuteen perustuvasta CSA-materiaalin tunnistamisesta (Puolan kompromissiehdotus) on luovuttu, ja tekstiin on palautettu velvoittava tunnistamismääräys sekä siihen liittyvät tekniset toiminnot.

Tunnistamismääräykset kohdistuisivat tunnetun ja uuden CSA-materiaalin visuaaliseen sisältöön ja URL-osoitteisiin. Teksti- ja äänisisältö olisi suljettu tunnistamismääräyksen soveltamisalan ulkopuolelle. Kompromissitekstissä tunnistamismääräys koskisi myös päästä päähän salattua viestintää.

Pöydällä olevan kompromissiesityksen mukaan edellä kuvattu tunnistamismääräyksen toteuttaminen olisi mahdollista vain sillä edellytyksellä, että jokainen käyttäjä antaa palveluntarjoajan ehtojen mukaisesti nimenomaisen suostumuksensa siihen, että ko. tunnistamistoimintoa voidaan kyseisessä palvelussa käyttää. Jos käyttäjä ei anna lupaa tällaiseen toimintoon, hän ei voisi lähettää kyseisessä palvelussa kuvia tai URL-osoitteita.

Kuten muistiossa on todettu tämä kompromissiehdotukseen sisältyvä kompromissimalli, jossa verkkopalveluntarjoajat veloitettaisiin tunnistamaan ja torjumaan lapsiin kohdistuvaa seksuaaliväkivaltaa sisältävää materiaalia, on sääntelyn keskeinen, mutta ongelmallinen osa.

Puolustusvoimat on tuonut aiemminkin esiin, että tämä yleinen ja erittelemätön pääsy viestien sisältöihin loukkaa yksityiselämän suojan keskeistä sisältöä ja on viestinnän luottamuksellisuuden kannalta ongelmallista (mikäli palveluntarjoajat voitaisiin yleisesti ja erotuksetta velvoittaa tarkastelemaan kaikkea palveluissaan jaettavaa sisältöä).

Asetusehdotuksessa olevan **tunnistamismääräyksen on oltava** kohdennettu ja käyttöönoton ei tule johtaa kaikkien viestintäpalveluiden ja tietoliikenteen yleiseen ja erotuksettomaan valvontaan. Tunnistamismääräyksen tulisi olla mahdollisimman kohdennettu henkilöihin, jotka liittyvät lapsiin kohdistuvien seksuaalirikosten selvittämiseen tai joiden voidaan epäillä olleen osallisina tällaisiin rikoksiin. Sääntelyn tulee olla kaikilta osin oikeasuhteista, ja sen tulee varmistaa, että puuttuminen perusoikeuksiin tapahtuu kohdennetusti ja yksilöidysti.

Puolustusvoimat toistaa aiemmin lausutun, että asetusehdotuksen vaikutukset luottamuksellisen viestin salaisuuden suojaan verkossa tulee huomioida, mikäli asetusehdotus voisi tarkoittaa luottamuksellisen viestinnän salauksen purkamista verkossa sekä yksityisten viestien sisällön laaja-alaisempaa valvontaa. Salausten purkamisen kohdalla on kiinnitettävä huomiota siihen, että heikennettäessä järjestelmän salausta heikennetään käytännössä aina myös järjestelmän tieto- ja kyberturvallisuutta. Jos salausta heikennetään, sen vaikutukset kohdistuisivat kaikkiin käyttäjiin.

Puolustusvoimat kiinnittää erityisesti huomiota siihen, että asetusehdotuksen käsittelyssä tulisi varmistaa, ettei sillä voida yleisesti velvoittaa palveluntarjoajia purkamaan tai heikentämään viestinnän vahvaa salausta. On olennaista pyrkiä varmistamaan mahdollisimman korkea ja tarkkarajainen kynnys sekä kattavat oikeussuojatakeet salausta purkavien tai heikentävien toimien käyttöön. Nyt ehdotettu järjestely voisi avata ovia laajemmille valvontamekanismeille, mikä puolestaan voisi lisätä väärinkäytösten riskiä ja heikentää tietoturvaa.

Lainvalvontaviranomaiset voivat käyttää perusteltua epäilyä ja perusteltua syytä rikosten ratkaisemiseen ja estämiseen ilman, että jokaisen käyttäjän laitetta tarvitsee tarkastella.

Puolustusvoimat pitää olennaisena ja korostaa sitä, että on erityisen tärkeää varmistaa, etteivät vapaaehtoiset toimetkaan edes tosiasialla johda päästä päähän- salauksen tai muiden vastaavien tietoturvatoinenpiteiden yleiseen heikentämiseen tai niiden purkamisen taikka niiden käytön rajoittamiseen.

Tunnistamismääräyksen kytkeytyvää suostumuksen periaatetta voidaan pitää vapaaehtoisuuden osalta kyseenalaisena siltä osin, kun tunnistaminen olisi palvelun osittaisen käytön ehtona.

Lopuksi

Puolustusvoiminen näkemyksen mukaan asetusehdotus on palannut takaisin ongelmalliseen muotoon.

Puolustusvoimat korostaa erityisesti kantoja, joissa painotetaan viestinnän luottamuksellisuuteen sekä sähköisen viestinnän tietosuojaan ja tietoturvaan liittyviä reunaehtoja.

Puolustusvoimat toteaa, että myös nyt ehdotetuilla toimilla on vaikutusta perusoikeuksina turvattuihin viestinnän luottamuksellisuuteen ja sähköisen viestinnän tietosuojaan. Ehdotettujen toimien tulee olla välttämättömiä ja perusoikeuksien rajoitusedellytysten on täytyttävä, mikä rajaa lainsäätäjän harkintavaltaa.

Vaarana on edelleen myös se, että mikäli heikennetään tietoturvaa ja yksityisyyden suojaa, tämä voi vaikuttaa yhteiskunnan kokonaisturvallisuuteen mm. tietoturvan sekä luottamuksellisen viestinnän kohdalla.

Puolustusvoimien tietosuojavastaava
Varatuomari Maarit Tulokas

Tämä asiakirja on sähköisesti allekirjoitettu.

LIITTEET

JAKELU

TIEDOKSI