

Liikenne- ja viestintävaliokunta

Poliisihallituksen asiantuntijalausunto asiassa HE 179/2025 vp Hallituksen esitys eduskunnalle kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi

1 Lausuntopyynnöstä

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt Poliisihallitukselta asiantuntijaa kuultavaksi ja kirjallista asiantuntijalausuntoa asiassa HE 179/2025 vp Hallituksen esitys eduskunnalle kyberkestävyysasetuksen toimeenpanoa koskevaksi lainsäädännöksi. Asiantuntijalausunto toimitetaan 19.2.2026 mennessä ja valiokunnan kuuleminen pidetään 20.2.2026.

2 Hallituksen esityksestä

Hallituksen esityksen pääasiallisesta sisällöstä todetaan, että *esityksessä ehdotetaan säädettäväksi laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifiointista sekä muutettavaksi eräiden tuotteiden markkinavalvonnasta annettua lakia, kyberturvallisuuslakia, sähköisen viestinnän palveluista annettua lakia ja sakon täytäntöönpanosta annettua lakia*. Esityksen tarkoituksena on säätää kyberkestävyysasetuksen kansallisesta toimeenpanosta täsmentämällä ja täydentämällä kansallista lainsäädäntöä. Kyberkestävyysasetuksen tavoitteena on ollut asettaa vähimmäisvaatimuksia digitaalisille tuotteille ja ohjelmistoille.

Edellä mainittujen tavoitteiden lisäksi tavoitteena on ollut täydentää kyberturvallisuusdirektiivin kansallista täytäntöönpanoa verkkotunnusten rekisteröintitietojen ja verkkotunnusvälittäjien osalta.

3 Poliisihallituksen kommentit hallituksen esitykseen

3.1 Yleistä

Kyberkestävyysasetuksen tavoitteet samoin kuin hallituksen esityksessä esitetyt yleiset tavoitteet kansalaisten ja organisaatioiden toiminnan turvaamisesta ovat luonnollisesti erittäin kannatettavia. Ohjelmistojen ja laitteiden nykyistä turvallisempaan toimintaan tähtäävä sääntely on kannatettavaa ja sillä on hyvin todennäköisesti suotuisaa vaikutusta myös tietoverkkorikosten ja tietoverkkoa hyväksikäyttäen tehtävien rikosten ennalta estämisessä.

Hallituksen esityksessä rikostorjuntaa ja poliisitoimintaa koskevat seikat liittyvät verkko-tunnusvälittäjiin, haavoittuvuustietoihin sekä vapaaehtoisesti luovutetun tiedon käytön rajoituksiin rikostutkinnassa.

3.2 Yksityiskohtaisemmat huomiot hallituksen esitykseen

3.2.1 Laki eräiden tuotteiden kyberkestävyydestä sekä kyberturvallisuussertifioinnista 9 § CSIRT-yksikön oikeus luovuttaa salassa pidettäviä tietoja.

Sääntelyssä tulisi ehdotettua täsmällisemmin huomioida kyberkestävyyssasetuksen 14–15 artiklan mukaisia haavoittuvuus- ja poikkeamailmoitusten käsittelyyn liittyvien sekä vapaaehtoisuuteen perustuvien ilmoitusten tietojen luovuttaminen poliisille yksittäistapauksessa rikoksen selvittämiseksi. Tietojen luovuttamisen tulisi kattaa sekä 9 § 1 että 2 momentin mukaiset tiedot. Kyse olisi tällöin tietojen luovuttamisesta pakkokeinolain (806/2011) 8 luvun 21 §:n säädetyn laite-etsinnän toimittamiseksi sekä pakkokeinolain 10 luvussa säädetyn pakkokeinon käyttämiseksi. Edellä mainituista pakkokeinoista päättää pääsääntöisesti tuomioistuin.

Pakkokeinolaissa on jo esimerkiksi säännöksiä, joissa tietojärjestelmän haltijalle on jo asetettu tiedonanto- ja avustamisvelvoitteita pakkokeinon käyttämiseksi, joten on perusteltua, että viranomaisten välisessä toiminnassa mahdollistetaan kyberkestävyyssasetuksen 14–15 artiklan mukaisten haavoittuvuus- ja poikkeamailmoitusten käsittelyyn liittyvien sekä vapaaehtoisuuteen perustuvien ilmoitusten salassa pidettävien tietojen luovuttaminen pakkokeinon toteuttamiseksi.

Lain perusteluissa tulisi todeta, että tietoja voidaan luovuttaa myös poliisille, sillä CSIRT-yksikön oikeudesta luovuttaa tietoja poliisille ei ole säädetty laissa sähköisen viestinnän palveluista (917/2014) 319 §:ssä vaikka tietoja voidaan luovuttaa muille tahoille ja myös ulkomaan viranomaisille. Olisi johdonmukaista, että edellä mainittuja tietoja voitaisiin luovuttaa kotimaisille viranomaisille, jos niitä voidaan luovuttaa ulkomaisille viranomaisille. Jotta nykyisen lain asettamat puutteet tietojen luovuttamiselle eivät aiheuta estettä tietojen luottamiseen tästä olisi todettava laissa yksiselitteisesti. Yhtenä tulkintana on pidetty myös sitä, että kun tietojen luovuttamisesta ei ole nimenomaisesti säädetty, se on silloin kiellettyä.

Yksityiskohtaisissa perusteluissa todetaan, että pykälä ei rajoittaisi CSIRT-yksikön oikeutta luovuttaa kyseisiä tietoja julkisuuslain vahinkoedellytyslausekkeiden puitteissa eikä tietojen luovuttamista muussa laissa kuten kyberturvallisuuslaissa tai sähköisen viestinnän palveluista annetun lain 319 §:ssä säädetyn perusteella. Tämä on omiaan aiheuttamaan sen, että tietojen luovuttamisessa tukeudutaan vain SVPL 319 § tulkintaan.

Asia on sikäli merkittävä, ettei tätä seikkaa voida jättää vain muotoutuvan tulkintakäytännön varaan, kun SVPL 319 §:ssä ei ole huomioitu tietojen luovuttamista polisille lainkaan. Lisäksi on syytä huomioida, että viitattu SVPL 319 § koskee eri tietoja kuin mitä nyt puheena olevat teknistä haavoittuvuutta koskevat tiedot ovat eli Liikenne- ja viestintäviraston ja tietosuojavaltuutetun 316 ja 317 §:n nojalla saamat ja hankkimat tiedot viesteistä, välitystiedoista, sijaintitiedoista sekä luottamuksellisen radiolähetyksen sisällöstä ja olemas-

saolosta on pidettävä salassa. Haavoittuvuutta koskevat tiedot eivät ole näitä erityissääntelyn alle asetettuja viestinnän tietoja vaan järjestelmien teknisiin ominaisuuksiin liittyviä tietoja. EU sääntely ei aseta estettä tai rajoitusta tietojen luovuttamiselle edellä ehdotetulla tavalla poliisille.

3.3 8 § Vapaaehtoinen ilmoittaminen

Pykälässä säädettäisiin kyberkestävyysasetuksen 15 artiklan mukaisista vapaaehtoisista ilmoituksista, joita CSIRT-yksikkö ottaisi 1 momentin mukaisesti vastaan Euroopan unionin kyberturvallisuusvirasto ENISA:n ohella valmistajilta ja muilta tahoilta. Pykälän 2 momentin mukaan ei saisi ilman ilmoittajan suostumusta käyttää muun muassa ilmoittajaan kohdistuvassa rikostutkinnassa. Hallituksen esityksen pykäläkohtaisessa perustelussa todetaan, että kyberkestävyysasetuksen 15 artiklan 5 kohdan mukaisesti vapaaehtoinen ilmoittaminen ei saisi johtaa sellaisten lisävelvoitteiden asettamiseen ilmoituksen tehneelle luonnolliselle henkilölle tai oikeushenkilölle, joita siihen ei olisi sovellettu, jos se ei olisi toimittanut kyseistä ilmoitusta, sanotun kuitenkin rajoittamatta rikosten ennaltaehkäisemistä, tutkimista, paljastamista ja rikoksiin liittyviä syytöksiä.

Edellä olevan perusteella vaikuttaa, että säädettäväksi esitetty rajoitus käyttää vapaaehtoisesti luovutettavaa tietoa rikostutkintaan on ristiriidassa kyberkestävyysasetuksen 15 artiklan 5 kohdan kanssa, jossa nimenomaisesti ja pykäläkohtaisessa perustelussa kerrotaan, ettei asetuksessa säädetty rajoita tiedon käyttämistä rikosten ennalta ehkäisemiseen, tutkimiseen, paljastamiseen tai syytöksiin. Asetusta säädettäessä on nimenomaisesti mahdollistettu vapaaehtoisesti luovutetun tiedon käyttö rikostorjunnallisiin tarkoituksiin eikä tarkoituksena ole ollut estää tällaisen tiedon käyttöä todisteena.

3.4 Laki sähköisen viestinnän palveluista 21 a luku

Poliisi nostaa esiin huolensa siitä ovatko ehdotetut muutokset ja velvoitteet verkkotunusvälittäjiä ja edelleenvälittäjiä koskevan 21 a luvun osalta riittäviä ja tehokkaita viranomaistoiminnan näkökulmasta. Sääntely vaikuttaa mahdollistavan sen, että tietoverkoon voidaan avata palveluita laajalle henkilökunnalle, jopa globaalisti ilman, että taustalla olevia henkilöitä tai yrityksiä voidaan tai pyritään tunnistamaan millään tasolla. Tämä mahdollistaa myös rikollisille tai valtiollisille toimijoille valtavan potentiaalin, ilman että viranomaisilla on mitään mahdollisuuksia puuttua toimintaan, koska ketään henkilöä toiminnan todellisenä harjoittajana ei voida tunnistaa annettujen tietojen pohjalta eikä lainvastaiseen sisältöön voida puuttua, koska viranomaismääräyksiä tai seuraamuksia ei voida osoittaa millekään taholle.

Kun saman aikaisesti itse rikollinen infrastruktuuri (palvelimet) vuokrataan anonymisti ja käytettävissä olevat poliisin tiedonhankintakeinot ovat rajattuja henkilöllisesti ja vain aivan vakavimpiin rikoksiin, tietoverkosta on syntymässä toimintaympäristö vailla rikosoikeudellista kiinnijäämisriskiä. Tähän voidaan vielä lisätä se, että tietoverkossa myöskään sähköisten palveluntarjoajalla ei ole pääsääntöisesti veloitetta tunnistaa asiakkaitaan elleivät palveluntarjoajat koe sitä itse liiketoiminnallisesti tarpeelliseksi. Poliisi pitää suuntausta kokonaisuutena huolestuttavana.

Poliisi ehdottaa, että sääntelyä täsmennetään siten, että 21 a luvussa asetetut velvoitteet koskevat verkkotunnusvälittäjää, edelleenvälittäjää sekä niiden puolesta tai lukuun toimivia tahoja, kuten yksityisyyspalveluntarjoajia, jälleenmyyjiä tai välittäjäpalveluja. Edellä mainitusta voitaisiin säätää joko 21 a luvussa tai lain 3 §:ssä määritelmien yhteydessä, tarkoituksena saada lainsäädäntö kattamaan NIS 2 direktiivin tarkoittamassa laajuudessa eri toimijat.

Verkkotunnus olisi merkittävä verkkotunnuksen käyttäjän nimiin siten, että tämä käyttäjä ja toiminnasta vastuussa oleva taho on yksiselitteisesti yksilöitävissä ja tunnistettavissa ja siihen voidaan todellisuudessa kohdistaa viranomaisen toimenpiteitä. Ilmoitettavien tietojen osalta on varmistettava riittävällä tarkkuudella, että ilmoitetut tiedot ovat oikeita ja ajantasaisia. Verkkotunnusrekisteriin merkittävät tiedot ovat keskeisiä tietoja viranomaistoiminnassa eikä voitane tulkita, että tietoja kerätään ja ylläpidetään vain rekisterinpitäjälle osoitettuja valvontatehtäviä varten vaan myös muita laissa säädettyjä viranomaistehtäviä varten. Viranomaistarpeet poliisin osalta liittyvät sekä laittoman toiminnan keskeyttämiseen, että mahdollisuuden puuttua sinänsä laillisen toiminnan yhteydessä ilmi tulevaan lainvastaiseen materiaaliin ja sisältöön.

Kimmo Ulkuniemi, poliisitarkastaja

Asiakirja on sähköisesti allekirjoitettu asianhallintajärjestelmässä. Poliisi 19.02.2026 klo 09:50. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Poliisihallitus

Vuorimiehentie 3, PL 1000, 02151 Espoo

kirjaamo.poliisihallitus@poliisi.fi

Puhelin +358 295 480 181, Faksi +358 295 411 780, poliisi.fi