



## Lausunto

18.9.2025

 VN/27546/2023  
 VN/27546/2023-VM-4

Oikeusministeriö

Viite: Oikeusministeriön lausuntopyyntö VN/27546/2023, 7.8.2025

## Valtiovarainministeriön lausunto luonnoksesta hallituksen esitykseksi eduskunnalle laeiksi turvallisuustutkintalain ja kyberturvallisuuslain 17 §:n muuttamisesta

### Tausta

Oikeusministeriö on pyytänyt lausuntoa otsikossa mainitusta luonnoksesta hallituksen esitykseksi.

Hallituksen esitysluonnoksessa esitetään Onnettomuustutkintakeskukselle uutta toimivaltuutta suorittaa kyberturvallisuuteen kohdistuneiden erittäin vakavien kyberturvallisuuspoikkeamien turvallisuustutkintaa, jäljempänä kyberturvallisuustutkintaa. Esityksellä ehdotetaan lisäksi pantavan kansallisesti täytäntöön Euroopan unionin merionnettomuustutkintadirektiiviin tehdyt lainsäädäntötoimenpiteitä edellyttävät muutokset. Turvallisuustutkintalakiä ehdotetaan tarkistettavaksi myös joidenkin muiden sääntelykysymysten osalta. Kyberturvallisuuslain muuttamisen osalta kyse olisi informatiivisesta viittauksesta turvallisuustutkintalakiin.

Onnettomuustutkintakeskukselle ehdotettu uusi toimivaltuus suorittaa kyberturvallisuustutkintaa toteuttaa hallitusohjelman kohdan 10.1. kirjausta: *”Selvitetään mahdollisuus lisätä Onnettomuustutkintakeskuksen toimialaan kyberturvallisuuteen kohdistuneiden vakavien häiriöiden turvallisuustutkinta. Hallitus valmistelee tarvittaessa säädösmuutokset turvallisuustutkintalakiin ja tekee siihen muut tarvittavat tarkistukset.”*

Hallituksen esitys on valmisteltu virkatyönä oikeusministeriössä. Valmistelu on tapahtunut yhteistyössä Onnettomuustutkintakeskuksen kanssa, jonka lisäksi valmistelun yhteydessä on eri asiakysymyksiin liittyen konsultoitu eri viranomaistahoja.

### Lausunto

Valtiovarainministeriö esittää lausuntonaan seuraavaa:

Esityksessä nykytilasta todetaan, että *”merkittävänä puutteena voidaan pitää, että vakavistakaan kyberturvallisuuteen liittyvistä haitallisista tai vahingollisista tapahtumista ei riittävästi kerätä ja jaeta oppeja vastaavanlaisten tapahtumien ennalta estämiseksi ja vahinkojen välttämiseksi”*. Esityksessä olisi voinut tuoda esille, että nykytilassakin erittäin vakaviksi luettaviin kyberturvallisuuspoikkeamiin voidaan kohdistaa turvallisuustutkintalakiin (525/2011) perustuen poikkeuksellisen tapahtuman tutkintaa.

Esityksessä olisi voinut myös arvioida Onnettomuustutkintakeskuksen uutta kyberturvallisuustutkinnan toimivaltuutta suhteessa kyberturvallisuuden nykyisten toimijoiden kuten Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen ja Keskusrikospoliisin tehtäviin, osaamiseen ja resursseihin. Esi-merkiksi tuoreesta Suomen Kyberturvallisuusstrategiasta 2024–2035 on löydettävissä kattava kuvaus kyberturvallisuuden toimijoista ja toimintamallista.

Postiosoite  
 Postadress  
 Postal Address  
 Valtiovarainministeriö

Käyntiosoite  
 Besöksadress  
 Office

Puhelin  
 Telefon  
 Telephone

Faksi  
 Fax  
 Fax

s-posti, internet  
 e-post, internet  
 e-mail, internet

PL 28  
 00023 Valtioneuvosto

Snellmaninkatu 1 A  
 Helsinki

0295 16001  
 +358 295 16001

kirjaamo.vm@gov.fi

Esityksessä ei ehdoteta resurssilisäyksiä Onnettomuustutkintakeskukselle. Esityksessä ei ole arvioitu osaavien kyberturvallisuustutkijoiden tarvetta tai saatavuutta Onnettomuustutkintakeskuksen toteuttamaa tutkintaa varten. Kyberturvallisuustutkinnan tulokset ja vaikuttavuus kuitenkin perustuvat tutkintaa koskevan osaamisen lisäksi myös kyberturvallisuusalaan koskevaan osaamiseen.

Esitykseen toisi lisäarvoa kyberturvallisuustutkinnan kohteena oleville toimijoille tutkinnasta aiheutuvien resurssitarpeiden arviointi. Erityisesti tarpeen olisi arvioida viranomaisille kyberturvallisuustutkinnan perusteella annettavien suositusten toteuttamisesta aiheutuvia resurssitarpeita. Suositusten vaikuttavuus vähenee, jos niiden toteuttamiseen ei ole resursseja tai toteuttamista ei voida priorisoida.

Turvallisuustutkinnan uuden kyberturvallisuustutkinnan toimivaltuuden toimivuutta ja vaikuttavuutta olisi hyvä seurata, mutta tätä ei esitetä lain toimeenpanon seurannassa.

Turvallisuustutkintalain 22 §:n 1 momenttiin ehdotetaan kyberturvallisuustutkintaa varten lisättäväksi esineiden ja asiakirjojen ohella oikeus tarkastaa järjestelmiä ja ohjelmistoja. Ehdotuksesta ei käy selkeästi ilmi, mitä termillä järjestelmä tarkoitetaan. Lain 1 a§:ssä erittäin vakavan kyberturvallisuuspoikkeaman määritelmä ehdotetaan kiinnitettäväksi viestintäverkkoihin ja tietojärjestelmiin. Lain 22 §:n 1 momenttiin ehdotettu tarkastuksen kohteen määrittäminen eroaa julkisen hallinnon tiedonhallinnasta annetussa laissa (906/2019, jatkossa tiedonhallintalaki) ja kyberturvallisuuslaissa säädetystä oikeudesta *”saada tutkittavakseen valvontatehtävän kannalta välttämättömät tiedot, asiakirjat, laitteet ja ohjelmistot, suorittaa tarvittavia testejä ja mittauksia sekä tarkastaa viranomaisen/toimijan toteuttamat turvallisuusjärjestelyt”*.

Onnettomuustutkintakeskukselle esitetyt uudet kyberturvallisuustutkintaan liittyvät tiedonsaantioikeudet eivät pääsääntöisesti näyttäisi kohdistuvan viranomaisiin, koska viranomaisten kyberturvallisuusvelvollisuuksista ja niiden noudattamisen valvonnasta on säädetty tiedonhallintalain 4 a luvussa eikä kyberturvallisuuslaissa. Erittäin vakavia kyberturvallisuuspoikkeamia voi kuitenkin tapahtua myös muissa kuin kyberturvallisuuslain tarkoittamissa toimijoissa. Esityksen perusteluissa on todettu, että *”Erittäin vakavien kyberturvallisuuspoikkeamien tutkintaan liittyvän tiedonsaantioikeuden eriyttäminen onnettomuuksien ja vaaratilanteiden turvallisuustutkinnan tiedonsaantioikeuksista (20 §) olisi perusteltua, koska erittäin vakavien kyberturvallisuuspoikkeamien tutkinnassa tarvittaisiin huomattavasti erilaisempia tietoja kuin onnettomuuksien ja vaaratilanteiden tutkinnassa”*. Tämän takia on epäselvyyttä, ovatko turvallisuustutkintalain 20 §:n mukaiset tiedonsaantioikeudet soveltuvia kyberturvallisuustutkintaa koskeviksi tiedonsaantioikeuksiksi viranomaisilta. Esitetyt viranomaisia koskevat tiedonsaantioikeudet suhteessa erittäin vakaviin kyberturvallisuuspoikkeamiin jäävät siten osin epäselviksi.

Finanssialan digitaalisesta häiriönsietokyvystä säädetään erikseen EU:n DORA-asetuksessa (EU) 2022/2554, jonka valvovana viranomaisena Suomessa toimii Finanssivalvonta. Tietyt DORA-asetuksen soveltamisalan piirissä olevat toimijat tulisivat jatkossa ehdotetun lainsäädännön piiriin CER-direktiivin tarkoittamina kriittisinä toimijoina. Finanssialan toimijoiden sisällyttämistä sääntelyn soveltamisalaan tulisi harkita jatkovalmistelussa siten, että Onnettomuustutkintakeskuksella on tosiasiallinen mahdollisuus tutkia erittäin vakavia kyberturvallisuuspoikkeamia myös tällä toimialalla. Jos finanssiala jätetään soveltamisalasta pois, tulisi valinta perustella asianmukaisesti hallituksen esityksessä.

Valtiovarainministeriön tehtäviin kuuluu julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Siten myös valtiovarainministeriö voi olla viranomainen, jolle Onnettomuustutkintakeskus luovuttaa kyberturvallisuustutkinnassa saamiensa tietoja turvallisuustutkintalain 39 §:n tarkoittamissa tilanteissa, joissa se on välttämätöntä tärkeän yleisen edun turvaamiseksi.

Valtiovarainministeriöön ei ole oltu yhteydessä kyberturvallisuustutkintaa koskevan esityksen valmistelun aikana. Kuitenkin esimerkiksi Onnettomuustutkintakeskuksen Helsingin kaupungin tietomurtoa 2024 koskevassa tutkintaselostuksessa annetut suositukset on kohdistettu ensi sijassa valtiovarainministeriölle.

ICT-johtaja, ylijohdaja

Jarkko Levasma

Jakelu OM Oikeusministeriö

Tiedoksi VM JulkICT Palveluiden ja turvallisuuden ohjausyksikkö  
VM JulkICT Tietopolitiikka

**VN/27546/2023-VM-4**

Seuraavat henkilöt ovat allekirjoittaneet tämän asiakirjan sähköisesti /

Följande personer har undertecknat denna handling elektroniskt /

This document has been signed electronically by the following persons: