FiCom ry | JH
9.9.2026

FiComin lausunto hallituksen esityksestä laeiksi turvallisuustutkintalain ja kyberturvallisuuslain 17 §:n muuttamisesta

Hallintovaliokunta on pyytänyt FiComilta lausuntoa hallituksen esityksestä eduskunnalle laeiksi turvallisuustutkintalain ja kyberturvallisuuslain 17 §:n muuttamisesta (HE 71/2026 vp). FiCom kiittää mahdollisuudesta lausua asiasta ja esittää seuraavaa.

FiComin keskeiset viestit

- **Erittäin vakavien kyberturvallisuuspoikkeamien riippumaton turvallisuustutkinta on lähtökohtaisesti kannatettavaa.** Sääntelyn tulee kuitenkin olla täsmällistä ja tarkkarajaista etenkin silloin, kun toimivaltuudet kohdistuvat teleyritysten tietoihin, viestintäverkkoihin tai tuotantojärjestelmiin.
- **Ehdotettua 20 a §:ää on täsmennettävä.** Sääntely sisältää avoimia tietoluokkia, ja 2 momentin viittaus ”1 momentissa tarkoitettuun toimijaan” on epäselvä. Laista tulee käydä selvästi ilmi myös se, millä edellytyksillä voidaan saada viestinnän luottamuksellisuuden piiriin kuuluvia tietoja.
- **Poikkeaman torjunnan, rajaamisen ja palvelujen palauttamisen on oltava turvallisuustutkintaan nähden ensisijaista.** Tämä lähtökohta ilmenee perusteluista pykälätekstiä selvemmin.
- **Järjestelmiin ja ohjelmistoihin kohdistuvien toimivaltuuksien perusoikeusvaikutukset on arvioitava kattavammin.** Tuotannossa olevan viestintäverkon tarkastaminen voi mahdollistaa pääsyn välitystietoihin ja myös luottamuksellisten viestien sisältöön.
- **Yhden ilmoituksen periaate on säilytettävä.** Suorasta tiedonsaannista toimijalta ei tule muodostua uutta rinnakkaista raportointikanavaa.
- **Yrityksille aiheutuvat hallinnolliset, tekniset ja taloudelliset vaikutukset on otettava paremmin huomioon.**

Yleistä hallituksen esityksestä

Merionnettomuustutkintadirektiivin muutosten kansallinen täytäntöönpano ei anna FiComille aihetta huomautuksiin. Lausunto keskittyy erittäin vakavien kyberturvallisuuspoikkeamien turvallisuustutkintaan.

Riippumaton turvallisuustutkinta voi tuottaa arvokasta tietoa vakavien kyberturvallisuuspoikkeamien syistä ja ehkäistä vastaavia tapahtumia. Turvallisuustutkintalain (525/2011) 1 §:n mukaan turvallisuustutkintaa ei kuitenkaan tehdä oikeudellisen vastuun kohdentamiseksi. Tutkinnan itsenäinen tarkoitus on otettava huomioon myös toimivaltuuksia ja tietojen käyttöä koskevassa sääntelyssä.

Uuden tutkintamuodon toimivuus edellyttää, että toimivaltuudet rajataan selkeästi ja niiden käyttö sovitetaan yhteen käynnissä olevan poikkeaman hallinnan kanssa vaarantamatta kriittisten viestintäpalvelujen jatkuvuutta.

Tiedonsaantioikeutta koskevaa 20 a §:ää on täsmennettävä

Ehdotettu 20 a § muodostaisi erittäin vakavien kyberturvallisuuspoikkeamien tutkintaa koskevan erityisen tiedonsaantisäännöksen.

Pykälän 1 momentissa tiedonsaantioikeus kohdistuu kyberturvallisuuslain 11–13 §:ssä ja 28 §:n 1 ja 2 momentissa tarkoitettuihin tietoihin sekä yleisesti muihin valvovalla viranomaisella oleviin tutkinnassa välttämättömiin tietoihin. Pykälän 2 momentin 1 kohdan nojalla tutkintaa tekevä voisi lisäksi saada suoraan toimijalta tai tämän lukuun toimivalta taholta kaikki tutkinnan kannalta välttämättömät tiedot, jos niitä ei ole saatavissa valvovalta viranomaiselta.

Pykäläteksti ei tältä osin täysin vastaa säätämisjärjestysperusteluissa annettua kuvaa. Perusteluissa tiedonsaantioikeus esitetään pitkälti lueteltuihin tietoryhmiin rajattuna, vaikka pykäläteksti sisältää myös avoimia tiedonsaantioikeuksia. Tietoryhmät tulee tämän vuoksi yksilöidä laissa nykyistä tarkemmin.

Lisäksi 20 a §:n 2 momentin 1 kohdassa oleva viittaus ”1 momentissa tarkoitettuun toimijaan” on epäselvä ja tulee korjata. Pykälän 1 momentissa ei käytetä toimijan käsitettä, vaan siinä säädetään tiedonsaannista valvovilta viranomaisilta ja Finanssivalvonnalta. Perustelujen perusteella säännöksessä näyttää olevan tarkoitus viitata kyberturvallisuuslain 3 §:ssä tarkoitettuun toimijaan. Tämän tulee ilmetä yksiselitteisesti pykälätekstistä.

Myös 20 a §:n suhde sähköisen viestinnän luottamuksellisuuteen on arvioitava nimenomaisesti. Perustuslakivaliokunta piti kyberturvallisuuslain 28 §:n tiedonsaantioikeutta hyväksyttävänä sen

rajatun käyttötarkoituksen vuoksi. Ehdotetun 20 a §:n nojalla samoja tietoja voisi tulla toisen viranomaisen saataville eri tarkoitusta varten.

Esityksen valmistelussa on lisäksi nimenomaisesti päätetty olla ulottamatta turvallisuustutkintalain 21 §:ssä säädettyä teleyrityksiin kohdistuvaa välitys- ja sijaintitietojen tiedonsaantioikeutta erittäin vakavien kyberturvallisuuspoikkeamien tutkintaan. Tätä rajausta ei tule voida kiertää 20 a §:n yleisen tiedonsaantioikeuden kautta.

Pykälässä tulee siten yksilöidä tiedonsaantioikeuden kohteena olevat tietoryhmät, korjata virheellinen viittaus toimijaan sekä säätää nimenomaisesti siitä, millä edellytyksillä voidaan saada välitys- tai sijaintitietoja taikka muita luottamuksellisen viestinnän suojan piiriin kuuluvia tietoja.

Hallintovaliokunnan on perusteltua pyytää perustuslakivaliokunnan lausunto ehdotetuista 20 a ja 22 §:stä.

Poikkeaman hallinnan ja palvelujen palauttamisen tulee olla ensisijaista

Ehdotetun 17 a §:n mukaan Onnettomuustutkintakeskuksen tulee tutkinnan aloittamisessa huomioida kyberturvallisuuspoikkeaman hallintatoimenpiteiden asianmukaisen suorittamisen tarpeet.

Perustelujen mukaan turvallisuustutkinta tulisi kuitenkin aloittaa vasta, kun tilanne on riittävästi vakautunut, ja arvioinnin tulisi perustua vuoropuheluun hallintatoimenpiteitä suorittavan tahon ja Onnettomuustutkintakeskuksen välillä. Perusteluissa omaksuttu lähtökohta on siten pykälätekstiä vahvempi.

Erittäin vakavan kyberturvallisuuspoikkeaman aikana teleyrityksen ensisijaisena tehtävänä on poikkeaman torjuminen ja rajaaminen sekä palvelujen palauttaminen. Samoja rajallisia asiantuntijaresursseja tarvitaan myös turvallisuustutkintaan.

Lisäksi ehdotetun 18 §:n mukaisessa selvityksessä voitaisiin jo ennen varsinaisen turvallisuustutkinnan aloittamista käyttää 19 §:ssä tarkoitettuja toimenpiteitä, 20 a §:n tiedonsaantioikeuksia ja 22 §:n tarkastusoikeutta. Poikkeaman hallinnan ensisijaisuuden tulee siksi koskea myös tätä vaihetta.

Ehdotettuja 17 a ja 18 §:ää tulee täsmentää siten, etteivät selvitys- tai tutkintatoimenpiteet saa estää tai olennaisesti haitata poikkeaman torjumista, rajaamista tai kriittisten palvelujen palauttamista. Toimenpiteet tulee sovittaa yhteen poikkeaman kohteena olevan toimijan ja toimivaltaisen valvovan viranomaisen kanssa.

Järjestelmien tarkastamista koskeva toimivalta edellyttää tarkempaa rajaamista

Ehdotetun 22 §:n mukaan tutkintaa tekevällä olisi oikeus ottaa haltuun ja tarkastaa myös järjestelmiä ja ohjelmistoja. Ehdotetun 46 §:n nojalla Onnettomuustutkintakeskus voisi lisäksi uhkasakolla velvoittaa sallimaan pääsyn järjestelmään.

Perustelujen mukaan järjestelmä voi tarkoittaa myös viestintäverkkoa. Tuotannossa olevan viestintäverkon tai muun keskeisen tuotantojärjestelmän tarkastaminen poikkeaa olennaisesti fyysisen esineen haltuunotosta. Pääsy järjestelmään voi samalla mahdollistaa välitystietojen ja joissakin tilanteissa myös luottamuksellisten viestien sisällön käsittelyn, vaikka tutkinnan tarkoituksena ei olisi viestinnän sisällön selvittäminen.

Pykälään lisätty haittojen minimointia koskeva säännös on perusteltu, mutta se ei poista tarvetta täsmentää toimivaltuuksia tuotannossa olevien viestintäverkkojen ja muiden kriittisten järjestelmien osalta.

Myös ”haltuunoton” ja ”järjestelmään pääsyn” välinen suhde jää epäselväksi. Turvallisuustutkinnan tarpeet voidaan tuotantojärjestelmien osalta lähtökohtaisesti toteuttaa pääsyllä tarvittaviin tietoihin ja teknisillä jäljennöksillä ilman, että järjestelmä otetaan tutkintaviranomaisen tosiasialliseen hallintaan tai sen käyttöä palvelujen ylläpitämiseen rajoitetaan.

Ehdotettuja 22 ja 46 §:ää tulee täsmentää siten, että tuotannossa oleviin järjestelmiin kohdistuvat toimivaltuudet rajataan välttämättömään pääsyyn ja aineiston jäljentämiseen silloin, kun laajempi toimenpide voisi vaarantaa palvelujen jatkuvuutta. Myös sääntelyn suhde viestinnän luottamuksellisuuteen tulee arvioida nimenomaisesti.

Yhden ilmoituksen periaate on säilytettävä

Ehdotetun 16 a §:n ratkaisu, jonka mukaan ilmoituksen Onnettomuustutkintakeskukselle tekee valvova viranomainen eikä toimija, on perusteltu. Toimijan ei tule joutua erikseen arvioimaan, täyttääkö jo ilmoitettu merkittävä poikkeama myös turvallisuustutkintalain erittäin vakavan poikkeaman kynnyksen.

Myös 20 a §:n mukaisen suoran tiedonsaannin toimijalta tulee säilyä aidosti toissijaisena suhteessa valvovalta viranomaiselta saataviin tietoihin, jotta siitä ei muodostu uutta rinnakkaista raportointikanavaa.

Sääntelyä olisi lisäksi perusteltua täydentää siten, että toimijalle ilmoitetaan sitä koskevien tietojen luovuttamisesta Onnettomuustutkintakeskukselle, jollei ilmoittamisen lykkäämiselle ole tutkinnan turvaamiseen tai muuhun painavaan yleiseen etuun liittyvää perustetta.

Kyberturvallisuustutkinnassa saatujen tietojen luovuttamisesta on säädettävä yksiselitteisesti

Esityksen lähtökohta, jonka mukaan 39 §:ssä säädetyt tiedonluovutusoikeudet eivät oikeuttaisi luovuttamaan erittäin vakavan kyberturvallisuuspoikkeaman tutkintaa varten saatuja salassa pidettäviä tietoja, on perusteltu. Rajaus ilmenee kuitenkin vain perusteluista. Koska 3 momenttiin siirtyvässä säännöksessä viitataan yleisesti turvallisuustutkinnassa saatuihin tietoihin ja kyse voi olla myös turvallisuuskriittisestä aineistosta, rajauksen tulee käydä yksiselitteisesti ilmi pykälätekstistä.

Tutkintaselostuksessa on suojattava verkkojen ja järjestelmien turvallisuutta koskevat tiedot

Esityksen perusteluissa tunnistetaan, että kyberturvallisuuspoikkeaman tutkinnassa voidaan käsitellä salassa pidettäviä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevia tietoja.

Julkiseen tutkintaselostukseen ei tule sisällyttää järjestelmien turvajärjestelyjä, haavoittuvuuksia, yksityiskohtaisia lokitietoja tai muita teknisiä tietoja, joiden julkaiseminen voisi vaarantaa viestintäverkkojen tai tietojärjestelmien turvallisuutta.

Vaikutukset yrityksille ja kustannukset on arvioitava

Esityksen taloudellisten vaikutusten arviointi keskittyy pääasiassa Onnettomuustutkintakeskuksen resursointiin. Yrityksille aiheutuvia hallinnollisia, teknisiä ja taloudellisia vaikutuksia ei ole arvioitu vastaavalla tarkkuudella.

Tutkinta voi edellyttää toimijalta merkittävää asiantuntijatyötä esimerkiksi loki- ja järjestelmätietojen kokoamisessa, aineiston tuottamisessa ja järjestelmiin pääsyn järjestämisessä. Tätä työtä tekevät usein samat asiantuntijat, jotka vastaavat poikkeaman torjunnasta ja palvelujen palauttamisesta.

Ehdotetun 20 a §:n nojalla tiedot olisi luovutettava maksutta. Tämä voi olla perusteltua tavanomaisten lakisääteisten tietojenluovutusvelvoitteiden osalta. Sen sijaan viranomaisen pyynnöstä tehtävästä poikkeuksellisesta teknisestä avustamisesta ja merkittävästä lisätyöstä aiheutuvat kustannukset tulee korvata.

Turvallisuustutkintalain 45 §:n 3 momentin korvaussäännös koskee 22 §:ssä tarkoitetuista toimenpiteistä aiheutunutta vahinkoa. Ehdotetun 19 §:n mukaiset toimenpiteet näyttäisivät jäävän sen ulkopuolelle, tai ainakaan tämä ei käy esityksestä selvästi ilmi. Esimerkiksi paikan eristäminen tai kielto liikuttaa laitteita, järjestelmiä tai aineistoa voi kuitenkin viivästyttää palvelujen palauttamista ja aiheuttaa vahinkoa.

Poikkeuksellisesta teknisestä avustamisesta aiheutuvat kustannukset tulee korvata täysimääräisesti, ja 45 §:n 3 momentin korvaussäännös tulee ulottaa myös 19 §:ssä tarkoitetuista toimenpiteistä aiheutuviin vahinkoihin.

Lopuksi

FiCom kannattaa erittäin vakavien kyberturvallisuuspoikkeamien riippumattoman turvallisuustutkinnan mahdollistamista. Ehdotettu sääntely edellyttää kuitenkin vielä täsmentämistä erityisesti tiedonsaantioikeuksien, poikkeaman hallinnan ensisijaisuuden, järjestelmiin kohdistuvien toimivaltuuksien sekä yrityksille aiheutuvien vaikutusten osalta.

Täsmennyksillä voidaan varmistaa, että turvallisuustutkinta tuottaa hyödyllistä tietoa vakavien kyberturvallisuuspoikkeamien ehkäisemiseksi vaarantamatta poikkeamatilanteen hallintaa tai kriittisten viestintäpalvelujen jatkuvuutta.

Kunnioittavasti

FiCom ry

Janne Hälinen
juristi