FiCom ry

Lausunto

21.05.2026

Asia: VN/36541/2024

Lausuntopyyntö luonnoksesta hallituksen esitykseksi poliisilain 5 a luvun (siviilitiedustelu) muuttamiseksi ja siihen liittyviksi laeiksi

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

FiComin lausunto poliisilain 5 a luvun muuttamisesta

Sisäministeriö on pyytänyt FiComilta lausuntoa hallituksen esitysluonnoksesta poliisilain 5 a luvun muuttamiseksi ja eräiksi muiksi laeiksi. FiCom kiittää mahdollisuudesta lausua ja toteaa seuraavaa.

FiComin keskeiset viestit:

- FiCom pitää kansallisen turvallisuuden suojaamista ja siviilitiedustelun ajantasaisia toimintaedellytyksiä tärkeinä ja esityksen tavoitteita lähtökohtaisesti perusteltuina.
- Sääntelyn on kuitenkin oltava yrityksille ennakoitavaa, täsmällistä ja oikeasuhtaista. Sääntelyn tulee turvata viestintäverkkojen ja -palvelujen käytettävyys, eheys, kyberturvallisuus ja asiakkaiden luottamus.
- Sääntelyä ei tule tulkita tai soveltaa tavalla, joka edellyttäisi viestinnän välittäjiltä, tietoyhteiskunnan palvelun tarjoajilta tai teleyrityksiltä vahvan salauksen heikentämistä, takaporttien rakentamista, tietoturvakontrollien kiertämistä tai muita verkkojen ja palvelujen turvallisuutta vaarantavia ratkaisuja.
- Tietoliikennetiedustelun rajoitusten lieventäminen vaikuttaa viestinnän luottamuksellisuuden suojaan ja edellyttää täsmällistä sääntelyä, tehokasta ennakkolupamenettelyä, kohdennettua käyttöä, dokumentointia ja riippumatonta jälkivalvontaa.
- FiCom esittää muutoksia erityisesti poliisilain 5 a luvun 16, 39 a, 39 b, 51 ja 52 §:ään sekä tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin ehdotettuihin muutoksiin.

- Keskeisimmät muutosehdotukset koskevat yritykselle annettavaa tietoa ja yrityksen läsnäolo-oikeutta silloin, kun sen laitetiloihin, järjestelmiin, verkkoon, kytkentöihin tai verkon kriittisiin osiin kohdistuu viranomaisen toimenpiteitä.

- Viestinnän välittäjälle, tietoyhteiskunnan palvelun tarjoajalle ja teleyritykselle tulee turvata oikeus täysimääräiseen korvaukseen kaikista kustannuksista, jotka aiheutuvat viranomaisten avustamisesta. Korvaukset eivät saa rajoittua vain välittömiin kustannuksiin.

- Sääntelyssä tulee selkeyttää vastuunjakoa ja yrityksen vastuuvapautta tilanteissa, joissa viranomaisen toimenpide aiheuttaa palvelukatkoja, suorituskykyvaikutuksia, laite- tai konfiguraatiovaurioita, kyberturvallisuuspoikkeamia, vastatoimia, sopimussanktioita tai muita vahinkoja.

- Esitysluonnoksen yritysvaikutusten ja omaisuuden suojaa koskevien perusoikeusvaikutusten arviointia tulee täydentää. Arvioinnissa tulee huomioida myös vaikutukset aineettomaan omaisuuteen, yrityssalaisuuksiin, sopimusvastuisiin, asiakasluottamukseen ja yritysten kykyyn täyttää lakisääteiset käyttövarmuus- ja kyberturvallisuusvelvoitteensa.

Yleistä

FiCom ry pitää kansallisen turvallisuuden tiedonhankintakykyä tärkeänä ja pitää perusteltuna, että tiedustelulainsäädäntöä kehitetään teknologisen kehityksen ja muuttuneen turvallisuusympäristön edellyttämällä tavalla. Viestintäverkot ja niissä tarjottavat palvelut ovat välttämätön osa yhteiskunnan kriittistä infrastruktuuria, ja myös tiedusteluviranomaisten toimintaedellytykset voivat edellyttää toimivia teknisiä yhteistyömenettelyjä viestintäalan yritysten kanssa.

Samalla on välttämätöntä, että siviilitiedustelun toimivaltuudet ja yrityksille asetettavat avustamisvelvoitteet säädetään riittävän täsmällisesti. Viestintäverkkoihin, palvelualustoihin, konesaliympäristöihin, pilvi- ja verkkopalveluihin sekä muihin tuotantoympäristöihin kohdistuvat viranomaistoimenpiteet voivat aiheuttaa merkittäviä operatiivisia, teknisiä, taloudellisia ja oikeudellisia riskejä. Nämä riskit korostuvat erityisesti silloin, kun toimenpiteet kohdistuvat verkon kriittisiin osiin, tuotantoympäristöihin, liikenteen ohjaukseen, verkon hallintajärjestelmiin, kyberturvallisuusratkaisuihin tai tiloihin, joissa käsitellään useiden asiakkaiden tai yhteiskunnan kriittisten toimintojen tietoliikennettä.

FiCom korostaa, että viestintäalan yrityksillä on jo nyt laajoja lakisääteisiä velvollisuuksia huolehtia verkkojen ja palvelujen toimivuudesta, turvallisuudesta, häiriönhallinnasta, varautumisesta ja asiakkaiden oikeuksista. Viranomaisten tiedustelutoimivaltuuksien käyttö ei saa johtaa siihen, että yritys ei tosiasiallisesti pysty täyttämään näitä velvoitteitaan tai että yritys joutuu kantamaan vastuun viranomaisen toimenpiteen seurauksista.

Yritysvaikutusten ja perusoikeusvaikutusten arviointia tulee täydentää

Esitysluonnoksen yritysvaikutusten arviointia tulee täydentää erityisesti viestinnän välittäjien, tietoyhteiskunnan palvelun tarjoajien ja teleyritysten näkökulmasta. Esityksessä ehdotetaan sellaisia uusia tai laajentuvia toimivaltuuksia ja avustamisvelvoitteita, jotka voivat käytännössä kohdistua yritysten verkkoihin, laitetiloihin, järjestelmiin, palvelualustoihin, asiakkaiden liikenteeseen tai verkon kriittisiin osiin.

FiComin näkemyksen mukaan muutokset eivät ole yritysten kannalta vähäisiä. Vaikutusarvioinnissa tulee arvioida ainakin seuraavia vaikutuksia:

- vaikutukset viestintäverkkojen ja -palvelujen käyttövarmuuteen, kapasiteettiin, latenssiin, häiriönhallintaan ja kyberturvallisuuteen;
- vaikutukset yritysten lakisääteisiin varautumis-, tietoturva- ja häiriöilmoitusvelvoitteisiin;
- vaikutukset asiakkaiden kanssa sovittuihin palvelutasoihin ja mahdollisiin sopimussanktioihin;
- vaikutukset yritysten aineettomaan omaisuuteen, yrityssalaisuuksiin, verkkoarkkitehtuuriin ja teknisiin toteutustietoihin;
- vaikutukset asiakkaiden ja kansainvälisten sopimuskumppaneiden luottamukseen suomalaisiin viestintä- ja verkkopalveluihin;
- yrityksille aiheutuvat henkilötyö-, suunnittelu-, testaus-, käyttöönotto-, ylläpito-, valvonta-, tilaturvallisuus-, päivystys- ja muut kustannukset;
- vastuu- ja korvauskysymykset tilanteissa, joissa viranomaisen toimenpide aiheuttaa vahinkoa yritykselle, asiakkaalle tai kolmannelle osapuolelle.

Esitysluonnoksen perusoikeusvaikutusten arviointia tulee täydentää erityisesti omaisuuden suojan osalta. Kun toimivallan käyttö kohdistuu yrityksen tai yhteisön omistamiin tai hallitsemiin tuotteisiin, palveluihin, järjestelmiin tai tiloihin, vaikutuksia ei voida arvioida vain fyysisen omaisuuden näkökulmasta. Arvioinnissa tulee huomioida myös aineeton omaisuus, yrityssalaisuudet, sopimussuhteet, asiakasluottamus, maine, palvelutasositoumukset ja yrityksen mahdollisuus harjoittaa liiketoimintaansa häiriöttömästi.

Poliisilain 5 a luvun 14 a §: valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu

Esityksessä ehdotetaan poliisilain 5 a lukuun lisättäväksi uusi 14 a §, jossa säädettäisiin valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta. FiCom pitää toimivaltuutta sinänsä perusteltuna. Esitysluonnoksen kuvaus kybervakoilun ja -vaikuttamisen luonteesta sekä laite- ja järjestelmäketjujen merkityksestä on oikeansuuntainen.

Toimivaltuuden käyttäminen voi kuitenkin synnyttää uusia avustamistilanteita, joissa 51 §:n mukaiset velvoitteet kohdistuvat viestinnän välittäjiin, tietoyhteiskunnan palvelun tarjoajiin ja teleyrityksiin. Näiltä osin FiCom viittaa tässä lausunnossa esittämiinsä huomioihin tiedonsaannista, läsnäolo-oikeudesta, teknisestä koordinoinnista, vastuunjaosta ja kustannusten täysimääräisestä korvaamisesta.

Tietojärjestelmätiedustelun toteutus voi teknisen rakenteen vuoksi ulottua lähelle teleyrityksen ydinjärjestelmiä tai sen hallinnoimien palvelujen kriittisiä osia. Toimenpiteet tulee rajata yksilöityyn tietojärjestelmän osaan, eikä niitä tule ulottaa teleyrityksen keskeisiin hallinta-, valvonta- tai tuotantojärjestelmiin muutoin kuin poikkeuksellisesti ja mahdollisimman rajoitetusti.

Uuden toimivaltuuden ja sen edellyttämän avustamisen taloudelliset vaikutukset viestinnän välittäjiin, tietoyhteiskunnan palvelun tarjoajiin ja teleyrityksiin tulee arvioida jatkovalmistelussa täsmällisemmin ja ottaa huomioon avustamistilanteiden määrä, tarvittavat järjestelmä- ja prosessimuutokset, henkilötyö sekä kyberturvallisuus- ja käyttövarmuusvaikutukset.

Poliisilain 5 a luvun 16 §: laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Esitysluonnoksessa 16 §:ää muutettaisiin siten, että siinä huomioitaisiin valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu sekä mahdollistettaisiin tietyissä tilanteissa myös suojelupoliisin ulkopuolisen henkilön käyttäminen yksittäisen asennus- tai poistamistoimenpiteen suorittajana suojelupoliisin pyynnöstä ja valvonnassa. Lisäksi sääntely mahdollistaisi yksityisen tai yhteisön laitteen tai tietojärjestelmän tilapäisen käytön laitteen, menetelmän tai ohjelmiston asentamiseksi, poisottamiseksi ja tiedonsiirtämiseksi.

FiCom pitää tärkeänä, että 16 §:n soveltaminen sovitetaan yhteen viestinnän välittäjien, tietoyhteiskunnan palvelun tarjoajien ja teleyritysten käyttövarmuus-, kyberturvallisuus- ja asiakasvastuiden kanssa. Pykälän soveltaminen voi käytännössä kohdistua myös yritysten kriittisiin tuotantoympäristöihin, jolloin riskit ovat korostuneita.

Ilmoitus ja läsnäolo-oikeus

Toimenpiteitä ei tule toteuttaa yrityksen hallinnoimiin laitteisiin, järjestelmiin tai laitetiloihin siten, että yritys ei ole tietoinen siitä, että sen ympäristöön kohdistuu viranomaisen toimenpide. Sääntelyä tulee muuttaa niin, että yrityksellä on oikeus olla läsnä silloin, kun sen laitteisiin, järjestelmiin tai laitetiloihin tehdään asennus-, käyttöönottamis- tai poistotoimia.

Ilmoittamisen tulee olla toteutettavissa siten, ettei tiedustelun kohde tai sisältö paljastu yritykselle. Tietojen minimointi ja tiedustelun suojaaminen voidaan toteuttaa ilman, että yritys jätetään kokonaan tietämättömäksi sen tuotantoympäristöön kohdistuvasta teknisestä toimenpiteestä.

Rajaus yksilöityihin kohteisiin

Asennus- ja poistotoimenpiteiden tulee kohdistua vain yksilöityyn ja rajattuun laitteeseen, menetelmään tai ohjelmistoon. Toimenpiteitä ei tule ulottaa yrityksen keskeisiin hallinta-, valvonta-, tuotanto-, asiakas- tai muihin ydinjärjestelmiin muutoin kuin poikkeuksellisesti ja erityisen painavin perustein. Silloinkin toimenpide tulee toteuttaa mahdollisimman rajoitetusti ja siten, ettei siitä aiheudu vaikutuksia muille asiakkaille, palveluille tai verkon osille.

Vähäistä suuremman haitan täsmentäminen

Säännöksessä tulee täsmentää, miten haittaa arvioidaan viestintäalan tuotantoympäristössä. Haitan arvioinnissa tulee nimenomaisesti huomioida suorituskykyvaikutukset, kuten viive, kapasiteetti, pakettihävikki ja palvelun laadun heikkeneminen, sekä palvelutasosopimusten rikkomisesta aiheutuvat seuraamukset, ylimääräinen häiriönselvitystyö, palautustoimet, mainehaitta ja asiakasluottamuksen heikkeneminen.

Teleyritysympäristössä esimerkiksi liikenteen hidastuminen, palvelun laadun heikkeneminen tai valvontajärjestelmien hälytykset ovat tyypillisesti vähäistä suurempaa haittaa. Siksi sääntelyssä tulee selvästi edellyttää, ettei toimenpiteestä aiheudu vaikutuksia verkon tai palvelujen toimintaan.

Toteutus ei saa johtaa valvonta- tai suojaustoimiin

Tekniset järjestelyt tulee suunnitella viranomaisen ja yrityksen välisessä teknisessä yhteistyössä siten, etteivät ne aiheuta yrityksen valvonta-, tietoturva- tai häiriönhallintajärjestelmissä poikkeamahavaintoja tai automaattisia suojaamistoimenpiteitä. Tämä on välttämätöntä sekä käyttövarmuuden että operatiivisen turvallisuuden kannalta.

Vastuu ja täysimääräinen korvaus

Viranomaisen tulee vastata 16 §:ssä tarkoitetuista toimenpiteistä aiheutuvista vahingoista ja kustannuksista. Korvattavia tulee olla myös välilliset kustannukset, kuten lisätyö vianrajauksessa,

palautustoimet, sopimussanktiot ja muut asiakas- tai kolmansien osapuolten suhteissa syntyvät seuraamukset.

Yritykselle tulee turvata vastuuvapaus asiakassuhteiden ja kolmansille osapuolille aiheutuvien seuraamusten osalta siltä osin kuin haitta johtuu viranomaisen toimenpiteestä, viranomaisen edellyttämästä järjestelystä tai viranomaisen pyynnöstä toteutetusta avustamisesta.

Poliisilain 5 a luvun 39 a ja 39 b §: tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi

Esitysluonnoksen mukaan suojelupoliisilla olisi oikeus estää tietoteknisin menetelmin Suomen ulkopuolella olevan tietojärjestelmän käyttö sekä haitata tai muokata sen toimintaa, jos tietojärjestelmällä tai sen kautta voidaan aiheuttaa kansalliselle turvallisuudelle vakavaa vaaraa. Toimenpiteen käytön olisi oltava välttämätöntä vakavan vaaran torjumiseksi, eikä sillä saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi.

FiCom pitää uutta toimivaltuutta sinänsä ymmärrettävänä ja kansallisen turvallisuuden näkökulmasta perusteltuna. Samalla FiCom kiinnittää huomiota toimivaltuuden käytännön vaikutuksiin tilanteissa, joissa toimenpiteen tekninen toteutus tai sen vaikutukset liittyvät kotimaisten yritysten tarjoamiin verkkoyhteyksiin, transit-palveluihin, pilvi-, konesali- tai muihin tietoyhteiskunnan palveluihin.

FiCom pitää tärkeänä, että 39 a §:n soveltamisala säilyy esitysluonnoksen perusteluissa kuvatulla tavalla sidottuna siviilitiedustelutoimintaan. Toimivaltuutta ei tule tulkita yleiseksi tietojärjestelmien käytön estämistä tai haittaamista koskevaksi toimivaltuudeksi, vaan sen tulee liittyä tiedustelutoiminnassa havaittuun kansallista turvallisuutta vakavasti vaarantavaan toimintaan.

Toiminnan lähteenä näyttäytymisen riski

Jos suojelupoliisin toimenpiteessä tukeudutaan tai toimenpide vaikuttaa kotimaisen yrityksen tarjoamiin verkkopalveluihin, transit-yhteyksiin, konesaliympäristöihin, pilvipalveluihin tai muuhun tekniseen infrastruktuuriin, yritys voi ulkopuolisen tahon näkökulmasta näyttäytyä toiminnan lähteenä tai osapuolena. Tämä voi altistaa yrityksen vastatoimille, kyberhyökkäyksille, vahingonkorvausvaatimuksille, sopimusoikeudellisille seuraamuksille tai mainehaitalle.

Yritykselle tulee tällaisissa tilanteissa säätää selkeä vastuuvapaus ja oikeusturva. Yritys ei saa joutua vastuuseen viranomaisen toimenpiteestä tai sen ulkopuolisille näyttäytyvistä vaikutuksista.

Yrityksen tiedonsaanti lakisääteisten velvoitteiden täyttämiseksi

Jos 39 a §:ssä tarkoitettu toimenpide voi vaikuttaa yrityksen lakisääteisiin velvoitteisiin, kuten häiriöiden torjuntaan, tietoturvapoikkeamien käsittelyyn, verkon suojaamiseen, palvelun jatkuvuuteen tai asiakkaille annettaviin ilmoituksiin, yrityksellä tulee olla mahdollisuus saada riittävä tieto vaikutuksista velvoitteidensa täyttämiseksi.

Tiedon tulee olla vaikutusperusteista ja teknisesti rajattua. Sen ei tule paljastaa tiedustelun kohdetta, sisältöä tai operatiivista tarkoitusta. Yritykselle tulee kuitenkin antaa riittävä tieto siitä, miten toimenpide voi vaikuttaa yrityksen verkkoon, palveluihin, kyberturvallisuusvalvontaan, häiriönhallintaan tai asiakkaisiin.

Suojatoimet ja korvaukset

Jos viranomaisen toiminta lisää yritykseen kohdistuvaa hyökkäysuhkaa, vastatoimien riskiä tai muuta turvallisuusriskiä, viranomaisen ja yrityksen tulee sopia tarvittavista suojaavista toimenpiteistä ja niiden kustannusten korvaamisesta. Kaikki yritykselle aiheutuvat kustannukset ja vahingot tulee korvata täysimääräisesti.

39 b §:ssä säädettyä päätöksentekoa tulee täydentää siten, että päätöksessä arvioidaan myös toimenpiteen vaikutukset mahdollisiin kotimaisiin viestinnän välittäjiin, tietoyhteiskunnan palvelun tarjoajiin, teleyrityksiin ja muihin teknisiin palveluntarjoajiin. Päätöksessä tulee arvioida ainakin toimenpiteen vaikutukset yritysten palveluihin, kyberturvallisuuteen, vastatoimiriskiin, sopimusvastuisiin ja kustannuksiin sekä määritellä tarvittavat suojaavat toimenpiteet ja vastuunjako.

Poliisilain 5 a luvun 51 §: viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan avustamisvelvollisuus

Esitysluonnoksen mukaan viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan olisi ilman aiheetonta viivytystä tehtävä televerkkoon telekuuntelun, televalvonnan ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun edellyttämät kytkennät sekä annettava suojelupoliisin käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskisi tilanteita, joissa valtiolliseen toimijaan kohdistuva telekuuntelu, televalvonta tai televerkkoon kohdistuva tietojärjestelmätiedustelu toteutetaan suojelupoliisin toimesta teknisellä laitteella.

FiCom pitää välttämättömänä, että 51 §:ää täsmennetään. Ehdotettu säännös on viestintäalan yritysten näkökulmasta laaja ja voi käytännössä tarkoittaa verkon kriittisiin osiin kohdistuvia teknisiä

toimenpiteitä. Säännöksen soveltaminen voi edellyttää muutoksia tuotantoverkkoon, kytkentöihin, valvontajärjestelmiin, tilaturvallisuusjärjestelyihin tai henkilöstön päivystys- ja asiantuntijaresursointiin.

Ilmoitus ja läsnäolo-oikeus

Viestinnän välittäjälle, tietoyhteiskunnan palvelun tarjoajalle ja teleyritykselle tulee antaa tieto toimenpiteestä, ja sillä on oltava oikeus olla läsnä aina, kun sen laitetiloihin, järjestelmiin, verkkoon, kytkentöihin tai verkon kriittisiin osiin kohdistuu viranomaisen toimenpiteitä. Läsnäolo-oikeus on välttämätön verkon eheyden, käyttövarmuuden, kyberturvallisuuden, häiriönhallinnan ja vastuunjaon kannalta.'

Toimenpiteitä ei tule toteuttaa yrityksen hallinnoimiin laitteisiin, järjestelmiin, tiloihin tai verkon kriittisiin osiin niin, että yritys ei ole tietoinen siitä, että sen ympäristöön kohdistuu viranomaisen toimenpide. Ilmoittaminen tulee toteuttaa siten, ettei tiedustelun kohde, sisältö tai operatiivinen tarkoitus paljastu yritykselle. Tiedustelun suojaaminen ei edellytä sitä, että yritys jätetään kokonaan ilman tietoa sen omiin järjestelmiin tai verkkoon kohdistuvista teknisistä toimenpiteistä.

Lakiin tulee lisätä edellytys, että toimenpiteet koordinoidaan soveltuvin osin vähintään tietoturvaselvitetyn, nimetyn yritysyhteyshenkilön kanssa. Jos ennakkoilmoittaminen poikkeuksellisesti vaarantaisi toimenpiteen, laissa tulee säätää, että yritykselle annetaan viipymättä jälkikäteinen ilmoitus ja vähimmäistasoinen tekninen dokumentaatio verkon eheyden, häiriönhallinnan ja kyberturvallisuuden varmistamiseksi ilman, että tiedustelun kohde tai sisältö paljastuu.

Tekninen koordinointi ja muutoksenhallinta

Viestintäverkot ja palveluympäristöt ovat teknisesti erilaisia. Yksittäisten verkkojen arkkitehtuurit, hallintamallit, varmistusjärjestelyt, valvontamekanismit, kapasiteettiratkaisut ja häiriönhallintaprosessit poikkeavat toisistaan. Tästä syystä kytkentöjen ja muiden teknisten järjestelyjen menettelyistä ja reunaehdoista tulee sopia kahdenvälisesti viranomaisen ja yrityksen välillä.

Toimenpiteet tulee toteuttaa yrityksen turvallisuus-, kulunvalvonta-, muutoksenhallinta- ja käyttövarmuuskäytäntöjä noudattaen sekä ensisijaisesti tavalla, joka minimoi riskit. Käytännössä tämä voi edellyttää esimerkiksi sovittuja aikaikkunoita, saattovelvoitetta, etäjärjestelyjä, testauksia, rollback-suunnitelmia, dokumentointia, vianhallinnan yhteyspisteitä ja toimenpiteen jälkeistä tarkistusta.

Ehdotettu ilmaisu “ilman aiheetonta viivytystä” ei saa johtaa siihen, että tuotantoverkkoon tehtäisiin muutoksia ilman asianmukaista riskinarviointia, muutoksenhallintaa, testausta tai turvallista toteutusikkunaa. Säännöstä tulee täydentää siten, että velvoitteen toteuttamisessa otetaan huomioon toimenpiteen tekninen vaativuus, vaikutukset verkon toimintaan ja yrityksen lakisääteiset käyttövarmuus- ja kyberturvallisuusvelvoitteet.

Toimenpiteestä ei saa aiheutua havaittavia vaikutuksia verkon tai palvelun toimintaan

Kytkennät, tekniset laitteet, liikenteen ohjaukset tai muut järjestelyt tulee toteuttaa siten, ettei niistä aiheudu havaittavaa viiveen kasvua, kapasiteetin heikkenemistä, pakettihävikkiä, palvelun laadun heikkenemistä, valvontahälytyksiä, automaattisia suojaustoimia tai muuta suorituskykyyn tai palvelun toimintaan liittyvää muutosta.

Teleyritysten ja muiden viestintäalan toimijoiden tuotantoympäristöissä myös näennäisesti vähäiset suorituskykyvaikutukset voivat käynnistää valvonta- ja häiriönhallintaprosesseja, lisätä kustannuksia, aiheuttaa asiakashäiriöitä, johtaa palvelutasosopimusten rikkomiseen ja paljastaa operatiivista toimintaa. Tämän vuoksi vaikutukset verkon tai palvelun suorituskykyyn eivät ole viestintäalan yritysympäristössä vähäisiä.

Pääsy tiloihin ja kulunvalvonta

Esitysluonnoksen mukaan suojelupoliisilla sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä olisi oikeus telekuuntelua ja televerkkoon kohdistuvaa valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin viestinnän välittäjän tai tietoyhteiskunnan palvelun tarjoajan hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin.

FiCom pitää tärkeänä, että tiloihin pääsyä koskevaa sääntelyä täsmennetään. Viestintäverkkojen laitetilat, konesalit ja muut tekniset tilat ovat usein korkean turvallisuustason ympäristöjä, joiden kulunvalvonta, saattovelvoitteet, lokitus, valvonta ja pääsyoikeudet ovat keskeinen osa yrityksen kyberturvallisuus- ja käyttövarmuusvelvoitteiden täyttämistä.

Lakiin tulee kirjata, että pääsy yrityksen tiloihin ja niihin rinnastuviin teknisiin ympäristöihin toteutetaan yrityksen turvallisuus- ja kulunvalvontakäytäntöjä noudattaen. Yrityksellä tulee olla oikeus nimetä toimenpiteeseen osallistuva tai sitä valvova yhteyshenkilö, ellei tästä poikkeaminen ole yksittäistapauksessa välttämätöntä ja erikseen perusteltua.

Vastuunjako ja vastuuvapaus

51 §:ää tulee täydentää vastuunjakoa ja yrityksen vastuuvapautta koskevilla säännöksillä. Yritykselle ei saa syntyä ankaraa, epäsuoraa tai sopimusperusteista vastuuta viranomaisen toimenpiteestä, viranomaisen teknisestä laitteesta, viranomaisen edellyttämästä kytkennästä tai muusta erityisjärjestelystä aiheutuvista vaikutuksista.

Viranomaisen tulee vastata toimenpiteistään ja niistä aiheutuvista vahingoista ja kustannuksista siltä osin kuin ne johtuvat viranomaisen toiminnasta, viranomaisen laitteesta, viranomaisen edellyttämästä järjestelystä tai viranomaisen antamasta ohjeesta. Yritykselle tulee säätää selkeä vastuuvapaus ainakin seuraavista:

- palvelukatkot, viive, kapasiteettivaikutukset, pakettihävikki tai muut suorituskykyvaikutukset, jotka johtuvat viranomaisen toimenpiteestä;
- laite-, ohjelmisto- tai konfiguraatiovauriot;
- kyberturvallisuuspoikkeamat tai häiriötilanteet, jotka johtuvat viranomaisen toimenpiteestä tai sen vuoksi tehdyistä erityisjärjestelyistä;
- asiakkaiden tai kolmansien osapuolten vahingonkorvausvaatimukset;
- palvelutasosopimusten rikkomisesta aiheutuvat sopimussanktiot;
- yritykseen kohdistuvat vastatoimet tai kyberhyökkäykset, jos ne liittyvät viranomaisen toimintaan tai sen seurauksena syntyneeseen riskiin.

Tietojen minimointi

FiCom korostaa, että yrityksen avustamisen tulee rajoittua teknisiin järjestelyihin. Yritykselle ei tule antaa eikä sen tule saada tietoa siitä, mitä tai ketä viranomainen tiedustelee, millä perusteella tai millä menetelmillä, ellei tieto ole välttämätön yrityksen lakisääteisten velvoitteiden, käyttövarmuuden tai kyberturvallisuuden varmistamiseksi.

Kytkennän sijainti ja toteutustapa tulee valita niin, ettei yritykselle muodostu ilmeistä päätelmää tiedustelun kohteesta. Samalla yritykselle tulee antaa riittävä tekninen tieto siitä, miten toimenpide vaikuttaa sen verkkoon, järjestelmiin, tiloihin, valvontaan, häiriönhallintaan ja asiakasvastuisiin.

Poliisilain 5 a luvun 52 §: korvaus siviilitiedustelussa avustamisesta ja tietojen antamisesta

Esitysluonnoksen mukaan viestinnän välittäjällä ja tietoyhteiskunnan palvelun tarjoajalla olisi oikeus saada valtion varoista korvaus 51 §:ssä tarkoitetusta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista. Korvauksesta säädettäisiin sähköisen viestinnän palveluista annetun lain 299 §:ssä.

FiCom katsoo, että sääntely on tältä osin puutteellinen. Korvausoikeuden rajaaminen välittömiin kustannuksiin ei vastaa avustamisvelvollisuuksista yrityksille tosiasiallisesti aiheutuvia kustannuksia. Viestintäverkkoihin ja palveluympäristöihin kohdistuvat kytkennät ja muut viranomaisen edellyttämät järjestelyt voivat edellyttää merkittävää henkilötyötä, asiantuntijaresursseja, suunnittelua, testausta, käyttöönottoa, ylläpitoa, valvontaa, tilaturvallisuusjärjestelyjä, päivystystä, dokumentointia, auditointia ja verkkomuutoksia.

Avustamisvelvoitteet ovat lisääntyneet, mutta niiden taloudellisia kokonaisvaikutuksia ei ole arvioitu riittävästi. Eduskunnan liikenne- ja viestintävaliokunta on lausunnossaan LiVL 1/2022 vp korostanut, että kaikki viranomaistyöstä aiheutuvat kustannukset tulee korvata täysimääräisesti myös henkilötyön osalta. FiCom katsoo, että sama lähtökohta tulee ottaa huomioon myös poliisilain 5 a luvun ja sähköisen viestinnän palveluista annetun lain 299 §:n jatkovalmistelussa.

FiCom esittää, että 52 §:ää tai vaihtoehtoisesti sähköisen viestinnän palveluista annetun lain 299 §:ää tarkistetaan siten, että korvattaviin kustannuksiin luetaan nimenomaisesti myös henkilötyökustannukset. Yrityksiä ei ole perusteltua kohdella eri tavoin viranomaisen avustamista koskevissa korvaustilanteissa.

Lisäksi FiCom esittää, että käsittely- ja luovutusedellytyksiä sekä viranomaisavustamiseen liittyviä korvaussäännöksiä arvioidaan kokonaisuutena lähiaikoina, koska nykyinen sääntely on hajautunut ja osin epäselvä.

Yrityksillä tulee aina olla oikeus täysimääräiseen korvaukseen kaikista kustannuksista, jotka aiheutuvat viranomaisten avustamisesta, tietojen antamisesta, kytkentöjen tekemisestä, teknisten järjestelyjen toteuttamisesta tai viranomaisen toiminnan edellyttämästä erityisjärjestelystä.

52 §:ää tulee muuttaa siten, että korvattavia ovat ainakin:

- henkilötyökustannukset;
- suunnittelu-, valmistelu-, testaus- ja käyttöönottokustannukset;
- ylläpito-, valvonta-, tilaturvallisuus- ja päivystyskustannukset;
- dokumentointi-, auditointi- ja muutoksenhallintakustannukset;
- välttämättömät verkko-, järjestelmä- ja palveluympäristömuutokset;
- vianrajauksesta, palautustoimista ja häiriönhallinnasta aiheutuvat kustannukset;

- suojatoimet, jos viranomaisen toiminta lisää yritykseen kohdistuvaa kyber- tai vastatoimien riskiä;

- sopimussanktiot ja muut kustannukset, jotka aiheutuvat viranomaisen toimenpiteen vaikutuksista asiakkaisiin tai kolmansiin osapuoliin.

Korvausperusteiden tulee olla samat riippumatta siitä, missä roolissa yritys avustaa viranomaista. Ei ole perusteltua, että samaan viranomaisen tiedonhankintaa palvelevaan tekniseen kokonaisuuteen liittyvät kustannukset korvattaisiin eri tavalla riippuen siitä, katsotaanko yrityksen toimivan viestinnän välittäjänä, tietoyhteiskunnan palvelun tarjoajana, teleyrityksenä, konesalipalvelun tarjoajana, verkkopalvelun tarjoajana tai muussa teknisessä avustamisroolissa.

Tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin ehdotetut muutokset

Esitysluonnoksessa ehdotetaan muutoksia tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin. Muutokset koskevat muun muassa valtiolliseen toimijaan kohdistuvan tietoliikennetiedustelun määritelmää ja edellytyskynnystä, hakuehtojen määrittämistä, viestin sisältöä kuvaavien hakuehtojen käyttöä sekä Suomessa olevan tai oletettavasti olevan telepäätelaitteen tai teleosoitteen käyttöä hakuehtona. Lisäksi ehdotetaan, että tietoliikenteeseen kohdistuvan tiedustelun ilmoittamisvelvollisuudesta luovutaan.

FiCom ei ota kantaa tiedustelun operatiiviseen tarpeeseen, mutta pitää välttämättömänä, että muutosten tekniset vaikutukset, yritysvaikutukset ja vaikutukset asiakkaiden luottamukseen arvioidaan huolellisesti. Tietoliikennetiedustelun hakuehtoihin ja kohdentamiseen liittyvät muutokset voivat vaikuttaa siihen, millaisia teknisiä järjestelyjä viestinnän välittäjiltä ja muilta palveluntarjoajilta edellytetään ja millaisia vaikutuksia toimenpiteillä voi olla verkon toimintaan, luottamuksellisen viestinnän suojaan ja asiakkaiden käsitykseen palvelujen luotettavuudesta.

FiCom pitää tärkeänä, että tietoliikennetiedustelun tekninen toteutus rajataan aina välttämättömään ja mahdollisimman täsmälliseen. Hakuehtojen ja teknisten järjestelyjen tulee minimoida sivullisten viestinnän käsittely ja samalla vähentää viestintäalan yritysten tuotantoympäristöihin kohdistuvia riskejä.

Tietoliikenteeseen kohdistuvan tiedustelun ilmoittamisvelvollisuudesta luopumisen vaikutuksia tulee arvioida myös asiakkaiden luottamuksen ja oikeusturvan näkökulmasta. Mitä vähemmän yksilölle tai yritykselle syntyy jälkikäteistä tietoa tiedustelutoimenpiteistä, sitä tärkeämpää on, että laissa säädetään täsmällisistä ennakollisista ja jälkikäteisistä valvonta-, dokumentointi- ja vastuujärjestelyistä.

Sisällöllisten hakuehtojen käyttö

FiCom tunnistaa esitetyt perusteet sille, että sisällölliset hakuehdot voivat mahdollistaa kohdennetumman ja vähemmän sivullista viestintää käsittelevän tietoliikennetiedustelun. Muutos kohdistuu kuitenkin viestinnän luottamuksellisuuden ydinalueelle ja edellyttää poikkeuksellisen tiukkoja reunaehtoja: korkeaa soveltamiskynnystä, tehokasta riippumatonta ennakkolupamenettelyä, rajattua kohdentamista, selkeää sidosta kansallista turvallisuutta vakavasti uhkaavaan toimintaan sekä kattavaa jälkivalvontaa ja dokumentointia.

FiCom korostaa, ettei sääntelyä tule tulkita tai soveltaa tavalla, joka edellyttäisi teleyrityksiltä tai muilta viestinnän välittäjiltä salauksen heikentämistä, takaporttien rakentamista, tietoturvakontrollien kiertämistä tai muita verkkojen ja palvelujen turvallisuutta vaarantavia ratkaisuja. Toimivaltuuksien tulee olla tarkasti rajattuja ja perustua riippumattomaan ennakkolupaan, dokumentointiin ja jälkivalvontaan.

Suomessa olevan teleosoitteen tai telepäätelaitteen käyttö hakuehtona

Esityksessä ehdotetaan poistettavaksi voimassa oleva kielto käyttää hakuehtona Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

FiCom kiinnittää huomiota siihen, että muutos vaikuttaa viestinnän luottamuksellisuuden suojaan myös Suomessa viestivien henkilöiden osalta. Vaikka teleosoitteen tai telepäätelaitteen yksilöivä tieto voi olla tarkka hakuehto, muutos voi käytännössä lähentää tietoliikennetiedustelua yksilöön kohdistuviin tiedonhankintakeinoihin myös tilanteissa, joissa teletiedustelumenetelmien edellytykset eivät täyty. Tämän vuoksi viimesijaisuusedellytyksen, lupaharkinnan ja jälkivalvonnan merkitys korostuu.

FiCom pitää tärkeänä, että perusteluissa kuvataan nykyistä täsmällisemmin, missä tilanteissa Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti käyttämän telepäätelaitteen tai teleosoitteen yksilöivää tietoa voitaisiin käyttää hakuehtona ja miten varmistetaan, ettei muutos muodosta kiertotietä yksilöön kohdistuvien teletiedustelumenetelmien edellytysten ohi.

Matalamman edellytyskynnyksen soveltamisala

Esityksessä ehdotetaan, että tietoliikennetiedustelun käytön matalampaa edellytyskynnystä voitaisiin soveltaa tilanteissa, joissa tuomioistuimen lupa koskee valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennetiedustelua, eikä merkitystä olisi sillä, voiko tietoliikenteessä, johon hakuehtoja vertaillaan, kulkea muutakin kuin valtiollista tietoliikennettä.

Muutos on sinänsä ymmärrettävä esityksessä esitetyistä teknisistä syistä. FiCom kiinnittää kuitenkin huomiota siihen, että se käytännössä laajentaa matalamman edellytyskynnyksen soveltamisalaa, minkä vastapainona ennakkolupamenettelyn kohdentavuuden ja jälkivalvonnan tehokkuuden tulee toteutua aidosti.

FiCom pitää tärkeänä, että matalamman edellytyskynnyksen soveltaminen sidotaan käytännössä selvästi valtiollisiin toimijoihin tai niihin rinnastuviin tahoihin. Siitä ei saa muodostu yleisempää perustetta laajentaa tietoliikennetiedustelua liikenteeseen, jonka yhteys kansallista turvallisuutta vakavasti uhkaavaan toimintaan jää etäiseksi.

Tietoliikennetiedustelun tekninen toteuttaminen ja teknisten tietojen käsittely

Esityksessä ehdotetaan tarkennuksia tietoliikennetiedustelun tekniseen toteuttamiseen sekä uutta sääntelyä teknisten tietojen käsittelystä viestintäverkon osan, tietoliikenteen reitittymisen ja muutosten tunnistamiseksi sekä hakuehtojen määrittämiseksi.

FiCom korostaa, että varsinaisen tietoliikennetiedustelun ja teknisten tietojen käsittelyn välillä tulee säilyä riittävä erottelu. Koska reitittymisen ja muutosten seuranta voi koskea laajaakin tietoliikennettä, sääntelyn tarkkarajaisuus on viestinnän luottamuksellisuuden suojan kannalta keskeistä. Myöskään yhteistyö sotilastiedusteluviranomaisen kanssa ei saa hämärtää toimivaltuuksien rajoja.

Teknisten tietojen käsittelyä koskevien uusien säännösten tulee olla rajattuja siihen, mikä on välttämätöntä tietoliikennetiedustelun tekniseksi kohdentamiseksi, viestintäverkon osan ja tietoliikenteen reitittymisen tunnistamiseksi sekä hakuehtojen määrittämiseksi. Sääntelystä ja sen perusteluista tulee käydä selvästi ilmi, ettei teknisten tietojen käsittely muodosta itsenäistä tai laajempaa tiedonhankintatoimivaltuutta eikä johda viestin merkityssisällön käsittelyyn hakuehtojen määrittämisen yhteydessä.

Ilmoitusvelvollisuuden rajaaminen ja hävittämisvelvollisuus

FiCom tunnistaa nykyiseen ilmoitusvelvollisuuteen liittyvät käytännön haasteet. Muutos on kuitenkin merkityksellinen oikeusturvan kannalta, joten ennakkoluvan, riippumattoman valvonnan ja jälkivalvonnan tulee toteutua aidosti. Lisäksi hävittämisvelvollisuuden toteutuminen on varmistettava käytännössä.

Jos yksilölle annettavaa jälkikäteistä ilmoitusta rajataan merkittävästi, riippumattoman valvonnan ja dokumentoinnin merkitys korostuu. Sääntelyssä ja sen perusteluissa tulee varmistaa, että valvontaviranomaisella on riittävät tiedot ja keinot arvioida toimivaltuuksien käytön lainmukaisuutta, kohdentamista ja tarpeettoman tiedon hävittämistä.

Rajavartiolaitoksen avustava rooli

Esitysluonnoksessa ehdotetaan Rajavartiolaitokselle mahdollisuutta avustaa suojelupoliisia eräiden tiedustelumenetelmien käytössä. FiCom ei vastusta viranomaisten välistä tarkoituksenmukaista yhteistoimintaa, mutta pitää tärkeänä, että yritysten näkökulmasta vastuut ja yhteydenpito eivät hämärry.

Jos Rajavartiolaitos avustaa suojelupoliisia toimenpiteessä, joka vaikuttaa viestinnän välittäjään, tietoyhteiskunnan palvelun tarjoajaan, teleyritykseen tai muuhun palveluntarjoajaan, suojelupoliisin tulee vastata viranomaisyhteydenpidosta, ohjeistuksesta, dokumentaatiosta, vastuista ja korvauksista suhteessa yritykseen. Yrityksen ei tule joutua epäselvään tilanteeseen siitä, mikä viranomainen vastaa toimenpiteestä, sen vaikutuksista, vahingoista tai kustannuksista.

Ehdotukset sääntelyn täsmentämiseksi

FiCom esittää, että jatkovalmistelussa poliisilain 5 a lukua ja siihen liittyviä lakeja muutetaan ainakin seuraavasti:

1. 51 §:ään lisätään säännökset yrityksen tiedonsaannista ja läsnäolo-oikeudesta. Yrityksellä tulee olla oikeus olla läsnä, kun sen laitteisiin, järjestelmiin, tiloihin, verkkoon, kytkentöihin tai verkon kriittisiin osiin kohdistuu viranomaisen toimenpiteitä.

2. 51 §:ään lisätään velvollisuus tekniseen koordinointiin. Toimenpiteet tulee koordinoida vähintään tietoturvaselvitetyn, nimetyn yritysyhteyshenkilön kanssa, ellei tästä poikkeaminen ole yksittäistapauksessa välttämätöntä ja erikseen perusteltua.

3. 51 §:ään lisätään vaatimus muutoksenhallinnan ja yrityksen turvallisuuskäytäntöjen noudattamisesta. Toimenpiteet tulee toteuttaa tavalla, joka minimoi käyttövarmuus-, kyberturvallisuus- ja häiriöriskit.

4. 51 §:ään ja 16 §:ään lisätään vaatimus siitä, ettei toimenpiteestä saa aiheutua vaikutuksia verkon tai palvelun toimintaan. Erityisesti viive, kapasiteetin heikkeneminen, pakettihävikki, palvelun laadun heikkeneminen, valvontahälytykset ja automaattiset suojaustoimet tulee huomioida.

5. 16 §:ää täsmennetään siten, että toimenpiteet rajataan yksilöityihin kohteisiin. Yrityksen ydinjärjestelmiin, hallinta- ja valvontajärjestelmiin tai tuotantoympäristöihin ei tule kohdistaa toimenpiteitä ilman erityisen painavia perusteita.

6. 39 a ja 39 b §:ään lisätään velvollisuus arvioida vaikutukset kotimaisiin palveluntarjoajiin. Päätöksenteossa tulee arvioida myös yrityksiin kohdistuvat vaikutukset, vastatoimiriskit, kyberturvallisuusriskit, sopimusvastuut, kustannukset ja tarvittavat suojatoimet.

7. 52 § muutetaan täysimääräisen korvauksen periaatteen mukaiseksi. Korvausten tulee kattaa kaikki viranomaisen avustamisesta, tietojen antamisesta, kytkennöistä, teknisistä järjestelyistä, suojatoimista, henkilötyöstä ja mahdollisista vahingoista aiheutuvat kustannukset.

8. Lakiin lisätään selkeät vastuunjako- ja vastuuvapaussäännökset. Yritys ei saa joutua vastuuseen viranomaisen toimenpiteestä, viranomaisen laitteesta, viranomaisen edellyttämästä järjestelystä tai viranomaisen toiminnasta aiheutuvista vahingoista, sopimussanktioista tai kolmansien osapuolten vaatimuksista.

9. Tietoliikennetiedustelun muutosten tekniset ja yritysvaikutukset arvioidaan tarkemmin. Erityisesti hakuehtojen muutokset, Suomessa olevan telepäätelaitteen tai teleosoitteen käyttö hakuehtona ja ilmoittamisvelvollisuudesta luopuminen edellyttävät huolellista vaikutusarviointia.

10. Tietoliikennetiedustelun hakuehtojen muutoksiin lisätään täsmälliset reunaehdot. Sisällöllisten hakuehtojen, Suomessa olevan teleosoitteen tai telepäätelaitteen käytön ja matalamman edellytyskynnyksen soveltamisen tulee perustua tehokkaaseen ennakkolupaan, kohdennettuun käyttöön, dokumentointiin ja riippumattomaan jälkivalvontaan.

11. Vahvan salauksen ja palvelujen tietoturvan suoja kirjataan selvästi perusteluihin. Sääntelyä ei tule tulkita siten, että se edellyttäisi salauksen heikentämistä, takaportteja, tietoturvakontrollien kiertämistä tai muita verkkojen ja palvelujen turvallisuutta vaarantavia ratkaisuja.

12. Teknisten tietojen käsittely rajataan välttämättömään. Sääntelystä tulee käydä selvästi ilmi, ettei teknisten tietojen käsittely muodosta itsenäistä tai varsinaista tietoliikennetiedustelua laajempaa tiedonhankintatoimivaltuutta.

Yhteenveto

FiCom pitää esityksen tavoitetta kansallisen turvallisuuden suojaamisesta tärkeänä ja siviilitiedustelun toimintaedellytysten kehittämistä lähtökohtaisesti perusteltuna. Sääntelyn tulee kuitenkin olla yrityksille täsmällistä, ennakoitavaa ja oikeasuhtaista.

Ehdotetut muutokset voivat vaikuttaa merkittävästi viestinnän välittäjiin, tietoyhteiskunnan palvelun tarjoajiin ja teleyrityksiin, jotka ylläpitävät yhteiskunnan kriittistä viestintäinfrastruktuuria. Siksi lakiin tulee lisätä täsmälliset menettely-, vastuu- ja korvaussäännökset. Yrityksille tulee turvata riittävä tiedonsaanti, läsnäolo-oikeus, tekninen koordinointi, vastuuvapaus ja täysimääräinen korvaus kaikista viranomaisten avustamisesta aiheutuvista kustannuksista ja vahingoista.

FiCom korostaa, että esitysluonnoksen muutokset on tarkoituksenmukaista käsitellä yhteen sovitettuna kokonaisuutena puolustusministeriössä valmistellun sotilastiedustelulainsäädännön

muutoksen kanssa. Avustamisvelvollisten ja korvauksensaajien joukko, korvauksen kattavuus, läsnäolo-oikeus, vastuunjako ja muut keskeiset ratkaisut tulee yhdenmukaistaa siten, ettei avustavaa yritystä kohdella eri tavoin eri sääntely-yhteyksissä.

FiCom pitää välttämättömänä, että siviili- ja sotilastiedustelun sääntelykokonaisuuksissa turvataan samantasoiset menettelylliset takeet, kustannusten korvaaminen ja avustavan yrityksen oikeusturva. Yrityksen näkökulmasta kustannukset, tekniset riskit ja vastuut eivät riipu siitä, perustuuko avustaminen siviili- vai sotilastiedustelua koskevaan sääntelyyn.

Näin voidaan turvata sekä tiedusteluviranomaisten toimintaedellytykset että viestintäverkkojen ja -palvelujen käyttövarmuus, kyberturvallisuus, asiakkaiden luottamus ja yritysten oikeusvarmuus.

Lahtinen Marko
FiCom ry