Teknologiateollisuus ry

Lausunto

21.05.2026 VN/36541/2024

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

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

Teknologiateollisuus, sekä Kyberala kiittävät mahdollisuudesta lausua hallituksen esitysluonnoksesta, joka koskee poliisilain 5 a luvun muuttamista sekä siihen liittyviä muita lainsäädäntömuutoksia (yhteinen lausunto). Teknologiateollisuus ry edustaa yli 1800 jäsenyritystä, jotka vastaavat puolesta Suomen viennistä, tutkimus- ja kehitysinvestoinneista ja työllistävät suoraan ja välillisesti neljäsosan suomalaisista. Kyberala ry on Teknologiateollisuus ry:n toimialayhdistys ja edustaa Suomessa toimivaa kyberturvallisuusalaa. Viittaamme lausunnossamme myös Elinkeinoelämän keskusliitto EK:n lausuntoon.

Tiivistelmä

Yhteenvetona toteamme, että:

Ehdotus ei täytä hallitusohjelman edellyttämää kokonaisvaltaista, talous- ja yritysvaikutukset huomioivaa lainvalmisteluaohjausta: yritys- ja kilpailukykyvaikutukset yritysten toimintaympäristöön, aineettomaan omaisuuteen, sopimussuhteisiin sekä Suomen houkuttelevuuteen luotettavan digitaalisen liiketoiminnan ja investointien sijaintipaikkana tulee sisällyttää ehdotukseen

Tietojärjestelmätiedustelun kohdentamisen laajentaminen loogisiin kokonaisuuksiin koskevasta sääntelystä ja sen perusteluista on selkeästi ilmettävä, miten tuomioistuimen laadukas ennakkokontrolli varmistetaan

Laitteen, menetelmän tai ohjelmiston asentamista koskevan sääntelyn perusoikeusarvio on omaisuudensuojan osalta puutteellinen, ulkopuolisen avustajan asema kestämätön suhteessa työnantajan ja asiakassopimusten velvoitteisiin, ja vahingonkorvausvastuusta on säädettävä täsmällisesti säännöstasolla

Peitetoiminnan kirjallinen lopettamispäätös tulee säilyttää, ja yksinomaan tietoverkossa toteutettavalta peitetoiminnalta on edellytettävä nykyistä tarkempaa kohdentamista

Ulkomaisiin tietojärjestelmiin kohdistuvien estotoimien päätöksenteon tulee olla poliittista ja poikkihallinnollista, ja kansainvälisoikeudellinen sekä talous- ja ulkopoliittinen vaikutusarvio on tehtävä huomattavasti nykyistä perusteellisemmin

Viestinnän välittäjien ja tietoyhteiskunnan palvelun tarjoajien avustamisvelvollisuuksia laajennettaessa kaikki välittömät kustannukset on korvattava täysimääräisesti ja eri toimijoille yhdenmukaisesti

Päästä-päähän-salausta (E2EE) ei tule heikentää avustamisvelvoitteen kautta

Tietoliikennetiedustelun sisällöllisten hakuehtojen rajauksista luopumiselle ei ole esitetty riittäviä perusteluja

Tietoliikennetiedustelun käyttöä koskevan ilmoitusvelvollisuuden rajaamista on harkittava esitettyä huolellisemmin

Yleistä

Pidämme tärkeänä, että Suomen tiedustelulainsäädäntöä kehitetään vastaamaan muuttunutta turvallisuus- ja kybertoimintaympäristöä. Turvallisuusympäristön heikkeneminen, valtiollisten toimijoiden lisääntynyt kyber-, hybridi- ja informaatiovaikuttaminen sekä teknologian nopea kehitys edellyttävät viranomaisilta riittäviä ja ajantasaisia toimivaltuuksia kansallisen turvallisuuden turvaamiseksi.

Samalla korostamme, että tiedustelutoimivaltuuksien laajentamisen tulee perustua perusoikeuksien kannalta tarkkarajaiseen, oikeasuhtaiseen ja ennakoitavaan sääntelyyn Säännösmuutoksia on osin perusteltu kapeasti ja erityisen valtiokeskeisesti, ennen kaikkea tiedustelun tarpeisiin ja kansalliseen turvallisuuteen liittyvien näkökohtien osalta. Esitettyjen tiedusteluvaltuuksien käyttö tulisi kuitenkin koskemaan laajsti yrityksiä, yhteisöjä ja kansalaisia, jotka yhdessä muodostavat sen toimijoiden kokonaisuuden, miksi valtio ylipäätään on olemassa. Yritysten toimintaympäristön vakaus, oikeusvarmuus ja luottamus digitaalisiin palveluihin sekä yritysten oikeuteen suojella liike- ja ammattisalaisuuksia ovat keskeisiä tekijöitä Suomen kilpailukyvylle ja investointien houkuttelevuudelle. Näiden näkökulmien huomiointi on välttämätöntä lainsäädännön valmistelussa. Kyse ei ole yksinomaan siitä, mitkä ovat toimivallan tosiasialliset rajat, vaan millainen vaikutelma Suomesta syntyy luottamukseen perustuvan liiketoiminnan sijaintipaikkana.

Lakiehdotuksessa perustellaan iedustelulainsäädännön kehittämistä Orpon hallitusohjelman turvallisuutta koskevista kirjauksista. Ehdotuksessa ei kuitenkaan huomioida riittävästi koko hallitusohjelman toimintaperiaatteita (s. 7–8), jotka muodostavat kaikkia kirjauksia ohjaavat, ja osin rajoittavatkin, reunaehdot eri toimenpiteiden toteuttamiselle.

Toimintaperiaatteiden mukaan Suomen vahva demokratia ja korkea luottamus julkisiin instituutioihin rakentuvat avoimesta, vastuullisesta ja johdonmukaisesta hallinnosta, joka edistää turvallisuutta, yhdenvertaisuutta, osaamista ja hyvinvointia sekä toimii osana sääntöpohjaista kansainvälistä järjestelmää. Hallitus vaalii oikeusvaltiota ja huolellista, tietoperustaista lainvalmistelua varmistaakseen yhteiskunnan vakauden ja perusoikeuksien suojan. Kansalaisten ja viranomaisten välisessä suhteessa vaalitaan hyvän hallinnon periaatteita. Muita periaatteita ovat:

Hyvinvoinnin perusta on kestävä talous ja tärkein talouspoliittinen tavoite on kestävä kasvu

Avoimeen markkinatalouteen perustuvan oikeusvaltion rooli on toimivan, turvallisen ja oikeudenmukaisen yhteiskunnan rakentaminen

Poliittisen- ja hallintovallan tehtävä on tarjota puitteet vapaudelle ja mahdollisuuksille

Ehdotuksessa on käsitelty kattavasti Orpon hallitusohjelman tavoitteita tiedustelulainsäädännön kehittämisestä viranomaisten toimintakyvyn turvaamiseksi osana kansallisen puolustuskyvyn ja turvallisuuden kokonaisuutta. Koska kestävä (ts. vahva) talous on myös yhteiskunnan kriisinsietokyvyn, kansallisen puolustuskyvyn ja sisäisen turvallisuuden ylläpitämisen tärkein strateginen edellytys, tulisi varmistaa, että ehdotetut sotilastiedustelun kehittämiseen tai toimivaltuuksien laajentamiseen liittyvät toimet eivät vaaranna tai heikennä tämän tavoitteen saavuttamista. Ehdotuksen vaikutukset elinkeinoelämään, yrityksiin ja talouteen tulisi siten käsitellä

kattavammin jatkovalmistelussa. Myös oikeussubjektien vapauden varmistaminen edellyttää, että valtio ei puutu lailliseen toimintaan enempää, kuin on välttämätöntä. Muiden yllä mainittujen reunaehtojen osalta huomiot löytyvät kustakin keskeistä muutosehdotusta koskevasta osiosta alta.

Esityksessä ehdotetaan useita muutoksia, joilla on suoria tai välillisiä vaikutuksia yrityksiin, erityisesti viestinnän välittäjiin, datakeskustoimijoihin sekä muihin digitaalisen infrastruktuurin ylläpitäjiin. Teknologiateollisuus korostaa, että yrityksiin kohdistuvien velvoitteiden tulee olla selkeästi määriteltyjä, teknisesti toteuttamiskelpoisia ja oikeasuhtaisia suhteessa tavoiteltuun turvallisuushyötyyn.

Velvoitteiden ei tule muodostaa kohtuutonta hallinnollista tai taloudellista taakkaa, eikä niiden tule heikentää Suomen asemaa houkuttelevana sijaintipaikkana digitaalisen teollisuuden investoinneille. Pidämme tärkeänä, että mahdolliset avustamisvelvollisuudet rajataan täsmällisesti ja että niiden soveltamiseen liittyvät menettelyt, kustannusten korvaaminen sekä vastuut määritellään selkeästi. Yritysten rooli kansallisen kyberturvallisuuden varmistamisessa on keskeinen, mutta tämän roolin tulee perustua ennakoitavaan sääntelyyn ja toimivaan yhteistyöhön viranomaisten kanssa. Tietosuojaan ja luottamuksellisen viestinnän suojaan liittyvät kysymykset ovat keskeisiä hallituksen esityksen arvioinnissa. Yritysten asiakkaat ja kansainväliset kumppanit edellyttävät korkeaa tietosuojan tasoa ja luottamusta palveluiden turvallisuuteen.

Teknologisen kehityksen nopeus edellyttää, että sääntely yleisesti on mahdollisimman teknologianeutraalia ja joustavaa. Liian yksityiskohtainen ja teknisesti sidottu sääntely voi vanhentua nopeasti ja johtaa tulkintaongelmiin. Lainsäädännön tulisi mahdollistaa viranomaisten toiminta muuttuvassa toimintaympäristössä ilman, että se samalla luo tarpeettomia epävarmuuksia yrityksille.

Teknologiateollisuus pitää tärkeänä, että esityksen jatkovalmistelussa arvioidaan huolellisesti yrityksiä koskeva vaikutusten arviointi. Samalla tulee varmistaa esityksen oikeasuhtaisuus sekä turvataan Suomen kilpailukykyä digitaalisessa taloudessa. Lopuksi Teknologiateollisuus korostaa viranomaisten ja yritysten välisen yhteistyön merkitystä. Siviilitiedustelun ja sisäisen turvallisuuden vahvistaminen edellyttää tiivistä ja luottamukseen perustuvaa yhteistyötä julkisen ja yksityisen sektorin välillä. Ehdotuksen tulisi tukea yhteistyötä ja kannustaa yhteisten toimintamallien kehittämiseen. Lainvalmistelussa tulisi välttää suppeata ja viranomaiskeskeistä vuoropuhelua.

Säännöskohtaiset perustelut

Laki poliisilain 5 a luvun muuttamisesta

14 a § Valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelu

Teknologiateollisuus pitää tietojärjestelmätiedustelun kohdentamisen laajentamista loogisiin kokonaisuuksiin lähtökohtaisesti kannatettavana, sillä nykyaikaiset tietojärjestelmät rakentuvat tyypillisesti hajautetuista ja toisiinsa kytkeytyvistä osakomponenteista, joiden tehokas tiedustelu edellyttää kokonaisuuden tarkastelua. Esitykseen sisältyy kuitenkin merkittäviä oikeusturvariskejä, jotka jatkovalmistelussa on otettava vakavasti. Keskeisin ongelma on, että ratkaisu yksittäisten osien kuulumisesta tiedustelun kohteena olevaan loogiseen kokonaisuuteen jää käytännössä viranomaisen tehtäväksi, jolloin tuomioistuimen tosiasiallinen ennakkokontrolli heikkenee ja kohdentaminen voi laajentua ennakoimattomalla tavalla muun muassa yritysten hallinnassa oleviin järjestelmiin.

Tämän vuoksi sekä säännöstekstistä että sen perusteluista tulee selkeästi ilmetä, miten tuomioistuimen laadukas ennakkokontrolli varmistetaan niin, ettei lupa loogisen kokonaisuuden määrittelylle muodostu tarpeettoman laajaksi. Tuomioistuimen on kyettävä jo lupaharkinnassa arvioimaan loogisen kokonaisuuden rajat riittävän täsmällisesti, ja viranomaisen myöhempi harkinta järjestelmän osien kuulumisesta kokonaisuuteen tulee sitoa nimenomaisiin, säädöstasolla määriteltyihin kriteereihin. Vain tällä tavoin voidaan turvata se, että toimivaltuuden käytön kohteena olevien yritysten ja muiden toimijoiden oikeusturva ja ennakoitavuus säilyvät tiedustelun tehokkuuden rinnalla. Säänetelyn tarkentamisen tarkoituksena ei ole suojata Suomen oikeudekäyttöpiirin alueelle laittomasti toimivaa valtiollista tahoa, vaan varmistua siitä, että sääntelyyn tutustuminen luo riittävän ymmärryksen ja luottamuksen siihen, että toiminnalle on olemassa uskottavasti valvotut rajoitteet ja siten kolmannet osapuolet ovat suojassa yksityiselämään puuttumisesta ja että salaisten viranomaistoimenpiteiden soveltamisen seuraukset ovat ennakoitavissa.

16 § Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen siviilitiedustelussa

Ehdotuksen mukaan suojelupoliisi saisi tilapäisesti käyttää yksityisen tai yhteisön laitetta tai tietojärjestelmää tiedustelumenetelmän asentamiseksi tai poistamiseksi, kunhan vähäistä suurempaa haittaa ei aiheudu. Yksittäisen toimenpiteen ei katsottu puuttuvan merkittävästi omaisuudensuojaan toimenpiteen lyhyen keston vuoksi.

Teknologiateollisuus pitää säännösehdotuksen perusoikeusvaikutusten arviota omaisuudensuojaan selvästi riittämättömänä. Kun toimenpiteen kohteena on yritys tai yhteisö, jonka tuotteisiin tai palveluihin toimivaltaa käytetään, vaikutukset on välttämätöntä arvioida myös aineettoman omaisuuden, sopimusvaikutusten, tuotanto- ja arvoketjun sekä toimintaan kohdistuvan luottamuksen kannalta. Yrityssalaisuudet, liiketoimintatiedon luottamuksellisuus ja kyky vastata toiminnasta sopimusehtojen sekä mm. ylikansallisten toimivaltavaatimusten mukaisesta toiminnasta ovat teknologia-alan yrityksille elintärkeitä – näiden tulee näkyä vaikutusarvioinnissa nykyistä selkeämmin ja yksityiskohtaisemmin.

Säännöksessä tulee myös täsmentää, miten haittaa arvioidaan esimerkiksi viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan tuotantoympäristöissä. Haitan arvioinnissa tulee nimenomaisesti huomioida tieto-, viestintä- ja tuotantojärjestelmien suorituskykyvaikutukset (mahdolliset viiveet, datapakettihävikki ja muut palvelun laadun heikkenemiseen vaikuttavat tekijät) sekä palvelutasosopimusten rikkomisesta aiheutuvat seuraamukset, toiminnasta seuraava häiriönselvitystyö, palautustoimet, mainehaitta ja asiakasluottamuksen heikkeneminen.

Esityksen mukaan viranomaisen ulkopuolisella henkilöllä olisi suojelupoliisin pyynnöstä oikeus toteuttaa yksittäinen asennus- tai poistotoimenpide. Perusteluiden mukaan kyse ei olisi avustamisvelvollisuudesta, vaan pyynnön vastaanottajalla olisi oikeus kieltäytyä, ja "avustajalle olisi myös tuotava ilmi hänelle mahdollisesti aiheutuvat seuraamukset, kuten mahdollisuus työpaikan menettämiseen".

Teknologiateollisuus katsoo, että ehdotus ei ole sellaisenaan hyväksyttävä, sllä ehdotus asettaisi pyynnön kohteen kestämättömään asemaan: hänen olisi valittava työnantajansa työjärjestystä ja -sääntöjä, muita työvelvoitteita (ml. lojaliteettivelvoite) tai asiakasyrityksensä sopimusvaatimusten ja viranomaisen pyynnön välillä, jotka ovat oletusarvoisesti ristiriidassa pyynnön kanssa. Tilanteen kestämättömyyttä korostaa vielä entisestään se, että toimivaltainen viranomainen todennäköisesti edellyttäisi tällaista pyyntöä koskevaa ehdotonta salassapitoa eli luonnollinen henkilö ei voisi edes viedä asiaa työnantajansa tai toiminnanharjoittajan määräysvaltaa käyttävien käsiteltäväksi. Katsomme myös, että vaikka pelkästään pyynnön esittämistä ei pääsääntöisesti katsottaisi julkisen vallan käytöksi pyynnön sitovuuden ja yksipuolisen velvoittavuuden puuttumisen vuoksi, kyse olisi silti aina tosiasiallisen hallintotoiminnan piiriin kuuluvasta asiasta. Pyyntö voisi sen merkityksen (esim. kansallisen turvallisuuden suojaaminen), salassapitoedellytysten sekä kohtuuttoman suuren vastuuntunnon kohdistumisen kautta muodostua pyynnön kohteelle käytännössä pakottavaksi. Tällöin kyse olisi mitä ilmeisimmin merkittävästä julkisen vallan käytöstä.

Ehdotuksessa ei kiinnitetä riittävää huomiota pyynnön toteuttavan henkilön eikä hänen työnantajayrityksensä tai muun henkilöön olennaisesti liittyvän yhteisön oikeusturvaan (esim. muut osakkaat, toimeksiantaja tai päämies). Säännöstekstissä tai perusteluissa ei käsitellä lähimainkaan riittävästi niiden asemaa, vaikutuksia tai oikeusturvaa, joiden oikeuksiin tai etuihin toimenpide voi vaikuttaa. Pidämme selvänä, että ko. pyyntöä ei voida kohdistaa luonnolliseen henkilöön, mikäli pyynnön toteuttaminen voisi olla ristiriidassa henkilöä sitovien muiden velvoitteiden kanssa, vaan se tulisi kohdistaa sen sijaan hänen työnantajalleen.

Vahingonkorvausvastuu on käsitelty 16 §:ssä hyvin rajallisesti ja vain perusteluissa (s. 78). Huomiotta jää, että työntekijän suojelupoliisin pyynnöstä tekemä toimenpide voi yksinäänkin laukaista esimerkiksi sopimussakon tai vahinkorvausvelvoitteen työnantajayrityksen ja sen asiakkaan välisessä sopimussuhteessa, välillisistä vahingoista kuten mainevahingoista, tai luottamuspulasta yrityksen ja sen henkilöstön välillä puhumattakaan. Vahingonkorvausvastuusta tulee säätää tarkasti ja säännöstekstin tasolla.

18 § Peitetoiminnasta siviilitiedustelussa päättäminen

Teknologiateollisuus katsoo, että kirjallisen päätöksen laatiminen peitetoiminnan lopettamisesta pidetään edelleen voimassa. Peitetoiminta puuttuu kohteen perusoikeuksiin, ja sen perusteet sekä harkinnassa merkitykselliset seikat on dokumentoitava jälkikäteistä arviointia varten. Kun peitetoimintaa koskeva päätös on voimassa enintään kuusi kuukautta, on osapuolten oikeusturvan kannalta perusteltua, että ennenaikaisesta lopettamisesta tehdään kirjallinen päätös. Päätöksessä todetun voimassaoloajan päätyttyä erillistä lopettamispäätöstä ei luonnollisestikaan tarvita.

18 b § Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen

HE-luonnoksessa (s. 79–80) esitetään, että yksinomaan tietoverkossa toteutettavan peitetoiminnan päätöksenteko erotetaan omaksi 18 b §:ksi. Päätöksen tekisi suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt päällystöön kuuluva poliisimies, ja päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Kirjallisessa päätöksessä olisi mainittava muun muassa toimenpiteen esittäjä, peitetoiminnan toteuttava ja siitä vastaava poliisimies, 3 §:ssä tarkoitettu toiminta, tosiseikat joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat, tavoite ja toteuttamissuunnitelma, voimassaoloaika sekä mahdolliset rajoitukset ja ehdot.

Olennaisin ero perinteiseen peitetoimintaan on, että päätökseltä ei edellytettäisi kohdehenkilön tai -ryhmän yksilöintiä. Perusteluna esitetään, että verkossa toimijoita voi olla erittäin runsaasti, toiminta tapahtuu nimimerkkien turvin ja yksittäisten henkilöiden liityntä tiedonhankinnan kohteena olevaan toimintaan on usein epäselvä. Sen sijaan päätöksessä yksilöitäisiin 5 a luvun 3 §:n mukainen siviilitiedustelun kohteena oleva toiminta (esimerkiksi "ulkomainen tiedustelutoiminta"), kohdistamisen perustelut, tiedonhankinnan tavoite ja toteuttamissuunnitelma. Luonnoksessa kuitenkin todetaan nimenomaisesti, että "tiedustelutehtävässä olisi pystyttävä rajaamaan kohteena olevaa toimintaa mahdollisimman tarkasti eikä peitetoiminta tietoverkossa voisi olla täysin kohdentumatonta".

Teknologiateollisuus pitää ymmärrettävänä lähtökohtaa, jonka mukaan yksinomaan tietoverkossa toteutettavassa peitetoiminnassa kohdehenkilöiden tai -ryhmien yksilöinti ei ole samalla tavoin mahdollista kuin perinteisessä peitetoiminnassa. Verkkoympäristön luonteenpiirteet – nimimerkkien käyttö, toimijoiden suuri ja vaihtuva joukko sekä yksittäisten henkilöiden epäselvä liityntä kohdetoimintaan – tunnistetaan asianmukaisesti myös HE-luonnoksen perusteluissa. Tämä ei kuitenkaan oikeuta sitä, että päätökselle asetettava kohdentamisvelvoite mitoitettaisiin niin avoimeksi kuin esityksessä ehdotetaan. Pelkkä mainita kohteena olevasta toiminnasta – esimerkkinä luonnoksessa käytetään "ulkomaista tiedustelutoimintaa" – jättää käytännössä peitetoiminnan kohdentamisen lähes kokonaan suojelupoliisin sisäisen harkinnan varaan ja tekee jälkikäteisestä laillisuusvalvonnasta varsin teoreettista.

Esitetty kategoriatason kuvaus ei täytä niitä tarkkarajaisuuden, oikeasuhtaisuuden ja ennakoitavuuden vaatimuksia, joita perustuslakivaliokunta ja Euroopan ihmisoikeustuomioistuin ovat toistuvasti edellyttäneet salaisten viranomaistoimivaltuuksien sääntelyltä. Vaarana on, että 18 b §:n mukainen päätös muodostuu tosiasiassa pikemmin laajaksi toimintavaltuudeksi kuin täsmälliseksi tiedustelumenetelmän käyttöä koskevaksi päätökseksi. Tämä korostuu erityisesti siksi, että perustelujen mukaan muutos "mahdollistaisi suojelupoliisin peitetoiminnan kohdistamisen laajemmin kansallista turvallisuutta uhkaavaan toimintaan tai ilmiöön ilman ehdotonta henkilöyhteyttä" – muotoilu, joka itsessään viittaa varsin avoimeen kohdentamiseen.

Luonnoksessa itsessään todetaan, että peitetoiminta tietoverkossa ei voi olla täysin kohdentumatonta ja että kohteena olevaa toimintaa on pystyttävä rajaamaan mahdollisimman tarkasti. Tämä ohjelmallinen kannanotto on välttämätöntä konkretisoida säännöstekstin tasolla. Teknologiateollisuus esittää, että 18 b §:n päätökseltä edellytetään nykyistä täsmällisempää kohdentamista esimerkiksi vaatimalla, että päätöksessä yksilöidään tarkemmin kohdetoiminnan ilmenemismuoto, käytettävät verkkoympäristöt, alustat tai foorumit, kohdetoimintaan liitettävät tunnistettavissa olevat tunnusmerkit sekä ne kriteerit, joiden perusteella yksittäisten henkilöiden tai keskusteluiden katsotaan kuuluvan tiedustelun kohteena olevaan toimintaan. Lisäksi päätöksen perusteluissa tulisi edellyttää nimenomaista arviota siitä, miksi tarkempi kohdentaminen ei tapauksessa ole mahdollista.

Tämä on tärkeää myös teknologia-alan yritysten näkökulmasta. Yksinomaan tietoverkossa toteutettava peitetoiminta tapahtuu lähes poikkeuksetta yksityisten yritysten tai yhteisöjen ylläpitämillä viestintä- ja alustapalveluilla, sosiaalisen median palveluissa, keskustelufoorumeilla tai muissa digitaalisissa ympäristöissä. Avoimeksi jäävä kohdentaminen altistaa nämä palvelut ja niiden käyttäjäkunnan ennakoimattomalle viranomaistoiminnalle, mikä voi heikentää käyttäjien luottamusta kotimaisiin digitaalisiin palveluihin ja vaikuttaa kielteisesti suomalaisten teknologiayritysten kilpailukykyyn sekä kansainväliseen toimintaympäristöön. Päätöksen tarkempi kohdentaminen palvelee siten samanaikaisesti sekä yksilöiden perusoikeussuojaa että digitaalisen liiketoimintaympäristön ennakoitavuutta ja luotettavuutta.

39 § Tiedustelumenetelmän käytöstä päättäminen eräissä tilanteissa

Ehdotuksen säännösteksti ja perustelut ovat keskenään ristiriitaisia tai vähintään epäselviä siltä osin, kattaako suojelupoliisin päällikön päätös ulkomailla tapahtuvasta siviilitiedustelusta myös operaatiossa käytettävät tiedustelumenetelmät. Perusteluissa (s. 84) näin todetaan, mutta säännöstekstistä asia ei ole näin.

Teknologiateollisuus vaatii, että säännöstekstiin lisätään jatkovalmistelussa nimenomainen maininta siitä, että suojelupoliisin päällikön päätös kattaa myös operaatiossa käytettävät tiedustelumenetelmät. Tämä on välttämätöntä, koska se rajaa, mitä tiedustelumenetelmää päällystöön kuuluva poliisimies voi yksittäistapauksessa käyttää.

39 a § Tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi

39 b § Tietojärjestelmän käytön estämisestä tai sen toiminnan haittaamisesta vakavan vaaran torjumiseksi päättäminen

Ehdotus sisältää uuden toimivaltuuden tietojärjestelmien toimintaan puuttumiseen, mukaan lukien mahdollisuus estää tai haitata tietojärjestelmän käyttöä kansallisen turvallisuuden turvaamiseksi. Vastatoimien ja eskalaation riskit eivät kohdistu pelkästään valtioon, vaan välittömästi myös suomalaisiin yrityksiin – erityisesti niihin viestinnän välittäjiin ja tietoyhteiskunnan palvelun tarjoajiin, teknologiatoimijoihin ja kansainvälisesti operoiviin yhtiöihin, joiden verkkojen, palvelujen tai liiketoimintaympäristön kautta toimivaltuutta käytännössä toteutettaisiin. Tietojärjestelmät ovat usein monimutkaisia ja keskinäisriippuvaisia kokonaisuuksia, ja yksittäiseen järjestelmään kohdistuvat toimenpiteet voivat vaikuttaa laajasti muihin toimijoihin. Tämän vuoksi esityksen tulee sisältää kattava vaikutusarvio yritysten toimintaan. Lisäksi tulee arvioida huolellisesti vastuu- ja korvauskysymykset tilanteissa, joissa toimenpiteet aiheuttavat haittaa yrityksille. Katsomme, että jatkovalmistelussa säännellään ko. toimijoiden vastuuvapaudesta, oikeusturvasta, tiedonsaantioikeudesta ja vahingonkorvauksista.

Olemme jo sotilastiedustelulakia koskevassa käsittelyssä katsoneet, että näin merkittävän toimivaltuuden käyttöä koskeva päätöksenteko tulee olla poliittista ja poikkihallinnollista, ei yksittäisen viranomaisjohtajan (kuten suojelupoliisin päällikön) yksinään tekemä operatiivinen ratkaisu. Sama linja on perusteltua kirjata myös nyt käsillä olevaan sääntelyyn. Toimivaltuuden käyttöä koskeva päätös tulee tehdä aina poliittisella tasolla – esimerkiksi tasavallan presidentin tai soveltuvan ministeriryhmän toimesta. Vähintäänkin päätöksentekijälle on säännökseen kirjattava velvollisuus informoida turvallisuus- ja ulkopolitiikan johtoa, mieluiten jo ennen toimivaltuuden käyttöä. Tähän nähden säännösteksti ja perustelut jättävät liian avoimeksi sen, missä tilanteissa suojelupoliisin päällikkö voi päättää asiasta itsenäisesti ja milloin asia on vietävä poikkihallinnolliseen käsittelyyn tai TP-UTVA:an. Myöskään 5 a luvun 58 §:ssä kuvattu menettely ei kuvaa prosessia riittävällä tarkkuudella.

Lisäksi toimivaltuuden kansainvälisoikeudellinen perusta on esityksessä käsitelty mielestämme riittämättömästi: osana rikostorjuntaa toiminta voidaan kiinnittää selkeämmin rikoksen keskeyttämiseen viranomaistoimin, mutta siviilitiedustelussa vastaava oikeuttamisperuste on hyvin hankalasti ymmärrettävissä, mikä korostaa kansainvälisoikeudellisen arvion merkitystä.

On myös aiheellista kysyä, onko tosiasiallisesti perusteltua, että kaksi erillistä viranomaista – Puolustusvoimat ja suojelupoliisi – käyttävät samansisältöistä toimivaltuutta, kun toimivaltuuden käytöllä voi olla yhtä lailla mittavia seurauksia riippumatta siitä, kumpi viranomainen sitä kulloinkin käyttää. Teknologiateollisuus korostaa, että kyseessä ei ole pelkkä oikeudellinen tai operatiivinen

kysymys, vaan yhtä lailla talous- ja ulkopoliittinen ratkaisu, jonka vaikutukset Suomen kansainväliseen asemaan, suomalaisten yritysten toimintaedellytyksiin ja maamme houkuttelevuuteen investointikohteena tulee arvioida huolellisesti jatkovalmistelussa.

51 §. Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan velvollisuus avustaa siviilitiedustelussa

52 § Korvaus viestinnän välittäjälle ja tietoyhteiskunnan palvelun tarjoajalle siviilitiedustelussa avustamisesta ja tietojen antamisesta

Säännöstä tulee täsmentää. Ehdotettu säännös on yritysten näkökulmasta laaja ja voi käytännössä tarkoittaa tieto- ja viestintäpaveluiden kriittisiin osiin kohdistuvia teknisiä toimenpiteitä. Säännöksen soveltaminen voi edellyttää muutoksia tuotanto- ja valvontajärjestelmiin, toimitilojen turvallisuusjärjestelyihin tai henkilöstön asiantuntijaresursointiin. On ilmeinen riski, että sääntely altistaisi yritykset ennakoimattomille kustannuksille, operatiivisille ja kyberturvallisuusriskeille sekä kilpailu- ja mainehaitoille – erityisesti kansainvälisillä markkinoilla, joilla asiakkaiden luottamus tietoturvan ja salauksen koskemattomuuteen on liiketoiminnan elinehto. Tämän vuoksi avustamisvelvollisuuden laajuus, korvausjärjestelmän kattavuus ja salauksen koskemattomuus tulee säätää säännöstekstissä huomattavasti nykyistä täsmällisemmin ja yhdenmukaisemmin.

Teknologiateollisuus katsoo, että kun viestinnän välittäjien ja tietoyhteiskunnan palveluiden tarjoajien avustamisvelvollisuutta laajennetaan ja koska viestinnän välittäjien käsite on määritelty hyvin laajaksi, tulee samanaikaisesti asiaa koskeva kustannusten korvaus säännellä kattavasti. Olemme johdonmukaisesti pitäneet kantanamme, että viranomaisavustamisesta yrityksille aiheutuvat välittömät kustannukset – mukaan lukien henkilötyökustannukset – on korvattava täysimääräisesti, ja että korvausjärjestelmien tulee olla yhdenmukaisia eri toimijoille toimialasta ja yrityksen koosta riippumatta. Tämä on välttämätöntä yritysten yhdenvertaisen kohtelun ja kilpailuneutraliteetin turvaamiseksi. Asia on todettu myös ehdotuksessa.

Lisäksi on ehdottoman tärkeää, ettei ko. avustamisvelvoite missään tilanteessa johda pakolliseen ja systemaattiseen päästä-päähän-salauksen (E2EE) heikentämiseen, sillä vahva salaus on koko yhteiskunnan ja kriittisen infrastruktuurin tietoturvan kulmakivi sekä keskeinen edellytys suomalaisten teknologiayritysten kansainväliselle kilpailukyvylle ja luottamuspohjalle.

Ehdotetun säännöksen olennainen ongelma on, että vaikka viestinnän välittäjille ja tietoyhteiskunnan palvelun tarjoajille luvataan korvata välittömät kustannukset, viittauksen kohteena oleva sähköisen viestinnän palveluista annetun lain (SVPL) 299 § ei kata avustamiseen liittyvän henkilöstön palkkakustannuksia. Avustustehtävien määrä on noussut koko kuluvan vuosituhannen aikana, ja elinkeinoelämän järjestöt ovat laajasti edellyttäneet muutosta useissa eri yhteyksissä. Myös Eduskunnan liikenne- ja viestintävaliokunta (LiVL 1/2022) on edellyttänyt, että

kansallista kustannusten korvaamista koskevaa lainsäädäntöä päivitetään siten, että kaikki viranomaistyöstä aiheutuvat kustannukset myös henkilötyön osalta korvataan täysimääräisesti. Yhä laajenevista avustamisevelvollisuuksista ei seuraa yrityksille liiketoiminnallista etua. Yritysten tehtävänä ei ole toimia viranomaistoiminnan jatkajana omalla kustannuksellaan, eikä monimuotoisia avustamisvelvollisuuksia siten voida katsoa ”toiminnan luonteeseen” kuuluviksi asioksi.

Teknologiateollisuus edellyttää, että joko SVPL 299 §:ää muutetaan tai muutoin säännellään henkilöstökustannusten korvaamisesta käsittelyssä olevan lakiehdotuksen mukaisista avustamistehtävistä.

Laki tietoliikennetiedustelusta siviilitiedustelussa annetun lain muuttamisesta

5 § Tietoliikennetiedustelun kohdistaminen

Luonnoksessa esitetään luovuttavaksi nykyisen 2 momentin viestin sisältöä kuvaavien hakuehtojen rajauksista. Perusteluna on, että sisällöllisen hakuehdon käytön kielto "haittaa merkittävästi tietoliikennetiedustelun tehokkuutta" (s. 93).

Teknologiateollisuus huomauttaa, että 2 momentin rajaukset on alun perin säädetty nimenomaan rajaamaan sellaisten hakuehtojen käyttöä, jotka puuttuisivat tarpeettoman paljon viestinnän osapuolten yksityisyydensuojaan. Esitettyä perustelua niistä luopumiseksi on tällä tavoin vaikea pitää uskottavana. Jatkovalmistelussa perusteluja on selkeytettävä ja avattava nykyistä paremmin sitä, miksi tiedusteluviranomaisten haltuun päätyy rajoitteista huolimatta sivullista, luottamuksellisen viestin suojaa nauttivaa viestintää.

Koska 7 §:n mukaisen vaatimuksen ja päätöksen sisältöä ei ehdoteta muutettavaksi, esitämme harkittavaksi, tulisiko 7 §:ään ja/tai sen perusteluihin kirjata tarkemmin, millaisia kriteerejä hakuehtojen on täytettävä – ja erityisesti, millaisia ne eivät saa olla. Tiedustelun tulee jatkossakin loukata yksityisyydensuojaa, erityisesti sivullisten suojaa, mahdollisimman vähän.

20 § Tietoliikennetiedustelun käytöstä ilmoittaminen

Ehdotuksen mukaan ilmoitusvelvollisuus rajoittuisi vain 2 momentissa kuvattuihin tilanteisiin, joissa kyse on todistamiskieltojen alaisista tiedoista.

Teknologiateollisuus pitää ilmoitusvelvollisuuden rajaamisen perusteita jokseenkin ymmärrettävinä mutta riittämättöminä. Suomessa laillisesti oleskelevalla henkilöllä tai laillisesti toimivalla yrityksellä on lähtökohtainen oikeus tietää joutumisestaan viranomaisen toimenpiteen kohteeksi – tämä on oikeusturvan kulmakivi. Kolmansien osapuolten valvonta ei yksinään riitä oikeusturvan takaajaksi. Viranomaisen ei tarvitse tosiasiassa käsitellä tietoja, jotta kyse olisi yksityiselämään puuttumisesta: jo tietojen kerääminen ja tallentaminen myöhempää käyttöä varten on puuttumista (EIT: Marper v. Yhdistynyt kuningaskunta).

EIT on toistuvasti korostanut, että salaiset viranomaistoimenpiteet mahdollistavan kansallisen sääntelyn on oltava oikeusvaltioperiaatteiden mukainen, kansalaisten saatavilla ja laadultaan sellainen, että soveltamisen seuraukset ovat ennakoitavissa. Luottamuksen säilyttämiseksi oikeusvaltioperiaatteen noudattamiseen – ja erityisesti Suomeen tietoyhteiskuntana – tulee huolehtia siitä, että tietoliikennetiedustelun kohteeksi joutunut Suomessa laillisesti oleskeleva henkilö, yritys tai yhteisö saa tiedon toimenpiteestä sen tarkoituksen lakattua. On mahdollista harkita, että lmoitusta ei kuitenkaan tarvitsisi tehdä, mikäli se vaarantaisi toimenpiteen tarkoituksen tai aiheuttaisi ennakoitavissa olevaa merkittävää haittaa valtion yleiselle edulle. Tällöinkin tuomioistuimen tulee päättää ilmoituksesta luopumisesta.

Peter Sund, toimitusjohtaja, Kyberala ry, peter.sund@teknologiateollisuus.fi, 050-5650621

Koskela Akseli
Teknologiateollisuus ry - Kyberala ry