



17.4.2018

Eduskunnan liikenne- ja viestintävaliokunnalle

Vastine asiantuntijalausuntoihin

Hallituksen esitys siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/2017 vp)

Eduskunnan liikenne- ja viestintävaliokunta on pyytänyt sisäministeriöltä kirjallista vastinetta hallituksen esityksestä siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/2017 vp) annettuihin asiantuntijalausuntoihin.

Sisäministeriö vastaa valiokunnalle toimitetuissa lausunnoissa esitettyihin asioihin siltä osin kuin ne kuuluvat sisäministeriössä valmisteltuun hallituksen esitykseen ja liikenne- ja viestintävaliokunnan toimialaan. Tarvittaessa sisäministeriö toimittaa myös muista asioista vastineen valiokunnalle.

Pääsääntöisesti lakiesityksistä annettu palaute on ollut positiivista ja lausunnonantajat ovat pitäneet ehdotuksia hyvinä ja kannatettavina. Sisäministeriön näkemys on, että lausunnot eivät yleisesti ottaen anna suurta aihetta ehdotettujen pykälien muuttamiseen.

Vastineen täydentämistarvetta saattaa aiheuttaa perustuslakivaliokunnan aikanaan antama lausunto. Osittain perustuslakivaliokunnan mahdollisiin tuleviin kannanottoihin liittyvistä syistä tässä vastineessa ei ole vielä otettu lopullista kantaa kysymyksiin, jotka koskevat luottamuksellisen viestin suojan puuttuvia tiedustelumenetelmiä.

Pydyttynä vastineena asiantuntijalausunnoista sisäministeriö esittää lausuntokohtaisesti, siltä osin kuin lausunto on edellyttänyt vastaamista, seuraavaa:

Liikenne- ja viestintäministeriö katsoo lausunnossaan, että: "Tiedusteluviranomaisille on esityksessä ehdotettu uutta tietoliikennetiedustelua koskevaa toimivaltuutta. Tietoliikennetiedustelusta on tekniseltä toteuttamistavaltaan sen kaltaista, että sen puitteissa tiedusteluviranomainen voisi saada teknisen mahdollisuuden seuloa myös hyvin monen suomalaisen luottamuksellista viestintää. Tämän vuoksi on erityisen tärkeää huolehtia riittävästä perusoikeuksien suojasta. Perusoikeussuojan toteutumisen kannalta laissa on keskeistä säätää riittävästä vaatimuksista tiedustelun kohdentamiselle sekä tiedustelumenetelmällä kerätyn luottamuksellisen viestin salaisuuden suojan alaisen tiedon käsittelylle. Lisäksi on huolehdittava siitä, että tiedustelu voidaan tosiasiaa teknisesti toteuttaa laissa säädettyjen perusoikeuksia suojaavien vaatimusten mukaisesti."

Sisäministeriön vastaus: Sisäministeriö yhtyy liikenne- ja viestintäministeriön näkemykseen perusoikeuksien suojan riittävästä turvaamisesta. Sisäministeriö katsoo, että perusoikeussuojan toteutumisen kannalta lakiehdotuksissa esitetään säädettäväksi riittävästä vaatimuksista tiedustelun kohdentamiselle. Siltä osin kuin puhutaan henkilötietojen käsittelystä, niin poliisin henkilötietojen käsittelyä koskevan lainsäädännön kokonaisuudistus on käynnissä. Esityksellä uudistetaan voimassa oleva henkilötietojen käsittelystä poliisitoimessa annettu laki poliisitoiminnan tarpeet huomioon ottaen. Säännöksissä huomioidaan Euroopan unionin tietosuojalainsäädännön vaatimukset. Kyseisen hankkeen on tarkoitus edetä eduskuntaan kuluvaan vuoden aikana.

Puolustusministeriö kiinnittää yksityiskohtana huomiota siihen, että käsiteltävänä olevan hallituksen esityksen 2. lakiehdotuksen 10 §:ssä sotilastiedustelusta annettuun lakiin viitataan sotilastiedustelulakina.

Sisäministeriön vastaus: Sisäasiainministeriö pitää puolustusministeriön muutosehdotusta kannatettavana.

Tietosuoja-valtuutetun toimisto toteaa, että nyt käsiteltävänä oleviin hallituksen esityksiin ei sisälly ehdotuksia valmisteilla oleviksi laeiksi henkilötietojen käsittelystä poliisitoimessa. Taustalla on puolestaan mm. Euroopan unionin tietosuojadirektiivistä (2016/680) aiheutuva implementointitarve. Näin ollen pelkästään nyt käsiteltävänä olevien hallitusten esitysten pohjalta ei ole mahdollista saada kokonaiskuvaa ko. viranomaisten henkilötietojen käsittelystä. Myös **Electronic Frontier Finland – EFF** ry on kiinnittänyt huomiota tietojen käsittelyyn kansainvälisessä yhteistyössä.

Sisäministeriön vastaus: Siviilitiedustelulainsäädännön yhteydessä ehdotetaan henkilötietojen käsittelystä poliisitoimessa annettua lakia muutettavaksi ainoastaan välttämättömiltä osilta. Poliisin henkilötietojen käsittelyä koskevan lainsäädännön kokonaisuudistus on käynnissä. Esityksellä uudistetaan voimassa oleva henkilötietojen käsittelystä poliisitoimessa annettu laki poliisitoiminnan tarpeet huomioon ottaen. Säännöksissä huomioidaan Euroopan unionin tietosuojalainsäädännön vaatimukset. Kyseisen hankkeen on tarkoitus edetä eduskuntaan kuluvaan vuoden aikana. Henkilötietojen käsittelystä säädetään siis tässä yhteydessä, kun siviilitiedustelulainsäädännön kohdalla kyse on pääsääntöisesti muiden tietojen käsittelystä.

Viestintävirasto katsoo viraston tehtävien hoitamisen kannalta olevan välttämätöntä, että suojelupoliisilla on salassapitosäännösten estämättä mahdollisuus luovuttaa tietoliikennetiedustelun avulla hankittu tieto haitallisesta tietokoneohjelmasta tai käskystä toimivaltaiselle viranomaiselle, kun tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi.

Sisäministeriön vastaus: Sisäasiainministeriö yhtyy Viestintäviraston näkemykseen. Tietoliikennetiedustelusta siviilitiedustelussa ehdotetun lain 16 §:ssa esitetään säädettäväksi haitallista tietokoneohjelmaa tai -käskyä koskevien tietojen luovuttamisesta viranomaiselle, yritykselle tai yhteisölle. Pykälän 1 momentin mukaan: "Suojelupoliisi saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankitun tiedon haitallisesta tietokoneohjelmasta tai käskystä viranomaiselle, yritykselle tai yhteisölle, jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi." Sisäministeriön näkemyksen mukaan kyseinen säännös turvaa Viestintäviraston tehtävien hoitamisen mainituilta osin.

Poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 55 §:ssä ehdotetaan säädettäväksi yhteistyöstä muiden viranomaisten ja yhteisöjen kanssa. Pykälän 2 momentin mukaan: "Suojelupoliisi voi siviilitiedustelutehtävänsä toteuttamiseksi toimia yhteistyössä yhteisöjen kanssa sekä luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä tietoja, jos tietojen luovuttaminen on välttämätöntä kansallisen turvallisuuden suojaamiseksi." Tietojen luovuttamisen kynnys on kyseisessä säännösehdoituksessa korkeampi kuin ensiksi mainitussa. Voidaan perustellusti kysyä onko "välttämättömyys" liian korkea kynnys tässä yhteydessä ja onko se yhdenmukainen tietoliikennetiedustelulakiehdotuksessa valitun kynnyksen "on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi" kanssa. Yleisemmässä luovuttamisesta koskevassa säännöksessä (PolL 5a:55.2) oleva kynnys "välttämätöntä" voi olla omiaan vaikeuttamaan ja supistamaan tiedusteluviranomaisen raportointitoimintaa ja yleisemminkin tiedon jakamista, koska yksittäisessä tiedonluovutustapauksessa tulisi pystyä erikseen osoittamaan, että tiedusteluraportin luovuttaminen on välttämätöntä kansallisen turvallisuuden suojaamiseksi. Koska siviilitiedustelulainsäädännön tarkoituksena on lisätä tiedusteluviranomaisen raportointia ja yhteydenpitoa muihin viranomaisiin sekä sitä kautta analysoidulla tiedustelutiedolla parantamaan kansallista turvallisuutta, niin sisäministeriö katsoo, että poliisilakiehdotuksen 5 a luvun 55 §:n 2 momentissa oleva kynnys muutettaisiin vastaamaan tietoliikennetiedustelulaissa käytettyä "jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi".

FiCom, DNA, EK, Elisa Oyj, Telia Oyj ovat kiinnittäneet huomiota teleyrityksille maksettavien kulujen korvaamiseen. Ehdotetuista säännöksistä aiheutuisi teleyrityksille ja tiedonsiirtäjille kustannuksia,

joiden määrä riippuisi poliisilain ehdotetun 5 a luvussa tarkoitettujen menetelmien sekä siviili- ja sotilastiedustelulaeissa tarkoitetun tiedustelun ja tiedonsiirtäjiltä vaadittavien toimenpiteiden kokonaismäärästä. Toimenpiteiden lukumäärä ei ole teleyritysten eikä tiedonsiirtäjien ennakoitavissa eikä myöskään kontrolloitavissa. Esityksen perusteella ei pysty ennakoimaan, tiedustelutoimenpiteistä teleyrityksille tai tiedonsiirtäjille aiheutuvia kustannuksia.

Sisäministeriön vastaus: Poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 52 §:ssä esitetään säädettäväksi korvauksesta teleyritykselle siviilitiedustelussa avustamisesta ja tietojen antamisesta. Korvauskäytäntö vastaisi sitä, mitä nykyisin poliisilain 5 luvussa 62 §:ssa ja pakkokeinolain 10 luvun 64 §:ssä osalta säädetään. Molempien lainkohtien mukaan teleyrityksellä on oikeus saada valtion varoista korvaus salaisten tiedonhankintakeinojen tai salaisten pakkokeinojen yhteydessä tapahtuvasta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista siten kuin tietoyhteiskuntakaaren [sähköisen viestinnän palveluista annetun lain] 299 §:ssä säädetään. Korvauskäytännöstä toisin sanoen säädetään sähköisen viestinnän palveluista annetun lain 299 §:ssä.

Korvauskäytännön muuttaminen kattamaan tältä osin kaikki kustannukset saattaisi aiheuttaa merkittäviä kustannusvaikutuksia erityisesti poliisille sekä myös muille esitutkintaviranomaisille, jotka käyttävät salaisia tiedonhankintakeinoja ja salaisia pakkokeinoja.

Siviilitiedustelua koskevan lainsäädäntökokonaisuuden yhteydessä puhtaasti yritystoiminnalle aiheutuvien euromääraisten arvioiden osalta on syytä olla varovainen, koska niiden etukäteinen laatiminen voi johtaa helposti harhaanjohtavaan lopputulokseen. Esimerkiksi teletiedustelumenetelmien (telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen) lukumäärät on ainoastaan hyvin yleispiirteisesti arvioitavissa ja ennakoitavissa.

Yleisellä tasolla voidaan kuitenkin arvioida, että lainsäädäntömuutoksen myötä teleyritysten työmäärä saattaisi lisääntyä, mutta työmäärän kasvua on omiaan hillitsemään tiedustelumenetelmiä koskevien lupa-aikojen pidentyminen. Tämä vähentäisi pidempikestoisessa tiedusteluoperaatiossa teleyrityksille aiheutuvaa henkilöresurssikuormitusta suhteessa siihen, kuin että luvat olisivat ajalliselta kestoaltaan yhden kuukauden mittaisia. Siviilitiedustelulainsäädäntöä koskevan esityksen taloudellisten vaikutusten arviointiin on sisällytetty euromääräisesti sanallinen kuvaus sekä yhteenvetotaulukot taloudellisista vaikutuksista koskien suojelupoliisia. Kyseisiin kuluihin on myös sisällytettynä arvio yrityksille maksettavista korvauksista, joiden täsmällinen jaottelu ei tiedustelumenetelmiä koskevien lupamääräarvioiden takia ole julkista tietoa.

Sisäministeriön arvion mukaan teleyritysten vastuulle jäävät kustannukset olisivat marginaalisia. Tämä johtuu edellä kerrotun lisäksi siitä, että suojelupoliisin rooli muuttuu tiedustelullisempaan suuntaan eikä rikostorjuntatoimivaltuuksilla tulisi olemaan niin merkittävää roolia kuin aiemmin.

Kyse on kokonaan uudesta ja sellaisesta lainsäädäntökokonaisuudesta, että vaikutusten arvioinnissa korostuu etukäteisarvioinnin lisäksi erityisesti jälkikäteisarviointi. Siksi on perusteltua esittää eduskunnalle harkittavaksi, että se asettaa lainsäädännön täytäntöönpanon ja toteutumisen seurantavelvoitteen. Seurantajakson olisi tarkoituksenmukaista olla riittävän pitkä, jotta jälkikäteiseen arviointiin olisi saatavilla tarvittava määrä materiaalia. Seurannan mittareita asetettaessa olisi kuitenkin tärkeää, että ne muodostaisivat sellaisen kokonaisuuden, josta voidaan saada mahdollisimman laajaa ja objektiivista tietoa tarvittavien johtopäätösten tekemiseksi. Tiedustelutoimintaan liittyvät ulkopoliittiset ja muut sensitiivisyydet asettavat tiettyjä rajoitteita seurannan mittarien asettamisessa.

FiCom, Ficix, CSC, Elisa Oyj, DNA Oyj ovat kiinnittäneet huomiota poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 16 §:ään, jossa ehdotetaan säädettäväksi laitteen, menetelmän tai ohjelmiston asentamisesta ja poisottamisesta siviilitiedustelussa. Lausunnonantajat katsovat, ettei tiedusteluviranomaisella tulisi olla pääsyä teleyritysten tai tietoyhteiskunnan palvelujen tarjoajien laitetiloihin.

Sisäministeriön vastaus: Sisäministeriö toteaa, että lausunnonantajien huomiot ovat perusteltuja, vaikka tilanteet olisivatkin erittäin harvinaisia Suomessa.

Todettakoon, että hyvin vastaavantyyppinen säännös on voimassa olevan poliisilain 5 luvun 26 §:ssa, joka koskee teknisen tarkkailun menetelmiä. Ehdotettavan 5 a luvun 16 §:n asentamistoimivaltuutta esitetään poliisilain 5 luvun 26 §:stä poiketen laajennettavaksi myös telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta sekä televalvontaan. Tässä suhteessa on syytä huomioida, että

telekuuntelun, tietojen hankkimisen telekuuntelun sijasta sekä televalvonnan kohdalla asentamistoimivaltuuden käyttäminen tulisi lähtökohtaisesti sovellettavaksi ulkomaan tiedustelussa. Tämä johtuu muun muassa siitä, että on hyvin epätodennäköistä, että ulkomainen teleyritys avustaisi suojelupoliisia tarvittavien kytkentöjen tekemisessä. Asioiminen kohdevaltiossa toimivan teleyrityksen kanssa myös aiheuttaisi merkittävän paljastumisriskin.

Sisämaassa käytettävien toimivaltuuksien käytössä toimittaisiin vastaavasti, kuten nykyisten poliisilain 5 luvussa tarkoitettujen telekuuntelun, tietojen hankkimisen telekuuntelun sijasta sekä televalvonnan kohdalla. Tiedusteluviranomainen hakisi luvan tuomioistuimelta mainittujen toimivaltuuksien käyttämiseksi. Jos tiedustelumenetelmän käytöstä päättäisi tuomioistuin, niin myös tiedustelumenetelmän käyttöä koskevassa luvassa tulisi erikseen sallia laitteen, menetelmän tai ohjelmiston asentaminen. Näin ollen asentamistoimivaltuutta sovellettaessa tuomioistuinmenettelyssä tulisi yksittäistapauksellisesti myös arvioitavaksi toimivaltuuden toteuttamisen tapa. Asiassa on syytä korostaa sitä, ettei esimerkiksi telekuuntelua tai televalvontaa saisi kiertää käyttämällä teknisen tarkkailun toimivaltuuksia, vaan suojelupoliisi saa käyttää toimivaltuuttaan vain säädettyyn tarkoitukseen (tarkoitussidonnaisuuden periaate).

Laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä tulisi aina pohtia sen mahdollisesti aiheuttamaa kiinnijäämisriskiä sekä myös asentamisen kohteelle aiheutuva mahdollista vahingon riskiä. Esimerkiksi salaa tietojärjestelmään asennettu teknisen laitetarkkailun ohjelmisto sisältää aina mahdollisen riskin tietojärjestelmän toiminnalle ja on omiaan heikentämään sen turvallisuutta. Suojelupoliisin toimenpiteillä ei saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä (vähimmän haitan periaate).

Poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 51 §:ssä ehdotetaan säädettäväksi teleyrityksen velvollisuus avustaa siviilitiedustelussa ja 55 §:ssä yhteistyöstä yhteisöjen kanssa. Jälkimmäisen pykälän 1 momentin mukaan suojelupoliisin on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi. Tämä voi tarkoittaa esimerkiksi suojelupoliisille ja teleyrityksille yhteisesti hyväksyttävien toimintatapojen ja -käytänteiden laatimista.

FICIX ry toteaa lausunnossa, että yhdysliikennepisteisiin kohdistettavilla tiedustelutoimenpiteillä ei saavuteta sille asetettuja tavoitteita.

Sisäministeriön vastaus: Sisäministeriö näkee FICIX ry:n lausuntoa vastaavasti, ettei yhdysliikennepisteisiin kohdistettavilla tiedustelutoimenpiteillä saavutettaisi tiedustelutoiminnan tavoitteita eikä yhdysliikennepisteitä nähdä merkittävänä siviilitiedustelun kannalta. Tämä ei kuitenkaan tarkoita sitä, etteivätkö yhdysliikennepisteet voisi olla tiedustelun kohteena, jos siviilitiedustelu olisi välttämätöntä kohdistaa yhdysliikennepisteeseen.

CSC esittää lausunnossaan, että yritysten henkilöstön oikeudellinen vastuu tulisi määritellä selkeästi silloin, kun yritys joutuisi avaamaan asiakkaiden luottamuksellista tietoliikennettä.

Sisäministeriön vastaus: Siviilitiedustelulainsäädäntö koskevassa hallituksen esityksessä ei esitetä säädettäväksi tai muutettavaksi sellaisia säännöksiä, joiden nojalla yritys voitaisiin velvoittaa avaamaan asiakkaansa luottamuksellista tietoliikennettä tiedusteluviranomaisen pyynnöstä.

EK, FiCom, DNA, Elisa Oyj, Telia Oyj. Lausunnonantajat kiinnittävät huomiota tietoliikennetiedustelulain 22 §:n yksityiskohtaisiin perusteluihin, jotka olisi tarpeellista oikaista vastaamaan sotilastiedustelulain perusteluja. Pykälän tarkoittaman tiedonantovelvollisuuden piiriin kuuluvat tiedot koskisivat ennen kaikkea sitä, mitkä asiakasorganisaatiot ovat varanneet tiedonsiirtäjältä siirtokapasiteettia käyttöönsä ja mitä tiedonsiirtäjän hallitsemia rajan ylittävän viestintäverkon osia tällaiset varaukset koskevat. Pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja myös muista mahdollisista seikoista, jotka vaikuttavat tietoliikenteen reitittymistodennäköisyyteen sen ylittäessä Suomen rajan tiedonsiirtäjän omistamassa tai sen hallinnassa olevassa viestintäverkon osassa. On syytä korostaa, että pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja vain siltä kapasiteettia varanneista asiakasorganisaatioista, ei sen sijaan viestintätapahtumien osapuolena

olevista kuluttaja-asiakkaistaan. Pykälä ei muutenkaan perustaisi suojelupoliisille oikeutta hankkia tai saada tietoja yksittäisistä viestintätapahtumista tai niiden osapuolina olevista henkilöistä.

Sisäministeriön vastaus: Sisäasiainministeriö pitää lausunnonantajien muutosehdotusta kannatettavana. Yhdenmukaistamisvaatimus koskee alla olevaa perustelukohtaa. Myös siviilitiedustelua koskevan tietoliikennetiedustelulakiehdotuksen 22 §:n kohdalla pykälän tarkoittamat tietoliikennetiedustelun kohdentamiseksi välttämättömät tiedot koskisivat verkon teknistä toteuttamistapaa ja topologiaa esimerkiksi tietyn maantieteellisen alueen osalta. Pykälän mukaan tiedonsiirtäjää ei voitaisi velvoittaa luovuttamaan asiakkaana olevaa yksittäiseen luonnolliseen tai oikeushenkilöön liittyviä tietoja.

Siviilitiedustelulainsäädäntö	Sotilastiedustelulaki
L tietoliikennetiedustelusta siviilitiedustelussa <i>22 §:n perustelut (HE 202/2017 vp, s. 261)</i> Pykälän tarkoittaman tiedonantovelvollisuuden piiriin kuuluvat tiedot koskisivat ennen kaikkea sitä, mitkä asiakasorganisaatiot ovat varanneet tiedonsiirtäjältä siirtokapasiteettia käyttöönsä ja mitä tiedonsiirtäjän hallitsemia rajan ylittävän viestintäverkon osia tällaiset varaukset koskevat. Pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja myös muista mahdollisista seikoista, jotka vaikuttavat tietoliikenteen reitittymistodennäköisyyteen sen ylittäessä Suomen rajan tiedonsiirtäjän omistamassa tai sen hallinnassa olevassa viestintäverkon osassa. On syytä korostaa, että pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja vain siltä kapasiteettia varanneista asiakasorganisaatioista, ei sen sijaan viestintätapahtumien osapuolena olevista kuluttaja-asiakkaistaan. Pykälä ei muutenkaan perustaisi suojelupoliisille oikeutta hankkia tai saada tietoja yksittäisistä viestintätapahtumista tai niiden osapuolina olevista henkilöistä.	<i>95 §:n perustelut (HE 203/2017 vp, s. 328)</i> Pykälän tarkoittamat tietoliikennetiedustelun kohdentamiseksi välttämättömät tiedot koskisivat verkon teknistä toteuttamistapaa ja topologiaa esimerkiksi tietyn maantieteellisen alueen osalta. Pykälän mukaan tiedonsiirtäjää ei voitaisi velvoittaa luovuttamaan asiakkaana olevaa yksittäiseen luonnolliseen tai oikeushenkilöön liittyviä tietoja.

Suomen Erillisverkot Oy toteaa, että kytkennän de-aktivoiminen tai purkaminen pitää vastaavalla tavalla perustua tuomioistuimen yksiselitteiseen päätökseen.

Sisäministeriön vastaus: Tietoliikennetiedustelulakiehdotuksen 7 §:n 2 momentin 6 kohdan mukaan tietoliikennetiedustelua koskevassa tuomioistuimelle osoitettavassa vaatimuksessa ja tuomioistuimen antamassa lupapäätöksessä on mainittava tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella. Näin ollen tuomioistuin käytännössä päättää myös kytkennän de-aktivoimisesta tai purkamisesta. On myös huomioitava, että poliisilain muuttamista koskevan lakiehdotuksen 5 a luvun 4 §:n 5 momentin mukaan tiedustelumenetelmän käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Kyseisellä säännöksellä korostetaan sitä, ettei tiedustelumenetelmiä voida missään tapauksessa käyttää kauempaa kuin on tarpeen, vaikka lupa olisikin vielä voimassa. Tämä ilmenee myös poliisioikeudellisista periaatteista, kuten vähimmän haitan periaatteesta, joiden merkitystä perustuslakivaliokunta on yleisesti painottanut salaisen tiedonhankinnan yhteydessä (PeVL 32/2013, s. 4 ja 33/2013, s. 4).

Electronic Frontier Finland – Effi ry katsoo, että tiedustelun kohteelle ilmoittamista koskevat säännösehdotukset ovat ristiriidassa Euroopan ihmisoikeustuomioistuimen (EIT) oikeuskäytännön

kanssa. Tiedustelun kohteella oltava tosiasiallinen mahdollisuus viedä asia oikeuden tutkittavaksi (HE 202/2017 vp, s. 258–259). Mahdollisuutta ei ole, jos tiedustelun kohteeksi joutumisesta ei ilmoiteta. Ei ole väliä aloitetaanko asiassa rikostutkintaa, kun yksityisyyteen puuttuminen on joka tapauksessa tapahtunut.

Sisäministeriön vastaus: Sisäministeriö toteaa, että salaisen tiedonhankinnan kohteelle ilmoittamista koskevaa sääntelyä muutettiin viimeksi esitutkinta-, pakkokeino- ja poliisilain kokonaisuudistuksen yhteydessä (PoL 5:58 ja PKL 10:60). Poliisilain 5 luvun 58 §:n 1 momentin (1. virkkeen) mukaan telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta, suunnitelmallisesta tarkkailusta, peitelystä tiedonhankinnasta, teknisestä tarkkailusta ja valvotusta läpilaskusta on viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu (pääsääntö). Pykälän 2 momentissa säädetään poikkeuksista ilmoitusvelvollisuuteen. Tuomioistuimien voi pidättämiseen oikeutetun poliisimiehen vaatimuksesta päättää, että 1 momentissa tarkoitettua ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoittamatta jättäminen tulisi kyseeseen ainoastaan kahdessa jälkimmäisessä tapauksessa. Kynnys kokonaan ilmoittamatta jättämiselle on puolestaan korkea, mitä kuvattaisiin ilmauksella ”välttämätöntä”. Lisäksi ilmoittamatta jättäminen tulee kyseeseen silloin, kun tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa.

Yhtä lailla kuin voimassa olevassa lainsäädännössä, niin ehdotettavan siviilitiedustelulainsäädännön mukaan tuomioistuimien voisi suojelupoliisin päälystössä kuuluvan poliisimiehen vaatimuksesta päättää, että tiedustelumenetelmästä tehtävää ilmoitusta tiedonhankinnan kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saataisiin tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Tietoliikennetiedustelun käytöstä ilmoittamista koskisi edellä kerrotusta poiketen hieman erilainen ilmoituskonstruktio, josta ehdotetaan säädettäväksi tietoliikennetiedustelulakiehdotuksen 20 §:ssä. Pykälän mukaan jos 6 §:ssä tarkoitettua käsittelyssä on manuaalisesti selvitetty Suomessa olevan henkilön luottamuksellisen viestin tai tallentaman tiedon sisältö, ilmoitetaan hänelle tietoliikennetiedustelusta noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan ole, jos tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

Edellä kerrotun perusteella velvollisuutta ilmoittaa tietoliikennetiedustelusta sen kohteelle ei olisi silloin, kun tietoliikennetiedustelusta on päätetty kiiretilanteessa ja tuomioistuimien katsoo, ettei edellytyksiä tietoliikennetiedustelulle ole ollut. Tuomioistuimen päätöksen perusteella tietoliikennetiedustelun käyttö lopetettava välittömästi sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot heti hävitettävä. Lisäksi, jos tietoliikennetiedustelulla saadut tiedot koskevat tietoja, jotka on hävitetty sen takia, että 1) viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui; 2) lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta 12 §:ssä tarkoitettulla tavalla; 3) tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi, niin tietoliikennetiedustelusta ei olisi velvollisuutta ilmoittaa tietoliikennetiedustelusta sen kohteelle.

Euroopan ihmisoikeustuomioistuimien on lukuisissa ratkaisuissaan ottanut kantaa kysymykseen siitä, tuleeko ja missä tilanteissa tiedonhankinnan kohdehenkilöllä olla oikeus saada viranomaiselta tieto häneen kohdistetusta tiedonhankintatoimenpiteestä, esimerkiksi tietoliikennetiedustelusta. EIT on ratkaisukäytännössään korostanut, että tiedonhankinnan kohdehenkilöllä on oltava käytössään tehokkaat oikeusturvakeinot mahdollisesti lainvastaista viranomaistiedonhankintaa vastaan. Valitus- tai kantelumahdollisuuden käytön edellytyksenä on ihmisoikeustuomioistuimien toteamalla tavalla yleensä se, että henkilö saa viranomaiselta tiedon häneen kohdistetusta salaisesta tiedonhankinnasta sen jälkeen kun salaisen tiedonhankintamenetelmän käyttö on päättynyt. EIT:n ratkaisukäytännön mukaan tästä ei kuitenkaan seuraa, että ilmoitus on tehtävä välittömästi tiedonhankinnan päätyttyä. Uhka, josta tiedonhankintamenetelmän avulla on hankittu tietoja, voi jatkua vuosia tai jopa vuosikymmeniä, jolloin ilmoituksen tekemistä on turvallisuusviranomaisten toiminnan suojaamiseksi välttämätöntä lykätä vastaavasti. Oikeussuojakeinon käytön mahdollistamiseksi ilmoitus olisi kuitenkin tehtävä sen jälkeen, kun ilmoittamatta jättämiselle ei enää ole yksilöllistä perustetta. Kuitenkin myös järjestelmä, joka ei edellytä kohdehenkilölle ilmoittamista, voi olla sopusoinnussa ihmisoikeussopimuksen kanssa. Tällöin oikeus kannella viranomaisen salaisesta tiedonhankinnasta

on tullut kansallisessa lainsäädännössä säätää sillä tavalla yleiseksi, että kuka hyvänsä saa kannella pelkästään sen perusteella, että epäilee viranomaisen saattaneen puuttua luottamuksellisen viestintänsä nauttimaan suojaan (EIT Kennedy v. Yhdistynyt Kuningaskunta).

Tiedustelutoimintaa varten ehdotetaan perustettavaksi oma laillisuusvalvontaa suorittava viranomainen, Tiedusteluvaltuutettu, joka olisi riippumaton ja sillä olisi laajat tiedonsaantioikeudet sekä viime kädessä mahdollisuus keskeyttää tiedustelumenetelmän käyttö. Useimmissa Euroopan maissa on parlamentaarisen valvontaelimen ohella erillinen tiedustelutoiminnan laillisuusvalvontaa harjoittava taho. Tiedusteluvaltuutettu toimisi tietosuojavaltuutetun toimiston yhteydessä ja olisi toiminnassaan itsenäinen ja riippumaton. Tiedusteluvaltuutetun tehtävänä olisi valvoa tiedustelumenetelmien käytön lainmukaisuutta sekä perus- ja ihmisoikeuksien toteutumista tiedustelutoiminnassa. Yksilöt voisivat tehdä tiedusteluvaltuutetulle kanteluita tiedustelutoiminnan laillisuuskysymyksistä. Lisäksi tiedustelutoiminnan kohteena ollut tai henkilö, joka epäilee, että häneen on kohdistettu tiedustelua, voisi pyytää valtuutettua tutkimaan häneen kohdistuneen toiminnan lainmukaisuuden. Valtuutettu voisi tehdä tarkastuksia tiedustelutoiminnan laillisuuden valvomiseksi, minkä lisäksi sille ehdotetaan oikeutta päästä valvonnan kannalta välttämättömiin tiloihin ja tietojärjestelmiin. Tiedusteluvaltuutettu voisi lisäksi määrätä tiedustelumenetelmän käytön keskeytettäväksi tai lopetettavaksi, jos hän katsoo valvottavan menetelleen lainvastaisesti tiedustelutoiminnassa.

Tiedusteluvaltuutettu harjoittaisi tiedustelutoiminnan kattavaa ja reaaliaikaista valvontaa.

Tiedustelutoiminnan valvonnasta annettavassa laissa säädettäisiin valtuutetun oikeudesta olla läsnä tiedustelumenetelmää koskevan lupa-asian tuomioistuinkäsittelyssä. Siviilitiedustelulainsäädännössä tiedusteluviranomaisille säädettäisiin puolestaan velvollisuus ilmoittaa valtuutetulle tiedustelumenetelmän käytön viranomais- ja tuomioistuinpäätöksistä.

Sisäministeriö katsoo mm. edellä kerrotuilla perusteilla, että siviilitiedustelua koskeva hallituksen esitys vastaa EIT:n ratkaisukäytäntöä.

Effi ry ehdottaa lainsäädäntöön ns. Whistleblower-suojaa. EU:n tietosuojasetuksen kansallista toimeenpanoa koskevassa TATTI-mietinnössä (Oikeusministeriön julkaisu 35/2017) on ehdotettu uuteen tietosuojalakiin 20 §:ää, jossa säädettäisiin väärinkäytöksen ilmiintymisen tahon henkilöllisyyden suojaamisesta. Vastaava sääntely tulisi omaksua tiedustelulainsäädäntöön.

Sisäministeriön vastaus: Tiedusteluvaltuutetulle tehtävä kanteluoikeus olisi yleinen eli kantelun voisi tehdä asianosainen tai kuka tahansa muu henkilö. Kantelun voisi tehdä myös oikeushenkilö. Kantelumenettely täydentäisi tiedusteluvaltuutetun oma-aloitteista toimintaa kattavan laillisuusvalvonnan takaamiseksi sekä turvaisi sen, että yksilöt pääsevät oikeuksiinsa ja että oikeusturvajärjestelmä toimii moitteettomasti. Käytännössä kantelun voisi tehdä myös anonymina ja tiedusteluvaltuutettu voisi kantelun perusteella ottaa asian oma-aloitteisesti tutkittavaksi.

Teknologian tutkimusliitto VTT Oy (VTT) toteaa lausunnossaan, että tiedusteluviranomaisen tiedustelutarkoituksessa hyväkseen käyttämä tietojärjestelmän haavoittuvuus voisi olla myös tieto, joka saattaisi olla merkityksellinen yritysten suojaamisen kannalta.

Sisäministeriön vastaus: Siviilitiedustelun ensisijainen tavoite on Suomen kansallisen turvallisuuden parantaminen. Siviilitiedusteluviranomaisena toimivan suojelupoliisin tehtävänä tulee olemaan Suomen kansallisen turvallisuuden suojaaminen. Näin ollen myös mahdollista tietojärjestelmän haavoittuvuutta koskevaa tietoa ja sen luovuttamista arvioidaan Suomen kansallisen turvallisuuden suojaamisen näkökulmasta.

Mahdollista tietojärjestelmän haavoittuvuutta koskevan tiedon luovuttaminen yritykselle on aina tapauskohtaista harkintaa. Tietoliikennelakiehdotuksen 16 §:n 1 momentin mukaan suojelupoliisi saisi salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankitun tiedon haitallisesta tietokoneohjelmasta tai käskystä viranomaiselle, yritykselle tai yhteisölle, jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi. Harkinnassa otetaan huomioon aina sekä Suomen kansallisen turvallisuuden suojaaminen että tiedon saajan edut. Voi olla, että kyseiset intressit ovat myös päällekkäisiä. Edellä tarkoitettujen tietojen luovuttamista koskevien kriteerien arvioinnissa sekä intressipunninnassa korostuu suojelupoliisin ammattitaito.

VTT kritisoi kaksikäyttötuotteiden kuulumista siviilitiedustelun kohteisiin, koska viime aikoina myös erilaiset tieto- ja kyberturvallisuusohjelmistot ja -työkalut on haluttu nähdä kaksikäyttötuotteina.

Joissakin maissa tulkinnat tai niiden epäselvyys ovat johtaneet tilanteisiin, joissa jopa salausten menetelmiin liittyvien teknisten ja matemaattisten menetelmien opettaminen vaihto-opiskelijoille voitaisiin nähdä kaksikäyttötuotteen luvattomana levittämisenä.

Sisäministeriön vastaus: Siviilitiedustelun kohteista ehdotetaan säädettäväksi poliisilain 5 a luvun 3 §:ssä. Ainoastaan siviilitiedustelun kohteista voitaisiin hankkia tietoa tiedustelumenetelmiä käyttäen. Siviilitiedustelun kohdeluettelo olisi tyhjentävä. Tietoliikennetiedustelusta siviilitiedustelussa ehdotettavan lain 3 §:ään ehdotetaan otettavaksi samansisältöinen säännös kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Mainitun pykälän 4 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä.

Kaksikäyttötuotteilla tarkoitetaan kaksikäyttötuotteiden vientivalvonnasta annetun lain 2 §:n mukaan tuotetta, teknologiaa, palvelua ja muuta hyödykettä, jota normaalin siviililuontoisen käyttönsä tai sovellutuksensa ohella voidaan käyttää joukkotuhousteiden tai niiden maaliin saattamiseen tarkoitettujen ohjusjärjestelmien kehittelyyn tai valmistukseen taikka jolla voidaan edistää yleistä sotilaallista toimintakykyä. Kaksikäyttötuotteiden vientivalvonnan tärkeimpänä tavoitteena on joukkotuhousteiden leviämisen estämiseen tähtäävä asesulkupolitiikka.

Kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö voisi ilmetä esimerkiksi kaksikäyttötuotteiden hankkimisena, kauttakuljetuksena tai välityksenä vastoin voimassa olevaa vientivalvontalainsäädäntöä taikka Euroopan unionin rajoittavia toimenpiteitä tai Yhdistyneiden kansakuntien asettamia pakotteita. Tietoa voitaisiin hankkia esimerkiksi ulkomaisen toimijan pyrkimyksistä, suunnitelmista tai valmisteluista hankkia vilpillisesti tai harhauttamalla suomalaiselta yritykseltä kaksikäyttötuotteita EU:n tai YK:n asettamien pakotteiden vastaisesti.

Huomioitavaa tiedustelumenetelmän käytössä on kuitenkin menetelmän käytön edellytykset, joista ehdotetaan säädettäväksi poliisilain 5 a luvun 4 §:ssä. Jokaisen tiedustelumenetelmän käytön yleisenä edellytyksenä siviilitiedustelussa on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta (1 momentti). Sen lisäksi, mitä tiedustelumenetelmien käytön erityisistä edellytyksistä jäljempänä säädetään, telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja paikkatiedustelua saadaan siviilitiedustelussa käyttää vain, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi 1 momentissa tarkoitettua toiminnasta. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että menetelmän käyttö on välttämätöntä. Peitetoiminnan käyttäminen edellyttää myös, että tiedonhankintaa on toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisenä (2 momentti).

Kuten muidenkin siviilitiedustelun kohteiden kohdalla, niin myös kaksikäyttötuotteiden suunnittelun, valmistamisen, levittämisen ja käytön tulee toimintana olla perustellusti ja oletettavasti sellaista, että kyseinen toiminta vakavasti uhkaa Suomen kansallista turvallisuutta.

VTT toteaa vertailumaiden lainsäädännöstä Norjan linjauksen kieltää tietoliikennetiedustelulla saatujen tiedon käytön oikeudessa kokonaan. Lisäksi VTT viittaa Ruotsin avoimuudesta onnistuneesta ennaltaehkäisystä voitaisiin ottaa mallia myös Suomessa

Sisäministeriön vastaus: Siviilitiedustelulainsäädäntöön ehdotetaan sisällytettäväksi ns. palomuuria koskeva säännös. Siviilitiedustelulainsäädäntöä valmistelleessa työryhmässä pidettiin suomalaisen rikosoikeusjärjestelmän näkökulmasta kestävämmänä sellaista ratkaisua, jossa suomalaisella viranomaisella olisi tietoa törkeästä rikoksesta eikä sillä olisi velvollisuutta luovuttaa sitä toimivaltaiselle viranomaiselle tai että sellaisen tiedon luovuttaminen olisi kielletty kokonaan.

Ruotsin turvallisuuspoliisi kertoi tammikuussa 2015 estäneensä edeltävän puolentoista vuoden aikana kaksi terrori-iskua signaalitiedustelupalvelulta saamiensa tietoliikennetiedustelutietojen avulla. Asiasta tiedottaminen on poikkeuksellista, sillä tiedustelusta säätäneet maat eivät salassapitosyistä yleensä käsittele julkisuudessa sitä, millä nimenomaisella tiedustelumenetelmällä jotkin tietyt uhkatiedot on hankittu.

VTT käsittelee lausunnossaan kysymystä massavalvonnasta. Ollakseen tehokas, lainsäädäntö edellyttää, että jokaiseen rajat ylittävään pisteeseen luodaan edellytykset tietoliikennetiedustelulle.

Sisäministeriön vastaus: Sisäministeriö katsoo, että tietoliikennetiedustelu ei muutu massavalvonaksi valmiuksia rakentamalla, vaan olennaista on toimivaltuuden käyttäminen tiedustelutoimintaan. Niiden kannalta asiaan vaikuttavia olennaisia tekijöitä ovat käyttötarve, tosiasialliset resurssitekniset edellytykset sekä viranomaisen toimivaltuudet. Suomen sääntelymalli eroaa verrokkivaltioista olennaisesti siinä, että Suomessa sisällölliset hakuehdot eivät ole mahdollisia. Tällöin tiedustelun tekninen toteuttaja ei voi irrottaa tietoliikennevirrasta satunnaista datamassaa sisältöhakuehtovertailuun, vaan irrotettava aineisto on ensin valikoitava teknisten hakuehtojen perusteella.

Effi ry ja **VTT** ovat lausunnoissaan esittäneet, että tiedustelutoiminnasta tulisi kertoa mahdollisimman avoimesti. Lausunnoissa on esitetty, että julkisissa esityksissä voitaisiin ilmoittaa määrällisiä tietoja muun muassa tietoliikennetiedustelun osalta, kuinka laajoihin henkilöryhmiin, kuinka isoon verkkoalueeseen ja data- ja viestimääriin myönnetyt tiedusteluluvat ja toisaalta toteutetut tiedustelutoimenpiteet ovat kohdistuneet. Lisäksi lausunnoissa esitetään, että julkisiin esityksiin voitaisiin lisätä tilastoja siitä, paljonko ja kuin monta eri henkilöä koskevia tietoja tiedusteluviranomaiset ovat saaneet muiden viranomaisten rekistereistä.

Sisäministeriön vastaus: Tiedustelutoiminnan yhteiskunnallisen hyväksyttävyyden näkökulmasta lausunnoissa esitettyä voidaan pitää lähtökohtaisesti kannatettavana ja mahdollisuuksien mukaan salassapitosäännökset huomioon ottaen toiminnasta voitaneen laatia myös julkisia lausunnossa tarkoitettuja tilastoja. Siviilitiedustelun tehtävänä on hankkia ennakoivaa ja merkityksellistä tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tiedonhankinnan tehokkuutta ei tällöin voida perustellusti arvioida määrällisten, vaan laadullisten kysymysten kautta. Määrällinen mittari voi olla jopa harhaanjohtava. Pelkästään tiedustelukysymykseen tietoa hankkiva toimeksianto voi olla vähempimerkityksellinen kuin tiedusteluoperaatio, jossa vain osa hankitusta tiedosta kuuluu tiedustelukysymykseen.

Kattavin kuva edellä tarkoitetuista tiedoista koko tiedustelutoiminnassa, siviili- ja sotilastiedustelussa, olisi tiedusteluvaltuutetulla. Julkaistavat tiedot ja tilastot tulee kuitenkin käydä tarkasti läpi tiedusteluviranomaisten ja tiedusteluvaltuutetun kanssa, jottei tiedustelun tarkoitus vaarannu. Päätös tietojen julkistamisesta tulisi olla aina viime kädessä tiedusteluviranomaisella.

Tuomas Ojasen näkemyksen mukaan olisi kuitenkin syytä säätää tietoliikenteen yleisen, kohdentamattoman ja kaiken kattavan seurannan kiellosta tiedustelutoiminnassa nimenomaisesti sotilastiedustelu- ja siviilitiedustelulaeissa siltä osin kuin niissä säädetään tiedonhankinnasta tietoliikenteestä. Tämä loisi osaltaan takeita niiden sääntelyn sopusoinnulle EU-oikeuden (samoin kuin Euroopan ihmisoikeussopimuksen) kanssa. (En ota tässä vaiheessa yksityiskohtaisemmin kantaa kieltoäännöksen muotoiluun, vaan tyydyn painottamaan tarvetta tällaiselle kieltoäännökselle Euroopan ihmisoikeussopimuksen ja EU-oikeuden kannalta.) **VTT, BaseN ja CSC** toteavat lausunnoissaan, että tiedusteluviranomaisille luotaisiin teknisten edellytykset valvoa kaikkea tietoliikennettä kaikissa tietoliikenteen solmukohdissa. Lisäksi lausunnoissa todetaan, että myös Suomen sisäinen liikenne saattaa joutua tietoliikennetiedustelun piiriin. **Google** ilmaisee huolen siitä, että lainkohdat sellaisena kuin ne nyt on ilmaistu, voitaisiin tulkita laajentavasti siten, että tulkinta mahdollistaisi tietojen massakeräämisen ja -tiedustelun.

Sisäministeriön vastaus: Suomen perustuslain 10 §:n muuttamista koskevassa hallituksen esityksen yksityiskohtaisissa perusteluissa todetaan, että: "[Perustuslain] Säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiinkin kuuluvasta välttämättömyysvaatimuksesta ja vaatimuksesta rajoituksen sopusoinnusta kansainvälisten ihmisoikeusvelvoitteiden kanssa samoin kuin EU-oikeudesta seuraa vaatimuksia muun muassa toimivaltuuksien yksilöimiselle. Ehdotettu sääntely ei siten mahdollistaisi yleisestä, kohdentamattomasta ja kaikenkattavasta tietoliikenteen seurannasta säätämistä." Sisäministeriö pitää tätä rajausta riittävänä eikä katso tarkoituksenmukaiseksi säätää nimenomaisesta tietoliikenteen yleisen, kohdentamattoman ja kaiken kattavan seurannan kiellosta tiedustelutoiminnassa laissa tietoliikennetiedustelusta siviilitiedustelussa.

Osana tietoliikennetiedustelun toteuttamista kartoitetaan se viestintäverkon osa eli ne yhteydet, joissa kulkee siviilitiedustelun kannalta merkityksellinen liikenne. Kyseiset yhteydet voivat vaihdella ja muutoksiin reagoidaan. Tiedustelutoiminnassa ei ole tarkoituksenmukaista eikä edes tarvetta rakentaa

jatkuvaa ja kaiken kattavaa seuranta kaikkii tietoliikenneyhteyksiin tai tietoliikenteen solmukohtiin. Suojelupoliisin sekä sotilastiedusteluviranomaisella on ennen teknisen kytkennän tekemistä viestintäverkon osaan pääsääntöisesti sellaista ennakkotietoa, jottei liityntäpisteiden rakentaminen ei tapahdu sattumanvaraisesti.

Tietoliikennetiedustelu ei olisi mahdollista, ellei tiedustelua voitaisi kohdistaa niihin tietoliikenneyhteyksiin, joissa kulkee tiedustelun kannalta merkittävää tietoliikennettä. Tämä ei kuitenkaan tarkoita sitä, että kyseisen tietoliikenneyhteyden kaikkea tietoliikennettä seurattaisiin. Jotta tietoliikennetiedustelua voitaisiin käyttää, tarvitaan aina tuomioistuimen lupa, jossa olisi ilmoitettava 1) tietoliikennetiedustelun kohteena oleva toiminta [siviilitiedustelun kohteet], 2) kyseistä toimintaa koskevat tosiseikat, 3) tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat¹, 4) tietoliikennetiedustelussa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille, 5) rajan ylittävän viestintäverkon osa, jossa liikkuvaan tietoliikenteeseen hakuehtoja käytetään, sekä perustelut viestintäverkon osan valinnalle, 6) tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella, 7) tietoliikennetiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystään kuuluva poliisimies, 8) mahdolliset tietoliikennetiedustelun rajoitukset ja ehdot².

Jos tuomioistuin myöntää luvan tiedusteluviranomaiselle, tietoliikennetiedustelun käytön aloittaminen edellyttää ulkopuolisen kytkennän suorittajan suorittamaa kytkentää tuomioistuimen myöntämän luvan tarkoittamaan viestintäverkon osaan. Myös tämä takaa sen, ettei tiedusteluviranomaisella ole suoraa pääsyä kaikkeen tietoliikenteeseen.

Tietoliikennetiedustelulaissa ehdotetaan säädettäväksi myös tiedustelukielloista (20 §). Tietoliikennetiedustelua ei saa kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat Suomessa, eikä tietoon, josta lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla. Tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä, jos käy ilmi, että se on kohdistunut tiedustelukiellon alaiseen tietoon. Käytännössä tämä tapahtuu pääosin tietoliikenteen käsittelyn automatisoidun käsittelyn vaiheessa. Jos tiedustelukiellon alaista tietoa päättyy manuaalisen käsittelyn vaiheeseen, sitoo hetihävittämisvelvollisuus edelleen tietoliikennettä käsittelevää virkamiestä.

Lopuksi on syytä todeta, että siviilitiedustelulainsäädäntö mahdollistaa tiedustelutoimivaltuuksien käytön defensiivisesti. Tämä tarkoittaa sitä, että tietoliikennetiedustelua ja muita tiedustelumenetelmiä tiedusteluviranomainen saa käyttää ainoastaan, jos pitää hankkia tietoa sellaisesta laissa tyhjentävästi säädetystä toiminnasta [siviilitiedustelun kohteet], joka muodostaa vakavan uhkan Suomen kansalliselle turvallisuudelle. Näin ollen tietoliikenneyhteyksien seuraaminen valvonnallisessa merkityksessä ei ole tiukkojen sekä täsmällisesti ja tarkkarajaisesti määriteltyjen oikeudellisten edellytysten perusteella mahdollista.

BaseN Oy kiinnittää lausunnossaan huomiota viestintäverkoissa liikkuvan tietoliikenteen määrään. Lisäksi lausunnossa kiinnitetään huomiota tietoliikenteen salaukseen.

Sisäministeriön vastaus: Kaapeleiden ja kuitujen osalta on huomioita se, että niistä mainitaan käytännössä aina niiden kokonaiskapasiteetti, mikä ei käytännössä koskaan ole käytössä. Lisäksi kaikkia Suomen rajan ylittävät kaapelit ja kuidut eivät ole käytössä kaiken aikaa. Tietoliikennetiedustelussa pystytään valitsemaan merkitykselliset viestintäverkkojen osat ja suodattamaan pois epäoleellista liikennettä.

Julkisista lähteistä saatujen tietojen mukaan noin puolet tietoliikenteestä on tällä hetkellä salattua. Tietoliikennetiedustelulla voidaan salauksesta huolimatta saada kansallisen turvallisuuden kannalta merkittävää tietoa esimerkiksi tunnistamistietojen perusteella. Tietoliikennetiedustelua käytettäisiin myös tietoverkkohyökkäysten havaitsemiseen, johon mahdollisella salaamisella ei ole vaikutusta. Tämän lisäksi myös salatusta tietoliikenteestä voidaan muodostaa olennaista tiedustelutietoa salausta

¹ 4 §. Tietoliikennetiedustelun käytön edellytykset.

Tietoliikennetiedustelun käytön yleisenä edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoa sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Jos tietoliikennetiedustelun hakuehtojen käyttö ei koske ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, on edellytyksenä lisäksi, että tietoliikennetiedustelun voidaan olettaa olevan välttämätöntä tiedon saamiseksi tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

² Tuomioistuin voi asettaa tietoliikennetiedustelun käytölle rajoituksia ja ehtoja. Myös tiedusteluviranomainen voi oma-aloitteisesti esittää hakemuksessa tietoliikennetiedustelun käytölle rajoituksia ja ehtoja.

purkamatta. Tietoliikennetiedustelujärjestelmän riittävä tehokkuus voidaan varmistaa vaatimatta yrityksiltä salausavaimia tai takaporttien asentamista.

Tietoliikennetiedustelun tehokkuus on kyseenalaistettu myös sen perusteella, että tietoliikennemäärät kasvavat tulevaisuudessa. Tietoliikennemäärien kasvun ei kuitenkaan voida katsoa vähentävän tietoliikennetiedustelun tarpeellisuutta, vaan pikemminkin lisäävän sitä. Tietoliikennemäärien kasvuun on voitava vastata toiminnan riittävällä resursoinnilla ja huolehtimalla siitä, että tiedusteluprosessi on riittävän valikoiva.

Google toteaa, että ehdotetussa säännöksessä asetetaan vuoden mittainen määräaika, jonka kuluessa tiedustelun tiedonkeräystapoja koskevat tiedot voidaan määrätä salassa pidettäväksi niin, ettei kolmas osapuoli saa niitä ilmaista tai paljastaa. Kieltoa voidaan kuitenkin uudistaa mahdollisesti loputtomiin, eikä kolmas osapuoli tällöin voi valittaa tästä (Poliisilaki, 5a-luku, 38 §). Tarkoituksena on ymmärrettävästi suojella yksittäistapauksissa tiedustelutiedon keräystä ja käytettyjä tiedustelutapoja. Läpinäkyvyyden varmistamiseksi tulisi lainsäädännössä kuitenkin yksilöidä, ettei ilmaisukielto saisi kerrallaan kestää yli vuoden mittaista aikaa, jonka jälkeen viranomaisilla olisi mahdollisuus hakea yhtä vuoden mittaista pidennystä.

Sisäministeriön vastaus: Poliisilain muuttamista koskevan poliisilakiehdotuksen 5 a luvun 38 §:ssä ehdotetaan säädettäväksi ilmaisukiellosta siviilitiedustelussa. Pykälän 1 momentin mukaan tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja tiedustelumenetelmän käytöstä siviilitiedustelussa, jos se on perusteltua tiedustelumenetelmän käytön suojaamiseksi. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytössä.

Tiedustelumenetelmän käytön perusteena on aina, että siviilitiedustelun kohteena oleva toiminta vakavasti uhkaa kansallista turvallisuutta. Tiedustelumenetelmää käytettäessä on mahdollista joutua tilanteeseen, joissa ulkopuolinen apu on tarpeen tai jopa välttämätöntä. Esimerkiksi paikkatiedustelussa voi olla tarpeen pyytää taloyhtiön huollosta vastaavan yhtiön palveluksia. Näin ollen sivulliset voivat saada tietoja, joiden ilmaiseminen voi vaarantaa ainakin tiedustelumenetelmän käytön, mutta samalla muodostaa uhkan kansalliselle turvallisuudelle. Tarkoitus olisi minimoida riski tiedustelumenetelmän käytön paljastumisesta sekä suojata samalla myös salassa pidettäviä taktisia ja teknisiä menetelmiä ja viime kädessä kansallista turvallisuutta.

Pykälän 1 momentin 2 virkkeen mukaan edellytyksenä olisi lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytössä. Ilmaisukieltoa ei siten voitaisi antaa kenelle tahansa henkilölle, esimerkiksi taloyhtiön asukkaalle tai muulle sivulliselle, joka sattumalta havaitsee teknisen tarkkailun laitteen asennuksen.

Säännöksessä tiedustelumenetelmän käytöllä tarkoitettaisiin tiedustelumenetelmien käyttöä laajemmin, joka pitäisi esimerkiksi sisällään siviilitiedustelussa sekä sotilastiedustelussa käytettävien tiedustelumenetelmien käytön suojaamisen silloin, kun suojelupoliisi ja sotilastiedusteluviranomainen toimisivat yhteistyössä. Ilmaisukielto olisi perusteltua antaa ainakin silloin, jos tiedustelumenetelmän käyttö saattaisi paljastua ilman kiellon määräämistä sivulliselle.

Ilmaisukiellon saanut saisi ilman määräaikaa kannella päätöksestä. Kantelu olisi käsiteltävä kiireellisenä. Ilmaisukieltoa koskevasta päätöksestä tulisi myös aina ilmoittaa tiedusteluvaltuutetulle, joka arvioisi ilmaisukiellon oikeudelliset edellytykset ja tarvittaessa puuttuisi tiedusteluviranomaisen menettelyyn.

EK ja Google kiinnittävät huomiota yrityssalaisuuden suojaan. EK pitää esitystä hyvänä, mutta muistuttaa, että yrityssalaisuuksia koskevasta tiedonluovutusrajoituksesta olisi perusteltua säätää perustelujen sijaan pykälätasolla. Google esittää huolensa siitä, ettei lakiehdotus aseta rajoituksia sille, minkälaista tietoa tiedusteluviranomainen saa ilmaista muille toimijoille. Ongelmallista on myös se, ettei ole olemassa ulkopuolista tahoa, joka valvoisi, minkälaista tietoa tiedusteluviranomainen ilmaisee muille yksittäisille toimijoille. Google katsoo, että kaikkeen lainsäädäntöön tulisi sisällyttää yleinen pääsääntö, jossa tällainen tietojen ilmaiseminen kielletään.

Sisäministeriön vastaus: Lausunnonantajien huomiot koskien yrityssalaisuuden suojaa ovat perusteltuja.

Suojelupoliisin oikeudesta luovuttaa tietoja ehdotetaan säädettäväksi muun muassa poliisilain muuttamista koskevan poliisilakiehdotuksen 5 a luvun 55 §:ssä (Yhteistyö muiden viranomaisten ja yhteisöjen kanssa) ja 57 §:ssä (Kansainvälinen yhteistyö) sekä tietoliikennetiedustelulakiehdotuksen 16 §:ssä (Haitallista tietokoneohjelmaa tai -käskyä koskevien tietojen luovuttaminen viranomaiselle, yritykselle tai yhteisölle). Muita paitsi kansainvälistä yhteistyötä koskevia säännösehdotuksia on käsitelty aiemmissa vastauksissa.

Kansainvälistä yhteistyötä koskevan 57 §:n 2 momentin mukaan suojelupoliisi voisi salassapitosäännösten estämättä luovuttaa tietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi eikä tietojen luovuttaminen ole vastoin kansallista etua. Tietojen luovuttaminen kansainvälisessä yhteistyössä tulisi ensinnäkin perustua suojelupoliisin tehtävään suojata kansallista turvallisuutta. Käytännössä kyse voisi olla tiedustelumenetelmien tekniikkaa ja taktiikkaa, haittaohjelmia koskevista tiedoista tai turvallisuusuhkia koskevista analyyseistä taikka muusta sellaisesta tiedosta, jonka luovuttaminen olisi Suomen intressien mukaista. Tiedon luovuttamisen tulee toisaalta aina olla kansallisen edun mukaista. Tällaisen edun piiriin kuuluvat esimerkiksi tiedot Suomen poliittisista tai taloudellisista suhteista toisen valtion kanssa, sotilastiedustelua tai sotilaallista maanpuolustusta koskevat tiedot taikka tiedot kansainvälisen tiedusteluyhteistyön turvaamiseksi. Tietojen luovuttamisen hyväksyttävyyttä tulisi näin ollen arvioida yhtäältä kansallisen turvallisuuden suojaamisintressin ja toisaalta kansallisten etujen turvaamisintressin kannalta. Tässä kokonaisarviointissa suojelupoliisin on otettava huomioon myös luovutettavan tiedon ominaisuudet sekä tiedon vastaanottajana oleva taho.

lainsäädäntöneuvos Marko Meriniemi