Eduskunnan liikenne- ja viestintävaliokunta

VNS 11/2011 vp

Valtioneuvoston selonteko tiedustelulainsäädännöstä

Tarkastelen siviili- ja sotilastiedusteluviranomaisten tehtävien ja toimivaltuuksien sääntelyn toimivuutta ja mahdollisia kehittämistarpeita seuraavassa kolmesta sellaisesta näkökulmasta, jotka kaikki liittyvät myös ja erityisesti sähköiseen viestintään. Käsittelen lisäksi lyhyesti siviili- ja sotilastiedustelutoiminnan valvontaa sekä siihen liittyvää oikeusturvan toteutumista siviili- ja sotilastiedustelun yhteydessä.

Siviili- ja sotilastiedustelutoiminnan laillisuusvalvojan rooliini ei kuulu arvioida siviili- ja sotilastiedustelulainsäädännön toimivuutta sen tehokkuuden ja tuloksellisuuden kannalta eli ottaa kantaa siihen, minkälaisia toimivaltuuksia siviili- ja sotilastiedusteluviranomaisilla tulisi niiden tehtävien tehokkaan ja tuloksellisen hoitamisen mahdollistamiseksi olla. Siviili- ja sotilastiedustelutoiminnan laillisuusvalvojan rooliini kuuluu sen sijaan arvioida siviili- ja sotilastiedustelulainsäädännön toimivuutta sääntelyn selkeyden näkökulmasta. Sääntelyn selkeys on tärkeää siviili- ja sotilastiedustelun kohdehenkilöiden ja siviili- ja sotilastiedustelua harjoittavien virkamiesten oikeusturvan sekä siviili- ja sotilastiedustelutoiminnan valvonnan kannalta. Sääntelyn selkeyteen vaikuttaa yksittäisten säännösten muotoilun lisäksi sääntelyn johdonmukaisuus eli yksittäisten säännösten asemoituminen osaksi laajempaa lainsäädäntökokonaisuutta ja koko oikeusjärjestystä. Sääntelyn johdonmukaisuuden kannalta voi haasteita liittyä tarkoituksiltaan ja tavoitteiltaan osin erilaisten siviili- ja sotilastiedusteluviranomaisten toimivaltuuksia koskevan sääntelyn sekä sähköisen viestinnän palveluja koskevan sääntelyn yhteensovittamiseen.

Yleisarvioni on, että sekä siviili- ja sotilastiedustelulainsäädäntö että siviili- ja sotilastiedustelutoiminnan valvontajärjestelmä vaikuttavat siviili- ja sotilastiedustelulainsäädännön soveltamisen alkuvaiheen kokemusten perusteella toimivilta.

Digitaalinen toimintaympäristö

Viranomaisten tiedonhankintatoimivaltuuksien ja tiedonsaantioikeuksien sääntely nopeasti kehittyvässä digitaalisessa toimintaympäristössä on vaativa tehtävä. Sääntelyn ja tekniikan eritahtinen kehitys voi vaikuttaa kahteen suuntaan: viranomaisille säädetyt toimivaltuudet ja oikeudet voivat muuttua teknisen kehityksen myötä tehottomiksi taikka viranomaisten toimivaltuuksien ja oikeuksien tosiasiallinen sisältö voi muuttua sellaiseksi, jota lainsäätäjä ei ole alun perin tarkoittanut tai jota se ei ole ainakaan osannut ennakoida. Sekä viranomaistoiminnan tehokkuuden että sähköiseen viestintään liittyvien yritysten yhdenvertaisen kohtelun kannalta olisi teknologianeutraali sääntely sinällään perusteltua, mutta täysin tekniikkariippumaton sääntely voisi olla sääntelyn täsmällisyyttä ja tarkkarajaisuutta koskevan vaatimuksen kannalta haasteellista.

Vaiheittainen siirtyminen perinteisistä kiinteistä puhelinverkoista nykyaikaisiin tietoverkkoihin on tarkoittanut verkossa välitettävien sähköisten viestien sisällöllistä monipuolistumista, sähköisten viestien välittämisessä käytettävän verkkokokonaisuuden monimutkaistumista sekä uudentyyppisiä sähköiseen viestintään liittyviä palvelukonsepteja ja palveluntarjoajia.

Sekä viranomaisten toimivaltuuksia koskevassa sääntelyssä että sähköisen viestinnän palveluja koskevassa sääntelyssä erotetaan toisistaan sähköisen viestin sisältö ja sähköisen viestin tunnistamistiedot (välitystiedot, liikennetiedot) sekä sähköisen viestinnän välittämiseen liittymättömät teleosoitteen tai telepäätelaitteen sijaintitiedot (paikkatiedot). Eri aikoina laadituissa säännöksissä tosin voidaan käyttää samoista tai lähes samoista käsitteistä eri termejä taikka käyttää samaa termiä osin eri käsitteistä. Siviili- ja sotilastiedustelulainsäädännössä otettiin lisäksi käyttöön tietoliikennetiedusteluun liittyvä tietoliikenteen teknisten tietojen käsite (muut kuin viestin sisältöön kuuluvat tietoliikenteen tiedot; laki sotilastiedustelusta 10 § 11 kohta).

Verkossa välitettävät sähköiset viestit voivat olla ihmisten välisiä viestejä, ihmisen ja teknisen laitteen välisiä viestejä sekä teknisten laitteiden välisiä viestejä. Oma erityistapauksensa ovat vastaanottajalleen haitallisen tietokoneohjelman (virus tai vakoiluohjelma) sisältävät viestit. Tietoliikenteen teknisissä tiedoissa on kyse tietoliikenteen ohjaamisessa käytettävistä tiedonsiirron eri kerrosten tiedoista. Erityyppiset sähköiset viestit ja tiedonsiirron eri kerrosten ohjaustiedot ovat viestinnän luottamuksellisuuden ja yksityisyyden suojan näkökulmasta merkittävyydeltään erilaisia. Tämän huomioiminen viranomaisten tiedonhankintatoimivaltuuksia koskevassa sääntelyssä voisi olla mahdollista varsinkin silloin, jos erityyppiset viestit ja tiedonsiirron eri kerrosten ohjaustiedot kyetään erottelemaan ja suodattamaan automatisoidusti tiedonhankinnan yhteydessä.

Sähköisten viestien välittämiseen käytettävä verkkokokonaisuus voi koostua toisiinsa liitetyistä teleyritysten hallitsemista yleisistä viestintäverkoista, yhteisötilaajien hallitsemista lähiverkoista ja viestintäpalvelun käyttäjien hallitsemista likiverkoista. Viranomaisten tiedonhankintatoimenpiteet kohdistetaan teleosoitteeseen tai telepäätelaitteeseen. Teleosoite voi olla telepäätelaitteiden lisäksi viestintäverkkolaitteilla. Telepäätelaitteita ja viestintäverkkolaitteita voi olla kytkettyinä verkkokokonaisuuden kaikkiin osiin. Verkkokokonaisuuden monimutkaistumisen seurauksena tiedonhankinnan yhteydessä voi muodostua aiempaa moniulotteisempia sivullissuhteita. Moniulotteiset sivullissuhteet voivat koskea erityisesti haitallisten tietokoneohjelmien torjuntaan liittyvää tiedonhankintaa. Kyse voi olla esimerkiksi vakoiluohjelman kohteena olevan yhteisötilaajan tilaaman viestintäpalvelun käyttäjistä ”ensimmäisen asteen sivullisina” ja heidän kanssaan viestivistä henkilöistä ”toisen asteen sivullisina” taikka henkilöistä, joiden toisiinsa ketjutettuja laitteita käytetään haitallisen tietokoneohjelman sisältävän viestin levittämiseen heiltä salaa tai heitä harhauttamalla. Tiedonhankintatoimenpiteiden erityyppisiin laitteisiin kohdistamisen myötä voi tiedonhankinnan yhteydessä kertyä aikaisempaa enemmän ylimääräistä tietoa. Myös tässä yhteydessä viestinnän luottamuksellisuutta ja yksityisyyden suojaa parantaa se, jos erityyppisiä viestejä ja viestien sisältämiä erityppisiä tietoja kyetään erottelemaan ja suodattamaan automatisoidusti tiedonhankinnan yhteydessä.

Digitaaliseen toimintaympäristöön liittyvät sääntelyn haasteet koskevat sekä siviili- ja sotilastiedustelua (tietojen hankkiminen kansallista turvallisuutta vakavasti uhkaavasta toiminnasta) että rikostiedustelua (rikosten estämistä, paljastamista ja selvittämistä tu-

keva tiedonhankinta), mutta niiden merkitys korostuu siviili- ja sotilastiedustelun yhteydessä, kun siinä tiedonhankinnan tarkoituksen vuoksi tiedonhankinnan kohteena oleva toiminta ja tiedonhankinnan kohdehenkilöiden piiri (tiedustelutehtävään liittyvät henkilöt) ovat rikostiedustelua väljemmin määritellyt. Toisin kuin rikostiedustelussa, siviili- ja sotilastiedustelussa tiedonhankintaa voidaan kohdentaa myös sellaiseen organisaatiotoimintaan, jolla ei ole kiinteää kytkentää tiettyyn yksilöityyn henkilöön.

Tiedonhankintatoimivaltuudet ja tiedolliset toimivaltuudet

Siviili- ja sotilastiedusteluviranomaisten sekä muiden rikostorjuntaviranomaisten tehtäviensä hoitamisessa käytettävissä olevat toimivaltuudet voidaan jaotella tiedonhankintatoimivaltuuksiin, tiedollisiin toimivaltuuksiin sekä konkreettisten vaaratilanteiden ja rikosten estämiseen ja keskeyttämiseen liittyviin vaikuttamistoimivaltuuksiin. Tiedollisissa toimivaltuuksissa on kyse tietojen käsittelystä eli tietojen keräämisestä, kerättyjen tietojen automatisoidusta ja manuaalisesta prosessoinnista ja analysoinnista, tietojen hyödyntämisestä viranomaisen omassa toiminnassa, tietojen rekisteriin tallettamisesta sekä tietojen luovuttamisesta. Henkilötietojen käsittelystä säädetään tietosuoja- ja henkilötietolainsäädännössä, mikä tarkoittaa siviili- ja sotilastiedustelun yhteydessä rikosasioiden tietosuojalakia sekä poliisin henkilötietolakia ja Puolustusvoimien henkilötietolakia. Viranomaisen tiedolliset toimivaltuudet voivat olla yksityisyyden suojan näkökulmasta vähintäänkin yhtä merkittäviä kuin viranomaisen tiedonhankintatoimivaltuudet.

Siviili- ja sotilastiedusteluviranomaisten sekä muiden rikostorjuntaviranomaisten salaisen tiedonhankinnan toimivaltuuksissa on kyse siviili- ja sotilastiedustelun tiedustelumenetelmistä sekä rikostiedustelun salaisista tiedonhankintakeinoista (rikosten estämistä ja paljastamista tukeva tiedonhankinta) ja salaisista pakkokeinoista (rikosten selvittämistä tukeva tiedonhankinta).

Jo ennestään rikostiedustelussa käytettävissä olleet telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta ja tukiasematietojen hankkiminen ovat käytettävissä myös siviili- ja sotilastiedustelussa. Tietojen hankkiminen telekuuntelun sijasta, takautuva televalvonta ja takautuva tukiasematietojen hankkiminen muistuttavat tosiasiallisella luonteeltaan tiedonsaantioikeuksia. Siviili- ja sotilastiedustelulakien voimaantulon yhteydessä teknisen laitetarkkailun piiriin sisällytettiin (rikosten selvittämistä tukeva rikostiedustelu poisluettuna) myös sellaisten sähköisten viestien sisältö ja tunnistamistiedot, jotka viestit eivät ole vielä tai enää välitettävinä. Välitetyt viestit voivat tallentua teleyrityksen tai yhteisötilaajan haltuun ja viestintäpalvelun käyttäjän tekniseen laitteeseen. Ne voivat tallentua tai viestintäpalvelun käyttäjä voi tallentaa ne myös muun palveluntarjoajan kuin teleyrityksen haltuun. Viranomainen voi saada tiedon viestin sisällöstä tai viestin tunnistamistiedot viestin tallentumispaikasta ja tietojen hankkimistavasta riippuen erilaisia tiedonhankintatoimivaltuuksiaan tai tiedonsaantioikeuksiaan käyttämällä.

Teleyrityksen on tehtävä televerkkoon telekuuntelun ja televalvonnan edellyttämät kytkennät (poliisilaki 5 luku 61 § 1 momentti ja 5 a luku 51 § sekä laki sotilastiedustelusta 96 §; ks. myös laki sähköisen viestinnän palveluista 243 § 1 momentti 16 kohta sekä 322 ja 323 §). Yhteisötilaajalle ei ole säädetty vastaavaa velvollisuutta, mutta tuomioistuimen viranomaiselle antama telekuuntelu- tai televalvontalupa voi oikeuttaa yhteisötilaajan tai muun palveluntarjoajan kuin teleyrityksen tekemään telekuuntelun tai televalvonnan mahdollistavan toimenpiteen taikka luovuttamaan viranomaiselle luvan

piiriin kuuluvat tiedot. Teleyrityksen avustamisvelvollisuus koskee myös niitä tilanteita, joissa telekuuntelu tai televalvonta toteutetaan viranomaisen toimesta teknisellä laitteella. Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisessa tietojen hankkiminen toteutetaan aina viranomaisen toimesta teknisellä laitteella.

Siviili- ja sotilastiedustelulaeissa säädettyjä uusia tiedonhankintatoimivaltuuksia ovat sekä siviili- että sotilastiedustelussa käytettävissä oleva tietoliikennetiedustelu ja vain sotilastiedustelussa käytettävissä olevat radiosignaalitiedustelu ja ulkomaan tietojärjestelmätiedustelu. Nämä uudet toimivaltuudet ovat viestinnän luottamuksellisuuden ja yksityisyyden suojan näkökulmasta vähemmän haasteellisia varsinkin silloin, jos tai kun niiden käytön kohteena on valtiollisen toimijan sotilaallinen tai siihen rinnastettava toiminta.

Tiedonhankinta tietoliikenteestä ei saa olla yleistä ja kohdentamatonta tietoliikenteen seurantaa (laki sotilastiedustelusta 65 §; ks. myös laki tietoliikennetiedustelusta siviilitiedustelussa 1 § 4 momentti). Varsinaista tietoliikennetiedustelua edeltävää teknisten tietojen käsittelyä harjoitetaan tietoliikennetiedustelun kohdentamisen tarkoituksessa (vrt. tiedonsiirtäjän velvollisuus antaa hallussaan olevat Suomen rajan ylittävän viestintäverkon rakenteeseen ja siinä kulkevan tietoliikenteen reitittymiseen liittyvät tekniset tiedot, jotka ovat tarpeen viestintäverkon osan yksilöimiseksi tietoliikennetiedustelua koskevaa tuomioistuimelle esitettävää lupavaatimusta ja -päätöstä varten; laki sotilastiedustelusta 98 § ja laki tietoliikennetiedustelusta siviilitiedustelussa 22 §). Teknisten tietojen käsittelyä koskevat säännökset mahdollistavat tietoliikenteen teknisten tietojen hetkellisen keräämisen tuomioistuimen antaman luvan mukaisesta viestintäverkon osasta ja kerättyjen teknisten tietojen käsittelemisen tilastollista analyysiä varten (laki sotilastiedustelusta 66 § 1 momentti). Jos tietoliikenteen teknisten tietojen kerääminen kohdistetaan kerrallaan ainoastaan osaan tuomioistuimen antaman luvan mukaisesta viestintäverkon osasta tai teknisten tietojen käsittely kohdistetaan ainoastaan osaan kerätyistä teknisistä tiedoista, voi olla osin tulkinnanvaraista, mitä tämä tarkoittaa tietojen hetkellisen keräämisen keston tai tilastollisen analyysin tuloksen sisällön kannalta. Tilastollisen analyysin tulokseen ei saa sisältyä tietoa, josta voidaan tunnistaa yksittäinen luonnollinen henkilö (laki sotilastiedustelusta 66 § 2 momentti).

Siviili- ja sotilastiedustelulaeissa säädetään siviili- ja sotilastiedusteluviranomaisten oikeudesta saada yksityiseltä yhteisöltä yritys-, pankki- tai vakuutussalaisuuden piiriin kuuluvia tietoja taikka muita asiakastietoja (poliisilaki 5 a luku 50 § ja laki sotilastiedustelusta 104 § 1 momentti). Tiedonsaantioikeus on merkityksellinen erityisesti muiden sähköiseen viestintään liittyvien palvelukonseptien ja palveluntarjoajien kuin viestintäpalvelujen ja teleyritysten kannalta (esimerkiksi sijaintitietoihin perustuvat lisäarvopalvelut ja pilvi- ja palvelinhotellipalvelut sekä niiden tarjoajat). Osa uudentyyppisistä palvelukonsepteista ja palveluntarjoajista kuuluu sähköisen viestinnän palveluista annetun lain soveltamisalaan ja osa on siihen kuulumattomia. Siviili- ja sotilastiedusteluviranomaisilla on lisäksi oikeus saada teleyritykseltä ja yhteisötilaajalta teleosoitteen yhteystiedot taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot (poliisilaki 4 luku 3 § 2 momentti ja laki sotilastiedustelusta 104 § 2 momentti).

Yksityisten tahojen vapaaehtoinen tietojen viranomaiselle luovuttaminen on oma kokonaisuutensa. Tällainen tietojen luovuttaminen voi perustua muun muassa yleisiin tai sähköistä viestintää koskeviin erityisiin tietosuojasäännöksiin (yleinen tietosuoja-asetus 6 artikla sekä laki sähköisen viestinnän palveluista 17 luku ja 160 §). Tietojen tietosuojasäännöksiin perustuva luovuttaminen voi liittyä viestinnän välittäjän (teleyritys tai

yhteisötilaaja) ja lisäarvopalvelun tarjoajan lakisääteiseen oikeuteen ja velvollisuuteen huolehtia tietoturvasta (laki sähköisen viestinnän palveluista 247 ja 272 §).

Tietoturvatoimenpiteet ja vaikuttamistoimivaltuudet

Siviili- ja sotilastiedusteluviranomaisten rooli haitallisten tietokoneohjelmien torjunnassa kytkeytyy erityisesti sellaisiin yhteiskunnan elintärkeisiin toimintoihin liittyviin tietojärjestelmiin ja tietoliikennejärjestelyihin kohdistuviin kyberhyökkäyksiin ja kyberiskuihin (haittaohjelmat) sekä muihin tietoturvaloukkauksiin (vakoiluohjelmat), jotka uhkaavat kansallista turvallisuutta. Kyse on tällöin tiedonvaihdosta, joka tukee viranomaisten ja yksityisten tahojen tietoturvatoimenpiteitä (operatiivinen tilannekuva) sekä ylimmän valtiojohdon päätöksentekoa (strateginen tilannekuva). Siviili- ja sotilastiedustelulaeissa säädetään erikseen tietoliikennetiedustelun avulla hankittujen haitallista tietokoneohjelmaa koskevien tietojen luovuttamisesta viranomaiselle tai yksityiselle taholle (laki tietoliikennetiedustelusta siviilitiedustelussa 16 § ja laki sotilastiedustelusta 74 §).

Tiedonhankinnasta ja tietoturvaloukkauksilta suojautumisesta erillinen viranomaisten vaikuttamistoimivaltuuksia koskeva kysymyksensä on tietoturvaloukkausten torjumiseksi tai muussa tarkoituksessa harjoitettava voimankäyttö digitaalisessa toimintaympäristössä sekä siihen liittyvä siviili- ja sotilasviranomaisten välinen toimivallanjako.

Valvonta ja oikeusturvan toteutuminen

Siviili- ja sotilastiedustelutoiminnan valvontajärjestelmä koostuu toiminnan parlamentaarista valvontaa harjoittavasta eduskunnan tiedusteluvalvontavaliokunnasta ja toiminnan lainmukaisuuden valvontaa harjoittavasta tiedusteluvalvontavaltuutetusta, siviili- ja sotilastiedusteluviranomaisten henkilötietojen käsittelyä valvovasta tietosuojavaltuutetusta sekä ylimmistä laillisuusvalvojista eduskunnan oikeusasiamiehestä (siviili- ja sotilastiedusteluviranomaisten sekä tiedusteluvalvontavaltuutetun toiminnan lainmukaisuuden valvonta) ja valtioneuvoston oikeuskanslerista (tiedustelutoiminnan strategisen tason lainmukaisuuden valvonta). Valvonnan kokonaisuudessa on tärkeä rooli myös siviili- ja sotilastiedusteluviranomaisten sisäisillä laillisuusvalvojilla sekä siviili- ja sotilastiedusteluviranomaisia ohjaavilla ja valvovilla sisäministeriöllä ja puolustusministeriöllä. Viestinnän luottamuksellisuuteen ja yksityisyyden suojaan merkittävästi puuttuvien tiedustelumenetelmien käytöstä päättää tuomioistuin (Helsingin käräjäoikeus).

Kuten selonteossa todetaan, Yhdistyneiden kansakuntien ihmisoikeuskomitea on kiinnittänyt Suomen osalta huomiota siviili- ja sotilastiedustelutoimintaa valvovien tahojen suureen lukumäärään ja valvontajärjestelmän monimutkaisuuteen. Komitean mukaan valvontajärjestelmän monimutkainen rakenne voi vähentää valvonnan tehokkuutta. Oma näkemykseni on, että useiden itsenäisten ja riippumattomien valvojien keskinäiseen yhteistyöhön perustuva suomalainen valvontamalli mahdollistaa eri näkökulmista tapahtuvan valvonnan ja siihen liittyvän erityisasiantuntemuksen yhdistämisen kustannustehokkaalla tavalla. Esimerkiksi tiedusteluvalvontavaltuutetun ja tietosuojavaltuutetun välinen kiinteä yhteistyösuhde mahdollistaa muun muassa sen, että tiedusteluvalvontavaltuutettu voi tarvittaessa hyödyntää tietosuojavaltuutetun toimiston ICT-asiantuntijoiden tietotaitoa tieto- ja viestintäteknologissa kysymyksissä.

Tietoliikennetiedustelun toteuttamisen valvontaan liittyen olen tehnyt yhteistyötä kytkennän suorittajan (Suomen Erillisverkot Oy) kanssa. Kytkennän suorittaja varmistaa osaltaan, että tietoliikennetiedustelu kohdistetaan tuomioistuimen antamassa luvassa määritettyyn viestintäverkon osaan luvan voimassaoloaikana. Kytkennän suorittaminen on Suomen Erillisverkot Oy:n julkisen hallinnon turvallisuusverkkotoiminnasta annetun lain mukaisesta toiminnasta erillinen tehtävänsä. Vaikka teleyritykset (tiedonsiirtäjät) eivät osallistukaan tietoliikennetiedustelun varsinaiseen toteuttamiseen, olen pyrkinyt pitämään yhteyttä myös niihin FiCom ry:n kautta.

Selonteossa mainitaan Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen viimeisimmät siviili- ja sotilastiedustelutoiminnan sekä sen valvonnan sääntelyyn vaikuttavat ratkaisut. Ratkaisujen merkityksen arviointia suomalaisen tiedustelu- ja tiedusteluvalvontajärjestelmän kannalta vaikeuttaa se, että kukin ratkaisu koskee tietyn valtion tiedustelu- ja tiedusteluvalvontajärjestelmän kokonaisuutta ja eri valtioiden tiedustelu- ja tiedusteluvalvontajärjestelmät eroavat puolestaan varsin huomattavasti toisistaan. Euroopan unionin osalta sen jäsenvaltioiden kansallinen turvallisuus sekä kansallisen turvallisuuden suojaamiseksi harjoitettava siviili- ja sotilastiedustelu kuuluvat sinällään kunkin jäsenvaltion yksinomaiseen toimivaltaan. Unionin oikeudella on kuitenkin välillistä vaikutusta myös kansallisen turvallisuuden suojaamiseen esimerkiksi silloin, kun on kyse unionin sisämarkkinoilla toimiviin yrityksiin kohdistuvasta sääntelystä. Unionin oikeuden kansallisen turvallisuuden suojaamiseen liittyvän välillisen vaikutuksen ulottuvuudesta on tosin esitetty erilaisia näkemyksiä toisaalta yrityksille asetettavien velvoitteiden (esimerkiksi teleyritysten velvollisuus säilyttää tietoja viranomaistarpeita varten) sekä toisaalta viranomaisten tiedonhankintatoimivaltuuksien ja tiedonsaantioikeuksien (esimerkiksi viranomaisten oikeus saada teleyritysten viranomaistarpeita varten säilyttämiä tietoja) osalta.

Kimmo Hakonen
Tiedusteluvalvontavaltuutettu