Lausunto puolustusministeriölle tiedonhankintalakityöryhmän mietinnöstä ”Suomalaisen tiedustelulainsäädännön suuntaviivoja” 14.1.2015

julkisoikeuden professori, IT-oikeuden dosentti Tomi Voutilainen
15.4.2015

Puolustusministeriölle

Puolustusministeriö on pyytänyt minulta lausuntoa tiedonhankintalakityöryhmän suomalaisen tiedustelulainsäädännön suuntaviivoja käsittelevästä mietinnöstä (14.1.2015). Kiitän mahdollisuudesta lausua mietinnöstä ja annan työnantajastani riippumattoman lausunnon alla ilmenevin osin.

Yleistä

Puolustusministeriön asettaman työryhmän mietinnössä on käsitelty suppeasti tiedonhankinnan ja tietoturvauhkien torjunnan nykytilaa, esitetty Pohjoismaihin, Saksaan ja Alankomaihin rajoittunut kansainvälinen tiivistelmä eri maiden tiedustelulainsäädännöstä sekä tehty nykytilan arviointi ja kehittämisehdotukset. Mietintö sisältää myös yhden eriävän mielipiteen sekä kaksi lausumaa. Niin ikään mietinnön liitteenä on vertailu Suomeen ja Ruotsiin tehtyjen IT-investointien tilanteesta sekä lisäksi siinä on arvioitu Ruotsin tiedustelulainsäädännön vaikutuksia IT-investointeihin.

Nykytilan tiivistettynä kuvauksena mietinnössä todetaan, että ”kansallisesta turvallisuudesta vastaavat viranomaiset harjoittavat lakisääteisten tehtäviensä hoitamisen edellyttämää tiedustelua. Tiedustelua varten ei kuitenkaan ole laissa säädettyjä toimivaltuuksia. Tiedustelu perustuu yksinomaan julkisiin lähteisiin sekä kansainvälisen ja muun vapaaehtoisen yhteistyön puitteissa saataviin tietoihin”. Nykytilan kuvaus itsessään pitää jo sisällään jonkinasteisen tarpeen sääntelyn kehittämiselle. Suomen turvallisuudesta vastaavien viranomaisten toiminnan riippuminen vapaaehtoisen yhteistyön kautta saatavista tiedoista, ei muodosta uskottavaa tiedonhankinnan perustaa, jos sitä käytetään sisäisen tai ulkoisen turvallisuuden toteuttamiseen taikka kyberturvallisuustoimenpiteiden suunnitteluun tai toteuttamiseen. Toiminta voi jopa itsessään muodostaa kansalliselle turvallisuudelle riskin, jos yhteistyö ei toimi tai sitä käytetään vääriin tarkoituksiin. Niin ikään tällaiseen vapaaehtoiseen yhteistyöhön voi liittyä riskejä, jos sitä tehdään yksityisten yritysten kanssa. Esimerkiksi kyberturvallisuuteen liittyviä tietoja kerätään kaupallisessa toiminnassa, joita myös viranomaiset saavat hyödynnettäväksi omassa toiminnassaan. Pitkällä tähtäimellä tällainen toimintamalli ei voi toimia.

Yhteiskunnan peruspalvelut ja -toiminnot perustuvat nykyään informaatio- ja viestintäteknologian (ICT) hyödyntämiseen. Valtion ja kuntien hallinnon perusviestintä perustuu sähköisten tiedonsiirtomenetelmien, erityisesti sähköpostin käyttöön. Viranomaisten tiedottaminen perustuu muun muassa niiden omilla www-sivuilla jaettavaan tietoon. Kriisiviestintää on pyritty kehittämään julkisen hallinnon erilaisissa hankkeissa vaihtelevalla menestyksellä.

Turvallisuusviranomaisten viestintä perustuu informaatio- ja viestintäteknologian käyttöön ja on riippuvaa sen toiminnasta. Verotuksen toimittaminen ja pankkitoiminta on täysin informaatio- ja viestintäteknologian varassa. Nämä toiminnot ovat tärkeitä yhteiskunnan toiminnan kannalta katsottuna.

Julkisessa hallinnossa on myös havaittavissa kehitysvaihe, jossa tietovarantoja pyritään keskittämään tietojärjestelmien yhteentoimivuuden parantamiseksi. Terveydenhuollon tietoja ollaan keskittämässä valtakunnalliseen Kanta-arkistopalveluun. Niin ikään sosiaalihuollon puolella on suunnitteilla vastaava tietovarantoratkaisua Kansaa. Näistä tietovarannoista tiedon saatavuus on turvattava niin normaali- kuin poikkeusoloissakin, koska tietovarannoissa olevien tietojen avulla toteutetaan osaltaan yksilön perusoikeuksia

välttämättömään toimeentuloon ja huolenpitoon sekä riittäviin sosiaali- ja terveyspalveluihin (PL 19 §).

Niin ikään tietovarantojen keskittäminen tarkoittaa, että julkisten palveluiden ja viranomaisten toiminta sekä viranomaisten tietojärjestelmät ovat yleisen tietoverkon toiminnan varassa. Häiriöt tietoverkossa ja tietojärjestelmien toiminnassa voivat vaarantaa hyvän hallinnon toteuttamisen (PL 21 §).

Laillisuusvalvonnassa on toistuvasti todettu, että viranomaisten on huolehdittava lakisääteisten tehtäviensä hoitamisesta myös poikkeusoloissa, kuten tietojärjestelmien toimintahäiriöissä (ks. EOA 206/4/11, 31.5.2012; EOA 3256/4/07, 24.2.2009; AOA 2379/4/11, 7.9.2011; EOA 3498/2/04, 29.8.2006; OKA 547/1/04, 14.12.2005). Niin ikään laillisuusvalvonnassa on vakiintuneesti katsottu, ettei tietojärjestelmiin liittyvillä syillä voida perustella poikkeamista hyvän hallinnon ja oikeusturvan viranomaismenettelylle asettamista vaatimuksista. Viranomaisten tulisikin tietojärjestelmiä kehittäessään ja käyttäessään kiinnittää huomiota myös siihen, että järjestelmät mahdollistavat hyvän hallinnon turvaavat toimintatavat (ks. esimerkiksi EOA 537/4/10, 12.8.2010; EOA 2523/4/08, 8.11.2010; AOA 3718/4/07, 17.12.2008; AOA 3951/4/09, 21.6.2010).

Onkin selvää, että viranomaisissa tietoturvatoimenpiteillä toteutetaan osaltaan perustuslain 22 §:ssä julkiselle vallalle säädettyä velvollisuutta turvata perusoikeuksien toteutuminen. Yhteiskunnan digitalisoituminen johtaa siihen, että tämä turvaamisvelvollisuus laajenee ja toimenpiteet sen mukaisesti. Tämä ei kuitenkaan ole ongelmatonta. Perusoikeuksien turvaaminen voi johtaa ristiriitaan, jonkin toisen perusoikeuden kanssa. Puolustusministeriön työryhmän mietinnössä käsitellään näitä perusoikeuksia perustuslain 10 §:ssä säädetyn luottamuksellisen viestinnän suojan sekä henkilötietojen suojan kannalta katsottuna. Tietoturvatoimenpiteet voivat olla ristiriidassa myös sananvapauden (PL 12.1 §) ja omaisuuden suojan (PL 15.1 §) kanssa. *Ministeriön mietinnössä olisi voitu tehdä laajemmin perusoikeuksia koskevaa intressivertailua, joten näkökulmia on syytä syventää ja laajentaa, jos mietinnön pohjalta käynnistetään lainvalmisteluhankkeita.*

Julkisessa hallinnossa eräänä kehitystrendinä näyttää olevan monella eri sektorilla tietoturvallisuuden ja kyberturvallisuuden nimissä resurssitarpeen lisäämisen perustelu. Toisaalta eri viranomaiset ovat ryhtyneet suhteellisen kevyillä perusteilla tieto- ja kyberturvallisuusviranomaisiksi. Selkeää vastuunjakoa ei ole valtion kyberturvallisuushallinnon järjestämisestä hajanaisen lainsäädännön vuoksi. Puolustusministeriön johdolla laadittu kyberturvallisuusstrategia ei ratkaissut eri toimijoiden vastuita tässä asiassa.

Yhteiskunnan tieto- ja kyberturvallisuuden varmistaminen voidaan nähdä osana Suomen ulkoisen ja sisäisen turvallisuuden varmistamista. Tässä suhteessa yhteiskunnan tieto- ja kyberturvallisuuden varmistaminen on ensisijaisesti puolustus- ja sisäministeriön toimialaan kuuluva tehtävä. Valtionhallinnon hajautuneet vastuut johtavat laajoihin kehittämishankkeisiin sekä hitaaseen kehittämiseen. Esimerkiksi valtionhallinnon tietoturvallisuudesta annettua asetusta (681/2010) valmisteltiin valtionhallinnon tietoturvallisuuden johtoryhmän ohjauksessa 3,5 vuotta.

Niin ikään valtionhallinnon tieto- ja kyberturvallisuuden hajautunut hallinnointi- ja ohjausjärjestelmä ovat omiaan aiheuttamaan ongelmia erilaisten tieto- ja kyberturvallisuustoimenpiteiden toteuttamiseksi. Esimerkiksi hajautuneesta mallista johtuen tieto- ja kyberturvallisuutta koskevia erityisen korkean suojaustason tietoja voidaan joutua

käsittelemään usean ministeriön hallinnonalalla, joka lisää riskiä näiden tietojen paljastumisesta. Puolustusministeriön työryhmän mietinnössä tiedustelutieto on todettu tällaiseksi suojattavaksi tiedoksi.

Nykyisessä rakenteessa, jossa valtionhallinnon tieto- ja kyberturvallisuushallintorakenne koostuu seuraavista osista, ei voi toimia pohjana tiedustelutiedon käytölle hallintorakenteen laajuuden vuoksi (ministeriöt ja toimialat merkitty yhteiskunnan turvallisuuden kannalta prioriteettijärjestyksessä):

- puolustusministeriö: puolustusvoimien eri laitokset ja Turvallisuuskomitea;
- sisäministeriö: Poliisihallitus, Keskusrikospoliisi ja Suojelupoliisi;
- valtioneuvoston kanslia: valtioneuvoston hallintoyksikkö, erityisesti tilannekeskustoiminta;
- ulkoasiainministeriö;
- liikenne- ja viestintäministeriö: Viestintävirasto, erityisesti Kyberturvallisuuskeskus;
- valtiovarainministeriö sekä
- eräiden lainsäädäntövastuiden osalta oikeusministeriö;

Edellä esitetystä johtuen jatkovalmistelussa on syytä linjata suppeasti ne viranomaiset, jotka voivat hyödyntää tiedustelutietoa.

Puolustusministeriön työryhmän mietinnössä ehdotetaan käynnistettäväksi yksi lainsäädäntöhanke tai useampia lainsäädäntöhankkeita tiedustelulainsäädännön kehittämiseksi, jolla mahdollistetaan tietoliikennetiedustelu, ulkomaan henkilötiedustelu ja ulkomaan tietojärjestelmätiedustelu. Työryhmän mietinnössä esitetään varsin yleisiä perusteluita tiedustelulainsäädännön kehittämiseksi nykytilan kuvauksessa. Mietintö pitää sinällään perustason analyysin perus- ja ihmisoikeuksien vaikutuksesta tiedustelulainsäädännön kehittämiseen, mutta selkeitä ja välttämättömiä perusteluita mietinnössä ei esitetä sille, että tiedustelutoiminnan kehittäminen olisi Suomen turvallisuuden ja valtion johdon päätöksenteon kannalta erityisen välttämätöntä ja että ehdotetulla tiedustelutoiminnalla saadaan niitä tuloksia, jotka luovat oikeutuksen ihmis- ja perusoikeuksien ainakin jonkinlaiselle rajoittamiselle tai puuttumiselle niihin. Toisaalta mietintöä voidaan pitää esiselvityksenä tarkemman sääntelytarpeen arvioimiseksi. Mietintö ei muodosta yksin pohjaa sen arvioimiseksi, minkälaista ja missä laajuudessa tiedustelulainsäädäntöä tarvitaan ja minkälaisilla viranomaisten toimivaltuuksilla tiedustelutoiminta olisi sille asetettuihin tavoitteisiin nähden tuloksellista.

Mietinnöstä saa hyvän käsityksen siitä, mitä suuntaviivoja ja ehtoja erityisesti Euroopan ihmisoikeustuomioistuin on asettanut tiedustelutoiminnalle. Tämä luo hyvän peruspohjan tiedustelulainsäädännön kehittämiselle, jos tälle nähdään tarve ja siihen on riittävät perustelut.

Mietinnöstä ilmenee, että ehdotetut toimenpiteet edellyttäisivät perustuslain muuttamista. Perustuslain säätämisjärjestyksen vuoksi tämä voi siten tarkoittaa, että mietinnössä esitetty tiedustelutoiminta voitaisiin käynnistää noin viiden vuoden kuluttua. Tästä syystä on vaikea nähdä, että ehdotetulle tiedustelutoiminnalle on välittömiä tarpeita valtion johdon päätöksenteon, valtion turvallisuuden taikka kyberturvallisuuden kannalta katsottuna. Toisaalta teknologian kehittyminen voi luoda tarpeita kehittää sääntelyä johonkin toiseen muotoon ja uusiin tiedustelukeinoihin.

Tietoliikennetiedustelu

Mietinnössä todetaan, että ”Viime vuosina erityisesti tietoverkkoympäristössä tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion turvallisuudelle ja sen eduille”. Mietinnöstä ei ilmene, miten Suomen tietoliikennetiedustelutoiminnan kehittämisellä voidaan estää toisen valtion tietoliikennetiedustelu. Perinteisesti tällainen tietoliikennetiedustelu on pyritty estämään erilaisin teknisin tietoturvatoimenpitein, jollaisena voidaan pitää laajassa mittakaavassa Suomen turvallisuusverkkotoiminnan kehittämistä ja turvallisuusverkon käyttöönottoa sekä siinä olevia suojausjärjestelmiä.

Mietinnössä todetaan, että ”kaapelivälitteisen tietoliikenteen merkitys kansalliseen turvallisuuteen kohdistuvien uhkien torjunnan kannalta on tunnistettu useissa Suomeen verrattavissa olevissa länsimaissa. Kansainvälisestä vertailusta käy ilmi, että useimpien verrokkimaiden lainsäädäntö mahdollistaa viranomaisten oikeuden kohdistaa tiedustelua kaapeliverkkoihin tai tällaista lainsäädäntöä suunnitellaan”. Mietinnöstä ei ilmene, mitä tuloksia tällä tiedustelutoiminnalla on saatu aikaan ja minkälaisia intressejä tällaisella tiedustelutoiminnalla on saatu suojattua. Tällainen tieto on merkityksellinen arvioitaessa tiedustelutoiminnan tuloksellisuuden ja vaikuttavuuden suhdetta puuttumiseen muun muassa perus- ja ihmisoikeutena turvattuun luottamuksellisen viestinnän suojaan.

Mietinnössä todetaan niin ikään, että ”tietoliikennetiedustelussa on kyse siitä, että viranomainen hankkii kansallisen turvallisuuden kannalta olennaista tietoa tietoliikenteestä ja sen sisällöstä. Tietoliikennetiedustelu voi yleisesti kohdistua valtion sisäiseen tai rajat ylittävään tietoliikenteeseen”. Lähtökohdiltaan mietinnössä luonnehdittu tietoliikennetiedustelu on ongelmallinen. Miten olennaisuus määritellään missäkin tilanteessa ja kuinka olennaisuus määritellään sääntelyssä riittävän täsmällisesti? Tiedustelutoiminta tietoverkossa erityisesti tietoturvallisuuteen liittyvien uhkien tunnistamisen osalta voi olla vaikeaa tästä asetelmasta. Epäolennainenkin tieto voi muuttua olennaiseksi ennakoimatta, jolloin ihmisoikeuksiin ja perusoikeuksiin puuttumista koskevat rajoitukset tiedustelutoiminnan osalta eivät välttämättä mahdollista näiden olennaisuuksien tunnistamista ja hyödyntämistä. Mietinnössä esitellyt ihmisoikeussopimuksien tulkintaan liittyvät linjaukset johtavat siihen, että olennaisuuteen perustuva verkkotiedustelutoiminta voi kohdistua vain rajattuun kokonaisuuteen, jolloin ainakaan tietoturvauhkien tunnistamiseksi tietoliikennetiedustelu ei ole toimiva ratkaisu tietoturvauhkien torjumiseksi yleisessä tietoverkossa.

Mietinnön perusteella rajattuihin ja täsmällisiin kohteisiin kohdistuva tietoliikennetiedustelu voi olla tarpeellista, mutta sääntely ja verkkotiedustelutoiminnan kehittäminen edellyttävät huolellista lainvalmistelua ja täsmällistä sääntelyä. Ihmisoikeussopimuksista johtuvat rajoitteet tiedustelutoiminnalle voivat johtaa myös siihen, ettei tietoliikennetiedustelutoiminnalla saavuteta niitä hyötyjä, joita sillä ennakoidaan. Tästä syystä mahdollisessa sääntelyn jatkovalmistelussa on syytä avoimien skenaarioiden kanssa käydä avoin keskustelu siitä, voidaanko tietoliikennetiedustelutoiminnalla saavuttaa mitään sellaista, jolla voidaan perustella perus- ja ihmisoikeuksiin puuttuminen. Mietintö ei ole tältä osin vakuuttava eikä sen perusteella voida tehdä pitkälle meneviä johtopäätöksiä sääntelyn kehittämisen tarpeellisuudesta tietoliikennetiedustelun osalta. Sinällään se tosiasia, että suomalaisten tietoliikennettä voidaan seurata muissa maissa, ei vielä tuo perustetta sille, että Suomeen tarvitaan tietoliikennetiedustelutoimintaa. Tätä tulee arvioida kansallisista tarpeista

käsin sekä erityisesti niiden hyötyjen ja haittojen näkökulmasta, joita tietoliikennetiedustelutoiminta tarkoittaa perus- ja ihmisoikeuksien kannalta katsottuna.

Ulkomaan tietojärjestelmätiedustelu

Työryhmän mietinnössä käsitellään varsin suppeasti ulkomaan tietojärjestelmätiedustelun tarvetta. Nähdäkseni ulkomaan tietojärjestelmätiedustelu on työryhmän mietinnön ehdotuksista ongelmallisin. Ulkomaan tietojärjestelmätiedustelun tarvetta ei ole perusteltu riittävästi mietinnössä. Toisaalta ulkomaan tietojärjestelmätiedustelu voi olla ongelmallinen Suomea sitovien ihmisoikeussopimuksien kannalta, koska tietojärjestelmätiedustelussa voidaan joutua tekemisiin omaisuuden suojan, henkilötietojen suojan sekä luottamuksellisen viestinnän suojan kanssa Suomen oikeudenkäytön ulkopuolella. Työryhmän mietinnön pohjalta ei ole nähtävissä sellaista tarvetta, että ulkomaan tietojärjestelmätiedustelu olisi erityisen tarpeellista Suomen kansallisen turvallisuuden tai Suomen valtion johdon päätöksenteon kannalta katsottuna normaalioloissa. Ulkomaan tietojärjestelmätiedustelu ei ole myöskään perusteltua tieto- ja kyberturvallisuustoimenpiteiden kannalta katsottuna normaalioloissa. Voitaisiin kuitenkin ajatella, että valmiuslainsäädäntöön tällainenkin sääntely voisi sisältyä poikkeusoloja varten.

Yhteenveto

Puolustusministeriön työryhmän mietintö ei ole täysin vakuuttava sen suhteen, että tiedustelulainsäädännön kehittämisellä ja jonkinasteisella puuttumisella perusoikeuksiin edistettäisiin niitä intressejä, joiden vuoksi tiedustelutoimintaa pitäisi laajentaa. Jos jatkovalmistelussa pystytään paremmin perustelemaan konkreettisesti erityisesti tietoliikennetiedustelun tarve tieto- ja kyberturvallisuuden edistämiseksi, ei tietoliikennetiedustelulainsäädännön kehittämiselle olisi esteitä, kun se tehdään ihmis- ja perusoikeuksien rajoittamista koskevien suuntaviivojen mukaisesti ja on sopusoinnussa kansainvälisten ihmisoikeussopimusten kanssa. Edellytykset tällaiselle kehitystyölle sinällään on olemassa perus- ja ihmisoikeuksien rajoitusta koskevien kansallisten ja kansainvälisten tulkintojen perusteella. Toiminnan käynnistäminen vaatii kuitenkin lisäresursseja sekä toimivan operatiivisen toiminnan ja valvontajärjestelmän luomisen eri intressien yhteensovittamiseksi. Joka tapauksessa tiedustelulainsäädännön puute on selvä epäkohta lainsäädännössämme, kun otetaan huomioon muuten tiedustelutoiminnan laaja-alaisuus muualla eri valtioissa. Suomi ei voi siten täysin jättää tiedustelutoimintaa vaille oikeudellista sääntelyä, vaikka säännöksiä sovellettaisiin vain poikkeuksellisissa tilanteissa.

Puolustusministeriön työryhmän mietinnön perusteella voidaan todeta, että Suomen valtionhallinnon tieto- ja kyberturvallisuuden ohjaus- ja hallintamallia pitäisi kehittää selkeämmäksi sekä virtaviivaisemmaksi. Mietintöä on ollut valmistelemassa seitsemän eri ministeriön edustajat ja perustason esiselvityksen tekemiseen kului aikaa vuosi. Julkisen hallinnon tieto- ja kyberturvallisuuden kehittäminen voi vaatia nopeita toimenpiteitä erilaisten riskien torjumiseksi. Tällöin eri ministeriöiden toimivaltasuhteet pitäisi olla selkeitä sekä reagointivalmiuden viivytyksetöntä. Kehittämistyön pitäisi tapahtua matalalla organisointirakenteella. Tiedustelulainsäädännön mahdollinen kehittäminen voisi toimia alustana myös edellä mainittujen epäkohtien korjaamiseksi sekä laajemmin tietoturvalainsäädännön kehittämiseksi. Tarve tietoturvallisuuslainsäädännön kehittämiseksi on tunnistettu jo noin 20 vuotta sitten valtiovarainministeriön teettämässä laajassa selvityksessä. Tähän kehittämistyöhön ei ole kuitenkaan kyetty edellä mainituista toimivaltasyistä. Onkin tärkeää, että valtioneuvostotasolla poliittisesti tehdään linjaukset siitä, millä mallilla tiedustelulainsäädäntöä kehitetään ja missä laajuudessa ja että tietoturvallisuuden kansallista sääntelyä kehitetään myös tämän rinnalla. Myös eduskuntaa on

syytä kuulla varhaisessa vaiheessa. Turvallisuusverkkotoiminnan lainsäädännön eduskuntakäsittelyn yhteydessä hallintovaliokunta joutui toteamaan mietinnössään (HaVM 35/2014 vp), että toimeenpanosta vastaava hallinto oli jo ryhtynyt turvallisuusverkkotoiminnan toimeenpanoon, jolloin lainsäätäjä on joutunut tapahtuneiden tosiasioiden eteen, eikä valiokunnalla ollut asiassa tosiasiallisesti käsityksensä mukaan juurikaan mahdollisuutta päätyä näiltä toteutuneilta osin hallituksen esityksestä poikkeavaan ratkaisuun. Edellä esitetystä syystä tiedustelulainsäädännön kehittäminen on suositeltavaa tehdä laaja-alaisessa parlamentaarisessa ohjauksessa. Tämä voi myös edistää lainsäädännön kehittämistä nopeammalla aikataululla, jos siihen saadaan riittävä poliittinen konsensus.

15.4.2015

Tomi Voutilainen
julkisoikeuden professori, IT-oikeuden dosentti