Puolustusministeriö
kirjaamo@defmin.fi

Puolustusministeriön lausuntopyyntö 9.2.2015; Suomalaisen tiedustelulainsäädännön suuntaviivoista; tiedonhankintalakityör

Poliisihallituksen lausunto tiedonhankintalakityöryhmän mietinnöstä

Puolustusministeriö asetti 13.12.2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista. Työryhmä luovutti mietintönsä puolustusministeri Carl Haglundille 14.1.2015.

Puolustusministeriö on pyytänyt lausuntoa työryhmän mietinnöstä. Mietinnössä arvioidaan tiedustelua koskevan lainsäädännön kehittämistarpeita. Puolustusministeriö toivoo näkemyksiä erityisesti mietintöön sisältyvistä kehittämisehdotuksista ja johtopäätöksistä (luvut 6 ja 7) sekä ehdotusten vaikutuksista lausunnonantajan toimintaan tai toimialalla.

Poliisihallitus pitää ehdotusta uusista tiedonhankintaa koskevista toimivaltuuksista periaatteessa kannatettavana. Poliisihallitus uudistaa työryhmän jäsenen Poliisihallituksen edustajan poliisijohtaja Tomi Vuoren työryhmän mietintöön liitetyn lausunnossa todetun ja haluaa lisäksi tuoda esiin muutamia asioita, joita tulisi huomioida.

Lähtökohdat

Rikollisuus ja sen tekotavat ovat muuttuneet voimakkaasti viimeisen kymmenen vuoden aikana. Maailman ja suomalaisen yhteiskunnan digitalisoituminen merkitsee monien käytännön asioiden ja ilmiöiden siirtymistä lisääntyvässä määrin tietoverkkoympäristöön. Näin tapahtuu tai on jo tapahtunut myös rikollisuuden osalta. Yhteiskuntaan, yritystoimintaan ja kansalaisiin kohdistuva tietoverkkorikollisuus on kasvava uhka. Muutaman vuoden kuluessa tietoverkkoihin tai tietojärjestelmiin joko kohdistuvien tai niitä hyväksikäyttävien rikosten määrä tulee lisääntymään myös Suomessa merkittävästi.

Turvallisuudesta vastaavilla viranomaisilla on täysin perusteltu tarve saada tietoverkoista tietoa, joka liittyy niiden toimialaan kuuluvien uhkien torjuntaan. Virustorjunnalla tai vastaavilla teknisillä keinoilla ei tietoverkkouhkia voida kokonaan torjua. Niiden jälkeen jää jäljelle vielä kaikkein vakavimmat uhat. Tietoverkkoja joko käytetään rikoksentekovälineenä tai niitä hyödynnetään rikosten suunnittelussa tai rikollisten välisessä yhteydenpidossa jne. Taloudellista hyötyä tavoittelevat tietoverkkoja hyväksikäyttävät rikolliset ovat jo nyt osa kotimaista rikolliskenttää. Kyberrikollisuus on globaalia rikollista toimintaa, jossa valtioiden rajat eivätkä viranomaisten perinteiset valvontamenetelmät enää muodosta estettä rikolliselle toiminnalle. Suomi ei

voi tämä huomioon ottaen ja tässä suhteessa olla kansainvälisestikään poikkeus jättämällä säätämättä tietoverkon tiedustelusta. Mietinnön lyhyestä kansainvälisestä vertailusta käy selvästi ilmi, että Suomi ei ole verrokkivaltioiden tasolla. Esitutkintaviranomaisilla olevan rikosperusteisen tiedonhankinnan lisäksi myös siviili- ja sotilastiedustelulla tulee olla Suomessa valmiudet muuhun kuin rikosperusteiseen tiedonhankintaan.

Puolustusministeriön asettaman työryhmän lähtökohdat lainsäädännön kehittämisestä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista olivat jossakin määrin hankalat. Asettamiskirjeessä työryhmän tehtäväksi oli asetettu selvittää asiaan liittyvät turvallisuusviranomaisten tarpeet. Kuitenkaan missään ei ollut eritelty niitä viranomaisia, jotka katsotaan kuuluvaksi turvallisuusviranomaisiksi, ja osaksi tästä syystäkin mietinnön katsantokanta tarpeiden määrittelylle jäi suppeaksi. Tämä lähtökohta-asetelma määritti pitkälle myös ne ratkaisuvaihtoehdot, joihin työssä päädyttiin. Lainsäädännön tarpeellisuutta on nyt tarkasteltu mietinnössä suurelta osin vain puolustusvoimien ja Suojelupoliisin toiminnan lähtökohdista.

Käsitteet

Viime vuosien turvallisuuskehitystä on leimannut perinteisen sotilaallisten ja siviiliuhkien välisen rajanvedon hämärtyminen. Suomessa tämä ilmenee muun muassa siinä, että käyttöön on otettu laaja-alainen turvallisuuskäsitys. Kansallisen turvallisuuden turvaaminen valtion rajojen ulkopuolelta suuntautuvaa uhkaa vastaan laajan turvallisuuskäsityksen mukaan pitänee sisällään myös kansainväliseltä ja järjestäytyneeltä rikollisuudelta suojautumisen eli sen torjumisen. Erityisesti tietoverkkoihin kohdistuvien uhkien osalta on ainakin alkuvaiheissa usein mahdotonta sanoa, kumman luonteisesta uhasta on kysymys. Mietinnöstä on kuitenkin havaittavissa, että "sotilaallinen" uhka osin sekoittuu siviililuontoisiin uhkiin. Toisaalta raja-aitojen tarpeeton pystyttäminen tiedustelun ja perinteisen poliisitoiminnan ja muun viranomaistoiminnan välille on vältettävä. On hyvin tärkeää, että turvallisuusviranomaisten tilannekuva muodostuu riittäväksi, vaikka rajanvetoa ei heti voitaisikaan tehdä.

Laajana käsitteenä tiedustelutoiminnalle, jota mietinnössä käsitellään, on erityistä se, että sen tulisi olla tilannekuvaa luovaa tiedonhankintaa jo siinä vaiheessa, kun varsinaista perusteltua epäilyä kenenkään syyllistymisestä tiettyyn rikokseen ei ole vielä olemassa. Ongelmaksi tässä laaja-alaisesti käsitettävässä tiedustelutoiminnassa muodostuvat perusoikeuksien vaatimukset ja yksityisyyden suoja, jotka edellyttävät, että toiminnalle tultaisiin asettamaan selkeästi ymmärrettävissä olevat rajat. Lisäksi poliisi ja muut lainvalvontaviranomaiset saavat jatkuvasti toiminnassaan tietoja, joilla voi olla mietinnössä tarkoitettua merkitystä yhteiskunnan turvallisuudelle. Mahdollisimman täydellisen tilannekuvan saavuttamiseksi sekä mietinnössä tarkoitetulla tiedustelulla että normaalilla poliisitoiminnalla saadut tiedot tulee voida tiedusteluprosessin analyysivaiheessa yhdistää.

Mietinnön mukaan tietoverkoissa tapahtuvaa tiedonhankintaa toimintona kuvataan luonteeltaan tiedusteluna, mutta Poliisihallituksen näkemyksen mukaan *verkkovalvonta* käsitteenä kuvaa paremmin kyseistä toimintaa. Tästä käytetään myös nimitystä massavalvonta, koska kyse on teknisestä pääsystä kaikkeen tietoliikenteeseen. Mietinnössä kuvattu tiedonhankinta

toimintona on rinnastettavissa käsitteisiin *tullivalvonta, rajavalvonta* tai *liikennevalvonta*, joissa valvonnan kohteeksi joutuu osa liikenne-, tavara- tai henkilövirrasta tiettyjen kriteerien perusteella, kuten vastaavasti kohteet valtion rajat ylittävään tietoliikenteeseen kohdistuvassa tiedonhankinnassa (verkkovalvonta).

Tarkoitus

Verkkovalvonnan tarkoituksena olisi havaita, tunnistaa ja hankkia tietoa uhista. Sillä ei mietinnön mukaan estettäisi uhkien toteutumista. Mietinnön mukaan rajapinta valvonnan ja torjuntatoimien välillä olisi järjestettävä erikseen. Mietinnössä mainitusta rajapinnasta tulee oletettavasti muodostumaan haaste, mikäli toiminnan painotus on lähinnä valtiojohdon päätöksentekoa tukevaa, eikä niinkään uhkien torjuntaan painottuvaa. Torjuntatoimien osalta keskeiseksi toimijaksi muodostuisi kuitenkin valtaosin poliisi.

Tiedonhankintakeinot

Mietinnössä esitetyt tiedonhankintakeinot jaotellaan kolmeen kategoriaan; 1) tietoliikennetiedustelu, 2) ulkomaan henkilötiedustelu ja 3) ulkomaan tietojärjestelmätiedustelu. Näistä kolmesta tiedustelumenetelmästä poliisin perinteiselle toimialueelle liittyvä lienee tietoliikennetiedustelu. Menetelmällä voidaan olettaa olevan olennaista merkitystä myös rikosuhkien torjunnan ja tutkinnan näkökulmasta. Tältä osin on jossain määrin vaikea nähdä, että toimivaltuus kategorisesti tai edes osin asettuisi puolustusvoimien nykyiselle tehtäväalueelle. Ulkovaltojen mahdollisesti Suomeen kohdistama laiton tiedustelutoiminta, jossa hyödynnetään tietoverkkoja, on poliisin tehtäväalueelle kuuluvaa. Rajanveto siitä, milloin tällainen toiminta ulottuu Suomen puolustuksellisiin tavoitteisiin, on kuitenkin varsin epäselvä. Tämä havainnollistuu selkeämmin silloin, kun puhutaan terrorismin torjunnasta, joka on ensisijaisesti poliisin tehtävä, joskin puolustusvoimilla on tässä kohden voimakas rooli kansainvälisen toiminnan kautta.

Mietinnössä tietoliikennetiedustelusta on mainittu, että siinä olisi kyse tiedustelutoimivaltuudesta, jonka tarkoituksena olisi tuottaa kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa ulkomaisista toimijoista ja olosuhteista ylimmän valtiojohdon päätöksenteon tueksi. Tiedustelu ei olisi samalla tavalla henkilö- ja rikossidonnaista toimintaa kuin rikosten ennaltaehkäiseminen. Tältä osin toimivaltuus määrittyy käyttöalaltaan varsin suppeaksi.

Poliisihallituksen arvion mukaan verkkovalvonta saattaa muuttua luonteeltaan summaarisesta tiedonhankinnasta helposti kohdennetuksi tiedonhankinnaksi. Tällainen tilanne syntyy, kun verkkovalvonnassa alun perin käytettyjen poimintaparametrien mukaan pystytään tunnistamaan viestinnän taustalla oleva taho. Henkilöön kohdistuvaan kohdennettuun tiedonhankintaan tarvitaan oma, erillinen toimivaltuutensa.

Vaikkakin mietintö käsittelee aihepiiriä vahvasti Suomen puolustuksellisesta näkökulmasta, joka toimialueensa osalta menee vahvasti puolustusvoimien toimivallan piiriin, ovat mietinnössä kuvatut toiminnot tietoliikennetiedustelun osalta sellaisia, jotka kuuluvat luontevammin poliisin tehtäväkenttään. Tältä osin keskeisimpinä toimijoina on luontevaa nähdä Suojelupoliisin lisäksi Keskusrikospoliisi.

Ulkomaan henkilötiedustelun ja ulkomaan tietojärjestelmätiedustelun osalta toiminta ei kuulune poliisin perinteiselle toimivalta-alueelle. Henkilötiedustelu (HumInt) on tosin rinnastettavissa poliisi- ja pakkokeinolaissa säädettyyn tietolähdetoimintaan (ohjattu tietolähteen käyttö). Tietojärjestelmätiedustelu taasen on tulkittavissa vieraan valtion alueella, tietoverkoissa tapahtuvaksi operatiiviseksi toiminnaksi, joka toiselta näkökannalta voidaan tulkita jopa aggressiiviseksi menetelmäksi. Molempien toimintojen osalta kansallinen lainsäädäntö ei anna tähän ratkaisua. Siviilitiedustelun osalta voidaan mainita Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän loppuraportissa ollut maininta, jossa todetaan ulkomaantoimivaltuuksien olevan joissakin rajoissa Suojelupoliisille tarpeen.

Lainsäädäntö tarpeet

Verkkovalvonnan tarpeet on järkevää jaotella kolmeen asiakokonaisuuteen; puolustusvoimien tarpeet, tiedustelun/siviilitiedustelun tarpeet sekä poliisin rikosprosessuaaliset muut tarpeet. Tästä näkökulmasta Poliisihallitus painottaa lausunnossaan poliisin tarpeita.

Tällä hetkellä poliisin tiedustelusta ei varsinaisesti ole säädöstä, jonka nojalla poliisilla olisi toimivalta suorittaa tiedustelua tietoverkoissa. Tiedustelua koskevaa voimassa olevaa lainsäädäntöä ei ole muiltakaan osilta säädetty. Varsinaista tiedustelun käsitettä ei ole myöskään määritelty lainsäädännössä ja tämä voidaan nähdä osin puutteena varsinkin tiedon keräämisen, tallentamisen ja analysoinnin näkökulmasta. Säädösten puuttuminen on vakava lainsäädännöllinen puute ja lisäksi on tarve säätää vakavan ja järjestäytyneen rikollisuuden torjunnassa tarvittavaa tiedustelulainsäädäntöä sekä ylipäätään poliisin toimialaan liittyvää tiedustelulainsäädäntöä. Erityisesti järjestäytynyttä ja vakavaa rikollisuutta, joka on kansainvälistä ja rajat ylittävää, tulisi torjua myös tietoverkoissa tapahtuvan tiedustelun avulla laissa säädetyin toimivaltuuksin. Tämä edistäisi myös poliisin ennalta estävää toimintaa ja parantaisi sisäistä turvallisuutta.

Tietoverkkouhissa on kuitenkin pääsääntöisesti kyse epäillyistä rikoksista, vaikkakaan ei aina, ja poliisi on rikostorjunnan yleistoimivaltainen viranomainen. Poliisille on tärkeää, ettei rikostorjunnan kokonaisuutta pilkota, ja että toimivaltuudet ulottuvat kaikkiin poliisin toimialalla esiintyviin tilanteisiin. Mietinnössä kuvattu tiedustelu on eräs tiedonhankintakeino, ja poliisin näkökulmasta siten yksi osa rikostorjunnan kokonaisuutta. Tiedusteluun liittyvää lainsäädäntöä tulisi tarkastella myös vakavan rikollisuuden torjunnan näkökulmasta, jolloin tiedonhankinta tulisi suunnata esim. järjestäytyneen rikollisryhmän koko rikollisen toiminnan torjumiseen yksittäisten rikosten paljastamisen sijasta. Nykylainsäädäntö on pitkälti sidottu "reaalimaailman" toimintaan, eikä ole olemassa tiedustelua koskevaa lainsäädäntöä, joka määrittelisi poliisin toimivaltuuksista esimerkiksi siltä osin, miten tai mitä ja missä roolissa poliisi saa suorittaa tiedustelua hankkiessaan tietoa tietoverkoista.

Puolustushallinnon ja poliisihallinnon tiedonsaantitarpeet voidaan mahdollisesti tyydyttää eri menettelytavoin. Asian ratkaisumallit saattavat olla lainsäädännöllisesti erilaisia poliisin ja muiden esitutkintaviranomaisten kuin puolustusvoimien kohdalla. Suojelupoliisin toimivaltuusvajeista osa voidaan täyttää yhdessä muun poliisin kanssa, osaa taas pitää tarkastella muussa

yhteydessä, kun kyse on esim. strategisten ilmiö- ja uhka-arvioiden tekemisestä. Poliisin rikosprosessuaaliset tarpeet saadaan täytettyä suurilta osin todennäköisesti jatkamalla esitutkinta- ja pakkokeinotoimikunnan työtä, puolustusvoimien tai siviilitiedustelun tarpeiden täyttymiseen tarvitaan todennäköisimmin perustuslain muuttamista.

Esitutkintaviranomaisten tarpeet tietoverkoissa tapahtuvan tiedonhankinnan tehostamiseksi voitaisiin tyydyttää perustuslain 10 §:n lakivarauksen puitteissa pysyen tarkastelemalla asiaa normaalissa rikosprosessuaalisessa säädösvalmistelujärjestyksessä. Tällöin tarkasteluun tulisi muun muassa rikosten tunnusmerkistöt ja niiden valmistelutekojen kriminalisoinnit. Yhteiskunnan turvallisuutta vaarantavien rikosten kriminalisointia voitaisiin kenties laajentaa terrorismirikosten tapaan. Joissakin valmistelurikoksissa on kriminalisoitu suunnittelu, rekrytoiminen ja vastaavat toimet, toisissa taas edellytetään konkreettisia tekoja, kuten erilaisten tavaroiden tai aseiden hankintaa taikka vastaavia toimia. On ilmeistä, että tällä tavoin voitaisiin lakivarauksen puitteissa pysyen turvata rikosperusteinen tiedonsaanti niissäkin tilanteissa, joissa epäilty rikos ei vielä kohdennu tiettyyn henkilöön (tuntematon uhka), mutta jossa alkuvaiheessa olevan rikoksen suunnittelusta tai vastaavasta alkuteosta on sellaista näyttöä, että tiedonhankintaan voitaisiin antaa lupa.

Verkkovalvontaa voitaisiin käyttää ylitörkeisiin rikoksiin. Mietinnössä oleva kahdeksankohtainen luettelo, joka vastaa Ruotsin FRA-lain vastaavaa kohtaa, sisältää elementtejä, joihin Poliisihallituksella ei sinällään ole huomautettavaa, mutta samalla on kuitenkin todettava, ettei tämä luettelo ole riittävä, sillä se ei mm. näyttäisi mahdollistavan esim. kouluampumisten tai Breivik -tyyppisten tekojen torjumista verkkovalvonnan keinoin. Niin ikään julkisuudessakin esillä ollut Helsingin yliopistoon suunnattu suunniteltu isku jäisi verkkovalvonnan ulkopuolelle. Kuitenkin luettelon mukaan esimerkiksi meidän Afganistanin operaatioomme kohdistuva mikä tahansa uhka olisi suurempi yhteiskunnallinen ongelma kuin vaikka edellä mainittu yliopistoisku. Täten tätä luetteloa tulee tarkasti miettiä uudelleen ja saattaa se sellaiseksi, jossa myös yhteiskuntamme edellä mainitut uhat on otettu huomioon. Muotoilu voisi tässä luettelossa olla kohtuullisen yleinen ottaen huomioon, että tässä perusoikeusherkkyydestään huolimatta on kyse hyvin harvoin käytettävästä tiedustelutiedosta, jolla sinällään ei ole suoria oikeusvaikutuksia.

Verkkovalvonnassa voi tulla eteen tilanteita, joiden yhteydessä tulee tietoon suunnittelu-, valmistelu- tai toteutusvaiheessa olevia rikokseksi arvioitavia tekoja, joiden täytäntöönpanoon ei vielä ole ryhdytty tai joissa jo aloitetun toiminnan seuraus olisi estettävissä. Rikoslain 15 luvun 10 §:ssä säädetään törkeän rikoksen ilmoittamatta jättämisestä. Mainitussa pykälässä on lueteltu varsin iso määrä erityyppisiä tekoja, joista on yksiselitteinen velvollisuus ilmoittaa viranomaiselle tai sille, jota vaara uhkaa. Ilmoitusvelvollisuus koskee kaikkia. Ei ole ajateltavissa, ettei mainittu ilmoittamisvelvollisuus tulisi koskemaan myös niitä henkilöitä, jotka mahdollisesti tulevaisuudessa toimivat verkkovalvontatehtävissä.

Monet rikoslain 15 luvun 10 §:ssä mainituista rikoksista ovat sellaisia, että ne voivat koskea kansallista turvallisuutta. Pykälässä mainittujen rikosten joukossa on myös puhtaasti yksilön henkeen ja terveyteen kohdistuvia ri-

koksia. Tiedon saaminen em. rikoksista muodostaa tiedon saaneelle taholle toimimisvelvollisuuden. Tämä asia on asia huomioitava mahdollisessa tulevassa verkkovalvontaa koskevassa lainvalmistelutyössä.

Jos verkkovalvonta tulee mahdolliseksi, valvontatietojen hyödyntämisen tulee olla mahdollista mm. kouluampumistapausten ja vastaavien muun tyyppisten joukkosurmien paljastamiseksi ja estämiseksi. Myös pommien valmistamisen (esim. case Myyrmanni) ja niiden avulla tehtyjen rikollisten tekojen paljastamiseksi ja estämiseksi tulisi pystyä hyödyntämään valvonnan avulla saatuja tietoja.

Kun verkkovalvonnan avulla sitten mahdollisesti saadaan riittäviä perusteita varsinaisille tiedonhankintakeinoille, on se täyttänyt sille asetetut tavoitteet. Ylimääräisen tiedon käyttämisen mahdollisuus tulisi lähtökohtaisesti tässä nimenomaisessa verkkovalvontaa koskevassa lainsäädännössä estää.

Asia on silti hyvin herkkä, koska kysymyksessä on puuttuminen kansalaisten perustuslaissa taattuun luottamuksellisen viestinnän suojaan ja rajanvetoa siitä, missä raja viranomaisten tiedonsaannin ja yksityisyyden suojan välillä kulkee. Samalla kun palvelut siirtyvät tietoverkkoihin, siirtyvät sinne valitettavasti myös uhat. Yhteiskunnan tulee turvata ihmisten, yritysten ja laajemminkin koko yhteiskunnan toimintaympäristö tietoverkoissa olevilta uhilta, mutta toisaalta myös viestinnän vapaus tulisi turvata. Järjestelmässä tulisi ottaa perusoikeudet huomioon, mutta kaikkia tulisi myös turvata niin sisäisen kuin ulkoisen turvallisuuden uhilta.

Tarpeellisuus ja tehokkuus

Poliisin kokemusten perusteella tutkinnan alkuvaiheessa ei ole aina heti selvää, onko tietoverkkoa käyttäen tehdyn teon takana yksityinen tai valtiollinen toimija, eikä myöskään se, mikä on teon perimmäinen tarkoitus ja tavoite. Tietoverkkorikosten esitutkinnassa kertyneen kokemuksen perusteella on havaittu, että joissain tapauksissa verkkolaitteiden ohjaustietojen virheelliset päivitykset ovat generoineet sellaista verkkoliikennettä, joka on kohdeorganisaatiossa tulkittu hyökkäysliikenteeksi. Samoin on esitutkinnan yhteydessä tehty joitakin havaintoja siitä, että asianomistajaorganisaatiot eivät ole kyenneet tunnistamaan omassa verkkovalvonnassaan koko organisaationsa kaikkien eri liitännäisosien tuottamaa verkkoliikennettä. Kyseistä verkkoliikennettä on pidetty aluksi epäiltävänä, vaikka sittemmin sille on löytynyt luonnollinen selitys. Näiden kokemusten ja havaintojen perusteella voidaan arvioida, että verkkovalvonnassa kohteeksi voi joutua aiheettomasti. Kaikki epäilyttäväksi arvioitu verkkoliikenne ei sitä välttämättä ole. Verkkovalvonnan tarpeellisuutta ja tehokkuutta arvioitaessa aiheettomaksi osoittautuneen toteutuneen valvonnan määrä tulee ottaa huomioon.

Ohjaus ja valvonta

Viime kädessä verkkovalvontaluvan antavan elimien tulee voida em. mainitun luettelon perusteella arvioida, onko luvan antamiselle perusteita. Kyse on tiedustelutoiminnasta; etsitään tuntematonta uhkaa niillä perustein, joita tuossa vaiheessa on käytettävissä. Poliisihallituksen näkemyksen mukaan tiedonhankintaa (verkkovalvontaa) koskeva lupamenettely tulisi ohjata Helsingin käräjäoikeuteen, jonne on jo keskitetty tiettyjen salaisten tiedonhan-

kintakeinojen lupaharkinta. Kyseisellä tuomioistuimella on jo asian edellyttämää vastaavaa kokemusta.

Poliisihallituksen näkemyksen mukaan on tarkoituksenmukaista, että tietoliikennetiedustelun tekninen toteuttaminen keskitetään mietinnön esityksen mukaisesti yhdelle viranomaiselle. Varsinainen tiedustelutoiminta tulisi keskittää valtakunnallisesti yhteen paikkaan. Tiedustelutoiminnan yhteydessä kerätyn tiedon tulee olla tarpeen mukaan kaikkien turvallisuusviranomaisten käytettävissä. Keskittäminen olisi järkevää kustannustehokkuuden ja osaamisen keskittymisen näkökulmasta.

Poliisihallitus on yhteistyössä sisäministeriön kanssa aloittanut jo toimenpiteet poliisin ja muiden lainvalvontaviranomaisten tietoverkoissa tapahtuvan rikosperusteisen tiedonhankinnan säädösperustan selvittämiseksi. Siinä tapauksessa, että tämän joka tapauksessa tarpeellisen hankkeen lisäksi myös mietinnössä ehdotettu massavalvontainen verkkotiedusteluhanke toteutetaan, on tarkoin arvioitava sitä, mikä viranomainen tai millainen moniviranomaisyhdistelmä ja -toiminta voisi siitä vastata, kun kuitenkaan siviilitietoliikennettä ja sotilastietoliikennettä ei voida käytännössä erottaa. Poliisihallituksen käsityksen mukaan ei ole valtiosääntöoikeudellisestikaan pidettävä mitenkään itsestään selvänä, että esim. puolustusvoimat voisi ainakaan yksin suorittaa siviilien viestiliikenteeseen kohdistuvaa valvontaa.

Oleellista on, että toiminnon ohjaus toteutetaan moniviranomaismallin mukaisesti, ja että toiminnolla on toiminnan luonteen mukaan määräytyvät laillisuusvalvontajärjestelyt. Puolustusvoimien ja poliisin toiminta tulee järjestää saumattomaksi, ja tämän yhteistyön sekä rikosten tutkinnan turvaamiseksi on lisäksi tarkoituksenmukaista, että mahdollisen tulevan tiedustelukeskusten henkilökunta koostuu paitsi puolustusvoimien myös poliisin viranhaltijoista. Yhteisiä valvonta- ja ohjausrakenteita tulee miettiä tarkoin. Poliisi haluaa olla näissä rakenteissa vahvasti mukana, osaksi jo siitäkin syystä, että sillä on pitkä kokemus toimimisesta hyvin perusoikeusherkällä alueella.

Mietinnön esitykset monitasoisesta ja jopa moninkertaisesta ulkoisesta valvonnasta ovat kannatettavia. Muistiossa kuvattu tiedonhankinta tietoverkoista (verkkovalvonta) on luonteeltaan toimintaa, jossa puututaan syvästi kansalaisten perustuslaissa taattuun luottamuksellisen viestinnän suojaan. Tämän tyyppisessä valvonnassa valvonnan kohteeksi joutuneen henkilön oikeussuojakeinoista on huolehdittava.

Oikeuteen antaa verkkovalvontaviranomaiselle toimeksiantoja kytkeytyy tiedusteluviranomaisten ohjaukseen. Poliisihallituksen käsityksen mukaan poliittinen ohjaus toteutuu sen mukaan kuin asiasta on muualla säädetty, mutta varsinaisia toimeksiantoja voisivat antaa puolustusvoimat, Suojelupoliisi ja Keskusrikospoliisi.

Lopuksi

Verkkovalvonnan ei missään nimessä tule olla mikään jokapäiväisen tietoverkkorikostutkinnan työväline, mutta sitä tulee voida käyttää vakavien yhteiskunnan turvallisuutta uhkaavien tekojen paljastamisessa.

Mietinnössä ja Poliisihallituksen lausunnossa tulee esille se, että verkkovalvontaa ei voi lokeroida vain yhdeksi asiaksi ja käsitteeksi. Verkkovalvonnassa on selkeästi eri tarpeet poliisilla rikosprosessuaaliselta näkökannalta, puolustusvoimilla sotilastoiminnan osalta sekä tiedustelun, erityisesti siviilitiedustelun, osalta. Nämä erilaiset tarpeet ja ratkaisuvaihtoehdot tulisi jatkotyöskentelyssä ja hankkeissa tulla ottaa huomioon. Mahdollisten tulevien säädösten valmistelu- ja esittelyvastuut toteutunevat valtioneuvoston normaalin toimialajaon mukaisesti.

Poliisiylijohtaja Mikko Paatero

Poliisiylitarkastaja Niina Uskali

Asiakirja on sähköisesti allekirjoitettu Aspo-asianhallintajärjestelmässä. Poliisihallitus 07.04.2015 klo 12.52. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Tiedoksi Poliisilaitokset
Poliisihallituksen poliisitoimintayksikkö