Amnesty International Suomen osasto

Lausunto

16.06.2017 AI FI 25/2017

Asia: SMDno-2015-1509; SM047:00/2015

Ehdotus siviilitiedustelua koskevaksi lainsäädännöksi; työryhmän mietintö 8/2017

Lausunnonantajan lausunto

Voitte kirjoittaa lausuntonne alla olevaan tekstikenttään

Sisäministeriölle

AI FI 25/2017

16.6.2017

Lausunto siviilitiedustelakityöryhmän mietinnöstä (ehdotukset siviilitiedustelulainsäädännöksi)

Amnesty International on maailman suurin ihmisoikeusjärjestö, jonka toiminta perustuu yksittäisten ihmisten tuelle. Tukijoita on yli 7 miljoonaa, 150 maassa eri puolilla maailmaa. Amnesty on poliittisesti ja uskonnollisesti sitoutumaton. Amnesty työskentelee kansainvälisesti muun muassa yksityisyyden suojan sekä sananvapauden puolesta ja verkossa tapahtuvia ihmisoikeusloukkauksia vastaan. Amnesty seuraa myös Suomessa vireillä olevia tiedustelulakihankkeita.

Amnesty International Suomen osasto kiittää mahdollisuudesta lausua otsikon asiassa ja lausuu kunnioittavasti seuraavaa:

Lausuttavana oleva mietintö on osa suomalaista tiedustelulainsäädäntöä koskevaa laajaa ja sirpaleista valmistelukokonaisuutta, ja sitä on luettava yhdessä aiemmin julkaistujen mietintöjen kanssa. Näitä ovat perustuslain yksityisyydensuojapykälän muutosta ehdottaneen työryhmän, sotilastiedustelulainsäädäntöä valmistelleen työryhmän ja tiedustelutoiminnan valvontaa valmistelleen työryhmän mietinnöt.

Hallituksen esityksen luonnokseksi kirjoitetussa mietinnössä ehdotetaan suojelupoliisin käyttöön uusia laajamittaisia tiedustelutoimivaltuuksia. Nämä toteutettaisiin säätämällä uusi laki tietoliikennetiedustelusta siviilitiedustelussa sekä muuttamalla polisiilakia niin, että siihen lisättäisiin uusi 5 a luku, jossa säädettäisiin muista tiedustelumenetelmistä ja niiden käytöstä siviilitiedustelussa.

Lisäksi esityksessä ehdotetaan muutettavaksi lakia poliisin hallinnosta, lakia henkilötietojen käsittelystä poliisitoimessa, esitutkintalakia, pakkokeinolakia ja lakia oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa. Suojelupoliisin tiedustelullisten toimivaltuuksien lisääntymisen myötä sen esitutkinta- ja pakkokeinotoimivaltuudet ehdotetaan poistettavaksi oikeudenmukaisen oikeudenkäynnin turvaamiseksi. Suojelupoliisilla olisi kuitenkin mahdollisuus osallistua esitutkintaan asiantuntijaviranomaisen ominaisuudessa. Tiedustelutietoa voitaisiin myös tietyin edellytyksin luovuttaa esitutkintaviranomaiselle tai muulle toimivaltaiselle viranomaiselle.

Esityksen tavoitteena on kansallisen turvallisuuden parantaminen ja säädöspohjan luominen suomalaiselle tiedustelulle. Tavoitteena on parantaa suomalaisen yhteiskunnan mahdollisuuksia suojautua kansalliseen turvallisuuteen kohdistuvilta vakavilta uhkilta, kuten terrorismilta, vieraiden valtioiden Suomeen kohdistamalta vakoilulta, joukkotuhoaseilta ja yhteiskunnan elintärkeisiin toimintoihin kohdistuvilta uhkilta.

Tietoliikennetiedustelun teknisestä toteuttamisesta ei säädetä lausuttavana olevassa esityksessä, vaan sotilastiedustelua koskevaan mietintöön sisältyvässä ehdotuksessa laiksi sotilastiedustelusta.

Tiedustelutoiminnan hyväksyttävyydelle perus- ja ihmisoikeuksien näkökulmasta kriittisen tärkeästä tiedustelutoiminnan riippumattomasta valvonnasta säädetään myös erikseen, tätä koskevassa erillisessä mietinnössä.

Amnestyn kanta viestintään kohdistuvaan tiedusteluun

Digitaalinen kehitys on merkinnyt rajattomia mahdollisuuksia, mutta myös uudenlaisia uhkia muun muassa yksilön oikeuksille. Vaadittaessa uusia tiedusteluvaltuuksia on yleisesti vedottu siihen, että teknologinen kehitys on saattanut rikollisten tai kansallista turvallisuutta uhkaavien tahojen

toimintaa viranomaisten perinteisten keinojen ulottumattomiin. Totuus on kuitenkin myös, että ihmiselämän siirtyminen verkkoon on mahdollistanut yksilön yksityisyyden alaan puuttumisen entistä läpitunkevammin, helpommin ja halvemmalla. Valtioiden harjoittama yksityiseen viestintään kohdistuva tiedustelutoiminta merkitsee syvälle käyvää puuttumista useiden perus- ja ihmisoikeuksien alaan, erityisesti yksityisyyden suojaan, mukaan lukien luottamuksellisen viestinnän ja henkilötietojen suojaan, sekä potentiaalisesti esimerkiksi sananvapauteen.

Amnesty katsoo, että viestintään kohdistuva tiedustelu voi olla ihmisoikeusnäkökulmasta hyväksyttävää tiettyjen tiukkojen edellytysten täyttyessä. Amnesty vastustaa viestinnän laajalle ulottuvaa ja massamittaista tarkkailua, kaappaamista, keräämistä, varastointia tai analysointia, jota ei ole kohdistettu tiettyyn yksilöön, ryhmittymään tai sijaintiin ja joka ei pohjaudu perusteltuun epäilyyn. Tällainen kohdentamaton ”massavalvonta” loukkaa suhteettomasti yksilön yksityisyyden suojaa ja sananvapautta, eikä voi olla hyväksyttävissä perus- ja ihmisoikeuksien valossa.

Viestintään kohdistuva tiedustelu voi olla hyväksyttävää vain, mikäli se on riittävän kohdennettua, pohjautuu perusteltuun epäilyyn ja on ehdottoman tarpeellista hyväksytyn päämäärän saavuttamiseksi. Tiedustelun tulee olla oikeasuhtaista tavoitteeseensa nähden. Tiedustelumenetelmien kohdentaminen ei saa olla syrjivää eli perustua ilman hyväksyttävää syytä esimerkiksi kohdehenkilön alkuperään, uskontoon, mielipiteeseen, yhteiskunnalliseen ryhmään kuulumiseen tai muuhun henkilöön liittyvään syyhyn. Tiedustelutoiminnasta on säädettävä täsmällisesti ja tarkkarajaisesti lailla. Tiedustelutoimenpiteisiin tulee olla tuomioistuimen tai muun ulkopuolisen viranomaisen lupa, ja tiedustelua toteuttavaa viranomaista tulee valvoa tehokkaasti. Vastaavat kriteerit tiedustelun hyväksyttävyydelle ovat johdettavissa niin keskeisistä kansainvälisistä ihmisoikeussopimuksista ja niissä turvattujen oikeuksien rajoittamista koskevista periaatteista, kuin kotimaisessa valtiosääntöperinteessä sovelletuista perusoikeuksien yleisistä rajoitusedellytyksistä.

Perus- ja ihmisoikeuksien rajoitusedellytyksistä: tehokkuusvaatimus

Aiemmassa, erillisessä mietinnössä on esitetty perustuslain yksityisyyden suojaa koskevan 10 §:n sisältämän kvalifioidun lakivarauksen laajentamista. Tältä taustalta nyt lausuttavassa esityksessä ehdotetaan useita toimivaltuuksia, jotka olisivat ilmeisessä ristiriidassa voimassa olevan perustuslain kanssa. Perustuslain 10 §:n nykyisen tai muutettavan sanamuodon ohella yksityisyysperusoikeuden rajoittamisen hyväksyttävyyttä ja siten nyt ehdotettavien keinojen perustuslainmukaisuutta on arvioitava myös kotimaisessa valtiosääntödoktriinissa ja perustuslakivaliokunnan käytännössä vakiintuneiden perusoikeuksien yleisten rajoitusedellytysten kannalta. Näiden mukaan ylipäänsä rajoitettavissa olevien perusoikeuksien alaan kajoamisen edellytyksiä ovat vaatimukset lailla säätämisestä, lain täsmällisyydestä ja tarkkarajaisuudesta, rajoituksen hyväksyttävyydestä, rajoituksen suhteellisuudesta, perusoikeuden ydinalueen koskemattomuudesta, oikeusturvajärjestelyjen riittävyydestä ja ihmisoikeusvelvoitteiden noudattamisesta.

Kotimaisen perustuslain ohella yksityisyyden alaan korostuneesti pureutuvien viestintään kohdistuvien tiedustelumenetelmien hyväksyttävyyttä on arvioitava myös Suomen hyväksymien kansainvälisten ihmisoikeusvelvoitteiden kannalta. Lausuttavana olevassa mietinnössä onkin pyritty jonkin verran esittelemään kansainvälisten ihmisoikeussopimusten yleisiä ja nimenomaisesti yksityisyyden suojaa koskevia rajoitusperusteita.

Huomionarvoista on, että sekä kotimaisista perusoikeuksien yleisistä rajoitusedellytyksistä että esimerkiksi Euroopan ihmisoikeussopimuksesta ja Euroopan ihmioikeustuomioistuimen käytännöstä johdettavat vaatimukset rajoituksen välttämättömyydestä hyväksyttävän tavoitteen toteuttamiseksi pitävät sisällään myös edellytyksen siitä, että laissa valitut keinot ovat tosiasiallisesti tehokkaita niillä tavoitellun hyväksyttävän päämäärän saavuttamiseksi, kuten kansallisen turvallisuuden suojelemiseksi tai nimenomaisemmin esimerkiksi terrorismin ehkäisemiseksi. Tältä osin on ongelmallista, että lausuttavana olevien lakiehdotusten perusteluissa, sen enempää kuin jo aiemmin lausuntokierroksella käyneessä perustuslain muutosta ehdottaneessa esityksessä, ei ole juurikaan käsitelty varsinkaan tietoliikennetiedustelun tehokkuutta keinona puuttua vakaviin kansallisen turvallisuuden uhkiin, kuten terrorismiin.

Ylipäänsä kansainvälisesti vaikuttaisi ainakin julkisista lähteistä olevan saatavissa melko vähän näyttöä sille, että laajamittaisella verkkovalvonnalla – perinteisempien poliisitoiminnan keinojen sijaan – olisi esimerkiksi onnistuttu ehkäisemään terrori-iskuja. Esimerkiksi salausteknologioiden valtavirtaistuminen ja verkkotiedustelun kohdeaineiston potentiaalisesti valtaisa koko saattaavat vaikuttaa toiminnan tehokkuuteen. Myös hakuehtojen määrittely käytännössä asettanee valtavia haasteita. Hakuehtojen epätäsmällisyys tai liiallinen täsmällisyys saattavat johtaa joko valtaisan laajamittaisen sivullisten viestinnän joutumiseen valvonnan kohteeksi tai vaihtoehtoisesti potentiaalistenkin kohdehenkilöiden rajautumiseen hakutulosten ulkopuolelle.

Tiedustelutoiminta on luonteeltaan lähtökohtaisesti salaista, ja tiedusteluviranomaisilla on perusteltuja syitä muun muassa menetelmiensä salailuun. Myös esimerkiksi tietojenvaihto muiden maiden viranomaisten kanssa saattaa edellyttää salailua. Ihmisoikeusnäkökulmasta jonkinlaisen näytön toivottujen tiedustelukeinojen tehokkuudesta tulisi kuitenkin olla lähtökohtainen ja selkeä edellytys niiden säätämisen hyväksyttävyydelle. Onkin ehdottoman toivottavaa, että viimeistään eduskunta vaatii konkreettista näyttöä valitun kaltaisten tiedustelumenetelmien osoitetusta tehosta vertailukelpoisissa valtioissa.

Tietoliikennetiedustelu

Tietoliikennetiedustelu olisi Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä.

Tietoliikennetiedustelulla saataisiin hankkia tietoja kansallista turvallisuutta vakavasti uhkaavista toiminnoista. sellaisiksi määriteltäisiin terrorismi, ulkomainen tiedustelutoiminta, valtio- tai yhteiskuntajärjestystä uhkaava toiminta, joukkotuhoaseet, kaksikäyttötuotteiden kansallista turvallisuutta vakavasti uhkaava leviäminen, suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta, vieraan valtion suunnitelma tai toiminta, joka voi aiheuttaa vahinkoa ulko- tai turvallisuuspolitiikalle taikka kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille, kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi, kansainvälistä kriisinhallintaoperaatiota uhkaava toiminta tai kansallista turvallisuutta vakavasti uhkaava kansainvälinen järjestäytynyt rikollisuus.

Kansallista turvallisuutta vakavasti uhkaavia toimintoja määrittelevä listaus on tyhjentävä ja vain siinä tarkoitettuja toimintoja voidaan käyttää tietoliikennetiedustelun lupahakemukseen kirjattavana kohteena. Listaus on kuitenkin niin laaja, epämääräinen ja tulkinnanvarainen, että jää käytännössä täysin tuomioistuinten päätöksenteon ja hakemuskäytännön varaan, minkälaisista uhkista tietoliikennetiedustelulla tullaan keräämään tietoa. Jokaista kohdelistauksen kohtaa on pyritty avaamaan esityksen yksityiskohtaisissa perusteluissa. Silti voidaan aiheellisesti kyseenalaistaa, onko esimerkiksi taloudellisia ”tai muita tärkeitä etuja” uhkaava toiminta syytä määritellä kansallista turvallisuutta vakavasti uhkaavaksi toiminnoksi, tai voisiko kansainvälinen järjestäytynyt rikollisuus vakavasti uhata kansallista turvallisuutta.

Mahdollisksi kansallisen turvallisuuden vakaviksi uhiksi listatut toiminnot ovat myös monelta osin samoja, joita ehdotetaan säädettäväksi sotilastiedustelun kohteiksi sitä koskevassa erillisessä mietinnössä. Tämä hämärtää osaltaan rajanvetoa siviili- ja sotilastiedusteluviranomaisten työnjaossa. Lähtökohta kuitenkin lienee, että sotilastiedustelu valvoo valtiollisia, sotilaallisia uhkia, ja siviilitiedustelu siviililuonteisia, ei-sotilaallisia uhkia.

Listaus vaikuttaisi joka tapauksessa mahdollistavan suojelupoliisin harjoittaman jatkuvankin valvontatoiminnan hyvin moninaisten uhkien seuraamiseksi. Esityksen perusteluissa todetaankin, että niin tietoliikennetiedustelua kuin muita tiedustelumenetelmiä voitaisiin käyttää ylipäätään Suomeen kohdistuvien ulkoisten uhkien kartoittamiseksi, esimerkiksi turvallisuusympäristön kehityksen seuraamiseksi ja kansalliseen turvallisuuteen kohdistuvan tilannekuvan muodostamiseksi. Perustelujen mukaan kansallista turvallisuutta vakavasti uhkaava toiminta voi olla myös toimintaa, joka ei ole Suomen lain mukaan rikos eikä voisi sellaiseksi muodostua edes toteutumisen asteelle edetessään. Maininta vaikuttaa epämääräiseltä, ja on vaikea nähdä, mitä tällainen, toiminta voisi käytännössä olla.

Vaikka kunkin menetelmän kohdalla säädettäisiin erikseen päätöksen voimassaoloajasta, mahdollista olisi perustelujen mukaan jatkuvakin tiedonhankinta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tiedonhankintaa ei olisi rajoitettu ajallisesti, sillä tiedustelun kohteena olevaa toimintaa on usein tarpeen seurata pitkäjänteisesti ja systemaattisesti. Perustelujen mukaan

seurattavan toiminnan ei itseasiassa välttämättä tarvitsisi olla edes välittömästi uhkaavaa seurannan aikana. (s. 186).

Nämä tiedustelutoiminnan laajuutta, kohdentamista ja kestoa koskevat seikat herättävät vakavia kysymyksiä kaavaillun toiminnan suhteesta ihmisoikeusnäkökulmasta tuomittavaan kohdentamattomaan massavalvontaan. Välttämättömässä tilanteessa poikkeuksellisesti käytettävien keinojen sijaan perustelut viittaavatkin jatkuvaan, laajamittaiseen ja hyvin moninaisiin uhkakuviin suuntautuvaan valvontaan. On myös aiheellista kysyä, millaisia resursseja tällainen jatkuva, laajamittainen uhkien seulonta edellyttää, ja onko tällöin resurssien käyttö juuri tällaisiin tiedustelumenetelmiin järkevintä ja tehokkainta mahdollista suomalaisten turvallisuuden suojelemisen kannalta.

Tietoliikennetiedustelun tekninen toteuttaja olisi puolustusvoimien tiedustelulaitos ja sen teknisestä toteutuksesta säädettäisiin erillisen mietinnön ehdottamassa laissa sotilastiedustelusta. Kun tietoliikennetiedusteluun olisi saatu tuomioistuimen lupa, kytkennän luvanmukaiseen viestintäverkon osaan tekisi valtion omistama Suomen Erillisverkot Oy, mikä merkitsisi merkittävän julkisen vallan käytön siirtämistä muulle kuin viranomaiselle.

Kytkennän tekemisellä luvanmukaisessa viestintäverkon osassa kulkeva tietoliikenne ohjautuisi suodatukseen. Tämä viestintäverkon tietty osa, jossa kulkevaan tietoliikenteeseen tiettyjä hakuehtoja voitaisiin käyttää, määriteltäisiin tuomioistuimen lupapäätöksessä. Suomen Erillisverkot Oy luovuttaisi näin suodatetun tietoliikenteen puolustusvoimien tiedustelulaitokselle, joka peilaisi kyseisen tietoliikenteen virtaamaan hallinnoimansa teknisen tiedustelujärjestelmän läpi. Puolustusvoimien tiedustelulaitoksen tiedustelujärjestelmään olisi ennakkoon syötetty tuomioistuimen lupapäätöksessä hyväksytyt hakuehdot, ja järjestelmä vertaisi läpivirtaavaa tietoliikennettä automatisoidusti niihin. Puolustusvoimien tiedustelulaitos toimittaisi hakuehtoja vastaavan tietoliikenteen suojelupoliisille. Näin seulottua ja suojelupoliisille luovutettua tietoliikennettä saataisiin käsitellä sekä automaattisesti että manuaalisesti, ja suojelupoliisi saisi selvittää myös yksittäisten luottamuksellisten viestien sisällön.

Esityksen yksityiskohtaisissa perusteluissa viitataan mahdollisina hakuehtoina esimerkiksi sähköpostiosoitteisiin, käyttäjätunnuksiin, teleosoitteisiin ja ip-osoitealueisiin, mutta myös esimerkiksi tietyn salaustekniikan tai aakkosmerkistön käyttöön (s. 233).

Aikana, jolloin niin valtiollisten toimijoiden harjoittama verkon massavalvonta kuin esimerkiksi verkkorikollisuus luovat ennennäkemättömän vakavia uhkia yksityisyyden suojalle, Amnesty pitää erilaisten salaustekniikoiden käyttöä, leviämistä ja valtavirtaistumista perusteltuna, myönteisenä kannatettavana kehityksenä. Jokaisella on oikeus luottamukselliseen viestintään, mutta erityisen keskeistä viestinnän suojaaminen on esimerkiksi sellaisille sananvapaustilanteeltaan vaikeissa maissa toimiville ihmisoikeuspuolustajille, joiden kanssa muun muassa Amnesty ja muut ihmisoikeusjärjestöt työskentelevät.

Huomattavaa on myös positiivinen kehitys, jossa salausteknologiat ovat valtavirtaistuneet entistä paremmin myös suurten kaupallisten palveluiden piiriin ja tulleet näin yhä laajemmin tavallisten verkon, viestintäpalveluiden ja matkapuhelinten käyttäjien saataville. Tilanne, jossa salausteknologian käyttö itsessään saattaa käyttäjänsä viranomaisten epäilyksen alaiseksi ja on yhtenä tekijänä oikeuttamassa viestinnän luottamuksellisuuteen kajoamista, on hälyttävä. Toinen esimerkkinä mainittu mahdollinen hakuehto, tietyn aakkosmerkistön käyttö, taas tarkoittaa käytännössä tietyllä kielellä kommunikoivien henkilöiden viestinnän luottamuksellisuuden murtamista.Tämä voi herkästi johtaa valvonnan kohdehenkilöiden syrjivään valikoitumiseen.

Lupahakemuksessa ja tuomioistuimen myöntämässä luvassa mainitut, suodatuksessa käytettävät hakuehdot olisivat pelkästään vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenteeseen kohdistuvaa tiedustelua tai haittaohjelmia koskevia hakuehtoja lukuunottamatta muita kuin viestin sisältöä kuvaavia. Lupapäätöksessä voitaisiin hyväksyä paitsi yksittäisiä hakuehtoja, myös hakuehtojen luokkia, jonka pohjalta suojelupoliisin sallittaisiin itse muodostaa hakuehdot. Ennakkoon määrättyjen hakuehtojen ohella voitaisiin tällöin käyttää kansallista turvallisuutta vaarantavan toiminnan sanallisia kuvailuja, jotka mahdollisimman konkreettisesti luonnehtisivat kohdetta. Sanallisen kuvailun kohteena voisivat olla viestinnälliset ja muut toimintamallit, joiden tiedetään tai voidaan olettaa liittyvän kansallista turvallisuutta vaarantavaan toimintaan.

Hakuehtojen luokka olisi tarkkarajainen sanallinen kuvaus tiedustelukysymyksen kannalta relevanteista hakuehdoista tilanteessa, jossa samaan selkeään kokonaisuuteen kuuluu joukko keskenään samantyyppisiä hakuehtoja, joista vain osa on tietoliikennetiedustelun käynnistyessä tiedossa. Yksityiskohtaisten perustelujen mukaan hakuehtojen luokka mahdollistaisi sen, että tietoliikennetiedustelulla saadun uuden tiedon myötä ei tarvitsisi käynnistää uutta lupamenettelyä hakuehtojen hyväksymiseksi. Uuden tiedon perusteella tarkoituksenmukaisiksi osoittautuvat uudet yksittäiset hakuehdot kuuluisivat jo aiemmin haetun luvan piiriin. Hakuehtojen luokka voisi liittyä esimerkiksi yksilöitävään henkilöryhmään, kuten terroristiryhmään tai vieraan valtion organisaatiossa työskenteleviin henkilöihin, viestiyhteyksien kuvaukseen, tai tietoliikenneyhteyksiin tietyn yksilöidyn, riittävän suppean maantieteellisen alueen ja Suomen välillä (s. 239).

Tietoliikennetiedustelulla saadun tiedon hahmotellaan esityksessä toimivan syötteenä poliisilain 5 a luvun tiedustelumenetelmien, eli käytännössä käyttöalaltaan dramaattisesti laajennettavien poliisilain salaisten tiedonhankintakeinojen ja parin uuden keinovaihtoehdon käytölle. Tietoliikennetiedustelulla pyrittäisiin siis kartoittamaan potentiaalisia kohteita kohdennetumpien keinojen käyttämiseksi edellytettävällä tarkkuudella.

Ehdotettu poliisilain 5 a luku tiedustelumenetelmistä

Poliisilakiin ehdotetaan lisättäväksi uusi 5 a luku suojelupoliisin muista tiedustelumenetelmistä kuin tietoliikennetiedustelusta. Ehdotetut tiedustelumenetelmät perustuisivat menetelmällisesti ja määritelmällisesti pääosin poliisilain 5 luvun nykyisiin salaisiin tiedonhankintakeinoihin. Näiden lisäksi tiedustelumenetelmiksi ehdotettaisiin nykyisiin poliisin käytössä oleviin keinoihin nähden uusina välineinä paikkatiedustelua, jäljentämistä ja lähetyksen pysäyttämistä jäljentämistä varten sekä erillisessä laissa säänneltävää, edellä kuvattua tietoliikennetiedustelua.

Poliisilain tiedustelumenetelmien käytön perusteena olevat kansallisen turvallisuuden vakavat uhat, joista suojelupoliisi saisi luvussa tarkoitetuilla menetelmillä hankkia tietoja, olisivat samat kuin ehdotetussa tietoliikennetiedustelua koskevassa laissa. Esityksen mukaan ajatuksena olisi, että tietoliikennetiedustelulla saatu, ennestään tuntemattomista uhkista kerätty tieto toimisi syötteenä poliisilain mukaisten tiedustelumenetelmien käytölle ja kohdentamiselle.

Nykyisiin poliisilain salaisiin tiedonhankintakeinoihin menetelmällisesti perustuvaa tiedustelua voidaan pitää ainakin jossain määrin kohdistettuna tiedustelutoimintana, ja siten perus- ja ihmisoikeuksien rajoittamisen näkökulmasta esimerkiksi laajamittaista verkkovalvontaa matalammalla kynnyksellä hyväksyttävinä keinoina. Kuitenkin myös näiden menetelmien osalta esityksessä ongelmallisesti hyväksytään, että menetelmiä voidaan käyttää, vaikkeivät kohdehenkilöt olisi tiedossa. Henkilöihin kohdennettuinakin tällaiset menetelmät, kuten viestintään kohdistuva telekuuntelu ja televalvonta, voivat kajota toiminnan tarkoitukseen nähden täysin sivullisten henkilöiden luottamuksellisen viestinnän alaan. Keinot joka tapauksessa kohdistuvat täysin olennaisesti suppeampaan henkilöpiiriin kuin tietoliikennetiedustelu eli verkkovalvonta.

Jo nykylain mahdollistamat salaiset tiedonhankintakeinot mahdollistavat esimerkiksi suunniteltuihin terroristisiin tekoihin puuttumisen ennen tällaisten vakavien rikosten toteutumista. Amnesty onkin tiedustelulakihankkeiden aikana painottanut suojelupoliisin käytössä jo nykyisin olevia salaisia tiedonhankintakeinoja, jotka on verkkovalvontavaltuuksien tarpeesta käydyssä julkisessa keskustelussa pitkälti sivuutettu.

Poliisilain nykyisessä 5 luvussa säädettyjä salaisia tiedonhankintakeinoja voidaan käyttää eräiden vakavien rikosten estämiseksi ja paljastamiseksi. Rikoksen estämisellä tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa. Salaisen tiedonhankintakeinon käytön yleisenä edellytyksenä on, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja.

Salaisten tiedonhankintakeinojen käyttö on nykyisin sidottu tiettyihin rikosnimikkeisiin. Niillä puututaan rikoksen valmisteluun, eikä käyttö edellytä, että kyseisten rikosten valmistelu olisi erikseen kriminalisoitu. Nykyisten salaisten tiedonhankintakeinojen kohteena oleva henkilö tulee

pystyä yksilöimään vähintään henkilön roolin tai tehtävän kautta, vaikka hän olisikin poliisille vielä henkilöllisyydeltään tuntematon. Telekuuntelu tai televalvonta voidaan kohdistaa myös tuntemattomaan henkilöön esimerkiksi IP-osoitteen tai IMEI-koodin perusteella.

Poliisilain 5 a lukuun nyt ehdotettujen, nimenomaan suojelupoliisin käyttöön tarkoitettujen uusien tiedustelutoimivaltuuksien käyttöperusteet olisi kuitenkin niiden perustana olevista nykyisistä salaisista tiedonhankintakeinoista poiketen irrotettu rikos- ja henkilöperustaisuudesta. Keinoja voitaisiin käyttää silloinkin, kun toiminnan perustana olevassa uhkassa on kyse on toiminnasta, joka ei ole Suomen lain mukaan rikos eikä voisi sellaiseksi muodostuakaan.

Alun perin tapahtuneiden rikosten tutkintaa varten pakkokeinolakiin säädettyjä salaisia pakkokeinoja on vuosien saatossa laajennettu uusin keinoin, minkä lisäksi samat keinot on ulotettu käytettäväksi myös vielä toteutumattomien rikosten estämiseksi poliisilakiin säädetyillä salaisten tiedonhankintakeinojen toimivaltuuksilla. Nyt samojen keinojen käyttöalaa ollaan siis jälleen merkittävästi laajentamassa, irrottamalla niiden käyttöedellytys nyt täysin rikoksen käsitteestä. Esimerkiksi poliisin ylijohdon tehtävissä sisäministeriön poliisiosastolla ja Poliisihallituksessa toiminut Arto Hankilanoja on osuvasti kuvannut salaisen tiedonhankinnan ”porttiteoriaa”: ”poliisille säädetty uusi salaisen tiedonhankinnan toimivaltuus johtaa myöhemmin toimivaltuuden soveltamisalan laajentamiseen ja usein kokonaan uuteen toimivaltuuteen” (Poliisin salainen tiedonhankinta, Helsinki 2014, s. 144).

Tiedustelulakihankkeiden yhteydessä parin viime vuoden ajan käyty keskustelu on pyörinyt ennen kaikkea tietoliikennetiedustelua koskeneiden suunnitelmien ympärillä, joihin tässäkin keskitytään. Viimeistään eduskuntakäsittelyssä olisi tärkeää, että laajaa keskustelua käytäisiin myös muista nyt ehdotetuista tiedustelutoimivaltuuksista.

Poliisilain salaisiin tiedonhankintakeinoihin nähden täysin uusina tiedustelumenetelminä ehdotetaan poliisilain 5 a lukuun sisällytettäväksi säännökset paikkatiedustelusta, jäljentämisestä ja lähetyksen pysäyttämisestä jäljentämisen sijasta. Paikkatiedusteluvaltuuden nojalla suojelupoliisi voisi salaa tunkeutua muuhun kuin kotirauhan suojaamaan tilaan esineen, omaisuuden, asiakirjan, tiedon tai muun seikan löytämiseksi. Paikkatiedustelua voitaisiin suorittaa esimerkiksi työpaikoilla tai ajoneuvoissa. Suojelupoliisilla ei olisi velvollisuutta ilmoittaa paikkatiedustelusta tiedonhankinnan kohteelle, ellei asiassa olisi aloitettu esitutkintaa. Lähetyksen pysäyttäminen ja jäljentäminen taas mahdollistaisivat kirjeiden avaamisen ja lukemisen. Tämän luottamuksellisen viestinnän murtamisen malliesimerkin osalta ei ehdoteta lainkaan ilmoitusvelvollisuutta asianosaisille.

Tietoliikennetiedustelun lisäksi myös näiden uusien keinojen, samoin kuin vanhoista poliisilain salaisista tiedonhankintakeinoista tiedustelukeinoiksi laajennettujen muiden menetelmien käyttömahdollisuus merkitsee potentiaalisesti syvälle käyvää puuttumista perus- ja ihmisoikeuksien alaan Yksilöillä ei ilmoitusvelvollisuuden olemattomuuden vuoksi ole välttämättä käytössään minkäänlaisia oikeussuojakeinoja niiden haastamiseksi.

Tuomioistuinkontrolli ja oikeussuojakeinot

Tiedustelutoiminnan hyväksyttävyydelle perus- ja ihmisoikeuksien näkökulmasta on kriittisen tärkeää toiminnan tehokas valvonta. Tiedustelun parlamentaarisesta valvonnasta ja riippumattoman valvontaviranomaisen, tiedusteluvaltuutetun, perustamisesta säädetään erilliseen mietintöön sisältyvissä lakiehdotuksissa.

Parlamentaarisen valvonnan ja perustettavan valvontaviranomaisen suorittaman jälkikäteisvalvonnan ohella keskeisen tärkeässä roolissa tiedustelun lainmukaisuuden turvaamisessa on etukäteinen tuomioistuinkontrolli. Ehdotettu tietoliikennetiedustelaki lähteekin siitä itsestään selvästä lähtökohdasta, että tietoliikennetiedustelusta päättää tuomioistuin suojelupoliisin päällikön yksilöidystä, perustellusta hakemuksesta. Lain ehdotetun 9 §:n mukaan suojelupoliisin päällikkö saa kuitenkin kiiretilanteessa päättää tiedustelusta siihen asti, kunnes tuomioistuin on ratkaissut lupahakemuksen, mikäli asia ei siedä viivytystä. Tällöin asia on saatettava tuomioistuimen ratkaistavaksi heti kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tietoliikennetiedustelun alkamisesta.

Ehdotetussa kiiretilanteita koskevassa pykälätekstissä ei täsmennetä kiireellisen päätöksen tekemisen edellyttämää poikkeuksellisuutta ja välttämättömyyttä, joskin yksityiskohtaisissa perusteluissa tältä osin viitataan muun muassa Euroopan ihmisoikeustuomioistuimen ratkaisukäytännöstä ilmeneviin edellytyksiin.

Perustelujen mukaan tarve tietoliikenentiedustelun käyttämiseen voi joskus syntyä niin nopeasti, että luvan hakemisesta aiheutuva viivästys vakavasti vaarantaisi kansallisen turvallisuuden. Kyse voisi perustelujen mukaan olla esimerkiksi kansainväliseen terrorismiin liittyvästä välittömästä ja vakavasta uhkatilanteesta. Kyseessä voisi kuitenkin olla myös tilanne, jossa välitöntä uhkatilannetta ei sinänsä ole, mutta hakemuksesta aiheutuva viivästys johtaisi tietoliikennetiedustelulla saatavissa olevan aineiston menetykseen (s. 243).

Nämäkin perustelut vaikuttavat ajavan hahmoteltua valvontaa yhä kauemmaksi alun perin esitetystä, vain ehdottoman välttämättömään rajoitetusta, vakavien uhkien torjumiseksi tapahtuvasta, poikkeuksellisesta toiminnasta. Lakitekstin muotoilulla tulisi pyrkiä nyt esitettyä paremmin takaamaan se, että kiireellisestä menettelystä ei muodostu käytännössä vakiokäytäntöä tiedustelun aloittamisen yhteydessä, ja tuomioistuimen harjoittamaa tiedustelutoiminnan valtiosääntöoikeudellisen hyväksyttävyyden kannalta elintärkeää kontrollia ei näin tehdä tyhjäksi. On myös syytä harkita, eikö kiireellisissäkin tapauksissa tuomioistuimen päätöksenteko olisi mahdollista varmistaa ennen valvonnan aloittamista.

Tuomioistuimen harkintavaltaan ja tuomiostuinkäytännön varaan jää pitkälti se, mitä viranomaisen tekemältä tiedusteluhakemuksen perusteluilta ja tarkkuudelta sekä pyydettävien menetelmien välttämättömyydeltä ja oikeasuhtaisuudelta tullaan käytännössä vaatimaan. On sinänsä positiivista, että tiedustelulupien myöntämisestä vastaa yleinen tuomioistuin, eikä salainen tiedustelutuomioistuin tai muu täysin läpinäkymätön elin, kuten eräissä muissa maissa. Jotta tuomioistuimen harjoittama etukäteiskontrolli myös käytännössä muodostuu merkittäväksi tiedustelun rajojen kontrollikeinoksi eikä vain viranomaispäätökset kyseenalaistamatta sinetöiväksi kumileimasimeksi, on huolehdittava tuomareiden syvällisestä kouluttamisesta tiedustelun, kansallisen turvallisuuden ja yksityisyyden suojan erityiskysymyksiin.

Esimerkiksi nykyisin poliisilain salaisina tiedonhankintakeinoina ja pakkokeinolain salaisina pakkokeinoina mahdollisia telekuuntelua ja televalvontaa koskevassa lupakäytännössä ennakkokontrollia harjoittava tuomioistuin on pitkään hyväksynyt lähes kaikki poliisin esittämät vaatimukset näiden keinojen käytöstä. Pakkokeinolain mukaisiin telepakkokeinoihin lupia myönnettiin vuonna 2016 2 606 kappaletta ja vuonna 2015 3 110 kappaletta. Pakkokeinolain mukaisen telekuuntelun ja televalvonnan kohteena vuonna 2016 oli 471 henkilöä ja vuonna 2015 551 henkilöä. Poliisilain mukaisen televalvonnan kohteena oli vuonna 2016 64 henkilöä, ja 2015 87 henkilöä. Kaikista poliisin telepakkokeinohakemuksista hylättiin vuonna 2015 vain kahdeksan kappaletta, eikä määrässä oikeusasiamiehen kertomuksen mukaan tapahtunut viime vuonna mainittavaa muutosta. Tilastot perustuvat oikeusasiamiehen sisäministeriöltä saamiin kertomuksiin. Tarkat lukumäärätiedot ovat osin salassa pidettäviä, ja merkille pantavaa on, että suojelupoliisin salainen tiedonhankinta ei sisälly lukuihin lainkaan. EOA:n julkaisemat luvut näyttävät kuitenkin suuntaa Helsingin käräjäoikeuden ratkaisukäytännöstä. (EOA:n toimintakertomus vuodelta 2016, http://www.oikeusasiamies.fi/dman/Document.phx?documentId=yx16517082433916&cmd=download)

Luonnollisesti hyväksimisprosenteista ei voida suoraan päätellä, voiko kyse olla jossain määrin tehottomasta ja kritiikittömästä tuomioistuinkäytännöstä vai esimerkiksi vain siitä, että poliisin tekemät hakemukset ovat säännönmukaisesti laadukkaita ja perusteltuja. Alhaiset hyväksymisprosentit vaikuttaisivat kuitenkin merkitsevän, että tärkeää tulkintäkäytäntöä rajanvedoista ihmisoikeusvelvoitteiden edellyttämän yksityisyyttä rajoittavien menetelmien välttämättömyyden suhteen ei juuri synny. Vastaava asetelma, jossa suojelupoliisin esittämiä perusteita ei tehokkaasti haasteta tuomioistuimessa, olisi erityisen huolestuttava ehdotettujen aiempia keinoja laajamittaisempien ja toisaalta perusteuhkiltaan hyvinkin epämääräisten tiedustelumenetelmien kohdalla.

Esityksen 20 §:n mukaan Suomessa olevalle henkilölle, jonka luottamuksellisen viestin tai tallentaman tiedon sisältö on tietoliikennetiedustelussa manuaalisesti selvitetty, ilmoitetaan tiedustelusta siten kuin poliisilain ehdotetussa 5 a luvussa säädettäisiin muiden tiedustelumenetelmien käytöstä ilmoittamisesta. Käytöstä olisi siis ilmoitettava viipymättä tiedonhankinnan kohteena olleelle sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu. Tuomioistuimen päätöksellä ilmoitusta voidaan kuitenkin lykätä enintään kaksi vuotta

kerrallaan, jos se on perusteltua käynnissä olevan tiedustelun turvaamiseksi, kansallisen turvallisuuden suojaamiseksi tai hengen tai terveyden suojaamiseksi. Ilmoitus voidaan myös jättää tuomioistuimen luvalla kokonaan tekemättä, jos se katsotaan välttämättömäksi.

Amnesty pitää hälyttävänä, että lähtökohtaisesta ilmoitusvelvollisuudesta huolimatta tietoliikennetiedustelusta ei kuitenkaan esityksen mukaan tietyissä tilanteissa olisi velvollisuutta ilmoittaa lainkaan. Ilmoitusvelvollisuutta ei olisi, jos näin saatu tieto on hävitetty joko siksi, että tuomioistuin on katsonut kiiretilanteessa tehdyn tiedustelupäätöksen perusteettomaksi, siksi, että viestinnän molemmat osapuolet ovat olleet Suomessa, lakimiestä, lääkäriä, pappia ja toimittajaa koskevien oikeudenkäymiskaareen liittyvien tiedustelukielтojen vuoksi, tai siksi, että tietoa ei yksinkertaisesti tarvita kansallisen turvallisuduen suojaamiseksi.

Käytännössä poikkeukset ilmoittamisvelvollisuuteen merkitsevät, että tiedustelutoiminnan kohteeksi aiheettomasti joutuneet sivulliset eivät koskaan saa tietää, että suojelupoliisin virkamies on päässyt lukemaan heidän viestintäänsä. Tämä koskisi niin tavallisen kansalaisen yksityiselämää koskevaa, arkaluonteista tietoa kuin lakimiehen ja asiakkaan välistä luottamuksellisia viestintää tai esimerkiksi toimittajan ja tietolähteen välillä viestittyä lähdesuojan turvaamaa tietoa. Esityksen mukaan tällainen tieto olisi viipymättä hävitettävä joko tietoliikennetiedustelun teknisen toteuttajan tai, jos tiedot on ehditty toimittaa toimeksiantajalle, toimeksiantajan eli suojelupoliisin toimesta.

Todennäköistä on, että viestin luonne useissa tapauksissa selviää vasta viestin avaamisen ja ihmissilmin tapahtuneen sisällön lukemisen jälkeen. Vaikka tällöin velvollisuus viestin hävittämiseen on selkeä, on väärinkäytösten riski ilmeinen. Kun kyse ei ole enää automaattisesta tiedonkäsittelystä, vaan inhimillisestä toiminnasta, niin virheet kuin suoranaiset väärinkäytökset ovat varteenotettava uhka. Kuten Euroopan unionin tuomioistuimen Schrems-tuomiosta ilmenee, riippumatta yksityisen viestin käytöstä, jo pelkästään viranomaisten pääsy käsiksi yleisesti luottamuksellisia viestejä sisältävän viestiliikenteen sisältöön on omiaan loukkaamaan yksityisyyden suojan keskeistä sisältöä (tuomio 6.10.2015 asiassa C-362/14, kappale 94). Koska aiheettoman urkinnan kohteeksi joutuneet, tiedustelutoiminnan tarkoitukseen nähden täysin sivulliset henkilöt eivät voisi kuitenkaan saada tietoa heihin kohdistuneesta salaisesta tiedustelutoiminnasta, ei heillä olisi mitään mahdollisuutta myöskään oikeussuojakeinojen käyttöön.

Tietojen luovuttaminen kansainvälisessä yhteistyössä

Muun muassa ihmisoikeuspuolustaja Edward Snowdenin mukaan Yhdysvaltain turvallisuusvirasto NSA:n Foreign Affairs Division -osasto on aktiivisesti lobannut Euroopan unionin jäsenmaita muuttamaan lainsäädäntöään massavalvonnan mahdollistamiseksi sekä jakanut maiden käyttöön teknologiaa ja osaamista. Snowden on maininnut Ruotsin, Saksan ja Alankomaat maina, joissa NSA:n painostus on ollut vaikuttamassa massavalvonnan kehittämiseen.

Lainsäädäntövaikuttamisen jälkeen NSA on perännyt pääsyä näiden valtioiden tietoliikenneverkkoihin. Snowden on kuvannut EU-valtioiden Yhdysvaltain viranomaisten kanssa tekemiä sopimuksia siten, että esimerkiksi Tanska on voinut myöntää yhdysvaltalaisviranomaisille pääsyn sen rajat ylittävään tietoliikenteeseen sillä ehdolla, että tanskalaisia henkilöitä koskevat haut eivät ole mahdollisia, ja Saksa taas vastaavasti sillä ehdolla, että saksalaisia ei urkita. Lopputuloksena NSA saisi käyttöönsä saksalaisten viestinnän tanskalaisilta ja toisinpäin. (Ks. Snowdenin paljastuksista esim. Euroopan parlamentin kuuleminen maaliskuussa 2014: http://www.europarl.europa.eu/document/activities/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf; Amnestyn raportti kesäkuussa 2015: https://www.amnesty.org/en/documents/act30/1795/2015/en/)

Tiedustelulakihankkeiden varrella muun muassa Suomen poliittinen johto on useita kertoja todennut, että kotimaiset viranomaiset ovat olleet tiedustelutiedon hankinnassa paljolti ystävällismielisten kumppanien ”hyvän tahdon” varassa. Tiedustelutietoa on paikoin kutsuttu myös eri valtioiden viranomaisten väliseksi vaihtokauppatavaraksi. Snowdenin tekemistä paljastuksista ilmeni, että Suomen sotilastiedustelu on tehnyt yhteistyötä esimerkiksi NSA:n kanssa. Paljastettujen dokumenttien mukaan Suomella oli vuonna 2013 kahdenvälinen yhteistyösopimus NSA:n kanssa. Puolustusvoimien tiedustelupäällikkö Harri Ohra-aho vahvisti yhteistyön olemassaolon. (ks. esim. http://www.hs.fi/kotimaa/art-2000002730962.html)

Kesästä 2013 lähtien saadut paljastukset mm. NSA:n, sen liittolaisten ja eräiden muiden valtioiden toteuttamista globaaleista massavalvontaohjelmista toivat elintärkeällä tavalla päivänvaloon valtioiden aiemmin salaista, monin paikoin laitonta, yksityisyyden suojaa mitätöivää urkintaa. Esityksessäkin mainitussa Euroopan unionin tuomioistuimen Schrems-tuomiossa vahvistettiin, että muun muassa NSA:lle pääsyn lukuisten yritysten ja verkkopalveluiden tietoihin tarjoavan PRISM-massavalvontaohjelman myötä ei ollut takeita siitä, että yritysten luovuttaessa käyttäjien henkilötietoja Euroopasta Yhdysvaltoihin oltaisiin voitu varmistua EU-lainsäädännön edellyttämästä tietosuojan riittävästä tasosta.

Suojelupoliisin tiedustelumenetelmiä koskevan poliisilakiin ehdotetun 5 a luvun 54 §:n mukaan suojelupoliisi voi tehdä yhteisiä operaatioita ulkomaisten turvallisuus- ja tiedustelupalveluiden kanssa sekä luovuttaa tietoja muiden maiden viranomaisille kansallisen turvallisuuden suojaamiseksi, jos tietojen luovuttaminen ei ole vastoin tärkeää kansallista etua. Henkilötietojen luovuttamisesta ulkomaisille viranomaisille säädetään laissa henkilötietojen käsittelystä poliisitoimessa.

Pykälää koskevissa yksityiskohtaisissa perusteluissa todetaan, että tällaisten tietojen luovuttamisen pitäisi perustua suojelupoliisin tehtävään suojata kansallista turvallisuutta. Tiedon luovuttamisen tulisi toisaalta olla tärkeän kansallisen edun mukaista. Perustelujen mukaan tällaisen edun piiriin kuuluisivat esimerkiksi tiedot Suomen poliittisista tai taloudellisista suhteista toisen valtion kanssa (s. 226). Maininta taloudellisista suhteista tiedustelutietojen kansainvälisen tietojenvaihdon

hyväksyttävyyden edellytysten yhteydessä on epäselvä. On kyseenalaista, mitä tekemistä taloudellisilla suhteilla olisi kansallisen turvallisuuden suojaamiseksi tapahtuvan tiedusteluyhteistyön ja tietojen luovuttamisen kanssa.

On ongelmallista, että ehdotetussa pykälässä tai edes esityksen perusteluissa ei mainita tiedustelun kohteeksi joutuneiden henkilöiden yksityisyyden suojaa ja yhteistyövaltion ihmisoikeuksien suojan tasoa huomioon otettavana seikkana kansainvälisestä tietojenvaihdosta päätettäessä.

Lopuksi

Syvälle käyvää puuttumista yksityisyyden suojan alaan merkitsevän tiedustelutoiminnan hyväksyttävyys perustuslain ja Suomen kansainvälisten ihmisoikeusvelvoitteiden kannalta edellyttää ihka ensimmäisenä ä sitä, että tällaisesta toiminnasta säädetään lailla. Lailla säätämisen vaatimus edellyttää oikeuden alaan puuttuvalta lainsäädännöltä myös laatuvaatimuksia: lainsäädännön on oltava täsmällistä ja tarkkarajaista sekä ennustettavaa siten, että kansalaisilla on edes jossain määrin mahdollisuus ennakoida, millaisen toiminnan kohteeksi he voivat joutua Näin siitä huolimatta, että tiedustelutoiminnan salainen perusluonne asettaa haasteensa ennustettavuutta ja läpinäkyvyyttä koskeville vaatimuksille.

On positiivista, että lausuttavana olevassa esityskokonaisuudessa tiedustelun menetelmät on ainakin periaatteessa pyritty kattavasti nimeämään ja esittelemään lainsäädännössä. Kaikkialla tämä ei kuitenkaan ole toteutunut. Lisäksi mietintötekstistä on vielä pitkä matka kuljettavana siihen, että kaavailtu tiedustelu olisi täysin sopusoinnussa kansainvälisten ihmisoikeusvelvoitteiden kanssa.

Laajamittainen viestintätiedustelu ei missään oloissa ole perus- ja ihmisoikeuksien kannalta ongelmatonta, koska tällainen toiminta merkitsee jo lähtökohtaisesti syvälle käyvää puuttumista useiden perus- ja ihmisoikeuksien, keskeisimpänä yksityisyyden suojan alaan. Olennaista on huolellisella lainvalmistelulla ja myöhemmin osaavalla, tehokkaalla ja riittävästi resursoidulla valvonnalla varmistaa mahdollisimman tehokkaat suojakeinot väärinkäytösten ja ylilyöntien ehkäisemiseksi ja tapahtuneisiin väärinkäytöksiin ja ylilyönteihin reagoimiseksi. On myös varmistettava, että lainsäädännössä ja viranomaistoimivaltuuksissa ei tulevaisuudessa livetä aina vain epämääräisempiin ja syvemmälle kansalaisten oikeuksien alaan kajoaviin keinoihin.

Edes kansallinen turvallisuus tai maailmaa järisyttävät surulliset terroriteot eivät ole hyväksyttävä peruste ihmisoikeussuojan nakertamiselle. Valitettavasti Amnesty International raportoi jatkuvasti eri puolilla maailmaa valtioista, laeista ja viranomaistoiminnasta, joissa epämääräisen kansallisen turvallisuuden käsitteen nimissä, terrorismin torjunnan ja pelon varjolla hyökätään aggressiivisesti keskeisiä kansalaisoikeuksia vastaan.

Kunnioittavasti

Amnesty International Suomen osasto

Niina Laajapuro

Ihmisoikeustyön johtaja

Mikko Aarnio

Oikeudellinen asiantuntija

Aarnio Mikko
Amnesty International Suomen osasto