Ulkoasiainvaliokunnalle

Pyydettynä lausuntona hallituksen esityksestä siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/2017 vp) esitän kunnioittavasti seuraavaa.

1. Johdannoksi

Valiokunnalta saamassani lausuntopyynnössä toivottiin, että lausuntoni keskittyisivät ihmisoikeuselementtien huomioimiseen ja ihmisoikeuksien toteutumiseen ehdotuksissa tiedustelulainsäädännöksi (HE 202/2017 vp siviilitiedustelusta ja HE 203/2017 vp sotilastiedustelusta). Näitä esityksiä on luonnollisesti luettava yhdessä samaan lainsäädäntökokonaisuuteen kuuluvan perustuslain 10 §:n muutoksen (HE 198/2017 vp) ja tiedustelun valvontaa koskevan esityksen (HE 199/2017 vp) kanssa. Ehdotettu kansallisen perusoikeussuojan kaventaminen suhteessa sotilas- ja siviilitiedustelun toimivaltuuksiin siirtäisi painopistettä kansainvälisten ihmisoikeussopimusten ja Euroopan Unionin perusoikeuskirjan suuntaan arvioitaessa tiedusteluvaltuuksien soveltamista ja mahdollisia tulevia lainsäädäntöhankkeita niiden alalla. Tiedusteluvaltuuksien tehokas valvonta puolestaan on eräs niistä perusteista, joiden nojalla jatkossa arvioitaisiin, pysyykö valtuuksien soveltaminen ihmisoikeussopimusten kannalta hyväksyttävissä rajoissa.

Tässä lausunnossa arvioin vain siviilitiedusteluhanketta (HE 202/2017 vp). Lisäksi viittaan erilliseen lausuntooni sotilastiedustelusta (HE 203/2017 vp). Kannanottojeni taustoittamiseksi lainaan kuitenkin tähän perustuslakivaliokunnalle 26.2.2018 antamassani lausunnossa esittämäni parannetun sanamuodon mahdollisesti säädettävälle perustuslain 10 §:n 3 momentille:

> ”Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Suomen kansalaisten tai Suomen perusoikeussuojan piirissä olevien muiden ihmisten luottamuksellisia viestejä sisältävän tietoliikenteen yleinen seuranta on kielletty.”

2. *Ihmisoikeusarvioinnin lähtökohdista – tutkimushanke SURVEILLE*

Käsillä oleva hallituksen esitys (siis HE 202/2017 vp) koskee ensi sijassa siviilitiedustelun toimivaltuuksia. Sen ihmisoikeusvaikutukset kohdistuvat välittömästi ja ensisijaisesti yksityisyyden tai yksityiselämän suojaan, sellaisena kuin se on turvattu mm. Euroopan ihmisoikeussopimuksessa (8 artikla) ja YK:n yleissopimuksessa kansalaisoikeuksista ja poliittisista oikeuksista (17 artikla). Tämä ihmisoikeus on laaja-alainen ja pitää sisällään myös kirjesalaisuuden ja luottamuksellisen sähköisen viestinnän suojan, kotirauhan, kunnian suojan ja henkilötietojen suojan. Viimeksi mainitusta on erillinen 8 artikla Euroopan Unionin perusoikeuskirjassa, jonka 7 artikla kattaa yksityiselämän suojan perinteisemmät osa-alueet.

Välillisesti tiedustelulla on vaikutuksia myös monien muiden ihmisoikeuksien alalla, kuten syrjinnän kielto, sananvapaus, uskonnonvapaus, liikkumisvapaus, yhdistymisvapaus ja kokoontumisvapaus. Tiedustelu voi johtaa luonteeltaan syrjivään profilointiin, maasta poistumisen tai maahan saapumisen epäämiseen, painetun tai sähköisessä muodossa julkaistun aineiston levityksen estämiseen jne. Tiedustelun välillisiä vaikutuksia muihin ihmisoikeuksiin on kuvattu mm. termillä *tukahduttava vaikutus* (*chilling effect*), millä tarkoitetaan ihmisten näennäisesti vapaaehtoista luopumista joidenkin ihmisoikeuksina suojattujen asioiden tekemisestä. Tieto laajamittaisen tiedustelun esiintymisestä voi merkittävästi vaikuttaa siihen, vieraileeko joku esimerkiksi moskeijassa, homobaarissa tai psykiatrilla. Kysymys ei ensi sijassa ole siitä, että näitä valintoja tekevillä ihmisillä olisi ”jotain salattavaa” – he vain pitävät kiinni yksityisyydestään ja haluavat itse päättää, kenen kanssa jakavat tiedon esimerkiksi uskonnostaan, seksuaalisesta suuntautumisestaan tai ammattiauttajaan tukeutumisestaan. Jokainen meistä suojaa esimerkiksi sähköpostinsa salasanaa ja pankkikorttinsa PIN-koodia. Samoin meillä on intiimejä salaisuuksia läheistemme kanssa, ja haluamme itse päättää, mitkä niistä jaamme vain puolison kanssa ja mitkä taas myös vanhempien, lasten, sisarusten jne. kanssa. Erityisesti älypuhelimen muodostuminen osaksi miltei kaikkien meidän jokapäiväistä elämää on radikaalisti muuttanut tiedustelutoiminnan toimintaympäristöä ja samalla sen ihmisoikeusvaikutuksia. Älypuhelimen kantaminen jatkuvasti mukana merkitsee, että ihmisen olinpaikka dokumentoidaan koko ajan ja hetki hetkeltä. Kun myös hänen kohtaamansa ihmiset kantavat vastaavaa laitetta, myös kaikista tapaamisistamme jää muistijälki, olivat ne sitten kahdenkeskisiä tai isoon kokoukseen osallistumisia. Kun reaaliaikainen paikkatieto liitetään kaikkeen muuhun ns. tunnistamistietoon, saatava tietojen kokonaisuus paljastaa ihmisestä enemmän kuin yksityisyyden perinteisenä ydinalueena pidetty viestien sisältö.

Johtamassani EU:n rahoittamassa tutkimushankkeessa SURVEILLE (*(Surveillance: Ethical Issues, Legal Limitations, and Efficiency)*[1] tutkimme vuosina 2012-2015 eri tarkkailuteknologioiden (tai tiedusteluteknologioiden) kykyä erilaisissa tilanteissa tuottaa turvallisuushyötyä, tuon hyödyn kustannustehokkuutta, teknologioihin liittyviä eettisiä

[1] Ks. https://surveille.eui.eu missä ns. SURVEILLE Briefing Note esittelee pähkinänkuoressa tutkimushankkeessa kehitellyn metodologian valvontateknologioiden arvioimiseksi.

ongelmia ja niiden vaikutusta ihmisoikeuksien/perusoikeuksien alalla. Kehitimme menetelmät, joiden avulla tarkkailuteknologioita voidaan yhdellä kertaa arvioida kaikissa näissä suhteissa sen ratkaisemiseksi, onko tietyn tarkkailumenetelmän käyttö jossakin konkreettisessa tilanteessa hyväksyttävää. Mallimme perustuu kolmen rinnakkaisen asiantuntijaraadin toteuttamaan pisteytykseen kunkin teknologian hyvistä ja huonoista puolista tietyssä käyttötilanteessa ja kolmen eri pisteytyksen yhteenkokoamiseen strukturoidulla tavalla. Euroopan Parlamentti hyväksyi 29.10.2015 päätöslauselman, jossa se antoi tunnustusta SURVEILLE-hankkeessa kehitetylle arviointimenetelmälle. Siinä Parlamentti

> 28. on sitä mieltä, että valvontateknologian käyttöä koskevat päätökset tulee perustaa tarpeellisuuden ja oikeasuhteisuuden perusteelliseen arviointiin; pitää myönteisinä tuloksia, jotka on saatu SURVEILLE-tutkimushankkeesta, joka tarjoaa menetelmän valvontateknologioiden arvioimiseen ja jossa otetaan huomioon oikeudelliset, eettiset ja teknologiset näkökohdat;[2]

Tässä yhteydessä nostan esiin kolme keskeistä SURVEILLE-hankkeen tutkimustulosta:

(1) Vaikka tarkkailuteknologioiden käyttö vaikuttaa monien ihmisoikeuksien alalla, päädyimme siihen tulokseen, että miltei poikkeuksetta noiden vaikutusten kokonaisarvio on mahdollista tehdä arvioimalla kattavasti ja huolellisesti vaikutukset yksityisyyden suojaan, johon puuttumisesta sitten seuraa koko joukko välillisiä vaikutuksia muiden ihmisoikeuksien toteutumiseen. On kuitenkin muistettava, että yksityisyyden suojan osa-alueena tulee aina erikseen arvioida vaikutukset tietosuojan alalla, koska useissa tapauksissa saimme kaikkein vakavimmat ihmisoikeusvaikutukset nimenomaan siellä.

(2) Monissa tutkimissamme tilanteissa saatoimme todeta, että tietyn tarkkailuteknologian käyttö tietyssä tilanteessa oli hyväksyttävää: sillä saavutettiin todellista hyötyä esimerkiksi yleiselle turvallisuudelle tai rikostutkinnalle ja siitä aiheutuvat ihmisoikeuksien rajoitukset olivat asteeltaan sellaisia, että saavutettu hyöty teki ne oikeutetuiksi. Ihmisoikeusrajoitusten suhteellisuusarviointi ei koske abstraktia *arvojen* painon vertailua, esimerkiksi yksilön yksityisyyden suoja vs. koko kansakunnan turvallisuus. Se koskee vertailua yhteen yksilöön tai laajaankin joukkoon ihmisiä kohdistuvan *ihmisoikeusrajoituksen* ja rajoituksen perustana olevan hyväksyttävän tarkoituksen toteuttamiselle juuri tuon rajoituksen kautta *saavutettavan hyödyn* välillä. Ei siis riitä, että ihmisoikeusrajoitus palvelee (tai sen vain sanotaan palvelevan) esimerkiksi kansallista turvallisuutta. On osoitettava, että se on *tehokas* siten, että sillä saavutetaan osoitettavissa tai jopa mitattavissa oleva hyöty kansallisen turvallisuuden kannalta. Ja sitten tuota hyötyä – ei siis abstraktia tarkoitusperää – verrataan ihmisoikeusrajoitukseen, jonka osalta on vielä otettava huomioon sekä rajoituksen sisällöllinen kohdentuminen ihmisoikeuden piirissä että sen aste.

[2] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0388+0+DOC+XML+V0//FI

(3) Edelleen SURVEILLE-tutkimushankkeeseen keskeisiin tuloksiin kuuluu, että sähköisen viestinnän massavalvonnan (tai ”laajamittaisen valvonnan”, mitä termiä käytetään edellä mainitun Euroopan Parlamentin päätöslauselman suomenkielisessä toisinnossa, vrt. saman päätöslauselman alkuperäisen englanninkielisen version termi ”mass surveillance” tai ruotsinkielisen version ”massövervakning”)[3] menetelmät (kuten tietyn tietoliikennekaapelin viestivirran seulonta algoritmien avulla) *epäonnistuvat* turvallisuushyödyn tuottamisessa eivätkä läpäise ihmisoikeusrajoituksen oikeasuhtaisuuden vaatimusta, kun taas sähköisen viestinnän kohdennettu valvonta (esim. yhden esimerkiksi henkilötiedustelun seurauksena valitun henkilön Facebook-yhteysverkoston pohjalta) tuottaa sekä paremman turvallisuushyödyn että asteeltaan hyväksyttävän ihmisoikeusrajoituksen.

3. *Hallituksen esityksen arviointia*

Hallituksen esitykseen sisältyy jaksot kansainvälisten ihmisoikeussopimusten (ss. 50-64) ja EU:n perusoikeuskirjan (ss. 64-68) merkityksestä asian yhteydessä. Ihmisoikeussopimusten tarkastelu keskittyy YK:n ns. KP-sopimukseen ja Euroopan ihmisoikeussopimukseen. KP-sopimusta koskevassa lyhyessä jaksossa (s. 51) ei ole varsinaisia virheitä, mutta pidän tarkastelua puutteellisena, kun se keskittyy KP-sopimuksen 17 artiklan (yksityisyyden suoja) tekstiin ja vuodelta 1988 olevaan – siis 30 vuotta vanhaan – 17 artiklan yleiskommenttiin ja lyhyesti toteaa, ettei YK:n ihmisoikeuskomitea toistaiseksi ole käsitellyt tietoverkkoturvallisuuteen tai sähköiseen viestintään liittyviä yksilövalituksia. Olisi ollut perusteltua sisällyttää tähän tarkasteluun myös sen raportin esittely, jonka vuonna 2009 laadin YK:n ihmisoikeusneuvostolle koskien yksityisyyden suojaa terrorismin torjunnassa.[4] Tuo raportti nimittäin merkittäviltä osin koskee KP-sopimuksen 17 artiklan tulkintaa ja kartoittaa asioita, joita YK:n ihmisoikeuskomitean tulisi käsitellä uudessa tuon artiklan yleiskommentissa, joka toivon mukaan on komiteassa työn alla. Myös komitean omaa valmista tulkinta-aineistoa olisi ollut saatavilla, nimittäin sopimusvaltioiden määräaikaisraporttien yhteydessä esitetyt ihmisoikeuskomitean maakohtaiset johtopäätökset, joissa etenkin vuoden 2013 Snowden-paljastusten jälkeen on varsin systemaattisesti arvioitu eri maiden tiedustelulakeja ja -käytäntöjä.

[3] Euroopan Parlamentin päätöslauselman eri kieliversiot osoittavat, että keskustelu ns. massavalvonnasta on osin käännösongelma, kun englannin *mass surveillance* ja ruotsin *massövervakning* on saanut suomeksi vastineen *laajamittainen valvonta*. Huomattakoon myös, että EU-tuomioistuin on (myös englanniksi) välttänyt ratkaisuissaan termiä *mass surveillance* ja sen sijaan valinnut ilmaisun *generalised access* (*Max Schrems*, kohta 94) tai *generalised manner* (*Digital Rights Ireland*, kohta 57). Euroopan ihmisoikeustuomioistuin puolestaan on ainakin ratkaisussaan *Szabo and Vissy v. Hungary* käyttänyt termiä *massive monitoring of communications*.

[4] YK-asiakirja A/HRC/13/37, http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

Erityisen merkittävinä tältä kannalta pidän komitean kannanottoja[5] Yhdysvaltain maaraportin käsittelystä vuonna 2014 ja Iso-Britannian maaraportin käsittelystä[6] vuonna 2015. Nuo kannanotot osoittavat, että ihmisoikeuskomitealla on varsin systemaattinen ote suhteessa tietoliikennetiedustelun arviointiin KP-sopimuksen 17 artiklan kannalta, vaikka vuoden 1988 yleiskommenttia ei vielä ole uudistettu. Komitea oli hyvin kriittinen Yhdysvaltain omaksumasta tietoliikennekaapelien viestivirran seulonnasta ja luonnehti Iso-Britannian tietoliikennetiedusteluvaltuuksia massavalvonnaksi (*mass interception)* ja katsoi, ettei se anna riittävää suojaa mielivaltaisilta puuttumisilta yksityisyyden suojaan. Komitea katsoi, että viranomaisten pääsy tietoliikenteeseen tuli rajoittaa tilanteisiin, joissa se oli ankaran välttämätöntä kaikkein vakavimpien rikosten saattamiseksi syytteeseen.

Hallituksen esitykseen sisältyy myös melko laajat säätämisjärjestysperustelut (ss. 270-278), joissa tietenkin päähuomio kohdistuu tehtyjen ehdotusten arviointiin Suomen omaa perustuslakia vasten. Kun tuossa yhteydessä suurelta osin on kysymys ehdotetun lainsäädännön perusoikeusvaikutusten arvioinnista ja kun kansalliset perusoikeussäännökset on laadittu mahdollisimman hyvin vastaamaan maamme kansainvälisiä ihmisoikeusvelvoitteita, tarkastelu on informatiivinen myös lakiehdotusten ihmisoikeusvaikutusten arvioinnissa. On myös huomattava, että kansainvälisten ihmisoikeusvelvoitteiden kunnioittaminen on vakiintuneesti eräs niistä ehdoista, joiden tulee täyttyä, jotta perusoikeuden rajoitus olisi kansallisen perustuslain kannalta hyväksyttävä (ks. PeVM 25/1994 vp). Tämä ulottuvuus on käsillä olevassa asiassa erityisen tärkeä, koska hallitus ehdottaa perustuslain 10 §:n muuttamista siten, että luottamuksellisen viestin salaisuus jatkossa väistyisi kansallisen turvallisuuden ja sotilaallisen tiedonhankinnan tieltä. Vaikka tuollainen perustuslain muutos toteutettaisiin, se ei vähimmässäkään määrin kavenna Suomen ihmisoikeusvelvoitteita, jotka jäävät koskemattomiksi. Jos ehdotettu perustuslain muutos toteutuu, tiedustelutoimintaa koskevia lainsäädäntöhankkeita on *entistä korostetummin* arvioitava suoraan kansainvälisiä ihmisoikeussopimuksia vasten, vaikka olisi kuinka selvää, että kansallisen perustuslain muutettua kirjainta ei loukata. Tuota ihmisoikeusarviointia tullaan tekemään sekä kansallisella että kansainvälisellä tasolla.

Jos tiedustelulainsäädäntöä koskevat hallituksen esitykset hyväksytään nykyisen eduskunnan toimikauden aikana tai lepäämään hyväksyttyinä hyväksytään uudelleen heti vuoden 2019 eduskuntavaalien jälkeen, Suomen tulee tuoreeltaan raportoida niiden sisällöstä YK:n ihmisoikeuskomitealle seuraavassa määräaikaisraportissaan, jonka määräpäivä on 26.7.2019. Uudet tiedustelulait tulevat siis ihmisoikeuskomitean arvioitaviksi ilman yksilövalituksiakin. Olisi ollut paikallaan, että hallitus olisi

[5] YK-asiakirja CCPR/C/USA/CO/4, http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/USA/CO/4&Lang=En

[6] YK-asiakirja CCPR/C/GBR/CO/7, http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR/C/GBR/CO/7&Lang=En

valmistautunut tähän tulossa olevaan arviointiin käymällä läpi ja esittämällä eduskunnalle muiden maiden ihmisoikeuskomitealta saamia kannanottoja.

Euroopan ihmisoikeussopimukseen ei liity säännönmukaista raportointimekanismia, vaan sopimusta valvotaan miltei yksinomaan yksilövalitusten kautta. Hallituksen esityksessä on varsin seikkaperäisesti selostettu Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntöä yksityiselämän suojan (8 artikla) ja tiedusteluvaltuuksien alalla (ss. 51-65). Tämän lisäksi esityksessä selostetaan (ss. 65-68) myös Euroopan Unionin tuomioistuimen ratkaisukäytäntöä yksityiselämän suojan (EU:n perusoikeuskirjan 7 artikla) ja henkilötietojen suojan (perusoikeuskirjan 8 artikla) alalla. Katsaukset ovat sinänsä asianmukaisia tähänastisen oikeuskäytännön kuvauksina. Niitä on kuitenkin syytä täydentää neljällä huomiolla, jotka kaikki ovat merkityksellisiä nyt tarkasteltavan hallituksen esityksen arvioinnissa.

(1) Vaikka EU-oikeudessa kansalliseen turvallisuuteen liittyvät kysymykset ovat jäsenvaltioiden (eikä unionin) toimivallan piirissä ja siten unionin tuomioistuimen tuomiovallan ja perusoikeuskirjan soveltamisalan ulkopuolella, tästä ei pidä tehdä johtopäätöstä, että EU-tuomioistuimen linjaukset olisivat kansallisella turvallisuudella perustellun tiedustelutoiminnan kannalta merkityksettömiä. Ensinnäkin EU-tuomioistuin osallistuu merkittävällä tavalla yksityisyyden suojan ja muiden ihmisoikeuksien sisällölliseen kehittämiseen. Esimerkiksi kysymys yksityisyyden suojan loukkaamattomasta ydinalueesta on merkityksellinen myös KP-sopimuksen ja Euroopan ihmisoikeussopimuksen tulkinnassa, ja EU-tuomioistuimen linjauksia seurataan silloin tarkasti. Jos jokin toiminta loukkaa yksityisyyden suojan ydintä, se on ihmisoikeuksien kannalta kielletty eikä mitään suhteellisuusarviointia suoriteta.

(2) Yleisemminkin hallituksen esityksen oikeustapauskatsauksia vaivaa staattisuus: niissä ei ole pyritty ennakoimaan niitä ihmisoikeushaasteita, joita tiedustelutoiminnan ja tiedusteluvaltuuksien arvioinnissa joudutaan kohtaamaan tämän vuosikymmenen loppuvuosina ja ensi vuosikymmenen aikana. Edward Snowdenin paljastuksista on kulunut vasta viisi vuotta, eivätkä niiden esiin nostamat kysymykset mm. tietoliikenteen massavalvonnasta ole vielä edes ehtineet Euroopan ihmisoikeustuomioistuimeen. Siellä on vireillä useita merkittäviä valitusasioita, ja esimerkiksi Iso-Britanniassa on jo saatu kansallisten tuomioistuinten ratkaisuja, jotka osoittavat maan tiedustelulainsäädännön ongelmalliseksi ihmisoikeuksien kannalta. Euroopan ihmisoikeustuomioistuimen marraskuulta 2017 oleva katsaus (*Factsheet*) massavalvontaa (*mass surveillance*) koskeviin asioihin esittelee joukon vireillä olevia valituksia mm. Ruotsista, Itävallasta, Iso-Britanniasta ja Ranskasta.[7] Eri maiden tiedustelulait ovat parhaillaan ihmisoikeustuomioistuimen arvioitavina, eikä tuomioistuimen aiemmista ratkaisuista ja noiden maiden lakien sisällöstä voi siksi tehdä päätelmää, että Suomessa nyt ehdotetut lait olisivat ihmisoikeussopimuksen kannalta

[7] https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

hyväksyttäviä. Hallituksen esityksen katsaukseen ihmisoikeustuomioistuimen ratkaisukäytännöstä on syytä suhtautua varauksin, koska niitä kysymyksiä, joita Suomessa ehdotetut tiedustelulait herättävät, ei suurelta osin ole vielä ratkaistu ihmisoikeustuomioistuimessa, vaan ne ovat siellä vireillä.

(3) Vaikka kansallinen turvallisuus on Euroopan ihmisoikeussopimuksessa ja sen ratkaisukäytännössä hyväksyttävä peruste yksityiselämän suojan rajoituksille, se ei merkitse avointa valtakirjaa mille hyvänsä tiedustelutoiminnalle, jonka perusteluksi esitetään kansallinen turvallisuus. Tämä on ohimennen todettu hallituksen esityksessä *Zakhrarov*-tapauksen yhteydessä (s. 60). Sinänsä pidän onnistuneina hallituksen tiedustelulakipaketissa esitettyjä luonnehdintoja kansallisen turvallisuuden käsitteestä. Mutta tästä ei seuraa, että ehdotetuissa lakiteksteissä olisi onnistuttu operationalisoimaan tuo yksityiselämän suojan sinänsä hyväksyttävä tarkoitusperä sillä tarkkuudella, mitä on edellytettävä, jotta tiedusteluvaltuuksien laajuus olisi ihmisoikeuksien kannalta hyväksyttävä. Esimerkiksi siviilitietoliikennetiedustelulakiehdotuksen (2. lakiehdotus) keskeisen 3 §:n luettelo tietoliikennetiedustelun kohteista on aivan liian yleisluontoinen, jotta se voisi hyväksyttävällä tavalla tarjota rajanvetoperusteet sen arvioinnille, milloin tietoliikennetiedustelu on 4 §:n nojalla hyväksyttävissä sen vuoksi, että käsillä on vakava uhka kansalliselle turvallisuudelle. Esimerkiksi ”terrorismi” esiintyy yleisluontoisesti yhtenä sanana 3 §:n luettelon 1 kohtana, ja 4 § vain edellyttää, että ”voidaan perustellusti olettaa” tietoliikennetiedustelusta saatavan tietoja toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Näiden säännösten yhteisvaikutus tulisi hyvin helposti olemaan, että Suojelupoliisin oma näkemys olisi ratkaiseva ja riittävä lain kirjaimen täyttämiseksi. Poliisilakiin ehdotetussa 5 a luvussa nämä säännökset ehdotetaan ulotettaviksi myös muihin tiedusteluvaltuuksiin, siis tietoliikennetiedustelun lisäksi (ks. siellä 3 ja 4 §).

(4) On vielä syytä korostaa, ettei tiedusteluvaltuuksien hyväksyttävyys ihmisoikeuksien kannalta tyhjene suhteellisuusarviointiin, missä oikeusturvajärjestelyillä on oma tärkeä osuutensa. Yksityisyyden suojan ydinalueen loukkaamattomuus ja vaatimus sääntelyn täsmällisyydestä ja tarkkarajaisuudesta ovat itsenäisiä arviointiperusteita, joita kansallisen turvallisuuden suuri painoarvo suhteellisuusarvioinnissa ei oikeuta sivuuttamaan. Otan taas esimerkin siviilitietoliikennetiedustelulakiehdotuksesta: sen 5 §:n säännöstä *hakuehdoista* tulisi olennaisesti täsmentää, jotta laki olisi täsmällisyydeltään ihmisoikeuksien kannalta hyväksyttävä. Nyt säännökseen sisältyy joitakin luonteeltaan negatiivisia rajauksia sille, mitä hakuehdot eivät saa olla, mutta ei mitään määritelmää tai positiivista kuvausta niistä. Mainittakoon, että se mitä hallituksen esitysten perusteluissa on sanottu hakuehdoista, ei selvennä asiaa, vaan ennemmin kertoo hakuehtojen käytön *tarkoitusperistä* kuin ehdoista itsestään.

Siirryn seuraavaksi valikoituihin kysymyksiin, joissa pidän ihmisoikeuksien suojan kannalta välttämättömänä, että siviilitiedustelua koskevan hallituksen esityksen sisältämiä lakiehdotuksia korjataan eduskuntakäsittelyssä.

4. Ihmisoikeuksien edellyttämät korjaukset

(1) Tietoliikennetiedustelu

Ensimmäinen ja suurin korjausehdotukseni koskee siviilitietoliikennetiedustelulaki-ehdotuksen perusratkaisua, hakuehtojen avulla toteutettavaa tietyn tietoliikennekaapelin (tai sen osan) viestivirran seulontaa. Näkemykseni mukaan tämä perusratkaisu on ristiriidassa Euroopan ihmisoikeussopimuksen 8 artiklan, KP-sopimuksen 17 artiklan ja EU:n perusoikeuskirjan 7 ja 8 artiklan kanssa.

Tietoliikennetiedustelu voi olla kohdennettua tai yleistä (ns. massavalvontaa), ja perimmältään tämä erottelu perustuu siihen, pyritäänkö sen avulla laajasta ja suurimmalta osin merkityksettömäksi tiedetystä tietovirrasta (esim. tietty tietoliikennekaapeli) seulomaan esiin epäilyttäviä henkilöitä (ns. *downstream*- eli myötävirtamenetelmä) vai onko lähtökohtana *muilla keinoin* kuin tietoliikennetiedustelulla ja sen myötävirtamenetelmällä, siis esimerkiksi henkilötiedustelun tai rikosepäilyn kautta, identifioitu kohdehenkilö, jonka yhteysverkkoa lähdetään analysoimaan kohdennetun tietoliikennetiedustelun menetelmin (ns. *upstream*- eli vastavirtamenetelmä). Vastavirtamenetelmä kajoaa viattomien sivullisten viesteihin vain pienessä murto-osassa tapauksia verrattuna myötävirtamenetelmään. Lisäksi sen mahdollisuudet tunnistaa alkuperäisen kohdehenkilön ohella muita oikeutettuja tiedustelun kohteita ovat ylivertaiset myötävirtamenetelmään verrattuna. Esimerkiksi Turussa 18.8.2017 tapahtuneet ISIS:n inspiroimat puukotukset olisi ehkä voitu välttää kohdennetulla tietoliikennetiedustelulla (vastavirtaan), koska suojelupoliisi oli kuukausia aiemmin saanut tekijästä vihjetiedon. Sen sijaan tietoliikennekaapelien viestivirran seulominen (myötävirtaan) olisi epäonnistunut tässäkin tapauksessa. Korostan myös, että surmatyöt olisi voitu estää myös ilman kohdennettuakin tietoliikennetiedustelua, jos poliisin ja suojelupoliisin saamat vihjeet olisi otettu vakavammin.[8] Perinteinen henkilötiedustelu on myös SURVEILLE-tutkimushankkeen tulosten mukaan selvästi tehokkaampi keino esimerkiksi terroritekojen estämiseksi kuin tietoliikennetiedustelu.

Kun jo tiedusteluviranomaisten pääsy tietoliikennekaapelehin merkitsee kajoamista yksityisyyden suojaan, kun tämä kajoaminen ylivoimaisessa valtaosassa tapauksia kohdistuu täysin viattomiin sivullisiin, ja kun seulonnasta saatava todellinen hyöty kansallisen turvallisuuden kannalta on vähäinen, itse tiedustelumenetelmä on sellainen, ettei se voi olla demokraattisessa yhteiskunnassa välttämätön mm. siten, että sen tuottamat turvallisuushyödyt olisivat ihmisoikeuksille aiheutuvaa haittaa suuremmat. Viittaan SURVEILLE-tutkimushankkeen tuloksiin ja kansainväliseen kokemukseen siitä, ettei tietoliikennetiedustelun myötävirtamenetelmä tuota todellista turvallisuushyötyä.

[8] Mainittakoon, että olen antanut asiaa käsittelevälle Varsinais-Suomen käräjäoikeudelle asiantuntijalausunnon siitä, millä ehdoin kyseiset puukotukset ovat rikoslain 34 a luvun 1 ja 6 §:ssä tarkoitettuja terroristisessa tarkoituksessa tehtyjä rikoksia.

Pahimmillaan tietoliikenteen seulonta myötävirtamenetelmällä ei ole vain hyödytöntä ja ihmisoikeuksien kannalta vahingollista, vaan se myös heikentää turvallisuusviranomaisten kykyä ennalta torjua terroritekoja. Näin käy, jos poliisin ja tiedustelupalvelujen voimavarojen kohdentaminen on teknologian ja kansainvälisen tietojenvaihdon ohjaamaa, sen sijaan että priorisoitaisiin yksilötason vihjetietoja mm. jalkautumalla väestön keskuuteen ja tietoliikennetiedustelun vastavirtamenetelmän käytöllä.

On osin semanttinen kysymys, kutsutaanko tietoliikennekaapelien myötävirtaseulontaa massavalvonnaksi. Viittasin jo edellä siihen, että Euroopan Parlamentti on käyttänyt suomeksi termiä ”laajamittainen valvonta”. Englanniksi termi *mass surveillance* on varsin vakiintunut, ja ehdotettu tietoliikennetiedustelu nähdäkseni hyvin mahtuu sen piiriin. Hallitus on pyrkinyt vakuuttamaan, että sen ehdotukset merkitsevät kohdennettua tietoliikennetiedustelua. Tätä on pyritty perustelemaan sillä, kuinka ylivoimainen valtaosa viestivirrasta seulotaan koneellisin menetelmin pois, niin että ihmissilmin nähtäväksi päätyy vain häviävän pieni murto-osa seulonnan kohteena olleesta viestivirrasta. Paradoksaalisesti juuri tämä perustelu osoittaa, että perusratkaisussa eli tiedusteluviranomaisten pääsyssä yleisesti viestivirtaan *on kyse massavalvonnasta*. Tarkkaan lukien tämä selviää myös ehdotetusta lakitekstistä, jossa ei puhuta kohdennetusta valvonnasta vaan siitä, kuinka tietoliikennetiedustelun avulla huomio *kohdistetaan* jatkoanalyysia vaativiin viesteihin. Siviilitietoliikennetiedustelulakiehdotuksen 5 §:n avausvirke kuuluu: ”Tietoliikennetiedustelu kohdistetaan tietoliikenteen automatisoidun erottelun avulla.” Tietoliikennetiedustelun kohteena siis on koko viestivirta, ja tiedustelun avulla toteutetaan viestien seulonta, niin että laillisten ja harmittomien viestien ylivoimainen valtavirta jää syvemmälle käyvien kajoamisten – kuten viestin sisällön lukeminen ihmissilmin – ulkopuolelle.

SURVEILLE-tutkimushankkeen tulosten, Euroopan ihmisoikeustuomioistuimen liiketilassa olevan oikeuskäytännön, massavalvontaan hyvin kriittisesti suhtautuvien EU-tuomioistuimen ratkaisujen (*Digital Rights Ireland, Max Schrems, Tele2 & Watson*) sekä YK:n ihmisoikeuskomitean Yhdysvaltain ja Iso-Britannian maaraporttien käsittelyssä esittämien kannanottojen valossa katson, että ehdotettu tietoliikennetiedustelun perusratkaisu (myötävirtamenetelmä) tulisi hylätä ja koko järjestelmä rakentaa vastavirtaan toteutettavan tietoliikennetiedustelun pohjalta, jolloin lähtökohtana siis olisi epäilyttäväksi arvioidun yksilön, telepäätelaitteen tai paikan identifiointi ja sitten tuosta pisteestä lähtevän tai sinne saapuvan tietoliikenteen seuranta. Tämän ohella tarvitaan perinteistä henkilötiedustelua.

(2) Suojelupoliisille ehdotetut muut toimivaltuudet

Julkinen keskustelu tiedustelulakihankkeesta on keskittynyt tietoliikennetiedusteluun. Perusteellista arviointia – myös ihmisoikeusarviointia – tarvittaisiin myös ehdotuksista perustaa Suomeen sotilastiedusteluorganisaatio ja muuttaa poliisin osana toimiva suojelupoliisi täysiveriseksi tiedustelupalveluksi. Jälkimmäinen kysymys kuuluu nyt käsittelyssä olevan esityksen piiriin.

Kun suojelupoliisista ehdotetaan tehtäväksi tiedustelupalvelu, oikeutetusti se lakkaisi toimimasta rikosten esitutkintaviranomaisena. Demokraattisten yhteiskuntien perusratkaisuihin kuuluu, ettei tiedustelupalvelu pidätä tai vangitse ihmisiä tai säilytä heitä vapautensa menettäneinä.[9] Epädemokraattisten yhteiskuntien tiedustelupalvelujen väärinkäytökset – ulottuen mielivaltaisista vapaudenriistoista kidutukseen ja katoamisiin – saavat usein alkunsa siitä, että niillä on oikeus pidättää ihmisiä uhkana kansalliselle turvallisuudelle tai muusta syystä. Tiedustelupalvelun tulee turvautua poliisin virka-apuun jos se haluaa ehdottaa henkilön pidättämistä.

Tätä periaatetta ei ole johdonmukaisesti seurattu hallituksen esityksessä, kun poliisilain 5 lukuun salaisista tiedonhankintakeinoista on etsi-ja-korvaa -toiminnolla siirretty uusia mainintoja suojelupoliisista toimivaltuuksien käyttäjänä. Jotta saavutetaan sopusointu Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa, tuon luvun säännösten uskominen suojelupoliisin käyttöön sen lakatessa olemasta esitutkintaviranomainen pitäisi huolellisesti harkita kohta kohdalta.

Oman arvioni mukaan ainakin poliisilain 5 luvun 36 § (valeosto) ja 44 § (valvottu läpilasku) ja niihin liittyvät uuden 5 a luvun säännökset tulisi poistaa suojelupoliisin keinovalikoimasta, kun suojelupoliisi ei enää olisi esitutkintaviranomainen. Riskit tiedustelupalvelun muuttumisesta ”valtioksi valtiossa” ovat liian suuret ihmisoikeuksien kannalta. Sama koskee uutena toimivaltuutena ehdotettua asiakirjan (tms.) jäljentämistä siihen liittyvine säännöksineen (poliisilain 5 a luvun 28-34 §). Jäljentäminen kuuluu nykyisin pakkokeinolain mukaisiin toimivaltuuksiin eli tehtyjen rikosten tutkintaan, ja on siksi jo tästä syystä tullut harvoin suojelupoliisin sovellettavaksi (ks. s. 30). Säännöksille ei ole vastinetta poliisilaissa eli rikostorjunnan puolella. Kun nyt suojelupoliisi ei enää olisi esitutkintaviranomainen, on nurinkurista, että sille ehdotetaan itsenäisiä jäljentämistoimivaltuuksia. Nähdäkseni riskit ihmisoikeuksille ovat myös tässä asiassa liian suuret.

(3) Kansainvälinen yhteistyö siviilitiedustelussa

Poliisilain 5 a lukuun ehdotetaan otettavaksi 57 §:n säännös kansainvälisestä yhteistyöstä siviilitiedustelussa. Sen 1 momentin mukaan suojelupoliisi voisi ”tehdä yhteistyötä” ja ”hankkia tietoja yhdessä” ulkomaisten tiedustelu- ja turvallisuuspalvelujen kanssa. Ilmaisu ”hankkia tietoja yhdessä” käsittääkseni ilmaisee, että tietoa sekä vastaanotettaisiin että luovutettaisiin. Tehdessään tätä yhteistyötä ulkomailla suojelupoliisin olisi noudatettava asianomaisen yhteistyövaltion asettamia ehtoja ja rajoituksia (2 momentti). Vieraan valtion tiedustelu- ja turvallisuusviranomaisilla puolestaan olisi 3 momentin mukaan suojelupoliisin kanssa yhteistyötä tehdessään joukko toimivaltuuksia Suomessa (poliisilain

[9] Ks. YK:n ihmisoikeusneuvostolle terrorismin vastatoimien ihmisoikeusvaikutuksia arvioivana erityisraportoijana laatimani raportti hyvistä käytännöistä tiedustelupalvelujen ja niiden valvontamekanismien alalla, YK-asiakirja A/HRC/14/46, http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.46.pdf

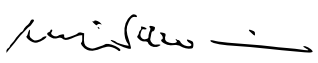
5 a luvun 9, 10, 18, 20 ja 24 §), joihin sisältyvät varsin ongelmallisesti mm. peitetoiminta (soluttautuminen) ja valeosto. Tiedustelupalvelun näkökulmasta voi tuntua houkuttelevalta käyttää tällaisiin operaatioihin ulkomaisten yhteistyökumppaneiden henkilöstöä, mutta ihmisoikeuksien kannalta on varsin ongelmallista uskoa noin arkaluontoisia tehtäviä ulkomaisten tiedustelupalvelujen agenteille, joiden ensisijainen lojaliteetti tietysti kohdistuu henkilön omaan maahan.

Suojelupoliisi voisi tietyin ehdoin luovuttaa tietoja ulkomaisille yhteistyökumppaneilleen (4 momentti). Nuo ehdot sisältävät viittauksia Suomen kansalliseen turvallisuuteen ja kansalliseen etuun, mutta ei esimerkiksi ihmisoikeuksien kunnioittamiseen. Perustelujen mukaan yhteys Suomen kansalliseen turvallisuuteen voi olla luonteeltaan välillinen, millä saatetaan viitata ns. oravannahkakauppaan eli Suomelle hyödyllisen tiedon hankkimiseen vaihtamalla sitä Suomella olevaan tietoon, jolla itsessään ei ole merkitystä Suomen kansallisen turvallisuuden kannalta. Henkilötietojen luovuttamista ulkomaille sovellettaisiin kuitenkin henkilötietojen käsittelystä poliisitoiminnassa annetussa laissa, joten ehdotettu 57 §:n 4 momentti ei koske yksilöityjä henkilötietoja.

Lakia henkilötietojen käsittelystä poliisitoimessa puolestaan ehdotetaan muutettavaksi mm. siten, että laajennetaan poliisin (ml. suojelupoliisi) oikeutta saada salassapitosäännösten estämättä ja myös teknisen käyttöyhteyden avulla tietoja erinäisistä henkilörekistereistä, jotka voivat sisältää arkaluontoisia henkilötietoja (13 §). Kansallisen turvallisuuden sisällyttäminen tiedonsaannin perusteisiin merkitsee tietosuojan merkittävää väistymistä suhteessa suojelupoliisiin. Saman lain 6 luvussa säännellään tietojen luovuttamista ulkomaille.

Sen paremmin ehdotetussa poliisilain 5 a luvun 57 §:ssä kuin henkilötietojen käsittelystä poliisitoiminnassa annetussa laissa ei ole ihmisoikeuksien suojalauseketta. Pidän sellaisen säätämistä välttämättömänä, jotta nyt tarkastellut kansainvälistä yhteistoimintaa ja suojelupoliisin laajennettua tiedonsaantia koskevat ehdotukset olisivat ihmisoikeuksien kannalta hyväksyttävissä. Laissa tulisi kieltää yhteistoiminta tai tietojen luovuttaminen, jos on perusteltua aihetta epäillä että ketään henkilöä tämän yhteistyön tai tietojen luovuttamisen vuoksi uhkaa kuolemanrangaistus, kidutus, muu ihmisarvoa loukkaava kohtelu, vaino, mielivaltainen vapaudenriisto tai epäoikeudenmukainen oikeudenkäynti.

Firenzessä 7.5.2018



Martin Scheinin, professori