Perustuslakivaliokunnalle

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

1. Johdannoksi

Perustuslain uusi 10 §:n 4 momentti tuli voimaan noin viikko sitten. Käsillä olevaa hallituksen esitystä on arvioitava tuota säännöstä vasten, mutta vain siltä osin kuin ehdotukset tarkoittavat luottamuksellisen viestin salaisuuteen kajoamista. Kaikissa muissa suhteissa perustuslaintasoinen oikeustila on säilynyt muuttumattomana. Vaikka kysymys tietoliikennetiedustelusta ja sen suhteesta luottamuksellisten viestien salaisuuteen on hallinnut julkista keskustelua, on heti alkuun todettava, että siviilitiedustelulakihanke on paljon laajempi ja tarjoaa merkittäviä valtiosääntöoikeudellisia haasteita myös monissa muissa suhteissa. Jäljempänä tarkasteltavat kysymykset ovat osin samoja, joihin kiinnitin huomiota 22.10.2018 päivätyssä lausunnossani hallituksen esityksestä laiksi sotilastiedustelusta ja eräiksi siihen liittyviksi laeiksi (HE 203/2017 vp). Korostan kuitenkin heti alkuun, että sotilastiedusteluhankkeen valtiosääntöoikeudelliset ongelmat ovat kertaluokkaa suurempia kuin käsillä olevan hankkeen. Tämä ei tarkoita, ettei käsillä olevaa hallituksen esitystä olisi korjattava sopusoinnun saavuttamiseksi perustuslain kanssa.

2. Luottamuksellisen viestin salassapitoon kajoamisen lähtökohdista: PL 10 §:n 4 momentti ja PeVM 4/2018 vp

Perustuslain 10 §:n muutoksella ei tietenkään ennalta hyväksytty nyt valiokunnankäsittelyssä olevien sotilas- ja siviilitiedustelulain sisältöjä perustuslain mukaisiksi. Perustuslakivaliokunta ei tuossa yhteydessä ottanut kantaa tiedustelulakiehdotusten sopusointuun perustuslain sanotun pykälän uudistetun sanamuodon kanssa vaan korosti sotilas- ja siviilitiedustelua koskevilla hallituksen

esityksillä olevan perustuslain muutoksen käsittelyssä ”lähinnä informatiivista merkitystä” (PeVM 4/2018 vp s. 4).

Perustuslain 10.4 §:ään kirjoitetun uuden rajoituslausekkeen ”on edelleen turvattava riittävästi luottamuksellisen viestin salaisuutta ja asetettava riittävän tiukat valtiosääntöiset rajat siihen puuttumiselle” (PeVM 4/2018 vp s. 5). Tuon perustuslainkohdan merkityksen arvioinnissa tiedustelulaeissa voi edelleenkin olla kyse vain luottamuksellisen viestin salaisuuteen kohdistuvista rajoituksista, ja PL 10.4 §:n rajoituslausekkeen tarkoituksena on turvata luottamuksellisen viestin salaisuutta liian pitkälle meneviltä rajoituksilta (sama). Valiokunta siis torjui käsityksen, jonka mukaan PL 10 §:n uusi 4 momentti merkitsisi luottamuksellisen viestin salaisuuden *dekonstitutionalisointia* suhteessa tiedustelu-toimintaan. Tämä oli erittäin tärkeä ja myönteinen ratkaisu, kun esimerkiksi itse pelkäsin perustuslain muutoksen johtavan tuollaiseen dekonstitutionalisointiin.

Mietinnössään valiokunta torjui hallituksen ehdottaman ”rikosten torjunnan” käsitteen ottamisen (tässä yhteydessä) osaksi PL 10.4 §:n säännöstä, koska asia vaatisi perusteellisempaa ja laajempaa selvitystyötä. Uusi perustuslainkohta siis viittaa edelleen ”rikosten tutkintaan”, millä ilmaisulla valiokunnan mukaan on voitu pitää ”myös sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei vielä olisi ehtinyt toteutuneen teon asteelle” (PeVM 4/2018 vp s. 6). Tästä ratkaisusta käsittääkseni seuraa, että siltä osin kuin tiedustelutoiminnan toimivaltuudet johtavat luottamuksellisen viestin salaisuuden rajoittamiseen, nuo rajoitukset on tyhjentävästi voitava oikeuttaa sen PL 10.4 §:n säännöksen nojalla, joka koskee *tiedon hankkimista* (… ”tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”). Rikosten tutkinnassa luottamuksellisen viestin salaisuuteen voidaan kajota laajemmin, mutta ei siis tiedustelutarkoituksessa ilman yhteyttä tehtyyn tai tekeillä olevaan rikokseen.

Sotilastiedustelua koskevan hallituksen esityksen arviointi valiokunnan mietinnössä keskittyi lausekkeeseen ”tiedon hankkimiseksi sotilaallisesta toiminnasta”, jonka tulee oikeuttaa perustuslain mukaisesti ne sotilastiedustelun toimivaltuudet, jotka merkitsevät puuttumista luottamuksellisen viestin salaisuuteen. Olen valiokunnalle antamassani lausunnossa tuosta hallituksen esityksestä eritellyt perustuslakivaliokunnan mietinnöstä (PeVM 4/2018 vp ss. 7-9) johdettavissa olevia lausekkeen soveltamista sotilastiedustelussa rajoittavia reunaehtoja, joista tärkein on, että tietoa voidaan hankkia vain ”sotilaallisesta toiminnasta”, millä tarkoitetaan *sotilaallisten joukkojen* (”sotilaallisesti järjestäytyneiden joukkojen” tai ”sotavoimaa käyttävien joukkojen”) toimintaa. Toisaalta sotilastiedustelussa *ei edellytä vakavaa uhkaa kansalliselle turvallisuudelle*, mikä on ymmärrettävä vain yhdessä sen kanssa, että valiokunta korosti tarvetta muutoin asettaa ”korkea kynnys” rajoituslausekkeen soveltamiselle, sen tulkitsemista ”suppeasti” ja perusoikeuksien yleisiin rajoitusedellytyksiin kuuluvaa välttämättömyysvaatimusta (PeVM 4/2018 s. 7).

Nyt tarkasteltavan siivilitiedustelulakiehdotuksen yhteydessä on huomionarvoista, että valiokunta varsin seikkaperäisesti käsitteli mietinnössään myös, mitä tarkoitetaan

kansallisella turvallisuudella ja siihen kohdistuvalla vakavalla uhalla, joihin siviilitiedustelun valtiosääntöoikeudellinen oikeutus kajota luottamuksellisen viestin suojaan tiedustelutarkoituksessa (siis ”tiedon hankkimiseksi”) pitää perustaa (ks. PeVM 4/2018 vp. ss. 8-9). Valiokunta mm. korosti, että kyseisellä turvallisuusuhalla tulee olla kytkentä Suomeen, että tiedustelu tulee keskittää vain harvojen erityisten tiedusteluviranomaisten käyttöön, että perusoikeuksien yleisiä rajoitusedellytyksiä tulee kunnioittaa ja että kansallisuuden turvallisuuden käsitettä tulee tutkia suppeasti ja samalla asettaa uhan vakavuuden kynnys korkealle. Erikseen painotettiin tarvetta seurata ja noudattaa sekä EU-tuomioistuimen että Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöä.

3. *Perustuslain 10 §:n 4 momentin nojalla toteutettavan arvioinnin asetelmasta käsillä olevassa asiassa*

Edellä esitetyistä lähtökohdista seuraa, että tietoliikennetiedustelun valtiosääntöoikeudellinen oikeutus pitää perustaa PL 10.4 §:n siihen kohtaan, joka koskee tiedon hankkimista sotilaallisesta toiminnasta, siltä osin kuin tiedustelua toteutetaan sotilastiedustelun omiin tarpeisiin ja toisaalta samassa perustuslainkohdassa tarkoitettuun vakavaan uhkaan kansalliselle turvallisuudelle silloin kun on kyse suojelupoliisin tietoliikennetiedustelusta. Asia voidaan havainnollistaa alla olevan taulukon muodossa.

Taulukko. Perustuslain 10 §:n 4 momentin tarjoama oikeutus tietoliikennetiedustelulle

Tiedonhankinnan kohde /Tiedusteluviranomainen	Sotilaallinen toiminta		Muu kansallista turvallisuutta uhkaava toiminta	
	Itsessään (ilman vakavaa uhkaa kansalliselle turvallisuudelle)	Jos muodostaa vakavan uhan kansalliselle turvallisuudelle	Ilman vakavaa uhkaa	Jos uhka on vakava
Sotilastiedustelu	**Sallittu**	**Sallittu**	Ei sallittu	*Ei sallittu*
Siviilitiedustelu	Ei sallittu	**Sallittu**	Ei sallittu	**Sallittu**

Asetelma on siten epäsymmetrinen. Tietoliikennetiedustelu siviilitiedustelussa edellyttää aina *vakavaa uhkaa* kansalliselle turvallisuudelle. Se voi periaatteessa kohdistua myös sotilaalliseen toimintaan, kunhan tuo ehto täyttyy. Sen sijaan sotilastiedustelu voi kohdistua vain *sotilaalliseen toimintaan*, mutta toisaalta ei edellytä vakavan uhan kynnystä – väljempi relevanssi Suomen (kansallisen) turvallisuuden kannalta riittää. Kun perustuslain 10 §:n 4 momenttia luetaan valiokunnan mietinnön PeVM 4/2018 vp valossa, sotilastiedustelun tietoliikennetiedustelu voi kohdistua vain sotilaalliseen toimintaan. Asia olisi voitu

toteuttaa toisinkin, luomalla sotilastiedustelulle perustuslaintasoinen oikeutus itsenäiselle toimivallalle tietoliikennetiedusteluun myös muun kuin sotilaallisen toiminnan seuraamiseksi, esimerkiksi jos kyse olisi Suomen maanpuolustuksen tai puolustusvalmiuden kannalta merkityksellisestä toiminnasta, joka samalla lisäksi muodostaa vakavan uhan kansalliselle turvallisuudelle. Vain vakavan uhan todentaminen oikeuttaisi sotilastiedustelun tiedonhankinnan muista toimijoista kuin sotilaallisista joukoista. Asia olisi edellyttänyt tarkkaa harkintaa muun muassa sen takia, että tiedusteluvaltuuksien uskominen sotilastiedustelulle nostaa esiin monia toiminnan johtoon, valvontaan ja parlamentaariseen katteeseen liittyviä kysymyksiä. Niiden vuoksi noiden toimivaltuuksien ulottaminen vähimmässäkään määrin kohdistumaan muuhun kuin sotilaalliseen toimintaan olisi vaatinut perinpohjaista sanamuotojen hienosäätöä jo perustuslain tasolla. Näin ei kuitenkaan tehty, ehkä sen takia, että sotilastiedustelun lainsäädännöllinen perusta on Suomessa aivan alkutekijöissään ja itse toimintaa peittää varsin kattava salassapidon verho.

4. Laki tietoliikennetiedustelusta siviilitiedustelussa PL 10 §:n 4 momentin kannalta

Pidän ehdotusta laiksi tietoliikennetiedustelusta siviilitiedustelussa (2. lakiehdotus) teknisesti hyvin valmisteltuna. Sen suuri ongelma on sotilastiedustelulakiehdotusta vastaava valinta tietoliikennetiedustelun toteuttamisesta myötävirtamenetelmän mukaisesti (*downstream*). Kun asian teknisen puolen eli valtakunnan rajan ylittävän tietoliikennekaapelin kytkennän ja liikenteen kopioinnin hoitaisi sotilastiedustelu myös siviilitiedustelun lukuun, muu ratkaisu siviilitiedustelussa ei ole käytännössä mahdollinen. ***Se on silti väärä ja samalla perustuslain kanssa ristiriitaan joutuva ratkaisu***.

Lakiehdotuksen soveltamisala- (1 §) ja määritelmäsäännökset (2 §) eivät edellytä myötävirtamenetelmää, mutta valinta on tehty sotilastiedustelulaissa ja kirjattu myös nyt arvioitavan lakiehdotuksen 7 §:n 1 momentin 5 kohtaan. Lakiehdotuksen keskeiset 3, 4, 5 ja 6 § on mielestäni onnistuneesti laadittu, mukaan lukien 4 §:n keskeinen edellytys vakavasta uhasta kansalliselle turvallisuudelle. Määritelmäsäännöksessä (2 §) tietoliikennetiedustelu on määritelty tavalla, joka sitoo sen luottamuksellisen viestin salaisuuteen kajoamiseen eli perustuslain 10 §:n 4 momentin alaan.

Ongelmakohta on siis ehdotettu 7 §, joka perustuu myötävirtamenetelmän valintaan. Kun tuo menetelmä ei tarjoa merkittävää hyötyä kansallisen turvallisuuden vakavien uhkien torjumisessa, se ei voi olla sen paremmin välttämätön kuin oikeasuhtainen tietoliikennetiedustelusta aiheutuvien perusoikeusrajoitusten kannalta. Siksi 7 § on väistämättä ristiriidassa perustuslain 10 §:n 4 momentin kanssa. Tuo ristiriita voidaan käsittääkseni ratkaista vain luopumalla myötävirtamenetelmästä tietoliikennetiedustelun teknisenä perusratkaisuna.

Toinen ongelma mainitussa 7 §:ssä on sen 1 momentin 4 kohdan säännös hakuehdoista, joka ei täytä perusoikeusrajoituksille asetettavia vaatimuksia sääntelyn laintasoisuudesta,

täsmällisyydestä ja tarkkarajaisuudesta. Hallituksen tiedustelulakipaketti ei missään sisällä kunnollista informaatiota siitä, mitä hakuehdoilla käytännössä tarkoitetaan. Jotain tiedämme siitä, mitä hakuehdot *eivät* saa olla, ja jotain niistä *tarkoitusperistä*, joita hakuehtojen valinnan taustalla olisi. Jos perustavampi ongelma tietoliikennetiedustelun menetelmän valinnasta onnistuttaisiin ratkaisemaan, hallituksen pitäisi esittää realistisia hypoteettisia esimerkkejä siitä, millainen voisi olla lupahakemukseen liitettävä *tyhjentävä luettelo* hakuehdoista. Olisiko esimerkiksi salausohjelmiston käyttö hyväksyttävä hakuehto? Tai viestin kieli tai siinä käytetty kirjaimisto?

Miksi tietoliikennetiedustelun toteuttaminen myötävirtamenetelmällä olisi virhe, josta seuraa sen perustuslainvastaosuus? Hallituksen tiedustelulakipakettiin on tiedustelutoiminnan kansainvälistä ja teknologiavetoista muotivirtausta seuraten omaksuttu tietoliikennetiedustelun menetelmäksi tietoliikennekaapelien viestivirran kopiointi myötävirtaan eli ns. *downstream*-menetelmä. Miljoonien viestien virrasta pyritään ensin algoritmien avulla ja sitten ihmisvoimin erottelemaan ne harvat, joiden varaan koko toiminnan oikeutus on rakennettu. Lakiehdotuksen säännökset toiminnan perustumisesta ”hakuehtojen käyttöön” eivät itsessään edellytä *downstream*-menetelmää, sillä hakuehtoja voitaisiin myös käyttää vastavirta- eli *upstream*-menetelmässä, jossa ensin *muilla keinoin kuin tietoliikennetiedustelulla* rajataan potentiaalisesti epäilyttävien viestijöiden (lähettäjiä tai vastaanottajia) joukko ja sitten hakuehtojen avulla analysoidaan heidän viestiliikennettään. Vastavirtamenetelmä on sekä tehokkuudeltaan että kielteisten perusoikeusvaikutusten minimoinnin kannalta ylivertainen myötävirtamenetelmään verrattuna. Se kohdentuu rajattavissa olevien potentiaalisten epäiltyjen joukkoon. Otan esimerkin ISIS:n inspiroimien ”yksinäisten susien” toteuttamista terrorismirikoksista läntisessä Euroopassa. Jos suojelupoliisilla on hyvien yhteiskuntasuhteiden, muiden viranomaisten ja tavallisten ihmisten vihjetietojen ja omien salaisten tiedonhankintakeinojensa perusteella vaikkapa tuhannen potentiaalisesti väkivaltaiseen terrorismiin suuntauneen henkilön seurantalista, heidän sähköpostiaan ja sosiaalisen median viestintäänsä voitaisiin tarkkailla algoritmien avulla siten, että saatuun hälytykseen kyetään reagoimaan minuuteissa tai tunneissa. Jos taas Suomen rajat ylittävän tietoliikennekaapelin koko viestivirtaa seurataan samassa tarkoituksessa, alustavien väärien hälytysten osuus on niin suuri, että esiin tulleet potentiaalisesti epäilyttävät viestit vaativat perinpohjaista ja aikaa vievää analyysia ennen kuin – valitettavan usein liian myöhään – päästään toiminnan asteelle.

Vastavirtamenetelmä ja perinteinen henkilötiedustelu ovat vuosina 2012-2015 johtamani SURVEILLE-tutkimushankkeen tulosten mukaan selvästi tehokkaampi keino esimerkiksi terroritekojen estämiseksi kuin myötävirtaan toteutettu tietoliikennetiedustelu. Vastavirtamenetelmän käyttö ei muodostu massavalvonnaksi sen takia, että siinä potentiaalisten epäiltyjen joukko perustuu muihin lähteisiin kuin tietoliikennetiedusteluun. Myötävirtamenetelmä taas edustaa eräänlaista kehäpäätelmää, jossa kohdennettu tietoliikennetiedustelu uskotaan voitavan perustaa kohdentavaan analyysiin, jonka lähtökohtana taas on viestivirran yleinen seuranta – siis massavalvonta.

Mainitussa 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 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 EU-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

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

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

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.

(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 myötävirtaan algoritmien avulla) *epäonnistuvat* turvallisuushyödyn tuottamisessa eivätkä läpäise ihmisoikeusrajoituksen oikeasuhtaisuuden vaatimusta, kun taas sähköisen viestinnän kohdennettu, vastavirtaan toteutettu valvonta (esim. yhden esimerkiksi henkilötiedustelun seurauksena valitun henkilön Facebook-yhteysverkoston pohjalta) tuottaa sekä paremman turvallisuushyödyn että asteeltaan hyväksyttävän ihmisoikeusrajoituksen.

Myötävirtamenetelmän valinta on tehty sotilastiedustelulakiehdotuksessa. Kun jo tiedusteluviranomaisten pääsy tietoliikennekaapeleihin 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, tuo tiedustelumenetelmä on itsessään sellainen, ettei se voi olla demokraattisessa yhteiskunnassa välttämätön mm. siten, että sen tuottamat turvallisuushyödyt olisi osoitettu ihmisoikeuksille aiheutuvaa haittaa suuremmiksi. Viittaan taas SURVEILLE-tutkimushankkeen tuloksiin ja kansainväliseen kokemukseen siitä, ettei tietoliikennetiedustelun myötävirtamenetelmä tuota todellista turvallisuushyötyä.

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 nyt ehdotettu tietoliikennetiedustelun teknologinen perusvalinta nähdäkseni hyvin mahtuu sen piiriin. Mainittakoon, että Britanniassa omaksuttiin uusi terminologia uuden tarkkailulainsäädännön (*Investigatory Powers Act 2016*) yhteydessä. Kohdennetun (*targeted*) viestien tarkkailun ohella lain terminologiaan kuuluu kategoria *bulk powers,* jonka voisi kääntää esimerkiksi *tukkutiedusteluksi*. Hallitus on pyrkinyt vakuuttamaan, että sen ehdotukset merkitsevät *kohdennettua* tietoliikennetiedustelua. Tätä

[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*.

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 tai vähintäänkin äsken mainitusta tukkutiedustelusta. Tarkkaan lukien tämä selviää myös hallituksen esityksistä, joissa ei puhuta kohdennetusta valvonnasta vaan siitä, kuinka tietoliikennetiedustelun avulla huomio kohdennetaan jatkoanalyysia vaativiin viesteihin. Kohdentaminen-termiä käytetään myös käsillä olevassa esityksessä. Myötävirtamenetelmässä tietoliikennetiedustelun alkuperäisenä kohteena on tietyn kaapelin 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. Hallitus siis ehdottaa: ei kohdennettua vaan *kohdentavaa* viestien tarkkailua, jonka lähtökohtana on massa- tai tukkuvalvonta ja jonka toteuttamistapa algoritmien avulla ja siis ihmissilmän näkemättä pyrkii lievittämään sivullisiin kohdistuvia perusoikeusvaikutuksia.

Niin sanotun massavalvonnan kielto seuraa perusoikeuksien yleisistä rajoitusedellytyksistä sovellettaessa perustuslain 10 §:n 4 momenttia. Tämä on kirjattu myös käsittelyssä olevaan hallituksen esitykseen: ”Uusi rajoitusperuste ei mahdollista yleisestä, kohdentamattomasta ja kaiken kattavasta tietoliikenteen seurannasta säätämistä” (s. 272).

SURVEILLE-tutkimushankkeen tulosten, Euroopan ihmisoikeustuomioistuimen liiketilassa olevan oikeuskäytännön, massavalvontaan hyvin kriittisesti suhtautuvien EU-tuomioistuimen ratkaisujen (*Digital Rights Ireland, Max Schrems, Tele2 & Watson*), Euroopan ihmisokeustuomioistuimen tuoreen *Big Brother Watch and Others v. UK* -ratkaisun sekä YK:n ihmisoikeuskomitean Yhdysvaltain ja Iso-Britannian maaraporttien käsittelyssä esittämien kannanottojen valossa katson, että ***sotilastiedustelulakiehdotuksessa ehdotettu tietoliikennetiedustelun perusratkaisu (myötävirtamenetelmä) tulisi hylätä ja tietoliikennetiedustelun toteutus rakentaa vastavirtaan toteutettavan tietoliikennetiedustelun pohjalta, jolloin lähtökohtana siis olisi muilla keinoin kuin tietoliikennetiedustelun kautta epäilyttäväksi arvioidun yksilön, telepäätelaitteen tai paikan identifiointi ja sitten tuosta pisteestä lähtevän tai sinne saapuvan tietoliikenteen kohdennettu seuranta. Tämä teknisen perusratkaisun muutos tietenkin edellyttäisi tarkistuksia myös nyt arvioitavan lakiehdotuksen tekstissä. Viittaan edellä mainittuihin 7 §:n 1 momentin 4 ja 5 kohtiin, jotka ainakin tulisi korjata.***

5. Kansainvälinen yhteistyö (poliisilain 5 a luvun 57 §)

Poliisilain ehdotettu 5 a luvun 57 § antaisi suojelupoliisille laajat toimivaltuudet vaihtaa tiedustelutietoja ulkomaisten tiedustelu- ja turvallisuuspalveluiden kanssa salassapitosäännösten estämättä ja osallistua tiedustelutietojen hankkimiseen ja arvioimiseen liittyvään kansainväliseen yhteistoimintaan. Säännöksen seurauksena

perusoikeuksien ja ihmisoikeuksien suoja (ensi sijassa yksityisyyden suoja ja tietosuoja) Suomessa saatettaisiin sivuuttaa suhteessa ulkomaiden tiedusteluviranomaisiin. Samoin suojelupoliisi saattaisi vastaanottaa yksityisyyden suojaa ja tietosuojaa loukkaavaa informaatiota taikka sellaista informaatiota, joka on hankittu ihmisoikeuksia loukkaamalla – jopa kidutuksella. Kidutuksen ja epäinhimillisen kohtelun kielto on merkityksellinen myös luovutettaessa tietoja Suomesta, koska on mahdollista, että tietojenvaihdon seurauksena joku joutuisi ulkomailla ihmisoikeusloukkauksen uhriksi – esimerkiksi kidutetuksi, vainotuksi, tuomituksi kuolemaan tai mielivaltaisen vapaudenriiston uhriksi. Tietojen luovuttamisen ehdoksi ehdotetaan hallituksen esityksessä vain, ettei se saisi olla ”vastoin kansallista etua”. ***Tähän tulisi ehdottomasti lisätä kielto luovuttaa tietoa, jos sen seurauksena saattaisi olla ihmisoikeuksien vakava loukkaus kuten esimerkiksi kidutus tai kuolemanrangaistus.***

Tietojenvaihdosta on tullut olennainen osa tiedustelupalvelujen toimintaa. Tämä merkitsee jatkuvaa riskiä siitä, että tiedustelu ei palvele suoraan maan omaa kansallista turvallisuutta vaan että tietoa hankitaan myös vaihdon välineeksi ja tiedustelupalvelun kansainvälisen arvostuksen kohottamiseksi. Myös Suomessa tiedustelulakihanketta on keskeisesti perusteltu sillä, että kun meidän lainsäädäntömme ei salli tietoliikennetiedustelua samassa laajuudessa kuin mikä on käytäntönä muualla (joskus jopa ilman lainsäädännöllistä perustaa), Suomi olisi ”jäänyt jälkeen” kansainvälisestä kehityksestä ja sen takia olisimme muiden maiden hyväntahtoisuuden varassa esimerkiksi terrorismin torjunnassa. Laajamittaista tietoliikennetiedustelua on siirrytty perustelemaan ns. oravannahka-kaupalla, jossa Suomella on – mm. maantieteellisen sijaintinsa takia – tarjottavanaan sellaista tiedustelutietoa, josta muut maat ovat valmiita ”maksamaan”.

Tämä perustelulinja on syvästi ongelmallinen. Se etäännyttää tiedustelutoiminnan ja sen yhteydessä tapahtuvat yksityisyyden suojaan ja muihin ihmisoikeuksiin kajoamiset tuon kajoamisen viimekätisestä hyväksyttävästä tarkoitusperästä, Suomen kansallisen turvallisuuden suojaamisesta. Samalla tiedustelun kohteena olevat ihmiset välineellistetään ”oravannahkakaupan” välikappaleiksi. Mitä etäisempi on tosiasiallisen tiedustelu-toiminnan yhteys välittömään hyötyyn Suomen kansalliselle turvallisuudelle, sen herkemmin sillä aiheutettavat kielteiset vaikutukset yksityisyyden suojalle ja muille ihmisoikeuksille ovat noiden oikeuksien kiellettyjä loukkauksia eivätkä hyväksyttäviä rajoituksia.

Lisäksi ”oravannahkakaupan” muodostuminen tiedustelutoiminnan moottoriksi uhkaa johtaa huomion ja voimavarojen väärään kohdentamiseen. Pahimmillaan suomalaisten turvallisuus *heikkenee*, kun todellisten tunnistettujen riskitekijöiden sijasta voimavarat suunnataan kansainvälisten tietoverkkojen loputtomaan kampaamiseen siinä toivossa, että sieltä löydettäisiin jotakin vaihdon välineeksi kelpaavaa ja Suomen tiedustelupalvelujen arvostusta ulkomaisten virkaveljien silmissä kohottavaa.

Edelleen 57 §:n 3 momentin mukaan vieraan valtion tiedustelupalveluilla tai vastaavilla viranomaisilla olisi suojelupoliisin niin päättäessä Suomen kanssa yhteistyötä tehdessään

joukko toimivaltuuksia Suomessa (poliisilain 5 a luvun 9, 10, 18, 20 ja 24 §). Näihin valtuuksiin sisältyvät varsin ongelmallisesti suunnitelmallinen tarkkailu (9 §), peitelty tiedonhankinta (10 §) peitetoiminta (18 §), valeosto (20 §) ja tietolähteen ohjattu käyttäminen (24 §). Sotilastiedustelun 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 heidän omaan maahansa ja jotka tehtävää suorittaessaan varmasti saisivat haltuunsa suojelupoliisin menetelmiä ja niiden heikkouksia koskevaa tietoa, jota pahimmillaan voitaisiin myöhemmin käyttää Suomen kansallista turvallisuutta vahingoittavalla tavalla.

Ehdotettu poliisilain 5 a luvun 57 § edellyttää merkittäviä korjauksia, jotta se olisi valtiosääntöoikeudellisesti hyväksyttävissä.

6. Poliisilain muutosten (1. lakiehdotus) muut perusoikeuskysymykset

Julkinen keskustelu tiedustelulainsäädännöstä on keskittynyt tietoliikennetiedusteluun, koska kyseessä on vilkkaan kansainvälisen keskustelun kohteena oleva asia ja samalla myös suomalaisten viranomaisten kannalta kokonaan uusi aluevaltaus, joka tietenkin edellyttää tarkkaa kansallista harkintaa ja valmistelua.

On kuitenkin aivan yhtä tärkeää, että suojelupoliisin harjoittaman tietoliikennetiedustelun oikeuttamisen rinnalla nyt käsittelyssä oleva hallituksen esitys merkittävissä suhteissa muuttaa poliisiorganisaation osana toimineen ja poliisille yleisesti kuuluvia toimivaltuuksia käyttävän suojelupoliisin muuttamista tiedustelupalveluksi. Tämä ratkaisu johtaa tärkeisiin rajanvetoihin yhtäältä poliisille kuuluvien rikostutkinnan ja rikostorjunnan toimivaltuuksien ja toisaalta tiedustelupalvelulle soveltuvien toimivaltuuksien välillä. Tiedustelupalvelu toimii pääosin ennakoivasti, keräten ja analysoiden tietoja tulevia tarpeita varten. Sen toiminta ei ole sidoksissa tehtyihin taikka tekeillä mahdollisesti oleviin rikoksiin. Kuten käsillä olevasta hallituksen esityksestä ilmenee, tiedustelupalvelun toiminta on keskeisesti sidoksissa kansallisen turvallisuuden suojaamiseen. Viittaan jo tässä yhteydessä poliisilakiin ehdotetun uuden 5 a luvun 1 §:n soveltamisalasäännökseen.

Viimeisten 30 vuoden aikana Suomessa on vähin erin laajennettu poliisin toimivaltuuksia, myös silloin kun ne merkitsevät kajoamista yksityisyyden suojaan tai muihin perusoikeuksiin. Kehityslinja avattiin tehtyjen rikosten tutkintaa varten (pakkokeinolaki ja esitutkintalaki) ja vähin erin samoja ja edelleen laajenevia toimivaltuuksia on siirretty myös poliisilain puolelle, siis rikostorjuntaan jossain määrin laajemmin kuin vain kohdistuen jo tehtyjen rikosten selvittämiseen. Samalla on luotu uusia kriminalisointeja mm. laajentamalla valmistelun rangaistavuutta rikoksena. Poliisiorganisaation osana suojelupoliisi on tullut osalliseksi yhä laajemmista toimivaltuuksista ilman, että missään vaiheessa olisi tehty huolellista harkintaa siitä, missä määrin rikostutkinnan ja rikostorjunnan toimivaltuudet ovat hyväksyttävästi ulotettavissa myös siviilitiedustelun

käyttöön. Valiokunnan käsittelyssä oleva siviilitiedustelulakiehdotus tarjoaa nyt mahdollisuuden näiden kysymysten perinpohjaiseen selvittämiseen ja pohdintaan.

Perustuslaintasoinen oikeustila on muuttunut vain perustuslain 10 §:n 4 momentin osalta, ja muutos koskee vain luottamuksellisen viestinnän suojan tarkkaan harkittua heikentämistä ”tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”. Perustuslain uusi säännös tarjoaa – edellyttäen, että perusoikeuksien yleisiä rajoitusedellytyksiä kunnioitetaan – oikeusperustan paitsi suojelupoliisin tietoliikennetiedustelulle myös suojelupoliisin muille tiedustelutoimintavaltuuksille, mutta vain siltä osin kuin ne kohdistuvat luottamuksellisen viestin salaisuuden murtamiseen ja joissa samalla on kyse tiedon hankkimisesta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Suojelupoliisin mahdollisille muille toimivaltuuksille on etsittävä oikeusperusta muualta kuin perustuslain 10 §:n 4 momentista. Kun tuo säännös on ainoa kohta perusoikeusluettelossa, jossa esiintyy kansallisen turvallisuuden käsite, oikeutusta noille muilla toimivaltuuksille on haettava kunkin perusoikeussäännöksen omista rajoituslausekkeista ja rajoitusedellytyksistä.

Nyt sanotusta seuraa, että ehdotettu poliisilain 5 a luvun 1 §:n soveltamisalasäännös on perustuslain kannalta ongelmallinen, kun siinä tiedonhankinta ”kansallisen turvallisuuden suojaamiseksi” esitetään yleisesti siviilitiedustelun lähtökohtana – siis ilman vakavan uhan edellytystä ja rajaamatta siviilitiedustelun toimivaltuuksia niihin, joissa on kysymys perustuslain 10 §:n 4 momentin alaan kuuluvasta luottamuksellisen viestin salaisuuden murtamisesta. Sama koskee saman luvun 4 §:n 1 momenttia, jossa vakava uhka kansalliselle turvallisuudelle on yleisesti esitetty kaikkien tiedustelumenetelmien käytön oikeutusperustana, vaikka se voi oikeuttaa vain luottamuksellisen viestin salaisuuteen kajoamisen.

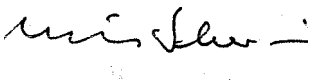
Kun mainitut 1 § ja 4 § ovat harhaanjohtavia ja voivat siksi käytännössä väärinkäsitysten vuoksi johtaa perusoikeuksien loukkaamiseen, pidän perusteltuna että 1 § korjattaisiin puhtaaksi soveltamisalasäännökseksi ja 4 § joko koskisi vain luottamuksellisen viestin salaisuuteen kajoamista taikka muotoiltaisiin uudelleen siten, että se yleisemmin viittaisi perusoikeuksien sallittuihin rajoituksiin.

Jos äsken mainitut säännökset korjataan, poliisilain 5 a luvun ehdotetut säännökset suojelupoliisin tiedustelutoiminnan toimivaltuuksista ovat nähdäkseni sinänsä pääosin hyväksyttävä. ***Valeostoa koskevan säännöksen (5 a luvun 20 §) ehdotan kuitenkin poistettavaksi***. Sen sijaan laajemmin ongelmallisena pidän tiedustelupalveluksi muuttuvan suojelupoliisin nimenomaista lisäämistä poliisilain 5 luvun (Salaiset tiedonhankintakeinot) moniin toimivaltuuksiin, myös sellaisiin, joille ei ole luontevaa ja hyväksyttävää käyttöalaa tiedustelupalvelun toiminnassa vaan, joissa tämän ennemmin tulisi turvautua poliisin virka-apuun. Perustuslakivaliokunnan tulisi lausunnossaan kattavasti käydä läpi kunkin toimivaltuuden perusoikeusvaikutukset, kunkin perusoikeuden hyväksyttävät rajoitusperusteet ja ne näkökohdat, joiden vallitessa rikostutkinnan ja -torjunnan toimivaltuudet ovat nyt ulotettavissa myös tiedustelutoiminnan käyttöön. Pidän

ongelmallisina ainakin seuraavia kahta säännöstä: ***Poliisilain 5 luvun 36 § (Valeostosta päättäminen) ja 44 § (Valvotusta läpilaskusta päättäminen).*** En näe näille säännöksille hyväksyttävää soveltamisalaa suojelupoliisin itsenäisessä käytössä.

Mainitut toimivaltuudet (tai suojelupoliisin lisääminen niiden käyttäjäksi) tulisi siis nähdäkseni poistaa poliisilain muutosehdotuksesta.

Firenzessä, 24 lokakuuta 2018



Martin Scheinin, professori (European University Institute)