Perustuslakivaliokunnalle

Pyydettynä lausuntona hallituksen esityksestä laiksi sotilastiedustelusta ja eräiksi siihen liittyviksi laeiksi (HE 203/2017 vp) esitän kunnioittavasti seuraavaa.

1. Johdannoksi

Perustuslain uusi 10 §:n 4 momentti tuli voimaan viikko sitten. Käsillä olevaa hallituksen esitystä on arvioitava tuota säännöstä vasten, mutta vain siltä osin kuin se tarkoittaa 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 sotilastiedustelulakihanke on paljon laajempi ja sisältää merkittäviä valtiosääntöoikeudellisia ongelmia monissa muissa suhteissa.

2. Yleinen perustuslakikysymys hallinnon perustumisesta lakiin (PL 2 ja 119 §)

Esityksen valtiosääntöoikeudellisesti tärkein ulottuvuus koskee sotilastiedusteluorganisaation perustamista Suomeen –- taikka laillisen oikeusperustan luomista sellaiselle ja samalla sitä koskevan sääntelyn valtiosääntöoikeudellisen moitteettomuuden varmistamista. Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin. Perustuslain 119 §:n 2 momentin mukaan valtionhallinnon toimielinten yleisistä perusteista on säädettävä lailla, jos niiden tehtäviin kuuluu julkisen vallan käyttöä. Valtionhallinnon yksiköistä voidaan muutoin säätää asetuksella. Nykyisin laki puolustusvoimista (551/2007) ja asetus puolustusvoimista (1319/2007) vaikenevat sotilastiedustelusta. Perustuslain 119 §:n 2 momentin tulkinnasta yhdessä 2 §:n 3 momentin kanssa viittaan valiokunnan tuoreeseen lausuntoon PeVL 24/2018 vp.

Nyt ehdotettu sotilastiedustelulaki on kovin niukkasanainen niistä asioista, joista äsken sanotun valossa tulisi säätää lailla. Varsin pitkälle oltaisiin –- epäasianmukaisesti –- lain 1 §:n soveltamisalasäännöksen varassa, vaikka tuo säännös vain luettelee asioita, joista laissa sitten jäljempänä säädetään -- tai tulisi säätää vaan ei säädetä. Ehdotetussa lain määritelmäpykälässä (9 §) ei ole nyt relevantteja määritelmiä Sen sijaan 10 §:ssä säädettäisiin, että sotilastiedusteluviranomaisia olisivat pääesikunta ja Puolustusvoimien tiedustelulaitos. Jälkimmäinen hoitaisi tiettyjä teknisluonteisia tehtäviä, kuten esimerkiksi tietoliikennekaapelin kytkennän suorittamisen (ks. 66 §). Pääosin esimerkiksi perusoikeuksiin kajoavat toimivaltuudet olisivat pääesikunnan käsissä.

Ehdotettu ratkaisu tarkoittaa läpinäkymättömän verhon luomista luonteeltaan salaiselle organisaatiolle, joka käyttäisi perusoikeuksiin merkittävässä määrin kajoavia toimivaltuuksia. Tämä seuraa useista hallituksen esityksestä nimenomaisesti tai implisiittisesti ilmenevistä ratkaisuista. Puolustushaarat olisi toiminnallisesti alistettu pääesikunnasta johdetulle sotilastiedustelulle, jolla olisi oma hierarkkinen organisaationsa ja joka siis tiedustelutoiminnan osalta syrjäyttäisi kunkin puolustushaaran oman käskyvaltahierarkian. Myös rajavartiolaitoksen rajajoukkoja voitaisiin kytkeä funktionaalisesti mukaan sotilastiedustelun alaisuuteen tasavallan presidentin asetuksella. Lakiehdotuksen 87 §:n mukaan muu puolustusvoimien virkamies voi funktionaalisesti olla sotilastiedustelun alainen ja käyttää lain tarjoamia tiedustelumenetelmiä. Sama koskisi 88 §:n mukaan reservin asevelvollisia kertausharjoituksissa. Jopa palveluksesta muodollisesti eronnut henkilö voisi 89 §:n nojalla käyttää sotilastiedustelun toimivaltuuksia ja päättää tiedustelumenetelmien käytöstä. Lakiehdotuksen 112 §:n mukaan sotilastiedustelun virkamiehen olisi joissain tilanteissa mutta ei suinkaan aina (ks. yksityiskohtaiset perustelut) ”pidettävä mukanaan” – ei siis näkyvissä – virkamerkkiä, ja pääesikunnan tiedustelupäällikkö päättäisi muista ”tunnisteista”, joiden avulla sotilastiedustelun virkamiehet voivat identifioida itsensä. Tämä säännös viitannee esimerkiksi koodikieliseen tunnussanaan.

Kyseessä olisi ensi sijassa salainen organisaatio, joka muuttaisi puolustusvoimien näkyvää organisaatiota ja sen käskyvaltasuhteita, antaisi perusoikeuksiin kohdistuvia toimivaltuuksia sellaisten henkilöiden käyttöön, joiden virkamiesasema on enemmän funktionaalinen kuin organisatorinen, ja tekisi ulkoisen valvonnan ja vastuunalaisuuden erittäin vaikeaksi. Viittaan julkisuudessa esillä olleeseen keskusteluun kaksoiskansalaisten mahdollisesta syrjinnästä puolustusvoimissa ja lainaan apulaisoikeusasiamiehen ratkaisua EOAK/652/2017:

> Pääesikunnan mukaan puolustusvoimissa ei ole pääesikunnan antamaa virallista ohjeistusta, norminantoa tai linjanvetoa koskien kaksoiskansalaisia varusmiehinä tai sotilasviroissa. Pääesikunnan mukaan oli kuitenkin käynyt ilmi, että joissain yksiköissä oli annettu jonkinlaista ohjausta siitä, miten kaksoiskansalaisuuden omaavien henkilöiden kanssa menetellään. Nämä olivat pääesikunnan mukaan yksittäisten virkamiesten omin päin laatimia ”soveltamisohjeita”.

Ymmärrän hyvin, että sotilastiedusteluun ja erityisesti vastatiedusteluun liittyy sen henkilöstön fyysiseen turvallisuuteen ja toimintaedellytyksiin liittyviä näkökohtia, jotka edellyttävät salassapitoa esimerkiksi sen suhteen, ketkä yksilöt kuuluvat sotilastiedusteluun. Tämä ei kuitenkaan tee oikeutetuksi perustuslain 2 ja 119 §:n kannalta, että koko organisaatio ja sen käskyvaltasuhteet piilotetaan näkyvistä niin tehokkaasti, ettei esimerkiksi tuomioistuimilla ja lainvalvojilla tulisi olemaan edes jälkeen päin mahdollisuutta selvittää, tehtiinkö jotakin sotilastiedusteluviranomaisen päätöksellä vai toimiko yksittäinen virkamies ”omin päin”, minkä selityksen pääesikunta esitti eduskunnan oikeusasiamiehelle kaksoiskansalaisia koskevassa asiassa.

3. Sotilastiedustelulakiehdotuksen 5-8 §§

Sotilastiedustelulakiehdotuksen 1 lukuun (Yleiset säännökset) sisältyy neljä pykälää, joilla nähtävästi on tavoiteltu laissa jäljempänä säädettäville toimivaltuuksille jonkinlaisia yleisiä ehtoja, jotka osaltaan ottaisivat huomioon perusoikeudet. Säännökset (tai kolme niistä) ovat huonosti laadittuja ja muodostuvat sen takia liki merkityksettömiksi yksittäisten toimivaltasäännösten arvioinnissa. Jos ne päätyvät esitetyssä muodossa lakiin, ne ovat perusoikeuksien kannalta vaarallisia, sillä ne ohjaisivat lain soveltajien huomioon vääriin kysymyksiin ja vääriin kriteereihin. Lainvalvojien ja tuomioistuinten olisi joka tapauksessa sovellettava perustuslakia oikein, kun toimivaltuuksien käyttö aikanaan tulee niiden arvioitavaksi. Tuossa kontekstissa nämä 1 luvun säännökset helposti loisivat olettaman, ettei sotilastiedusteluviranomainen ole soveltanut perustuslakia oikealla tavalla, kun kerran lain oma soveltamiskehikko poikkeaa perusoikeuksien rajoitusedellytyksistä. Kun sotilastiedustelulaki aikanaan tulee Euroopan ihmisoikeustuomioistuimen arvioitavaksi, nämä säännökset tulevat herättämään epäuskoa ja ihmetystä, millä tuskin on myönteinen vaikutus ulkoministeriön mahdollisuuksiin vakuuttaa ihmisoikeustuomioistuimen tuomarit sopusoinnusta Euroopan ihmisoikeussopimuksen kanssa.

5 §. *Suhteellisuusperiaate*. Säännösehdotuksen mukaan ”sotilastiedustelun toimenpiteiden on oltava puolustettavia suhteessa tiedon hankinnalla saatavien tietojen tärkeyteen sekä välttämättömyyteen ja tietojen saamisen kiireellisyyteen, tavoiteltavaan sotilastiedustelun päämäärään, sotilastiedustelun kohteeseen, muille tiedustelutoimenpiteen käytöstä aiheutuvaan oikeuksien loukkaamiseen sekä muihin asiaan vaikuttaviin seikkoihin”. Tämä ei ole ihmisoikeussopimusten ja perustuslain perusoikeussäännösten yhteydessä sovellettava suhteellisuusperiaate. Hyväksyttävä muotoilu voisi olla esimerkiksi:

> Sotilastiedustelun toimenpiteiden on oltava puolustettavia, kun verrataan keskenään tiedon hankinnalla saatavien tietojen merkitystä kansalliselle turvallisuudelle ja sen aiheuttamia oikeuksien rajoituksia, samalla varmistaen, että vastaava hyöty ei olisi saavutettavissa oikeuksia vähemmän rajoittavin keinoin ja ettei oikeuksien rajoituksilla loukata niiden olennaista sisältöä.

6 §. *Vähimmän haitan periaate.* Säännösehdotuksen mukaan ”sotilastiedustelun toimivaltuuden käytöllä ei kenenkään oikeuksiin saa puuttua enempää eikä kenellekään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi”. Tämä ei ole ihmisoikeussopimusten ja perustuslain perusoikeussäännösten yhteydessä sovellettava välttämättömyysperiaate. Ehdotettu säännös tarkoittaa sotilastiedustelun toimivaltuuksien *etusijaa* suhteessa perusoikeuksiin, ei perusoikeuksista seuraavaa reunaehdota niiden käytölle. Vain oikein muotoillun suhteellisuusperiaatteen kannalta oikeutettu hyöty tiedustelulla tavoitellun tarkoitusperän saavuttamiseksi (ks. muotoiluani edellä) voidaan osoittaa oikeutetuksi, vaikka siitä seuraa perusoikeuksien rajoittaminen vähimmässä välttämättömäksi osoitetussa määrin.

7 §. *Tarkoitussidonnaisuuden periaate*. Poiketen muista tämän jakson säännöksistä, tämä pykälä on onnistuneesti muotoiltu. Sen ongelmaksi kuitenkin muodostuu, ettei sotilastiedustelun yksittäisten toimivaltuuksien tarkoituksia ole määritelty lakiehdotuksessa. Siltä osin kuin toimivaltuudet kohdistuvat luottamuksellisen viestin salaisuuden murtamiseen, niiden tarkoituksena oletettavasti on PL 10 §:n 4 momentissa tarkoitettu tiedon hankkiminen sotilaallisesta toiminnasta. Lakiehdotukseen on kuitenkin kerätty valtava määrä muita toimivaltuuksia, joista aiheutuu eri perusoikeuksien rajoituksia luottamuksellisen viestin salassapidon murtamisen ohitse, eikä näille toimivaltuuksille ole esitetty tarkoitusperiä, joihin nähden 7 §:n säännöstä voitaisiin soveltaa.

8 §. *Syrjinnän kielto.* Säännös saattaa sitä sovellettaessa muodostua oikeutukseksi ihmisoikeussopimuksissa kielletylle syrjinnälle ja siten kääntyä tarkoitustaan vastaan. Tämä seuraa ”ainoastaan”-sanan sisällyttämisestä lainkohdan toiseen virkkeeseen. Tuo toinen virke voidaan yksinkertaisesti poistaa lakiehdotuksesta.

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

Perustuslain 10 §:n muutoksella ei tietenkään ennalta hyväksytty nyt käsittelyssä olevan sotilastiedustelulain sisältöä perustuslain mukaiseksi. Perustuslakivaliokunta ei 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 sotilastiedustelutoiminnan 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”).

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. Perustuslakivaliokunnan mietinnön (PeVM 4/2018 vp ss. 7-9) valossa lausekkeen soveltamista rajoittavat seuraavat reunaehdot:

1) Tietoa hankitaan vain ”sotilaallisesta toiminnasta”, millä tarkoitetaan *sotilaallisten joukkojen* (”sotilaallisesti järjestäytyneiden joukkojen” tai ”sotavoimaa käyttävien joukkojen”) toimintaa, ei esimerkiksi jonkin maan puolustusvalmiutta, sotilaallista varustautumista tai siihen liittyvää teollisuutta tai tuotekehittelyä yleisemmin.
2) Kyseiset sotilaalliset joukot voivat olla *valtiollisia tai ei-valtiollisia*, mahdollistaen siis sotilaallisiksi joukoiksi järjestäytyneiden terroristijärjestöjen sotilaallisen toiminnan seuraamisen signaalitiedustelun avulla. Lauseke ei kuitenkaan oikeuta ei-sotilaallisesti järjestäytyneen organisoidun rikollisuuden taikka terroristijärjestöjen propagandasta vaikutteita omaksuneiden erillisten toimijoiden (ns. yksinäiset sudet) seurantaa. Jälkimmäiset saattavat toki olla toimintaa, joka vakavasti uhkaa kansallista turvallisuutta ja siksi siviilitiedustelun oikeutettu kohde.
3) Säännös tiedon hankkimisesta sotilaallisesta toiminnasta *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).
4) Vaikka valiokunta mietinnössään liittää *välttämättömyysvaatimuksen* myös tiedon hankintaan sotilaallisesta toiminnasta ja siis sotilastiedusteluun, se ei tuossa yhteydessä toista niitä täsmentäviä näkökohtia, jotka samassa mietinnössä esitetään kansallisen turvallisuuden vakavan uhan ja siis siviilitiedustelun yhteydessä. Niitä ovat ehdot, jotka koskevat laintasoisen sääntelyn tyhjentävyyttä, perusoikeuksiin

vähemmän puuttuvien keinojen ensisijaisuutta, ja puuttumisen toteuttamista ”mahdollisimman kohdennetusti ja rajoitetusti”. Pidän selvänä, että nämä ehdot valiokunnan mietinnön rakenteesta huolimatta kuitenkin koskevat myös sotilastiedustelun toimivaltuuksia suhteessa luottamuksellisen viestin salaisuuteen.

5) *Tämä koskee myös kysymystä ns. massavalvonnan kiellosta*. Valiokunnalle perustuslain muutoksesta antamassani lausunnossa pidin aiheellisena, että perustuslakiin olisi otettu nimenomainen massavalvonnan kielto. Valiokunta ei kuitenkaan sisällyttänyt ehdotukseensa tuollaista kieltoa, eikä liioin käsitellyt perusteluissaan, mitkä seikat puhuisivat tuollaisen perustuslaintasoisen kiellon puolesta ja sitä vastaan. Tätä taustaa vasten katson, että ns. massavalvonnan kielto on ymmärrettävä osaksi toteutetun perustuslainmuutoksen sisältöä, koska hallituksen esityksissä vakuutettiin, etteivät sen paremmin perustuslain muutos kuin sotilastiedustelua tai siviilitiedustelua koskevat lakiehdotukset voisi tarkoittaa ns. massavalvontaa (ks. mm. käsillä olevan hallituksen esityksen ss. 352-353). Tämän vuoksi en pidä valtiosääntöoikeudellisesti merkityksellisenä, että valiokunnan mietinnössä massavalvonnan kielto näennäisesti esiintyy vain kansallisen turvallisuuden ja siis siviilitiedustelun yhteydessä (PeVM 4/2018 vp s. 8 ”… ehdotettu sääntely ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa”). Perusoikeusrajoitusten yleisistä ehdoista nimittäin seuraa, että tämän lausuman on ymmärrettävä yhtäläisesti koskevan myös tiedon hankintaa sotilaallisesta toiminnasta ja siis sotilastiedustelua. Käsillä olevassa hallituksen esityksessä onkin nimenomaisesti vakuutettu, ettei sotilastiedustelulain oikeuttamiseksi tarvittava perustuslain muutos ”mahdollista yleisestä, kohdentamattomasta ja kaiken kattavasta tietoliikenteen seurannasta säätämistä” (s. 352).

6) Kun uhkaa kansalliselle turvallisuudelle ei sotilaallisen toiminnan yhteydessä edellytetä (toisin kuin omassa lausunnossani valiokunnalle ehdotin), herää kysymys, mikä oikeastaan on sotilaalliseen toimintaan kohdistuvien valtuuksien oikeutus, siis se *hyväksyttävä tarkoitus*, joka mahdollistaa perusoikeusrajoituksen. Vastaus ei ole itsessään toiminnan sotilaallisessa luonteessa, ei sen ensi sijassa valtiollisessa luonteessa eikä tiedon hankkimisessa. Avainasemassa on tiedonhankinnan kohteeksi joutuvan toiminnan *relevanssi Suomen (turvallisuuden) kannalta*. Valiokunnan mukaan säännöksen soveltamisala rajoittuu tiedon hankkimiseen ”*Suomeen kohdistuvasta* sotilaallisesta toiminnasta taikka *Suomen turvallisuusympäristön kannalta merkityksellisestä* sotilaallisesta toiminnasta” (PeVM 4/2018 vp s. 7, korostukset lisätty). Kun Suomi aikanaan joutuu asiassa tilille Euroopan ihmisoikeustuomioistuimessa, sen on esitettävä Euroopan ihmisoikeussopimuksen kannalta hyväksyttävä tarkoitusperä sotilastiedustelun toimivaltuuksille. Suomen hallituksen vastauksena tulee olemaan, että toimivaltuudet ovat oikeutettuja ”kansallisen turvallisuuden vuoksi”, mitä ilmentää niiden rajoittaminen Suomeen kohdistuvaan tai Suomen turvallisuusympäristön kannalta muutoin merkitykselliseen sotilaalliseen toimintaan. Kansallisen turvallisuuden asema perusoikeusrajoituksen hyväksyttävänä tarkoitusperänä jäi kirjaamatta perustuslain tekstiin, mutta viimeistään ihmisoikeustuomioistuimen

edessä siihen joudutaan palaamaan toimivaltuuden viimekätisenä hyväksyttävänä tarkoitusperänä. Tämä tulee ottaa huomioon myös perustuslainkohtaa kansallisesti sovellettaessa, koska sopusointu Suomen ihmisoikeusvelvoitteiden kanssa kuuluu perusoikeusrajoitusten hyväksyttävyyden yleisiin ehtoihin.

7) Valiokunnan mietinnössä onkin asianmukaisesti korostettu, että myös sotilastiedustelun toimivaltuuksien on oltava *sopusoinnussa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa*, missä yhteydessä valiokunta korosti mm. riittävien oikeusturva- ja valvontajärjestelyjen välttämättömyyttä (PeVM 4/2018 vp s. 9).

Päädyn siihen, että perustuslakivaliokunnan mietinnön PeVM 4/2018 vp valossa luettuna sotilastiedustelun valtuuksia, siltä osin kuin ne kajoavat luottamuksellisen viestin suojaan, on arvioitava PL 10.4 §:n lausekkeen ”tiedon hankkimiseksi sotilaallisesta toiminnasta” kautta, missä operaatiossa yhteys kansalliseen turvallisuuteen on arvioinnin sisällöllinen osatekijä mutta ei arvioinnin varsinainen perustuslaintasoinen mittapuu. ”Vakavaa uhkaa” kansalliselle turvallisuudelle *ei edellytetä* (kuten siviilitiedustelussa), mutta perusoikeuksien yleisiin rajoitusedellytyksiin kuuluva sopusointu kansainvälisten ihmisoikeussopimusten kanssa edellyttää riittävää *kytkentää* kansalliseen turvallisuuteen, jotta tuossa yhteydessä sovellettava vakavaa uhkaa matalampi ”painavan yhteiskunnallisen tarpeen” (*pressing social need*) kynnys ylittyy.

Edellä sanotun vuoksi jätän siivilitiedustelulakiehdotuksen yhteyteen sen arvioinnin, mitä samassa perustuslainkohdassa tarkoitetaan kansallista turvallisuutta vakavasti uhkaavalla toiminnalla ja millaiset toimivaltuudet tuo lauseke oikeuttaa. Viittaan valiokunnalle lähipäivinä annettavaan erilliseen lausuntooni tuossa asiassa. Sotilastiedustelua ja siivilitiedustelua koskevat lakiehdotukset ovat kuitenkin sikäli kytköksissä toisiinsa, että sotilastiedustelulla olisi käytössään laitteisto ja tekniset valmiudet, joiden nojalla se käytännössä huolehtisi tietoliikennetiedustelusta myös suojelupoliisin lukuun, siis siviilitiedustelua varten. Nyt käsittelyssä olevan asian yhteydessä riittää todeta, että pidän perustuslain kannalta hyväksyttävänä, että sotilastiedustelu toimii suojelupoliisin alihankkijana silloin, kun suojelupoliisi harjoittaa tietoliikennetiedustelua perustuslain ja siviilitiedustelulain kannalta hyväksyttävällä tavalla.

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

Edellä esitetyistä lähtökohdista seuraa, että sotilastiedustelun toteuttaman 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 sotilastiedustelu toimii suojelupoliisin alihankkijana. Asia voidaan havainnollistaa alla olevan taulukon muodossa.

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

	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 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.

On kokonaan toinen – ja varsin valitettava – asia, ettei tuota perustuslain 10 §:n 4 momenttiin nyt kirjattua ja edellä esitetyssä taulukossa havainnollistettua rajanvetoa ole toteutettu valiokunnan käsittelyssä olevassa hallituksen sotilastiedustelulakiehdotuksessa. Vaikka tiedustelulakeja on valmisteltu pitkään ja eri hankkeita keskenään koordinoiden, lakiehdotukset on kuitenkin valmisteltu eri ministeriöissä ja eri ministereiden johdolla. Seurauksena on ollut, etteivät sotilastiedustelulakiehdotuksen eräät perusratkaisut ole sopusoinnussa perustuslain muutosta koskeneen esityksen ja juuri viikko sitten voimaan tulleen perustuslain muutoksen kanssa. Puolustusministeriö ja pääesikunta olisivat kipeästi tarvinneet parempia juristeja kuin mitä niillä on ollut käytössään. Ongelmat jäävät nyt

eduskunnan korjattaviksi, eikä tällöin voida luottaa siihen, että puolustushallinnosta nyt löytyisi se valtiosääntöoikeudellinen asiantuntemus, jota siellä ei aikaisemmassa vaiheessa ollut. Näyttää vahvasti siltä, että sotilastiedustelun toimivaltuuksia joudutaan karsimaan varsin kovalla kädellä.

Jos valiokunta nyt haluaa lukea perustuslain 10 §:n 4 momentin säännöstä toisin kuin vain muutama viikko sitten, ja hakea osalle sotilastiedustelun itsenäisistä toimivaltuuksista oikeutuksen perustuslainkohdan viittauksesta vakavaan uhkaan kansalliselle turvallisuudelle, tämä toki mahtuisi perustuslainkohdan sanamuodon puitteisiin. Se kuitenkin heikentäisi valiokunnan uskottavuutta asiassa, joka on laajan yhteiskunnallisen keskustelun kohteena. Perustuslain muutos vietiin läpi siinä uskossa, että sotilastiedustelun tietoliikennetiedustelu tulee kohdistumaan vain sotilaalliseen toimintaan. Jos tuosta muutoksesta nyt halutaan oikeutus sotilastiedustelun laajemmille tiedusteluvaltuuksille, tarvitaan tarkkaa ja huolellista erittelyä siitä, mitkä sotilastiedustelun tietoliikennetiedustelun toimivaltuudet kohdistuvat vain sotilaalliseen toimintaan ja mitkä puolestaan halutaan oikeuttaa kansallisen turvallisuuden ja siihen kohdistuvan vakavan uhan käsiteparin kautta.

6. Esityksen arviointi PL 10 §:n 4 momentin kannalta

Siirryn nyt arvioimaan niitä sotilastiedustelulakiesityksen kohtia, jotka tarkoittavat luottamuksellisen viestin salassapidon murtamista sotilastiedustelun muin toimenpitein kuin niiden, joissa se toimii suojelupoliisin eli siviilitiedustelun alihankkijana. Niitä ovat ensi sijassa 63-69 §§:n säännökset tiedon hankinnasta tietoliikenteestä, mutta myös eräät muut säännökset: 32 § (telekuuntelu), 33 § (tietojen hankkiminen telekuuntelun sijasta), 35 § (televalvonta), 37 § (tukiasematietojen hankkiminen) ja 58 § (radiosignaalitiedustelu).

Jos nämä toimivaltuudet halutaan antaa sotilastiedustelun käyttöön, ne on rajoitettava koskemaan tiedon hankintaa valtiollisten tai ei-valtiollisten sotilaallisten joukkojen toiminnasta. Muilta osin perustuslain 10.4 § ei voi toimia näiden toimivaltuuksien oikeutuksena. Jos kyse olisi tapahtuneen rikoksen tutkinnasta tai tekeillä olevaksi epäillyn yksilöidyn rikoksen torjunnasta, sotilastiedustelu saatettaisiin kytkeä siihen lainsäätäjän päätöksellä mukaan. Mutta tuollaisia kynnyksiä ei ole säännöksiin rakennettu. Jos kyse on vakavasta uhasta kansalliselle turvallisuudelle mutta ei sotilaallisten joukkojen toiminnasta, mainitut toimivaltuudet saattavat tämän vuoksi olla hyväksyttäviä myös tiedustelutoiminnassa, mutta niiden käyttö tulee uskoa siviilitiedustelulle eli suojelupoliisille.

Kaikkia edellä lueteltuja säännöksiä tulee korjata siten, että toimivaltuus voi kohdistua vain tiedon hankkimiseen sotilaallisesta toiminnasta, jos toimivaltuudet todella halutaan uskoa sotilastiedustelun käyttöön.

Siirryn nyt tarkastelemaan esityksen ydinkysymystä, sotilastiedustelun tietoliikennetiedustelua (63-69 §), rajaten pois sotilastiedustelun toiminnan lailliseksi

oletetun siviilitiedustelun alihankkijana (70 §). Ymmärrän, että 63 ja 64 § ovat alisteisia seuraavissa pykälissä määritellyille varsinaisille toimivaltuuksille enkä näe niissä itsenäisiä ongelmia, jos varsinaiset toimivaltuudet saadaan lailliselle tolalle.

Lakiehdotuksen 65 §:ään ja 67 §:ään olisi perustuslain 10.4 §:n takia välttämätöntä lisätä rajaus, jonka mukaan toimivaltuus voi koskea vain tiedon hankkimista sotilaallisesta toiminnasta eli valtiollisten tai ei-valtiollisten sotilaallisten joukkojen toiminnasta.

Vaikka sotilastiedustelun tietoliikennetiedustelun kohteena mm. lupamenettelyssä olisi sotilaallinen toiminta, tiedustelun toteuttamistavalla voi silti olla merkittäviä perusoikeusvaikutuksia ohi toiminnan hyväksyttävän kohteen. Tämä seuraa siitä, että lakiehdotukseen on tiedustelutoiminnan kansainvälistä ja teknologiavetoista muoti-virtausta seuraten omaksuttu tietoliikennetiedustelun menetelmäksi tietoliikennekaapelien viestivirran kopiointi myötävirtaan eli ns. *downstream*-menetelmä. Miljoonien viestien virrasta pyritään algoritmien avulla erottelemaan ne harvat, joiden varaan koko toiminnan oikeutus on rakennettu. Lakiehdotuksen 65 ja 67 §§:ssä esiintyvät säännökset toiminnan perustumisesta ”hakuehtojen käyttöön” eivät itsessään edellytä *downstream*-menetelmää, sillä hakuehtoja voitaisiin myös käyttää vastavirta- eli *upstream*-menetelmässä, jossa ensin 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. 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 voidaan 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.

Tässä 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

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

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 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.

Myötävirtamenetelmän valinta on tehty lakiehdotuksen 66 ja 68 §§:ssä. 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 tietoliikennetiedustelu 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 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 äsken mainitusta tukkutiedustelusta. Tarkkaan lukien tämä selviää myös ehdotetusta lakitekstistä, jossa ei puhuta kohdennetusta valvonnasta vaan siitä,

[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*.

kuinka tietoliikennetiedustelun avulla huomio kohdennetaan jatkoanalyysia vaativiin viesteihin. Kohdentaminen-termiä käytetään ainakin 68 §:n 3 momentissa. 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. 352-353).

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 **66 ja 68 §§:ssä *ehdotettu tietoliikennetiedustelun perusratkaisu (myötävirtamenetelmä) tulisi hylätä ja tietoliikennetiedustelun toteutus 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***.

7. Kansainvälinen yhteistyö (19 §)

Lakiehdotuksen 19 § antaisi sotilastiedusteluviranomaisille 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 sotilastiedusteluviranomaisiin. Samoin Suomen sotilastiedustelu saattaisi vastaanottaa yksityisyyden suojaa ja tietosuojaa loukkaavaa informaatiota muualla taikka 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. Pykälän viimeisen momentin mukaan tietojen luovuttamisessa ja vastaanottamisessa olisi kuitenkin noudatettava, ”…mitä siitä erikseen Suomea

velvoittavissa kansainvälisissä sopimuksissa määrätään…". Tämä lauseke olisi helposti korjattavissa ihmisoikeuksia suojaavaan muotoon kirjoittamalla se muotoon: "…Suomea velvoittavia kansainvälisiä sopimuksia…". Ihmisoikeussopimuksissa ei "erikseen määrätä" kansainvälisestä tietojenvaihdosta, mutta niistä kyllä seuraa Suomelle velvoitteita, jotka on otettava huomioon tietojenvaihdossa. Mietinnön laativaa puolustusvaliokuntaa tulisi evästää selventämään perusteluissa, että uudelleen muotoilu lauseke kieltää yhteistoiminnan tai tietojen luovuttamisen, 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. Viittaan ulkoasiainvaliokunnan jo antamaan lausuntoon asiassa.

Tietojenvaihdosta on tullut olennainen osa siviili- ja sotilastiedustelupalvelujen toimintaa. Tämä merkitsee jatkuvaa riskiä siitä, että tiedustelun kohdentaminen 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. oravannahkakaupalla, 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 "oravannauhkakaupan" 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 sotilastiedustelun arvostusta ulkomaisten virkaveljien silmissä kohottavaa.

Edelleen 19 §:n 3 momentin mukaan vieraan valtion tiedustelu- ja turvallisuusviranomaisilla puolestaan olisi 3 momentin mukaan Suomen sotilastiedustelun kanssa yhteistyötä tehdessään joukko toimivaltuuksia Suomessa (lakiehdotuksen 20, 22, 41,

45, 49, ja 63 §). Näihin valtuuksiin sisältyvät varsin ongelmallisesti mm. peitelty tiedonhankinta (22 §) peitetoiminta (ml. soluttautuminen, 41 §), valeosto (45 §) ja tietolähdetoiminta (49 §). 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.

Lakiehdotuksen 19 § edellyttää merkittäviä korjauksia, jotta se olisi valtiosääntöoikeudellisesti hyväksyttävissä.

8. 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 tietoliikennetiedustelun rinnalla nyt käsittelyssä oleva hallituksen esitys luo laintasoisen pohjan tähän asti Suomesta puuttuneelle tai Suomessa ilman laintasoista sääntelyä toimineelle sotilastiedustelulle. Tässä lausuntoni viimeisessä jaksossa tarkastelen kysymystä siitä, mitä muita perusoikeuskysymyksiä sotilastiedustelun virallistaminen ja laillistaminen herättää luottamuksellisten viestin salassapidon murtamisen ohella. Noiden muiden perusoikeusrajoitusten valtiosääntöoikeudellinen oikeutus joudutaan hakemaan muualta kuin juuri säädetystä perustuslain 10.4 §:stä. Valitettavasti hallituksen esitykseen sisältyy useita ehdotettuja toimivaltuuksia, joille ei ole perustuslain kannalta hyväksyttävää oikeusperustaa.

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 erillinen siviilitiedustelulakiehdotus tarjoaa nyt mahdollisuuden näiden kysymysten perinpohjaiseen selvittämiseen ja pohdintaan.

Nyt on kuitenkin kyse sotilastiedustelusta. Ehdotettu sotilastiedustelulaki on laaja (116 §§) suurelta osin juuri sen vuoksi, että tehtyjen rikosten tutkinnan ja tekeillä oleviksi epäiltyjen rikosten torjunnan tarpeisiin vähin erin luotu mittava keinovalikoima ehdotetaan nyt

kertarysäyksellä annettavaksi sotilastiedustelun käyttöön ilman tehtyihin tai tekeillä oleviin rikoksiin liittyvää kytkentää, viime kädessä vain tiedon hankkimiseksi tai tilannekuvan muodostamiseksi. Tämä ei ole perusoikeuksien kannalta hyväksyttävää.

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”.

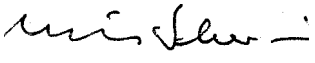
Edellä sanotun perusteella katson, että alla luetellut toimivaltuudet tulee tämän esityksen käsittelyssä poistaa sotilastiedustelulaista. Jos jotkin niistä voidaan osoittaa välttämättömäksi ja perusoikeuksien kannalta hyväksyttäväksi, sotilastiedustelulakia voidaan myöhemmin täydentää uusilla toimivaltuuksilla. Tämä vastaisi sitä vähittäisten muutosten etenemistapaa, jota poliisin valtuuksien laajentamisessa on seurattu.

20 §. *Tarkkailu ja suunnitelmallinen tarkkailu*. Toimivaltuudet eivät rajoitu luottamuksellisiin viesteihin, sillä ainakin perustuslain 10 §:n 1 momentin yleislauseke ja 3 momentti, jonka osalta eduskunta hylkäsi hallituksen ehdottaman muutoksen, ovat niiden kohteina.
21 §. *Peitelty tiedonhankinta*. Äsken sanottu koskee tätä toimivaltuutta.
24 §. *Tekninen kuuntelu.* Vaikka toimivaltuus osittain kohdistuu luottamuksellisiin viesteihin, myös perustuslain 10 §:n 1 ja 3 momentit olisivat rajoituksen kohteina.
26 §. *Tekninen katselu.* Viittaan 20 §:n yhteydessä äsken sanottuun.
28 §. *Tekninen seuranta.* Viittaan 20 §:n yhteydessä äsken sanottuun, minkä lisäksi on syytä mainita perustuslain 9 § (liikkumisvapaus), 11 § (uskonnon ja omantunnon vapaus), 12 § (sananvapaus), 13 § (kokoontumis- ja yhdistymisvapaus) ja 15 § (omistusoikeus). Paikkatietoa sotilastiedustelulle lähettävän laitteen sijoittaminen esimerkiksi henkilön autoon kajoaa merkittävällä tavalla kaikkien näiden perusoikeuksien käyttöön.
30 §. *Tekninen laitetarkkailu*. Ks. edellä 24 §:n yhteydessä sanottua.
40 §. *Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen*. Nämä ns. hacking-valtuudet ovat eräs koko lakiehdotuksen kaikkein syvimmistä kajoamisista perusoikeuksiin. En näe valtiosääntöistä oikeutusta näiden valtuuksien antamiseen sotilastiedustelulle. Jos näistä valtuuksista ylipäätään pitää säätää, ne tulisi varata rikostorjuntaan. Toimivaltuus kohdistuu yksityisyyden suojaan ohi luottamuksellisen viestin salaisuuden, mukaan lukien kotirauhan suojaan (PL 10 §), sekä omaisuuden suojaan (PL 15 §) ja välillisesti muihin perusoikeuksiin kuten esimerkiksi sananvapaus (12 §).
41 §. *Peitetoiminta*. Viittaan 20 §:n yhteydessä sanottuun, mutta myös 28 §:n yhteydessä sanottuun, koska peitetoiminnalla voi olla vaikutuksia moniin perusoikeuksiin.
45 §. *Valeosto*. Viittaan äsken sanottuun. Erityisesti PL 15 § (omistusoikeus) on tässä yhteydessä relevantti PL 10 §:n ohella.
49 §. *Tietolähdetoiminta*. Toimivaltuus on ongelmallinen yksityisyyden suojan (PL 10 §) kannalta, koska siihen voi liittyä viranomaisen tahallinen toiminta toiminnan kohteiden yksityiselämän suojan murentamiseksi. Se voi vaikuttaa myös perustuslain 11, 12 ja 13 §:ssä turvattujen perusoikeuksien rajoituksena.

52 §. *Paikkatiedustelu.* Nämä valtuudet vaikuttavat lähinnä PL 10 §:n rajoituksena, mukaan lukien kotirauhan suojan osalta.
54-55 §. *Jäljentäminen ja lähetyksen jäljentäminen*. Nämä toimivaltuudet kajoavat mm. yksityisyyden suojaan (PL 10 §) ja omaisuuden suojaan (PL 15 §).
60 §. *Ulkomaan tietojärjestelmätiedustelu.* Tämä toimivaltuus kohdistuu osin luottamuksellisen viestin salassapitoon ja on siltä osin PL 10.4 §:n ja sen uuden rajoituslausekkeen alalla. Mutta kun valtuuden käyttö ei rajoitu tietojärjestelmästä lähteviin tai sinne saapuviin viesteihin, se kohdistuu yksityisyyden suojaan (PL 10 §) myös yleisemmin, samoin kuin sananvapauteen (PL 12 §) ja omaisuuden suojaan (PL 15 §).
72 §. *Sotilastiedustelun suojaaminen*. Viittaan edellä 41 §:n (peitetoiminta) yhteydessä sanottuun.

Kaikki nämä toimivaltuudet tulisi siis nähdäkseni poistaa sotilastiedustelulakiehdotuksesta.

Firenzessä, 22 lokakuuta 2018



Martin Scheinin, professori (European University Institute)