Kirjallinen lausunto
Niklas Vainio

Perustuslakivaliokunnalle

Hallituksen esitys 202/2017 vp eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi

1 Arvioinnin lähtökohdat

Hallituksen esitys on osa tiedustelulainsäädäntöä koskevaa kokonaisuutta, jossa säädettäisiin siviili- ja sotilastiedustelusta sekä tiedustelun valvonnasta. Esityksessä ehdotetaan muun muassa säädettäväksi uusi laki tietoliikennetiedustelusta siviilitiedustelussa (jäljempänä tietoliikennetiedustelulaki) sekä muutettavaksi poliisilakia niin, että siihen lisättäisiin uusi 5 a luku, jossa säädettäisiin tiedustelumenetelmistä ja niiden käytöstä siviilitiedustelussa.

Ehdotettu laki sisältää useita viranomaistoimivaltuuksia, joilla rajoitettaisiin niiden kohteiden perusoikeuksia. Perusoikeusrajoitus kohdistuisi muun muassa perustuslain 10 §:ssä suojattuihin luottamuksellisen viestin suojaan, kotirauhan suojaan ja henkilötietojen suojaan. Osalla ehdotetuissa valtuuksista on yhteys liikkumisvapauteen (9 §).

Perustuslain 10 §:n 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. 15.10.2018 voimaan tulleella lailla (817/2018) perustuslakiin on lisätty 10 §:n 4 momentti, jonka mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Perustuslain muutosta koskevassa mietinnössään (PeVM 4/2018 vp) perustuslakivaliokunta totesi, että luottamuksellisen viestin salaisuuden suojan rajoittamiselle asetettaisiin hallituksen esityksen yleisperusteluiden (s. 31) mukaan korkea kynnys. Säännös rajoittaisi sitä, millä edellytyksillä tiedustelutoimivaltuuksista voitaisiin säätää. Säännöksessä mainittavasta ja perusoikeuksien yleisiin rajoitusedellytyksiin kuuluvasta välttämättömyysvaatimuksesta seuraa perustuslakivaliokunnan mielestä, että luottamuksellisen viestin salaisuuden suojaan puuttumisen tulee olla mahdollisimman kohdennettua ja rajattua. Tämä tarkoittaa muun ohella sitä, että tavallisen lain tasoisessa sääntelyssä on huolehdittava tiedonhankintatoimivaltuuksien yksilöimisestä. Ehdotettu sääntely ei hallituksen

esityksen mukaan mahdollistaisi "yleisestä, kohdentamattomasta ja kaiken kattavasta tietoliikenteen seurannasta säätämistä".

Säännöksen soveltamisrajoituksista perustuslakivaliokunta korosti, että ensinnäkin tiedonhankinta kansallista turvallisuutta uhkaavasta toiminnasta voitaisiin säännöksen perusteella osoittaa vain kansallisesta turvallisuudesta huolehtivien viranomaisten (nykyisin suojelupoliisi, pääesikunta ja puolustusvoimien tiedustelulaitos) tehtäväksi. Toiseksi rajoitusedellytys koskisi vain tiedon hankkimista sellaisesta toiminnasta, joka luonteensa takia voi muodostua vakavaksi uhkaksi kansalliselle turvallisuudelle. Kolmanneksi lailla tulee säätää tyhjentävästi toimivaltuuksien kohdentumisesta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Neljänneksi ehdotettu sääntely ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa.

2 Siviilitiedustelun käyttöedellytykset

Kansallisen turvallisuuden käsite. Perustuslain muutosta koskevassa perustuslakivaliokunnan mietinnössä (PeVM 4/2018 vp) valiokunta totesi, että kansallinen turvallisuus ja vakava uhka ovat sisällöltään varsin laaja-alaisia käsitteitä. Valiokunnan mukaan kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitettaisiin säännöksessä kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä tai kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Edellytyksenä olisi se, että toiminnalla olisi jokin kytkentä Suomeen ja että se uhkaisi nimenomaan Suomen kansallista turvallisuutta, vaikka toiminta voisikin maantieteellisesti tapahtua Suomen rajojen ulkopuolella. Kyse voisi olla esimerkiksi Suomen kansallista turvallisuutta vakavasti uhkaavasta terrorismiin liittyvästä toiminnasta, väkivaltaisesta radikalisoitumisesta tai ulkomaisten tiedustelupalvelujen toiminnasta taikka Suomen turvallisuuden kannalta keskeisen valtion levottomuuksista.

Poliisilain 5 a luvun 3 §:ssä ja tietoliikennetiedustelulain 3 §:ssä säädettäisiin kohteista, joista tiedustelulla saataisiin hankkia tietoa. Nämä luettelot vastaavat valiokunnan mietinnössä kuvattuja lähtökohtia siitä, millainen toiminta voi uhata kansallista turvallisuutta.

Yleiset edellytykset. Ehdotuksen mukaan tiedustelumenetelmien käyttämisen yleisenä edellytyksenä olisi, että niillä voidaan perustellusti olettaa saatavan tietoja sellaisesta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta (poliisilain 5 a luvun 4 § ja tietoliikennetiedustelulain 4 §). Säännöksissä lueteltuja, yksityiselämän suojaan puuttuvia tiedustelumenetelmiä saisi käyttää vain, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi 1 momentissa tarkoitetusta toiminnasta. Peitotoiminta ja valeoston käyttäminen edellyttäisi lisäksi, että menetelmän käyttö on välttämätöntä (PolL 5 a:4 §). Välttämättömyys olisi edellytyksenä myös muuhun kuin valtiolliseen toimijaan kohdistuvan tietoliikennetiedustelun käyttämiseksi (tietoliikennetiedusteluL 4 §).

Esitettyjä yleisiä edellytyksiä voi pitää suhteellisen tiukkoina. Perustuslain muutosta koskevassa mietinnössään valtiosääntöoikeudellisen tulkinnan lähtökohtana valiokunta tähdensi sitä, että perustuslaista johtuu tarve yhtäältä tulkita kansallisen turvallisuuden käsitettä suppeasti sekä toisaalta asettaa uhan vakavuusaste korkealle. Rajoitusperusteeseen vetoavalla on myös velvollisuus

esittää riittävät perustelut sille, että jokin toiminta voi muodostua vakavaksi uhaksi kansalliselle turvallisuudelle.

Välttämättömyys. Ehdotuksen mukaan vain osassa tiedustelumenetelmiä edellytyksenä olisi "välttämättömyys". Kuitenkin perustuslain 10 §:n 4 momentin mukaan luottamuksellisen viestinnän suojaan tehtävien rajoitusten on oltava välttämättömiä. Siten herää kysymys, tulisiko kaikkien tiedustelumenetelmien käyttöedellytyksiin kirjata menetelmän käytön "välttämättömyys". Aiemmassa tulkintakäytännössä näin ole edellytetty (esimerkiksi pakkokeinolakia ja poliisilakia koskevat lausunnot PeVL 66/2010 vp ja PeVL 67/2010 vp).

Valiokunnan mietinnön mukaan välttämättömyys-kriteeri tarkoittaa, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti. Valiokunta korosti muutenkin perusoikeuksien yleisten rajoitusedellytysten merkitystä uutta ehdotettua rajoitusperustetta tulkittaessa. Valiokunta myös viittasi siihen, että välttämättömyyttä on harkittava kussakin yksittäistapauksessa. Mietinnön mukaan välttämättömyysvaatimuksen täyttymiseksi ei riitä, että tiedon hankkimisen luottamuksellisista viesteistä voidaan yleisesti katsoa edistävän kansallista turvallisuutta. Sen sijaan on osoitettava, että tiedon hankkiminen kussakin yksittäistapauksessa ja siihen liittyvät yksilökohtaiset perusoikeuksien rajoitukset ovat tehokkaita ja välttämättömiä keinoja hankkia tietoja kyseisessä tilanteessa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Ei-valtiolliset toimijat. Ehdotuksen mukaan tiedustelun yleiset edellytykset olisivat matalammat, jos kohteena on valtiollinen toimija. Valtiollisen ja ei-valtiollisen toimijan välinen rajanveto on hyvin olennainen perus- ja ihmisoikeussuojan kannalta, joten valiokunnan huomiota tarpeesta tulkita kansallisen turvallisuuden käsitettä suppeasti on syytä korostaa.

Yleiset periaatteet. Poliisilain 5 a luvun tiedustelumenetelmiä käytettäessä on otettava huomioon myös poliisilain 1 luvun säännökset suhteellisuusperiaatteesta (3 §), vähimmän haitan periaatteesta (4 §) ja tarkoitussidonnaisuuden periaatteesta (5 §). Nämä periaatteet tulevat sovellettavaksi myös tietoliikennetiedustelussa tietoliikennetiedustelulain 1 §:n 1 momentissa olevan viittauksen kautta. Kumpaankaan lakiin ei sisältyisi sotilastiedustelulain 8 §:ää vastaavaa säännöstä syrjinnän kiellosta. Mielestäni tällainen säännös on syytä lisätä myös poliisilakiin.

3 Ehdotetut tiedustelumenetelmät

3.1 Valtuuksien laajuudesta

Lakiehdotuksessa on otettu lähtökohdaksi, että suojelupoliisi saisi tiedonhankintatoimivaltuudet, jotka olisivat samantyyppisiä kuin nyt on käytössä rikosten torjunnassa. Lisäksi ehdotukseen sisältyy uutena toimivaltuutena tietoliikennetiedustelu. Suuri osa ehdotetuista toimivaltuuksista rajoittaa luottamuksellisen viestin suojaa.

Valiokunnan aiempi tulkintakäytäntö on perustunut aiemmin voimassa olleeseen perustuslain 10 §:n 3 momentin sanamuotoon, jonka mukaan välttämättömistä rajoituksista luottamuksellisen viestin salaisuuteen voidaan säätää lailla muun muassa yksilön tai yhteiskunnan turvallisuutta taikka

kotirauhaa vaarantavien rikosten tutkinnassa. Yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten piiriin kuuluvat perusoikeusuudistuksen esitöiden mukaan esimerkiksi huumausaine-rikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetosrikokset (HE 309/1993 vp, s. 54/II). Tavallisesti toimivaltuuksien käytön edellytyksenä on ollut yhteys tiettyihin laissa määriteltyihin rikoksiin. Esimerkiksi poliisilain 5 luvun 5 §:ssä telekuuntelun käyttö on sidottu laissa lueteltuihin törkeisiin ja ylitörkeisiin rikoksiin. Valiokunta on kuitenkin pitänyt mahdollisena, että tunnistamis-tietojen saaminen jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset (PeVL 26/2001 vp, s. 3/II, PeVL 37/2002 vp, s. 3/I; PeVL 66/2010 vp).

Poliisilain 5 a lukuun esitetyt toimivaltuudet ovat soveltamisedellytyksiltään poliisilain salaisia tiedonhankintakeinoja väljempiä. Tämä on ymmärrettävää tiedustelutoiminnan luonteen vuoksi. Väljemmät edellytykset on syytä ottaa huomioon menetelmien muissa piirteissä kuten kestoajassa ja niihin liitetyissä oikeussuojakeinoissa. Toimivaltuuksien enimmäiskestoksi on tyypillisesti määritelty kuusi kuukautta siinä missä poliisilain 5 luvussa luottamuksellisen viestin suojaan puuttuvien toimivaltuuksien enimmäiskesto on yksi kuukausi. Toimivaltuuksien käytössä ei olisi kyse rikoksen ennalta estämisestä ja torjunnasta kuten poliisilaissa, vaan paljon abstraktimmasta ja vaikeammin kohdennettavasta tiedustelutiedon hankinnasta, mikä voi omalta osaltaan puoltaa sitä, että asiaa tarkastellaan tuomioistuimessa useammin.

Erona poliisilain 5 lukuun tiedusteluperusteilla tapahtuvaa telekuuntelua, muiden vastaavien tietojen hankkimista tai televalvontaa koskevan luvan ei tarvitsisi perustua tiettyyn teleosoitteeseen tai telepäätelaitteeseen, vaan se voisi perustua tiettyyn henkilöön. Tämä on olennainen edellytysten lavennus poliisilain 5 luvun mukaisiin edellytyksiin verrattuna. Kun lupa perustuu teleosoitteeseen tai telepäätelaitteeseen, pakkokeinolla on objektiiviset rajat. Jos lupa perustuu henkilöön, viranomaisella on oikeus omalla päätöksellään kohdentaa seuranta myös muihin teleosoitteisiin tai telepäätelaitteisiin, mikä on jossain määrin ongelmallista perusoikeusrajoituksen ennakoitavuuskriteerin kannalta. Säännöksessä ei ole määritelty niitä edellytyksiä, joiden perusteella viranomainen voi tämän päätöksen tehdä. Henkilöön kohdistuvan telekuuntelun enimmäisaika olisi kolme kuukautta eli lyhyempi kuin teleosoitteeseen tai telepäätelaitteeseen perustuvassa telekuuntelussa. Tämä toisi telekuuntelun perusteet useammin tuomioistuimen tarkasteltavaksi. Pidän kuitenkin erikoisena esityksen perusteluissa (s. 182) esitettyä kantaa, jonka mukaan "se, ettei tiedusteluvaltuutettu olisi puuttunut telekuuntelun käyttöön, ilmentäisi telekuuntelun käytön hyväksyttävyyttä sekä sen lainmukaisuutta." Tiedusteluvaltuutetun puuttumattomuudesta ei voi mielestäni tehdä tällaista päätelmää.

Perustuslain muutosta koskevassa mietinnössään perustuslakivaliokunta katsoi, että vaara viranomaisten tilapäisestä pääsystä yksittäisten, tiedustelutehtävään liittymättömien henkilöiden viestintää koskeviin tietoihin tulee rajata mahdollisimman vähäiseksi ja muutoinkin valiokunta painotti tarvetta tulkita perustuslain 10 §:n 4 momentin rajoitusperustetta suppeasti (PeVM 4/2018 vp). Tiedusteluviranomaisille annettavia valtuuksia on tarpeen arvioida muun muassa perusoikeuksien rajoitusedellytyksiin kuuluvan välttämättömyysvaatimuksen näkökulmasta. Kunkin esitetyn toimivaltuuden kohdalla on erikseen arvioitava, onko se välttämätön ja onko sen taustalla painava yhteiskunnallinen tarve (vrt. PeVL 6/2018 vp). Esityksen mahdollisen hyväksymisen

jälkeen lakien toimeenpanoa on syytä seurata muun muassa sen suhteen, minkä verran eri tiedustelumenetelmiä on käytetty ja mikä niiden tuloksellisuus on ollut.

Ehdotetun poliisilain 5 a luvun 53 §:n mukaan sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentin mukaisesti säilytettyjä tietoja voitaisiin käyttää myös tiedustelutarkoituksessa. Huomautan, että jäljempänä kuvattavan Euroopan unionin *Tele2/Watson*-tuomion jälkeen voidaan perustellusti kysyä, onko 157 §:n tarkoittama säilytysvelvollisuus ylipäänsä Euroopan unionin oikeuden mukainen.

3.2 Yleisluontoiset tiedustelumenetelmät

3.2.1 Yleisluontoista valvontaa koskevasta tulkintakäytännöstä

Kaksi ehdotettua tiedustelumenetelmää ei kohdistu yksittäiseen henkilöön, vaan niillä seurataan tietoliikennettä laajemmin. Nämä ovat keinot tukiasematietojen hankkiminen (poliisilain 5 a:8 §) ja tietoliikennetiedustelu.

Erona yksilöön kohdistuviin tiedonhankintakeinoihin, tietoliikenteeseen yleisesti kohdistuvat tiedonhankintakeinot ovat luonteeltaan spekulatiivisempia ja ne eivät perustu tietyn henkilön seuraamiseen vaan yleisempään tiedonhankintaan. Saatujen tietojen perusteella voidaan myös suunnata yksilöön kohdistuvia muita tiedonhankintakeinoja. Tietoja voidaan yhdistellä muista lähteistä saatuihin tietoihin ja niistä voidaan tilastollisilla menetelmillä luoda henkilöprofiileja.

Perustuslakivaliokunta on teletunnistetietoja koskevassa yhteydessä katsonut, että kun lainsäädäntö antaa mahdollisuuden tietojen kokoamiseen ja yhdistämiseen, huomiota on kiinnitettävä rajoitusten merkittävyyteen (PeVL 18/2014 vp). Oikeasuhtaisuusvaatimuksen vastaisena voidaan pitää ainakin sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin (PeVL 18/2014 vp; PeVL 20/2016 vp; PeVL 26/2016 vp). Valiokunta on kiinnittänyt huomiota EU-tuomioistuimen oikeuskäytännön merkitykseen (erityisesti asioissa *Digital Rights Ireland*, *Schrems* ja *Tele2/Watson;* PeVL 9/2017 vp).

Mietinnössään PeVM 4/2018 vp perustuslakivaliokunta painotti, että perustuslain 10 §:n 4 momentin rajoissa säädettävien valtuuksien, esimerkiksi siviili- ja sotilastiedustelua koskevissa hallituksen esityksissä tiedusteluviranomaisille ehdotettavien toimivaltuuksien, on oltava sopusoinnussa myös Suomen kansainvälisten ihmisoikeusvelvoitteiden, erityisesti Euroopan ihmisoikeussopimuksen, ja EU-oikeuden kanssa. Valiokunta on korostanut myös, että perustuslaissa turvattu perusoikeussuojan taso voi olla korkeampi kuin suojan vähimmäistason asettavista ihmisoikeusvelvoitteista johtuu (PeVL 59/2017 vp, PeVL 43/2016 vp, PeVL 24/2016 vp, PeVL 59/2014 vp).

Euroopan unionin perusoikeuskirjan 7 artiklassa turvataan yksityiselämän suoja, mukaan lukien luottamuksellisen viestinnän suoja. Perusoikeuskirjan 8 artiklassa turvataan henkilötietojen suoja. 51 artiklan mukaan perusoikeuskirjan määräykset koskevat jäsenvaltioita ainoastaan silloin, kun ne soveltavat unionin oikeutta. Euroopan unionista tehdyn sopimuksen toimivallanjakoa koskevan 4 artiklan 2 kohdan mukaan kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla,

joten perusoikeuskirjan soveltuvuus riippuu siitä, pidetäänkö muun muassa ehdotettuja sähköiseen viestintään puuttuvia toimia Euroopan unionin lainsäädännön alaan kuuluvina. Euroopan unionin tuomioistuimessa on käsiteltävänä ennakkoratkaisupyyntö asiassa C-623/17, jossa on kysymys nimenomaan Euroopan unionin lainsäädännön soveltumisesta tiedustelutoiminnassa.

Euroopan unionin tuomioistuimen mukaan jos henkilön viestinnästä tai paikkatiedoista kerätään tietoja pitkäkestoisesti, syntyy tietojen kokonaisuus, joka "voi mahdollistaa hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä, kuten elämäntavoista, vakituisista tai tilapäisistä oleskelupaikoista, päivittäisestä tai muusta liikkumisesta, tekemisestä sekä näiden henkilöiden sosiaalisista suhteista ja heidän sosiaalisesta ympäristöstään" (*Digital Rights Ireland*, kohta 27*).* Näiden tietojen perusteella voidaan laatia asianomaisten henkilöiden profiili, joka on yksityiselämän kunnioittamista koskevan oikeuden kannalta aivan yhtä arkaluonteista tietoa kuin itse viestinnän sisältö (*Tele2/Watson*, kohta 99). Tietojen säilyttäminen ja niiden myöhempi käyttö ilman, että sähköisten viestintäpalvelujen käyttäjille ilmoitetaan siitä, voi aiheuttaa kyseisille ihmisille tunteen siitä, että heidän yksityiselämänsä on jatkuvan tarkkailun kohteena (*Digital Rights Ireland*, kohta 27; *Tele2/Watson*, kohta 100). Tällä voi olla vaikutusta myös Euroopan unionin perusoikeuskirjan 11 artiklassa turvatun sananvapauden käyttämiselle (*Digital Rights Ireland*, kohta 25). Tuomioistuin on pitänyt viestinnän liikenne- ja paikkatietojen säilyttämistä vakavana puuttumisena perusoikeuksiin ja siten vain vakavan rikollisuuden torjuminen voi olla tällaisen toimenpiteen perusteena. Tuomioistuin katsoi, että välttämättömän puuttumisen rajat ylitti kansallinen lainsäädäntö, jonka mukaisesti kaikkien käyttäjien ja kaikkien sähköisten viestintävälineiden kaikki liikennetiedot tuli säilyttää ilman mitään erottelua tai rajoituksia taikka poikkeuksia asetetun tavoitteen perusteella. Lainsäädäntö ei myöskään edellyttänyt, että henkilöt, joiden tietoja säilytetään, olisivat edes epäsuorasti sellaisessa tilanteessa, joka voisi johtaa rikosoikeudellisiin toimiin. Lainsäädäntöä sovellettiin siis myös henkilöihin, joiden osalta ei ole mitään seikkaa, jonka perusteella voitaisiin olettaa, että heidän toimintansa voisi olla edes epäsuorasti tai kaukaisesti yhteydessä vakavaan rikollisuuteen. Laissa ei myöskään säädetty minkäänlaisesta poikkeuksesta, joten sitä sovelletaan jopa henkilöihin, joiden viestintään sovelletaan kansallisen lainsäädännön mukaan salassapitovelvollisuutta. Tällaisessa säännöstössä ei vaadittu minkäänlaista yhteyttä säilytettäviksi säädettyjen tietojen ja yleistä turvallisuutta koskevan uhan välillä eikä säilyttämistä ollut rajoitettu joko tiettyyn ajanjaksoon ja/tai maantieteellisesti määriteltyyn alueeseen ja/tai sellaisten tiettyjen henkilöiden piiriin, joilla on yhteys vakavaan rikollisuuteen tai rikollisuuden torjumiseen (*Tele2/Watson*, kohdat 102–107). Euroopan unionin oikeus on myös esteenä sellaiselle lainsäädännölle, jossa viranomaisille säädetään oikeus saada säilytettäviä tietoja, jos samalla ei rikollisuuden torjumisen puitteissa rajoiteta tätä tietojen saantia vain vakavan rikollisuuden torjumisen tarkoitukseen, eikä tietojen saannin edellytykseksi aseteta tuomioistuimen tai riippumattoman hallintoviranomaisten suorittamaa ennakkovalvontaa eikä vaadita, että kyseessä olevat tiedot säilytetään unionin alueella (*Tele2/Watson*, kohta 125).

Tuomioistuin toteaa kuitenkin, että tietojen säilyttäminen on mahdollista, jos se on kohdennettua ja sillä edellytyksellä, että näiden tietojen säilyttäminen on, siltä osin kuin kyse on säilytettävistä tietoluokista, tarkoitetuista viestintävälineistä, asianomaisista henkilöistä ja aiotun säilytyksen kestosta, rajoitettu täysin välttämättömään (*Tele2/Watson*, kohta 108).

Euroopan ihmisoikeussopimuksen 8 artikla edellyttää, että yksityiselämän suojaan kohdistuvien rajoitusten on perustuttava lakiin, niillä on oltava hyväksyttävä tavoite ja niiden on oltava välttämättömiä demokraattisessa yhteiskunnassa. Euroopan ihmisoikeustuomioistuin on salaisia tiedustelumenetelmiä koskevassa oikeuskäytännössään kiinnittänyt huomiota erityisesti menetelmiä koskevan lainsäädännön ennakoitavuuteen. Tuomioistuimen mukaan salaiseen valvontaan liittyy ilmeinen väärinkäytösten riski, joten siihen on liitettävä selkeät ja yksityiskohtaiset säännöt. Laista tulee riittävällä selkeydellä ilmetä, millaisissa olosuhteissa ja millä edellytyksillä viranomaiset voivat käyttää salaisia tiedustelukeinoja. Mielivaltaisen oikeuksiin puuttumisen estämiseksi laista tulee myös ilmetä viranomaisilla olevan harkintavallan ala ja miten sitä käytetään (*Big Brother Watch ym.* v. *Yhdistynyt kuningaskunta*, kohdat 305–306 ja viitattu oikeuskäytäntö).

Ihmisoikeustuomioistuin on luetellut oikeuskäytännössään kuusi vähimmäisvaatimusta, jotka viestintäsalaisuutta rajoittavasta lainsäädännöstä on ilmettävä: 1) millaisten tekojen perusteella viranomaiselle voidaan antaa oikeus puuttua viestintäsalaisuuteen, 2) ne henkilöryhmät, joihin kuuluminen altistaa viestinnän valvonnalle, 3) valvonnan kestolle asetetut rajat, 4) toimenpiteet, joiden mukaisesti hankittuja tietoja tutkitaan, käytetään ja tallennetaan, 5) turvatoimet, joita noudatetaan luovutettaessa tietoja muille osapuolille ja 6) olosuhteet, joissa saadut tiedot voidaan tai on velvollisuus poistaa tai tuhota. Tapauksissa, joissa viestintäsalaisuutta on rajoitettu kansallisen turvallisuuden nimissä, tuomioistuin on kiinnittänyt huomiota myös seuraaviin tekijöihin: 7) salaisen valvonnan valvonnan järjestäminen, 8) ilmoitusmenettelyt ja 9) kansalliseen lakiin sisältyvät oikeussuojakeinot (*Big Brother Watch ym.* v. *Yhdistynyt kuningaskunta*, kohta 307).

Euroopan ihmisoikeustuomioistuin on äskettäin arvioinut Ruotsin tietoliikennetiedustelua koskevaa lainsäädäntöä ja katsonut sen olevan ihmisoikeussopimuksen mukainen (*Centrum för rättvisa* v. *Ruotsi*). Ruotsin järjestelmä muistuttaa paikoin nyt ehdotettua tietoliikennetiedustelua, mutta sen käyttöala on rajattu sotilastiedusteluun.

3.2.2 Tukiasematietojen hankkiminen

Ehdotettuun poliisilain 5 a lukuun sisältyy toimivaltuus tukiasematietojen hankkimiseen (8 §). Tällä toimivaltuudella viranomainen saa tiedon tiettyyn tukiasemaan kirjautuneista tai kirjautuvista telepäätelaitteista ja teleosoitteista. Ehdotettu toimivaltuus vastaisi poliisilain 5 luvun 11 §:n vastaavaa säännöstä.

Toimivaltuus kohdistuu potentiaalisesti laajaan henkilöjoukkoon. Tukiasemia on erityisesti kaupungeissa varsin tiheässä, ja yhden tukiaseman piirissä voi olla kymmeniä tai satoja päätelaitteita. Toimivaltuuden perusteella viranomainen saa siis luettelon kaikista tukiaseman lähistöllä olevista päätelaitteista (esimerkiksi matkapuhelimista) ja käytännössä siis myös tiedon niiden omistajien summittaisista sijainneista. Jos viranomainen saa luvan useampaan tukiasemaan, se voi seurata tiettyjen henkilöiden liikkumista eri tukiasemien alueilla ja jos seurantaa tehdään pitkällä aikavälillä, viranomaiselle muodostuu tietokanta niistä henkilöistä, jotka liikkuvat tietyllä alueella toistuvasti. Ehdotettu säännös ei aseta rajoituksia pitkäkestoiselle ja alueellisesti laajalle tukiasematietojen seurannalle.

Rikostutkinnassa tukiasematietojen hankkimisen hyöty perustuu siihen, että sen perusteella voidaan saada selville rikoksen tapahtumapaikalla oleskelleita henkilöitä. Tiedustelukontekstissa tällä toimivaltuudella saataisiin tietoja siitä, keitä tietyllä alueella tai tilassa liikkuu. Viranomainen saisi siis haltuunsa luettelon kymmenistä tai sadoista alueella oleskelevista henkilöistä, joiden yhteydestä tiedustelun kohteeseen ei olisi tuossa vaiheessa tietoa.

Tukiasematietojen hankkiminen otettiin uutena toimivaltuutena pakkokeinolakiin lailla 646/2003 (HE 52/2002 vp). Perustuslakivaliokunta arvioi tuolloin ehdotusta perustuslain 10 §:n turvaaman yksityiselämän suojan ja 9 §:ssä turvatun liikkumisvapauden kannalta. Valiokunta totesi, että ehdotettu sijaintitiedon hankkiminen eroaa rikoksesta epäiltyyn kohdistettavista pakkokeinoista siinä, että paikantaminen kohdistuu ennalta määräämättömään joukkoon matkaviestimiä ja koskee siten periaatteessa laajuudeltaan tuntematonta henkilöjoukkoa. Valiokunnan mukaan yksityiselämän suojan lähtökohtana on yksilön oikeus elää omaa elämäänsä ilman viranomaisten ja ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista ja tähän oikeuteen sisältyy muun muassa yksilön oikeus solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön (PeVL 36/2002 vp). Ehdotuksessa tietojen hankkiminen oli sidottu laissa lueteltuihin rikoksiin, joita perustuslakivaliokunta piti "verraten törkeinä". Valiokunta antoi lausuntonsa mukaan suurta painoa sille, että kysymyksessä oleva yksityiselämän suojan rajoitus oli "varsin vähäinen verrattuna rajoituksen perusteena olevan yhteiskunnallisen intressin tärkeyteen". Tästä lähtökohdasta valiokunta arvioi myös uutta pakkokeinolakia (PeVL 66/2010 vp).

Valiokunnan käytännön mukaan paikkatiedot kuuluvat perustuslain 10 §:n 1 momentissa turvatun yksityiselämän suojan piiriin ja niitä koskevia rajoituksia on arvioitava perustuslain yleisten rajoitusedellytysten kannalta (PeVL 24/2001; PeVL 53/2005 vp; PeVL 66/2010 vp). Valiokunnan arvioissa paikkatiedoille on annettu samankaltainen asema kuin viestinnän tunnistamistiedoille (PeVL 9/2004 vp; PeVL 11/2005 vp; PeVL 3/2006 vp). Euroopan unionin yleisen tietosuoja-asetuksen 4 artiklan mukaan sijaintitietoa pidetään henkilötietona (ks. PeVL 1/2018 vp), joten paikkatietojen käsittelyä on tarkasteltava myös henkilötietojen suojaa koskevan perusoikeuden kannalta.

Pakkokeinolain säätämisen jälkeen valiokunta on arvioinut uudelleen linjaansa koskien massaluontoista viestintätietojen keräämistä. Kuten edellä on todettu, valiokunta on katsonut, että kun lainsäädäntö antaa mahdollisuuden tietojen kokoamiseen ja yhdistämiseen, huomiota on kiinnitettävä rajoitusten merkittävyyteen (PeVL 18/2014 vp). Oikeasuhtaisuusvaatimuksen vastaisena voidaan pitää ainakin sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin (PeVL 18/2014 vp; PeVL 20/2016 vp; PeVL 26/2016 vp).

Esitetty 8 § on sanamuotonsa puolesta varsin lavea. Lupaa tukiasematietojen hankkimiseen arvioitaisiin ehdotetun poliisilain 5 a luvun 4 §:n mukaisesti. Säännös ei rajoittaisi tietojen keruuta esimerkiksi ajallisesti, henkilömäärän suhteen tai maantieteellisen alueen suhteen. Tietojen keruulle ei olisi – muista tiedustelumenetelmistä poiketen – säädetty lainkaan enimmäiskestoa. Euroopan

ihmisoikeustuomioistuin on katsonut, että toimivaltuuden enimmäiskestoajan määritteleminen laissa on yksi suojakeino, jolla estetään toimivaltuuksien väärinkäyttö.

Mielestäni tällä tavoin säänneltynä ehdotus ei täytä edellä viitattuja perustuslakivaliokunnan periaatteita, Euroopan ihmisoikeustuomioistumen määrittelemiä vähimmäisedellytyksiä eikä Euroopan unionin *Tele2*-tuomiossa todettuja linjauksia ja sitä tulee rajata ja täsmentää.

3.2.3 Tietoliikennetiedustelu

Hallituksen esityksen 2. lakiehdotus koskee lakia tietoliikennetiedustelusta siviilitiedustelussa. Lailla sallittaisiin tietoliikenteeseen kohdistuva tiedustelu. Viestitietojen kerääminen tapahtuisi hakuehtojen käyttöön perustuvan automatisoidun erottelun avulla. Tietojen kerääminen toteutettaisiin tunnistamalla tietty viestintäverkon osa, jossa kohteena olevan tietoliikenteen oletetaan kulkevan ja tarvittaessa vertailemalla tietoliikennettä hakuehdoiksi kutsuttaviin ennakkoon asetettuihin kriteereihin.

Tietoliikennetiedustelun käytön edellytykset määriteltäisiin 4 §:ssä. Käytön yleinen edellytys olisi että tietoliikennetiedustelulla voidaan perustellusti olettaa saatavan tietoja sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Jos kyseisessä verkossa liikkuu muutakin kuin valtiollisen tahon tietoliikennettä, edellytyksenä olisi lisäksi, että tietoliikennetiedustelun voidaan olettaa olevan välttämätöntä. Edellytys tiedustelun välttämättömyydestä on osin tiukempi edellytys kuin muissa säädettäväksi ehdotetuissa luottamuksellisen viestin salaisuuden suojaan puuttuvissa tiedustelumenetelmissä. Esityksen perusteluissa (s. 237) välttämättömyyden ymmärretään tarkoittavan kyseisen keinon viimesijaisuutta. Perusteluiden mukaan koska telekuuntelun ja televalvonnan käyttö pääsääntöisesti voidaan kohdentaa tarkemmin kuin tietoliikennetiedustelun käyttö, sisältää telekuuntelun ja -valvonnan käyttö vähäisemmän mahdollisuuden, että sivullista viestintää tulee tiedustelun piiriin. Näin ollen, jos telekuuntelun tai -valvonnan käyttö ei yksittäistapauksessa olisi mahdotonta tai huomattavan vaikeaa, tulisi niitä käyttää ensisijaisina keinoina suhteessa tietoliikennetiedusteluun.

5 §:n 3 momentissa säädettäisiin nimenomainen kielto käyttää hakuehtona Suomessa oleskelevan henkilön hallussa olevaa tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja. Säännöksessä ei kuitenkaan kiellettäisi käsittelemästä Suomessa oleskelevan henkilön viestintätietoja, jos hän on viestinnän lähettävänä tai vastaanottavana osapuolena.

Tietoliikennetiedustelussa on kysymys toimivaltuudesta, joka puuttuu kaikkien välitettävänä olevien viestinnän osapuolten luottamuksellisen viestinnän suojaan ja henkilötietojen suojaan. Ehdotuksen mukaan viranomainen voisi puuttua myös viestien sisältöön. Tiedustelu voi periaatteessa olla laajamittaistakin ja koskea suurta viesti- tai ihmisjoukkoa. Potentiaalisesti kyseessä on sitten erittäin merkittävä rajoitus, joka sellaisenaan merkitsisi puuttumista perusoikeuden ydinalueeseen.

Euroopan ihmisoikeustuomioistuimen mukaan Euroopan ihmisoikeussopimuksesta ei seuraa periaatteellista estettä massamuotoisen tiedustelujärjestelmän käyttämiselle. Olennaista on, täyttääkö tiedustelua koskeva lainsäädäntö muut ihmisoikeussopimuksesta seuraavat, muun muassa tarkkarajaisuutta ja ennakoitavuutta koskevat vaatimukset (*Big Brother Watch ym.* v. *Yhdistynyt*

kuningaskunta, kohdat 314–315). Lisäksi ehdotettua sääntelyä on tietenkin arvioitava erikseen perustuslain ja mahdollisesti Euroopan unionin oikeuden kannalta.

Ehdotetussa muodossaan tietoliikennetiedustelussa seulottaisiin koneellisesti vain osa viesteistä virkamiehen tutkittavaksi, mikä olennaisesti vähentää puuttumisen intensiteettiä. Toisaalta seulonnan tekninen epäonnistuminen, liian väljät seulontakriteerit tai tahallinen väärinkäytös voivat johtaa hyvinkin merkittävään perusoikeusloukkaukseen. On olennaista arvioida, pystytäänkö tätä riskiä hallitsemaan riittävässä määrin teknisesti, ehdotetuilla säännöksillä ja ehdotetulla valvontajärjestelmällä.

Luvan tietoliikennetiedusteluun myöntäisi tuomioistuin. Tuomioistuimelle tehtävään hakemukseen sisällytettävät tiedot on kuvattu 7 §:n 2 momentissa. Pidän luetteloa varsin kattavana. Tietoliikennetiedustelua koskevissa säännöksissä ei tosin rajata sitä, kuinka suureen viesti- tai ihmisjoukkoon tiedustelu voi kohdistua. Tuomioistuin voi kuitenkin asettaa tällaisia rajoituksia luettelon 8 kohdan perusteella. Tiedustelun oikeasuhtaisuus jää muutenkin merkittävissä määrin tuomioistuimen arvion varaan. Oikeasuhtaisuutta arvioitaessa on syytä kiinnittää huomiota perustuslakivaliokunnan mietinnössään esittämään näkemykseen, jonka mukaan perustuslain 10 §:n uusi 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa. Valiokunta arvioi lisäksi välttämättömyys-kriteeriä siten, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti (PeVM 4/2018 vp).

Tuomioistuimen tehtävänä on myös arvioida luvan oikeasuhtaista kestoaikaa. Luvan kesto on suhteutettava tiedustelutoimen välttämättömyyteen. Lähtökohtana ei voi olla, että luvat ovat aina maksimikeston mittaisia.

Ehdotus sisältää mahdollisuuden siihen, että kiiretilanteessa päätöksen tietoliikennetiedustelusta tekee suojelupoliisin päällikkö (9 §). Tällöin asia on kuitenkin vietävä 24 tunnin kuluessa tuomioistuimen päätettäväksi. Vastaava menettely sisältyy poliisi- ja pakkokeinolakeihin, jotka on perustuslakivaliokunnan myötävaikutuksella säädetty (PeVL 66/2010 vp ja 67/2010 vp). Euroopan ihmisoikeustuomioistuin arvioi vastaavaa Ruotsin tiedustelulainsäädäntöön sisältyvää menettelyä ja katsoi sen olevan ihmisoikeussopimuksen mukainen, mutta muistutti että tällaisen menettelyn tulee pysyä poikkeuksellisena (*Centrum för rättvisa* v. *Ruotsi*, kohta 140).

4 Lupapäätöskäsittely

Arvioidessaan luottamuksellisen viestinnän suojan rajoituksia poliisi- ja pakkokeinolakien yhteydessä perustuslakivaliokunta on pitänyt oleellisena oikeusturvakysymyksenä, että kuunteluvaltuuden edellytyksenä on aina riippumattoman tuomioistuimen yksittäistapauksessa konkreettisen rikosepäilyn johdosta antama lupa (PeVL 8/1994 vp, s. 2/II; PeVL 36/2002 vp; PeVL 37/2002 vp). Valiokunta on korostanut, että tuomioistuimen on huolellisesti harkittava luvan myöntämisen tarvetta ja laajuutta erityisesti kun hakemuksen perusteena on törkeysasteeltaan suhteellisen vähäinen rikos (PeVL 32/2013 vp, s. 4/II; PeVL 33/2013 vp, s. 4/II). Valiokunta on

myös edellyttänyt tuomioistuimen antamaa lupaa edellytyksenä telepakkokeinolla saadun ylimääräisen tiedon käyttämiselle (PeVL 66/2010 vp, s. 10/II; PeVL 67/2010 vp, s. 5/I).

Tuomioistuinkontrollilla on siis ollut keskeinen asema luottamuksellisen viestin suojan rajoitusten oikeutuksena. Kuitenkin voi kysyä, toimiiko tuomioistuinkontrolli sillä tavoin rajoittimena kuin perustuslakivaliokunta sen olettaa toimivan. Oikeuspoliittinen tutkimuslaitos on tutkinut käräjäoikeuksien telepakkokeinopäätöksiä vuonna 2006. Tutkimuksen kohteena olevien lupapäätösten perustelut olivat tavallisesti hyvin kaavamaisia ja ne oli perusteltu suppeasti tai ei lainkaan. Noin kolmanneksessa hakemuksista konkreettinen peruste jäi jossain määrin epäselväksi. Pelkistetyimmillään käräjäoikeuden perusteluissa vain toistettiin pakkokeinolain sanamuodot ja viitattiin hakemuksessa esitettyihin perusteluihin ilman päätökseen kirjattua arviointia siitä, miten hakemus konkreettisesti täyttää pakkokeinoluvan edellytykset.

Eduskunnan oikeusasiamies on toistuvasti ainakin vuodesta 2001 lähtien kiinnittänyt huomiota ongelmiin telepakkokeinohakemuksissa ja niitä koskevien päätösten käsittelyssä ja perusteluissa. Ongelmia on ollut muun muassa pakkokeinohakemusten sekä niitä koskevien päätösten perusteluissa. Hakemusten käsittely vaikuttaa summaariselta, mitä kuvastaa muun muassa hylättyjen vaatimusten hyvin vähäinen osuus. Vaatimuksia hylätään vuosittain kymmenkunta, mikä on 0,2–0,4 % vuosittaisesta hakemusmäärästä (noin 3 000).

Tiedustelutoiminnan lupia ei voida samalla tavoin sitoa perusterikoksiin kuin poliisi- ja pakkokeinolakien tapauksessa. Lisäksi tiedustelu koskee potentiaalisesti suurempaa viesti- ja henkilöjoukkoa kuin poliisitutkinta. Tiedustelulupien tuomioistuinkäsittely ei ole julkinen etu- eikä jälkikäteen. Nämä seikat korostavat tuomioistuimen erityisen keskeistä roolia oikeusturvan takaajana luvista päätettäessä.

Jotta tuomioistuinkäsittely ei jää muodollisuudeksi, vaan jotta luvan edellytykset tulevat aidosti tutkituksi, tuomioistuimelle on varmistettava riittävät henkilö- ja aikaresurssit ja koulutus. Lisäksi tuomioistuinprosessia tulee kehittää siten, että tuomioistuin ei ole vain hakijan esittämien arvioiden varassa, vaan prosessissa on mukana myös osapuoli, joka tarkastelee lupahakemusta kriittisesti tiedustelun kohteena olevien henkilöiden perus- ja ihmisoikeuksien näkökulmasta.

Telepakkokeinojen yhteydessä valiokunta on toistuvasti ehdottanut, että telekuuntelussa otettaisiin käyttöön julkinen asiamies, jonka tehtävänä olisi valvoa telekuuntelun kohteena olevan rikoksesta epäillyn ja muiden kuuntelun kohteeksi mahdollisesti joutuvien etuja (PeVL 36/2002 vp, s. 7/II; PeVL 66/2010 vp, s. 10/I). Tehtävä voisi olla kuitenkin tarkoituksenmukaista antaa hallituksen esityksessä HE 199/2017 vp tarkoitetulle tiedusteluvaltuutetulle, jolla olisi oikeus tulla kuulluksi tuomioistuimen käsitellessä tiedustelulupaa. Valtuutetulla tulisi olla myös oikeus kannella käräjäoikeuden päätöksestä hovioikeuteen.

5 Ylimääräinen tieto

Ehdotetun poliisilain 5 a luvun 44 § sallii tai velvoittaa tiedusteluviranomaisen ilmoittamaan keskusrikospoliisille tiedustelumenetelmää käytettäessä ilmi tulleestä tehdystä rikoksesta tai tekeillä olevasta rikoksesta, joka on vielä estettävissä. Koska tiedustelumenetelmistä seuraavia perusoikeusrajoituksia perustellaan tarpeella hankkia tietoa kansallista turvallisuutta uhkaavasta

toiminnasta ja tästä syystä tiedustelumenetelmät ovat vaikutuksiltaan kenties laveampia ja pitkäkestoisempia kuin mikä olisi mahdollista rikoksentutkinta- tai torjuntakontekstissa, on ongelmallista, jos tiedustelumenetelmillä hankittua tietoa käytetään kovin vähäisten rikosten torjumiseen.

44 §:n 2 momentin mukaan tietoa saisi luovuttaa sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Rikoslain noin 450:stä nimikkeestä 58 % tulisi tämän säännöksen piiriin. Pidän näin alhaista rajaa ongelmallisena ehdotuksen oikeasuhtaisuuden kannalta.

6 Tiedustelusta ilmoittaminen

Ehdotetun tietoliikennetiedustelua siviilitiedustelussa koskevan lain 20 §:n mukaan viranomaisella ei ole velvollisuutta ilmoittaa viestien manuaalisesta käsittelystä, jos tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella. Käytännössä tämä tarkoittaa muun muassa tilannetta, jossa tietoliikennetiedustelua on tehty kiiretilanteessa suojelupoliisin päällikön päätöksellä ja tuomioistuin on jälkeenpäin katsonut, että lain mukaisia edellytyksiä tietoliikennetiedustelulle ei ole ollut. Ilmoittaa ei tarvitsisi myöskään muun muassa silloin, jos käy ilmi, että viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui tai jos kyseessä on tiedustelukiellon alainen viesti eli viestintä asianajajan, lääkärin, papin tai toimittajan kanssa.

Koska tiedustelu tapahtuu kohteiltaan salassa, jälkikäteisellä ilmoituksella on tärkeä rooli siinä, että kohde voi saattaa tiedustelun laillisuuden valvontaviranomaisen tutkittavaksi. Vaikka tiedustelutoiminnan valvontaa koskevan lakiesityksen (HE 199/2017 vp) 12 §:n mukaan kuka tahansa voi pyytää tiedusteluvaltuutettua tutkimaan häneen mahdollisesti kohdistuneen tiedustelumenetelmän käytön lainmukaisuuden, tiedustelun kohteen oikeusturva on aivan eri tasolla silloin, jos hän saa tietää häneen tosiasiallisesti kohdistuneesta tiedustelusta. Pelkkään yleiseen epäilyyn perustuva tutkintapyyntö ei todennäköisesti edes voi johtaa mihinkään tulokseen, koska tiedot tapahtuneesta viestin avaamisesta on jo poistettu. 9 §:n 2 momentissa tarkoitetuissa tapauksissa on kyse tilanteesta, jossa viranomainen on tehnyt tiedustelua omalla päätöksellään lain edellytysten vastaisesti, joten tiedustelun kohteella on erityinen intressi saada halutessaan oikeudenloukkaus tutkittavaksi. Lisäksi kyseessä on poikkeuksellinen menettely, johon ei liity etukäteistä tuomioistuinkontrollia, mikä on syytä ottaa huomioon ilmoittamisvelvollisuuden laajuudessa.

Tiedustelukieltojen alainen viestintä nauttii erityistä suojaa. Yksityisyyden suojan ohella tiedustelukiellot suojaavat muun muassa oikeusturvaa (PL 21§), terveyttä (PL 19 §), uskonnonvapautta (PL 11 §) ja sananvapautta (PL 12 §) koskevia perusoikeuksia. Tämä korostaa viestinnän osapuolten tarvetta saada tietää heihin kohdistuneesta tiedustelusta. Poikkeuksia perustellaan esityksen perusteluissa siten, että "Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei tällaisissa tapauksissa voitane pitää perusteltuna, sillä sen henkilön luottamuksellisen viestin sisältö, jolle ilmoitus olisi muuten tehtävä, olisi hävitetty tiedusteluviranomaisen hallusta." Luottamuksellisen viestin suojassa ei ole kuitenkaan kyse pelkästään siitä, onko viranomaisella kopio viestistä. Henkilöllä, jonka luottamuksellisen viestinnän suojaa on rajoitettu, on

lähtökohtaisesti oikeus tietää, että viestin on lukenut kolmaskin osapuoli ja oikeus harkita oikeusturvakeinojen käyttämistä.

Katson siten, että 20 §:n 1 momentin viimeinen lause tulee muuttaa siten, että velvollisuus ilmoittaa tietoliikennetiedustelusta koskee myös 9 §:n 2 momentin ja 15 §:n 1 momentin 2 kohdan mukaisia tilanteita.

Helsingissä 23.10.2018

Niklas Vainio
OTM, FM