Professori *Jukka Viljanen*

HE 202/2017 vp, HALLITUKSEN ESITYS EDUSKUNNALLE SIVIILITIEDUSTELUA KOSKEVAKSI LAINSÄÄDÄNNÖKSI

Perustuslakivaliokunta 25.10.2018

1. Hallituksen esitykseen sisältyvästä perus- ja ihmisoikeusproblematiikasta

Perustuslain 10 §:ään tehdyt muutokset astuivat voimaan 15.10.2018 (SK 817/2018, HE 198/2017 vp, PeVM 4/2018 vp). Perustuslakivaliokunnan kannanotot perustuslain muutosta koskevaan mietintöön muodostavat keskeiset periaatteet, joiden varaan myös varsinaiset tiedustelua koskevat lakipaketit on hyvä rakentaa.

Perustuslain 10 §:n 4 momenttiin on kirjattu, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen … ”sekä tiedonhankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”. Olen ollut prosessissa mukana oikeusministeriön nimittämän asiantuntijatyöryhmän jäsenenä ja laatimassa mietintöön liitettyä arviota EIT:n tiedonhankintakeinoja koskevasta tulkintakäytännöstä. Lisäksi olen lausunut muistakin tiedustelulainsäädäntöön liittyvistä luonnoksista valmistelun aikana. En ole kuitenkaan kommentoinut aikaisemmin siviilitiedustelua koskevaa lakipakettia.

Perustuslakivaliokunta on mietinnössään perustuslain muuttamisesta (PeVM 4/2018 vp) todennut, että ”kansallista turvallisuutta vakavasti uhkaavalla toiminnalla” on yhteys siviilitiedustelupakettiin.

> 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. Ehdotus liittyisi tältä osin hallituksen esitykseen siviilitiedustelua koskevaksi lainsäädännöksi (ks. HE 202/2017 vp

Jos tiivistää tiedustelulainsäädännön tuoman muutoksen aikaisempaan verrattuna on kyse, että viranomaiset saavat mahdollisuuden salaiseen tiedonhankintaan täysin uudenlaisella perusteella. Siviilipuolella on kyse nimenomaan suojelupoliisille annettavista uusista toimivaltuuksista. Aikaisempiin salaisiin pakkokeinoihin ehdotetaan lisäksi uutena keinona tietoliikennetiedustelua. Keskeisinä uudistuksina on poliisilain 5 a luku Siviilitiedustelu ja laki tietoliikennetiedustelusta siviilitiedustelussa.

Normaalisti poliisi- ja pakkokeinolainsäädännössä kaikki lähtee nimenomaan rikoksesta, jonka ratkaisemiseen erilaisia salaisia pakkokeinoja käytetään. Suojelupoliisin käyttämien toimivaltuuksien (salaisten tiedonhankintakeinojen) yhteinen piirre on se, että ne on määritelty henkilö- ja rikoslähtöisesti. Niitä voidaan kohdistaa vain sellaiseen henkilöön tai käyttää hankittaessa tietoa vain sellaisen henkilön toiminnasta, jonka voidaan perustellusti olettaa tulevaisuudessa syyllistyvän tai jo syyllistyneen tietyn vakavuusasteen rikokseen tai sellaisen valmisteluun. (HE s.72) Tiedustelutoiminnassa ajatus lähtee siitä, että mitään rikosta ei ole vielä tapahtunut, joten toimivaltuuksia ei voi sitoa rikoksiin tai niiden vakavuuteen. Hallituksen esityksessä korostetaan, että tiedustelutoimivaltuuksien erityiset edellytykset tulisi määritellä uhkalähtöisesti. Lakiesitys lähtee laajentamaan tiedonhankintaa siten, että se koskisi toimintaa, joka vakavasti uhkaa Suomen kansallista turvallisuutta joko suoraan tai välillisesti. Hallituksen esityksen mukaan Kansallista turvallisuutta vakavasti uhkaava toiminta voi olla sellaista, joka konkretisoituessaan olisi rikos, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä. Samoin kyse voi olla toiminnasta, joka ei ole Suomen lain mukaan rikos eikä voisi sellaiseksi muodostuakaan.

Perusasetelman lisäksi uutta ovat myös menetelmät. Kyse on massaluonteisen tiedonhankinnan keinoista erityisesti koskien tietoliikennetiedustelua. Kyse on hallituksen esityksen termein seulonnasta, josta syntyy massaluonteista tiedonhankinnasta, josta Euroopan ihmisoikeustuomioistuin käyttää termiä ”bulk interception”. Tässä hallituksen esityksessä käytetään termiä laajamittaisesta viestiyhteyksien uhkaperusteisesta yleisvalvonnasta (s. 54) Esityksessä todetaan, että tiedonhankinta toteutetaan viesti- ja tietoliikennevirtaa suodattavan järjestelmän avulla (s.78). Sotilastiedustelulailla ja nyt käsiteltävällä ehdotuksella on selkeä yhteys ja se näkyy myös siinä, että käytännössä tietoliikennetiedustelussa on myös puolustusvoimain tiedustelulaitos mukana.

Perustuslakivaliokunta on asettanut tarkan listan, joka toimii hyvin pohjana tiedustelulainsäädännön yhteensopivuutta arvioitaessa (PeVM 4/2018 vp. s. 8).[1]

Tarkoitukseni on arvioida lakiesitystä erityisesti perus- ja ihmisoikeuksien näkökulmasta. Oman erityisasiantuntemukseni vuoksi keskityn käsittelemään Euroopan ihmisoikeussopimuksen ja Euroopan ihmisoikeustuomioistuimen tulkintakäytännön sekä muiden kansainvälisten ihmisoikeusvelvoitteiden valossa.

2. Yleisesti Euroopan ihmisoikeussopimuksen siviilitiedustelulainsäädännölle asettamista vaatimuksista

Lähtökohtaisesti Euroopan ihmisoikeussopimuksen 8 artiklan tulkintakäytännössä kehittyneet vaatimukset asettavat Huvig/Kruslin kriteeristön, joita erilaisia salaisia pakkokeinoja koskevan lainsäädännössä on noudatettava riippumatta siitä, mikä toimija tai millainen väline on kyseessä. Keskeiset tiedustelutapaukset on varsin perusteellisesti esitelty esitöissä (s. 50-64), niistä mainittakoon tapaukset Weber ja Saravia v. Saksa, Liberty v. Yhdistynyt Kuningaskunta, Roman Zakharov v. Venäjä sekä Szabo ja Vissy v. Unkari.

Erityisesti Unkaria koskevaa tapausta on tarpeen esitellä tässä yhteydessä. Unkarin kohdalla oli järjestelmästä, joka luotiin vuonna 2011 nimenomaan terrorismin vastaiseen toimintaan. Ongelmana oli järjestelmän rakentuminen puhtaasti toimeenpanovallan tekemiin päätöksiin ilman riittävää tuomioistuinkontrollia.

Szabo ja Vissy tuomiossa pohditaan huolellisesti niitä vaatimuksia, joita uudet tiedustelumenetelmät edellyttävät (the potential of cutting-edge surveillance technologies to invade citizens' privacy). Uudet tiedustelumenetelmät johtavat helposti sellaisten ihmisten tutkimiseen, joihin toimenpiteitä ei ollut alun perin tarkoitus kohdistaa.

---

[1] PeVM 4/2018 vp. Säännöksen soveltamisrajoituksista perustuslakivaliokunta korostaa, 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. Välttämättömyys-kriteeri puolestaan tarkoittaa, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedonhankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti. Valiokunta korostaa muutenkin perusoikeuksien yleisten rajoitusedellytysten merkitystä uutta ehdotettua rajoitusperustetta tulkittaessa.

Kaksi keskeistä vaatimusta seuraa uudenlaisesta teknologiasta. EIT muistuttaa (kohta 73), että testi tarkoittaa ensinnäkin sitä, että tiedustelun tarkoituksena on suojata demokraattisia instituutioita ja toiseksi toimenpiteeltä pitää edellyttää *ehdotonta välttämättömyyttä* (strict necessity) elintärkeän tiedon saamiseksi tiedustelutoimenpiteellä. Jos nämä ehdot eivät täyty, mikä tahansa toimenpide voi uuden teknologian ansiosta johtaa väärinkäytöksiin. EIT hyödyntää tässä yhteydessä niin EU-tuomioistuimen (Digital Rights Ireland) kuin YK:n erityisraportoijan Frank La Ruen näkemyksiä (2013)[2] , joita esitellään tuomion vertailuosuudessa (kohdat 23 ja 24). EIT tukee näitä kantoja.

Lopputuloksena on se, että Unkarin järjestelmä oli monelta osin puutteellinen. Sen ja aikaisempien tapausten oppeja on huomioitu hallituksen esityksessä. Kysymys ehkä kohdentuu siihen, miten operaation kohdentamisesta huolimatta voi seurata puuttuminen uuden teknologian ansiosta myös henkilöihin, jotka olivat toimenpiteiden ulkopuolella.

> 1. In total sum, the Court is not convinced that the Hungarian legislation on "section 7/E (3) surveillance" provides safeguards sufficiently precise, effective and comprehensive on the ordering, execution and potential redressing of such measures.
>
> Given that the scope of the measures could include virtually anyone, that the ordering is taking place entirely within the realm of the executive and without an assessment of strict necessity, that new technologies enable the Government to intercept masses of data easily concerning even persons outside the original range of operation, and given the absence of any effective remedial measures, let alone judicial ones, the Court concludes that there has been a violation of Article 8 of the Convention

Hallituksen esityksen jälkeen tuoreimpana ratkaisuna Euroopan ihmisoikeustuomioistuin antoi kesällä tuomion asiassa *Centrum för Rättvisa v. Ruotsi* (19.6.2018, *Application no. 35252/08), jossa* tarkastellaan perusteellisesti Ruotsin tiedustelulainsäädäntöä ja sen valvontaa. Tämän vuoksi kyse on tiedustelulainsäädäntöpaketin kannalta tärkeästä tulkintaratkaisusta. Lisäksi hiljattain annettiin laaja jaostotuomio *Big Brother Watch ym. v. Yhdistynyt Kuningaskunta* (13.9.2018), jossa puolestaan brittien tiedusteluvalvontaregiimien todettiin loukanneen ihmisoikeussopimuksen 8 artiklaa. Siinä testattiin muun muassa, olivatko yksilöiden oikeussuojakeinot riittäviä ja toisaalta olivatko edellytykset tiedonhankinnalle riittävällä tavalla kirjattu tiedusteluregiimeihin.

Ihmisoikeussopimuksen kanssa yhteensopivuuden varmistaminen lähtee siitä, että tiedustelujärjestelmien aiheuttamat puuttumiset perustuvat sopimuksen asettamiin rajoitusedellytyksiin. Kyse on ensinnäkin rajoittamisen täsmällisyydestä ja tarkkarajaisuudesta. Lainsäädännön tulee ilmaista ihmisryhmät, joihin valvontaa voidaan kohdistaa; sellaisten

[2] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17.4.2013, A.HRC.23.40
https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

rikkomusten luonne, joissa valvonta tulee kyseeseen; valvonnan kesto; menetelmä, jolla valvotuista keskusteluista raportoidaan sekä nauhoitusten hävittäminen.

Rajoituksen välttämättömyyden testi puolestaan sisältää kolme keskeistä osaa. Rajoitukselle on oltava painava yhteiskunnallinen tarve (pressing social need), puuttumisen ja tavoiteltavan hyväksytyn päämäärän tulee olla oikeassa suhteessa keskenään (reasonable relationship between the interference and pursued legitimate aim) ja kolmanneksi puuttumiselle pitää olla relevantit ja riittävät perustelut.

3. Eräitä perus- ja ihmisoikeushavaintoja siviilitiedustelua koskevasta valvonnasta, tiedustelukielloista ja tietojen hävittämisestä

Lakiesityksistä tekee vaativan erityisesti laajat pykälät, joissa määritellään tiedustelumenetelmien käytön edellytykset. Nyt jokaisen yksittäisen poliisilain 5 a luvun pykälän kohdalla on erilaiset vaatimukset päättämisestä. Lakiteknisesti 5 a luvusta muodostuu tämän vuoksi erittäin pitkä ja lukijalle jossain määrin vaikeaselkoinen kokonaisuus.

Erilaisten valvontamuotojen kestosta on selkeästi omaksuttu uudenlainen linja verrattuna nykyiseen salaisia pakkokeinoja koskevaan sääntelyyn. Monissa salaisia pakkokeinoja koskevissa asioissa luvan kesto on nykyisen lainsäädännön mukaan vain yhden kuukauden. Nyt tiedustelun puolella pääsääntönä esitetään kuuden kuukauden lupaa, näin on esimerkiksi telekuuntelun kohdalla. Tätä perustellaan tiedustelutoiminnan luonne ja rikostorjunnan tarpeet poikkeavat toisistaan. Telekuuntelun pidempää kestoa perustellaan erityisesti siviilitiedustelun luonteella ja tiedustelumenetelmien käytön perusteen vuoksi. Sitten esityksessä todetaan, että uusi käsittely antaisi tuomioistuimelle *aidon* mahdollisuuden kontrolloida luvan edellytysten olevan edelleen voimassa.

Ilmaisu ”aidon/aidosti” on kirjoitettu useampaankin kohtaan. Ilmaisu aidosta mahdollisuudesta kontrolloida luvan olemassa olon edellytyksiä herättää kysymyksiä, joiden osalta jää miettimään sitä, kuinka hyvin siviilitiedustelulle asetettuja edellytyksiä, tiedustelukieltoja tai oikeusturvaa pystyään varmistamaan, jos järjestelmien hallinnan tunnistetaan olevan vaikeaa. Euroopan ihmisoikeussopimuksen näkökulmasta kyse on siitä, onko valvonta tehokasta ja onko se toimiva paitsi teoriassa myös käytännössä.

EIT on esimerkiksi Centrum för Rättvisa tapauksessa todennut (kohta 127), että kokonaiskesto voidaan jättää jäsenvaltioiden viranomaisten harkintaan, kunhan riittävät oikeussuojakeinot ovat olemassa. Se sisältää selkeän ajan, jonka jälkeen lupa päättyy ja ehdot sille milloin lupa voidaan

uudistaa ja missä olosuhteissa se pitää peruuttaa. Kuuden kuukauden raja on tässä suhteessa linjassa Ruotsin lainsäädäntöön.

On varmasti perusteltua, että muuttaa lupien kestoaikoja, mutta onko jotenkin sisäänkirjoitettuna näissä näkemyksissä, että ennakkolupavaiheessa ei ole aitoa mahdollisuutta kontrolloida tilannetta. Pienenä kuriositeettina voidaan mainita 3 kk keston kohdalla epäselväksi jäävä virke tiedusteluvaltuutetun roolista.[3]

Vastaavasti herää kysymys aidosta valvonnasta, kun esityksessä todetaan, että hävittämisvelvollisuudesta säätämisen välttämättömyys johtuu siitä, että kotimaisen viestinnän luotettava tunnistaminen ja sen erottaminen *aidosti* kansainvälisestä viestinnästä ei yleensä ole mahdollista teknisin menetelmin tapahtuvassa tietoliikenteen automatisoidussa erottelussa.

Tämän vuoksi on tärkeää, että laajenevien toimivaltuuksien ohella asetetaan muita rajoituksia viranomaisille. Samalla on muistutettava yleisistä poliisilainsäädäntöön kirjatuista periaatteista. Poliisilakiin ensimmäiseen lukuun sisältyvät 2-5 §:t ovat tiedustelutoiminnassakin keskeisessä asemassa, koska niihin sisältyvät perus- ja ihmisoikeuksien kunnioittaminen, suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate. Myös 9 §:n määräys toimenpiteestä luopumisesta, jos se johtaa kohtuuttomaan lopputulokseen on tärkeä.

Esimerkiksi tietoliikennetiedustelun osalta on asetettu maksimiaika enintään kuusi kuukautta (Laki tietoliikennetiedustelusta siviilitiedustelussa 7.3 §). Esityksen mukaan tähän liittyy tuomioistuimen ja hakevan viranomaisen harkinta tapauskohtaisesti. Esityksen mukaan tapaukseen suhteellisuus ja vähimmän haitan periaatteen soveltaminen.

Jälleen kerran näen tarpeen seurata huolellisesti, miten hyvin lupaan perustuva tuomioistuinjärjestelmä onnistuu kokonaan uudenlaisessa tilanteessa. Kyse ei ole rikosperusteisesta pakkokeinojen käytöstä, vaan kuten hallituksen esityksessäkin mainitaan tiedustelutoimenpiteitä ja niiden kestoa perustellaan toiminnan luonteella ja tiedustelumenetelmien käytön perusteella. Toiminnan luonne perusteen käyttö ei saa johtaa tilanteeseen, jossa viranomaisten käyttöön annetaan kokonaan uusi työkalupakki ilman, että sen käyttöä huolellisesti valvotaan.

[3] HE s. 182.”Esimerkiksi pelkästään se, ettei tiedusteluvaltuutettu olisi puuttunut telekuuntelun käyttöön, ilmentäisi telekuuntelun käytön hyväksyttävyyttä sekä sen lainmukaisuutta.”

Nykyisten salaisten pakkokeinojen sisäisen valvonnan rooli on muodostunut tärkeäksi. Tärkeää on muodostaa suojelupoliisiin sisäisen lainvalvonnan mekanismit. Niitä ei ole vielä ollut. Tämä on tunnustettu myös hallituksen esityksessä (s. 137).

Uutena tiedustelumenetelmänä niin sotilas- kuin siviilitiedustelun puolella on tietoliikennetiedustelu. Seulonnassa erotetaan uhkan kannalta olennainen viestintä muusta. Tärkeässä asemassa ovat tietoliikennetiedustelussa käytettävät seulontaparametrit, joista voidaan käyttää nimitystä hakuehdot, voivat seuloa tiedustelujärjestelmän läpi virtaavan viesti- ja tietoliikenteen sisältöä tai sen muita tietoja. Muita tietoja ovat esimerkiksi sellaiset tiedot, jotka ovat tarpeen tietoliikennevirtaan sisältyvien yksittäisten viestien ohjaamiseksi niiden lähettäjältä vastaanottajalle, sekä viestinnän aikaa ja paikkaa koskevat tiedot.

Esityksessä viitataan laajasti tiedonhankinnan rajaamisen teknisiin ongelmiin. Esimerkiksi tiedustelukieltojen noudattaminen siten, että tietoliikenteestä ei lainkaan kerättäisi kieltojen piiriin kuuluvia tietoja, ei ole teknisesti mahdollista. Monien asioiden kohdalla juuri ongelma kiinnittyy niihin toimiin, joita tarvitaan lupahakemusta varten. Tietoliikennetiedusteluun liittyy puolustusvoimien tiedustelulaitoksen keräämä tieto, jota käytetään tunnistamaan lupahakemusta varten viestintäverkon osa. Se edellyttäisi useimmin paitsi puolustusvoimien tiedustelulaitoksen toimenpiteitä myös sitä, että suojelupoliisi saisi viestintäverkon omistajina ja haltijoina olevilta yrityksiltä eräät niiden hallussa olevat tiedot.

Erityisen vaativaa on nähdäkseni sen arviointi, miten hyvin väärän tiedon estämiseksi asetetut tiedustelukiellot ja hävittämistä koskeva erityissääntely toimii. Siinä arvioinnissa ihmisoikeusvelvoitteiden kanssa yhteensopivuuden kannalta keskeinen vaatimus on laadukas tuomioistuinharkinta, joka takaa selkeät toimenpiteet lain vastaisen tiedon poistamiseksi. Erityisen tärkeää on, että tietoliikennetiedustelulain 9 §:ssä (päätöksenteko kiireellisessä tilanteessa) mainitut toimet, kun tiedustelu ei täytä 4 §:n asettamia edellytyksiä. Lain 9 § 2 viimeinen virke kuitenkin näyttäisi mahdollistavan tiedon luovuttamisen rikostorjuntaan. Vaikka oltaisiin siis menetelty virheellisesti ja saatu tietoa, joka on vastoin lain edellytyksiä sen käyttö olisi sallittua. Hallituksen esityksessä todetaan, että tämä kohdistuu vain ankarimpiin rikostyyppeihin.

Merkittävänä asiana hallituksen esityksen perusteluissa on tietoliikennetiedustelusta ja keskustelu pilvipalveluihin tallettamisesta. Kun sotilastiedustelulainsäädäntöpaketissa pilvipalveluihin viitattiin lähinnä 62 §:n yksityiskohtaisissa perusteluissa, on siviilitiedustelun osalta asiaa tarkasteltu paljon

yksityiskohtaisemmin (ks. 130-132), koska vielä aikaisemmassa vaiheessa esitettiin tiedustelukieltoa koskien pilvipalveluihin talletettavaa tietoa.

Nykymaailmassa pilvipalvelut ovat käytössä lähes kaikessa verkossa tapahtuvassa toiminnassa, on kyse sitten sähköposteista kuin tietojen tallettamisesta. Pilvipalveluja koskevat perustelut ovat osaltaan kertomassa siitä kuinka vaikeaa asettaa tiedustelukieltoja. Jatkossa tämä tarkoittaa, että kohdentaminen on hyvin vaikeaa ja väistämättä tietoliikennetiedustelu lähestyy sitä rajaa, jonka mukaan tiedustelulainsäädäntö ei saa ”mahdollistaa yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa”. Tämän vuoksi ihmisoikeusnäkökulmasta jää kysymään sitä, miten varmasti ja tehokkaasti rajoitukset pilvipalvelujen osalta toimivat. Hallituksen esityksessä esimerkiksi todetaan, että pilvipalvelujen kohdalla hakuehtona ei voitaisi käyttää Suomessa olevan henkilön teleosoitteen tai telepäätelaitteen yksilöintitietoa, koska lain 4 §:n 3 momentti nimenomaisesti kieltäisi sen. Samaan aikaan puhutaan siitä, että pilvipalveluun tallentamista koskevana hakuehtona voisi lähinnä tulla kyseeseen pilvipalvelun sijaintipaikkaa kuvaava tieto.

Siviilitiedustelua koskevassa esityksessä korostetaan, että ”laki sisältäisi useita sellaisia viestintäsalaisuuden suojaamisen tarkoituksessa tietoliikennetiedustelun käytölle asetettuja rajoitteita, joille ei ole vastinetta vertailuvaltioissa. Näistä merkittävin koskisi sitä, että tietoliikennetiedustelussa ei saataisi käyttää viestin sisältöä kuvaavaa hakuehtoa muuten kuin tarkoin rajatuissa poikkeustapauksissa.”

Hakuehtojen rajoittaminen siten, että ne eivät saa koskea viestin sisältöä ovat tärkeitä osasia arvioitaessa tietoliikennetiedustelun yhteensopivuutta luottamuksellisen viestin suojan kanssa. Epäilys erityisesti pilvipalveluiden osalta syntyy kuitenkin siitä, että esityksessä viitataan arvioon, jonka mukaan sivullinen pilvipalveluliikenne voi vastata tietoliikennetiedustelussa käytettäviä hakuehtoja vain varsin poikkeuksellisesti. Riskiä pienentää esityksen mukaan ”valittu sääntelymalli, jossa tietoliikennetiedustelun hakuehdot eivät voisi kuvata viestin sisältöä.”

Tietoliikennetiedustelulla saatavaan materiaalin osalta on asetettu runsaasti tiedustelukieltoja ja hävittämisvelvollisuuksia, jotka tarkoittavat merkittäviä rajoituksia saatujen tietojen tallentamisessa. Nykytekniikka mahdollistaa voimakkaat puuttumiset yksityisyyden suojaan. Kyse on vaikeasti hahmottuvasta teknisesti monimutkaisesta kokonaisuudesta, jonka merkitystä yksilön yksityisyyden suojan kannalta on varsin vaikea arvioida kokonaisuutena.

Kokonaisarviointiin vaikuttaa niin monta erilaista tekijää ja myös teknisiä, käytännön tiedustelutoimien suorittamiseen liittyviä kysymyksiä, että abstraktilla tasolla on lähes mahdotonta sataprosenttisesti varmistaa, että tiedustelujärjestelmä toimii yhteensopivasti ihmisoikeussopimuksen vaatimusten kanssa. Tämän vuoksi katse kääntyykin siihen, että kotimaisen valvontajärjestelmän kokonaisuus on sellainen, että se muodostaa riittävän vastapainon ja pystyy rajoittamaan tiedusteluviranomaisten harkintaa ja varmistamaan välttämättömyysvaatimuksen sisältämien kriteerien toteutumisen. Se vaatii nykyistä laadukkaampaa tuomioistuinvalvontaa.

4. EIT ja ihmisoikeussopimuksen kanssa yhteensopiva valvontakokonaisuus

Olen sotilastiedustelulainsäädännön yhteydessä nostanut esille tarkempia havaintoja kahdesta tapauksesta. Tässä yhteydessä kiinnitän huomiota vain ennakollista valvontaa koskeviin havaintoihin. EIT arvioi tiedustelujärjestelmiä erityisesti siltä kannalta, miten niissä varmistettiin ennakollinen valvonta. Kyse on kokonaisuudesta, jossa on usein sekä ennakollinen lupajärjestelmä tuomioistuimen toimesta (judicial authorisation) ja toisaalta jälkikäteinen valvonta (judicial oversight) voi tasapainottaa mahdolliset puutteet, jotka koskevat valtuutta suorittaa tiedustelutoimenpiteitä.

Centrum för Rättvisa -tapauksessa yksityiskohtaiseen tarkasteluun joutunut Ruotsin malli perustuu erityistuomioistuimeen (puolustustiedustelutuomioistuimeen), jossa toimivat myös erityiset yksityisyydensuojaa valvovat valtuutetut. Toistan sotilastiedustelua koskevasta lausunnostani saman kommentin eli pitäisikö tapauksesta vetää suorat johtopäätökset, että juuri tällaista mallia pitäisi myös suomalaisessa tiedusteluvalvonnassa korostaa. Tuomareiden ammattitaito pitää olla uudella tasolla verrattuna normaaleihin salaisia pakkokeinoja koskeviin käsittelyihin. Ainakin on selkeästi nähtävissä, että Ruotsin malli täyttää EIT:n vaatimukset. (ks. HE 203/2017 vp s. 63)[4] . Tuomioistuimen ja tiedusteluviranomaisten lisäksi mallissa ovat yksityisyyden suojaan valvovat valtuutetut.

[4] Signaalitiedustelu edellyttää aina erityistuomioistuimena toimivan puolustustiedustelutuomioistuimen lupaa. Kaapelitiedustelua koskevan lupahakemuksen tulee sisältää kuvaus tiedonkeräystehtävästä, tieto siitä, mihin kaapelin kuituihin tiedonhankinta halutaan kohdistaa, käytettävät hakuehdot, luvan kesto ja muut seikat, joihin signaalitiedusteluviranomainen haluaa vedota. Laissa on myös annettu tarkat edellytykset sille, milloin tuomioistuin voi myöntää luvan, ja mitä luvasta tulee käydä ilmi. Myöntämisedellytykset liittyvät erityisesti toiminnan ja tehtävän lainmukaisuuteen ja suhteellisuuteen. Lupa voi olla voimassa korkeintaan kuusi kuukautta ja se voidaan uusia korkeintaan kuudeksi kuukaudeksi kerrallaan. Tuomioistuimessa kansalaisten yksityisyyttä edustavat erityiset **yksityisyydensuojaa valvovat valtuutetut** (integritetsskyddsombud), jotka ovat tai ovat olleet tuomareita tai asianajajia.

Vaikka EIT löytää Ruotsin sääntelystä puutteita, se katsoo, että valvontajärjestelmä toimii vastapainona tilanteessa. Valvontajärjestelmän osalta kiinnitetään huomiota sen riippumattomuuteen ja siihen millä vakavuudella sen esittämiin huomautuksiin on suhtauduttu. Tämä on tärkeä tulkintalinjaus kaikille tuleville ratkaisuille. *EIT on nähnyt keskeiseksi ajatuksen, että pelkkä lainsäädännön olemassaolo ei riitä, vaan arvioon liittyy se, miten lainsäädännön määrittelemä järjestelmä käytännössä toimii* (not only in theory but also in practice. kohta 158).

Pidänkin tärkeänä, että samalla kun erilaisia ratkaisuja nyt mietitään, tehdään myös linjaus siitä, että niiden toteutumisen arviointi suoritetaan mahdollisimman huolellisesti. Ruotsin kohdallakin EIT juuri näkee tärkeänä sen, että puutteita on matkan varrella jatkuvasti korjattu. *Yhtenä keskeisenä positiivisena ja hallituksen argumentteja puoltavana tekijänä todetaan, että Ruotsissa järjestelmää on jatkuvasti uudistettu tavoitteena yksityisyyden suojan parantaminen (kohta 180).* Mutta samalla EIT myös jättää mahdollisuuden palata asiaan konkreettisen puuttumisen kohdalla.

EIT on useampaan otteeseen viitannut tarpeeseen päivittää uuden teknologian aikakaudelle nykyisiä tulkintalinjauksia, koska se on myöntänyt tiedonhankintamenetelmät ovat uuden teknologian ansiosta entistä voimakkaammin yksityisyyden suojaan puuttuvia. Se on toisaalta myös toistuvasti todennut, että uusien minimikriteerien lisääminen ei ole tarpeellista. Näin tapahtui myös Big Brother Watch tapauksessa. EIT ei kuitenkaan lisännyt valittajien ehdottamia vaatimuksia minimikriteereihin. Jossain vaiheessa todennäköisesti kriteerien päivitys tapahtuu.

EIT korostaa parhaana käytäntönä tuomioistuinten toimesta tapahtuvaa ennakkolupajärjestelmää. Tässä mielessä HE täyttää ihmisoikeussopimuksen vaatimukset. Merkittäväksi puuttumiseksi luottamuksellisen viestin suojaan lasketaan esityksen mukaan teknistä kuuntelua, teknistä laitetarkkailua, telekuuntelua ja tietojen hankkimista telekuuntelun sijasta, televalvontaa, lähetyksen jäljentämistä ja tietoliikennetiedustelua. Tämä on huomioitu oikeusturvajärjestelyissä eli esityksessä tuomioistuinlupaa edellyttäviä tiedustelumenetelmiä olisivat telekuuntelu ja tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, paikkatiedustelu ja tietoliikennetiedustelu.

Lupa voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan lukuun ottamatta telekuuntelussa ja sen sijasta toimitettavassa tietojen hankkimisessa, jos kohteena on henkilö. Näissä tilanteissa lupa voitaisiin antaa enintään kolmeksi kuukaudeksi kerrallaan. Lain 7 §:n tuomioistuimen päättäminen luvasta ja siinä tietoliikennetiedustelulle asetetut ehdot luvalle ovat riittävän täsmälliset ja tarkkarajaiset ihmisoikeussopimuksen näkökulmasta.

On erityisen tärkeää, että yksittäisistä tiedustelumenetelmistä päättävät pystyvät lakiesityksen ja sen perustelujen pohjalta pohtimaan ja punnitsemaan toimintaan liittyviä perus- ja ihmisoikeuskysymyksiä ja myös tunnistamaan erilaisia tilanteita ja niihin liittyviä perus- ja ihmisoikeusongelmia. Kaikkein uusimmalla alueella ollaan tietoliikennetiedustelussa, jossa on kyse teknisestä tiedonhankinnasta, joka edellyttää vielä teknisen tiedon jatkokäsittelyä. Tämä on kysymys, johon seurannassa tulee kiinnittää erityinen huomio

5. Yhteenveto huomioista Euroopan ihmisoikeustuomioistuimen tulkintakäytännön pohjalta

Siviilitiedustelulainsäädäntöä on laadittu siten, että se olisi yhteensopiva perustuslakivaliokunnan vaatimuksen kanssa. PeVM 4/2018 vp todetaan, että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedonhankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti.

Ongelmana on jatkossa se, miten hyvin lainsäädännön tasolla laaditut tiedustelukiellot ja hävittämisvelvollisuudet tosiasiassa estävät puuttumiset myös viestien sisältöön. Samoin on syytä olla tarkkana siitä, miten perusoikeuksien yleiset rajoitusedellytykset ja yleiset poliisilain periaatteet huomioidaan harkinnassa. Nykyisessä Euroopan ihmisoikeustuomioistuimen ratkaisukäytännössä on varsin joustavasti hyväksytty erilaisia kansallisia ratkaisuja. Olennaista on nähdä tiettyjen kokonaisvalvontaa määrittelevien ehtojen muodostavan riittävän vastapainon uusille toimivaltuuksille.

Euroopan ihmisoikeustuomioistuin on käsitellyt useassa tapauksessa tiedustelulainsäädäntöjä ja niiden yhteensopivuutta Euroopan ihmisoikeussopimuksen yksityisyyden suojaa koskevan 8 artiklan kannalta. Kun perustuslakia muutettiin, monet olivat huolissaan muutoksen vaikutuksista. Kuitenkin perusajatus on ollut, että muutoksen jälkeen perustuslakivaliokunta määrittelee omilla tulkintakannanotoillaan sen, että uudet tiedusteluvaltuudet ja niiden ympärille luotu tiedusteluregiimi täyttää ihmisoikeussopimuksen, EU:n perusoikeuskirjan ja kotimaisten perusoikeuksien asettamat vaatimukset.

Erityisesti Ruotsia koskeva ratkaisu Cenrum för Rättvisa antaa asiantuntijallekin hyvin selkeän viestin. On turhaa kuvitella, että kaikki mahdolliset ongelmakohdat voidaan tunnistaa abstraktin tason etukäteisvalvonnan yhteydessä. Järjestelmän on oltava jatkuvan kehittämisen kohteena. Se on asenne,

jolla myös EIT vakuutetaan, kun väistämättä valituksia suomalaista tiedustelulainsäädäntöä kohtaan tullaan esittämään.

Se tarkoittaa sitä, että aukottomaksikin ajateltu systeemi voi osoittautua tositilanteessa ongelmalliseksi. Erityisesti Ruotsin kohdalla valtioita kannustava viesti liittyy siihen ajatukseen, että kansallisen turvallisuuden luoma laaja harkintamarginaali muuttuu järjestelmän toimiessa kapeammaksi. Kun lainsäätäjä ottaa yksityisyyden suojan vakavasti huomioon myös lainsoveltajan ja regiimin ympärille muodostetun valvontakoneiston on otettava yksityisyyden suoja vakavasti. Ihmisoikeustuomioistuin korostaa, että se ei anna vapaita käsiä, vaan kansallisten viranomaisten saama harkintamarginaali kulkee aina käsikädessä eurooppalaisen valvonnan kanssa.

EIT:n tarkka tutkiminen voi konkretisoitua myös Suomen kohdalla, jos follow up asenteesta ei huolehdita. Näen välttämättömäksi kirjata eduskunnan vastaukseen viestin siitä, että uutta järjestelmää ja erityisesti lupajärjestelmää arvioidaan nopealla aikataululla. Lupajärjestelmän toimivuus sekä teoriassa että käytännössä on tässä tutkimisessa pääosassa. Kansallisten tuomioistuinten on päätöksillään annettava kuva siitä, että sen lisäksi että pinnan päällä oleva tiedusteluvalvonta täyttää sopimuksen vaatimukset, myös pinnan alla olevaa arvioidaan valvontajärjestelmän ja erityisesti tuomioistuinten toimesta.

Tampereella 25.10.2018

Jukka Viljanen
Julkisoikeuden professori
Tampereen yliopisto