Professori *Jukka Viljanen*

HE 203/2017 vp, HALLITUKSEN ESITYKSEKSI EDUSKUNNALLE LAIKSI SOTILASTIEDUSTELUSTA SEKÄ ERÄIKSI SIIHEN LIITTYVIKSI LAEIKSI

Perustuslakivaliokunta 17.10.2018

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). Näihin muutoksiin sisältyy 4 momenttiin kirjattu ”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 myös käsiteltävänä olevasta sotilastiedustelulaista.

Jos tiivistää tiedustelulainsäädännön tuoman muutoksen aikaisempaan verrattuna on kyse, että viranomaiset saavat mahdollisuuden salaiseen tiedonhankintaan täysin uudenlaisella perusteella. Normaalisti poliisi ja pakkokeinolainsäädännössä kaikki lähtee nimenomaan rikoksesta, jonka ratkaisemiseen erilaisia salaisia pakkokeinoja käytetään. Tiedustelutoiminnassa ajatus lähtee siitä, että mitään rikosta ei ole vielä tapahtunut, joten toimivaltuuksia ei voi sitoa rikoksiin tai niiden vakavuuteen (s.91).

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”. Esityksessä todetaan, että tiedonhankinta toteutetaan viesti- ja tietoliikennevirtaa suodattavan järjestelmän avulla (s.103). 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. Käsittelen myöhemmin EIT:n kantaa näihin seulontajärjestelmiin.

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 tiedustelulainsäädännölle 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, niistä mainittakoon tapaukset Weber ja Saravia v. Saksa, Liberty v. Yhdistynyt Kuningaskunta sekä Roman Zakharov v. Venäjä.

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 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.

Perustuslain tarkistamistyöryhmä toi mietinnössään esille useita tärkeitä vaatimuksia, jotka paaluttivat muiden rinnakkaisten tiedonhankintatyöryhmien työtä. Mietinnössä korostetaan korkeaa kynnystä, joka tiedonhankinnalla on. Esityksessä on asetettu välttämättömyys kynnys tiedustelutoiminnalle. Välttämättömyyskriteeri sisältää vaatimuksen puuttumisesta tiedustelutoimilla mahdollisimman kohdennetusti ja rajoitetusti (OMML 41/2016, s. 50) yksilöiden perus- ja ihmisoikeuksiin. Lisäksi työryhmän esityksessä korostetaan sitä, että tavallisen lain tasolla on säädettävä riittävistä oikeusturva- ja valvontajärjestelyistä. Tästä nousevat vaatimukset valvonnan tehokkuudesta ja asianmukaisuudesta.

Nyt esillä olevassa sotilastiedustelua koskevassa lakiesityksessä on pyritty ottamaan huomioon keskeisiä vaatimuksia, joita perustuslain 10 § edellyttää. On tunnustettava, että lain esityöt sisältävät varsin kattavan kuvauksen niistä vaatimuksista, joita EIT ja EUT asettavat sotilastiedustelulainsäädännölle. Suhteellisuusvaatimuspykälää on muokattu niistä alustavista versioista, joita olen aikaisemmin kommentoinut. Välttämättömyys on kirjattu 5 ja 6 §:iin. Samoin se mainitaan pykälissä 17, 41, 45, 67, 72, 75, 76 ja 86. Välttämättömyyskriteeriin viitataan myös lain esitöissä. Erityisen tärkeänä pidän tietoliikennetiedustelun kytkemistä välttämättömyysvaatimukseen (67 §). Lain 7 luku sisältää runsaasti EIT:n käytäntöön perustuvia vaatimuksia esimerkiksi tietojen hävittämisestä ja käytöstä ilmoittamisesta.

Kuitenkin valitut ratkaisut herättävät kysymyksiä siitä, miten hyvin ne vastaavat niillä tavoiteltuihin päämääriin ja miten ne viime kädessä ovat yhteensopivia perus- ja ihmisoikeusvelvoitteista nousevien vaatimusten kanssa. Tätä pohdintaa avaan seuraavaksi erityisesti tietoliikennetiedustelun ja ennakkolupajärjestelmän osalta, mutta ensin käyn läpi tuoreimmat EIT:n oikeustapaukset.

3. Ruotsin sotilastiedustelun arviointi EIT:ssä: Centrum for Rättvisa

Olen jo aikaisemmin perustuslakivaliokunnalle ja eri ministeriöille toimittamissani lausunnoissa korostanut, että lain esitöiden kohdalla tulee pitää huolta siitä, että esitys sisältää viittaukset yksilöitäisiin tiettyihin ihmisoikeustuomioistuimen kannanottoihin. Tällöin muodostuu myös ulospäin kuva siitä, että lainvalmistelussa on huolellisesti kartoitettu niitä potentiaalisia kysymyksiä, jotka voivat osoittautua ihmisoikeussopimuksen näkökulmasta ongelmallisiksi. Tältä osin pitää antaa myös tunnustusta lainvalmistelulle. Pidin myös mielenkiintoisena, että lainsäädännön arviointineuvosto oli käynyt läpi esityksen. Siinä nostettiin esille tärkeitä havaintoja ja esitystä oli siltä pohjalta korjattu. Se mikä on kaiken kaikkiaan arviointineuvoston työstä käsitys sai vahvistusta. Arviointineuvostolla ei selkeästikään perus- ja ihmisoikeusarviointiin resursseja.

Kaiken kaikkiaan HE:n luku 4 jossa käsitellään esityksen suhdetta perustuslakiin ja säätämisjärjestystä on poikkeuksellisen laaja. Tapauksista puuttuvat lähinnä Centrum för Rättvisa tuomio viime kesältä ja tuore Big Brother Watch ym.. Keskeinen piirre EIT:n argumentaatiossa on antaa merkittävää painoarvoa niille lainvalmistelutoimille, joissa on ymmärretty painottaa tiedustelutoiminnan yhteydessä kehiteltyä oikeussuojakeinojen valikoiman kokonaisuutta ja muutenkin yksityisyyden suojalle annettavaa painoarvoa.

Centrum för Rättvisa tapauksessa käydään läpi yksityiskohtaisesti muutamia keskeisiä minivaatimuksia, joita tiedustelujärjestelmältä ja sen toiminnalta edellytetään. Siinä mielessä se on linjassa HE:n pohjana käytetyn vakiintuneen tulkintakäytännön kanssa. Kyse on armeijan signaalitiedustelusta ja siten se voidaan kiinteästi yhdistää käsiteltävään lainsäädäntökokonaisuuteen.

Kuten HE:ssä todetaan, EIT on hyväksynyt massaluonteiset seulontajärjestelmät. Ne ovat yhteensopivia Euroopan ihmisoikeussopimuksen yksityisyyden suojalle asettamien vaatimusten kanssa ja mahtuvat valtioille kuuluvaan laajan harkintamarginaaliin silloin, kun on kyse kansalliseen turvallisuuteen liittyvistä toimista.

Tapauksessa Centrum för Rättvisa (kohta 112) ns. bulk interception regime käsitellään jatkona Weber ja Saravia sekä Liberty tapauksille:

> Given the reasoning of the Court in those judgments and in view of the current threats facing many Contracting States (including the scourge of global terrorism and other serious crime, such as drug trafficking, human trafficking, sexual exploitation of children and cybercrime),

> advancements in technology which have made it easier for terrorists and criminals to evade detection on the internet, and the unpredictability of the routes via which electronic communications are transmitted, the Court considers that the decision to operate a bulk interception regime in order to identify hitherto unknown threats to national security is one which continues to fall within States' margin of appreciation.

Heti perään EIT kuitenkin toteaa, että järjestelmien niin kohdistettujen kuin massaluontoisten (targeted and bulk interception regimes) pitää sisältää minimivaatimukset, jotta ne olisivat ennakoitavia ja siten pienentäisivät vallan väärinkäytön mahdollisuuksia.

Ihmisoikeustuomioistuin siis käy läpi erityisesti Ruotsin osalta seuraavat kysymykset: kansallisen lainsäädännön saavutettavuus, signaalitiedustelun ala ja kesto, toiminnan valtuutus, menettelytavat joita noudatetaan hankitun tiedon säilytyksessä, saatavuudessa, tutkinnassa, käytössä, kertomisessa ja tuhoamisessa, toimenpiteiden täytäntöönpanon valvonta, ilmoitusmenettely sekä mahdolliset oikeussuojakeinot.[1]

Listan perusteella on helppo ymmärtää, että väistämättä tällaisen kriteeristön läpikäynti edellyttää EIT:ltä varsin yksityiskohtaista ja laajaa tutkintaa.

EIT arvioi kutakin tiedustelujärjestelmää erityisesti siltä kannalta, miten siinä 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.

Ruotsin kohdalla keskeinen oikeussuojakeino tulee tuomioistuimen myöntämästä luvasta, koska Ruotsissa tuomioistuimella on mahdollisuus rajata signaalitiedustelulaitoksen harkintavaltaa. Kiireellisissäkin tapauksissa asia viedään välittömästi tuomioistuimen käsiteltäväksi. Tämä Ruotsin ennakollinen tuomioistuimen lupaa edellyttävä systeemi tarjosi kokonaisuutena tärkeät takeet väärinkäytöksiltä (important guarantees against abuse). Siinä ratkaisevan tärkeää (crucial importance) oli tuomioistuimen mahdollisuus asettaa rajoja puolustusvoimain radiolaitoksen (FRA) harkintavallalle.

Ruotsin malli perustuu siis erityistuomioistuimeen (puolustustiedustelutuomioistuimeen), jossa on myös erityiset yksityisyydensuojaa valvovat valtuutetut. Pitäisikö tapauksesta vetää suorat

[1] The accessibility of the domestic law, the scope and duration of signals intelligence, the authorisation of the measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the arrangements for supervising the implementation of the measures, any notification mechanisms and the remedies provided for by national law)

johtopäätökset, että juuri tällaista mallia pitäisi myös suomalaisessa tiedusteluvalvonnassa korostaa. Ainakin on selkeästi nähtävissä, että Ruotsin malli täyttää EIT:n vaatimukset. (ks. HE s. 63)[2]

EIT käy todella huolella läpi kaikki järjestelmään liittyvät menettelyt ja kiinnittää esimerkiksi huomiota puutteisiin siinä, mitä tietoa voidaan antaa muille valtioille ja kansainvälisille organisaatioille.

Vaikka EIT löytää 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. Vain tällainen follow up-ajattelu, joka on vahvistunut kansainvälisessä ihmisoikeusvalvonnassa saa jalansijaa myös suomalaisessa lainsäädännön arvioinnissa. Laajat ja näin mittavat lakiuudistukset väistämättä jättävät epäselväksi sen, miten erilaisissa konkreettisissa tilanteissa lainsäädännön määrittelemä valvontajärjestelmä pystyy tehokkaasti toimimaan. Abstraktin perustuslakikontrollin suorittaminen ei ole riittävää silloin, kun kokonaan uusi regiimi ajetaan sisään. 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. Nyt oli kyse abstraktin tason arviosta järjestelmästä, joka ei ollut virheetön,

[2] 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.

mutta jossa erityisesti tuomioistuimen suorittama ennakkolupamenettely, sekä useiden riippumattomien valvontaelinten kokonaisuus täytti sopimuksen edellyttämät minimivaatimukset. Muina toimijoina mainitaan valtion tiedustelutarkastuksen (SIUN) lisäksi oikeuskansleri, oikeusasiamies ja tietosuojavaltuutettu.

4. Big Brother Watch ja massaluontoisten puuttumisten tulkinnan päivittäminen

Jos otetaan Centrum Rättvisa tapauksen rinnalle Big Brother Watch tuomio, löytyy aivan uudenlainen tarkastelutaso ja järjestelmien monimutkainen kokonaisuus. Kyse on laajasta yli 212 sivuisesta ratkaisusta, jossa tarkastellaan useita eri regiimejä.

Suomalaiseen keskusteluun nostaisin kuitenkin myös brittiläisen tiedustelutuomioistuimen (IPT) roolia koskevan analyysin, koska Suomessakin pitää pohtia mikä on tuomioistuimen rooli ja voisiko tuomioistuin toimia koko tiedustelujärjestelmän valottajana. EIT nimittäin katsoi, että IPT oli tärkeä nostamaan esille järjestelmän pinnanalaisia osia (Below waterline[3]). Kaikkia asioita ei voida paljastaa, koska siten vaarantuu kansallisen turvallisuuden uhkien estäminen ja toisaalta kansallisten tuomioistuinten ja valvontaelinten rooliin kuuluu määritellä ja valottaa asioita, jotka ovat näkymättömissä. Valvonta, joka toimii tehokkaasti niin teoriassa kuin käytännössä, edellyttää kansallisilta toimijoilta juuri tämän kysymyksen arviointia. Mitkä asiat voidaan kertoa ja miten pinnan alla olevia menettelyitä voidaan arvioida.

EIT toteaa (kohta 326), että kaikkea ei voida julkistaa, mutta julkisten aineistojen (above waterline material) avulla voidaan arvioida salaisten menettelyn lainmukaisuutta ja välttämättömyyttä ja sitä onko riittävät takeet, jotka pienentävät väärinkäytösten riskiä[4].

Ratkaisevana tekijänä kotimaisten oikeussuojakeinojen käyttöä koskevan vaatimuksen tulkinnassa oli ajankohta, jolloin IPT oli omaksunut EIT:n mukaisen linjauksen arvioidessaan

[3] In so far as the claimants challenged the IPT's decision to look "below the waterline" when assessing the adequacy of the safeguards, the IPT considered itself entitled to look at the internal arrangements in order to be satisfied that there were adequate safeguards and that what was described as "above the waterline" was accurate and gave a sufficiently clear signposting as to what was "below the waterline" without disclosing the detail of it. In this regard, the IPT did not accept that the holding of a closed hearing, as had been carried out in the applicants' case, was unfair.
[4] Kohta 326. In the context of secret surveillance, it is inevitable that "below the waterline" arrangements will exist, and the real question for the Court is whether it can be satisfied, based on the "above the waterline" material, that the law is sufficiently foreseeable to minimise the risk of abuses of power.

tiedustelujärjestelmiä. Kansallisten tuomioistuinten ratkaisuja seurataan tällä alueella tarkasti. Tuomioistuinten rooli rikosperusteisissa salaisissa pakkokeinoissa ei välttämättä ole riittävä.

Uuden teknologian käyttäminen tiedustelutoiminnassa nostettiin esille Big Brother Watch tapauksessa. Mielenkiintoinen oli valittajien (316) vaatimus päivittää nykyinen massaluontoisia järjestelmiä koskeva tulkintakäytäntö. EIT ei kuitenkaan lisännyt valittajien ehdottamia vaatimuksia minimikriteereihin.

> However, while the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasised this point in its case-law, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. In any event, although the Court would agree that the additional requirements proposed by the applicants might constitute important safeguards in some cases, for the reasons set out below it does not consider it appropriate to add them to the list of minimum requirements in the case at hand.

Tietyt vaatimukset eivät sovi EIT:n mielestä tiedustelun ja erityisesti massaluontoisen tietoliikennetiedustelun maailmaan. Esimerkiksi vaatimus järkevästä epäilystä tai ilmoitusvaatimus eivät ole perusteltuja. Sen sijaan vaatimus etukäteisluvasta on puolestaan perusteltu. Sitä voidaan pitää parhaana käytäntönä. Se ei kuitenkaan sellaisenaan ole riittävä, jos tuomioiden ennakkovalvonta ei käytännössä estä väärinkäytöksiä, kuten joissain maissa on tapahtunut[5]. Lisätekijöinä, muttei minimivaatimuksina, ovat Zakharov tapauksessa mainitut valvontaa koskevat järjestelyt, ilmoitusmekanismit ja kansalliset oikeussuojakeinot.

Erityisesti Big Brother tapauksessa ongelmaksi nousevat tilanteet, joissa kynnystä puuttumiselle ja pääsy kerättyyn tietoon ei ole asetettu riittävän korkealle (serious crime sijasta combating crime). Brittijärjestelmässä puuttui myös mahdollisuus valvontaan, jota ennakollisesti olisi tehnyt tuomioistuin tai riippumaton hallintoelin (tyyppiä tiedusteluvaltuutettu).

> It is therefore clear that domestic law, as interpreted by the domestic authorities in light of the recent judgments of the CJEU, requires that any regime permitting the authorities to access data retained by CSPs limits access to the purpose of combating "serious crime", and that access be subject to prior review by a court or independent administrative body. As the Chapter II regime permits access to retained data for the purpose of combating crime (rather than "serious crime") and, save for where access is sought for the purpose of determining a journalist's source, it is not subject to prior review by a court or independent administrative body, it cannot be in accordance with the law within the meaning of Article 8 of the Convention.

[5] Ks. Roman Zakharov v. Venäjä ja *Mustafa Sezgin Tanrıkulu v. Turkki*, no. 27473/06, § 64, 18.7.2017

Viimeisenä lisäyksenä keskusteluun, jota hallituksen esityksessä ei käydä mutta joka pitäisi ottaa tarkasteluun, Big Brother Watch-tapaus tuo lehdistön lähdesuojan merkityksen tiedusteluregiimeissä. EIT katsoi, britti-järjestelmän loukkaavan sananvapauden suojaa ja viittasi chilling effect vaikutukseen, joka tällaisella lähdesuojaa vaarantavilla tiedustelutoimilla voi olla.

> 1. Nevertheless, in view of the potential chilling effect that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any "above the waterline" arrangements limiting the intelligence services' ability to search and examine such material other than where "it is justified by an overriding requirement in the public interest", the Court finds that there has also been a violation of Article 10 of the Convention.

Sitä ei ole kuitenkaan huomioitu HE:n 4 luvun sananvapautta koskevassa kohdassa. Pitäisin tärkeänä, että lähdesuojaa koskeva asia otettaisiin tarkempaan tarkasteluun, vaikka se näkyykin osittain lain 79 §:n (tiedustelukiellot) yksityiskohtaisissa perusteluissa (HE s.309). HE:n mukaan myös Ruotsin lainsäädännössä on nimenomainen kohta tietojen hävittämisen osalta, kun on kyse lähdesuojasta. Mielestäni asia on jollakin tavalla hyvä huomioida erityiskysymyksenä ja keskeisenä sananvapauskysymyksenä esityksen kannalta.

5. Ennakkolupajärjestelmästä ja tietoliikennetiedustelusta

EIT siis 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 68 §: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 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. Esityksessä on hyvin ilmaista tietoliikennetiedustelun ydin. ”Tietoliikennetiedustelussa Suomen alueella liikkuvasta tietoliikenteestä kerättäisiin automatisoidusti ja tallennettaisiin lupaehtojen mukaisessa viestintäverkon osassa, kuten esimerkiksi tietoliikennekaapelin kuiduin aallonpituudessa, liikkuvaa tietoliikennettä hakuehtojen mukaisesti.” Tietoliikennetiedustelu kattaa laajan määrän viestintää. Tietoja voitaisiin saada puheluista, sähköpostiviesteistä, pikaviestinnästä ja muista vastaavista viestintäkanavista ja -menetelmistä. Tärkeään rooliin nousevat myös erilaiset pilvipalvelut kuten perusteluissa kerrotaan (s.276).

Nykytekniikka mahdollistaa voimakkaat puuttumiset yksityisyyden suojaan. Kyse on vaikeasti hahmottuvasta teknisesti monimutkaisesta kokonaisuudesta, jonka merkitystä yksilön yksityisyyden suojan kannalta on varsin vaikea arvioida kokonaisuutena. Asiaan vaikuttaa niin monta erilaista tekijää ja myös teknisiä, käytännön tiedustelutoimien suorittamiseen liittyviä kysymyksiä. Esityksen perusteluissa puuttuminen luottamuksellisen viestin salaisuuteen on arvioitu olevan ongelmaton (s. 352). Kysymyksiä on paljon, mutta vedenpitäviä vastauksia on vaikea antaa. Esimerkiksi onko teknisen kehityksen myötä teknisen tiedon käsittely ongelmatonta? Voiko hakuehtoja, hakuehtojen luokkia ja niiden perusteluita valvomalla oikeasti estää lain tarkoituksen vastaisen tietoliikennevalvonnan? Miten välttämättömyysvaatimus huomioidaan valtuuksia pohdittaessa? Kysymyksiin on valtiosääntöasiantuntijana vaikea antaa täsmällistä vastausta, luotan sellaisen systeemin rakentamiseen, jossa vastapuolena olisi asioihin perehtynyt erikoistuomioistuin, joka pystyisi aidosti vaatimaan tiedustelutoimenpiteistä päättäviltä riittävät perustelut. Ennakkovalvonta ei ole tehokasta, jos se automaattisesti hyväksyy kaikki luvat. Erityistuomioistuimen lisäksi toivoisin järjestelmää, jossa asiaan perehtyneet erityiset yksityisyyden suojaa valvovat valtuutetut olisivat oikeudenkäsittelyissä mukana haastamassa tiedusteluviranomaisia perustelemaan tiedustelumenetelmien käytön huolellisesti ja tietoliikennetiedustelua käytetään vain välttämättömään.

6. Yhteenveto huomioista Euroopan ihmisoikeustuomioistuimen tulkintakäytännön pohjalta

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 ennakkolupajärjestelmää arvioidaan nopealla aikataululla. Ennakkolupajärjestelmän 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.

Tampereella 17.10.2018

Jukka Viljanen
Julkisoikeuden professori
Tampereen yliopisto