Juha Lavapuro 9.4.2015

**Puolustusministeriölle**

Puolustusministeriö on pyytänyt minulta asiantuntijalausuntoa tiedonhankintalakityöryhmän

mietinnöstä. Lausuntopyyntöä on erikseen täsmennetty siten, että huomiota tulisi

kiinnittää erityisesti niihin seikkoihin, jotka tulisi ottaa huomioon mahdollisessa jatkovalmistelussa.

Esitän asiantuntijalausuntonani kunnioittavasti seuraavaa.

***Lausunnon kohde ja keskeinen sisältö***

Tiedonhankintatyöryhmän mietintö on liitteineen kohtuullisen seikkaperäinen selvitys

suomalaisen tiedustelulainsäädännön yleisestä toimintaympäristöstä, sen keskeisistä

haasteista ja nykyisistä oikeudellisista puitteista. Mietintöön ei sisälly konkreettisia

säännösehdotuksia, vaan se on tässä suhteessa selvästikin tarkoitettu vasta esiselvitykseksi.

Aivan yleisellä tasolla ei kuitenkaan liikuta, vaan lukuihin 6 ja 7 on kirjattu sekä

tietoliikennetiedustelua että ulkomaan henkilötiedustelua ja tietojärjestelmätiedustelua

koskevia kehittämisehdotuksia.

Keskityn lausunnossani arvioimaan erityisesti tietoliikennetiedustelua koskevia kehittämisehdotuksia.

Selvyyden vuoksi tästä tiedustelusta voitaisiin hyvin käyttää yleisnimitystä

”verkkovalvonta”, mutta olen kuitenkin pyrkinyt pitäytymään muistiossa syystä tai

toisesta omaksuttujen käsitteiden puitteissa. Arvioin mietinnössä käsiteltävää tietoliikennetiedustelua

(so. verkkovalvontaa) erityisesti perus- ja ihmisoikeuksien sekä Euroopan

Unionin perusoikeuskirjassa turvattujen perusoikeuksien kannalta. Kysymys on toisin

sanoen siitä, millaisia rajoituksia perus- ja ihmisoikeudet, ml. EU:n perusoikeudet

asettavat sen kaltaiselle verkkovalvontaan pohjautuvalle tiedustelulainsäädännölle, johon

mietinnössä tähdätään.

Pidän sinänsä asiamukaisena ja jopa välttämättömänä, että mietinnössä on pyritty tarkastelemaan

tiedustelulainsäädännön yhteyksiä myös perus- ja ihmisoikeuksiin ja että tätä

on tehty nimenomaan viimeaikaisen oikeuskäytännön valossa. Esitän kuitenkin eräitä

täydentäviä, osin poikkeavia, näkökohtia mietinnössä esitettyyn. Merkittävimmät poikkeavat

kannat koskevat yhtäältä mietinnössä esillä olevaa mahdollisuutta ratkaista ongelmat

perustuslakia muuttamalla ja toisaalta EU:n tuomioistuimen Digital Rights Ireland

–ratkaisun (yhdistetyt asiat C-293/12 ja C-594/12) merkitystä. Nähdäkseni ajateltavissa

olevat vaihtoehdot perustuslain muuttamiseksi eivät ratkaisisi niitä ongelmia, joita

sen on ehkä oletettu ratkaisevan. Digital Rights Ireland –tuomion osalta puolestaan pidän

tarpeellisena tähdentää, että sitä on syytä pitää mietinnössä käsiteltävän asian kan2

nalta selvästi keskeisempänä ja laajakantoisempana kuin mietinnössä joissakin kohdin

pidetään. Kyse on tämän hetken merkittävimmästä auktoritatiivisesta tulkintakannanotoista

siihen, millaisia rajoituksia yksityiselämän suoja asettaa luottamuksellisten

viestien erittelemättömälle massavalvonnalle, josta mietinnön ehdotuksessa on tietenkin

keskeisin osin kysymys.

Päädyn lausunnossani katsomaan, että

- Mietinnössä ehdotetut viestin sisältöön ja tunnistamistietoihin kohdistuvat tietoliikennetiedusteluvaltuudet

merkitsisivät ehdotetussa muodossaan syvälle käyvää,

todennäköisesti perusoikeuden ytimeen ulottuvaa, kajoamista yksityiselämän

suojaan ja luottamuksellisen viestin salaisuuteen.

- Näin pitkälle meneviä rajoituksia ei voitaisi hyväksyä tavallisen lain säätämisjärjestyksessä

sen paremmin PL 10.3 §:n mukaisen kvalifioidun lakivarauksen kuin

perusoikeuksien yleisen rajoitustestin valossa.

- Poikkeuslain välttämisen periaatteen vuoksi rajoituksia ei myöskään voitaisi hyväksyä

perustuslain 73 §:ssä tarkoitettuina poikkeuksina perustuslakiin.

- Perustuslain muutoskaan (10.3. §:n lakivarauksen poistaminen) ei ratkaisisi ongelmia,

koska

o ehdotukset eivät täytä perusoikeuksien yleistä rajoitustestiä

o ehdotukset ovat hyvin todennäköisesti ristiriidassa niiden tulkintaperiaatteiden

kanssa, joita EU:n tuomioistuin noudatti massavalvontaa koskevassa

Digital Rights Ireland –ratkaisussaan.

- Jatkovalmistelua ei ole perusteltua jatkaa mietinnössä esitetyn mallin pohjalta.

Sen sijaan olisi syytä tarkemmin tarkastella, missä määrin tietoliikennetiedustelua

on mahdollista toteuttaa poliisilla nykyisten toimivaltuuksien pohjalta.

***Lähtökohdat perus- ja ihmisoikeuksien kannalta***

Kuten työryhmän mietinnössä esitetään, tiedustelulainsäädäntö ja varsinkin yksilöiden

luottamuksellisten viestien sisältöön sekä tunnistamistietoihin kohdistuva valvonta merkitsee

tyypillisesti puuttumista etenkin yksityiselämän suojaa, luottamuksellisen viestin

salaisuutta sekä henkilötietojen suojaa koskeviin ihmis- ja perusoikeuksiin. Nämä oikeudet

on turvattu Suomen Perustuslain 10 §:ssä, YK:n kansalaisoikeuksia ja poliittisia

oikeuksia koskevan yleissopimuksen (KP-sopimus) 17 artiklassa, Euroopan ihmisoikeussopimuksen

(EIS) 8 artiklassa sekä Euroopan Unionin perusoikeuskirjan 7 ja 8 artikloissa.

Näiden oikeuksien soveltamisalaan ja rajoitettavuuteen liittyviä kysymyksiä on käsitelty

varsin tarkasti jo mietinnössä (s. 51-60), enkä ala tässä toistaa siinä esitettyjä näkökohtia.

Verkkovalvonnan kannalta merkillepantavaa lähinnä on, etteivät yksityiselämän suojaa

koskevat perus- ja ihmisoikeudet ole ehdottomia, vaan niitä saadaan rajoittaa muun

muassa yhteiskunnan turvallisuuden toteuttamiseksi. Pelkästään tällaisen hyväksyttävän

rajoitusperusteen käsilläolo ei kuitenkaan riitä, vaan myös muiden rajoitusedellytysten

on täytyttävä, mukaan lukien perustuslain 10 §:n 3 momentissa mainitut luottamuksellisen

viestin salaisuutta koskevat erityiset rajoitusedellytykset. Tämän työryhmä selvästi

on kuitenkin havainnut, mikä voidaan päätellä muun muassa siitä, että mietinnössä eh3

dotetaan harkittavaksi perustuslain muuttamista lähinnä sillä perusteella, ettei ehdotetunkaltaista

tiedustelutarkoituksessa harjoitettavaa verkkovalvontaa voida perustuslain

10.3 §:ssä mainittujen edellytysten valossa hyväksyä tavallisena lakina.

Asia, mihin mietinnössä ei kuitenkaan kovinkaan paljoa kiinnitetä huomiota, liittyy päällekkäisten

oikeussuojajärjestelmien keskinäissuhteisiin. Tältä osin vakiintunut oikeudellinen

lähtökohta on, että jos ja kun samaan tapaukseen tai tilanteeseen tulee sovellettavaksi

useita päällekkäisiä oikeussuojajärjestelmiä, oikeuksien *vähimmäissisältö* määrittyy

varsinkin yksilön ja julkisen vallan välisissä vertikaalisuhteissa sen järjestelmän mukaan,

joka antaa kyseiselle *yksilön oikeudelle parhainta suojaa*. Tämä pääperiaate ilmenee

muun muassa Euroopan ihmisoikeussopimuksen 53 artiklasta, jonka mukaan minkään

ihmisoikeussopimuksessa ei pidä katsoa rajoittavan tai loukkaavan lainsäädännössä

turvattuja tai jossain muussa jäsenvaltion allekirjoittamassa sopimuksessa tunnustettuja

ihmisoikeuksia ja perusvapauksia. Samansisältöinen määräys sisältyy myös muun muassa

EU:n perusoikeuskirjan 53 artiklaan ja sen on katsottu olevan voimassa Suomessa

myös yleisenä valtiosääntöperiaatteena muun muassa sen seurauksena, että perusoikeuksien

rajoitukset eivät saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden

kanssa (ks. PeVM 25/1994 vp s. 4 ja 5). EU-oikeuden etusijaperiaatteesta puolestaan

seuraa, EU:n perusoikeuskirjan kanssa ristiriitaiset kansallisen oikeusjärjestyksen

säännökset on jätettävä EU-oikeuden soveltamisalueella soveltamatta.

Suomalaisissa valtiosääntökäytännöissä on tämän lisäksi lähdetty siitä, että perusoikeudet

saavat vähimmäissisältönsä suoraan vastaavia oikeuksia koskevista kansainvälisistä

ihmisoikeussopimuksista, kun taas perustuslaissa on tarkoitus määritellä sellaiset yksilön

oikeuksien paremmat ehdot joista haluamme kansallisesti sopia. Korkein oikeus on esimerkiksi

katsonut oikeuskäytännössään, että perustuslain 10 §:ssä tarkoitettua yksityiselämän

suojaa tulee tulkita vähintään yhdenmukaisesti Euroopan ihmisoikeussopimuksen

8 artiklan ja sen oikeuskäytännön kanssa. Tämän seurauksena korkein oikeus on

katsonut, että tavallinen laki voi olla perustuslain 106 §:ssä tarkoitetulla tavalla ilmeisessä

ristiriidassa perustuslain kanssa myös silloin, kun sen soveltaminen olisi selvästi ja

riidattomasti ristiriidassa Euroopan ihmisoikeustuomioistuimen ratkaisuissa omaksutun

tulkintalinjan kanssa, ja että tällainen laki tulee jättää PL 106 §:n nojalla soveltamatta

(Ks. KKO 2012:11). Vastaavalla tavalla korkein oikeus on tuoreessa ennakkopäätöksessään

jättänyt soveltamatta eräät oikeudenkäymiskaaren valituksen sillensä jättämistä

koskevat säännökset, kun noiden säännösten soveltaminen olisi ollut selvästi ristiriidassa

EIS 6 § artiklaa koskevan oikeuskäytännön kanssa, ja kun PL 21 §:ää oli tulkittava yhdenmukaisesti

EIS 6 §:n oikeuskäytännön kanssa (ks. KKO 2015:14). Kansallisen lain

säännös voi siten olla voimassa olevan perustuslain vastainen sen vuoksi, että se on

Suomen kansainvälisten ihmisoikeusvelvoitteiden vastainen.

Tiivistäen: Suomalaista tiedustelulainsäädäntöä kehitettäessä joudutaan väistämättä ottamaan

huomioon paitsi perustuslaissa myös EU:n perusoikeuskirjassa sekä Suomea

sitovissa kansainvälisissä ihmisoikeussopimuksissa taatut yksityiselämän suojaa, luottamuksellisen

viestin salaisuutta sekä henkilötietojen suojaa koskevat perus- ja ihmisoikeudet.

Nämä oikeussuojajärjestelmät määrittävät yhdessä perus- ja ihmisoikeuksien

vähimmäissuojan tason. Perussoikeussuojaa alentamalla ei voida vaikuttaa oikeuksien

kansainväliseen tai eurooppalaiseen suojan tasoon. Tämä kansainvälinen ja eurooppalai4

nen taso sitoo kuitenkin myös viranomaisia, joiden on muun ohella perustuslain 22 §:n

mukaisesti turvattava perus- ja ihmisoikeuksien toteutuminen.

Käsittelen seuraavaksi tätä yleistä taustaa vasten tiedonhankintatyöryhmän mietintöön

sisältyviä kehittämisehdotuksia ja suuntaviivoja.

**Mietinnön keskeiset ehdotukset ja niiden arviointi**

***Tietoliikennetiedustelun toteuttamista koskevat ehdotukset***

Mietinnössä esitetään tietoliikennetiedustelun lähtökohdaksi sen toteuttaminen siten, että

tietoliikenteen joukosta voitaisiin seuloa mahdollisimman tehokkaasti tiedustelutehtävän

kannalta olennainen liikenne ja estää tehtäviin kuulumattoman liikenteen päätyminen

analysoinnin kohteeksi. Vaikka asiaa ei aivan selkeästi esitetäkään, kyse olisi ilmeisesti

hyvin laajamittaisesta, sekä viestien sisältöjä että niiden tunnistamistietoja selvittämään

pyrkivästä toiminnasta. Tarkkailtavia viestintäverkkoja ei ole mietinnössä yksilöity,

mutta ei toisaalta ole poissuljettu sitäkään, etteivätkö periaatteessa kaikki viestintäverkot

voisi olla tarkkailun kohteena. Nimenomaan todetaan, että myös se tietoliikenteen valtaosa,

jolla ei ole merkitystä kansallisen turvallisuuden kannalta, olisi automaattisesti suoritetun

vertailun kohteena.

Viestit seulottaisiin ensin automaattisesti. Ensivaiheen toiminnassa käytettävät hakuehdot

voisivat mietinnön mukaan olla tunnistamistietoja. Jotta tietoliikennetiedustelun

kohteena olevista uhista saataisiin riittävät tiedot, olisi hakuehtojen perusteella valikoidusta

viestinnästä kuitenkin voitava selvittää myös sisältö.

Mietintö jättää jossain määrin epäselväksi, miten tämä sisältöjen selvittäminen tapahtuisi

käytännössä ja kuinka suuri osa tarkkailtavasta viestinnästä joutuisi itse asiassa joko

koneellisesti tai manuaalisesti tapahtuvan sisällöllisen analyysin kohteeksi. Voitaneen

kuitenkin lähteä siitä, että siltä osin kuin viestiliikennettä tarkkaillaan, merkittävä joukko

tiedustelun kannalta merkityksetöntäkin viestintää on alkuvaiheessa tarkkailun kohteen

ja että viestien tunnistamistietoja ja mahdollisesti niiden sisältöjäkin on jo pitänyt merkittävässä

määrin analysoida ennen kuin viestintä tulee ”manuaalisen käsittelyn kohteeksi”.

Tällaista viestintää nimittäin tulee mietinnön mukaan pitää tiedustelutehtävän

kannalta lähtökohtaisesti merkittävänä ja tähän lopputulokseen voidaan tuskin päästä

ilman luottamuksellisen viestin salaisuuteen tapahtuvaa merkittävää kajoamista.

*Luottamuksellisten viestien sisällön selvittäminen ja ydinalueen suoja*

Perustuslain esitöiden mukaan perustuslain 10 §:n 2 ja 3 momentin luottamuksellisen

viestin salaisuutta koskevan sääntelyn ensisijaisena tarkoituksena on suojata luottamukselliseksi

tarkoitetun viestin sisältö ulkopuolisilta. Sääntely turvaa jokaiselle oikeuden

luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon

hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Säännös

ei suojaa vain viestin lähettäjää, vaan kyseessä on molempien viestinnän osapuolten

perusoikeus (HE 309/1993 vp , s. 53/II). Sama periaate on sittemmin vahvistettu useaan

otteeseen perustuslakivaliokunnan käytännössä (ks. esim. PeVL 33/2013 vp).

5

Ehdotetunkaltainen valvontajärjestelmä merkitsisi vaiheittainkin toteutettuna Suomessa

ennennäkemättömän syvällekäyvää *ja* laajamittaista puuttumista yksityiselämän suojaan

ja luottamuksellisen viestin salaisuuteen. Jollei tiedustelun käyttöä merkittävästi rajoiteta

esimerkiksi konkreetin rikosepäilyn perusteella, tarkoittaisi ehdotus käytännössä luottamuksellisen

viestin salaisuuden tekemistä tyhjäksi. Periaatteessa kenen tahansa harjoittama

viestintä olisi altis ensivaiheen seulonnalle, joka väistämättä – riippumatta kokonaan

siitä, että seulonta tehdään automaattisesti – murtaa viestin salaisuuden. Tilanne on

perusoikeuksien kannalta selvästi vakavampi, kuin se, mihin EU:n tuomioistuin kiinnitti

huomiota Digital Rights Ireland –tapauksessa. Siinähän EU-tuomioistuin katsoi, että

vaikka tietojen säilyttäminen, johon tietojen tallentamisvelvollisuutta koskevassa direktiivissä

2006/24 velvoitetaan, merkitsee erityisen vakavaa puuttumista näihin oikeuksiin,

se ei ole omiaan aiheuttamaan haittaa perusoikeuskirjan 7 artiklassa vahvistettujen oikeuksien

keskeiselle sisällölle, koska direktiivissä ei sallita tiedon saamista sähköisen viestinnän

sisällöstä sellaisenaan.

Tiedonhankintalakityöryhmän mietinnössä ehdotettu järjestely sen sijaan merkitsisi nimenomaisesti

tiedon hankkimista sähköisten viestien sisällöstä sellaisenaan. Jos tunnistamistietojen

tallentamista voitiin pitää erityisen vakavana puuttumisena yksityiselämän

suojaan, viestien sisältöjen selvittäminen nyt ehdotetulla tavalla merkitsee hyvin todennäköistä

yksityiselämän suojan keskeisen sisällön loukkausta. Perusoikeuskirjan 52 artiklan

1 kappaleen 1 virkkeen sanamuodon perusteella tällaisesta rajoituksesta ei voida

säätää lailla. Oikeuden keskeisen sisällön kunnioittaminen on toisin sanoen sikäli ehdoton,

ettei sen rajoittaminen ole sallittua vaikka rajoitusta perustelisi kuinka painava intressi

tahansa.

EU:n perusoikeusdoktriini vastaa suomalaista perusoikeuksien yleistä rajoitustestiä, jonka

mukaan perusoikeuksien rajoitus ei saa loukata perusoikeuden ydinaluetta (PeVM

25/1994 vp). Vaikka perustuslakivaliokunta ei käytännössä ole tähän mennessä vielä

joutunut soveltamaan ydinalueen loukkaamattomuuden vaatimusta siten, että sen olisi

katsottu estävän jonkin lain säätämisen tavallisen lain säätämisjärjestyksessä, ei valiokunnalla

toisaalta ole ollut vielä käsiteltävänään yhtään näin syvälle käyvästi ja laajamittaisesti

perusoikeuksiin puuttuvaa lakiehdotusta. Pidän hyvin mahdollisena, että ehdotetunkaltainen

järjestely todettaisiin perustuslakivaliokunnassa ydinalueen suojan vastaisena,

kun otetaan huomioon sekä EU-tuomioistuimen kanta, että tapa, jolla perustuslakivaliokunta

seurasi siinä esitettyjä kantoja tietoyhteiskuntakaarta koskevassa lausunnossaan

PeVL 18/2014 vp. Merkitystä tässä on myös valvonnan massamuotoisuudella. Kuten

EU-tuomioistuin totesi, tallentamisvelvollisuus oli perusoikeuskirjan 7 ja 8 artikloiden

kannalta ongelmallinen myös sen vuoksi, että tietojen säilyttäminen ja niiden myöhempi

käyttö ilman, että tilaajalle tai rekisteröidylle käyttäjälle ilmoitetaan siitä, voi aiheuttaa

kyseisille ihmisille tunteen siitä, että heidän yksityiselämänsä on jatkuvan tarkkailun

kohteena.

On ilmeistä, että sama argumentti on perustuslain kannalta merkittävä myös kansallisella

tasolla ja tilanteessa, jossa merkittävä osa tietoverkoissa harjoitettavasta viestinnästä on

jatkuvan sisällöllisen tarkkailun kohteena.

Jos kuitenkin katsottaisiin, että sisältöön kohdistuva massavalvonta ei loukkaisi luottamuksellisen

viestin salaisuuden ydintä, pitäisi sen täyttää vielä perusoikeuksien yleiset

6

rajoitusedellytykset. Mietinnössä todetaankin tältä osin (s. 69), että ”tietoliikennetiedustelun

hyväksyttävyyttä harkittaessa on arvioitava sitä, onko toiminnasta kansalliselle

turvallisuudelle aiheutuva hyöty suurempi kuin toiminnasta mahdollisesti aiheutuva haitta

yksityisyyden suojalle sekä kansantaloudelle ja yrityksille.” Oikeasuhtaisuusvaatimuksen

liittyy kuitenkin kiinteästi myös vaatimus rajoituksen täsmällisyydestä ja tarkkarajaisuudesta.

Tältä osin mietinnössä viitataan sinänsä asianmukaisesti EIT:n ja EUtuomioistuimen

oikeuskäytäntöön. Kuten sivulla 64 todetaan, EIT:n mukaan laista on

riittävän selkeästi käytävä ilmi, missä olosuhteissa ja millä edellytyksellä kansalaiset

voivat joutua viranomaisten salaisesti toteutettavan tarkkailun kohteeksi. Lisäksi edellä

jo mainittu Digital Rights Ireland -tuomio edellyttää henkilötietojen käsittelyn rajaamista

ennakkoon.

Niin kuin työryhmä toteaa, nämä reunaehdot on otettava huomioon tietoliikennetiedustelun

toteuttamista harkittaessa. Ilmeisesti tässä tarkoituksessa siinä ehdotetaankin menetelyä,

jossa tietoliikenteestä erotetaan ensin ne tiedot, joilla on merkitystä kansallisen

turvallisuuden kannalta. Mietinnössä todetaankin, että ”eräs tapa täyttää vaatimukset

olisi käyttää toiminnan suuntaamiseen riittävän tarkkoja ennakkoon määrättyjä hakuehtoja

tai kansallista turvallisuutta vaarantavan toiminnan sanallisia kuvailuja, jotka mahdollisimman

konkreettisesti luonnehtisivat tiedonhankinnan kohdetta.”

Tällainen rajaus ei luonnollisestikaan vastaa niitä vaatimuksia, joita EIT:n ja EUtuomioistuimen

oikeuskäytännössä tarkoitetaan. Kun sanahaut kohdistuisivat kuitenkin

periaatteessa ennalta rajoittamattomaan joukkoon yksityistä viestintää, eivät ne lainkaan

rajaa niitä olosuhteista ja edellytyksiä, joiden vallitessa ihmiset voivat joutua viranomaisten

salaisesti toteutettavan tarkkailun kohteeksi. Kaikki ovat edelleenkin tarkkailun

kohteina, tarkkailu vain toteutetaan rajatuilla sanahauilla.

Käsitykseni mukaan Suomen oikeusjärjestys ei tällä hetkellä mahdollista tietoverkoissa

harjoitettavan viestinnän sisältöjen massavalvontaa ehdotetussa muodossa eikä tätä tarkoittavan

lainsäädännön valmistelua ole nähdäkseni syytä jatkaa ainakaan mietinnössä

esillä olevalta pohjalta. Pidän myös selvänä, että lopputulos on sama riippumatta siitä,

sisältyykö perustuslain 10 §:n 3 momenttiin nykyisenkaltainen kvalifioitu lakivaraus vai

ei. Ehdotetunkaltainen tarkkailuvaltuus merkitsisi hyvin todennäköisesti yksityiselämän

ydinalueen suojan loukkausta, eikä se tämän johdosta täyttäisi perusoikeuksien yleisiä

rajoitusedellytyksiä.

*Tunnistamistietoja koskeva tietoliikennetiedustelu*

Mietinnössä käsitellään myös mahdollisuutta käyttää tietoliikennetiedustelua erilaisten

luottamukselliseen viestintään liittyvien tunnistamistietojen hankkimiseen tiedustelutarkoituksessa.

Arvioin seuraavaksi mahdollisuutta toteuttaa ehdotetunkaltainen tiedustelu

tunnistamistietoihin rajattuna, mutta edelleen massamuotoisena, lähtökohtaisesti kaikkeen

verkkoviestintään ulottuvana valvontana.

Perus- ja ihmisoikeudet antaa turvaa myös sellaisille muillekin kuin viestin sisältöä koskeville

tiedoille, joilla voi olla merkitystä viestin säilymiselle luottamuksellisena. Tällaisina

tietoina on jo perustuslain esitöissä pidetty esimerkiksi viestien tunnistamistietoja.

7

(HE 309/1993 vp , s. 53/II). Tunnistamistiedot ovat kuitenkin vanhastaan jääneet luottamuksellisen

viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (ks.

esim. PeVL 6/2012 vp , s. 3/II, PeVL 66/2010 vp , s. 7/I, PeVL 29/2008 vp , s. 2/II).

Tämän seurauksena tunnistamistietojen luottamuksellisuuteen on saatettu kajota lievemmillä

perusteilla kuin mikä olisi mahdollista viestien sisällön suhteen. Perustuslakivaliokunta

on esimerkiksi pitänyt mahdollisena, että tunnistamistietojen saaminen jätetään

sitomatta tiettyihin perustuslain 10 §:n 3 momentissa mainittuihin rikostyyppeihin,

jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset (ks. esim. PeVL

66/2010 vp , s. 7/I, PeVL 29/2008 vp , s. 2/II).

Tulkinta-asetelma on kuitenkin jossain määrin muuttunut perustuslakivaliokunnan tietoyhteiskuntakaarta

koskevan lausunnon PeVL 18/2014 vp sekä EU-tuomioistuimen Digital

Rights Ireland –tuomion johdosta. Perustuslakivaliokunta toteaa lausunnossaan nimittäin

EU-tuomioistuimen tuomioon viitaten nimenomaisesti, että sähköisen viestinnän

käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen

voivat käytännössä kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin

ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua,

vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen.

Samoin valiokunta kiinnittää huomiota siihen, että ”Unionin tuomioistuimen tuomion

perusteella on pääteltävissä, että pelkästään säilytettävien tietojen laaja kattavuus - kaikki

ihmiset, kaikki sähköisen viestinnän välineet ja kaikki viestintätiedot - on oikeasuhtaisuuden

kannalta ongelmallista”. Kuten perustuslakivaliokunta toisaalta toteaa, avoimeksi

kuitenkin jää, merkitseekö viranomaistarpeita varten säädetyn tunnistamistietojen säilyttämisvelvollisuuden

ulottuminen käytännössä kaikkien sähköisiä viestimiä käyttävien

ihmisten tietoihin jo yksinään – siis sellaisenaan – oikeasuhtaisuusvaatimuksen loukkausta.

Asiasta on EU:n jäsenvaltioiden valtiosääntökäytännöissä ja kommentaarikirjallisuudessa

esitetty kaksi vaihtoehtoista tulkintalinjaa. Tiukan tulkintalinjan mukaan EUtuomioistuimen

tuomio johtaa käytännössä väistämättä siihen, että yleinen tallentamisvelvollisuus

on sellaisenaan perusoikeuskirjan 7 ja 8 artiklan vastainen. Tämä kanta perustuu

etenkin siihen, mitä EU-tuomioistuin toteaa perustelukappaleissa 58-59. Kyseisissä

kappaleissa tuomioistuin kiinnittää huomiota erityisesti siihen, että direktiivi asettaa

velvoitteen tallentaa erottelematta kaikki direktiivin soveltamisalaan kuuluvat tiedot.

Ongelmana siis oli, että direktiivi koski

”yleisellä tavalla sähköisiä viestintäpalveluja käyttäviä kaikkia henkilöitä ilman,

että henkilöt, joiden tietoja säilytetään, olisivat edes epäsuorasti sellaisessa tilanteessa,

joka voisi johtaa rikosoikeudellisiin toimiin. Sitä sovelletaan 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. Siinä ei myöskään säädetä minkäänlaisesta poikkeuksesta,

joten sitä sovelletaan jopa henkilöihin, joiden viestintään sovelletaan kansallisen

lainsäädännön mukaan salassapitovelvollisuutta.”

Tämän ongelman merkitystä korosti EU-tuomioistuimen tulkinnassa myös se, ettei direktiivissä

vaadittu minkäänlaista yhteyttä säilytettäviksi säädettyjen tietojen ja yleistä

turvallisuutta koskevan uhan välillä, eikä siinä varsinkaan rajoituttu säilyttämään joko

8

tiettyyn ajanjaksoon ja/tai maantieteellisesti määriteltyyn alueeseen ja/tai sellaisten tiettyjen

henkilöiden piiriin, jotka voisivat olla sekaantuneita tavalla tai toisella vakavaan

rikollisuuteen, liittyviä tietoja, tai henkilöihin, joiden tietojen säilyttäminen voisi muilla

perusteilla myötävaikuttaa vakavan rikollisuuden ehkäisemiseen, selvittämiseen tai syyteharkintaan,

liittyviä tietoja.

EU-tuomioistuin näyttää siis pitävän erityisen ongelmallisena sellaista tunnistamistietojen

tallentamisvelvollisuutta, jota sovellettaisiin yleisesti kaikkiin, siis lähtökohtaisesti

myös sellaisiin ihmisiin, joilla ei ole minkäänlaista yhteyttä, ei edes etäistä, tallentamisvelvollisuuden

tavoitteena olevaan vakavien rikosten torjuntaan. Tämä lähtökohta lienee

ollut myös yksi keskeinen peruste sille, että eräiden jäsenvaltioiden valtiosääntötuomiot

ovat EU-tuomioistuimen tuomion jälkeen (ja osin jo sitä ennen) pitäneet tunnistamistietojen

tallentamisvelvollisuutta koskevaa lainsäädäntöä perustuslain vastaisena.1

Toisaalta eräissä jäsenvaltioissa on omaksuttu joustavampi tulkinta. Esimerkiksi perustuslakivaliokunta

katsoi, ettei Digital Rights Ireland -tuomiosta johdu suoranaista estettä

sellaiselle sääntelylle, jossa oikeasuhtaisuuden vaatimukset toteutetaan muilla tavoin,

kuten rajaamalla säilytettävät tiedot vain siihen, mitä pidetään välttämättömänä sääntelyn

taustalla olevan tarkoituksen eli vakavien rikosten tutkimisen, selvittämisen ja syyteharkintaan

asettamisen kannalta.

Vaikka joustavamman tulkinnan kautta näyttäisikin avautuvan mahdollisuus toteuttaa

mietinnössä ehdotetunkaltaista verkkovalvontaa vain tunnistamistietoihin rajautuen,

eroaa tietoliikennetiedustelu kuitenkin eräissä merkittävissä suhteissa teleoperaattoreille

asetettavasta tunnistamistietojen tallentamisvelvollisuudesta. Tallentamisvelvollisuus

koskee ensinnäkin teleyritysten velvollisuutta säilyttää tietoja viranomaistarpeita varten.

Suurelta osin kysymys on sellaisten tietojen tallentamisajan jatkamisesta, joita teleyritykset

tallentavat muutoinkin laskutustarpeita varten. Tietoja ei myöskään välittömästi

käsitellä rikoksentorjunnan tarkoituksessa, vaan säilytettäviä tietoja voivat saada ainoastaan

ne viranomaiset, joilla on jonkun muun lain perusteella oikeus saada tiedot. Esimerkiksi

tietojen saaminen pakkokeinolaissa ja poliisilaissa tarkoitetuista televalvontatiedoista

edellyttää näiden lakien perusteella tuomioistuimen lupaa.

Tiedonhankintalakityöryhmän mietinnössä on sinänsä hahmoteltu ansiokkaasti tietoliikennetiedustelun

organisoinnin tapoja ja siihen liittyviä oikeusturvatakeita. Perusongelmaksi

kuitenkin jää, että tiedustelu merkitsisi välitöntä puuttumista lähtökohtaisesti suuren

ja erittelemättömän ihmisoikeusjoukon luottamuksellisen viestin salaisuuteen. Viestiliikennetietoihin

kohdistuva seulonta ei kytkeytyisi välttämättä mihinkään konkreettiseen

rikosepäilyyn, koska kyse olisi edelleenkin varhaisvaiheen tietojen” keräämistä

luottamuksellisista viesteistä tarkoituksessa vaikuttaa ja varautua “uhkiin, riskeihin,

mahdollisuuksiin ja muutoksiin”. Niin kauan kuin tiedustelu sidotaan näin abstrakteihin

vaaroihin, ei yksityiselämään puuttumiselle oikeastaan ole osoitettavissa sellaista vält-

1 Ks. esim. Itävallan valtiosääntötuomioistuimen ratkaisu G 47/2012, 27.6.2014, ks.

myös ratkaisua koskeva lehdistötiedote https://www.vfgh.gv.at/cms/vfghsite/

attachments/1/5/8/CH0006/CMS1409900579500/press\_releasedataretention.pdf. Ks.

vastaavasti myös Romanian perustuslakituomioistumen tuomio 8.7.2014, lehdistötiedote

http://www.ccr.ro/noutati/COMUNICAT-DE-PRES-99

9

tämätöntä perustetta, jota puuttumisen rajoittaminen edellyttää. Tiedustelun tavoitteiden

yleisluontoisuudesta ja epätarkkuudesta myös seuraa, että oikeusturvakeinojen tehokkuus

jää herkästi olemattomaksi. Mitä yleisempi ja epämääräisempi tavoite asetetaan

valvonnan perusteeksi, sitä laajemmaksi muodostuu luonnollisesti myös tiedustelua harjoittavien

viranomaisten harkintavalta ja sitä hankalampaa on myöhemmin osoittaa, että

viranomaiset olisivat menetelleet asiassa lainvastaisesti.

*Haittaohjelmat*

Mietinnössä käsitellään myös jonkin verran haittaohjelmien havaitsemiseen tähtäävää

tietoliikennetiedustelua. Tarkoituksena on tällöin havaita haittaohjelmien avulla toteutettavaa

tietoverkkovakoilua, tulisi myös sisältöön kohdistuvia hakuehtoja voida poikkeuksellisesti

käyttää heti ensivaiheessa. Mietinnön mukaan hakuehtona olisi tällöin tekninen

haittaohjelmatunniste, ja toimintamalli olisi sama kuin tietoyhteiskuntakaaren 272 §:ssä

säädetyssä toiminnassa.

Haittaohjelmien tunnistaminen tiedustelutarkoituksessa ei nähdäkseni muodostu perustuslain

kannalta ongelmalliseksi. Viittaan tältä osin varsinkin perustuslakivaliokunnan

lausuntoon sähköisen viestinnän tietosuojalaista (PeVL 9/2004 vp). Tuolloin valiokunta

kiinnitti haittaohjelmien poistamista koskevaa sääntelyä koskevassa arviossaan huomiota

etenkin siihen, että sääntelyn keskeisenä tarkoituksena on viestinnän eri osapuolten

etujen mukaisesti turvata tietoverkkojen toimivuutta ja turvallisuutta sekä näin luoda

edellytyksiä sananvapauden käyttämiselle ja viestinnän luottamuksellisuudelle tietoverkoissa.

Kysymys oli siis nimenomaan viestinnän luottamuksellisuuden varmistamiseen

tähtäävistä toimenpiteistä eikä sen suoranaisista rajoituksista. Sääntely ei valiokunnan

mielestä ollut käsillä olevassa yhteydessä lähtökohdiltaan ongelmallinen perustuslain 10

§:ssä turvatun luottamuksellisen viestin salaisuuden kannalta eikä merkitse perustuslain

12 §:n 1 momentissa tarkoitettua viestinnän ennakollista estettä. Tämä sama lähtökohta

pätee haittaohjelmiin myös silloin kuin niiden havaitseminen ja poistaminen tapahtuu

tiedustelutarkoituksessa.

***Perustuslain muuttamista koskeva esitys***

Mietinnössä esitetään (s. 80), ettei tiedustelutarkoituksessa toteutettavasta tietoliikennetiedustelusta

”näyttäisi olevan mahdollista säätää perustuslakia muuttamatta, pelkästään

vieraan valtion tietoliikenteeseen kohdistuvaa tiedustelua ehkä lukuun ottamatta”.

Tätä kantaa mietinnössä käsiteltyjen tiedusteluvaltuuksien ongelmallisuudesta voidaan

pitää valtiosääntöoikeudellisesti oikeana, joskin se on esitetty tarpeettomasti konditionaalimuodossa.

Kun mietinnössä tarkoitetaan tiedustelulla ”varhaisvaiheen tietojen”

keräämistä luottamuksellisista viesteistä tarkoituksessa vaikuttaa ja varautua “uhkiin,

riskeihin, mahdollisuuksiin ja muutoksiin”, ei tällainen toiminta mitenkään vastaa perustuslain

vaatimusta lailla säädettävistä *välttämättömistä* rajoituksista viestin salaisuuteen

yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien *rikosten tutkinnassa,*

*oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.*

Ehdotettu tietojen kerääminen puuttuisi luottamuksellisen viestin salaisuuteen, mutta

siltä selvästi puuttuisi tällaiselta puuttumiselta perustuslaissa edellytetty peruste. Ehdote10

tunkaltaiset valtuudet eivät mahdu PL 10 §:n 3 momentin rajoitusedellytysten sisään

vaikka perustuslakivaliokunnan käytännössä rikosten tutkinnan käsitettä onkin tulkittu

osin laajentavasti siten, ettei momentissa tarkoitetun rikoksen ole tarvinnut edetä toteutuneen

teon asteelle. Tällöinkin perustuslakivaliokunta on säännönmukaisesti edellyttänyt,

että luottamuksellisen viestin salaisuuteen puuttuviin toimenpiteisiin ryhdytään vasta

*jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta*. (Ks. esim. PeVL 49/2014 vp

ja siinä mainitut PeVL 19/2008 vp , s. 3-4, PeVL 37/2002 vp , s. 3).

Valtiosääntöoikeudelliset ongelmat eivät kuitenkaan välttämättä poistu yksinkertaisesti

perustuslakia muuttaen esimerkiksi poistamalla nyt ongelmia aiheuttava lakivaraus perustuslaista.

Tällaisen muutoksen jälkeenkin yksityiselämänsuojan ja henkilötietojen

suojan sekä luottamuksellisen viestin salaisuuden rajoitusten tulisi täyttää perusoikeuksien

yleiset rajoitusedellytykset, ml. oikeasuhtaisuuden vaatimus samoin kuin vaatimus

siitä, että rajoitusten on oltava sopusoinnussa Suomen kansainvälisten ihmisoikeusvelvoitteiden

kanssa. Perustuslain muutoksilla ei myöskään ratkaistaisi mahdollisia ristiriitoja

EU-oikeuden kanssa, millä on merkitystä erityisesti sen vuoksi, että EUtuomioistuimen

*Digital Rights Ireland* –tapauksessa omaksuma tulkinta yksityiselämän

suojasta asettaa merkittäviä rajoituksia yksityisten viestien massavalvonnalle. Palaan

näihin kysymyksiin jäljempänä.

*Poikkeuslakimenettelyn käyttö*

Mietinnössä ei käsitellä mahdollisuutta säätää tiedonhankintalaki poikkeuslakina. Tämä

olisi kuitenkin periaatteessa yksi Suomen perustuslain sinänsä mahdollistama ratkaisu.

Tällöin, koska laki on ristiriidassa perustuslain kanssa, se voitaisiin säätää ts. perustuslain

73 §:ssä tarkoitettuna rajattuna poikkeuksena perustuslakiin ilman että samalla kuitenkaan

muutettaisiin perustuslakia.

Tämä mahdollisuus on kuitenkin viimeaikaisten valtiosääntökäytäntöjen valossa lähinnä

teoreettinen. Poikkeuslakien säätämiseen on perustuslakivaliokunnan käytännössä suhtauduttu

erittäin pidättyvästi ja varsinkin silloin, kun syyt poikkeuslain säätämiselle ovat

puhtaasti kansallisia. (ks. PeVL 67/2014 vp, s. 14 ja siinä mainitut perustuslain esityöt

ja perustuslakivaliokunnan lausunnot). Käsitykseni mukaan on hyvin todennäköistä,

ettei perustuslakivaliokunta tulisi hyväksymään poikkeuslakimenettelyn käyttämistä

säädettäessä laajamittaista verkkotiedustelua koskevaa lakia. Tällainen poikkeus merkitsisi

hyvin syvällekäyvää ja pysyväisluonteista poikkeamista perusoikeuden ydinsisällöstä

eikä se siinäkään mielessä ole vaikeuksitta yhteen sovitettavissa perustuslain 73 §:n

vaatimukseen rajatusta poikkeuksesta.

***Johtopäätökset***

Olen lausunnossani joutunut ottamaan varsin kriittisen kannan mietinnössä ehdotettuihin

tiedusteluvaltuuksiin lukuun ottamatta haittaohjelmien tunnistamista. Kritiikki saattaa

johtua osaltaan siitä, että tarkasteltavana oleva mietintö on vielä luonteeltaan esiselvitys

eikä se sellaisenaan sisällä kovinkaan tarkkoja konkreettisia ehdotuksia. Kun toisaalta

kyse on perusoikeuksia merkittävästi rajoittavista toimenpiteistä, joita koskevalta sääntelyltä

voidaan edellyttää erityistä tarkkuutta ja täsmällisyyttä, voi asetelma johtaa tarpeet11

toman epäileviin lopputuloksiin. Niin tai näin, perusongelmaksi silti jää, että ehdotetunkaltainen

laajamittainen ja erittelemätön tietoliikennetiedustelu muodostuu lähtökohdiltaan

hyvin herkästi perustuslainvastaiseksi. Yksinkertaisin ratkaisu näihin ongelmiin on

kytkeä tiedustelutoiminta konkreettisiin ja yksilöityihin rikosepäilyihin ja niin ollen täydentämään

muilla keinoilla jo hankittuja tai saatuja tietoja.

Kuten mietinnössäkin todetaan, poliisin tiedonhankintatoimivaltuudet on pakkokeino- ja

poliisilain osalta vastikään uudistettu ja niissä tiedonhankintatoimivaltuuksien käyttö on

sidottu rikoksen ennalta estämiseen ja paljastamiseen. Valtion tiedustelutarpeiden kannalta

saattaa tietenkin muodostua ongelmaksi, ettei suojelupoliisille ole ”säädetty erityisiä

toimivaltuuksia tiedusteluun liittyvää tiedonhankintaa varten vaan sen tiedonhankintatoimivaltuudet

perustuvat poliisia koskeviin yleislakeihin”. Ehkä onkin niin, että *poliisi*

*koskevissa yleislaeissa olevat tiedonhankintavaltuudet jo osoittavat sen rajan, jolla*

*perustuslain 22 §:ssä tarkoitettu julkinen valta saa harjoittaa salaista tiedustelutoimintaa,*

*kun sen kuitenkin on samanaikaisesti turvattava myös perus- ja ihmisoikeuksien*

*toteutuminen.*

Tampereella 9.4.2014

Juha Lavapuro

apulaisprofessori