***Puolustusministeriölle***

**Asia**: Asiantuntijalausunto tiedonhankintalakityöryhmän mietinnöstä

**Viite**: Sähköpostitse 6.3.2015 saatu lausuntopyyntö ja siinä viitattu 9.2.2015 päivätty yleinen lausuntopyyntö FI.PLM.2015-218; 909/40.02.00/2013

Pyydettynä asiantuntijalausuntona esitän kunnioittavasti seuraavaa.

Asiakohdassa mainittua mietintöä ei ole laadittu hallituksen esityksen muotoon eikä se muutoinkaan sisällä selkeitä ehdotuksia lainsäädännön sisällöksi tai muiksi toimenpiteiksi. Julkisessa lausuntopyynnössä lausunnonantajien on toivottu lausuvan erityisesti lukujen 6 ja 7 kehittämisehdotuksista ja johtopäätöksistä. Pyrin noudattamaan tätä pyyntöä lausunnossani.

Keskityn tässä lausunnossa arvioimaan työryhmän mietinnössä esitettyjä olettamuksia, argumentteja ja alustavia ehdotuksia Suomen perustuslaissa ja Euroopan Unionin perusoikeuskirjassa turvattujen perusoikeuksien sekä kansainvälisissä ihmisoikeussopimuksissa turvattujen ihmisoikeuksien suojan näkökulmasta. Lausunnon lopussa kuitenkin tarkastelen lyhyesti myös työryhmän kannanottoja koskien valtioiden välistä ns. vakoilua.

**I. Arvioinnin peruslähtökohdat**

Suomen kansalaisten, muiden Suomessa asuvien ja ulkomailla asuvien käyttämiin sähköisen kommunikaation välineisiin ja niihin liittyviin tietoverkkkoihin kohdistuva Suomen viranomaisten harjoittama tarkkailutoiminta kohdistuu väistämättä kyseisten yleisten viestintäpalvelujen käyttäjien perusoikeuksiin ja ihmisoikeuksiin, muodostuen niihin kohdistuvaksi *kajoamiseksi* (interference). Jos kyseessä on kaikki asiaan vaikuttavat seikat huomioon ottaen oikeudellisesti hyväksyttävä kajoaminen, puhumme perusoikeuden tai ihmisoikeuden *rajoittamisesta* (limitation tai restriction). Jos taas kajoaminen – jälleen kaikki asiaan vaikuttavat seikat huomioon ottaen – on oikeudellisesti ei-hyväksyttävä, kyseessä on perusoikeuden tai ihmisoikeuden *loukkaus* (violation). Kansakunnan elämää uhkaavan ja virallisesti julistetun yleisen hätätilan aikana valtio voi *poiketa* (derogate) eräistä perus- tai ihmisoikeuksista, mikä siirtää kielletyn loukkauksen ja hyväksyttävän rajoituksen välistä rajalinjaa mutta ei poista tuon perustavan erottelun tärkeyttä.

Mietinnössä hahmoteltu verkkovalvonta kohdistuu ensi sijassa ja välittömästi siihen perus- ja ihmisoikeuksien ryhmään, joka koostuu yksityisyyden tai yksityiselämän suojasta ja henkilötietojen suojasta. Nämä oikeudet on turvattu mm. Suomen Perustuslain 10 §:ssä, Euroopan ihmisoikeussopimuksen 8 artiklassa, YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskevan yleissopimuksen 17 artiklassa sekä Euroopan Unionin perusoikeuskirjan 7 ja 8 artikloissa. Verkkovalvonnalla saattaa olla vaikutuksia myös muihin perus- ja ihmisoikeuksiin, kuten sananvapaus, yhdistymisvapaus, kokoontumisvapaus, uskonnonvapaus, yhdenvertaisuus ja syrjinnän kielto, liikkumisvapaus, omaisuuden suoja ja oikeus työhön. Johtamassani SURVEILLE-tutkimushankkeessa (ks. jäljempänä) tehty tutkimus kuitenkin osoittaa, että tarkkailuteknologioiden käytön kattava ja kokonaisvaltainen perusoikeusvaikutusten arviointi – myös suhteessa sivullisiin – yksityisyyden suojan ja tietosuojan kannalta yleensä tavoittaa perus- ja ihmisoikeuksiin kohdistuvat vaikutukset myös yleisellä tasolla eikä vain suhteessa näihin oikeuksiin. Tämä johtuu siitä, että pyrkiessämme kvantifioimaan tarkkailuteknologioiden käytöstä seuraavaa perusoikeuteen kajoamisen astetta, saamme säännönmukaisesti vakavimman puuttumisen kun tarkastelun kohteena ovat yksityisyyden suoja ja henkilötietojen suoja.

Jäljempänä (jaksossa II) jäsennän tarkasteluni seuraavien viiden ehdon varaan, joiden vallitessa perus- tai ihmisoikeuteen kajoamista voidaan pitää oikeudellisesti hyväksyttävänä rajoituksena:

1. Rajoitus ei saa kohdistua oikeuden loukkaamattomaan ydinsisältöön.
2. Rajoituksen tulee olla laissa säädetty, ts. sillä on oltava oikeusvaltiollisesti hyväksyttävä säädösperusta.
3. Rajoituksen on palveltava hyväksyttävää tarkoitusperää.
4. Rajoituksen on oltava välttämätön (tai todistetusti tarpeellinen) tuon hyväksyttävän tarkoitusperän saavuttamiseksi.
5. Perus- tai ihmisoikeuteen kohdistuvan rajoituksen on oltava oikeasuhtainen verrattuna siihen hyötyyn, mikä toimenpiteellä saavutetaan sen perusteena käytetyn hyväksyttävän tarkoitusperän toteuttamiseksi.

**II. Perus- tai ihmisoikeuksien rajoitusten viisi hyväksyttävyysehtoa**

***(1) Perusoikeuden ydinsisällön loukkaamattomuus: tunnistamistiedot ja viestin sisältö***

Verkkovalvonta saattaa kohdistua yksityisyyden suojan tai henkilötietojen suojan ydinsisältöön ja olla siksi oikeudellisesti ei-hyväksyttävä riippumatta siitä, miten se muutoin on järjestetty. Esimerkiksi henkilön sukupuolisen suuntautumisen tai psykiatrisen diagnoosin selvittäminen verkkovalvonnan kautta murtamalla ja julkistamalla hänen luottamuksellisiksi tarkoittamiensa ja erityisessä luottamussuhteessa lähettämiensä viestien sisältö merkitsisi kiellettyä kajoamista yksityisyyden suojan ytimeen. Perinteisesti on lähdetty siitä, että luottamuksellisen viestin *sisältö* saattaisi kuulua yksityisyyden suojan ydinalueeseen, mutta vastaavasti viestin *tunnistamistiedot* eli tiedot esimerkiksi lähettäjän ja vastaanottajan IP-osoitteista ja lähetysajasta eivät kuuluisi. *It’s only metadata*, kuuluu vanha sanonta.

Kuvattu perinteinen käsitys on vanhentunut eikä sitä tule Suomessa hyväksyä uusien lainsäädäntöhankkeiden lähtökohdaksi. Tunnistamistietojen kategorian nopea laajeneminen ja mahdollisuus yhdistellä tunnistamistietojen eri tyyppejä keskenään, mukaan lukien algoritmien ja automaattisen tietojenkäsittelyn avulla, on johtanut tilanteeseen, jossa kattavasti kootut ja analysoidut tunnistamistiedot kertovat henkilöstä ja tämän yksityisyyden suojan piiriin kuuluvista asioista *enemmän* kuin yksittäisten viestien sisältö. Matkapuhelinverkon tukiasemiin, älypuhelimen GSM-paikannukseen, IP-osoitteisiin ja WiFi-verkkoihin perustuva *paikkatieto* on eräs osoitus tunnistamistietojen läpitunkevuudesta, kun sen avulla voidaan nykyisin esimerkiksi kartoittaa kahden henkilön väliset yksityiset tapaamiset, tai yksilön vierailut psykiatrin tai gynekologin luona jne. Jaottelu tunnistamistietoihin ja viestin sisältöön luhistuu, kun sitä yritetään soveltaa henkilön omiin tiedonhankintakäytäntöihin: henkilön vierailemien nettisivujen osoitteet tai hänen kirjoittamiensa hakusanojen yhdistelmät kertovat yhtä paljon viestien sisällöstä kuin ne vastaukset, mitä hän saa.

Työryhmän mietinnössä (s. 56-57) on tarkasteltu EU-tuomioistuimen 8.4.2014 antamaa ratkaisua, jolla ns. Data Retention Directive katsottiin perusoikeuksia loukkaavana pätemättömäksi. Perinteistä kantaa seuraten tuomioistuin toki totesi, että kun direktiivi rajoittui tunnistamistietoihin, se ei loukannut yksityisyyden suojan ja tietosuojan ydinsisältöä. Silti tuomioistuin katsoi, että kyseessä oli *erittäin vakava* kajoaminen kyseisiin perusoikeuksiin ja vahvisti niiden loukkauksen. Eduskunnan perustuslakivaliokunta on sittemmin tehnyt tuomiosta oikean johtopäätöksen, kun se on korostanut, että perinteisen kahtiajaon sijasta on syytä arvioida perusoikeusrajoituksen astetta kokonaisuutena (PeVL 18/2014 vp). Tämä on oikein todettu myös työryhmän mietinnössä (s. 60-61).

***(2) Vaatimus perusoikeusrajoitusten säädösperustasta***

Perus- tai ihmisoikeuksien rajoitukset voivat olla hyväksyttäviä vain, jos niille on olemassa asianmukainen säädösperusta. Kansainväliset ihmisoikeussopimukset eivät suoranaisesti ota kantaa siihen, millä kansallisen säädöshierarkian tasolla asiasta olisi säädettävä, vaan ne keskittyvät lainsäädännön laatuvaatimuksiin julkisuudesta, täsmällisyydestä, tarkkarajaisuudesta, lailla myönnetyn harkintavallan rajoitetusta luonteesta ja tehokkaista oikeussuojakeinoista. Kansallinen perustuslaki usein – kuten Suomen Perustuslaki järjestelmällisesti – täydentää näitä vaatimuksia asettamalla ehdon, että perusoikeuksia voidaan rajoittaa vain kansanedustuslaitoksen säätämällä laila. Perustuslain viittaukset lailla säätämiseen siis tarkoittavat muodollista lakia, eduskuntalakia. Lainsäädäntövallan delegointi on kielletty, jos se mahdollistaisi perusoikeuksien rajoittamisen lakia alemmanasteisin normein.

Kansainvälisessä vertailussa muodostaa suuren ongelman, että verkkotiedustelu usein perustuu epämääräisiin ja väljiin säännöksiin, jotka jättävät hallinnollisille viranomaisille paljon harkintavaltaa ja joiden toimeenpanossa saatetaan käyttää ei-julkista alemmanasteista normistoa ja ei-julkisia valvontamekanismeja. Yhdysvaltain ja Yhdistyneen Kuningaskunnan järjestelmät ovat varsin ongelmallisia näissä suhteissa.

Kun työryhmä ei ole edes hahmotellut sen mietinnöstä seuraavia lakihankkeita, on mahdotonta arvioida, miten lailla säätämisen vaatimus täyttyisi, jos Suomessa säädettäisiin verkkovalvonnasta. Sinänsä huomionarvoista on, että työryhmä (s. 80) väläyttää ajatuksen perustuslain muuttamisesta verkkovalvonnan mahdollistamiseksi tiedustelutarkoituksessa. Tämä lausuma osoittaa, että työryhmä on mieltänyt laissa säätämisen vaatimuksen vakavuuden.

***(3) Vaatimus hyväksyttävästä tarkoitusperästä***

Sekä kansainväliset ihmisoikeussopimukset että Suomen Perustuslaki usein sisältävät tyhjentävän luettelon tietyn perusoikeuden rajoittamisessa hyväksyttävistä tarkoitusperistä. Esimerkiksi perustuslain 10 §:ssä yksityiselämän suojasta (ml. tietosuoja) hyväksyttävinä rajoitusperusteina kotirauhan piirissä on mainittu vain perusoikeuksien turvaaminen ja rikosten selvittäminen. Luottamuksellisen viestin salaisuuteen taas saadaan hyväksyttävästi kajota vain yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana (3 momentti).

Työryhmän toimeksiannon mukaan (s. 7) työryhmän tehtävänä oli arvioida Suomeen kohdistuvien uhkien vaikutusta “Suomen turvallisuudelle ja kilpailukyvylle”. Molemmat perusteet ovat varsin kaukana perustuslain 10 §:n 3 momentin sanamuodosta, ja myönteisenä voidaan pitää sitä, ettei työryhmä ole edes yrittänyt ulottaa verkkotiedustelua palvelemaan Suomen kilpailukykyä.

Työryhmän kaavailema “tiedustelu” ei kuitenkaan kohdistuisi vain tehtyjen rikosten tutkintaan tai edes konkreettisiin rikosuhkatilanteisiin (kuten yksittäisten terroritekojen torjunta) vaan tiedustelu on mietinnössä määritelty tavoitteensa kautta tuottaa “*varhaisvaiheen* tietoa, joka mahdollistaa uhkiin, riskeihin, *mahdollisuuksiin* ja *muutoksiin* *vaikuttamisen* ja *varautumisen*” (s. 15, korostukset lisätty). On selvää, että jos perusoikeuksiin kajoavaa lainsääntöä lähdettäisiin laatimaan näin avaran tarkoitusperän toteuttamiseksi, lakiehdotus törmäisi perustuslakiin. Noin laajalle viety tiedustelutoiminta ei olisi oikeutettua ilman muutoksia perustuslakiin (ks. mietinnön s. 80)

***(4) Vain tosiallisesti tehokas perusoikeusrajoitus voi olla välttämätön***

Mietinnön mukaan tietoliikennetiedustelu on käytössä useissa länsimaissa, mistä tehdään se johtopäätös, että olisi “ilmeistä, että näissä valtioissa sitä pidetään tehokkaana tiedonhankintakeinona” (s. 69). Verkkovalvonnan tosiasiallinen tehokkuus on kaikkea muuta kuin ilmeistä. Epäilemättä useissa länsimaissa on yksittäisiä henkilöitä jotka uskovat verkkovalvonnan toimivuuteen, ja osa näistä henkilöistä on sellaisissa asemissa, että he voivat päättää toiminnan jatkumisesta ja uusien voimavarojen kohdentamisesta. Samaan aikaan verkkovalvonnan tehokkuuteen kohdistuu vakavia epäilyjä.[[1]](#footnote-1)

Mietinnössä (s. 8) mainitaan työryhmän kuulleen tehokkuuskysymyksessä luottamuksellisesti kahta ulkomaista tietoliikennetiedustelun asiantuntijaa. Näiden henkilöllisyys tai taustaorganisaatio eivät ilmene mietinnöstä, ei liioin saatujen lausuntojen asiasisältö.

Elektronisen massavalvonnan tehokkuus on erittäin kiistanalainen kysymys. Edward Snowdenin paljastusten jälkeen asiasta on käyty perusteellista keskustelua ennen muuta Yhdysvalloissa mutta myös kansainvälisesti. Silti on edelleen vallalla tilanne, että ne, jotka katsovat massavalvonnasta olleen todellista hyötyä esimerkiksi terrorismin torjunnassa, ovat toiminnasta vastanneiden viranomaisten omien arvioiden varassa. Nuo arviot puolestaan ovat vahvasti defensiivisiä ja näyttävät perustuvan esimerkiksi Yhdysvaltain NSA:n ja Yhdistyneen Kuningaskunnan GCHQ:n pyrkimykseen oikeuttaa aiempi toimintansa ja saada hyväksyntä sen jatkumiselle ilman perustavampia muutoksia esimerkiksi toiminnan laajuuden, oikeudellisen perustan tai valvontamekanismien suhteen. Esitän seuraavassa kolme rinnakkaista perustelulinjaa, jotka kaikki johtavat päinvastaiseen arvioon.

*4.1 Taloudelliset ja henkilöstövaikutukset ovat selvittämättä*

Työryhmän mietinnössä on lyhyt yleisluonteinen viittaus siihen, että verkkovalvonnalla olisi taloudellisia ja henkilöstövaikutuksia (s. 79). Ilman noiden vaikutusten selvittämistä on mahdotonta arvioida Suomeen kaavaillun verkkovalvonnan hyväksyttävyyttä. Toiminta ei voi olla välttämätöntä ellei se ole tehokasta, mukaan lukien kustannustehokasta.

Terrorismin torjunnan nimissä Yhdysvalloissa tehtyjen toimenpiteiden kustannustehokkuus on ollut vakavan kritiikin kohteena, muun muassa sen vuoksi ettei noiden toimenpiteiden kustannustehokkuutta ole yleensä edes yritetty arvioida ennen niiden käyttöönottoa. Asian jatkovalmistelussa tulisi perehtyä niihin malleihin, joihin kustannustehokkuuden arviointi ja Yhdysvaltain terrorismintorjunnan kritiikki niiden näkökulmasta ovat perustuneet.[[2]](#footnote-2)

*4.2 SURVEILLE-tutkimushankkeen tuloksia*

Johdan EU:n seitsemännen puiteohjelman turvallisuustutkimuksen alaan kuuluvaa monitieteistä tutkimushanketta SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency).[[3]](#footnote-3) Tutkimushankkeen keskeisenä tavoitteena on kehittää menetelmiä tarkkailuteknologioiden (surveillance technologies) arvioinnille teknologian, kustannustehokkuuden, eettisten ongelmien ja laillisuuden näkökulmista. Hanke on jatkunut tätä kirjoitettaessa runsaat kolme vuotta ja päättyy kesäkuun lopussa 2015.

Eräs SURVEILLE-hankkeen tärkeimmistä linjoista on ollut yksittäisten tarkkailuteknologioiden skenarioperustainen arviointi eri näkökulmista. Hankkeessa kehitetyt kolme skenariota sisälsivät kaikkiaan 35 tarkkailuteknologioiden käyttötilannetta, sijoitettuina realistiseen toimintaympäristöön. Ensimmäinen skenario koski valtioiden rajat ylittävän perinteisen organisoidun rikollisuuden torjuntaa,[[4]](#footnote-4) toinen skenario Charlie Hebdo –tyyppisten terrori-iskujen ennaltaehkäisyä,[[5]](#footnote-5) ja kolmas tarkkailuteknologioiden käyttöä yleisen järjestyksen ylläpitämiseksi nykyaikaisessa kaupunkiympäristössä.[[6]](#footnote-6)

Tiedonhankintalakityöryhmän mietinnön arvioinnissa tärkein on keskimmäinen skenario (D2.8) ja sen yhteydessä tuotetut kaksi julkista raporttia:

(a) Michelle Cayford: *SURVEILLE Paper on Mass Surveillance by the National Security Agency (NSA) of the United States of America;* ja

(b) Coen van Gulijk, Michelle Cayford, Bert-Jan Kooij, Martin Scheinin, Mathias Vermeulen, Juha Lavapuro, Tuomas Ojanen, Jonathan Andrew, Douwe Korff, John Guelke, Tom Sorell and Katerina Hadjimatheou: *SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act[[7]](#footnote-7)*

Ensin mainittu Delftin teknologisessa yliopistossa tuotettu Michelle Cayfordin raportti (a) on faktuallinen kuvaus Yhdysvaltain NSA:n käyttämistä verkkovalvonnan menetelmistä, dokumentoituna Edward Snowdenin paljastamien asiakirjojen ja muiden lähteiden avulla. Se on asiantunteva selvitys siitä, miten verkkovalvonta käytännössä toimii teknisesti. Se tarjoaa vertailukohdan arvioitaessa työryhmän alustavasti hahmottelemaa suomalaisen verkkovalvonnan mallia (ks. myös mietinnön s. 64-65).

Jälkimmäinen raportti (b) tuotettiin kolmen tiimin yhteistyönä: Delftin ryhmä toteutti teknologia-arvioinnin, Warwickin yliopisto eettisen arvioinnin ja johtamani EUI:n ryhmä oikeudellisen arvioinnin, joka keskittyi Euroopan ihmisoikeussopimuksen ja Euroopan Unionin perusoikeuskirjan vaatimuksiin. Raportti perustuu realistiseen mutta hypoteettiseen askel askeleelta etenevään tapahtumakuvaukseen, jossa EU:n jäsenmaan epäillään olevan valmisteilla olevan terrori-iskun kohteena. Iskun estämiseksi viranomaiset ottavat käyttöön erilaisia tiedustelun, tarkkailun ja poliisitoimenpiteiden keinoja. Osa niistä on NSA-raportista tuttuja verkkovalvonnan menetelmiä, osa taas perinteisiä, ei-teknologisia tarkkailukeinoja (matkalaukun avaaminen ja epäillyn henkilön fyysinen seuraaminen jalkatyönä).

Kustakin tarkkailukeinosta tehtiin kolme arviota: teknologinen (sisältäen kustannustehokkuuden yhtenä ulottuvuutena), eettinen ja oikeudellinen. Arvioiden tulokset koottiin matriisiksi, joka muodostui seuraavanaiseksi:



Selitykset:

* Vasemmassa sarakkeessa on esitetty kuusi toisiaan seuraavaa tarkkailukeinoa. Niistä kolme ensimmäistä vastaavat verkkovalvonnan menetelmiä: ensin (1) koko liikenteen kerääminen valtakunnan rajan ylittävästä tietoliikennekaapelista ja sitten (2) algoritmeihin perustuva tunnistettavien kohdehenkilöiden seulominen, joka johtaa (3) manuaaliseen analyysiin (tässä tapauksessa) edellisessä vaiheessa identifioitujen kohdehenkilöiden kontaktiverkon selvittämiseksi. Vaiheet 4 ja 5 ovat perinteisiä ei-teknologisen tarkkailun menetelmiä. Vaihe 6 edustaa jälleen elektronista tarkkailua, mutta nyt kohdennettuna tiettyihin tietokoneisiin niiden aktiviteetin kattavaksi seuraamiseksi.
* Toinen sarake vasemmalta edustaa teknologia-arvioinnin lopputulosta. Kukin tarkkailumenetelmä arvioitiin asteikolla 0-10 siten, että kymmenen eri osatekijää erikseen tuotti kukin enintään yhden pisteen. Osatekijät kattoivat mm. saavutetun informaation luotettavuuden ja käyttökelpoisuuden sekä menetelmän kustannustehokkuuden. Huomionarvoista on, että elektronisen massavalvonnan vaiheet 1 ja 2 saivat hyvin keskinkertaisen arvosanan 5.
* Värikoodit edustavat kuuden eri eettisen riskin arviointia siten, että vihreä väri edustaa pientä (mutta tunnistettua) riskiä, keltainen suurempaa riskiä ja punainen suurinta mahdollista eettistä riskiä. Huomionarvoista on, että kaikkiin elektronisen valvonnan muotoihin – sekä massaluonteisiin että kohdennettuihin – liitettiin suurin mahdollinen eettinen riski.
* Neljäs ja viides sarake vasemmalta edustavat perusoikeusarviointia, keskittyen tietosuojaan (neljäs sarake) ja yksityisyyden suojaan (viides sarake, joka samalla sisältää yhden eettisen riskin värikoodin). Yllä tulokset on esitetty kertolaskun muodossa perustuen kolmeen osatekijään: perusoikeuden tärkeys yksilön kannalta x perusoikeuspuuttumisen syvyys x tehdyn arvion luotettavuuskerroin perustuen Euroopan ihmisoikeustuomioistuimen ratkaisukäytännön olemassaloon. Elektronisen massavalvonnan menetelmät (vaiheet 1 ja 2) tuottivat korkeimman mahdollisen perusoikeuspuuttumisen (16), samoin kuin tietyn tietokoneen totaalinen valvonta (vaihe 6), kun taas henkilön kontaktiverkoston analyysi (vaihe 3) tuotti astetta lievemmän perusoikeuspuuttumisen (8) ja perinteiset ei-teknologiset tarkkailumenetelmät (vaiheet 4 ja 5) hyvin vähäisen perusoikeuspuuttumisen asteen (3/4)

Itse raportti sisältää perustelut jokaiselle kolmelle arviolle jokaisesta kuudesta vaiheesta, mukaan lukien teknologia-arvioinnin osatekijät (ks. s. 22). Lainaan vielä raportin viimeisen kappaleen tähän:

In D2.8 we have considered the case of mass Internet monitoring systems that are publicly justified on the basis of their counter-terrorism application, and we bring our analysis to bear on their use for a counter-terrorism investigation – exactly the sort of case where justification of its use ought to be strongest. Various kinds of Internet monitoring techniques are applied side by side with more traditional surveillance techniques. We find most of the Internet monitoring applications both ethically and legally impermissible, assessing them poorly in comparison with traditional, non-technology based surveillance methods. Furthermore, the Internet monitoring techniques compare poorly with the traditional techniques also in terms of usability. The conclusions of D2.8 are much more clear cut than those of D2.6: Internet monitoring techniques, with the exception of targeted social networking analysis, represent an unacceptable interference with fundamental rights to privacy and data protection, the deepest ethical risks of chill and damage to trust, intrusion and discrimination, while also violating moral norms of proportionality of methods and consent of the policed. Meanwhile these high moral and legal costs reflect a mostly middling to poor usability benefit, performing worse with regard to cost, efficiency and privacy-by-design than lower tech alternatives. The case for a mass Internet monitoring system is found wanting.

Monitieteinen tutkimushankkeemme on siis tuottanut lopputuloksen, jonka mukaan työryhmän mietinnössä hahmotellun kaltainen verkkovalvonta tuottaa varsin vaatimattoman hyödyn potentiaalisten terroristien paljastamisessa, samalla kun sen eettiset riskit ja vaikutukset perusoikeuksiin ja ihmisoikeuksiin ovat niin huomattavat, että suuremmatkaan hyödyt eivät voisi oikeuttaa sitä.

*4.3 Oletettuihin todennäköisyyksiin perustuva ajatuskoe*

Massavalvonnan tehokkuutta voidaan arvioida myös yksinkertaisen ajatuskokeen avulla. Oletetaan, että Suomeen kohdistuu terrorismin uhka, siten että jokaisesta miljoonasta massavalvonnan kohteena olevasta ihmisestä kymmenen olisi todellisia terroristeja, jotka muodostavat uhkan Suomelle. Arvio on todennäköisesti ylimitoitettu. Yksinkertaistaen se tarkoittaisi, että Suomessa olisi noin 55 todellisen vaaran muodostavaa terroristia.

Massavalvonta ei voi vedenpitävästi ja poissulkevasti tunnistaa sen kohteena olevasta tietovirrasta todellisia terroristeja. Voimme olettaa, että massavalvonnan muotona on yhdistelmä koko tietovirtaan kohdistuvaa *tunnistamistietojen tarkkailua* ja siitä seuraavan seulonnan avulla valikoitavan suppeamman henkilöjoukon viestien *sisällön analysointi* algoritmien avulla. Vain näiden kahden vaiheen jälkeen esiin seulottu “epäiltyjen terroristien” kommunikaatio tulee tiedustelua harjoittavien henkilöiden analysoitavaksi mahdollisia toimenpiteitä varten. Viimeistään tässä vaiheessa kysymys on syvälle käyvästä kajoamisesta toimenpiteen kohteena olevien henkilöiden yksityisyyden suojaan (ml. tietosuoja), kun analyysin kohteena on tämän valitun henkilöjoukon ja heidän kanssaan komunikoineiden sivullisten luottamuksellisten viestien koko sisältö.

Olettakaamme, että tätä vaihetta edeltävä seulonta on onnistunut karsimaan pois 99 % viattomista sivullisista, niin että väärien positiivisten osuus on vain yksi prosentti. Tuo luku on todennäköisesti alimitoitettu, koska oikeat terroristit käyttävät peiteilmaisuja, ja sen takia heidän löytämisensä ei salli liian tiuhan seulan käyttämistä.[[8]](#footnote-8) Jotta peiteilmaisuja käyttävät oikeat terroristit tavoitettaisiin, joudutaan hyväksymään korkeampi väärien positiivisten osuus – siis jatkoanalyysin kohteiksi joutuvien viattomien sivullisten joukko.

Olettakaamme edelleen, että jokainen näistä viattomista sivullisista on kommunikoinut 100:n muun viattoman sivullisen kanssa ja inhimillisten analyytikkojen kohteena on tämä luottamuksellinen kommunikaatio näiden sivullisten kanssa. Se voi koskea esimerkiksi terveystietoja, sukupuolielämää, raha-asioita, luottamuksellisia työasioita jne. Luku on jälleen todennäköisesti alimitoitettu.

Tietenkin myös oikeat terroristit kommunikoivat viattomien sivullisten kanssa. Ajatuskokeen yksinkertaistamiseksi jätämme kuitenkin heidät huomiotta. Sen sijaan joudumme olettamaan, että tapauksessamme käytetty tiedustelutoiminta tavoittaa 90 % oikeista terroristeista. Väärien negatiivisten (eli seulan läpi menneiden oikeiden terroristien) osuus on suurempi kuin väärien positiivisten (seulaan jääneiden viattomien sivullisten), koska juuri oikeat terroristit osaavat paremmin suojautua tiedustelutoiminnalta kuin syyttömät sivulliset – esimerkiksi käyttämällä peiteilmaisuja, vaihtamalla päätelaitetta, turvautumalla viestien salaukseen[[9]](#footnote-9) ja kokonaan välttämällä tiedustelutoiminnan kohteena olevaa kommunikaatiota.

Mikä on tiedustelutoiminnan anti edellä esitettyjen oletusten perusteella? Jos tiedustelutoiminnan kohteena oli miljoona ihmistä (ja näiden kanssa kommunikoineet sivulliset), inhimillisen syväanalyysin kohteeksi joutuisi:

* 9 oikeaa terroristia (90 % x 10)
* 10.000 viatonta henkilöä (1 % x 999.990) terrorismista epäiltyinä
* 1.000.000 viatonta terrorismista epäiltyjen kanssa kommunikoinutta henkilöä (100 x 10.000)

Yhteenlaskien 1.010.000 viattoman sivullisen yksityisyyden ydinalue (luottamuksellisten viestien sisältö) uhrattaisiin 9 oikean terroristin tavoittamiseksi. Toimenpide kohdistui alun perin miljoonaan ihmiseen ja sen aiheuttaman yksityisyyden suojan murtamisen kohteiksi joutui enemmän kuin tuo määrä viattomia sivullisia (osa tosin ulkomailla).

Jos tämä olisi ensimmäinen ja ainoa keino noiden yhdeksän oikean terroristin identifioimiseksi, joku voisi sanoa, että perusoikeuksiin puuttuminen on radikaalista asteestaan huolimatta ollut tehokas keino paljastaa terroristeja ja on siis ollut välttämättömyysvaatimuksen mukainen. Jäljellä olisi vain erillinen suhteellisuusarviointi (ks. seuraava kohta).

Tämä ei kuitenkaan ole oikea tapa arvioida välttämättömyysvaatimuksen toteutumista, koska on erittäin epätodennäköistä, ettei noista yhdeksästä terroristista olisi jo olemassa muihin menetelmiin perustuvaa tietoa. Kerta kerran jälkeen todellisten terrori-iskujen yhteydessä saadut tiedot viittaavat siihen, ettei massavalvonnan ongelmana ole se, että se identifioisi liian harvoja kohteita. Päin vastoin, esimerkiksi Bostonin ja Pariisin terroristi-iskujen tekijät olivat jo ennalta viranomaisten tiedossa, mutta he hukkuivat informaation paljouteen ja ehkä viranomaisten muiden resurssien niukkuuteen. Pahassa tapauksessa edellä esitetyssä ajatuskokeessa on uhrattu yli miljoonan ihmisen yksityisyyden suoja, ja sen tuloksena vain saatu lisää tietoa yhdeksästä jo ennestään tiedetystä terroristiepäillystä. Ja kaikkein pahimmassa tapauksessa usko massavalvonnan toimivuuteen on johtanut siihen, että epäsuhtainen määrä voimavaroja käytetään lisätiedon hankintaan hyllyille pölyttymään, sen sijaan että estettäisiin, että yksi noista yhdeksästä jo aiemmin epäillystä terroristista onnistuu toteuttamaan terrori-iskun, joka olisi ollut oikein toimien estettävissä.

Myös tämä ajatuskoe vahvistaa SURVEILLE-tutkimushankkeen keskeisen lopputuleman: massavalvonnan hyötyjä ei ole osoitettu, ja sikäli kuin ne on mahdollista arvioida, massavalvonta ei ole kustannustehokasta tai yksityisyyden suojaan liittyvän välttämättömyysvaatimuksen kannalta hyväksyttävää.

Mainittakoon, että työryhmän mietintöön sisältyy yksittäinen lause, joka saattaisi osin muuttaa edellä esitetyn ajatuskokeen tuloksia: “Yksityisyyden suojan näkökulmasta olennaista olisi, että mikään sellainen viesti tai viestin tunnistamistieto, joka ei vastaa hakuehtoa, ei päädy manuaaliseen käsittelyyn.” (ss. 64-65) Käsittääkseni tätä virkettä ei voi ottaa vakavasti, tai ainakaan kirjaimellisesti. Jos ihmisanalyytikoiden käsittelyyn päätyisivät vain hakuehdon täyttävät yksittäiset viesit tai tunnistamistiedot, ne olisivat hyödyttömiä tiedon sirpaleita ilman kontekstia. Mietintötekstin kirjoittajan on täytynyt tarkoittaa, että ihmisanalyytikoiden arvioitaviksi päätyvät niiden *henkilöiden* viestit (kokonaisuudessaan), jotka ovat laukaisseet hakuehdon täyttymisen. Ja siinä tapauksessa arvioni 1 %:n virhemarginaalista väärien positiivisten suuntaan ei liene ylimitoitettu.

***(5) Perusoikeusrajoitusten suhteellisuusvaatimus***

Vain hyväksyttävän tarkoitusperän toteuttamiseksi välttämätön ja tehokas keino voi olla oikeasuhtainen siitä seuraavaan perusoikeusrajoitukseen verrattuna. Edellä esittämäni kritiikki verkkotarkkailun tehokkuutta kohtaan johtaa arvioon, että melkeinpä määritelmän mukaan siitä seuraavat perusoikeusrajoitukset eivät voi olla suhteellisuusperiaatteen kannalta hyväksyttäviä. Tämä koskee myös äskeistä ajatuskoetta, jossa yli miljoonan ihmisen yksityisyyden suojan ydinalueeseen kajottiin yhdeksän terroristin seuraamiseksi, vaikka suuri osa noista yhdeksästä jo oli viranomaisten tiedossa ja oikeasuhtaisuuden vaatimus olisi voitu toteuttaa kohdistamalla tarkkailutoimet heihin, esimerkiksi perinteisten (ei-teknologisten) tarkkailumenetelmien muodossa.

Työryhmän mietinnössä suhteellisuusperiaate on ilmaistu aivan oikein: “Tietoliikennetiedustelun hyväksyttävyyttä harkittaessa on arvioitava sitä, onko toiminnasta kansalliselle turvallisuudelle aiheutuva hyöty suurempi kuin toiminnasta mahdollisesti aiheutuva haitta yksityisyyden suojalle sekä kansantaloudelle ja yrityksille.” (s. 69) Juuri niin. Hyöty on ensin osoitettava ja sen suuruus arvioitava. Vasta sitten voidaan kysyä, onko toimenpide oikeasuhtainen. Vastakkain eivät ole yleisellä tasolla valtion ja kansakunnan turvallisuus ja yhden yksilön yksityisyyden suoja. Vertailun kohteena ovat konkreettinen ja tosiasiallinen turvallisuushyöty toimenpiteestä, jonka toteuttamisessa on ollut välttämätöntä rajoittaa tietyn yksilön perusoikeuksia, ja tämän perusoikeusrajoituksen aste.

**III. Perus- ja ihmisoikeuksien alueellinen ulottuvuus**

Yhdysvaltain ja Yhdistyneen Kuningaskunnan esimerkkejä seuraten mietinnössä lähdetään siitä, että tietoverkkotiedustelu olisi perusoikeuksien ja ihmisoikeuksien kannalta ongelmatonta, jos se kohdistuu “ulkomailla sijaitsevassa tietojärjestelmässä käsiteltäviin tietoihin” (s. 17). Tähän lyhyeen ilmaisuun sisältyy kolminkertainen erehdys:

(a) Kyseinen toimenpide (tietoverkkokaapelin kautta kulkevan viestinnän massakopiointi) toteutettaisiin Suomessa ja suomalaisten viranomaisten voimin.

(b) Ainakin yksi kommunikaation kahdesta osapuolesta olisi Suomessa, ja usein jopa molemmat (kun esim. jomman kumman käyttämä sähköpostipalvelin on kansainvälinen).

(c) Myös ulkomaalaisilla on ihmisoikeudet, myös silloin kun he sijaitsevat ulkomailla.

Sama virheellinen olettamus toistuu s. 50: “Kansainvälinen viestiliikenne pitää sisällään Suomesta lähtevän ja Suomeen päättyvän rajat ylittävän liikenteen… ”, ja tietoliikennetiedustelun “toteuttaminen edellyttää, että tiedusteluviranomaisella on pääsy tietoliikennekaapeleiden liityntäpisteisiin”.

Mietinnön jaksossa 6.1.2 perusoikeuksista ja ihmisoikeuksista ihmisoikeussopimusten sitovuus niiden velvoittaman valtion toimenpiteiden ulkomailla ilmeneviin vaikutuksiin on sivuutettu vähin äänin, joskin tarkkaavainen lukija huomaa alaviittestä 34 (s. 51), että ainakin YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskeva yleissopimus velvoittaa valtiota myös sen omien rajojen ulkopuolella.

Mietinnön johtopäätösluvussa (s. 80) käytetään toista käsitettä, “rajat ylittävä tietoliikenne” ja tässä yhteydessä käytetty teksti osoittaa, että toiminta tapahtuisi kotimaassa: “teleyrityksille tai rajat ylittävien tietoliikennekaapeleiden omistajille asetetaan velvoite osoittaa liityntäpisteet”.

Suomen ei tule sivuuttaa YK:n KP-sopimuksen täysin vakiintunutta tulkintalinjaa, jonka mukaan valtio on ihmisoikeusvelvoitteidensa sitoma myös suhteessa ulkomailla sijaitseviin ei-kansalaisiin kun se oman toimintansa kautta aiheuttaa näiden henkilöiden ihmisoikeuksien loukkauksen.[[10]](#footnote-10)

**IV. Lopuksi: Lyhyesti vakoilusta**

Tarkasteluni painopiste on ollut yksilön oikeuksissa. Esitän kuitenkin lopuksi lyhyen kommentin siltä osin kuin mietinnössä pohditaan myös Suomen harjoittamaa tiedustelutoimintaa suhteessa toisiin valtioihin. Mietintö edustaa tässä asiassa myötäsukaista suhtautumista ja pyrkii oikeuttamaan Suomen harjoittaman vakoilun tukeutuen muiden valtioiden hiljaiseen hyväksyntään, jonka kautta kaikki valtiot joutuvat sietämään toistensa harjoittamaa vakoilua (s. 74, 76). Mietintö edustaa myös kantaa, jonka mukaan kansainvälisen oikeuden subjekteina valtiot voivat omalla toiminnallaan luoda oikeutta. Jos lähes kaikki valtiot vakoilevat, se ei voisi olla kansainvälisen oikeuden vastaista (s. 78). Ja kun mahdolliset oikeudelliset ongelmat suhteessa kansainväliseen oikeuteen ja vakoilun kohteina olevien toisten valtioiden oikeuteen on lakaistu maton alle, seuraa mietinnön johtopäätös: “Ulkomaan tiedusteluun liittyvien toimien oikeudettomuus olisi poistettava kansallisesti säätämällä.” (s. 76)

Suhtaudun näihin perusteluihin suurin epäilyksin. Suomi ei voi omalla lainsäädännöllään poistaa harjoittamansa vakoilun oikeudettomuutta toisten valtioiden lainsäädännön nojalla. Rangaistukset voivat olla ankaria, olkoonkin että viisas vakoilija ei jää kiinni, ja viisas valtio pyrkii toteuttamaan vakoilunsa diplomaattisen immuniteetin suojassa, toivoen että käytännössä ainoa rangaistus olisi kiinni jääneen vakoojan poistaminen maasta. Tämä on toiveajattelua.

Tärkeämpi ongelma kuitenkin on, että tässä mietinnön jaksossa on unohdettu ihminen. Vaikka suomalainen vakooja ei jäisi kiinni tai vaikka kohdevaltio ei koskaan nostaisi meteliä kansainvälisen oikeuden normeihin vedoten, tarkasteltavaksi jää silti kysymys siitä, loukkaako Suomi ulkomailla tapahtuvan tiedustelutoimintansa kautta siellä elävien ihmisten yksityisyyden suojaa ja muita ihmisoikeuksia. Viittaan tämän lausunnon edelliseen tekstijaksoon ja korostan, että myös vakoilun arviointiin tulisi sisällyttää perusoikeus- ja ihmisoikeusnäkökulma.

Firenzessä, 6.4.2015



Martin Scheinin

Kansainvälisen oikeuden ja ihmisoikeuksien professori (Eurooppalainen yliopistollinen instituutti EUI)

EU:n rahoittaman SURVEILLE-tutkimushankkeen vastuullinen johtaja (2012-2015)

Aiemmin: YK:n erityisraportoija terrorismin vastatoimien ihmisoikeus-vaikutuksia koskevissa kysymyksissä (2005-2011) ja YK:n ihmisoikeuskomitean jäsen (1997-2004)

1. Ks. esim. <http://digg.com/2015/why-mass-surveillance-cant-wont-and-never-has-stopped-a-terrorist> (Ote teoksesta Bruce Schneier: Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World. W.W.Norton 2015) [↑](#footnote-ref-1)
2. Ks. John Mueller & Mark G. Stewart: Terror, Security and Money. Balancing the Risks, Benefits and Costs of Homeland Security. Oxford University Press 2011. [↑](#footnote-ref-2)
3. Ks. <http://www.surveille.eu> [↑](#footnote-ref-3)
4. SURVEILLE deliverable D2.6, julkaistu kokonaisuudessaan osoitteessa <http://www.surveille.eu/index.php/research/publications/> [↑](#footnote-ref-4)
5. SURVEILLE deliverable D2.8, joka on pääosin julkaistu kahden toisiaan täydentävän paperin muodossa samassa osoitteessa. [↑](#footnote-ref-5)
6. SURVEILLE deliverable D2.9, joka on toimitettu EU:n komissiolle 31.3.2015 mutta ei vielä ole julkinen. [↑](#footnote-ref-6)
7. <http://www.surveille.eu/PDFs/SURVEILLE%20Paper%20on%20a%20Terrorism%20Prevention%20Scenario%20based%20on%20D2.8.pdf> [↑](#footnote-ref-7)
8. Kun vuonna 2007 olin YK:n erityisraportoijana maavierailulla Yhdysvalloissa, seurasin yhden päivän ajan terrorismista syytetyn Jose Padillan oikeudenkäyntiä Miamissa. Todistelu keskittyi FBI:n nauhoittamien puhelujen laajasta aineistosta valittujen yksittäisten lauseiden esittämiseen näyttönä siitä, että Padilla oli osallistunut ulkomaisten terroristijärjestöjen tukemiseen. Kyseisissä lauseissa ei puhuttu mitään rahasta tai pommeista vaan pelkästään jalkapallojoukkueista ja jalkapallokengistä. [↑](#footnote-ref-8)
9. On paradoksaalista, että Yhdysvallat ja Yhdistynyt Kuningaskunta sisällyttävät salausohjelmien käytön niiden parametrien joukkoon, jotka tekevät henkilöstä potentiaalisen epäillyn. Pankit, asianajajat, liikeyritykset, lääkärit ja psykiatrit ja aivan tavalliset kansalaiset käyttävät salausohjelmia täysin hyväksyttävistä syistä. Jos salausohjelmien käyttö on yksi parametri potentiaalisten terroristien esiin seulomiseksi, se saattaa *lisätä* valvonnan kohteeksi joutuvien viattomien sivullisten suhteellista osuutta, sen sijaan että se tekisi toiminnasta enemmän tarkkarajaisen. [↑](#footnote-ref-9)
10. Ks. esim. Martin Scheinin, ‘Extraterritorial Effect of the International Covenant on Civil and Political Rights’, teoksessa Fons Coomans and Menno T. Kamminga (eds): Extraterritorial Application of Human Rights Treaties, (Antwerp-Oxford: Intersentia, 2004), ss. 73-81. [↑](#footnote-ref-10)