Anna Leppänen & Jarmo Houtsonen

Viranomaisvalvonta verkoissa

Näkemyksiä poliisin ja tiedusteluviranomaisten salaisesta tiedonhankinnasta verkossa

Poliisiammattikorkeakoulun raportteja 140

VIRANOMAISVALVONTA VERKOISSA

NÄKEMYKSIÄ POLIISIN JA TIEDUSTELUVIRANOMAISTEN SALAISESTA TIEDONHANKINNASTA VERKOSSA

Anna Leppänen & Jarmo Houtsonen

POLIISIAMMATTIKORKEAKOULUN RAPORTTEJA 140

Poliisiammattikorkeakoulu
Tampere, 2021

Anna Leppänen & Jarmo Houtsonen
VIRANOMAISVALVONTA VERKOISSA: NÄKEMYKSIÄ POLIISIN JA TIEDUSTELUVIRANOMAISTEN SALAISESTA TIEDONHANKINNASTA VERKOSSA

Poliisiammattikorkeakoulun raportteja 140
ISBN 978-951-815-399-6
ISSN 1797-5743

Grano Oy 2021

1 TIIVISTELMÄ

Tässä raportissa esitellään Poliisiammattikorkeakoulussa toteutetun kansainvälisen tutkimushankkeen ”Taking Surveillance Apart? Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers” (5/2017 - 7/2020) empiirisiä tuloksia Suomen osalta. Lisäksi raportissa kuvataan tiedustelulakien valmisteluprosessia sekä poliisin ja tiedusteluviranomaisten keskeisiä toimivaltuuksia hankkia tietoa tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista. Hankkeessa tarkasteltiin, mitä poliisin ja tiedusteluviranomaisten toimivaltuuksista verkossa ajatellaan Suomessa, Britanniassa ja Norjassa. Tulokset perustuvat kussakin maassa toteutettuihin Q-metodologisiin sidosryhmäasiantuntijahaastatteluihin (Suomessa n=25) sekä yliopistojen opiskelijoilta ja henkilökunnalta kerättyihin kysely- (Suomessa n=236) ja haastatteluaineistoihin (Suomessa n=20).

Tutkimus on ajankohtainen, koska siviili- ja sotilastiedustelulait astuivat voimaan Suomessa kesällä 2019. Keskeinen lainsäädännön muutos oli, että suojelupoliisin ja puolustusvoimien harjoittamalle tiedustelulle luotiin säädöspohja, joka mahdollistaa tiedustelumenetelmien käyttämisen kotimaassa ja ulkomailla kohteisiin, jotka on määritelty vakaviksi uhkiksi kansalliselle turvallisuudelle. Uusi määritelmä mahdollistaa tiedustelutoiminnan aiempaa varhaisemmassa vaiheessa sekä soveltamisen laajempaan viestijoukkoon, kun tiedustelutoimien käytön perusteena ei enää ole vain rikosepäily. Samalla suojelupoliisi luopui toimivallastaan suorittaa rikosten esitutkinta ja siitä tuli puhtaasti tiedusteluviranomainen. Siviili- ja sotilastiedustelumenetelmät ovat menetelmällisesti pitkälti tuttuja esitutkintaviranomaisia säätelevästä lainsäädännöstä, mutta eniten keskustelua on herättänyt kokonaan uusi, tietoliikennetiedusteluksi kutsuttu menetelmä, jossa tietoliikenteestä suodatetaan hakuehdot täyttävä, Suomen rajan ylittävä tietoliikenne tarkempaa analyysia varten.

Käyttämistämme aineistoista sidosryhmäasiantuntijahaastattelut nostavat esiin kolme näkökulmaa tiedustelulainsäädäntöön: Yksityisyyden, vapauksien ja turvallisuuden välillä tasapainoilijat, Ihmisoikeuksien merkityksen korostajat sekä Valvontaoikeuksien laajentajat. Jokaisella näkökulmalla on ollut merkittävä roolinsa viranomaisten toimivaltuuksien ympärillä käydyssä keskustelussa. On huomionarvoista, että osallistujamme pitivät tiedustelulainsäädännön valmistelua alun vaikeuksien jälkeen suhteellisen onnistuneena. Yliopistoväen haastatteluissa ja kyselyssä puolestaan kartoitettiin muiden kuin asiantuntijoiden näkemyksiä poliisin ja tiedusteluviranomaisten toimivaltuuksista verkossa yleisemmällä tasolla. Havaitsimme, että tutkimukseen osallistuneet henkilöt pääsääntöisesti hyväksyvät turvallisuusviranomaisten tiedonhankinnan, jos sitä tarvitaan vakavien rikosten selvittämiseen tai estämiseen, mutta kyselyn vastaajien joukosta paljastui myös kriittisempiä näkökantoja. Lisäksi tiedonhankinnalle ei anneta avointa mandaattia, vaan myös yliopistolaiset haluavat asettaa viranomaisvalvonnalle reunaehtoja, tuovat esiin huoliaan sekä puntaroivat kantaansa suhteessa moniin arvoihin ja intresseihin.

Tutkimuksemme keskeisiä havaintoja on maallikkojen suhteellisen heikko tietoisuus viranomaisten uusista tiedustelutoimivaltuuksista. Vaikka tiedustelulakipaketin asiantuntijakeskustelu oli lainvalmistelun aikana paikoin vilkasta, ja asia oli välillä esillä tiedotusvälineissä, suojelupoliisin ja puolustusvoimien harjoittama tiedustelutoiminta ja uuden lainsäädännön tuomat muutokset voivat olla hyvinkin

vieraita tavallisille kansalaisille. Poliisin toiminta on sen sijaan tutumpaa ja siitä osallistujat olivat saaneet tietonsa moninaisia reittejä pitkin, aina televisiosarjoista uutisiin. Poliisin ja tiedusteluviranomaisten toimivaltuudet verkossa on teema, josta tietäminen koetaan kyllä tärkeäksi, jopa osaksi yleissivistystä, mutta toisaalta tietoa ei olla valmiita erikseen hankkimaan. Tiedonhankinnan kokonaiskuvan ja teknisten yksityiskohtien ymmärtämistä pidetään haastavana. Maallikot olivat huolissaan esimerkiksi kaupallisten toimijoiden ja rikollisten harjoittamasta tiedonkeruusta, mitä osallistujat pitivät tyypillisesti selvästi suurempana uhkana kuin kotimaisten viranomaisten toimintaa.

Tietoisuuden lisääminen eri tahojen tiedonhankinnasta ja käyttömahdollisuuksista mahdollistaisi tavallisten kansalaisten aktiivisemman osallistumisen yhteen 2000-luvun alkupuoliskon merkittävimmistä keskusteluista, yksityisyyteen tietoverkoissa. Kansalaisten tietämyksen ja valveutuneisuuden parantaminen on tärkeää tekoälyn lisääntyessä, tietoverkkojen käytön monipuolistuessa ja esineiden internetin laajentuessa, koska ne kaikki lisäävät tiedonkeruu- ja hyödyntämismahdollisuuksia. Turvallisuusviranomaiset voivat tarjota perustietoa toimivaltuuksistaan ja niiden ympärille rakennetuista mekanismeista, joiden tarkoitus on suojata yksityisyyttä sekä havaita ja estää järjestelmän väärinkäytökset. Mahdollisuuksien mukaan esimerkit toimivaltuuksien mahdollisista käyttötilanteista sekä suojamekanismien toiminnasta käytännössä, on tietoa, jota myös sidosryhmäasiantuntijat arvostavat.

2 ABSTRACT

This report presents the Finnish empirical results of an international research project "Taking Surveillance Apart? The Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers" carried out between May 2017 and July 2020 at the Police University College. In addition, we describe the preparation process for Finnish intelligence legislation and introduce some relevant online surveillance capabilities of the police and intelligence authorities. Overall, the project examined perceptions of online surveillance in Finland, the UK and Norway. The results are based on Q-methodological stakeholder interviews of experts (Finland n=25) as well as a survey (Finland n=236) and interviews (Finland n=20) conducted among university students and staff in each country.

The study is topical due to the new civilian and military intelligence legislation that entered into force in summer 2019 in Finland. Briefly, the new legislation created a legal framework for state intelligence by the Security Intelligence Service and the Defence Forces. It provides for gathering intelligence from domestic and foreign targets defined as serious threats to national security. The amendment enables more proactive intelligence gathering and mining of intelligence from a broader volume of communications, since access to capabilities is no longer limited to suspected crimes only. Simultaneously, the Security Intelligence Service waived its power to conduct pre-trial investigation and, therefore, became a pure intelligence authority. The surveillance techniques provided for civilian and military intelligence were drawn from the existing capabilities of criminal investigation or crime prevention. However, the most debated part of the legislation was the introduction of a totally new technique for network traffic intelligence, where cross-border network traffic meeting the search parameters can be picked up for further analysis.

Our expert interviews among the stakeholders produced three views of intelligence legislation: *Balancing privacy and security*, *Protecting human rights* and *Expanding surveillance powers*. Each view has significantly contributed to the discussions on the capabilities. It is necessary to acknowledge that the participants regarded the intelligence legislation process as relatively successful, after the early obstacles had been overcome. The interviews and survey carried out among university students and staff focused on non-experts' perceptions of the police and intelligence authorities' online surveillance capabilities on a more general level. According to our observations, the participants of this study mainly approve of intelligence gathering, if it is required for investigating or preventing serious crime, even though some of the survey respondents were found to hold opinions that were more critical. The university students and staff did not give the authorities an open mandate for online surveillance, but they found it necessary to set limitations for it, bring up concerns and weight their opinions in relation to many values and interests.

One of the key findings is that non-experts have relatively poor awareness of the new online surveillance capabilities of the authorities. Although the experts debated quite actively during the intelligence legislation preparation and the discussions gained media attention every now and then, civilian and military intelligence and changes brought by the new legislation may be well unknown to ordinary citizens. Instead, they are more familiar with police work, basing their knowledge on several

sources varying from TV series to news. On one hand, online surveillance capabilities by the police and intelligence authorities are an issue that people consider they should be aware of, and some even regard it as general knowledge, but on the other hand, they are not ready to seek such information by themselves. However, they find it difficult to understand the big picture and technical details of online surveillance. Furthermore, non-experts are concerned about, for example, the data collection conducted by commercial companies and criminals, and typically regard it as a more serious threat than data collection by domestic authorities. Increasing public awareness of data collection and how different bodies use it would enable ordinary citizens more actively to participate in one of the most significant discussions of the new millennium, online privacy.

Increasing the awareness of this issue is important in a world where AI is gaining a stronger foothold, ways of using networks are diversifying and the Internet of Things keeps expanding, all of which are diversifying data collection and utilisation. Security authorities can provide basic knowledge on their capabilities and safeguards or remedies designed for protecting privacy and for detecting and preventing misuse of the whole system. Where possible, providing examples of situations where the capabilities could possibly be used and how the safeguards or remedies work in practice would be something that stakeholders would appreciate.

SISÄLLYS

3 JOHDANTO

Ihmisistä, heidän sosiaalisista verkostoistaan ja toiminnastaan jää paljon jälkiä tietoverkkoihin ja -järjestelmiin. Esimerkiksi viestin välittäminen ja verkkopalvelun toteuttaminen perustuvat välitys- ja sijaintitietojen käyttöön. Välitys- ja sijaintitiedot voivat paljastaa muiden muassa viestinnän osapuolet, fyysiset sijainnit, kellonajat, nimimerkit, käyttäjätunnukset ja puhelinnumerot. Sähköpostit ja tekstiviestit puolestaan välitetään vastaanottajalle tyypillisesti salaamattomana, jolloin mikä tahansa taho voi yrittää tarkastella niitä välitystoimenpiteiden aikana. Lisäksi sosiaalinen media tarjoaa jopa vuosia kattavan näkymän yksilön elämään ja sosiaalisiin verkostoihin. Tiedot, joita ihmiset luovuttavat vapaaehtoisesti sosiaalisen median yrityksille ovat arvokasta kauppatavaraa, jota voidaan käyttää myös eettisesti epäilyttäviin tarkoituksiin, kuten ohjailemaan ihmisten käyttäytymistä ilman, että he tunnistavat joutuneensa piilovaikuttamisen, propagandan, manipuloinnin tai indoktrinaation kohteeksi.

Myös rikolliset ja turvallisuutta uhkaavia tekoja suunnittelevat henkilöt käyttävät tieto- ja viestintäjärjestelmiä, joten niistä on kerättävissä jälkiä myös heidän toiminnastaan. Tätä muuttunutta toimintaympäristöä, johon liittyvät kiinteästi myös uhkien kansainvälistyminen sekä sisäisen ja ulkoisen turvallisuuden rajojen hämärtyminen, on käytetty perusteena säätää lakeja, jotka mahdollistavat esitutkinta- ja tiedusteluviranomaisille toimivaltuudet hankkia tietoa myös tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista. Toimivaltuuskenttä on ollut murroksessa ympäri maailmaa ja samalla on lisääntynyt yhteiskuntien pyrkimys estää ennalta vakavimmiksi koettujen uhkien, kuten terrori-iskujen, toteuttaminen. Rikostutkinnan osalta toimivaltuudet verkossa ovat tyypillisesti melko selkeät: tapahtuma, jota epäillään rikokseksi tai sen valmisteluksi, pyritään selvittämään kohdistamalla ensisijaisesti epäiltyyn henkilöön tai hänen käyttämäänsä laitteeseen toimenpiteitä, joiden käytön edellytykset on määritetty laissa. Rikosten lisäksi yhteiskuntia uhkaavat tapahtumat, joita kutsutaan kansallisen turvallisuuden uhkiksi. Tiedonhankinta niistä kuuluu pitkälti tiedusteluviranomaisten tontille. Osa kansallisen turvallisuuden uhkista on myös rikoksia, mutta osa muita tapahtumia, kuten valtion edun vaarantavia vieraan valtion tekemiä toimia, joita ei ole aina mahdollista tai tarkoituksenmukaista käsitellä rikosprosessissa. Esimerkiksi vaikuttaminen vaaleihin tai maassa asuvien ihmisten vastakkainasettelun lisääminen internetissä provosoimalla ja suuntaamalla valeuutisvirtaa harkituille kohderyhmille, voivat olla valtiojohtoisia operaatioita. Toisin kuin rikoslaissa määritellyt yksityiskohtaiset rikoksen tunnusmerkistöt, kansallisen turvallisuuden uhkat ovat usein lakiin kirjattuja listoja mahdollisista kohteista, joista tiedusteluviranomaiset ovat oikeutettuja hankkimaan tietoa tiedustelumenetelmiä käyttämällä. Suomen osalta lainsäädäntö lisäksi edellyttää, että uhkien on oltava vakavia. Sallitut siviili- ja sotilastiedustelukohteet on lueteltu tämän raportin Taulukossa 1 (s. 28).

Kansallisen turvallisuuden uhkien toteutumisen ennalta estäminen asettaa paineen kohdistaa viranomaisvalvontaa aiempaa suurempaan joukkoon viestintää, varhaisemmassa vaiheessa, matalammalla kynnyksellä sekä epätarkemmin määriteltyihin tilanteisiin. Tämä puolestaan lisää todennäköisyyttä, että syyttömien ihmisten toimia tarkkaillaan yhteiskunnassa tavalla, joka ulottuu heidän perusoikeuksiensa,

kuten esimerkiksi yksityisyyden, sananvapauden ja kokoontumisvapauden piiriin. Tiedusteluviranomaisten toiminta on salaista muille paitsi toimintaa sen ulkopuolelta valvoville virallisille tahoille. Sen sijaan, jos rikosepäilyn johdosta nostetaan syyte, julkinen oikeudenkäynti toimii suojamekanismina mahdollisia viranomaisvalvonnan väärinkäytöksiä vastaan. Muiden muassa näiden syiden vuoksi tiedusteluviranomaisten toiminnan raamit, kuten missä tilanteissa, millä menetelmillä ja millä perustein tiedustelu on sallittua sekä miten toimintaa tulisi luotettavasti valvoa, ovat herättäneet kriittistäkin keskustelua eri maissa, myös Suomessa.

Siviili- ja sotilastiedustelu oli maassamme sääntelemätön alue, kunnes eduskunta hyväksyi maaliskuussa 2019 suojelupoliisia ja puolustusvoimia koskevat tiedustelulait, jotka astuivat voimaan kesäkuussa 2019. Poliisin perustyöhön tiedustelulakipaketti ei merkittävästi vaikuta, vaan poliisin omat rikostiedustelun ja -tutkinnan toimivaltuudet säilyivät ennallaan. Tosin joissakin tapauksissa uusien toimivaltuuksien perusteella kerättyä tietoa on mahdollista luovuttaa poliisille. Tiedustelulait määrittävät suojelupoliisin ja puolustusvoimien salaisen tiedonhankinnan kohteet ja tiedustelumenetelmien käytön edellytykset. Siviilitiedustelun tarkoituksena on saada tietoa kohteista, esimerkiksi terrorismista, *joka vakavasti uhkaa kansallista turvallisuutta* (poliisilaki 5a:3-4). Lakimuutos irrottaa suojelupoliisin tiedustelutoiminnan rikosepäilyihin liittyvästä salaisesta tiedonhankinnasta ja on jatkumoa suojelupoliisin viime vuosien muutokselle esitutkintaviranomaisesta tiedustelupalveluksi. Sotilastiedustelun osalta uusi lainsäädäntö loi puuttuneet raamit toiminnalle, mikä tekee puolustusvoimien tiedusteluperiaatteista ja keinovalikoimasta aiempaa avoimempia.

Tässä julkaisussa esitetään *"Taking Surveillance Apart? Accountability and Legitimacy of Internet Surveillance and Expanded Investigatory Powers"* -tutkimushankkeen[1] keskeisiä haastattelu- ja kyselyaineistoihin perustuvia Suomea koskevia tuloksia[2]. Tutkimuksessa tarkastellaan asiantuntijasidosryhmien näkemyksiä erityisesti tiedustelulainsäädännöstä (ks. myös Leppänen & Houtsonen, Hyväksytty julkaistavaksi) sekä yliopisto-opiskelijoiden ja henkilökunnan käsityksiä poliisin ja tiedusteluviranomaisten toimivaltuuksista verkossa. Tämä julkaisu on suunnattu kaikille aihepiiristä kiinnostuneille, ja se avaa näkökulmia ennen kaikkea kysymykseen *Mitä Suomessa ajatellaan poliisin ja tiedusteluviranomaisten toimivaltuuksista kerätä, säilyttää ja analysoida tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista saatavaa tietoa?* Aihe on tärkeä ja ajankohtainen, koska tieto uuden lainsäädännön tuntemuksesta ja vastaanotosta voi vaikuttaa viranomaistoimien koettuun legitimiteettiin eli hyväksyttävyyteen. Raporttimme on korostuneen empiirinen, koska keskitymme tuomaan esiin eri osapuolten esittämiä käsityksiä ja mielipiteitä. Lisäksi taustoitamme aihepiirin lainsäädäntöä ja tarjoamme lukijoille vinkkejä toimivaltuuksiin liittyvistä yksityiskohtaisemmista lähteistä. Tarkoituksemme on myös dokumentoida kansainvälisen tutkimusprojektimme Suomen osuutta kattavasti. Toivomme

1 Projektin rahoitti NordForsk Nordic Societal Security -ohjelmasta projektinumerolla 80895. Projektin pääpartnereita olivat Poliisiammattikorkeakoulun lisäksi Dundeen yliopisto ja Norjan poliisiammattikorkeakoulu. Lisäksi projekti hyödynsi asiantuntijoita mm. Uppsalan yliopistosta, St. Andrewsin yliopistosta, Oslon yliopistosta, Glasgown yliopistosta ja Edinburghin yliopistosta. Projektin kotisivut: https://sites.dundee.ac.uk/eyes-online-project/

2 Tutkimustuloksia on vertaisarvioitavana myös kansainvälisessä tieteellisessä aikakausjulkaisussa. Tässä raportissa avataan suomen kielellä empiirisiä tutkimustuloksia ja taustaa laajemmin kuin se on mahdollista lyhyessä artikkelissa.

tutkimustulostemme ja raporttimme kannustavan eri toimijoita työskentelemään yhdessä vastuullisen ja legitiimin viranomaisvalvonnan puolesta. Vastaamme raportilla myös tutkimuksemme esiin nostamaan tiedontarpeeseen: kansalaiset kaipaavat lisää tietoa turvallisuusviranomaisten toimivaltuuksista verkossa.

Julkaisun rakenne on seuraava. Ensiksi rajaamme käsitteellisesti tutkimuskysymyksemme. Sen jälkeen tarkastelemme esitutkinta- ja tiedusteluviranomaisten tiedonhankinnan toimivaltuuksia Suomessa keskittyen salaiseen tiedonhankintaan sekä kuvaamme tiedustelulakipaketin valmisteluprosessia. Seuraavaksi siirrymme tutkimuksen empiirisiin havaintoihimme ja kuvaamme, mitä asiantuntijat sekä suomalaisten yliopistojen opiskelijoista ja henkilökunnasta koottu vastaajajoukko ajattelevat viranomaisten toimivaltuuksista verkossa. Lopuksi kokoamme yhteen eri vastaajaryhmien tulokset ja pohdimme tuloksiamme sekä esitämme kaksi toimenpidesuositusta.

4 TUTKIMUSKYSYMYKSEMME KÄSITTEELLINEN RAJAAMINEN

Tässä raportissa tutkimuskysymyksemme on *Mitä Suomessa ajatellaan poliisin ja tiedusteluviranomaisten toimivaltuuksista kerätä, säilyttää ja analysoida tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista saatavaa tietoa?*

Kansainvälisen tutkimusprojektimme lähtökohtana oli englanninkielinen käsite *”online surveillance by the state”*, jolle ei ole vakiintunutta määritelmää eikä täysin kuvaavaa suomenkielistä vastinetta. Surveillance-tutkimuksen alalla työskentelevä konkari David Lyon (2007, 14) mieltää, että termi *”surveillance”* tarkoittaa *”keskittynyttä, systemaattista ja rutiininomaista huomiota henkilötietoihin vaikuttamis-, johtamis-, suojelemis- tai ohjaamistarkoituksessa”*. Sanastokeskuksen TEPA-termipankkiin kokoamien, eri lähteistä tallennettujen määritelmien mukaan *”surveillance”* käännetään valvonnaksi, tarkkailuksi ja seurannaksi sekä joskus myös peitetoimina suoritettavaksi tarkkailuksi[3]. Ideaalikäännös olisi sana, joka käsittäisi nuo kaikki ominaisuudet. *”Online”* on puolestaan suomen kielessä tutuimmin käytössä etuliitteenä, jolla viitataan jonkin, esimerkiksi palvelun, toimivan tietoliikenneyhteyden välityksellä tai esimerkiksi laitteen, kuten tulostimen, olevan linjatilassa[4]. *”By the state”* käsitteen alle tutkimusryhmämme rajasi kunkin tutkimuskohteena olevan maan valtion viranomaisten harjoittaman toiminnan, joka tarkennettiin viranomaiskentän moninaisuudesta johtuen suppeammin lainvalvonta- ja tiedusteluviranomaisiin, joiden muodostamasta kokonaisuudesta käytämme käsitettä turvallisuusviranomaiset. Koska tiedusteluviranomaisten suorittama sotilas- ja siviilikohteiden tiedustelu tapahtuu eri viitekehyksissä ja niihin liittyvät rajoitukset ovat siten erilaiset, päätimme keskittyä ensisijaisesti siviilikohteisiin, vaikka rajanveto ei aina olekaan selkeä (FRA 2017, 27). Siviilihenkilöihin kohdistuvien tiedustelutoimenpiteiden kulmakivi on niiden toteuttaminen perus- ja ihmisoikeuksien asettamien reunaehtojen sisällä (FRA 2017). Perus- ja ihmisoikeuslähtöiset reunaehdot pätevät myös lainvalvontaviranomaisten perustehtäviin eli valvontaan, että lakia noudatetaan, epäiltyjen rikosten esitutkintaan ja epäiltyjen rikollisten pidättämiseen[5]. Sen sijaan esimerkiksi yksityiskohtaisissa perusteluissa Hallituksen esityksessä sotilastiedustelulaiksi todetaan, ettei valtiollinen toimija, kuten vieraan valtion viranomainen tai sellaiseen rinnastuva toimija, joihin siis sotilastiedustelu merkittävin osin kohdistuu, nauti perusoikeussuojaa (HE 203/2017 vp, 200-201).

Käytännössä tutkimuksemme painopiste on Suomen osalta poliisin ja suojelupoliisin tehtäväkentässä, mutta koska tiedustelulait valmisteltiin pakettina, käsittelemme jonkin verran myös sotilastiedusteluviranomaisten eli Puolustusvoimien tiedustelulaitoksen ja pääesikunnan, toimintaa. Lainvalvontaviranomaisista käytetään Suomessa yleisemmin nimitystä esitutkintaviranomainen. Pilottihaastattelujen perusteella tuntui kuitenkin luontevimmalta puhua asiantuntijoille aineistonkeruuvaiheessa tiedusteluviranomaisten ohessa lainvalvontaviranomaisista, mikä kuvasi

3 TEPA-termipankki, ”surveillance”. https://termipankki.fi/tepa/fi/haku/surveillance Saatavilla: 28.1.2021.
4 TEPA-termipankki, ”online”. https://termipankki.fi/tepa/fi/haku/online Saatavilla 28.1.2021
5 Tiedusteluviranomaisten ja lainvalvontaviranomaisten, kuten poliisin, tehtäväkentän eroista puhutaan tarkemmin seuraavassa pääluvussa.

parhaiten kansainvälistä kontekstia ja oli asiantuntijoille tuttu käsite. Aihepiiriä tuntemattomille puhuimme puolestaan selkeyden vuoksi tiedusteluviranomaisten lisäksi poliisista, koska käsitteet lainvalvonta- tai esitutkintaviranomainen vaikuttivat vierailta. Lisäksi poliisi on esitutkintaviranomaisistamme tunnetuin ja sen toimivaltuudet ovat kattavimmat.

Käytämme tässä raportissa tutkimuksemme pääkäsitteestä eli edellä avatusta ”online surveillance by the state” seuraavaa määritelmää sekä tekstin sujuvuuden takia siitä tehtyjä lyhenteitä:

- poliisin ja tiedusteluviranomaisten toimivaltuudet kerätä, säilyttää ja analysoida tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista saatavaa tietoa
- sekä lyhennettynä: viranomaisten toimivaltuudet verkossa, viranomaisvalvonta verkossa ja viranomaisvalvonta

Yllä esitetyt ovat sateenvarjokäsitteitä, jotka kattavat tässä raportissa kaikki erilaiset menetelmät, joilla poliisi ja tiedusteluviranomaiset suorittavat tiedonhankintaa tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista. Käsitteisiin on sisäänrakennettuna myös tiedonvaihto esimerkiksi toisten valtioiden kanssa. Puhuessamme tiedusteluviranomaisten uusien tiedustelulakien nojalla kohteelta salaa suoritetusta tiedustelusta yleisellä tasolla, käytämme käsitettä tiedustelu(menetelmät) ja poliisin keinovalikoimaa kutsumme salaisiksi pakkokeinoiksi. Käsite salaiset tiedonhankinta(menetelmät) kattaa tässä raportissa kummankin toiminnan tai puhumme yleisellä tasolla haluamatta täsmentää viranomaista. Samalla logiikalla puhumme tiedonhankinta(menetelmistä), kun tarkoitamme tiedonhankintaa yleisesti, esimerkiksi täsmentämättä, onko kyse poliisin vai tiedusteluviranomaisten suorittamasta tai onko se määritetty salaiseksi vai ei. Lisäksi tutkimustuloksista kerrottaessa käytämme myös aineistonkeruun aikana osallistujille esitettyjä käsitteitä, joiden avulla pyrimme saamaan tietoa tutkimusaiheestamme puhuttuun kieleen sopivalla tavalla.

5 ESITUTKINTA- JA TIEDUSTELUVIRANOMAISTEN TOIMIVALTUUDET VERKOSSA

Suomessa viranomaistoiminta perustuu lakeihin. Perusteet, joiden nojalla esitutkinta- ja tiedusteluviranomaisilla on oikeus kerätä, säilyttää ja analysoida tietoa, on määritelty joukossa eri lakeja. Lait asettavat viranomaistoiminnalle myös perus- ja ihmisoikeuksista johdetun arvoviitekehyksen. Esimerkiksi tiedustelulainsäädäntö sisältää pykälätasoisesti kirjattuna perus- ja ihmisoikeuksien kunnioittamisesta, toimenpiteiden suhteellisuudesta, vähimmän haitan periaatteesta, toimivaltuuksien käytön tarkoitussidonnaisuudesta ja syrjinnän kiellosta[6]. Merkittävä osa tiedonhankinnasta tapahtuu salassa rikoksesta epäillyltä tai kohteelta, jottei tieto viranomaistoimista vaikuta henkilön käyttäytymiseen tai saa häntä tuhoamaan jälkiä mahdollisesta rikoksesta tai muusta uhkaksi tulkittavasta toiminnasta. Tämän luvun tarkoitus on tarjota yksinkertainen yleiskuvaus niistä toimivaltuuksista, joilla salaista tiedonhankintaa tehdään, sekä auttaa aihepiiristä kiinnostunutta lukijaa löytämään syvällisempää tietoa esimerkiksi oikeustieteellisestä kirjallisuudesta ja oikeuslähteistä. Kuvauksemme ei ole aiheen oikeustieteellinen yleisesitys tai oikeudellinen analyysi lainsäädännöstä.

Monet tiedonhankintamenetelmät soveltuvat käytettäväksi sekä verkossa että fyysisessä maailmassa. Keskitymme pääasiassa salaisiin menetelmiin, koska tiedustelulainsäädännössä on kyse salaa tapahtuvasta tiedustelusta ja toisaalta, pitkälti samat pykälät mutta eri kohdentamisalalla ja edellytyksin ovat koskeneet jo vuosien ajan poliisin ja suojelupoliisin toimintaa. Lisäksi salaiseen tiedonhankintaan liittyy todennäköisesti eniten epätietoisuutta, koska se paljastuu kohteeksi joutuneille vasta viiveellä, tai joissakin tapauksissa tuomioistuin voi päättää kertomatta jättämisestä kokonaan. Käsittelemme salaisen tiedonhankinnan pääpiirteitä, minkä takia monia lakien yksityiskohtia on jätetty käsittelemättä ja tekstissä viitataan lakipykäliin vain tärkeimmiltä osin. Osa käytetyistä oikeuslähteistä mainitaan alalukujen lopuksi vinkkeinä, joista kiinnostuneet voivat etsiä lisätietoa.

5.1 Tiedonhankinta rikosepäilyn yhteydessä

Rikosten tunnusmerkistöt ja rangaistusasteikot esitetään rikoslaissa (39/1889, jatkossa rikoslaki). Suomessa poliisi tutkii epäillyt rikokset, mitä kutsutaan esitutkinnaksi. Esitutkinnasta säädetään esitutkintalaissa (805/2011, jatkossa esitutkintalaki). Myös rajavartio-, tulli- ja sotilasviranomaiset ovat erillisten lakien ohjaamina esitutkintaviranomaisia omilla toimialoillaan eli toimivaltaisia hoitamaan esitutkinnan erikseen rajatuissa tilanteissa. Esitutkinnan päätarkoitus on selvittää, onko tapahtunut rikosta, keitä henkilöitä tapahtumiin liittyy sekä mitä vahinkoa ja hyötyä siitä on osapuolille aiheutunut. Esitutkinta on perusta, johon nojaten syyttäjä arvioi, onko tapahtumasta aihetta nostaa syyte ja saattaa se näin oikeuden ratkaistavaksi. Tilanteet, joissa syyttäjä on velvollinen nostamaan syytteen tai joissa hänellä on harkintavaltaa olla nostamatta syytettä, on määritetty laissa

6 Katso lisää: poliisilaki (872/2011) 1:2-5; laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019) 1.2-3 §; laki sotilastiedustelusta (590/2019) 5-9 §.

oikeudenkäynnistä rikosasioissa (689/1997) (jatkossa: ROL). Pääsäännön mukaan syyte nostetaan, jos tapahtuma on rikos, se ei ole vanhentunut ja esitutkinnassa on löytynyt näyttöä syyllisyydestä (ROL 1:6). Syyttäjällä on kuitenkin harkintavaltaa esimerkiksi lievien ja alaikäisten tekemien rikosten osalta sekä kustannusperusteisesti (ROL 1:7-8). Lisäksi on olemassa myös joukko rikoksia, joita kutsutaan asianomistajarikoksiksi ja joista voidaan nostaa syyte vain asianomistajan eli uhrin pyynnöstä tai jos erittäin tärkeä yleinen etu niin vaatii (ROL 1:6a.3; rikoslaki ks. esim. 28:15.) Esimerkkejä asianomistajarikoksista, jotka voivat tapahtua myös verkossa, ovat muiden muassa kunnianloukkaus, luvaton käyttö, törkeä luvaton käyttö, salakatselu ja -kuuntelu sekä tekijänoikeusrikos.

Vaikka keskitymme tässä raportissa salaiseen tiedonhankintaan, on tarpeen ymmärtää, että osa poliisin tiedonhankinnasta, kuten esimerkiksi rikostutkinnan perusmenetelmät *kotietsintä*, *takavarikko* ja *laite-etsintä*, suoritetaan avoimemmin. Yksinkertaistettuna menetelmien tarkoitus on löytää, ottaa haltuun ja saattaa tarkemmin tutkittavaksi rikokseen liittyvää tietoa ja esineitä. Menetelmistä säädetään pakkokeinolain (806/2011, jatkossa pakkokeinolaki) luvuissa 7 ”Takavarikoiminen ja asiakirjan jäljentäminen” sekä 8 ”Etsintä”. Henkilöllä, jonka luona kotietsintä suoritetaan, on pääsääntöisesti oikeus olla läsnä ja pyytää todistaja mukaan seuraamaan toimenpidettä. Läsnäolon edellytys on, ettei se viivytä kotietsintää merkittävästi, eivätkä paikalla olevat henkilöt käyttäytymisellään haittaa tai vaaranna sen tarkoituksen toteutumista (pakkokeinolaki 8:5-6). Kotietsinnässä löydetyn teknisen laitteen sisältö voidaan kopioida tai tarvittaessa koko laite takavarikoida laitteen sisällön selvittämiseen tähtäävää laite-etsintää varten. Laite-etsinnän avulla voidaan saada tietoa esimerkiksi asiakirjoista, ääni-, video- tai kuvatiedostoista sekä ohjelmistojen käyttöön liittyvistä lokitiedostoista. Verkkoon kytketyn laitteen laite-etsinnästä ilmoittaminen poissaolevalle epäillylle, jotta tämä voisi saapua paikalle, on kyseenalaista, koska epäilty voi pyrkiä tuhoamaan tutkinnan kannalta merkityksellistä tietoa tietojärjestelmistä etäyhteyden kautta (Riekkinen 2019, 236). Toisaalta poliisi voi myös suorittaa laite-etsinnän etänä käymättä epäillyn kotona tai käyttämättä hänen fyysistä laitettaan (pakkokeinolaki 8:27).

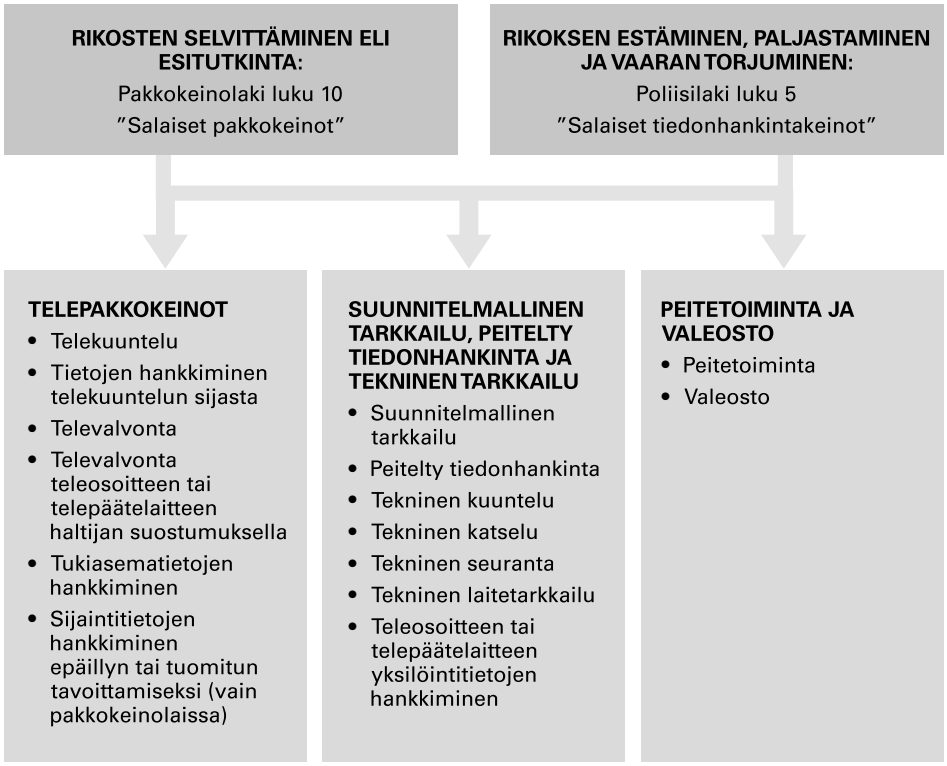
Poliisin salaiset tiedonhankintamenetelmät sekä menetelmien käytön edellytykset, vaatimat luvat ja käytöstä ilmoittaminen on määritelty pakkokeinolain 10 luvussa ”Salaiset pakkokeinot” ja poliisilain (872/2011, jatkossa poliisilaki) 5 luvussa ”Salaiset tiedonhankintakeinot”. Lukujen sisällöt vastaavat pitkälti toisiaan, mutta pakkokeinolain pykäliä sovelletaan rikosten esitutkinnassa, kun taas poliisilain käyttöala on rikoksen estäminen, paljastaminen ja vaaran torjuminen (Kuvio 1). Lisäksi menetelmien nimikkeet vaihtelevat hieman laista riippuen. Tässä raportissa käytämme pakkokeinolaista tuttuja nimikkeitä.

Esitutkinnassa on siis jo syytä epäillä rikosta ja poliisi pyrkii selvittämään, mitä on tapahtunut ja rakentamaan näyttöä mahdollista oikeuskäsittelyä varten. Rikosten estäminen, paljastaminen ja vaaran torjuminen puolestaan kohdistuvat aikaan, jolloin esitutkinnan kynnys ei ole vielä ylittynyt, mutta poliisi pyrkii selvittämään, onko esitutkinnan aloittamiseen aihetta. Salaisten pakkokeinojen yleiset käytön edellytykset ovat, että niillä voidaan olettaa saatavan rikoksen selvittämiseksi, estämiseksi, paljastamiseksi tai vaaran torjumiseksi tarvittavia tietoja (pakkokeinolaki 10:2.1; poliisilaki 5:2.1). Lisäksi joihinkin salaisiin pakkokeinoihin, kuten telekuunteluun, suunnitelmalliseen tarkkailuun ja tekniseen laitetarkkailuun, sisältyy erityinen edellytys, että niillä on oltava erittäin tärkeä merkitys edellä mainittujen

tietojen hankkimiseksi. Peitetoiminnan ja valeostojen kynnys on kaikkein korkein: sen on oltava lisäksi välttämätöntä rikoksen selvittämiseksi, tutkimiseksi tai paljastamiseksi. (Pakkokeinolaki 10:2.2; poliisilaki 5:2.2.) Menetelmien käyttöä rajataan myös määräajalla sekä velvoitteella lopettaa salaisen pakkokeinon käyttö, jos käytön tarkoitus on saavutettu tai käytölle ei enää ole edellytyksiä (pakkokeinolaki 10:2.3; poliisilaki 5:2.3).

Rikokset ja rikostyypit, joihin kutakin salaista pakkokeinoa saa käyttää sekä millaisen lupaprosessin niiden käyttö edellyttää, on määritelty pakkokeino- ja poliisilaissa jokaisen menetelmän osalta. Lisäksi päätökselle ja lupahakemukselle on määritelty kriteerit, mitä niiden pitää sisältää. Lievemmiksi määriteltyjen keinojen käytöstä päätetään poliisilaitoksen sisällä ja päätöksen tekee tyypillisesti tutkinnanjohtaja tai muu pidättämiseen oikeutettu virkamies. Keinojen, joilla puututaan enemmän yksityisyyteen, käytöstä päättää tuomioistuin. Lupa pyritään hankkimaan ennen salaisen pakkokeinon käytön aloitusta, mutta jos aloitus ei siedä viivytystä, poliisilla on 24 tuntia aikaa saattaa aloituspäätös tuomarin uudelleenarvioitavaksi. Lisäksi salaisten pakkokeinojen käytöstä on ilmoitettava epäillylle tai kohteelle pääsääntöisesti viimeistään vuoden kuluttua sen käytön lopettamisesta tai kun tiedonhankinnan tarkoitus on saavutettu, esimerkiksi juttu on siirretty syyttäjälle syyteharkintaan. Tuomioistuimen päätöksellä ilmoittamista on mahdollista lykätä ja vakavimmissa tapauksissa, jos kertominen vaarantaisi valtion turvallisuuden tai jonkun hengen tai terveyden, ilmoitus voidaan jättää kokonaan tekemättä.

Tässä raportissa esitellään kolmen tyyppisiä salaisia pakkokeinoja, joita voidaan soveltaa tiedonhankintaan tieto- ja viestintäverkoista tai niihin kytketyistä laitteista: 1) Telepakkokeinot, 2) Suunnitelmallinen tarkkailu, peitelty tiedonhankinta ja tekninen tarkkailu sekä 3) Peitetoiminta ja valeostot (Kuvio 2). Kukin tyyppi on erillinen alaotsikkonsa pakkokeinolain 10 luvussa ja poliisilain 5 luvussa. Poliisihallitus raportoi vuosittain poliisin käyttämät salaisen tiedonhankinnan menetelmät julkisesti. Vuoden 2018 vuosiraportista selviää, että lupia haetaan selvästi enemmän rikostutkintaan eli pakkokeinolainmukaiseen tiedonhankintaan kuin poliisilainmukaiseen tiedonhankintaan (Poliisihallitus 2019). Tyypillisimmät rikostutkintaan myönnetyt luvat koskivat vuonna 2018 televalvontaa (3754 kpl) sekä telekuuntelun ja -valvonnan yhdistelmää (2867 kpl) (Poliisihallitus 2019, 4). Poliisilakiperustaisia televalvontalupia myönnettiin 270, sen sijaan telekuuntelua ja -valvontaa mainitaan toteutetun vain muutamien yksittäisten rikosten estämiseksi tai torjumiseksi (Poliisihallitus 2019, 15-16). Vertailun vuoksi, esimerkiksi teknisestä kuuntelusta tehtiin 171 pakkokeinolaki- ja 15 poliisilakiperustaista päätöstä. Suosituin teknisen tarkkailun menetelmä oli tekninen seuranta, josta tehtiin 321 pakkokeinolaki- ja 48 poliisilakiperusteista päätöstä (Poliisihallitus 2019, 23-24; 28). Peitetoiminta on yleisempää verkossa kuin fyysisessä maailmassa ja sitä koskevia uusia ja jatkopäätöksiä on tehty kumpaakin muutamia (Poliisihallitus 2019, 35).



Kuvio 1 Poliisin salaiset pakkokeinot ja salaiset tiedonhankintakeinot hankkia ja hyödyntää tieto- ja viestintäverkoista ja verkkoon kytketyistä laitteista saatavaa tietoa.

Telepakkokeinot

Poliisin salaista tiedonhankintaa tieto- ja puhelinverkoista kutsutaan pakkokeinolaissa telepakkokeinoiksi ja poliisilaissa tiedonhankinnaksi televerkoista. Tässä julkaisussa puhumme jatkossa telepakkokeinoista. Telepakkokeinot jakautuvat kuuteen osa-alueeseen: *telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella, sijaintitietojen hankkiminen epäillyn tai tuomitun tavoittamiseksi* sekä *tukiasematietojen hankkiminen* (Kuvio 1).

Televalvonnan tarkoitus on selvittää viestinnän välitystietoja, kuten viestinnän osapuolet, ajankohta ja kesto, ja se on mahdollista suorittaa myös jälkikäteen. Televalvonta kohdistuu yleisessä viestintäverkossa liikkuviin viesteihin ja edellyttää, että tietty laite tai teleosoite pystytään yhdistämään rikosepäilyyn (pakkokeinolaki 10:6; poliisilaki 5:8). Yleinen viestintäverkko tarkoittaa esimerkiksi kaupallista laajakaistaverkkoa tai puhelinverkkoa, erotuksena esimerkiksi yritysten sisäverkoista, jotka eivät ole yleisiä. Televalvonnalla ei hankita tietoa viestin sisällöstä. Selvitettävät tiedot voivat olla esimerkiksi puhelinnumeroita, aikaleimoja, paikkatietoja, IP-osoitteita, laitetietoja, sähköpostiosoitteita ja käyttäjätunnuksia sekä niihin liittyviä henkilöllisyyksiä. Laissa sähköisen viestinnän palveluista (19:157) tietyille

yrityksille, esimerkiksi matkapuhelin- ja internetoperaattoreille, on määrätty välitystietojen säilyttämisvelvollisuus viranomaisia, kuten poliisia varten. Säilytysaika riippuu viestinnän tyypistä ja on joko 6, 9 tai 12 kuukautta. Lisäksi poliisilaki (5:61) ja pakkokeinolaki (10:63) velvoittavat teleyrityksiä avustamaan telekuuntelun, televalvonnan ja teknisen seurannan toimeenpanossa. Kuten jo aiemmin todettiin, televalvontaa saa käyttää rikosten esitutkinnassa, estämisessä, paljastamisessa sekä vaaran torjumisessa, jos sillä voidaan olettaa saatavan kyseisten tehtävien kannalta tarvittavia tietoja. Selvästi tyypillisintä on käyttää sitä huumausainerikosten pakkokeinolain mukaiseen esitutkintaan (Poliisihallitus 2019, 6; 17). Televalvonnan on tarkoitus kohdistua epäillyn hallussa olevaan tai hänen oletettavasti käyttämäänsä laitteeseen tai teleosoitteeseen (pakkokeinolaki 10:6; poliisilaki 5:8). Poliisi voi pyytää tietoja esimerkiksi älypuhelimen laitekohtaisen tunnusnumeron eli IMEI-koodin, IP-osoitteen tai keskustelupalstan nimimerkin perusteella. Rikosepäilyt, joissa televalvontaa saa käyttää, on määritelty pakkokeinolain 10:6:ssä ja poliisilain 5:8:ssä. Esimerkkejä tapauksista ovat seuraavat: rikokset, joiden maksimirangaistus on neljä vuotta vankeutta tai enemmän, rikokset, jotka on tehty teleosoitetta tai telepäätelaitetta käyttäen, huumausainerikokset, lapsen houkutteleminen seksuaalisiin tarkoituksiin ja joukko terrorismiin liittyviä rikoksia. Televalvonta ja sijaintitietojen hankkiminen edellyttävät tuomioistuimelta haettua lupaa. Lupa haetaan ensisijaisesti etukäteen, ja jos tilanne ei siedä viivettä, viimeistään 24 tunnin kuluttua toiminnan aloittamisesta. Lupahakemuksessa poliisi perustelee päätöksen tekevälle tuomarille muiden muassa mitä rikosta se epäilee, kuka on epäiltynä sekä miksi salaista pakkokeinoa tarvitaan ja kuinka pitkäksi aikaa. (Pakkokeinolaki 10:9; poliisilaki 5:10). **Televalvontaa voi suorittaa myös teleosoitteen tai telepäätelaitteen haltijan suostumuksella** lievemmissä rikoksissa, esimerkiksi tilanteissa, joista voi seurata vankeutta enimmillään kaksi vuotta tai enemmän tai jos telepääteosoitetta on käytetty rikoksen tekemiseen (pakkokeinolaki 10:7; poliisilaki 5:9).

Telekuuntelulla siepataan viestejä, kun ne ovat välitettävänä yleisessä viestintäverkossa. Viestejä, kuten sähköposteja, tekstiviestejä ja puheluita voidaan kuunnella reaaliaikaisesti tai ne voidaan tallentaa myöhempää sisällön selvittämistä varten. Telekuuntelu on määritelty laissa järeämmäksi keinoksi kuin esimerkiksi televalvonta ja kynnys siihen on korkeampi kuin televalvonnassa. Telekuuntelua saa käyttää vain, jos menetelmän käytön merkity*s* on arvioitu *erittäin tärkeäksi* rikoksen selvittämiseksi, estämiseksi tai paljastamiseksi (pakkokeinolaki 10:2; poliisilaki 5:2). Telekuuntelu kohdistetaan epäillyltä lähtöisin olevaan tai epäillylle tarkoitettuun viestiin. Rikoksia, joissa telekuuntelua voi käyttää, ovat esimerkiksi henkirikokset murha, tappo tai surma, joukko törkeitä rikoksia, lapsen seksuaalinen hyväksikäyttö, joukko terrorismirikoksia, vakoilu, valtiopetoksen valmistelu ja joukkotuhonnan valmistelu. (Pakkokeinolaki 10:3; Poliisilaki 5:5.) Telekuuntelun lisäksi hankintaan usein lupa myös televalvontaan. Tyypillisin perusterikoslaji telekuuntelun ja -valvonnan yhdistelmälle oli vuonna 2018 huumausainerikollisuuden tutkinta, mikä kattoi 75 % perusterikoksista (Poliisihallitus 2019, 6). Lupa telekuunteluun haetaan käräjäoikeudesta korkeintaan kuukaudeksi kerrallaan (pakkokeinolaki 10:5; poliisilaki 5:7). **Tietojen hankkiminen telekuuntelun sijasta** kohdistuu viesteihin, joiden sisältöä ja tunnistetietoja ei ole enää saatavissa telekuuntelulla (pakkokeinolaki 10:4; poliisilaki 5:6). Siihen pätee samat edellytykset kuin telekuunteluun. Käytännössä lakipykälää voidaan soveltaa esimerkiksi silloin, jos käyttäjä on poistanut sähköpostiviestin, mutta se on vielä

tallessa teleyrityksellä tai yhteisötilaajalla, kuten oppilaitoksella, joka tarjoaa viestintäpalveluita henkilökunnalle ja opiskelijoilleen.

Sijaintitietojen hankkimisessa on kyse epäillyn tai tuomitun henkilön paikantamisesta laitteen tai teleosoitteen, esimerkiksi puhelimen sijaintitietojen avulla (pakkokeinolaki 10:8). **Tukiasematietoja hankkimalla** puolestaan pystytään selvittämään, mitkä laitteet ovat olleet yhteydessä tiettyihin tukiasemiin esimerkiksi rikoksen tapahtumisaikana (pakkokeinolaki 10:10; poliisilaki 5:11). Tukiasematietoihin tallentuu kaikki tukiasemaan kytkeytyneet laitteet, joiden joukosta poliisi pyrkii analysoimaan epäillyn rikoksen kannalta olennaiset, kuten esimerkiksi tunnistamaan epäiltyjen henkilöiden hallussa olleet laitteet ja saamaan siten vihjeen heidän henkilöllisyyksistään.

Suunnitelmallinen tarkkailu, peitelty tiedonhankinta ja tekninen tarkkailu

Tässä kategoriassa esitellään *peitelty tiedonhankinta* ja *tarkkailukeinoja, joita ovat suunnitelmallinen tarkkailu sekä joukko teknisen tarkkailun menetelmiä*. **Peitellyssä tiedonhankinnassa** poliisi salaa henkilöllisyytensä ja pyrkii hankkimaan henkilöltä tietoja lyhytkestoisessa vuorovaikutuksessa asuntoa lukuun ottamatta missä tahansa paikassa, esimerkiksi internetin keskustelupalstalla. Toiminnan aikana poliisi voi käyttää myös vääriä, harhauttavia ja peiteltyjä tietoja. Peiteltyä tiedonhankintaa saa käyttää rikoksissa, joiden rangaistusmaksimi on vähintään neljä vuotta vankeutta tai kyse on esimerkiksi parituksesta, huumausainerikoksesta, törkeästä tulliselvitysrikoksesta, joukosta terrorismiin liittyviä rikoksia tai toistuvaan rikolliseen toimintaan liittyvästä varkaudesta. (Pakkokeinolaki 10:14; poliisilaki 5:15.) Peitelty tiedonhankinta ei edellytä lupaa tuomioistuimelta, mutta perusteltu päätös siitä tehdään kirjallisesti (pakkokeinolaki 10:15; poliisilaki 10:16).

Poliisi saa tarkkailla salaa esimerkiksi henkilön toimintaa julkisilla keskustelupalstoilla ja sosiaalisessa mediassa ilman että olisi kyse salaisesta tiedonhankinnasta. Mutta siinä vaiheessa, **kun tarkkailu muuttuu suunnitelmalliseksi** eli kohdistuu rikoksesta epäiltyyn tai henkilöön, jonka voidaan perustellusti olettaa syyllistyvän rikokseen ja on luonteeltaan muuta kuin lyhytaikaista tarkkailua, se täyttää salaisen pakkokeinon kriteerit. (Pakkokeinolaki 10:12; poliisilaki 5:13.) Riekkinen (2019, 296-297) pitää epäselvänä kynnystä, milloin tarkkailu verkossa on muutettava salaiseen pakkokeinon (suunnitelmallisen tarkkailun) käytöksi eli kyse on muuten kuin lyhytaikaisesti tapahtuvasta tarkkailusta. Hän kokee ongelmalliseksi tarkkailun ajanjakson määrittelyn, koska verkkojäljet voivat sisältää vuosien aikana tapahtunutta toimintaa sekä automatisoidut tiedonkeruutavat, jotka voivat tallentaa kerralla tietoa hyvin laajasti useista verkkolähteistä (Riekkinen 2019, 296-297). Suunnitelmallista tarkkailua saa käyttää pääsääntöisesti rikostapauksissa, joissa enimmäisrangaistus on vähintään kaksi vuotta vankeutta. Tyypillisin perusterikos suunnitelmalliselle tarkkailulle esitutkinnassa oli huumausainerikokset (Poliisihallitus 2019, 17). Suunnitelmallinen tarkkailu ei edellytä lupaa tuomioistuimelta, mutta perusteltu päätös siitä tehdään kirjallisesti ja se on voimassa enintään kuusi kuukautta. (Pakkokeinolaki 10:12.3;13 [lue: 10 luku 12 § 3 mom. ja 13 §]; poliisilaki 5:13.3;14).

Suunnitelmallisen tarkkailun lisäksi tarkkailukeinoja ovat neljä teknisen tarkkailun menetelmää: *tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu*. Teknisen tarkkailun menetelmästä riippumatta kyse on toiminnasta, jossa poliisi ei ole vuorovaikutuksessa epäillyn kanssa, vaan tarkkailee laitteella,

menetelmällä tai ohjelmistolla salaa toimintaa tai viestintää, jota ei ole tarkoitettu ulkopuolisten tietoon (ks. esim. pakkokeinolaki 10:16). Tietoa ei siis haeta yleisestä viestintäverkosta, vaan päätelaitteen välittämänä. Kaikkiin teknisen tarkkailun menetelmiin sisältyy edellytys, että niitä saa käyttää vain, jos menetelmän käytön *merkitys* on arvioitu *erittäin tärkeäksi* rikoksen selvittämiseksi, estämiseksi tai paljastamiseksi (pakkokeinolaki 10:2.2; poliisilaki 5:2.2). Teknisen seurannan osalta edellytys tosin koskee vain henkilön teknistä seuraamista, ei esimerkiksi esineen.

Tekninen kuuntelu on tarkoitettu viestinnän sisältöjen, osapuolten tai epäillyn toiminnan selvittämiseen ja se voidaan kohdistaa vakoiluohjelman avulla myös teknisiin laitteisiin. Näin voidaan selvittää esimerkiksi tietokoneella kirjoitetun viestin sisältö ennen kuin viesti on lähetetty. Päätös teknisestä kuuntelusta tehdään korkeintaan kuukaudeksi kerrallaan poliisissa sisäisesti paitsi, jos kyse on vapautensa menettäneen epäillyn kuuntelusta tai asuntokuuntelusta, jolloin päätöksen tekee tuomioistuin (pakkokeinolaki 10:16-18; poliisilaki 5:18). Teknistä kuuntelua voidaan käyttää rikoksissa, joiden maksimirangaistus on vähintään neljä vuotta vankeutta sekä esimerkiksi huumausainerikoksissa ja terrorismirikoksissa (pakkokeinolaki 10:16; poliisilaki 5:17-18). Jos kuuntelua suoritetaan vakituiseen asumiseen käytettävässä tilassa, kyse on silloin rikoksen esitutkinnassa käytettävästä asuntokuuntelusta, mitä saa tehdä vain erikseen nimetyissä törkeissä rikoksissa (pakkokeinolaki 10:17).

Teknisessä katselussa tarkkaillaan epäiltyä henkilöä, paikkaa tai tilaa, joka ei ole vakituinen asunto. Riekkisen (2019, 298) mukaan teknisessä katselussa voi käyttää epäillyn oman laitteen kameraa ja sillä pystytään esimerkiksi kuvaamaan, kuka on ollut laitteen tosiasiallinen käyttäjä tiettyyn aikaan sekä kuvaamaan tilassa olevan teknistä laitetta käyttävän henkilön näyttöruutua, jos se näkyy kamerassa. Teknistä katselua on sallittua käyttää, jos epäillään rikosta, jonka rangaistusmaksimi on vähintään vuosi vankeutta. Tekninen katselu edellyttää poliisiyksikön sisäisen kirjallisen päätöksen korkeintaan kuukaudeksi kerrallaan. Jos teknistä katselua suoritetaan kotirauhan piirissä olevassa paikassa tai epäilty on menettänyt rikoksen johdosta vapautensa, tarvitaan tuomioistuimen lupa, ja edellytykset menetelmän käytölle on korkeammat. (Pakkokeinolaki 10:19-20; poliisilaki 5:19-20.)

Teknistä seurantaa voidaan käyttää esimerkiksi esineen tai henkilön liikkumisen seurantaan, eli siinä seurataan sijaintia. Toiminto voidaan toteuttaa joko erillisellä laitteella tai hyödyntämällä epäillyn omaa laitetta. Edellytyksenä kuitenkin on, että seurattava esine tai vastaava on joko rikoksen kohteena, epäillyn hallussa tai hänen oletetusti käyttämänsä. Henkilöön kohdistuva tekninen seuranta edellyttää tuomioistuimen päätöksen viimeistään vuorokauden kuluttua toiminnan aloittamisesta. Omaisuuteen kohdistuvasta seurannasta päätetään poliisilaitoksella sisäisesti ja sitä saa käyttää, jos epäillään rikosta, jonka rangaistusmaksimi on vähintään vuoden vankeustuomio. Henkilöön kohdistuva tekninen seuranta edellyttää vakavampia rikosepäilyjä. (Pakkokeinolaki 10:21-22; poliisilaki 5:21-22.)

Tekninen laitetarkkailu on tarkoitettu nimenomaan tietokoneiden ja muiden vastaavien teknisten laitteiden sekä ohjelmistojen tarkkailuun, mutta ei viestien sisällön tai tunnistamistietojen selvittämiseen. Tekninen laitetarkkailu kohdistetaan rikoksesta epäillyn todennäköisesti käyttämään laitteeseen. Sitä saa käyttää rikoksissa, joiden rangaistusmaksimi on vähintään neljä vuotta vankeutta sekä muutamassa muussa rikoksessa, kuten huumausainerikos ja joukko terrorismirikoksia. Päätöksen teknisestä laitetarkkailusta tekee tuomioistuin viimeistään 24 tunnin kuluttua toiminnan aloittamisesta. (Pakkokeinolaki 10:23-24; poliisilaki 5:23-24.) **Teleosoitteen tai**

telepäätelaitteen yksilöintitietojen hankkimisella tarkoitetaan niiden selvittämistä toimintaan tarkoitettua, erillistä laitetta käyttämällä (pakkokeinolaki 25; poliisilaki 5: 25).

Peitetoiminta ja valeosto

Peitetoiminta fyysisessä maailmassa on yksi poliisin haastavimmista, tarkimmin rajatuista ja suojatuimmista salaisista tiedonhankintamenetelmistä. Peitetoiminnan tarkoitus on vääriä tietoja ja luottamusta hyväksikäyttäen soluttautua asemaan, josta käsin poliisi voi saada tietoja epäillystä rikoksesta tai sellaisen valmistelusta. Luonteeltaan se on pitkäkestoista ja suunnitelmallista. Peitetoiminta kohdistuu pääsääntöisesti törkeäksi määriteltyyn rikolliseen toimintaan, jolla on suunnitelmallisuutta, järjestäytyneisyyttä, ammattimaisuutta tai jatkuvuutta. Peitetoiminnan edellytykset verkossa ovat lievemmät. Sitä saa kohdistaa tietoverkossa epäiltyyn, jota on syytä epäillä rikoksesta, jonka rangaistusmaksimi on vähintään kaksi vuotta vankeutta tai kyseessä on sukupuolisiveellisyyttä loukkaavan kuvan levittäminen. (Pakkokeinolaki 10:27; poliisilaki 5:28.) **Valeostossa** poliisi tekee ostotarjouksen esineestä, aineesta, omaisuudesta tai palvelusta saadakseen esimerkiksi todisteen rikoksesta. Valeostolla ei saa johdattaa kohdetta tai muuta henkilöä tekemään rikosta, jota tämä ei muuten tekisi. (Pakkokeinolaki 10:34; poliisilaki 5:35.) Valeosto voi tapahtua verkossa esimerkiksi huumausainerikosta tutkittaessa. Sitä voidaan käyttää rikosepäilyissä, joiden maksimirangaistus on vähintään kaksi vuotta vankeutta tai varkauden tai kätkemisrikoksen tutkinnassa. Valeostosta päättää pääsääntöisesti keskusrikospoliisin tai suojelupoliisin päällikkö. (Pakkokeinolaki 10:34-35; poliisilaki 5:35-36).

VINKKI! TIESITKÖ, ETTÄ FINLEX.FI ON OIKEUSMINISTERIÖN OMISTAMA LAKITIETOPANKKI, JOSTA VOIT HAKEA AJANTASAISET SÄÄDÖKSET ILMAISEKSI?

Esimerkiksi Finlexin hakukenttään kirjoitettu hakusana ”poliisilaki” vie sinut poliisilakiin.

Tässä alaluvussa käytetyt oikeuslähteet ovat:

39/1889 Rikoslaki
689/1997 Laki oikeudenkäynnistä rikosasioissa
805/2011 Esitutkintalaki
806/2011 Pakkokeinolaki
872/2011 Poliisilaki
917/2014 Laki sähköisen viestinnän palveluista (ent. Tietoyhteiskuntakaari)

Tutustu myös muuhun aihepiirin kirjallisuuteen:

Hankilanoja, Arto (2014). Poliisin salainen tiedonhankinta. Viro.
Poliisihallitus (2019). Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta 2018. Raportti 8.3.2019. POL-2018-55595, ID-1948204.
Riekkinen Juhana (2019). Sähköiset todisteet rikosprosessissa. Alma Talent: Helsinki.

5.2 Tiedonhankinta vakavista uhkista kansalliselle turvallisuudelle

Siviili- ja sotilastiedustelu on tiedonhankintaa vakavista kansallisen turvallisuuden uhkista. Suojelupoliisi vastaa siviilitiedustelusta ja Puolustusvoimien tiedustelulaitos sekä pääesikunta sotilastiedustelusta. Näitä viranomaisia kutsutaan tiedusteluviranomaisiksi. Tiedustelutietoa ja siihen nojaavaa analyysia tarvitaan viranomaistehtävien hoitamiseksi sekä valtion ylimmän johdon päätöksenteon tukemista varten.

Siviilitiedustelusta säädetään poliisilain luvussa 5a ”Siviilitiedustelu” ja sen yhdestä erityismenetelmästä, tietoliikennetiedustelusta, laissa tietoliikennetiedustelusta siviilitiedustelussa (582/2019, jatkossa laki tietoliikennetiedustelusta siviilitiedustelussa). Kaikki sotilastiedustelua koskeva lainsäädäntö on koottu lakiin sotilastiedustelusta (590/2019, jatkossa laki sotilastiedustelusta). Lait ovat olleet voimassa 1.6.2019 alkaen ja niitä on täydennetty myös asetuksin. Suurin osa siviili- ja sotilastiedustelumenetelmistä on sisällöllisesti samoja kuin aiemmin esitellyt poliisin toimivaltuudet, mutta niiden käytön perusteet ovat erilaiset. Sen takia emme kuvaa poliisilaista johdettuja tiedustelumenetelmiä tässä raportissa enää uudestaan, vaan taustoitamme raportin empiirisiä tuloksia esittelemällä tiedustelulakipaketin valmisteluprosessia sekä keskitymme lakien sisällön osalta käyttöperusteisiin ja esittelemään tietoliikennetiedustelua, joka on kokonaan uusi, pelkästään tiedusteluviranomaisia varten säädetty toimivaltuus. Siviili- ja sotilastiedustelun ulkoista valvontaa varten on myös rakennettu oma järjestelmänsä, jonka uudet komponentit koostuvat tiedusteluvalvontavaltuutetun suorittamasta laillisuusvalvonnasta ja eduskunnan tiedusteluvalvontavaliokunnan harjoittamasta parlamentaarisesta valvonnasta. Valvonnasta säädetään laissa tiedustelutoiminnan valvonnasta (121/2019).

Tiedustelulakipaketin valmistelu: kohti hyväksyttävää lakiesitystä

Suomen ensimmäisessä kyberturvallisuusstrategiassa ei käytetty vielä käsitteitä siviili- ja sotilastiedustelu, ja suojelupoliisiin tehtäviin viitattiin osana poliisitointa. Strategiassa kuitenkin tunnistettiin tarve arvioida vastuuviranomaisten oikeutta hankkia tietoa kyberuhkista ja niiden aiheuttajista, sekä toimivaltuuksien laajentamisen mahdollinen ristiriita perusoikeuksiin kuuluvien yksityisyydensuojan ja luottamuksellisen viestin suojan kanssa (Valtioneuvoston periaatepäätös 24.1.2013, s. 35). Tiedonhankintalakityöryhmäksi kutsuttu puolustusministeriövetoinen viranhaltijatyöryhmä asetettiin 13.12.2013 arvioimaan turvallisuusviranomaisten toimivaltuuksien nykytilaa ja kehittämistarpeita. Puolustusministeriön lisäksi työryhmään kuului jäseniä ja pysyviä asiantuntijoita tasavallan presidentin kansliasta, sisäministeriön, ulkoasianministeriön, valtiovarainministeriön, liikenne- ja viestintäministeriön, työ- ja elinkeinoministeriön ja oikeusministeriön hallinnonaloilta.

Tiedonhankintalakityöryhmä luovutti loppuraporttinsa ”Suomalaisen tiedustelulainsäädännön suuntaviivoja” tammikuussa 2015. Mietinnössä esitettiin, että Suomi tarvitsee säädösperustan tiedustelutoiminnalle kokonaisvaltaisesti, ja että lakimuutokset koskisivat erityisesti suojelupoliisin ja puolustusvoimien toimialueita. Tiedustelua tultaisiin käyttämään pääosin tiedon keräämiseen vakavista kansainvälisistä uhkista ja toiminnan tarkoituksena olisi kansallisen turvallisuuden parantaminen. Keskeisimpiä toimivaltuuksia tulisivat olemaan tietoliikennetiedustelu ja ulkomaantiedustelu. (Tiedonhankintalakityöryhmä 2015.)

Raportti herätti kuitenkin kysymyksiä työryhmän työskentelystä ja lopputuloksesta, sillä Liikenne- ja viestintäministeriön edustaja jätti raporttiin eriävän mielipiteen (Tiedonhankintalakityöryhmä 2015, Liite 3, 109-133) ja Työ- ja elinkeinoministeriön edustaja kyseistä eriävää mielipidettä osin tukevan lausunnon (emt. Liite 4, 135-136). Erimielisyys koski tietoliikennetiedusteluksi nimettyä, ehdotettua uutta toimivaltuutta. Tietoliikennetiedustelu on signaalitiedusteluksi luettavaa toimintaa, joka kohdistuu Suomen rajat ylittävään tietoliikennekaapeleissa kulkevaan tietoliikenteeseen (Tiedonhankintalakityöryhmä 2015, 17). Ajatuksena oli, että tietoliikennetiedustelu kohdistuu sekä viestin välitystietoihin – joiden avulla voidaan saada selville esimerkiksi viestin vastaanottaja, lähettäjä, koko ja lähetysaika – että sisältöön. Liikenne- ja viestintäministeriö totesi lausunnossaan tietoliikennetiedustelun olevan verkkovalvontaa ja rinnastivat sen englanninkieliseen käsitteeseen ”mass surveillance” sekä huomauttivat tiedonhankintalakityöryhmän luopuneen verkkovalvonta-käsitteen käyttämisestä siihen liitettyjen kielteisten mielikuvien takia (Tiedonhankintalakityöryhmä 2015, Liite 3, 114). Heidän mukaansa työryhmä ei ollut kartoittanut riittävällä tavalla vaihtoehtoisia, kohdennetumpia tiedonkeruutapoja, eikä kyennyt osoittamaan tietoliikennetiedustelun tehokkuutta ja vaikutuksia (emt., Liite 3, 116-118). Lausunnon mukaan suunniteltu lainsäädäntö rajoittaa tavallisten ihmisten oikeutta yksityisyyteen tavalla, joka edellyttää perustuslain muuttamista (emt., Liite 3, 124). Lisäksi sen yritysvaikutukset voivat olla kielteisiä erityisesti tele-, tietoturva- ja ICT-yrityksille sekä tehdä Suomesta vähemmän houkuttelevan sijoittumispaikan esimerkiksi palvelinkeskuksille (emt., Liite 3, 121).

Liikenne- ja viestintäministeriön varauksista huolimatta tiedustelulakipaketin valmistelua jatkettiin tiedonhankintalakityöryhmän ehdotuksen mukaisesti toimialakohtaisesti eri hallinnonaloilla jo syksyllä 2015. Puolustusministeriö vastaisi valmistelusta sotilastiedustelulainsäädännön osalta, sisäministeriö siviilitiedustelulainsäädännön osalta ja oikeusministeriö paitsi toiminnan valvonnan, myös perustuslain muutoksen osalta. Kaikki työryhmät kuulivat valmistelun aikana eri alojen asiantuntijoita, mutta niiden varsinainen jäsenistö koostui pääsääntöisesti viranhaltijoista. Viranhaltijoiden lisäksi siviilitiedustelulain valmisteluun osallistui työryhmän pysyvinä asiantuntijoina edustajat Elinkeinoelämän keskusliitosta (EK) ja Suomen asianajajaliitosta (Siviilitiedustelulakityöryhmä ja siviilitiedustelulakityöryhmän sihteeristö 2017). EK:n edustaja osallistui myös sotilastiedustelulain valmisteluun ja ryhmän osaamista täydennettiin lisäksi kansainvälisen oikeudellinen asiantuntijalla Helsingin yliopistosta (Työryhmä Nordstrom H. et al. 2017). Lisäksi perustuslain muutosta valmistelevaan työryhmään kuului useampi oikeudellinen asiantuntija eri ylipistoista (Työryhmä Manninen S. et al. 2016). Valmistelutyön tueksi perustettiin myös parlamentaarinen seurantaryhmä, jonka jäsenistö koostui 12 kansanedustajasta sekä joukosta asiantuntijaviranhaltijoita. Edustettuna oli hallituspuolueiden lisäksi oppositio. (Sisäministeriön tiedote 043/2017.)

Hallituksen esityksen muotoon kirjoitetut työryhmien mietinnöt siviili- ja sotilastiedustelusta sekä niiden valvonnasta julkaistiin huhtikuussa 2017. Samalla esitysluonnoksista pyydettiin kommentteja sidosryhmiltä ja yksityisiltä kansalaisilta verkkoalustan kautta (https://www.lausuntopalvelu.fi/). Lausunnot ovat julkisia ja luettavissa vapaasti verkkoalustalla. Siviilitiedustelua koskevaan mietintöön kirjattiin 65 lausuntoa ja sotilastiedustelua koskevaan mietintöön 72 lausuntoa (Meriniemi & Lohse 2017; Honkanen & Kim 2017). Siviilitiedustelun osalta lausuntojen kommentit kohdistuivat eniten tiedustelun kohteisiin, tietojen luovuttamiseen

rikostorjuntaan, tietoliikennetiedustelun kohdentamiseen, vaikutusarviointiin sekä perustuslakikysymyksiin (Meriniemi & Lohse 2017, 107). Toteutunut mietintö erosi osin tiedonhankintalakityöryhmän mietinnön ja Sipilän II hallituksen hallitusohjelman (VNT 1/2015 vp., 33) tavoitteesta luoda säädösperusta ulkomaantiedustelulle ja tietoliikennetiedustelulle, sillä kevään 2017 mietinnössä esitettiin tietoliikennetiedustelun ja ulkomaantiedustelun lisäksi toimivaltuuksia kotimaassa tapahtuvaan tiedusteluun (Siviilitiedustelulakityöryhmä ja siviilitiedustelulakityöryhmän sihteeristö 2017, 132).

Reilun neljän kuukauden aikana 26.5.–2.10.2017 eli lausuntokierrosten loppupuolelta muutaman seuraavan kuukauden ajan toteuttamamme mediaseuranta osoitti, että mediakeskustelu tiedustelulaeista pohjautui tuolloin pääsääntöisesti annettuihin lausuntoihin ja oli määrällisesti maltillista aina Turun puukotukseksi nimettyyn terrori-iskuun saakka. Arviomme mukaan 18. elokuuta 2017 tapahtunut Turun puukotus kytki tiedustelulakipaketin julkisuudessa entistä selvemmin terrorismin torjuntaan ja lisäsi poliitikkojen painetta perustuslakimuutoksen kiirehtimiselle, sillä tiedustelulait edellyttivät perustuslain muuttamista. Perustuslakia ei voi muuttaa yhdellä vaalikaudella, ellei eduskunta julista sitä kiireelliseksi. Julkinen keskustelu ja lausunnot myös paljastivat, että tiedustelulaeille on ollut tiedonhankintalakityöryhmän erimielisyyksien jälkeen laaja kannatus ja keskustelua on käyty lähinnä sisällön yksityiskohdista sekä siitä, tulisiko perustuslain muutos toteuttaa kiireellisenä. Kriittisimpien arvioiden mukaan perustuslakiin kirjattu yksityisyydensuojan heikentäminen tulisi johtamaan tiedusteluvaltuuksien lisääntymiseen myös pitkällä tähtäimellä, koska ilman perustuslain takaamaa rajoitetta enemmistöhallitus voisi tulevaisuudessa säätää mieleisensä tiedustelulait ilman opposition tukea (Scheinin 2017). Lisäksi kiireelliseksi julistamisesta tulisi samalla ennakkotapaus, mikä voisi madaltaa kynnystä perustuslain muutoksille myös jatkossa.

Hallituksen esitykset luovutettiin eduskunnalle tammikuussa 2018. Vaikka kiireellisyyttä alleviivattiin paljon syksyllä 2017 terrori-iskun jälkimainingeissa, tiedustelulakipaketin valiokuntakäsittelyt ja kysymys perustuslain muutoksesta väistyivät muiden muassa sote-uudistuksen käsittelyn alta syksyyn. Perustuslakivaliokunta totesi lausunnossaan, että estettä kiireelliseksi julistamiselle ei ole, mutta korosti lausunnossaan normaalimenettelyn käyttöä pääsääntönä (PeVM 4/2018 - HE 198/2017 vp). Perustuslain muuttaminen on tarkoituksella säädetty tavallista lakimuutosta hitaammaksi, kahden vaalikauden aikana tapahtuvaksi prosessiksi. Vuonna 2000 voimaan tullutta Suomen perustuslakia (731/1999) oli muutettu vain kolme kertaa[7], eikä kertaakaan kiireelliseksi julistettuna. Kiireellinen menettely edellyttää 5/6 enemmistöpäätöksen – käytännössä opposition tuen – jotta lakiesitys ei jäisi lepäämään vaalikauden ylitse vaan tiedustelulakien sisällöt voitaisiin hyväksyä jo Sipilän II:n hallituksen aikana.

Lokakuun 3. päivä eduskunnan täysistunto julisti perustuslain muutoksen kiireelliseksi äänin 13-178 (PTK 94/2018vp). Perustuslain muutos astui voimaan lokakuun 15. päivänä 2018, ja se sisälsi muutoksen 10 §:n 3 momenttiin ja uusi 4 momentti kirjattiin seuraavalla tavalla:

7 731/1999 Suomen perustuslaki. Muutokset. http://www.finlex.fi/fi/laki/smur/1999/19990731 [Luettu 30.4.2020]

”Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. (5.10.2018/817)

Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. (5.10.2018/817)”

Alkuperäinen säädös kuului seuraavasti:

”Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.” (731/1999)

Keskeinen ero uuden ja vanhan muotoilun välillä on viestin salaisuuden rajoittamisen laajentaminen rikosten tutkinnasta *”tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta”*. Lisäksi alkuperäisen säädöksen 3 momentin alkuosa erotettiin muutoksessa omaksi momentikseen. Perustuslain muutoksen tarve juonsi juurensa Suomen perustuslain aiemmin takaamista laajemmista perusoikeuksista kuin esimerkiksi Euroopan ihmisoikeussopimuksen 8 artikla 2 edellyttää (ETS No. 005). Eurooppalaisessa viitekehyksessä kansallisen turvallisuuden uhka on kirjattu hyväksyttäväksi perusteeksi puuttua esimerkiksi kirjeenvaihtoon. Suomen muutetussa perustuslaissa haluttiin lisäksi määritellä uhka vakavaksi, mitä Euroopan ihmisoikeussopimus ei edellyttänyt.

Perustuslakimuutoksen lisäksi vuoden 2018 loppupuolella ennätettiin hyväksyä myös laki tiedustelutoiminnan valvonnasta, mikä astui voimaan 1. helmikuuta 2019 (121/2019). Siviili- ja sotilastiedustelulait oli tarkoitus käsitellä eduskunnan täysistunnossa helmikuussa 2019, mutta hallintovaliokunta pyysi yllättäen puhemiestä poistamaan ne päiväjärjestyksestä. Lakiesitykset palautettiin takaisin hallinto- ja puolustusvaliokuntaan ja niistä pyydettiin uusi perustuslakivaliokunnan lausunto. (Eduskuntakäsittely HE202/2017 vp; Eduskuntakäsittely HE203/2017 vp.) Eduskunnan puhemies kertoi medialle, että käsittelyn lykkäämisen syynä on tarve varmistaa lakiesitysten perustuslainmukaisuus ja että hallintovaliokunta on tehnyt hallituksen esitykseen perustuslakivaliokunnan lausunnossaan esittämät tarkennukset (Risikko 2019). Julkisuuteen Twitterin kautta ponnahtanut perustuslakiasiantuntijoiden kritiikki koski erityisesti massavalvonnan kieltoa, syrjinnän kieltoa ja hakuehdon määrittelyä[8]. Perustuslakivaliokunta esitti uusissa lausunnoissaan (PeVL

8 Ks. esimerkiksi Juha Lavapuron ja Martin Scheinin ylläpitämä Twitter-tili perustuslakitweet ”Massavalvonnan kielto, syrjinnän kielto ja hakuehdon määrittely kaikki toteutettu tyhjin tautologioin siviilitiedustelulain 1-2 §:ssä (HaVM 30/2018 vp). Kokonaisuus ei saavuta perustuslain mukaista hyväksyttävää tasoa” 7.2.2019.

75/2018 vp - HE 202/2017 vp; PeVL 76/2018 vp - HE 203/2017 vp) erilaista muotoilua syrjintäkiellolle ja tuomioistuimen kokoonpanolle sekä tarkennuksia hakuehtojen määrittelylle ja siviilitiedustelun osalta tekniselle laitetarkkailulle. Muutokset toteutettiin ja eduskunta hyväksyi lait maaliskuussa 2019. Lait astuivat voimaan 1. kesäkuuta 2019. Lisäksi lakeja täydentää useat asetukset. Siviili- ja sotilastiedustelulain valmistelun keskeiset vaiheet esitetään Kuviossa 2.

Kuvio 2 Siviili- ja sotilastiedustelulakien valmistelun keskeiset vaiheet.

Millä edellytyksin tiedustelumenetelmiä saa käyttää?

Tiedustelulainsäädännön valmistelussa yksi keskeinen kysymys oli sen määritteleminen, mihin tarkoituksiin tiedustelua saa käyttää eli toisin sanoen, mitkä ovat ne tilanteet, jotka voivat muodostaa vakavan uhkan kansalliselle turvallisuudelle. Taulukkoon 1 on koottu siviili- ja sotilastiedustelulaeissa määritellyt, mahdolliset tiedustelun kohteet. Suurin osa kohteista on sellaisia, jotka vaarantavat henkeä, terveyttä tai Suomen valtion olemassaoloa joko suoraan tai välillisesti.

Siviilitiedustelun kohteet painottuvat terrorismin, suuren ihmismäärän henkeä ja terveyttä uhkaavien toimintojen sekä vieraiden valtioiden muiden kuin sotilaallisten uhkien torjuntaan. Lisäksi siviilitiedustelun keinoin voi hankkia tietoa valtiollisesta toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille (poliisilaki 5a:3.7; laki tietoliikennetiedustelusta siviilitiedustelussa 3.7 §). Sotilastiedustelu puolestaan keskittyy uhkien kartoittamiseen ja torjumiseen maanpuolustuksellisista näkökulmista, kuten vieraan valtion asevoimien toiminnasta ja sotatarvikkeista. Kohteissa on kuitenkin jonkin verran yhteneväisyyksiä, mutta pääjaon mukaan puolustusvoimat keskittyy tiedusteluun sotilaallisesta näkökulmasta. Molemmat ovat toimivaltaisia hankkimaan tietoja esimerkiksi joukkotuhoaseista sekä toiminnasta, joka vaarantaa yhteiskunnan elintärkeitä toimintoja, kansainvälistä toimintaa sekä kansainvälistä rauhaa ja turvallisuutta uhkaavista kriiseistä ja toiminnasta, joka uhkaa kansainvälisten kriisinhallintaoperaatioiden turvallisuutta.

Taulukko 1 Siviili- ja sotilastiedustelun kohteet

Siviilitiedustelun kohteet	**Sotilastiedustelun kohteet**
1) terrorismi; 2) ulkomainen tiedustelutoiminta; 3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö; 4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö; 5) kansanvaltaista yhteiskuntajärjestystä vakavasti uhkaava toiminta; 6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta; 7) vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille; 8) kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi; 9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta; 10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta vakavasti uhkaava toiminta; 11) kansanvaltaista yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus.	1) vieraan valtion asevoimien ja niihin rinnastuvien järjestäytyneiden joukkojen toiminta ja toiminnan valmistelu; 2) Suomen maanpuolustukseen kohdistuva tiedustelutoiminta; 3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö; 4) vieraan valtion sotatarvikkeiden kehittäminen ja levittäminen; 5) kansainvälistä rauhaa ja turvallisuutta vakavasti uhkaava kriisi; 6) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta vakavasti uhkaava toiminta; 7) Suomen kansainvälisen avun antamisen ja kansainvälisen muun toiminnan turvallisuutta vakavasti uhkaava toiminta. Lisäksi sotilastiedustelun kohteena on vieraan valtion toiminta tai muu sellainen toiminta, joka vakavasti uhkaa Suomen maanpuolustusta tai vaarantaa yhteiskunnan elintärkeitä toimintoja.
Lähde: poliisilaki (872/2011) 5a 3 § ja laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019) 3 §.	Lähde: laki sotilastiedustelusta (590/2019) 4 §.

Sen lisäksi, että toiminta, josta hankitaan tietoa, on määritelty vakavaksi uhkaksi kansalliselle turvallisuudelle, siviilitiedustelumenetelmien käytön yleinen edellytys on, että menetelmän käyttö on *välttämätöntä tärkeiden tietojen saamiseksi* (poliisilaki 5a:4.1; laki tietoliikennetiedustelusta siviilitiedustelussa 4.1 §). Myös sotilastiedustelumenetelmien käytön edellytys on välttämättömyys, mutta tärkeyden sijasta jo oletus tiedon tärkeydestä riittää perusteeksi. Valtiollisten ja niihin rinnastettavien tahojen tiedustelukynnys on matalampi kuin tavallisten ihmisten ja toimivaltansa puitteissa sekä suojelupoliisi että puolustusvoimat voivat hankkia niistä tietoa. Valtiollisia ja niihin rinnastettavia tahoja saa tiedustella, jos kriteeri vakavasta uhkasta kansalliselle turvallisuudelle täyttyy, ja tiedustelumenetelmän käyttö on siviilitiedustelussa *tarpeen tietojen saamiseksi* tai sotilastiedustelussa, *tarpeen tiedustelutehtävän kannalta.* (Poliisilaki 5a:4.3; laki tietoliikennetiedustelusta siviilitiedustelussa 4.2 §; laki sotilastiedustelusta 12.1 §.) Tiedustelumenetelmien käytön yleisiin edellytyksiin kuuluu myös niiden kohdistaminen muualle kuin pysyväisluoteiseen asumiseen käytettävään tilaan sekä tiedustelun keston määräaikaisuus ja käytön lopettaminen, kun tarkoitus on saavutettu tai tiedustelulle ei ole enää edellytyksiä (poliisilaki 5a:4.4; laki sotilastiedustelusta 12.3 §).

Tietoliikennetiedustelu, josta kerrotaan seuraavassa alaluvussa tarkemmin, on määritelty laissa viimesijaiseksi keinoksi. Muiden kuin valtiollisten ja niihin rinnastettavien tahojen tietoliikennetiedustelua koskee rajoitus, että menetelmä on käytettävissä, jos tietoja ei voi hankkia muulla tiedustelumenetelmällä (laki sotilastiedustelusta 70.1 §; laki tietoliikennetiedustelusta siviilitiedustelussa 4.1 §).

Tietoliikennetiedustelu

Eniten julkisuutta saanut osa tiedustelulainsäädännöstä koskee tietoliikennetiedusteluksi kutsuttua tiedustelumenetelmää, jota voi soveltaa sekä siviili- että sotilastiedustelussa. Lain mukaan tietoliikennetiedustelu on *”Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä”* (laki tietoliikennetiedustelusta siviilitiedustelussa 21 §; laki sotilastiedustelusta 10.10 §). Käytännössä tietoliikennetiedustelussa suodatetaan hakuehdot täyttävä, Suomen rajan ylittävä tietoliikenne tarkempaa analyysia varten. Puolustusvoimien tiedustelulaitos toteuttaa suodatuksen sekä sotilas- että siviilitiedustelun tarpeisiin, mutta luovuttaa siviilitiedusteluun tarkoitetun materiaalin suojelupoliisille analysoitavaksi (laki tietoliikennetiedustelusta siviilitiedustelussa 10 §; laki sotilastiedustelusta 73 §). Suodatettua verkkoliikennettä analysoidaan aluksi tietoteknisin keinoin, mutta jos se ei riitä, seulottua liikennettä myös mahdollista käsitellä manuaalisesti, esimerkiksi lukea lähetettyjen viestien sisältöjä tai muita luottamuksellisia tietoja.

Tietoliikennetiedustelua koskee rajoite, joka kieltää yleisen ja kohdentamattoman tietoliikenteen seurannan (laki tietoliikennetiedustelusta siviilitiedustelussa 1.4; laki sotilastiedustelusta 65 §). Kiellon ja laissa esitettyjen muiden rajoitusten tarkoitus on estää massavalvonta. Suomen mallissa tietoliikenteen suodattamisen on perustuttava hakuehtoihin, joita käytetään määritellyssä osassa verkkoa. Hakuehto saa kuvata viestin sisältöä vain silloin, jos kyse on haittaohjelman koodista tai vieraan valtion tai siihen rinnastettavan tahon tietoliikenteestä.

Hakuehto ei voi olla myöskään Suomessa sijaitseva telepäätelaite. (Laki tietoliikennetiedustelusta siviilitiedustelussa 5 §; 7 §; laki sotilastiedustelusta 68–71 §). Tiedustelumenetelmästä riippumatta viranomaiset ovat velvollisia hävittämään kerätyn materiaalin, jonka kerääminen ei ole ollut sallittua (poliisilaki 5a:45; laki tietoliikennetiedustelusta siviilitiedustelussa 12 §; 15 §; laki sotilastiedustelusta 82 §; 86 §). Esimerkiksi, jos tietoliikennetiedustelun viestinnän molemmat osapuolet ovat fyysisesti Suomessa, kyse ei ole lain tarkoittamasta rajan ylittävästä viestinnästä, vaikka tietoliikenne olisikin reitittynyt toisten valtioiden kautta. Lisäksi pääsääntö on, että jos kerätty siviilitiedustelutieto osoittautuu tarpeettomaksi kansallisen turvallisuuden suojaamisessa, se pitää hävittää, ellei kyse ole tiedosta, joka pitää tai sen saa luovuttaa rikostorjuntaan keskusrikospoliisille tai toimivaltaiselle viranomaiselle (poliisilaki 5a:45; laki tietoliikennetiedustelusta siviilitiedustelussa 15 §). Ilmoitusvelvollisuus on esimerkiksi rikoksista, joiden maksimirangaistus on vähintään kuusi vuotta vankeutta. Lisäksi tietoa saa luovuttaa esimerkiksi rikoksen estämiseksi, jos teosta määritetty ankarin rangaistus on kaksi vuotta vankeutta tai enemmän. (Poliisilaki 5a:44; laki tietoliikennetiedustelusta siviilitiedustelussa 17 §.) Myös sotilastiedusteluviranomaisilla on samankaltaisia velvollisuuksia ja lievemmissä tapauksissa harkintavaltaa ilmoittaa tiedustelun aikana ilmenneistä, rikoksia koskevista tiedoista toimivaltaiselle viranomaiselle (laki sotilastiedustelusta 79–80 §).

Tietoliikennetiedustelu edellyttää lupaa tuomioistuimelta, mikä on hankittava ensisijaisesti etukäteen, mutta viimeistään vuorokauden kuluessa menetelmän käytön aloittamisesta. Lupahakemuksesta ja annetun ratkaisussa perustellaan esimerkiksi, miksi tietoliikennetiedustelua tarvitaan sekä määritetään toiminnan ajankohta ja verkon osa, johon se kohdistetaan. Lisäksi asetetaan ja perustellaan hakuehdot tai hakuehtojen luokat, millä suodatus tapahtuu. Tietoliikennetiedustelun kohteelle on pääsääntöisesti ilmoitettava jälkikäteen tiedustelusta, jos luottamuksellista viestintää on tarkasteltu manuaalisesti. Velvollisuus ei koske koneellista tarkastelua. Tuomioistuin voi päättää ilmoittamisen lykkäämisestä korkeintaan kahdeksi vuodeksi kerrallaan tai kokonaan ilmoittamatta jättämisestä, jos perusteet ovat riittävän vahvat. Esimerkiksi tilanteissa, joissa ilmoittaminen vaarantaisi hengen tai terveyden tai se katsottaisiin välttämättömäksi kansallisen turvallisuuden varmistamiseksi, ilmoitus voidaan jättää tekemättä. (Laki tietoliikennetiedustelusta siviilitiedustelussa 7-9 §; 20 §; laki sotilastiedustelusta 89 §.) Sen sijaan kerätystä tiedosta, joka on hävitetty tai kerätty valtiolliselta taholta, ei ilmoiteta (laki tietoliikennetiedustelusta siviilitiedustelussa 20 §; poliisilaki 5a:47.7; laki sotilastiedustelusta 89 §).

VINKKI! JOS KIINNOSTUIT AIHEPIIRISTÄ, LISÄTIETOJA LÖYDÄT ESIMERKIKSI OHEISISTA TEOKSISTA, LAEISTA SEKÄ VERKKOSIVUILTA.

Ajantasaiseen lainsäädäntöön voit tutustua osoitteessa finlex.fi.

Tässä luvussa käytetyt oikeudelliset lähteet ovat:

Laki sotilastiedustelusta (590/2019)

Laki tiedustelutoiminnan valvonnasta (121/2019)

Laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019)

Poliisilaki (872/2011)

Muuta lukemistoa:

Lohse, Mikael, Honkanen, Kosti & Meriniemi, Marko (2019). Tiedustelumenetelmät. Alma Talent: Helsinki

Lohse, Mikael & Viitanen, Marko (2019). Johdatus tiedusteluun. Alma Talent: Helsinki.

Kuvitteellisia esimerkkejä tiedustelulainsäädännön soveltamisesta. Sisäministeriön verkkosivu. https://intermin.fi/tiedustelu/esimerkkeja-lain-tarpeesta

Siviilitiedustelulainsäädäntö – kysymyksiä ja vastauksia. Sisäministeriön verkkosivu. https://intermin.fi/tiedustelu/usein-kysytyt-kysymykset

Tiedustelusta suojelupoliisin verkkosivulla: https://supo.fi/

Tutustu tiedusteluvalvontavaltuutetun toimintaan ja vuosikertomuksiin: https://tiedusteluvalvonta.fi

6 TUTKIMUKSEN AINEISTOT JA TOTEUTUS

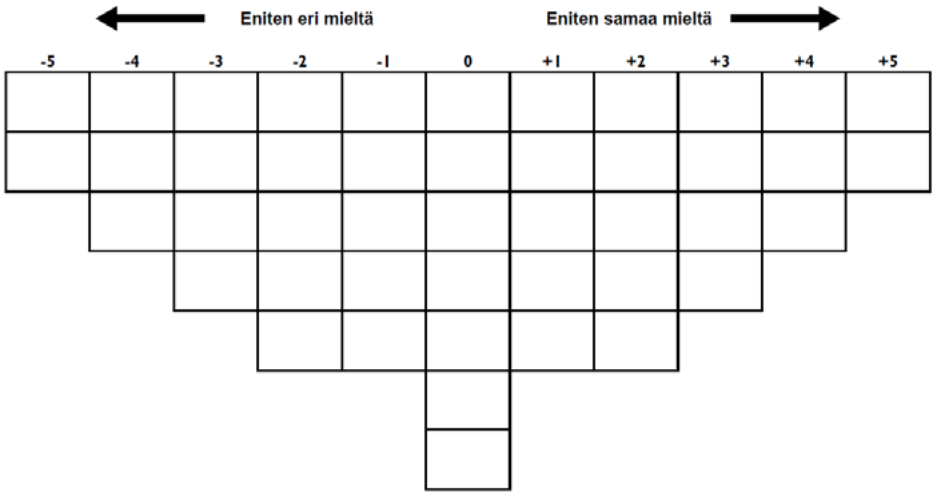
Tämä raportti on syntynyt osana kansainvälistä tutkimusprojektia, jonka keskeinen tavoite oli tuottaa vertailukelpoista tietoa sidosryhmien ja kansalaisten näkemyksistä lainvalvonta- ja tiedusteluviranomaisten toimivaltuuksista kerätä, säilyttää ja analysoida tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista saatavaa tietoa kolmessa maassa, Suomessa, Britanniassa ja Norjassa. Esittelemämme tulokset perustuvat Suomessa kerättyyn kolmeen aineistoon, joita olivat 1) sidosryhmille kohdistetut asiantuntijahaastattelut (n=25) sekä yliopiston opiskelijoille ja henkilökunnalle suunnatut 2) kysely (n=236) ja 3) haastattelut (n=20). Kuvaamme seuraavaksi aineistonkeruun ja tutkimuksen toteuttamisen. Aineistonkeruuvälineet luotiin yhdessä projektitiimin kesken ja kansalliset tutkimustiimit toteuttivat maakohtaiset haastattelut sekä aineistojen analyysin.

6.1 Asiantuntijahaastattelut

Aineistonkeruun suunnittelusta ja koordinoinnista projektiryhmän sisällä vastasivat Poliisiammattikorkeakoulun tutkija Anna Leppänen ja erikoistutkija Jarmo Houtsonen. Aineistonkeruu toteutettiin Q-metodologian mukaisina haastatteluina, joissa vastaajat lajittelevat väitelausekortteja normaalijakaumaa muistuttavalle ruudukolle ja perustelevat tekemänsä järjestyksen (Watts ja Stenner 2012). Haastattelussa esitetyt väitelauseet poimittiin ajankohtaisesta, lainvalvonta- ja tiedusteluviranomaisten tiedonhankintaa verkossa käsittelevästä julkisesta keskustelusta, kuten lainvalmisteluasiakirjoista, raporteista, lehtiartikkeleista ja sosiaalisesta mediasta Suomessa, Norjassa ja Britanniassa. Aihepiiriä koskevia ajatuksia ja väitelauseita kerättiin otosta varten Suomessa noin 700 Britanniassa yli 1300 ja Norjassa lähes 300. Maakohtaiset väitelauseet luokiteltiin teemoittain, jolloin päällekkäiset väitteet voitiin yhdistää ja väitteiden määrää vähentää, mutta silti kattaa kyseisen maan viranomaisvalvontaa koskeva julkinen keskustelu. Kansainvälinen projektiryhmämme työsti supistetuista väitelauseotoksista useamman välivaiheen kautta yhteisen, 45 väitelausetta sisältävän joukon, joka kuvasi mahdollisimman kattavasti julkisen keskustelun eri näkökulmia näissä kolmessa eri maassa.

Haastatteluja suoritettiin Suomessa ja Norjassa molemmissa 25 sekä Britanniassa 24. Suomen osalta haastattelut toteutettiin vuonna 2018 kesä-syyskuussa. Kasvotusten tehdyt väitekorttien luokittelut ja haastattelut kestivät kokonaisuudessaan noin 1,5 tuntia per osallistuja. Tapaamisen aluksi haastateltava vahvisti suostumuksensa osallistua tutkimukseen allekirjoittamalla suostumuslomakkeen ja hänelle varattiin mahdollisuus esittää lisäkysymyksiä tutkimuksesta. Tutkimusta koskevat tiedot oli lähetetty vastaajille myös sähköpostiin jo aiemmin. Lyhyen taustatietolomakkeen täyttämisen jälkeen alkoi kaksivaiheinen Q-haastattelu. Haastatelluille annettu ohjeistus on esitetty liitteessä 1 ja väitelauseet liitteessä 2. Q-haastattelussa vastaaja järjesti 45 verkossa tapahtuvaan viranomaisvalvontaan liittyvää väitelausekorttia lajitteluruudukolle (Kuvio 3) sen perusteella, missä määrin hän oli samaa tai eri mieltä niiden kanssa. Lajittelussa osallistuja antaa kullekin väitelauseelle arvon -5 ja + 5 välillä ja kuhunkin ruutuun voi sijoittaa vain yhden kortin. Ääripäihin, eli jyrkimpiä mielipiteitä kuvastaviin

laitoihin pystyy sijoittamaan vähiten kortteja, kun taas keskiosaan niitä mahtuu eniten. Perinteinen Q-metodologinen lajitteluprosessi (esim. Watts ja Stenner 2012) alkaa lukemalla väitelausekortit läpi ja sijoittamalla ne oman mielipiteen mukaisesti kolmeen pinoon: samaa mieltä, eri mieltä ja neutraali. Neutraalin mielipiteen lisäksi kyseiseen pinoon sijoitetaan myös kortit, jotka herättävät ristiriitaisia tunteita tai joiden osalta vastaaja on epävarma mielipiteestään. Sen jälkeen vastaaja lajittelee kunkin pinon yksitellen ruudukolle noudattaen prosessia, jossa hän vertaa pinon kortteja toisiinsa ja valitsee jäljellä olevien joukosta aina sen, jonka kanssa on eniten samaa mieltä (eri mieltä -pinon osalta eniten eri mieltä). Neutraali pino lajitellaan viimeiseksi. Lajittelu etenee näin ruudukon ääripäistä kohti keskustaa ja ruudukolle sijoitettujen korttien paikka on vaihdettavissa, kunnes osallistuja on tyytyväinen tekemäänsä järjestykseen. Korttien asettelun jälkeen vastaajamme selostivat ääninauhalle keskeiset kohdat rakentamastaan järjestyksestä sekä kuvailivat väitelauseiden ohjaamina ajatuksiaan viranomaisvalvonnasta verkossa. Vastaajien täyttämät taustatietolomakkeet, tallennetut väitelausekorttien järjestykset ja tekstimuotoon puretut ääninauhat muodostavat asiantuntijahaastattelujen aineiston. Haastattelut litteroitiin eli kirjoitettiin tekstimuotoon ja niistä poistettiin henkilöön viittaavat tunnistetiedot. Haastateltavien tunnistamattomuuden varmistamiseksi taustatiedoista säilytettiin vain pieni osa.



Kuvio 3 Q-haastattelun lajitteluruudukko, jolle vastaajat asettelivat 45 väitelausetta.

Vaihtoehtoinen kuvateksti: Lajitteluruudukko muistuttaa ulkonäöltään ylösalaisin käännettyä pyramidia, joka koostuu yhdestätoista sarakkeesta. Pyramidin pohjassa eli lajitteluruudukon yläreunassa kullekin sarakkeelle on annettu arvo. Arvot ovat vasemmalta oikealle -5, -4, -3, -2, -1, 0, + 1, +2, +3, +4, +5. Sarakkeisiin -5 ja +5 mahtuu kumpaankin kaksi väitelausekorttia. Korttipaikkojen määrä kasvaa pääsääntöisesti yhdellä pyramidin keskustaan päin. Sarakkeeseen 0 mahtuu eniten kortteja, seitsemän.

Haastateltaviksi valittiin henkilöitä, jotka olivat osallistuneet tai vaikuttaneet keskusteluun lainvalvonta- ja tiedusteluviranomaisten toimivaltuuksista verkossa. Osallistuminen ja vaikuttaminen määriteltiin esimerkiksi annettujen lausuntojen, blogikirjoittelun, työryhmäjäsenyyksien, mediahaastattelujen tai henkilön edustaman organisaation perusteella. Käytännössä suurin osa Suomen haastateltavista oli ollut aktiivisia tiedustelulakipaketin valmistelussa tai kommentoinnissa. Tavoitteena oli, että erilaisten näkemysten kirjo oli mahdollisimman hyvin edustettuna. Tämän vuoksi kutsuimme haastateltavaksi erilaisia vastaajia seuraavissa kategorioissa: kansalaisjärjestöt, yksityinen sektori, poliitikot, viranomaiset, tutkijat, media, aktiiviset kansalaiset sekä kategoria muut, joka koostui henkilöistä, jotka eivät kuuluneet edellisiin kategorioihin. Tutkimuksen vastaanotto oli hyvä, sillä kohtasimme vain yksittäisiä, yleensä hyvin perusteltuja, kieltäytymisiä. Arviomme mukaan keräämämme aineisto kuvastaa hyvin suomalaisten sidosryhmäasiantuntijoiden ajatuksia viranomaisten toimivaltuuksista verkossa, erityisesti tiedustelulakipaketin näkökulmasta.

Q-haastattelujen tulkinta

Q-haastattelujen tulkinta on kaksivaiheinen. Ensiksi suoritetaan tilastollinen Q-faktorianalyysi, jonka perusteella osallistujat, jotka ovat lajitelleet väitelauseet keskenään samankaltaisesti, sijoittuvat samoille faktoreille eli muodostavat jaetun näkökulman (Watts ja Stenner 2012). Näkökulmien tulkinnassa hyödynnetään väitelauseiden sisältöä ja sijaintia ruudukolla sekä osallistujien vapaamuotoista, äänitettyä kerrontaa tekemästään lajittelusta.

Tämän tutkimusaineiston osalta tilastollisesta analyysista kerrotaan yksityiskohtaisesti tieteellisessä artikkelissa Leppänen ja Houtsonen (Hyväksytty julkaistavaksi), jossa on julkaistu myös tilastollisen analyysin alkuperäiset tulokset. Tässä raportissa ei mennä syvemmälle tilastolliseen analyysiin, koska esitämme ainoastaan tiivistelmän aiemmin julkaisemistamme tuloksista. Sen sijaan keskitymme syventämään aiempia löydöksiämme esittämällä sitaatteja haastatteluista sekä kuvaamalla tiedustelulakipaketin valmisteluun osallistuneiden henkilöiden ajatuksia valmisteluprosessista, mitkä kumpikin ovat aiemmin julkaisematonta analyysia.

6.2 Yliopisto-opiskelijoiden ja henkilökunnan verkkokysely

Tutkimushankkeen aikana toteutettiin verkkokysely, jossa kartoitettiin suomalaisten, norjalaisten ja brittiläisten yliopistojen opiskelijoiden ja henkilökunnan näkemyksiä omasta verkkokäyttäytymisestään sekä valtion viranomaisten toimivaltuuksista kerätä, säilyttää ja analysoida verkkoviestintää ja -liikennettä. Aineistonkeruun toteutti skotlantilaisen Dundeen yliopiston tutkimusryhmä, jossa siitä vastasivat tutkija Amy Humphrey ja yliopistonlehtori Jonathan Mendel. Muut partnerit antoivat palautetta ja korjausehdotuksia kyselylomakkeen eri versioihin. Lisäksi projektikumppanit sekä useampi testivastaaja kustakin maasta täytti kyselyn sekä kommentoi sitä ennen kuin lomake saavutti lopullisen muotonsa. Myös vaihto-opiskelijat ja kansainvälinen henkilökunta olivat tervetulleita vastaamaan. Kyselyn suuntaaminen yliopistoihin perustui käytännölliseen harkintaan siitä, että näin eri maista saataisiin riittävästi vertailukelpoisia vastaajia kyselyyn. Vastaaminen tapahtui SoSci Survey -verkkolomakkeen kautta englanniksi ja vastaaja valitsi itse, koskivatko hänen antamansa

vastaukset Suomea, Norjaa vai Britanniaa. Kyselyä levitettiin Suomessa useiden yliopistojen intranetissä sekä opiskelijajärjestöjen kanavien kautta ajanjaksolla joulukuu 2018 - toukokuu 2019. Vastaajat saivat halutessaan ilmoittaa yhteystietonsa 50 € arvoisen lahjakortin arvontaan.

Suomalaisista yliopistoista kertyi 236 vastaajaa. Määrä on suurempi kuin Britanniassa ja Norjassa, mutta silti erittäin pieni, joten kysely tavoitti kohderyhmänsä heikosti. Kerätyn aineiston perusteella ei ole mahdollista tehdä tilastollisia yleistyksiä kaikkiin suomalaisten yliopistojen opiskelijoihin ja henkilökuntaan.

6.3 Yliopisto-opiskelijoiden ja henkilökunnan haastattelut

Yliopisto-opiskelijoiden ja henkilökunnan näkemyksiä viranomaisten toimivaltuuksista verkossa täydennettiin teemahaastattelujen avulla. Niihin osallistui yhteensä 20 suomalaisissa yliopistoissa opiskelevaa tai työskentelevää henkilöä eri puolilta Suomea. Osa haastattelun osallistujista päätyi vastaajiksi projektin kyselytutkimuksen kautta ja muita kohderyhmään kuuluvia henkilöitä etsittiin yliopistojen intranet-sivuilla olleiden ilmoitusten, opiskelijajärjestöjen ja tutkijaprofiilien kautta sekä kyselemällä muilta kontakteilta henkilöitä, joilla voisi olla mielipide aiheesta. Kyselyn ja haastattelun vastauksia ei yhdistetä toisiinsa.

Puolistrukturoidun teemahaastattelurungon laatimisprosessista vastasivat Dundeen yliopiston tutkijat Amy Humphrey ja yliopistonlehtori Jonathan Mendel. Haastattelurunko saavutti lopullisen muotonsa projektiryhmän ja testivastaajien kommenttien jälkeen. Haastattelurungon kysymykset liittyivät kuuteen teemaan: 1) lämmittelykysymykset, 2) tietämyksesi verkkojen valvonnasta Suomessa, 3) asenteet valvontaa ja yksityisyyttä kohtaan, 4) vastuullisuus ja luottamus ja 5) näkemysten, asenteiden ja käyttäytymisen vuorovaikutus. Lisäksi Suomessa toteutetuissa haastatteluissa kysyttiin täällä ajankohtaisesta aiheesta, tiedustelulakipaketista. Pyrimme välttämään haastatteluissa asiantuntijakieltä ja esimerkiksi lainsäädännöstä sekä lainvalmistelumateriaaleista tuttuja erikoistermejä, kuten kansallinen turvallisuus, tietoliikennetiedustelu, salaiset pakkokeinot tai verkkovalvonta. Pilottihaastattelut olivat osoittaneet, että vastaajat todennäköisesti eivät tunne erityissanastoa. Sen sijaan puhuimme esimerkiksi poliisin ja tiedusteluviranomaisten harjoittamasta tiedonkeruusta ja valvonnasta verkossa, tieto- ja viestiliikenteen tarkkailusta tai valvonnasta, sekä tavoista, joilla poliisi ja tiedusteluviranomaiset keräävät, analysoivat ja säilövät netistä ja nettiin kytketyistä laitteista saatavaa tietoa.

Haastattelut olivat kahdenkeskisiä ja ne toteutettiin pääasiassa puhelimitse tai Skype for Business -sovelluksen kautta, mutta haastateltavan oli halutessaan mahdollista myös tavata tutkija Tampereella. Haastattelujen kesto vaihteli 33 minuutista 66 minuuttiin ja ne toteutettiin kesäkuun 2019 ja tammikuun 2020 välisenä aikana. Suomea koskevien haastattelujen kieli oli pääosin suomi. Tietojen keruu perustui vastaajalta suullisesti nauhoituksen aikana kysyttyyn suostumukseen. Vastaajat olivat saaneet perustiedot tutkimuksesta kirjallisesti ennen haastattelua, ja heille varattiin aikaa esittää mahdollisia lisäkysymyksiä haastattelun aluksi. Varsinaisten haastattelukysymysten lisäksi vastaajilta kysyttiin myös muutamia taustatietoja ja pyydettiin lupa aineiston arkistointiin. Vain yksi kieltäytyi aineiston arkistoinnista. Haastattelut äänitettiin, jonka jälkeen ne litteroitiin eli kirjoitettiin tekstimuotoon ja tekstistä poistettiin vastaajaan viittaavat tunnistetiedot. Ääninauhoite ja vastaajien yhteystiedot tuhottiin tunnisteiden poiston ohessa.

Osallistujilta varmistettiin etukäteen, ettei heillä ole erityisasiantuntemusta poliisin ja tiedusteluviranomaisten toimivaltuuksista verkossa. Erityisasiantuntemukseksi olisi laskettu esimerkiksi työskentely turvallisuusviranomaisissa tai merkittävä rooli tiedustelulainsäädännön valmistelussa. Rajausta arvioitiin myös sen perusteella, olisiko henkilö voinut tulla erityisasiantuntijuutensa perusteella haastatelluksi sidosryhmäasiantuntijoiden kategoriassa. Kiinnostusta aihepiiriä kohtaan ei määritelty eritysasiantuntemukseksi. Tietämysvaatimusta toiseen suuntaan ei ollut, joten haastateltavilta ei edellytetty mitään etukäteistietoa haastattelun aihepiiristä.

7 ASIANTUNTIJOIDEN NÄKEMYKSIÄ VIRANOMAISTEN TOIMIVALTUUKSISTA VERKOSSA

7.1 Kokemuksia tiedustelulakipaketin viranomais-valmistelusta

Monet haastatteluun osallistuneet asiantuntijat ja sidosryhmien edustajat tunsivat tiedustelulakipaketin vaiheet hyvin ja halusivat kuvailla lainvalmistelun kompastuskiviä sekä toisaalta onnistumisia omasta näkökulmastaan. Esimerkiksi lainsäädäntövalmistelun aloittaneen ensimmäisen virkamiestyöryhmän työtä pidettiin monin paikoin suljetun piirin toimintana, jossa viestintä epäonnistui. Julkisen keskustelun koettiin jumittuneet erityisesti massavalvonnan ja salausten purkuavainten ympärille sekä saaneen välillä kohtuuttomalta tuntuneita piirteitä. Massavalvonnan pelko tuli hyvin esille esimerkiksi Liikenne- ja viestintäministeriön lausunnossa, jossa tietoliikennetiedustelua kritisoitiin massavalvonnaksi (Tiedonhankintalakityöryhmä 2015, Liite 3). Lisäksi valmistelun jatkon reunaehdoksi asetettiin, ettei lainsäädäntöhankkeen puitteissa vaadita yrityksiltä salausavaimia tai takaporttien asentamista (Siviilitiedustelulakityöryhmä ja siviilitiedustelulakityöryhmän sihteeristö 2017, 9). Mutta prosessin edetessä tyytyväisyys lainvalmistelua kohti kasvoi.

Osallistuja V14 pohtii, että keskustelu lähti alussa väärille raiteille ja jumittui hedelmättömäksi vastakkainasetteluksi. Hän arvioi eräänä syynä olleen sen, ettei keskustelua saatu sovitettua Suomen oloihin sopivaksi. Tilannetta lähestyttiin liiaksi ulkomaisten keskustelujen kautta.

> *”Siinä oli tahtotila, joka oli haettu vieraista maista, mutta siellä ei ollut sitten ehkä puolustusministeriössä eikä suojelupoliisissakaan mun mielestä riittävää kompetenssia siihen asiaan, että he olisivat osanneet nostaa ne oikeat terät, nostaa ne oikeat arvopunninnat siihen keskusteluun riittävän aikaisessa vaiheessa, jotta oltaisi päästy pois siitä juupas-eipäs -keskustelusta.” (V14)*

Haastateltu V16 ajattelee, ettei sidosryhmiä otettu riittävästi mukaan lainvalmisteluun. Tiedotuksessa olleet puutteet johtivat jälkikäteen arvioituna aiheettomien pelkojen kehittymiseen.

> *”Tämä on aika paljon viestinnästä kiinni ja jos ajatellaan tiedustelulakien määrittelyä, niin siinä alkuvaiheessa tätä tehtiin eräällä tavalla termospullossa, jonka takia siellä sitten pääsi tällaiset vähän niin kuin epäilykset ja asiat, joille ei ehkä ollut edes perustettakaan leviämään, koska ei kerrottu avoimesti, että minkälaisia asioita tehdään ja miten. […] Mediassahan oli paljon, niin kuin elinkeinoelämässäkin, epäilyksiä ja epäluottamusta, kun sitä ei suostuttu tai osattu kertoa. Tämä salausavainkeskustelu on esimerkiksi sellainen, joka kesti liian pitkään se, että siellä todettiin, että hei tässä täytyy tehdä tämän suuntainen liike. Se asia velloi liian kauan ja valitettavasti velloo edelleen.” (V16)*

Myös osallistuja V3 tunnistaa alun tulehtuneen julkisen keskustelun ja tiedotusvälineissä levinneet väärinkäsitykset. Hän kuvasi oloaan lehtikeskustelun edessä voimattomaksi: *"--sulle tulee sellainen olo, että miten tuohon voi puuttua ja miksi ei kukaan tuohon puuttunut -- et sä voi mennä itse lehteen ja sanoa, että tämä on muuten valhe, vaan se että miten se korjataan. Ja sitten siihen kuitenkin pitäisi reagoida nopeasti, koska muuten se valhe jää elämään." (V3)* Mutta vaikeanakin koetut tilanteet ratkesivat hänen mukaansa avoimuudella. *"Periaatteessa väitteiltä on katkennut kärki pikkuhiljaa, kun on menty eteenpäin ja tiedotettu ihmisille ja pidetty tiedotustilaisuuksia, kerrottu missä mennään. Faktoilla, ei siinä mikään muu auta kuin faktat." (V3)*

Siviilitiedustelulainsäädännön edellyttämä perustuslain muutos koettiin haastavaksi. Vuodelta 1999 oleva Suomen perustuslain yksityiselämän suojaa koskeva pykälä 10 oli varsin yksiselitteinen sen osalta, että kirjeen, puhelun tai muun luottamuksellisen viestin salaisuus on loukkaamaton. Yksityiselämän suojan rajoittaminen oli määritelty rikosperusteiseksi, kun taas tiedustelulakipaketin lähtökohta oli tiedon kerääminen vakavista kansallisen turvallisuuden uhkista. Lisäksi vastaajia askarrutti kysymys, tulisiko perustuslain muutos käsitellä kiireellisenä, jolloin tiedustelulait olisi mahdollista hyväksyä ennen kevään 2019 eduskuntavaaleja.

Osallistuja V3 kokee, että kansallinen turvallisuus olisi pitänyt kirjata perustuslakiin perusteeksi puuttua luottamukselliseen viestintään jo alun perin. Kansallinen turvallisuus on hänen mukaansa Euroopassa tyypillinen peruste, jolla rajoitetaan kirjesalaisuutta.

> *"Ongelmahan on se, että pl 10 perustuslakihan tehtiin silloin syvän rauhan aikana vuonna 2000, kun Neuvostoliitto oli luhistunut ja Venäjä demokratisoitui kovaa vauhtia jolloin siihen pl 10 ei tajuttu ottaa luottamuksellisen viestin puuttumiseen perusteeksi kansallista turvallisuutta, vaan siinä on tietyn kynnyksen ylittävät rikokset. […] Normaalisti eurooppalaisessa valtiossa myöskin kansallinen turvallisuus on peruste puuttua luottamuksellisen viestin suojaan, meillä ei sitä ajateltu. En tiedä miksi sitä ei ajateltu, mutta tavallaan siinä on valuvika meidän perustuslaissa tältä osin." (V3)*

Haastateltu V12 pohtii, että perusteet julistaa perustuslain muutos kiireelliseksi murenee, kun aikaa kuluu ja asialistalle tulee myös muita laajoja säädöshankkeita.

> *"Alkuvuodesta yksi tämän perustuslain kiireelliseksi julistamisen puolesta puhuva seikka oli se, että nyt tämä pitää saada nopeasti voimaan, koska Suomen kansallinen turvallisuus on tärkeä ja se pitää priorisoida, mutta sitten maakunta-sote meni edelle. Se on herättänyt aika paljon vasta-argumentteja, että onko tämä nyt kuitenkaan niin kiireellinen tämä perustuslain tarkistaminen. Mitä enemmän aikaa menee, niin sitä vähemmän perusteltua on julistaa se perustuslain tarkistamista koskeva hallituksen esitys kiireellisenä käsiteltäväksi." (V12)*

Haastateltu V21 puolestaan näkee perustuslain muutoksen ennakkotapauksena, joten kiireelliseksi julistaminen mietityttää häntä.

”Moneen asiaan kiinnitetty huomiota, muun muassa se kiireellisyys. Tässä on kysymys ensimmäisestä - perusoikeusuudistuksen jälkeen - ensimmäisestä merkittävästä heikennyksestä meidän perusoikeussuojaan ja sitä ei voi tehdä kovin kevein perustein. Sekin on oma ennakkotapauksensa, että lähdetään madaltamaan sitä suojan tasoa.” (V21)

Osallistuja V25 ei ymmärrä, miksi siviili- ja sotilastiedustelulait pitää saada voimaan yhtä aikaa. Hänen mukaansa sotilastiedustelusta olisi ollut helpompi säätää ensin ja siviilitiedustelulaki olisi voinut seurata perässä. Nyt asiasta kasvoi liian iso politisoitunut kysymys, kun siviilitiedustelulaki edellyttää perustuslain muuttamista kiireellisenä.

”Jos itseltäni olisi kysytty alun perin, miten se asia pitää hoitaa, niin olisin hoitanut sen toisin päin. Eli olisin lähtenyt tekemään sitä siitä, että olisin rakentanut ensiksi sotilastiedustelun, joka olisi ollut mahdollinen nykyisen puitteissa ainakin jossakin määrin. Nyt kun se on niin kuin peruutettu se asia niin päin, että ensin perustuslain muutos ja sitten vasta kaikki muu. En pidä tätä järjestystä lähtökohtaisesti ollenkaan hyvänä. Tämä on huono järjestys, joka aiheuttaa juuri politisoitumisen ja muun ongelman.” (V25)

Toisaalta tiedustelulainsäädännön rakentaminen nähtiin myös oppimisprosessina, jossa haasteista selvittiin avoimuutta ja dialogia lisäämällä. Lopputuotteena syntyneet lait olivat usean asiantuntijan mukaan laadukkaat. Myös monet sellaiset tahot, jotka kritisoivat prosessin alkuvaihetta, olivat valmistelun jälkimmäiseen osaan ja lakiehdotusten sisältöön pääpiirteittäin tyytyväisiä. Lainsäädäntöä koskeva kritiikki koski enemmän yksityiskohtia ja muotoiluja kuin suurempia kokonaisuuksia tai periaatteita.

Osallistuja V24 on tiedustelulakipaketin luonnokseen melko tyytyväinen, mutta toivoisi siihen vielä joitakin muutoksia. Hän antaa kuitenkin tunnustusta prosessin loppuvaiheelle ja toivoo, että prosessista on opittu.

”Tämä uusin esitys on hyvin erilainen kuin ne esitykset, joita tässä on matkanvarrella esitetty. Siltä osin minä ajattelen, että tämä on ollut iso oppimisprosessi varmaan kaikille suomalaisille turvallisuuden piirissä toimiville tahoille, mutta myöskin niille henkilöille, jotka hanakasti käy turvallisuuspoliittista keskustelua, niin myöskin politiikan puolella. Siltä osin asiat ei ole aina niin yksinkertaisia kuin ne saadaan vaan näyttämään. [...] On selvää, että se [lakiesitys] on enemmän tasapainossa kuin koskaan aiemmin, mutta meillä on siinä epäilyksiä, joita haluamme tässä valmisteluvaiheessa tehdä, jotta viestinnän luottamuksellisuuden suojaa voidaan murentaa joskus, kun turvallisuusarvomme ovat uhattuna, suhteessa siihen, että yksityisyys voi estyä.” (V24)

Osallistuja V6 ajattelee, että tiedustelulakipaketin valmistelu on ollut viime aikoina avointa ja pitää parlamentaarisen seurantaryhmän kokouksia hyvänä foorumina tuoda tietoa suoraan kansanedustajille.

”Mun mielestä [tiedustelulakipaketin valmistelussa] on oltu niin avoimia kuin mahdollista. Kyllä väittäisin, että monessa muussa hankkeessa

jotka vaikuttaa ehkä enemmän siihen tavallisen kadunmiehen- tai naisen elämään, ollaan paljon vähemmän tiedotettu ja suhmuroidaan enemmän. […] Valmisteluvaiheessa on parhaimmillaan varmaan viikoittainkin parlamentaarisen seurantaryhmän kokouksia. Ennen sitä tai sen aikana on infotilaisuuksia eri eduskuntapuolueille ja sitten on ollut erilaisia kuulemistilaisuuksia esimerkiksi elinkeinoelämän edustajille ja kansalaisjärjestöille." (V6)

Haastateltu V10 kutsuu parlamentaarista seurantaryhmää Suomen oloissa poikkeukselliseksi ja kokee, että poliitikot ovat saaneet riittävästi tietoa.

"Tässähän tuli hyvinkin laaja parlamentaarinen työ taustalla ja voi sanoa, ettei ole ikinä missään lainsäädännössä koskaan valtioneuvostossa ollut niin laajaa tällaista valmistelua, jossa on ollut mukana sekä oppositio että hallituspuolueita. Joiden on sitten oletettu ja kannustettu ja myöskin pyydetty välittämään tietoa eteenpäin omissa viiteryhmissään. Ja heille (poliitikoille) on annettu kyllä niin paljon tietoa kuin vain suinkin ikinä on mahdollista." (V10)

Osallistuja V21 antaa tunnustusta suojelupoliisin viranhaltijoille perus- ja ihmisoikeuskysymyksissä ja kokee, ettei nykytilassa ole syntynyt varsinaista vastakkainasettelua, vaan viranhaltijat ovat tietoisia perus- ja ihmisoikeuksien asettamista raameista.

"Mä olen toisaalta huomannut, että suojelupoliisin virkamiehet on itse asiassa perus- ja ihmisoikeuksista hyvin kartalla. Että ne ei tavallaan edusta ikään kuin toista vastapoolia." (V21)

Osallistuja V14 on suhteellisen tyytyväinen lakiluonnosten sisältöön, vaikka prosessin alkuvaiheet eivät sujuneet optimaalisella tavalla.

"Mun mielestä tässä ollaan kuitenkin päästy siihen pisteeseen, että me sääntely on sääntelyn osalta kohtuullisen hyvällä tasolla. On tärkeä erottaa, miten se hanke vietiin läpi ja minkälaisia kompastuskiviä siihen on. Kyllä se lopputulos on kuitenkin varsin laadukas." (V14)

Yhteenvetona valmisteluprosessista voidaan sanoa seuraavaa. Alussa lakipaketin valmistelu herätti eri näkemysten välillä voimakkaitakin vastakkainasetteluja. Ajan myötä valmistelusta kehittyi avoimempaa ja osallistavampaa. Lopputuloksena syntyi kaikkia osapuolia pääpiirteittäin tyydyttävä lakipaketti. Tuloksia tarkastellessa on kuitenkin syytä huomata, että aineistonkeruumme ajoittui vuoteen 2018, jolloin lakiesitysten käsittely eduskunnassa oli vasta alkamassa. Tämän vuoksi haastateltavien arviot koskivat vain viranomaisten tekemää valmistelua.

7.2 Sidosryhmien kolme näkökulmaa viranomaisvalvontaan verkossa[9]

Suomalaiset viranomaisvalvonnan sidosryhmävaikuttajat ryhmiteltiin väitelausekorttien järjestämisen ja jälkihaastatteluiden perusteella seuraavaan kolmeen näkökulmaan tai ryhmään: 1) Yksityisyyden, vapauksien ja turvallisuuden välillä tasapainoilijat (myöhemmin *Tasapainoilijat*), 2) Ihmisoikeuksien merkityksen korostajat (*Korostajat*) ja 3) Valvontaoikeuksien laajentajat (*Laajentajat*). Jokainen ryhmä lähestyy viranomaisten toimivaltuuksia verkossa, erityisesti tiedustelulainsäätöä, omanlaisesta näkökulmastaan. Yhteen ryhmään kuuluvien henkilöiden näkökulma ja siihen kytkeytyvä tapa järjestää väitteet ja ottaa kantaa haastattelussa ovat keskenään samankaltaisia, mutta toisaalta erilaisia kuin muihin ryhmiin kuuluneilla vastaajilla. Yhdeksää vastaajaa ei kuitenkaan voitu sijoittaa yksiselitteisesti mihinkään kolmesta ryhmästä tai näkökulmasta, vaan heissä yhdistyi piirteitä vähintään kahdesta näkökulmasta. Vaikka nämä vastaajat jäivät ryhmittelyn ulkopuolelle, aineistosta löytyy viitteitä, että he voisivat toimia sillanrakentajina eri näkemysten välillä.

Lisäksi tutkimuksemme löysi näkökulmien väliltä myös yhdistäviä tekijöitä. Yhdistävät tekijät laskettiin väitelauseiden lajittelun perusteella ($p < 0.05$). Yhdistävät tekijät eivät edustaneet väitelausekorttien lajittelussa kumpaakaan ääripäätä asteikolla (-5 = eniten eri mieltä ja +5 = eniten samaa mieltä), vaan lievempiä kantoja. Merkittävin jaettu ajatus on se, että julkisella keskustelulla on vaikutusta lakien sisältöön. Keskustelua ei koeta yhdentekeväksi ja turhaksi, vaikka se on monien mielestä välillä ollut turhauttavaa. Keskustelun merkityksellisyys kuitenkin kannustaa jatkamaan yhteistyötä ja muokkaamaan lainsäädäntöä yhdessä jatkossakin. Ei ole turvallisuusviranomaisten etu saada läpi lainsäädäntöä, jota merkittävät sidosryhmät tai kansalaiset eivät hyväksy, koska se voisi vaarantaa viranomaistoiminnan legitimiteetin.

Kolme näkökulmia yhdistävää väitelausetta liittyy siihen, kuinka viranomaisten tiedonhankintaa tulisi valvoa. Vastaajat kokivat, että lupaprosessi ei viivytä kohtuuttomasti tutkintaa ja tiedusteluviranomaisten valvojilla tulee olla riittävä ymmärrys valvontansa kohteista. He olivat osittain samaa mieltä myös siitä, että tiedustelumenetelmien käytöstä on pystyttävä kertomaan – salainen luonne huomioiden – myös vuosiraportin tai vastaavan puitteissa. *Laajentajat* eivät arvottaneet tätä keskimäärin yhtä korkealle kuin muut, mutta jälkihaastattelut paljastavat, että he ovat kuitenkin asiassa samoilla linjoilla. Seuraavaksi esitellään kaikki kolme näkemystä ja havainnollistetaan niiden sisältöä sitaattien avulla.

Yksityisyyden, vapauksien ja turvallisuuden välillä tasapainoilijat (Tasapainoilijat)

Tämän näkökulman alle sijoittui viisi tutkimukseen osallistunutta asiantuntijaa, jotka edustivat taustaltaan intressiryhmiä (3 henkilöä), ulkopuolisia tarkkailijoita (1 henkilö) ja toimivaltuuksien käyttäjiä (1 henkilö). *Tasapainoilijoiden* näkemyksiä yhdistää heidän pyrkimyksensä löytää tasapaino yksityisyyden, vapauksien ja

9 Kolmea näkökulmaa koskevat tulokset julkaistaan artikkelissamme ”Key Stakeholders’ Frames on the Police and Intelligence Agencies’ Online Surveillance Capabilities in Finland” Leppänen & Houtsonen (Hyväksytty julkaistavaksi). Tässä raportissa esitetään tulosten tiivistelmä sekä syvennetään tulosten tulkintaa näyttämällä lainauksia haastateltavien puheesta. Lainaukset julkaistaan ensimmäistä kertaa tässä raportissa.

turvallisuuden välillä. Turvallinen internet on tälle vastaajajoukolle yksi vapaan ja demokraattisen yhteiskunnan perusaines, jonka koskemattomuutta pitää suojella niin rikollisilta kuin valtiollisilta toimijoilta. Nämä henkilöt kannattavat samoja perusoikeuksia, esimerkiksi oikeutta yksityisyyteen, niin verkkoympäristössä kuin reaalimaailmassa, mutta korostavat myös yksilöiden vastuuta ja velvollisuuksia. *Tasapainoilijat* kannattavat tiedustelulakipakettia ja ajattelevat viranomaisten uusien toimivaltuuksien ensisijaisesti parantavan suomalaisen yhteiskunnan ja kansalaisten turvallisuutta.

Osallistuja V16 kiteyttää sen, mitä muutkin tämän näkemyksen jakavista vastaajista ajattelevat: viranomaisten pääsy yritysten kautta salaustenpurkuavaimiin heikentäisi kybertuvallisuutta yleisesti.

> *”Salaus on se, mikä mahdollistaa tällaisissa epäluotettavissa verkoissa turvallisen toiminnan ja nämä ehdotukset, joissa on puhuttu, että salausavaimia pitäisi viranomaisille luovuttaa, niin se on esimerkiksi teollisuudelle ja asioita ymmärtäville ehdoton punainen lippu. Vaikka viranomaisten toimintaan yleensä luotetaan, niin se on avain niin isoon massaan, niin paljoon asiaan, että siellä yksinkertaisesti ei luoteta kykyyn pitää ne salausavaimet vain siinä käytössä, missä ne olisi. Sitten on toinen, että ne ketkä haluaa toimintaansa salata tai suojata, niin tekee sen joka tapauksessa käyttämällä sellaisia voimia mitä viranomaisilla ei ole. Käytännössä heikennettäisiin asiallisesti asiansa hoitavien ihmisten turvallisuutta yleisesti verkossa.” (V16)*

Haastateltava V2 arvostaa yksityisyyttä korkealle, mutta näkee selvät perusteet sille, että viranomaisten on päästävä verkossa tapahtuvien vakavien turvallisuutta vaarantavien tekojen ja ihmisten jäljille. Hän edellyttää kuitenkin vahvaa viranomaistoiminnan kontrollia ja prosessien läpinäkyvyyttä, koska kansalaisten pitää saada varmistaa, ettei toimivaltuuksia käytetä perusteettomasti.

> *”Mun järkeily on se, että viranomaisilla pitää olla pääsy penkomaan nurkkia, kun on perustelu ja meillä pitää olla lupa olettaa, että viranomainen ei asiattomasti, perusteettomasti niitä toimivaltuuksia tule käyttämään. Haluan myös jollain tavalla ajatella, että Suomessa toimivan, Suomesta käsin vaikuttavan terroristin tai vakoojan tai suurrikollisen täytyy elää jatkuvassa paljastumisen pelossa. Tämän pitää olla vihamielinen paikka kovanluokan vihollisille.” (V2)*

Haastateltava V6 kokee, että tiedusteluviranomaiset turvaavat toiminnallaan suomalaisen yhteiskunnan laajat vapaudet ja pyrkivät estämään vapauksien ja ihmisoikeuksien väärinkäyttöä. Hän myös toivoo, että kansanedustajat, jotka valitaan tiedusteluvalvontavaliokuntaan suhtautuvat työhönsä vakavasti ja parlamentaarisesta valvonnasta kehitetään hyvin toimiva kokonaisuus, jonka sanalla on oikeasti painoarvoa.

> *”Tiedusteluviranomaiset mahdollistavat vapaan ja liberaalin yhteiskunnan toiminnan, koska mitä enemmän on vapauksia toimia, toteuttaa itseään ja ilmaista mielipiteitään, niin siinä on nähdäkseni olemassa se riski, että joku ulkopuolinen tulee ja käyttää niitä hyväksi. Sellaisessa ympäristössä pitää*

olla joku taho, joka tarkkailee sitä, että siihen yhteiskuntaan ei vaikuteta huonolla tavalla, että jonkun pitää vähän turvata sitä, että täällä voidaan olla ja ajatella sillä tavalla kuin me täällä keskenämme haluamme olla. [...] Yksi mullistava asia on parlamentaarinen valvonta, että siitä tulee tehokasta. Että siellä valvontavaliokunnassa on asialle vihkiytyneet kansanedustajat, jotka mielellään on useamman kuin yhden kauden ja että he osaavat myös käyttää valtaansa oikein ja osaavat kysyä oikeita kysymyksiä ja että siellä tiedusteluviranomaiset joutuvat myös vastaamaan oikeasti asioihin. Ettei kyse ole pelkästään siitä, että käydään vaikka Ratakadulla juomassa kahvit ja saadaan yleispätevä briiffi, vaan oikeasti on sitten siinä asiassa kiinni. Sehän on joka tapauksessa kehittämisen paikka, koska vastaavaa rakennetta ei ole aiemmin Suomessa ollut." (V6)

Tasapainoilijat kokevat, että tiedustelulakipaketti on selkeä kokonaisuus, jonka sisällössä on yhtäläisesti huomioitu eri tavoitteita ja intressejä. He luottavat suomalaiseen yhteiskuntaan, viranomaisiin ja päättäjiin, mutta ovat valmiita reagoimaan väärinkäytöksiin. Viranomaisten toimivaltuuksien käytön uskottava ja riittävä valvonta sekä yhteiskunnan avoimuus ovat avainasemassa luottamuksen säilyttämisen näkökulmasta. Tietoliikennetiedustelu uutena tiedustelumenetelmänä on asia, jonka toimivuudesta ja valvonnasta he odottavat kuulevansa kokemuksia, mutta ymmärtävät, että kyse on salaisesta tiedonhankintakeinosta, josta ei voi kertoa kaikkea.

Osallistuja V22 pitää hyvänä, jos tiedustelulupia päätettäessä läsnä saisi olla myös julkinen asiamies, joka pitäisi huolta luvan kohteiden oikeuksista. Hän perustelee tarvetta erityisasiantuntemuksen kautta, koska tuomari ei voi olla joka alan asiantuntija.

"Mitä merkittävämpi intressi asiassa on perusoikeuksissa, niin sitä parempi, että siinä on tällainen ulkopuolinen julkinen asiamies, koska asiantuntemus täytyy tämmöisellä asiamiehellä olla ihan eri luokkaa kuin yksittäisellä tuomarilla. Sitä kautta tulee tehokkaampaa kontrollia, että tuomari voi ainoastaan vain tiettyihin rajoihin asti arvioida sitä." (V22)

Haastateltavat V14 ja V16 luottavat viranomaisiin, mutta ymmärtävät, ettei luottamus voi olla sokea, vaan tarvitaan kontrollimekanismeja, jotka hillitsevät väärinkäytöksiä ja ylilyöntejä sekä tarvittaessa paljastavat niitä.

"Aina tulee väärinkäytöksiä, siitä ei päästä mihinkään, mutta ne väärinkäytökset pitää havaita ja niihin pitää sitten tehokkaasti puuttua." (V14)

"Kun me eletään yhteiskunnassa, joka perustuu siihen, että tehdään sääntöjä, niin ne säännöt pitää olla tämmöisessäkin toiminnassa. Mulla on hyvin korkea käsitys suomalaisten viranomaisten moraalista ja toiminnasta, mutta kuitenkin on tämmöinen sanonta, että valta korruptoi ja absoluuttinen valta korruptoi absoluuttisesti. Jos ei ole mitään pidäkkeitä, valvontaa, niin se johtaa siihen, että siellä tehdään ylilyöntejä. Ja kun sitä valvontaa ei ole, niin ne ylilyönnit ei edes paljastu." (V16)

Osallistuja V6 toivoo, että valvontakeinoja käytettäisiin niiden mahdollistamassa laajuudessa. Esimerkiksi tietoliikennetiedustelun kohteeksi joutuneet ja asiasta tiedon saaneet ihmiset voivat pyytää tiedusteluvalvontavaltuutettua tutkimaan tapausta ja hän toivoo, että näin myös välillä kävisi.

> *”Ylipäätänsä, kyllä siinä yhteiskunnan pitää olla ainakin vähän hereillä, ettei tule mitään ylilyöntejä. Toivottavasti ihmiset ovat myös valmiita haastamaankin välillä niitä ratkaisuja, että jos he vaikka saavat ilmoituksen, että olette joutuneet tietoliikennetiedustelun kohteeksi, he sitten myös käyttäisivät oikeuksiansa muun muassa tiedusteluvaltuutetun suuntaan, että tiedusteluvaltuutettu kävisi tutkimaan sitä asiaa tarkemmin. (V6)*

Haastateltava V2 kannustaa tiedusteluviranomaisia aidosti pohtimaan niitä rajoja, joissa tiedustelusta voidaan keskustella julkisesti. Sidosryhmät ja kansalaiset tarvitsevat tietoa erityisesti siitä, miksi tiedustelulait tarvitaan. Tällainen keskustelu kytkeytyy periaatteelliselle tasolle, mistä puhumisen ei pitäisi olla mahdotonta.

> *”Voi olla, että on myös alan piireissä heikosti ymmärretty, mitkä niistä tiedustelumenetelmistä on tämmöisiä ikuisia totuuksia, joista voitaisiinkin käydä keskustelua, periaatteellisia tasoja ja mitkä on taktisia menetelmä- ja operaatiotasoja, jotka pitää ollakin salaisia. Kun lakiin on pakko kirjata, mitä valtuuksia halutaan, on pakko kertoa vähän miksi niitä valtuuksia halutaan. Se ”miksi” on ollut tosi vaikea kertoa.” (V2)*

Tämä vastaajajoukko tunnistaa myös useita, monimutkaisia tiedonhankintaan liittyviä arvokysymyksiä ja tilanteita, joissa asiat eivät ole mustavalkoisia. Esimerkiksi tiedonvaihdon kumppanivaltiot eivät välttämättä noudata YK:n ihmisoikeussopimusta, mutta se ei poista tosiasiaa, että kumppanilla voisi olisi tietoa, joka olisi tärkeää Suomen turvallisuuden parantamiseksi tai toisinpäin. Tai suojelemalla tiettyjä ammattiryhmiä tiedustelulta, saatettaisiin samalla luoda lakiin porsaanreikiä, joita epärehelliset toimijat voisivat hyödyntää.

Lisäksi osallistuja V14 odottaa poliitikoilta arvokeskustelua tiedustelulainsäädännön ympärillä. Hänelle on tärkeää, että kerrotaan avoimesti esimerkiksi tietoliikennetiedustelun vaikutuksista perusoikeuksiin ja tehdyt ratkaisut olisivat perusteltuja arvoratkaisuja.

> *”Mun mielestä poliitikkojen vastuulla olisi sen aidon arvokeskustelun käyminen. Että tässä [tiedustelulakihankkeessa] ja monissa muissa hankkeissa pystyttäisiin käymään sitä perusoikeustasoista keskustelua näkyvästi ja ammattitaitoisesti. Monessa meidän toiminnassa on se haaste, että poliittinen päätös syntyy puoluetasolla ja sitä puolustetaan niillä argumenteilla mitä ehditään asian ympärille haalia. [...] Että siellä oikeasti tunnustettaisiin se tosiasia, että tälläkin hankkeella on perusoikeuksia heikentäviä puolia, mutta nähdään, että nämä, nämä ja nämä syyt puoltaa sitä, että meidän täytyy tällaisia toimenpiteitä tehdä. Se on mun mielestä poliittisten päättäjien keskeinen rooli, että tuodaan näkemyksiä pöytään ja niitä pystyttäisiin myös arvottamaan, että meille nämä ja nämä syyt ovat tärkeimpiä.” (V14)*

Ihmisoikeuksien merkityksen korostajat (Korostajat)

Toiseen näkökulmaan sijoittuu seitsemän vastaajaa, jotka edustavat intressiryhmiä (2 henkilöä), ulkopuolisia tarkkailijoita (3 henkilöä), poliitikkoja (1 henkilö). Yksi vastaaja ei halunnut paljastaa taustaansa. *Korostajat* alleviivaavat ihmisoikeuksien ja perusvapauksien tärkeyttä ja ovat huolissaan lisääntyvän viranomaisvalvonnan mahdollisista negatiivisista vaikutuksista yhteiskunnassa. He rakentavat näkökulmansa monin paikoin vähemmistöjen ja heikoimpien ihmisryhmien suojelemisen ympärille, mutta arvioivat viranomaisten harjoittamaa tiedonhankintaa verkossa myös ns. tavallisten ihmisten toiminnan kautta. Tälle ryhmälle viranomaisvalvonnan syrjimättömyys ja toimivaltuuksien käytön valvonta ovat avainasemassa. Voimakkaista ideologisista mielipiteistä huolimatta he tunnistavat, että jotkin tiedonhankintaan liittyvät asiat, kuten kansainvälinen tiedonvaihto tai tietyille ammattiryhmille annettu suoja viranomaistiedustelulta, voivat olla monitahoisia ja olosuhderiippuvaisia kysymyksiä. Osallistujia askarruttaa tiedustelulaeissa, kuinka valvonnan haitoilta voi suojella erityisesti heikoimpia yksilöitä sekä miten estää mahdolliset valtiovallan väärinkäytökset. Toisaalta ilmassa on myös epätietoisuutta tietoliikennetiedustelulla saavutettavista hyödyistä.

Osallistuja V11 pohtii, ettei yhteiskunnan turvallisuus parane pelkkää viranomaisvalvontaa lisäämällä, koska tiedustelulait eivät ratkaise terrorismin ydinongelmia: miksi ihmiset radikalisoituvat ja ryhtyvät terroritekoihin? Miten väkivaltaisen radikalisoitumisen prosessin voi estää? Hän odottaa, että terrorismin torjuntaan kohdennetaan myös toimenpiteitä, joilla voidaan ehkäistä radikalisoitumista. Valvonnan lisääminen yksistään johtaa hänen mukaansa ihmisten viestintätapojen muutokseen. Hän ei ymmärrä, miksi turvallisuusviranomaiset eivät pysty selittämään paremmin julkisuuteen, mitä konkreettista hyötyä tietoliikennetiedustelun kaltaisista menetelmistä on ollut muualla maailmassa.

> *”Jos miettii ihan syvällisemmin sitä, että mitkä on ne asiat, jotka vaikuttaa ihmisen tai yhteiskunnan turvallisuuteen, niin joku yksittäinen tiedustelukeino ei muuta sitä asiaa, että jos ihmiset radikalisoituu jostakin syystä niin pahasti, että he tekee terroriteon tai suunnittelee sitä, niin siinä on myös muut asiat taustalla. Jos lisätään vaan tiedustelukeinoja, mutta ei puututa samanaikaisesti niihin syihin, mistä syistä ihmiset radikalisoituu puolin ja toisin, niin silloinhan se ei lisää myöskään yhteiskunnan turvallisuutta millään tavoin. Se muuttaa vaan ihmisten keinoja kommunikoida. [...] ”Minulle on oikeasti jäänyt todella epäselväksi Suomen tiedustelulakipaketin käsittelyssä, että mitkä ne konkreettiset keinot tai konkreettiset tavat on ollut muissa valtioissa, joissa verkkoviestintään kohdistuva valvonta olisi parantanut turvallisuutta. Voi olla, että nämä ovat asioita mitä on ensin tehty jossain puolustusvaliokunnan tai ulkoasianvaliokunnan kuulemisissa, niissä kuulemisissa, joihin meillä ei ole mahdollisuutta päästä ja jotka pidetään turvahuoneessa. Mutta mun mielestä sen ei tulisi olla niin vaikeaa selittää konkreettisesti, että millä tavoin eri verkkoviestintävalvonta on parantanut turvallisuutta muissa maissa.” (V11)*

Myös osallistuja V21 miettii, että lisääntyvä viranomaisvalvonta voi vaikuttaa ihmisten viestintään ja rajoittaa esimerkiksi aiheita, joista uskalletaan puhua sekä kannustaa käyttämään kiertoilmauksia. Itsesensuurista on hänen mukaansa näyttöä jo ulkomailta ja kyseessä on asia, johon tuomioistuimet ovat kiinnittäneet huomiota.

”Itsesensuurin pelko, siihen moni tuomioistuin on kiinnittänyt huomiota tässä. Että jos on pitkälle menevä ja erittelemätön verkkovalvonta, niin se saattaa johtaa sekä siihen, että ihminen kokee olevansa jatkuvan valvonnan kohteena. Kiinasta esimerkiksi konkreettisia esimerkkejä, kun tiedetään, että Kiinan tiedusteluviranomaiset valvovat käytännössä kaikkea viestintää, niin sehän on jo johtanutkin siihen, että ei uskalleta keskustella samoista teemoista tietenkään ja käytetään kiertoilmaisuja ja muuta. Kyllä sekin on jo tukahduttamista.” (V21)

Haastateltava V20 näkee yhdeksi riskiksi tiedustelun valvonnan riippumattomuuden ja osaamisen. Valvovan elimen perustaminen ei takaa, että elimeen valitaan pätevä, osaava ja soveltuva henkilökunta, jolle annetaan riittävät resurssit. Vaikka tilanne olisi hyvä aluksi, se voi muuttua tulevaisuudessa poliittisten voimasuhteiden vaihtuessa.

”Kuinka riippumattomaksi tiedusteluvaltuutettu saadaan ja minkälainen osaaminen hänen ympärilleen saadaan kasattua, että pystyy järkevästi valvomaan. Vaikka laissa sanotaan, että tällainen perustetaan, niin voidaanhan se resursoida riittämättömästi ja täyttää sellaisilla ihmisillä, jotka eivät ole tehtäviensä tasalla. Vaikka nyt ei niin tehtäisikään, niin entä sitten seuraava hallitus tai 10 vuoden päästä oleva hallitus tai mikä tahansa? Tämmöiset asiat itseä askarruttaa.” (V20)

Osallistuja V17 korostaa tuomioistuimen vastuuta tiedustelulupien myöntämisessä ja kokee tiedustelulupien myöntämisen edellyttämän harkinnan haastavammaksi kuin rikosperustaisten, koska henkilön liittyminen rikokseen on helpommin perusteltavissa kuin kohdentamattomampi tiedustelu. Hänen näkemyksensä suojattujen ammattiryhmien viestinnän tiedustelukiellosta on tiukka, eikä hän pidä hyvänä, että heidän suojatuksi tarkoittamaa viestintää päätyy viranomaisten haltuun. Osallistuja näkee tarpeelliseksi, että näiden ammattiryhmien edustajille, kuten toimittajille, ilmoitettaisiin, jos esimerkiksi lähdesuojaa on rikottu.

”Mä voin hyvin kuvitella, että yksi syy minkä takia rikoksen tutkintaan ja selvitykseen liittyvät lupa-anomukset menee helposti läpi, liittyy juuri siihen, että yleensä on tosiseikkoja, joiden perusteella voidaan joko uskottavasti tai vähemmän uskottavasti perustella, miksi tämän henkilön puhelinkuunteleminen on järkevää tämän rikoksen selvittämiseksi. Mutta nyt kun on kyse tällaisesta, tietyssä mielessä kohteen tai yksilön näkökulmasta enemmän kohdentamattomasta valvonnasta, jonka tavoitteena on vain kerätä tietoa, niin se vielä entuudestaan korostaa tuomioistuimen tekemän harkinnan merkitystä. [...] Minä en kannata sitä, että tiedustelu kohdistetaan esimerkiksi lakimiesten, toimittajien ja lääkärien viestintään. Nythän niin tullaan tekemään, kun sitä ei voida etukäteen sulkea pois, sitä voidaan vain hävittää jälkeenpäin. Kyllä mä näkisin, että juuri se on julkilausutusti mahdollista, niin kuin tuossa haetaan tuolla väittämällä [väitelausekortti 15], että sitten se aika pitkälti myöskin murentaa meidän riippumattoman tiedonvälityksen yhtä perusfundamenttia, joka on lähdesuoja. Nyt ne joutuu vaan luottamaan siihen, että

hävittämisvelvollisuus sitten pätee, mikä on mielestäni ongelmallista. Vähintä mitä näiden osalta pitäisi tehdä on automaattinen ilmoittamisvelvollisuus, että toimittaja saisi tiedon siitä, jos lähdesuojaan on kajottu." (V17)

Vastaaja V24 pitää merkittävänä, että kansainvälisessä yhteistyössä huomioidaan ihmisoikeudet ja niihin liittyvä arvopohja. Hänelle se tarkoittaa erityisesti sitä, että tietojenvaihdolla ei riskeerata kolmansia osapuolia ja harkitaan, millaisten maiden kanssa ollaan tekemisissä.

"Mun mielestä ois tärkeää, että ulkomaantiedustelussa pystytään ylläpitämään sellaista kansainvälistä yhteistyötä, jossa noudatetaan sitä, että katsotaan minkälaisten maiden kanssa ollaan tekemisissä siltä osin, että ihmisoikeussopimuksen noudattaminen kuten myös muut sellaiset kansainväliseen arvopohjaan liittyvät kysymykset otetaan huomioon. Ja siltä osin mun mielestä kansainvälinen yhteistyö on tärkeää. Ei se ole täysin itsearvoista, mutta että se liittyy kuitenkin siihen, että kun tehdään kansainvälistä yhteistyötä, meidän pitää pitää huolta siitä, että näissä vakavissa uhissa me myös mietitään, että mitä sillä yhteistyöllä saavutetaan tai mitä siitä voi aiheutua kolmansille osapuolille." (V24)

Tämän ryhmän suhtautuminen tiedustelulakipakettiin on monin paikoin kriittinen ja *Korostajien* näkemyksiä leimaa epävarmuus erityisesti tietoliikennetiedustelun toteutuksesta, tarkkuudesta, vaikutuksista ja tehokkuudesta sekä huoli menetelmän mahdollisesta liukumisesta massavalvonnan suuntaan. Huomattavaa on, että epävarmaan suhtautumiseen tuntuu vaikuttavan joillakin ryhmän jäsenillä se, ettei kotimaisesta tiedustelutoiminnasta ole ollut saatavilla kovin paljoa luotettavaa julkista tietoa. Niinpä heidän on vaikea arvioida, onko lainsäädäntöluonnos oikeasuhtainen turvallisuusuhkiin nähden ja parantuuko turvallisuus uuden lainsäädännön myötä niin kuin on ajateltu. Kritiikistä ja koetusta epätasapainosta turvallisuustavoitteiden ja yksityisyydensuojan suhteen huolimatta monet näkökulman kannattajat antavat tunnustusta siitä, miten tiedustelulakien aiottu sisältö on kehittynyt prosessin aikana.

Osallistuja V7:n kritiikki kulminoituu tietoliikennetiedustelun vaikutuksiin ja hyötyihin. Hän kokee, että toiminnan vaikutukset ja hyödyt on määritelty ja analysoitu puutteellisesti ja perusteellisempi riskikartoitus toimisi hyvänä pohjana keskustelulle.

"Minun ymmärrykseni mukaan ainakin siinä lakiehdotuksessa oli aika suppeasti näistä yhteiskunnallisista vaikutuksista ja yksilöön kohdistuvista vaikutuksista. Siellä ei ihan hirveän kattavasti näkynyt sitä, eikä myöskään näkynyt tällaista arviota siitä, miten hyvin näillä ehdotetuilla menetelmillä voidaan saavuttaa niitä tavoiteltuja asioita. […] Jos meillä ei ole tällaista riskianalyysia, on vaikea käydä keskustelua, kun ei ole mitään konkreettista olemassa. Tällaisella riskikartoituksella voitaisiin saada selville ne hyödyt ja haitat, vaikutukset yleisestikin ottaen. Siitä voitaisiin lähteä käymään keskustelua laajemmin ja arvioimaan sitten miten tarkasti mitäkin tarvitsee kertoa." (V7)

Haastateltava V20 on huolissaan siitä, että tietoliikennetiedustelua varten rakennettavat tekniset kyvykkyydet mahdollistavat massavalvonnan. Vaikka poliittinen tahto olisi tällä hetkellä massavalvonnan vastainen, tulevaisuudessa voi tulla paineita hyödyntää kytkentöjen tarjoamaa koko kapasiteettia. Lisäksi rakennettuja kytkentöjä voidaan väärinkäyttää lain hengen vastaisesti.

> *”Laki sellaisenaan kuin se on kirjoitettu, ei mahdollista massavalvontaa. Siellä on ne kohdennetut parametrit ja kaikki muut, mutta, tulee iso mutta, ne lain velvoitteet joita tulee palveluntarjoajille ja muille, antaa tekniset mahdollisuudet valvoa kaikkea tietoliikennettä. [...] Se oma näkemys, varsinkin kun tulee tekniseltä taustalta on vähän se, että sitten kun se kyvykkyys siellä on – ja se on kohtuu kallistakin – niin jossain kohtaa joku poliitikko voi sanoa, että miksi me ei käytetä sitä koko potentiaalia? Toinen mahdollisuus on, että jos joku on ovela ja käyttää sitä väärin.” (V20)*

Osallistuja V24 pitää äärimmäisen merkittävänä, että perusoikeuksia rajoitetaan ainoastaan kaikkein vakavimpiin rikoksiin puuttumisessa ja että kansallisen turvallisuusuhkan on oltava vakava, ennen kuin viranomaiset saavat valvoa verkkoviestintää. Hän näkee asian tasapainotteluna yksityisyydensuojan ja turvallisuuden välillä.

> *”Tasapainoilu, miten yksityisyydensuojaan ja turvallisuuteen liittyvät perusarvot asetetaan yhteen niin, ettei kenenkään perusoikeuksien suojaa vaaranneta. Silloin ehdottoman tärkeä lähtökohta on se, että se koskisi vain kaikkein vakavimpia rikoksia ja tätä kansallisen turvallisuuden vakavaa uhkaa. Työryhmätyössä ja koko keskustelussa on pidetty erityisen tärkeänä, että se ei ole vain kansallisen turvallisuuden uhka, vaan sille pitää olla jokin määritelmä, minkä tyyppinen uhka. Se on ollut ainakin minulle hyvin tärkeää, että sitä määrittelyä tehdään.” (V24)*

Osallistuja V21 on melko tyytyväinen tiedustelulakiluonnosten sisältöön ja hän kiittääkin lainvalmistelijoita siitä, että lupahakemuksille on asetettu tarkkoja kriteerejä, joita vasten lupia myöntävät tuomarit pystyvät arvioimaan onko luvan myöntämiselle perusteita.

> *”Tuomioistuimen itsenäisyys ja riippumattomuus on erittäin tärkeä oikeusvaltiollinen periaate, eikä voida lähteä siitä, että pelkästään viranomaisen lupa-arvioon nojaten tehtäisiin näitä päätöksiä. Kyllä mun nähdäkseni tässä tiedustelulakihankkeessa on pyritty takaamaan tätä asettamalla sille lupahakemukselle varsin tarkkoja kriteerejä ja sellaisia, jotka ovat myös oikeudellisestikin arvioitavissa. Niin kyllä mä ajattelisin, että valtaosin ne esitykset on ihan kohtuullisen hyvässä kunnossa.” (V21)*

Valvontaoikeuksien laajentajat (Laajentajat)

Kolmas vastaajaryhmä pyrkii perustelemaan, miksi turvallisuusviranomaiset tarvitsevat laajemmat toimivaltuudet verkkoympäristössä. Ryhmään kuuluu neljä henkilöä, joista yksi on poliitikko, yksi ulkopuolinen tarkkailija ja kaksi toimivaltuuksien käyttäjää. He lähestyvät viranomaisten toimivaltuuksia verkossa erityisesti viranomaisten tehtävien hoitamisen näkökulmasta ja turvallisuusviranomaiset palvelevat heidän näkökulmastaan ensisijaisesti valtion ja kansalaisten etua. Tämän vastaajaryhmän mukaan Suomen lainsäädäntö vaatii päivittämistä tieto- ja viestintäverkoissa tehtävän tiedonhankinnan osalta, koska toimintaympäristö – kuten uhkat ja teknologia – on olennaisesti muuttunut ja viranomaiset eivät suoriudu riittävällä tavalla niille asetetuista lakisääteisistä tehtävistä, jos lakia ei uudisteta. Esimerkiksi Ulkoministeriön tietoverkkoihin kahden valtion kohdistama vakoilu vuonna 2015 oli vakava kansallisen turvallisuuden uhka, mitä Suomi ei julkisten lähteiden mukaan kyennyt havaitsemaan itse. Kansainvälinen tiedonvaihto koettiin tässä ryhmässä merkittäväksi edellytykseksi niin uhkien torjunnassa kuin rikostutkinnassa.

Osallistujat V15, V8 ja V3 perustelevat tiedustelulainsäädännön tarpeellisuutta kansallisen turvallisuuden parantamisella. Heidän mielestään muuttuneet uhkakuvat edellyttävät myös viranomaisten toimivaltuuksien kehittämistä ennakoivampaan suuntaan. Vastaaja V15 ei näe lisääntynyttä valvontaa uhkana demokraattiselle yhteiskunnalle, vaan sen muodostavat terrori-iskut ja muu kansallista turvallisuutta uhkaava toiminta, jota viranomaiset pyrkivät estämään. Haastateltu V8 kokee, että nimenomaan valtion johto tarvitsee tietoa Suomea koskevan päätöksenteon tueksi ja tiedusteluviranomaisten suorittama tiedonhankinta on yksi väline siinä. Osallistuja V3 puolestaan näkee puutteet tiedustelukyvyssä ja kyvyssä suojata omaa maatansa esimerkiksi vakoilulta tekijöinä, jotka heikentävät luottamusta kansainväliseen yhteistyöhön ja muodostavat riskin esimerkiksi EU:lle.

> *”Valtion tehtävänä on nimenomaan suojella kansalaisiaan terroriteoilta ja lisätä luottamusta. Jos siinä verkkovalvonta on toimiva keino, niin ilman muuta sitä tulee käyttää. Ettei tässä valvonta niitä arvoja heikennä, vaan nämä ulkoiset uhkat.” (V15)*

> *”Maailman turvallisuustilanne on niin paljon muuttunut, että meidän viranomaisten pitää olla riittävän tietoisia, mitkä asiat uhkaavat vakavasti meidän kansallista turvallisuutta. Ja tämä tieto ei ole vain turvallisuusviranomaisia varten, vaan nimenomaan valtion johtoa varten. Tässä minusta ei ole kysymys urkinnasta, vaan siitä, että pystytään reagoimaan ajoissa niihin uhkiin mitkä on näköpiirissä.” (V8)*

> *”Me ei tiedetä, että kuka meidän verkoissa liikkuu. Me ei tiedetä, että onko meillä tälläkin hetkellä sellaisia vastaavanlaisia vakoilukeissejä päällä kuin oli Ulkoasianministeriön verkossa. Onko muissa ministeriöissä, onko meidän teollisuudessa sellaista? Onko meidän muissa organisaatioissa sisällä haittaohjelmia, jotka tuottaa tietoa sille vastustajalle, taikka rikollisille tai vastaaville? Esimerkiksi tuolla UM:n tietovuodolla me menetettiin varmaan EU:n silmissä osittain sellainen luotettavan partnerin kuva. Elikkä että täältä voi kuka tahansa hakea EU-tietoa, jos se haluaa.” (V3)*

Myös vastaaja V18 kokee, että turvallisuusuhkat ja rikollisuus ovat muuttuneet tavalla, joka edellyttää viranomaisten toimivaltuuksien päivittämistä. Hän näkee, että lainvalvonta- ja tiedusteluviranomaiset pyrkivät kohdistamaan tiedonhankintaa tiettyihin paikkoihin – aivan niin kuin esimerkiksi liikennevalvontaa ja muita verkon ulkopuolisia valvontakeinoja. Viranomaiset ja niiden käytössä olevat toimivaltuudet varmistavat, ettei yhteiskuntaan synny paikkoja, joissa yhteiset säännöt eivät päde.

> *”On toki totta, että lainsäädäntö laahaa jäljessä ja tavallaan turvallisuus- ja rikollisuustilanne kehittyy niin, että meidän näkökulmasta, ja oma henkilökohtainenkin mielipide, että viranomaisten valvontavaltuudet ei kyllä missään nimessä ole sillä tasolla missä pitäisi olla. […] Se että halutaan kohdentaa tiettyihin paikkoihin valvontaa, jossa se rikollisuuden toteutumisen riski on suurempi, kuin sitten muilla paikoilla. Ja samahan pätee verkossa, että sitten on tiettyjä paikkoja verkossa, keskusteluryhmiä, joissa todennäköisimmin esimerkiksi terroristit linkittyy keskenään tai tapahtuu joitakin kunnianloukkauksia, niin kyllä siellä sitten sen lainvalvontaviranomaisen roolin tulisi olla vahvempaa. Se verkko ei voi olla kuitenkaan niin kuin täysin vapaa paikka rellestää” (V18)*

Tämän ryhmän vastaajat ottavat kantaa erityisesti julkisuudessa usein esitettyihin voimakkaisiin väittämiin. He haluavat tuoda esille, ettei Suomeen suunnitellussa tietoliikennetiedustelussa ole kyse massavalvonnasta eikä toimivaltuuksien laajentaminen heikennä yhteiskuntamme arvoja tai tyrehdytä demokraattista keskustelua. Sen sijaan vastaajat kokevat, että nykyinen ja suunniteltu lainsäädäntö ovat tasapainossa turvallisuustavoitteiden sekä yksityisyydensuojan näkökulmasta. He ymmärtävät avoimuuden, tiedon ja valvontamekanismien arvon ja puhuvat niistä ensisijaisesti turvallisuusviranomaisten toiminnan kontekstissa (vrt. *Korostajat*, jotka puhuvat kansalaisten näkökulmasta). Tämän ryhmän vastaajat tuntuvat myös uskovan esimerkiksi tietoliikennetiedustelusta saataviin hyötyihin enemmän kuin kahden muun näkökulman kannattajat.

Osallistuja V3 antaisi tiedusteluviranomaisille viitisen vuotta aikaa kehittää tietoliikennetiedustelua ja uskoo, että sen jälkeen prosessi toimii hyvin. Hän on vakuuttunut, että tiedusteluviranomaiset pyrkivät jo oman toimintansa takia määrittelemään tietoliikennetiedustelun hakuehdot mahdollisimman hyvin. Ylimääräisestä tiedosta koituu lisätyötä, joten intressi on kohdentaa suodatus mahdollisimman tarkasti.

> *”Tiedusteluviranomaisen tavoitehan on taas saada se mahdollisimman tarkkaan kohdennettua pelkästään siihen mitä se etsii, koska jokainen väärinkerätty signaali, jokainen väärinkerätty viesti on ikään kuin kivi kengässä, koska se pitää käsitellä ja hylätä ja siitä pitää tehdä pöytäkirjat sun muuta. […] Että se tiedusteluviranomainen on äärimmäisen tarkka, etenkin tämän toiminnan alussa, ettei vaan tule mitään virheitä. Niin hukataan paljon [tietoa], mutta pikkuhiljaa, se vie sellaisen viisi vuotta, sitten toimii tämä homma hyvin.” (V3)*

Haastateltava V15 kokee, että media ja ulkomaiset tiedustelukohut ovat paisuttaneet aiheetta huolta massavalvonnasta. Hän luottaa, että viranomaisilla on tietoon perustuva käsitys tietoliikennetiedustelun toimivuudesta ja sen kautta saavutettavissa olevista hyödyistä.

”Kyllä mä uskon, että viranomaisilla itsellään on ihan selvä käsitys, minkälaisissa tapauksissa tästä [tietoliikennetiedustelusta] on hyötyä ja mitä tällä voidaan tehdä. Tällaiset massavalvontapelottelut, niin nehän on median aikaansaamia ja tällaiset NSA-esimerkit, niin mä luulen että viranomaiset on tässä paljon realistisempia ja paremmin kartalla kuin median jutut ja pelottelut.” (V15)

Osallistuja V18 peräänkuuluttaa demokraattisen yhteiskunnan vastuuta muuttaa lainsäädäntöä, jos nykyinen todetaan toimimattomaksi. Sen sijaan hän ei antaisi pelolle valtaa etukäteen vaan kokee, että lait tulee säätää tarpeen mukaan eikä olla säätämättä sen takia, että niitä pelätään väärinkäytettävän tulevaisuudessa.

”Demokraattinen yhteiskunta rakentuu siihen, että lainsäädäntöä muutetaan, jos koetaan, ettei se toimi siinä yhteiskunnassa. Mutta me ei voida ehkä jättäytyä siihen, että ei luoda tehokkaita toimivaltuuksia ehkäistä ja torjua sen tyyppistä rikollisuutta mikä meitä kohtaa tällä hetkellä, jos pelätään, että miten niitä valtuuksia tulevaisuudessa käytetään.” (V18)

Osallistuja V8 pitää asiallisena, että suojelupoliisi tulee tiedottamaan tiedustelumenetelmien käytöstä kansalaisille. Hän pitää vuosikertomusta sopivana tapana ja kehuu ruotsalaisen Säkerhetspolisenin tiedotuslinjaa. Sen sijaan yksityiskohtia operaatioista ei voida hänen mukaansa paljastaa eikä mitään sellaista, jonka kertominen vaarantaisi turvallisuutta.

”Silloin tällöin tästä [tiedustelumenetelmien käytöstä] tiedottaminen on tarpeen. Esimerkiksi suojelupoliisin vuosikertomus ja siitä kertominen minusta ihan kuuluu avoimeen yhteiskuntaan, että kertoo niin kuin Ruotsissa Säkerhetspolisen, että näillä verkkotiedustelutiedoilla on pystytty pari terroristi-iskua torjumaan. Mutta tolkkua siinä mitä kerrotaan: eihän semmoista, mitä turvallisuuden takia pidetään tallessa.” (V8)

Vastaaja V15 ei pidä tiedustelulakeja liian läpitunkevina, koska ihmisillä säilyy edelleen oikeus suojata viestintänsä haluamillaan keinoilla. Viestinnän suojaaminen ei hänen mukaansa edellytä edes erityisosaamista. Hän toivoo lisää avoimuutta ja tietopohjaa julkiseen keskusteluun, etteivät osapuolet muodosta mielipidettään väärinkäsityksiin nojaten.

”Mun mielestä avoimuus on tärkeintä. Että ihmisellä, sillä peruskansalaisella, on aika kummallisia käsityksiä kuitenkin tästä (tietoliikennetiedustelusta). Ei kansalaiset ymmärrä näitä salausasioita ja ei ymmärtänyt yrityksetkään aluksi. Siitähän oli hirveä vastustus silloin kun tätä lakia alettiin puuhata. Nämä isot tietoturvayrityksetkin oli sitä vastaan. Jos tämä on yrityksille vaikea asia, niin on tämä kansalaisillekin. Niin sen takia juuri tämä avoimuus ja näistä käytännöistä kertominen, niin se on mun mielestä kaiken a ja o jatkossa. [...] Kyllähän mulla on jatkossa edelleen keinoja välttää kaikenlainen valvonta, tai ainakin melkein kaikenlainen valvonta, ei tietenkään kaikkea, mutta mulla on keinoja suojata viestintä, jokaisella kansalaisella on. Ei se vaadi edes teknistä osaamista. Niin kyllä mun mielestä tässä säilyy tasapaino.” (V15)

7.3 Yhteenveto ja pohdinta[10]

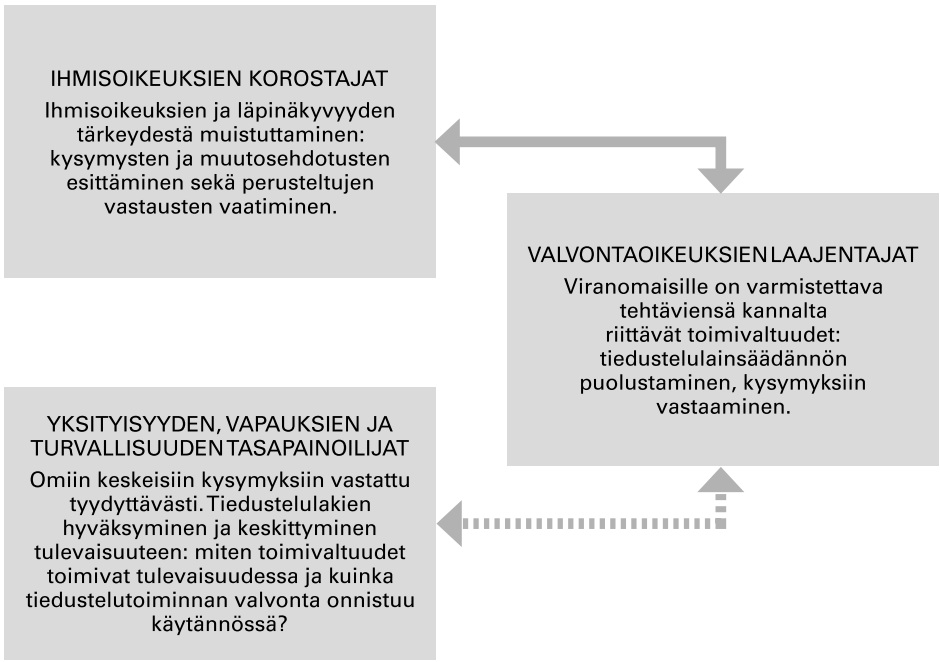
Tutkimukseen osallistuneet sidosryhmien edustajat (n=25) jaettiin vastaustensa perusteella Q-faktorianalyysia käyttämällä kolmeen ryhmään: Yksityisyyden, vapauksien ja turvallisuuden välillä tasapainoilijat (*Tasapainoilijat*), Ihmisoikeuksien merkityksen korostajat (*Korostajat*) ja Valvontaoikeuksien laajentajat (*Laajentajat*). Vastaajat, jotka lajittelivat väitelausekortit samankaltaisesti, päätyivät samaan ryhmään ja heidän ajatuksensa muodostivat näkökulman tai tulokulman, jonka valossa he tarkastelivat viranomaisten toimivaltuuksia verkossa. Syntyneet näkökulmat ulottuvat laajemmalle kuin vain näihin vastaajiin ja niitä voi tulkita myös kehyksinä, joiden kautta sidosryhmäasiantuntijat osallistuivat toimivaltuuskeskusteluun (ks. tarkemmin Leppänen & Houtsonen, Hyväksytty julkaistavaksi). Yhdeksän vastaajaa jäi ryhmien ulkopuolelle, koska heidän tekemässä lajittelussa oli piirteitä vähintään kahdelle näkökulmalle tärkeistä asioista, mikä voi viitata toimimiseen välittäjänä ja intressien sekä arvojen yhteensovittajina eri näkökulmien välillä. On huomionarvoista, että näkökulmat ovat piileviä ja niiden tarkoitus on auttaa ymmärtämään poliittista keskustelua, eikä sidosryhmäasiantuntijoita ole mielekästä lokeroida oikeasti. Koostetut näkökulmat ovat vain työkalu, joka tuo näkyväksi niitä asioita ja perusteluja, joiden kautta mielipiteet viranomaisvalvonnan oikeutuksesta muodostuvat suhteessa toisiinsa.

Vaikka väitelausekorteissa kysyttiin sekä lainvalvonta- että tiedusteluviranomaisten toimivaltuuksista verkossa, muodostuneet näkökulmat kuvaavat erityisesti suhtautumista tiedustelulakeihin. Tiedustelulainsäädäntöprosessi ei ollut Suomessa kitkaton ja varsinkin prosessin alkuvaiheissa eri näkemysten välillä oli suuriakin eroja. On kuitenkin huomionarvoista, että moni sidosryhmän edustaja koki, että valmisteluaikaiset haasteet tunnistettiin, niistä opittiin, valmisteluprosessia parannettiin ja lopputuloksena oli hyväksyttävissä oleva lakipaketti. Jokaisella ryhmittymällä ja näkemyksellä on ollut oma roolinsa tiedustelulainsäädännön ympärillä käydyssä julkisessa keskustelussa. Kuvio 4 esittää, miltä roolit näyttivät kesällä ja syksyllä 2018, kun tiedustelulakipaketin luonnokset oli julkaistu.

Suurin osa keskustelusta käytiin tiedustelulakimietintöjen julkaisun jälkeen *Korostajien* ja *Laajentajien* välillä. Ihmisoikeuksia korostavien rooli keskustelussa oli pyrkiä varmistamaan, että niin tavallisten kansalaisten kuin vähemmistöjen ja heikoimmassa asemassa olevien ihmisoikeudet toteutuvat tiedustelulakipaketissa. *Korostajat* tunnustivat uudet turvallisuusuhat, kuten hybridivaikuttamisen, vakoilun ja väkivaltaisen ääriajattelun, mutta olivat epäileväisiä erityisesti tietoliikennetiedustelua kohtaan. *Korostajat* nostivat esiin lakien kehitysehdotuksia. He arvostivat esimerkiksi tiedustelutoiminnalle asetettavia kontrollimekanismeja ja pyrkivät vaikuttamaan, ettei tiedustelutoiminnassa rikottaisi esimerkiksi toimittajien lähdesuojaa. Heidän intressinään oli varmistaa, ettei viranomaisten käyttöön anneta suhteettoman suurta, piilossa toimivaa järjestelmää, joka mahdollistaa ihmisten perusteettoman valvonnan. Siirtymä rikosperustaisesta tiedonhankinnasta vakavien kansallisen turvallisuuden uhkien kartoittamiseen ja torjuntaan näyttäytyi *Korostajille* suurena muutoksena, joka väärin käytettynä heikentää ihmisten vapauksia demokraattisessa yhteiskunnassa. *Laajentajat* puolestaan keskittyivät

10 Tämä luku ja siinä esitetyt kehittämisehdotukset perustuvat julkaisuun Leppänen & Houtsonen (Hyväksytty julkaistavaksi). Kuvio 4 on laadittu tätä raporttia varten.

perustelemaan, miksi turvallisuusviranomaiset eivät selviä lakisääteisistä tehtävistään ilman uusia tiedustelutoimivaltuuksia. Heidän näkökulmastaan viranomaiset ovat kansalaisten puolella ja pyrkivät suojelemaan demokraattista yhteiskuntaa erilaisilta turvallisuusuhkilta. *Laajentajat* huomioivat myös ihmisoikeuksia, mutta heidän ensisijainen tavoitteensa on rakentaa turvallisuusviranomaisille muuttuneeseen toimintaympäristöön soveltuvat lailliset ja tehokkaat toimivaltuudet. *Laajentajat*, pyrkivät myös vastaamaan kysymyksiin ja tiedontarpeisiin, joita *Tasapainoilijat* ja *Korostajat* nostavat esiin.



Kuvio 4 Sidosryhmäasiantuntijoiden kolme näkökulmaa viranomaisten toimivaltuuksiin verkossa: Tasapainoilijat, Korostajat ja Laajentajat sekä näkökulmien roolit julkisessa tiedustelulakikeskustelussa.

Tasapainoilijat ja *Laajentajat* ovat näkemystensä osalta lähempänä toisiaan kuin *Korostajia*. Suurin syy samankaltaisuudelle on, että molemmat näkevät tiedustelulainsäädäntöluonnoksen onnistuneena ja tarpeellisena. Keskeinen ero ryhmien välillä syntyy *Laajentajien* keskittyessä ensisijaisesti perustelemaan tiedustelulainsäädännön tarpeellisuutta, *Tasapainoilijat* suuntautuvat tulevaisuuteen: miten tiedustelulainsäädäntö ja sen valvonta toimivat käytännössä, koska heille tärkeät kysymykset oli jo ratkaistu prosessin aiemmassa vaiheessa. *Tasapainoilijoiden* joukossa on mahdollisesti myös sellaisia vastaajia, jotka vielä tiedustelulakiprosessin alussa vastustivat tietoliikennetiedustelua, mutta ovat lopulta tyytyväisiä lainsäädäntöluonnoksen sisältöön. Ihmisoikeuksien turvaamisen lisäksi toinen keskeinen huoli tiedustelulakikeskustelussa oli yritysten asema ja siihen liittyvät kysymykset. Esimerkiksi epäselvyys, velvoitetaanko yritykset luomaan takaportteja ja luovuttamaan salauksenpurkuavaimia viranomaisille, mikä

heikentäisi yritysten liiketoimintamahdollisuuksia, huolestutti monia sidosryhmäasiantuntijoita lakivalmistelun ensimmäisessä vaiheessa. Lisäksi tarjolla oli kaksi kilpailevaa toimintastrategiaa: tiedustelulainsäädännön rakentaminen turvallisuusviranomaisten kannattaman strategian mukaan, ja tälle osin vastakkainen strategia, jossa erityisesti tietoliikennetiedustelusta pidättäytyminen nähtiin kilpailuetuna ja Suomesta toivottiin tiedon turvasatamaa, joka houkuttelisi esimerkiksi ulkomaisia datakeskusinvestointeja.

Jokaisella kolmella näkökulmalla on ollut tärkeä rooli suomalaisen tiedustelulainsäädännön kehitystyössä. On merkittävää tunnistaa kullekin näkökulmalle ominaiset ydinkysymykset, intressit ja arvot, joiden ymmärtäminen ja huomioiminen ovat olennaista. Sidosryhmät heijastavat mielipiteitä eri puolilta yhteiskuntaa ja julkisuudessa esitettyjä kannanottoja, joten niitä ei voi sivuuttaakaan, koska demokraattisessa yhteiskunnassa lait tarvitsevat taakseen laajan tuen. On epätodennäköistä, että sidosryhmät luopuisivat arvojensa ja intressiensä asettamista raameista. Esimerkiksi ihmisoikeuksien korostajat tulevat aina olemaan kiinnostuneita ihmisoikeuskysymyksistä ja lainsäädännön vaikutuksesta haavoittuvimpiin henkilöihin. Sen sijaan neuvotteluvaraa on siinä, miten rakennetaan lainsäädäntö, jossa sidosryhmien kynnyskysymykset on huomioitu hyväksyttävällä tavalla. Ongelmien lähestyminen ratkaisukeskeisesti mahdollisuuksia pohtimalla tuottaa luultavasti parempia tuloksia kuin keskittyminen erimielisyyksiin. Avoimuus, dialogi ja kompromissit vähentävät myös väärinymmärryksiä ja auttavat palauttamaan keskustelun painopisteen ongelmista ratkaisuihin. Hyvä esimerkki suunnanmuutoksesta on keskustelu tietoliikennetiedustelusta, jossa voimakas vastustus saatiin käännettyä hyväksynnäksi. Julkisista lähteistä on vaikea arvioida, millainen vuonna 2015 ehdotettu, vastustajien massavalvonnaksi leimaama malli todella oli, koska raportissa se kuvattiin hyvin niukasti rajat ylittävään verkkoliikenteeseen kohdistettavana signaalitiedusteluna. Haastattelujen perusteella on syntynyt käsitys, että avoimuuden puute laittoi liikkeelle väärinkäsityksiä, jotka saatiin vähitellen korjattua, kun hankkeen valmistelusta alettiin tiedottaa yksityiskohtaisemmin keskeisille sidosryhmille enemmän ja valmisteluun osallistui laajempi kirjo asiantuntijoita.

Julkinen keskustelu tiedustelun ympärillä toivottavasti jatkuu vielä. Listasimme julkaisussa Leppänen ja Houtsonen (Hyväksytty julkaistavaksi) joukon sidosryhmiin kohdistuvia odotuksia ja kysymyksiä, joihin vastaamalla tiedustelutoimivaltuuksien ympärillä käytävää keskustelua voisi kehittää tulevaisuudessa:

- Mitkä ovat tietoliikennetiedustelun havaitut vahvuudet ja heikkoudet? Kuinka hyvin tietoliikennetiedustelulla on onnistuttu täydentämään muita tiedustelumenetelmiä?
- Ovatko tiedustelun kustannukset pysyneet hallinnassa?
- Tutkimuksen osallistujat korostivat, että lainsäädäntöä on voitava kehittää tarvittaessa ja on ymmärrettävää, jos tiedustelulakipaketti tarvitsee muutoksia tulevaisuudessa. He odottavat, että viranomaiset pystyvät kertomaan avoimesti lainsäädännön kehitystarpeista sekä niihin johtavista syistä myös jatkossa.

- Vastaajat odottavat, että viranomaiset arvioivat aidosti, mitä tietoa tiedustelutoiminnasta voi kertoa julkisuuteen. Taktiikoista ym. yksityiskohdista tietoa ei ymmärrettävästi edes oleteta saavan, vaan osallistujat kaipaavat yleisemmällä tasolla olevaa tietoa tuloksista.
- Ovatko viranomaiset onnistuneet huolehtimaan tiedustelun kohteeksi joutuneiden henkilöiden oikeuksista ja onko siitä saatavilla ”todisteita”? Koetaanko tiedustelun valvonta toimivaksi?
- Kuinka hyvin tietoliikennetiedustelun kohdentamisessa on onnistuttu vai uhkaako se luisua massavalvonnan puolelle?

8 YLIOPISTO-OPISKELIJOIDEN JA HENKILÖKUNNAN NÄKEMYKSIÄ VIRANOMAISVALVONNASTA VERKOSSA

Tässä osiossa analysoimme kysely- ja haastattelututkimuksiin osallistuneiden yliopisto-opiskelijoiden ja henkilökunnan näkemyksiä poliisin ja tiedusteluviranomaisten toimivaltuuksista kerätä, säilyttää ja analysoida tieto- ja viestintäverkoista ja niihin kytketyistä laitteista saatavaa tietoa seuraavan viiden pääkysymyksen kautta:

1. Mitä osallistujat ajattelevat poliisin ja tiedusteluviranomaisten harjoittaman tiedonhankinnan ja valvonnan verkossa olevan? (haastattelut)

2. Missä olosuhteissa, jos missään, ja millä ehdoilla he voisivat hyväksyä viranomaisten toimivaltuudet verkossa? (haastattelut ja kysely)

3. Huolestuttaako viranomaisvalvonta heitä? (kysely)

4. Mitä turvallisuusviranomaisten pitäisi kertoa tiedonhankintamenetelmistään ja niiden käytöstä? (haastattelut ja kysely)

5. Missä määrin osallistujat kokevat luottavansa viranomaisiin? Miten he perustelevat luottamustaan tai epäluottamustaan? (haastattelut)

Suluissa on kerrottu millä aineistolla kuhunkin pääkysymykseen on etsitty vastauksia. Haastatteluja on analysoitu teemoittain ja kyselytuloksia suorien jakaumien avulla. Tulokset käsittelevät osallistujajoukkomme näkemyksiä, eikä niiden perusteella pysty tekemään koko väestöä tai kaikkien suomalaisten yliopistojen opiskelijoita ja henkilökuntaa koskevia johtopäätöksiä. Luultavasti erityisesti kyselyyn on valikoitunut vastaajiksi henkilöitä, joilla saattaa olla keskimääräistä voimakkaampia mielipiteitä turvallisuusviranomaisten toimivaltuuksista verkossa. Havaitsemamme mielipiteet ja käsitykset ovat kuitenkin johdonmukaisia ja uskottavia ja niissä näkyy myös selkeää hajontaa. Tulokset ovat tärkeitä, koska ne havainnollistavat, millaisten kysymysten ja kannanottojen ympärille laajemmat kansalaismielipiteetkin luultavasti muodostuisivat.

8.1 Osallistujien tausta

Kysely

Kyselyyn osallistui suomalaisista yliopistoista yhteensä 236 vastaajaa, joista suurin osa, 201, oli opiskelijoita (Taulukko 2). Henkilökunnaksi määriteltiin vastaajat, jotka työskentelivät yliopistolla opettajina, tutkijoina tai teknisenä, hallinnollisena tai muuna henkilöstönä, mutta eivät olleet samanaikaisesti opiskelijoita. Heitä oli 35. Kaikista vastaajista 40 oli tutkijoita tai opettajia. Tässä joukossa oli mukana myös 23 vastaajaa, jotka olivat samalla opiskelijoita. Opiskelijat olivat tyypillisesti

iältään nuoria, alle 25-vuotiaita ja heillä oli enintään kandidaatin tutkinto suoritettuna. Henkilökunnan osalta vastaajat painottuivat nuorehkoihin maistereihin tai maisterin tutkintoa suorittaviin, joten kysely ei juurikaan tavoittanut varttuneempaa henkilöstöä.

Taulukko 2 Kyselyn osallistujien (n=236) taustatiedot.

	Opiskelija	**Henkilökunta***
Sukupuoli		
Nainen	90	9
Mies	85	19
Muu/ei vastausta	26	7
Yhteensä	201	35
Korkeakoulututkinto		
Enintään kandidaatin tutkinto	100	6
Enintään maisterin tutkinto	58	20
Tohtoriopiskelija tai tohtori	5	6
Ei tietoa	38	3
Yhteensä	201	35
Ikäryhmä		
20-24	110	3
25-34	69	17
35 tai vanhempi	22	15
Yhteensä	201	35

* Henkilökuntaan luokiteltiin vain ne vastaajat, jotka eivät olleet samalla opiskelijoita. Opiskelijoista 30:llä oli myös jokin työtehtävä yliopistolla, mutta heidät esitetään opiskelija-kategoriassa.

Kyselyssä oli numeeristen kysymysten lisäksi useita tarkentavia avoimia kysymyksiä. Näihin annettujen vastausten perustella syntyi vaikutelma, että vastaajien (n = 236) joukossa on useita henkilöitä, jotka ovat tietoisia tietojärjestelmiin ja -verkkoihin liittyvistä tietoturvallisuuden ja yksityisyyden kysymyksistä, mutta tiedot suomalaisten turvallisuusviranomaisten toimivaltuuksista verkossa olivat sen sijaan vähäisiä. Avovastauksissa nostettiin esiin usein tiedotusvälineiden kautta paljon julkisuudessa olleet uutiset yksityisyyden loukkauksista, tietovuodoista, verkkorikoksista ja eri valtioiden tiedusteluviranomaisten harjoittamasta hyvin vahvasta valvonnasta. Myös seuraavassa luvussa esitetyt haastatteluanalyysit kertovat siitä, ettei suomalainen tiedustelulainsäädäntö ole kovin tuttu monellekaan tutkimukseen osallistuneelle. Ihmiset saattavat kuitenkin paikata nämä tiedon aukot uutisista ja verkkokeskusteluista lukemillaan jutuilla ja keskusteluilla ulkomaisten viranomaisten harjoittamasta tiedonhankinnasta.

Haastattelut

Kahdestakymmenestä haastateltavasta yliopistolaisesta kymmenen oli opiskelijoita ja kymmenen kuului henkilökuntaan (Taulukko 3). Miehiä ja naisia oli yhtä paljon. Henkilökunnan vastaajista suurin osa (6) oli suorittanut tohtorin tutkinnon,

kun taas opiskelijoista viidellä ei ollut vielä mitään valmista korkeakoulututkintoa. Opiskelijavastaajat painottuivat nuoriin, alle 30-vuotiaisiin. Henkilökunnasta puolestaan puuttuivat alle 30-vuotiaat vastaajat kokonaan ja kuusi haastateltavista oli 40-vuotias tai vanhempi.

Taulukko 3 Haastattelun osallistujien (n=20) taustatiedot.

	Opiskelija	**Henkilökunta**
Sukupuoli		
Nainen	6	4
Mies	4	6
Yhteensä	10	10
Korkeakoulututkinto		
Ei tutkintoa	5	1
Kandidaatin tutkinto	4	1
Maisterin tutkinto	1	2
Tohtorin tutkinto	0	6
Yhteensä	10	10
Ikäryhmä		
20-29	7	0
30-39	2	4
40 tai vanhempi	1	6
Yhteensä	10	10

Kysyimme haastattelun lopuksi vastaajilta, tuntevatko he uutta tiedustelulakipakettia ja jos tuntevat, niin minkä verran, seurasivatko he lainvalmistelua ja tietävätkö, mitä muutoksia tiedustelulakipaketti aiheutti sekä mille viranomaisille. Jaottelimme vastaajat vastausten perusteella kahteen pääryhmään: ”Tuntee tiedustelulakeja” (n = 5) ja ”Ei juurikaan tunne tiedustelulakeja” (n = 15). Esitämme tulokset näiden kahden ryhmän mukaisesti, koska siviili- ja sotilastiedustelulainsäädännön tuntemus heijastuu vastaajien käsityksiin viranomaisvalvonnasta verkossa.

Selvästi suurin osa vastaajista myöntää, ettei juurikaan tunne Suomen uutta tiedustelulainsäädäntöä. Monet tähän kategoriaan luokitelluista vastaajista kertoivat kuulleensa lakipaketista, ja osa muisti lukeneensa siitä esimerkiksi lehtijuttuja, mutta he eivät osanneet eritellä tarkemmin sen sisältöjä, kuten millaisia toimivaltuuksia lakipaketti antoi eri viranomaisille. Kategoriaan kuului myös vastaajia, jotka kuulivat haastattelussa ensimmäistä kertaa lakimuutoksesta. On huomionarvoista, että muutamalla tähän kategoriaan luokitellulla vastaajalla on tietoturva-asiat erityisen hyvin hallussa ja sitä kautta ymmärrystä, kuinka viranomaiset voivat saada tietoa kansalaisten tieto- ja viestiliikenteestä, vaikka lakisisällöt eivät ole niin tuttuja. Sitaateissa O-alkuiset vastaajat ovat opiskelijoita ja H-alkuiset henkilökunnan jäseniä.

> *”En oo [seurannut]. Tän tiedustelulakipaketin oon otsikkona kuullu, mutta et en oo silleen perehtyny, et mitä se sisältää. Mut et muistan kyllä, et siit on paljon just lehissä kirjotettu ja on ollu silleen, iso aihe. Mutta et nyt on vähän laantunu se keskustelu. [...] Mut et ei oo mitään sisällöst jääny mieleen.” O10: NAINEN*

”Nyt tuli kyllä aivan uusi termi [nauraa]. En oo seurannu. Mutta varmasti pitää kyllä ainakin googlettaa [nauraa], ja perehtyä vähän.” O1: NAINEN

”Seurasin hyvin heikosti. En oo oikein selvillä siitä. Se voi osittain johtua omasta laiskuudesta tai sitten, että se oli asiana hankala ja poliittisesti jotenkin tavallaan. Sitä ei jotenkin käsitelty julkisuudessa avoimesti ja esitetty niitä tietoon perustu- tai tietoja siitä, että mitä se tarkoittaa, kovin selkeesti. Oon aika huonosti perillä asiasta. [...] Mun käsittääkseni se oli, poliisin ja suojelupoliisin toimintaan. Mun mielestä siinä ei puhuttu puolustusvoimista. Näiden kahden.” H10: NAINEN

Vastaaja H4:n tietämys tiedustelulakipaketista edustaa tämän kategorian selkeää parhaimmistoa: hän kertoo seuranneensa lainvalmistelua ja muistaa muutaman yksityiskohdan lukemastaan, mutta ei aivan yllä samalle tasolle kuin he, joiden luokiteltiin tuntevan tiedustelulait.

”Kyllä mä sitä seurasin siinä määrin mitä sitä uutisoitiin esimerkiks Hesarissa, niin kyllä mä niitä uutisia siitä luin. Mut siitä ehkä jäi silti, siitä uutisoinnista, vähän epäselkeä kuva, että mitä siinä nyt sitten loppupeleissä päätettiin. Ja miten tavallaan sit käytännöntasolla ne muutokset siitä lainsäädännöstä vaikuttaa ihmisten yksityisyydensuojaan. [...] Siis käsittääkseni suojelupoliisille tuli [uusia toimivaltuuksia]. Sitten mun mielestä siinä tuli myös jotain puolustusvoimien toteuttamalle tiedustelulle. Ainakin jossain kohtaa mun mielestä puhuttiin tästä, että missä määrin puolustusvoimat voi toteuttaa tiedustelua kotimaassa, mutta en kyllä tarkalleen muista, että mitä siinä muuttuu.” H4: MIES

Neljä osallistujaa sanoi seuranneensa tiedustelulakiprosessia jo pidemmän aikaa. Heillä oli enemmän tietoa aiheesta kuin ryhmällä, joka ei tuntenut lakeja sekä tyypillisesti selkeä mielipide joko lakien sisällöstä, tarpeellisuudesta tai valmisteluprosessista. Seuraaminen oli tapahtunut pääosin median ja sosiaalisen median välityksellä, mutta myös lainvalmisteluasiakirjojen kautta, ja pienessä mittakaavassa osallistumalla jopa itse aiheesta käytyyn julkiseen keskusteluun. Viides vastaaja kertoi perehtyneensä aihepiiriin tähän tutkimukseen osallistumista varten. Tiedustelulakeihin tutustumisesta huolimatta myös nämä osallistujat kokivat, että tiedustelutoimivaltuudet eivät ole aiheena selkeä ja helposti ymmärrettävä.

”Hyvinkin aktiivisesti silloin ja myöskin nyt jälkikäteen. Sekä uutislähteistä, mut ennen kaikkee ni ihan noista ministeriöiden ja poliittisten päätöksentekoelinten asiakirjalähteistä. [...] Se on just tää Supon roolin uusi muuttuminen puhtaasti tiedusteluorganisaatioksi sekä sitten puolustusvoimien tiedustelupuolelle näitä verkkoliikenteen oikeuksia siinä valtion rajan ylittävässä viestinnässä. Ja sitten tietenkin siihen liittyvä tää valvontaviranomaiskuvio.” O9: MIES

”Yritin kyllä seurata tosi paljon, se oli musta, niinku mä sanoin, se oli tosi tärkee kysymys koska se paaluttaa niitä asioita tosi pitkälle tulevaisuuteen, ja just kun siinä tiedustelulakipaketissa oli hirveen paljon hyvää, joka olis

pitäny säätää jo aikaa sitten, niinku tää ulkomaantiedustelu ja kaikki. Sitten siellä oli tää, mitenkä tää verkkoseuranta nyt päätettiin toteuttaa, mikä oli musta aivan totaalinen susi, eikä olis ees pitäny olla siinä paketissa, vaan olis saanu olla erillinen juttu, joka oltais säädetty pitkän kaavan mukaan, jos oltais säädetty lainkaan, niin kuin tuossa muodossaan. Kyllä mä tosi paljon seurasin ja saatoin siitä nettiin jonnekin palstoille tai uutiskommentteihin jotain huudellakin." H1: MIES

"Mä seurasin sitä eduskunnan kautta ehkä enimmäkseen, ja valtioneuvoston tiedotteista ja muista kautta. Se oli ehkä semmonen vähän enemmän pro-lähestyminen, versus johonkin henkilöön, joka ei opiskele politiikkaa." [...] Lähtökohtasesti mä olen itte sitä mieltä, että tiedustelulaki tarvittiin. Se ois tarvittu jo jokin aikaa sitten taaksepäin. Mutta, se mikä oli mielenkiintosta että, sen lopulliseen muotoutumiseen ja läpimenoon vaikutti niin paljon, esimerkiks Turun puukotukset ja muut tommoset terroriteot, millä saatiin vähän epätavallisella menettelyllä eduskunnassa nopeesti läpi. [...] Ydin käsittääkseni on se, et ylipäätään pystytään tekemään verkkotiedustelua kansainvälisesti, tekemään kansainvälisiä avunpyyntöjä. Tällä hetkellä, tai tähän mennessä Suomen tiedustelu, sanotaan tommonen valtiotason tiedustelu, on ollu aika hampaatonta, juuri sen takia että siellä ei oo ollu näitä lakityökaluja takana." O8: MIES

8.2 Käsityksiä viranomaisten harjoittamasta tiedonhankinnasta verkossa

Jokaisen haastattelun alussa selvennettiin, että tutkimuksemme kohde on valtion viranomaisten, kuten poliisin ja tiedusteluviranomaisten, harjoittama tiedonkeruu ja valvonta tietoverkossa. Kerroimme, että kysymykset koskevat sitä, miten poliisi ja tiedusteluviranomaiset keräävät, analysoivat ja säilövät netistä sekä nettiin kytketyistä laitteista saatavaa tietoa. Sen jälkeen vastaajia pyydettiin kuvailemaan, minkälaista toimintaa he ajattelevat tämän olevan ja mitä tietoja he arvelevat viranomaisten saavan esimerkiksi älypuhelimesta.

Tiedustelulakeja tuntemattomat vastaajat

Suurimmalla osalla haastateltavista oli vain vähän tietoa suomalaisten viranomaisten toimivaltuuksissa verkossa, valvonnan mahdollistavista teknologisista ratkaisuista ja tiedustelulakipaketin sisällöistä. Tietämättömyys näkyy suppeina ja epävarmoina vastauksina, jotka pysyttelevät yleisellä tasolla menemättä yksityiskohtiin. Vastaajat kuvaavat poliisitoimintaa tuomatta juurikaan esiin suojelupoliisin ja puolustusvoimien harjoittamaa siviili- ja sotilastiedustelua. Joukossa oli lisäksi muutama vastaaja, joilla oli hyvät pohjatiedot teknologiasta ja sitä kautta ymmärrys, millaista tietoa on saatavissa teknisellä tasolla, vaikka eivät aina pystyneet kertomaan, onko se mahdollista lain puitteissa.

Vastaaja H7:n käsitys kotimaisten viranomaisten toimivaltuuksista sekä tapa vastata epäröiden ja epäillen, on hyvin tyypillinen. Hän liittää viranomaisten toimivaltuudet verkossa ensisijaisesti rikosten selvittämiseen ja ennaltaehkäisyyn.

Vastaaja arvelee, että toimintaan tarvitaan oikeuden päätös ja lupien saamisen edellytykset liittyvät rikoksen vakavuuteen eli hän tuntee poliisitoiminnan perusviitekehyksen, mutta kokee verkkoympäristön haastavaksi. Hän ajattelee, että viranomaiset pääsevät käsiksi puhelujen ja viestien lisäksi myös sosiaalisen median palveluihin. Hän tiedostaa, että viestintää voi myös salata, jolloin viranomaisten pääsy viestiliikenteeseen heikentyy. Vastaaja on myös sikäli tyypillinen, että hän ei oma-aloitteisesti erottele puheessaan sitä, hankkivatko viranomaiset viestin välitystietoja (esimerkiksi viestinnän osapuolet ja kellonajat) vai sisältöjä.

> *”Varmaan siis olettaisin, että liittyen vaikkapa rikosten selvittämiseen ja ennaltaehkäisyyn. Ehkä, joitakin ihmisryhmiä voitas tarkkailla, heidän toimintaansa siellä. [...] Siis mä en todellakaan tiedä, hyvin tätä aihepiiriä tunne. Mun käsittääkseni siinä tarvitaan ehkä oikeuden päätös, että voi ikään kuin seurata vaikka jonkun viestintää verkossa. Että se ei käy... siis Suomen viranomaiset ei voi automaattisesti lähtee seurailee ketään yksityishenkilöä, käsittääkseni. [...] Täytyy olla rikos, josta rangaistus on tietty maksimi- tai minimirangaistus, jotta voi ees sellasta esittää, että sais kerätä sitä tietoo. Mutta, en mä siit sen tarkemmin tiedä. […] Siis älypuhelimissahan on ihmisillä nykyisin koko elämä. Et kyllä sieltä varmaan vois saada vaikka mitä, jos ihminen ei ikään kuin epäile mitään, tai ei osaa varoa. Että puhelut, viestit, WhatsApp-viestit, kaikki sosiaalisen median käyttö, varmaan siitä pystyis seuraamaan aika kattavasti. Mut et kyllä varmaan myös sit ihmisillä on keinot näitä salata. Ja siis sähköposti tietenki. Mut et kyllähän näitä pystyy salaamaankin.” H7: NAINEN*

Paikannustiedot, tekstiviestit ja sosiaalisen median käyttö ovat asioita, jotka vastaajat tyypillisesti osasivat nimetä tiedoiksi, joita viranomaiset voivat hyödyntää. Vastaaja O10 myöntää, ettei hänellä ole selkeää käsitystä viranomaisten toimivaltuuksista verkossa, mutta kertoo oppineensa poliisisarjoista, että viranomaiset voivat esimerkiksi hankkia puhelimen paikannustietoja ja tekstiviestejä sekä tietoja kohdehenkilön sosiaalisen median käytöstä. Osallistuja ei tiedä, kuinka tieto hankitaan, mutta arvelee, että viranomaiset voisivat ostaa kaupallisten toimijoiden tallentamaa tietoa.

> *“No varmaan semmosta, että kun ihmiset tuolla vaikka somessa pyörii, niin valtio pystyy sit sitä kautta ehkä jotenki keräämää sitä dataa itelleen. Ehkä, en tiiä onko samalla lailla ku miten yritykset pystyy, mutta ainakin jollain määrin pystyy sit yrityksiltä ostamaan sitä tietoo. […] Poliisisarjoista oon kuullut, että just tekstiviestejä ja tommosii, puhelimen kautta pystyy seuraa, et missä on vaikka liikkunut, tai tommosia. […] En tiiä, et miten sit pääsee vaik siihen et mitä sovelluksia on ladannu tai käyttäny, nii miten sitä pystyis seuraan.” O10: NAINEN*

Myös haastateltavat O3 ja O1 pohtivat, voivatko suomalaiset viranomaiset päästä ulkomaisten sovellusten, kuten WhatsAppin ja Facebookin kautta käytyyn viestintään, ja jos voivat, niin miten se tapahtuu. O1 arvelee, että yritys voi itse vaikuttaa siihen, minkälaista dataa se kerää ja luovuttaa viranomaisille. O3 pohtii tallentavatko tallentuvatko keskustelut jonnekin.

”Niin, niitä että mitenkä joku sovellus kerää erilaista dataa ja säilyttääkö ne sitä miten pitkään, esimerkiks semmosiin mä kuvittelisin, että jossakin tilanteessa varmasti on myös viranomaisilla pääsy. Mut mä luulen, et se on myös riippuvainen siitä, että esimerkiks Facebookhan on hirmu tarkka, että miten se antaa käsitellä yksilöiden dataa, ja esimerkiks vaikka näitä Messengerissä käytyjä pikaviestikeskusteluja, että sen mä luulen, että on sitten vähän eri prosessi, et miten sieltä saa ne käsiinsä.” O1: NAINEN

”Mutta en tiedä sitten, että jos ne on vaikka yhdysvaltalaisia palveluita, niin miten sitten niitä tietoja vaikka Suomen viranomaiset voi saada, jos tarvitsee vaikka jotain keskusteluja eikä jotenkin niitä oo. En tiedä, onko näissä keskusteluissa ja muissa, vaikka datan lähettämisessä muuten, jotain varmuuskopiointia jonnekin.” O3: NAINEN

Joukossa oli myös vastaajia, jotka kokivat tietonsa niin hatariksi, etteivät halunneet antaa edes arviota, milloin poliisi ja tiedusteluviranomaiset voivat kerätä ja hyödyntää tieto- ja viestintäverkoista tai niihin kytketyistä laitteista saatavaa dataa. Esimerkiksi osallistuja H2 on varma, että toiminta on säädeltyä, mutta hän ei tiedä miten. Vastaaja O6 puolestaan on epävarma siitä, onko Suomessa ylipäätään mitään sääntelyä asiasta.

”En osaa yhtään sanoa, mikä niiden toimintatapa on ja mitä rajoituksia niille on asetettu. [...] En osaa sanoa, mikä kriteeristö paikallispoliisilla on käytössä. Tai poliisilla ja Suomen valtiolla, mutta varmasti toimintaa säätelee jotkin protokollat.” H2: MIES

”Mä en ole tietoinen, että onks täs mitään lainsäädäntöö, mikä yhtään rajoittais viranomaisten mahdollisuutta seurata tätä, joten en osaa oikein sanoa.” O6: NAINEN

Vastaaja O5 mieltää viranomaisten harjoittaman tiedonkeruun ja valvonnan massavalvonnaksi, jolla profiloidaan ihmisiä ja paikannetaan esimerkiksi terroristeja. Tiedustelulakeja tuntemattomien vastaajien ryhmässä hän on ainoa, joka puhuu suoraan massavalvonnasta. O7 käyttää puolestaan ilmausta *NSA-tyyppinen tiedustelu*. O5 ei täysin luota tietämykseensä suomalaisten viranomaisten toimivaltuuksista, mutta arvelee, että ne voivat saada älypuhelimesta teletunnistetietojen ja tekstiviestien lisäksi applikaatioiden viestejä.

”No siis mä oon ymmärtäny, että se ois semmosta massavalvontaa, millä etsitään jotain tietynlaisella profiloinnilla olevia ihmisiä. Esim. jotain terroristeja. [...] No, en tiedä Suomen viranomaisista. Ainakin jotain teletunnistetietoja saa, ja sitten lähetettyjä tekstiviestejä. Kyllähän näitä WhatsApp-viestejäkin, tai jotain Facebook-viestejä, on käytetty käsittääkseni jossain, tuomioistuimen päätöksessä ihan. Ilmeisesti tämmösiä saa.” O5: MIES

Haastateltava H8 hallitsee tietoturva-asiat ja on jonkin verran perillä poliisin rikosperustaisista toimivaltuuksista. Hän tekee selkeän eron esimerkiksi reaaliaikaisen viestintään kohdistuvan kuuntelun ja takavarikoidun laitteen tutkimisen välillä,

mutta ei ole varma, saako poliisi tarkkailla epäillyn laitteita reaaliaikaisesti murtautumalla niihin.

> *”Toki sitten kun on se tietty rikosepäily ja tuomioistuimen päätös, niin sen jälkeen voidaan alkaa kuunteleen puheluita. Sit on paikkatietoo, yksi. Siitä mä en oo nyt ihan varma, että miten se meni, et voidaanko sen pidemmälle mennä, eli sen ihan laitteen sisälle tietyillä edellytyksillä, et sitä itse laitetta tarkkaillaan. Siihen mä en oo nyt niin tarkkaan perehtynyt, et osaisin siihen sanoo suoraan, mitenkä se meni Suomessa. Kyllähän se sillain ainakin on, että laite voidaan takavarikoida ja sen jälkeen voidaan tarkkailla, tai katsoa että mitä siellä laitteessa on.” H8: MIES*

Osallistuja H9:llä on ICT-taustaa. Hän osaa kertoa poikkeuksellisen yksityiskohtaisesti, miten operaattorit ovat velvollisia luovuttamaan viestinnän välitystietoja poliisille, jos tietoihin on hankittu lupa. Osallistujalla on selkeästi myös käsitys, miten eri laitteet jättävät jälkiä ja miten niistä on teknisesti mahdollista saada tietoa. Hän kuvailee miten tietoliikenteen jäljet voivat johtaa harhaan ja kertoo analysoineensa oman kotiverkkonsa tietoliikennettä kiinnostuksen vuoksi. Osallistuja on myös hyvin perillä viestien salaamisesta, eikä luota esimerkiksi ilmaisten sähköpostipalvelujen tarjoamiin salausratkaisuihin. Vankasta ICT-osaamisesta huolimatta hän ei ole perehtynyt juurikaan tiedustelulainsäädäntöön.

> *”Siis mul on käsitys, että siihen tarkkailuun tarvitaan lupa joka tapauksessa, esimerkiks puhelinkuunteluun tai sit verkkoliikenteen seurantaan, koska verkkoliikenteen seuranta on operaattoririippuvaista ja operaattorilla pitää olla joku paperi siihen takataskussa, että minkä takia ne antais tietoja ulos. [...] No just puhelin- ja verkkoliikenne ylipäänsä, et kyllähän sieltä operaattoritiedoista saadaan aika paljonkin dataa ulos loppupeleissä, et sielt saa pelottavankin paljon tietoo pihalle. Lähdeosoite, kohde-osoite, käytetty protokolla. Tosin protokollia nyt voidaan sit jemmata toisten sisään, mut se on toinen tarina. Nää perustiedot. Toki sieltä pystyy sitten myöskin kuunteleen ihan sivusta sitä liikennettä. Sekin on mahdollista. Verkkoliikenteen analysointiin on olemassa ihan hyvii työkaluja. Vaikka en ole ammattilainen, niin tiedän ja olen käyttänyt joskus ihan kokeilutarkoituksessa, että mitä kaikkee oikeesti kotiverkossa liikkuu. […] Jos sulla on älypuhelin taskussa, niin sä oot hävinny pelin joka tapauksessa. [nauraa] Mutta no, siitähän nyt saa paikkatiedot, jos sulla on GPS päällä, mastojen perusteella joka tapauksessa pystytään tekee jonkinlaista kolmiomittausta, missä sä suurin piirtein oot. Ja se nyt riippuu ihan siitä, et mitä sä sillä puhelimellas puuhastelet. On olemassa liikennettä jota ilmeisesti ei pysty saamaan selville, mitä näit on näitä.. no WhatsApp on yks. Se on mun omassa mielessä siinä hilkulla, että onks se mukamas salattua vai ei, ja sit toinen oli tää, venäläisten tekele. […] Periaatteessa kaiken liikenteen pystyy kryptaamaan. Mut sit taas kun käytetään jotain julkisia, ilmaisia sähköpostipalvelimia, niin kun Googlee tai vastaavia, niin me ollaan taas hävitty tää peli. H9: MIES*

Jotkut vastaajat, kuten H10, tunnistavat, että poliisin lisäksi myös suojelupoliisi tekee tiedonhankintaa verkossa. Hän arvelelee, että siihen liittyy esimerkiksi

terrorismiin viittaavien avainsanojen etsintä sosiaalisen median lähteistä. Hän osaa myös eritellä, että viestinnästä voi saada sekä välitystietoja että sisältötietoja.

> *”No, se tarkoittaa ihmisten, esimerkiks sähköpostien lähettämistä, sitä koskevia sisältöjä ja, keille tai keiden välillä sitä viestintää tehdään. Ehkä siihen kuuluu, en oo ihan varma, myös some ja tällainen, julkisempi kirjoittelu, jossa ehkä sitten etsitään avainsanoja, jotka esimerkiks liittyy vaikka terrorismiin tai tän tyyppiseen toimintaan. Keskusteluryhmät joissa esimerkiks voidaan, vaikka vaihtaa tietoja. Johonkin terrorismiin liittyvästä toiminnasta tai tän tyyppisistä asioista. […] Tietysti [yllä kuvattu liittyy] poliisin toimintaan, myös supon tai mikä se nyt nykyään onkaan. Lähinnä heidän toimintaan.” H10: NAINEN*

Tiedustelulakeja tuntevat vastaajat

Tiedustelulakeja tuntevat vastaajat pystyivät rakentamaan pääsääntöisesti monipuolisen kontekstin viranomaisten tiedonkeruulle verkossa ja tunnistivat, että kyse voi olla rikostutkinnan lisäksi suojelupoliisin tai puolustusvoimien suorittamasta tiedustelusta, joka tähtää vakavien kansallisen turvallisuuden uhkien torjuntaan. He heijastavat ajatuksiaan enemmän siihen, mikä on laissa sallittua kuin mikä on teknisesti mahdollista. Tiedustelulakien tuntemuksesta huolimatta tämänkään ryhmän vastaajat eivät ole täysin varmoja, ovatko heidän käsityksensä oikeita.

Vastaaja O9 suhtautuu omien sanojensa mukaan viranomaisten toimivaltuuksiin harjoittaa tiedonkeruuta tietoverkossa *”kansalaisvapauslähtöisesti”* ja *”kohtalaisen kriittisesti”*. Hän ajattelee, että, että viranomaiset voisivat esimerkiksi siepata tietoliikennettä, kohdistaa siihen semanttisia hakuja ja purkaa salauksia. Hän tunnistaa, että tiedustelulakien myötä viranomaisten on mahdollista tarkkailla Suomen rajat ylittävää tietoliikennettä.

> *”No, se voi tarkottaa tällasta sosiaalisen median tietojen mahdollista keräämistä, tai sit se voi tarkottaa tällasen viestiliikenteen, esimerkiks sähköpostien tai muitten sovellusten kautta tapahtuvan viestien sieppaamista ja tän tiedon käsittelyä. Ainakin, erilaisia näitä tunnistetietoja, eli näitä että mitä laitteita on käytetty, missä on käytetty. Sit käsittääkseni pystytään uusien lakien mukaan myös jonkuntyylisiä semanttisia hakuja tekemään, eli siis kieleen liittyviä tunnisteita käyttämään ja hakemaan tietoja. Ja myös, murtamaan salauksia silloin kun se on mahdollista. Näissä tiedustelulaeissa käsittääkseni, kun tämä ylittää tämän Suomen rajan, niin siirrytään tähän, että pystytään purkamaan ja nappaamaan tätä tietoa.” O9: MIES*

Myös osallistuja H1 kertoo suhtautuvansa tiedustelulakipaketin tuomiin muutoksiin kriittisesti. Hän kutsuu toimintaa massavalvonnaksi ja ajattelee, että kaikki Suomen rajat ylittävä verkkoliikenne suodatetaan. Lisäksi hän arvelee, että poliisi voi käyttää vakoiluohjelmia kerätessään tietoa yksittäisten kansalaisten laitteista.

> *”No, meidän kontekstissahan se nykyään tarkoittaa käytännössä nettiliikenteen massavalvontaa eli kaikki Suomen rajat ylittävä liikennehän nykyään suodatetaan ja sitten sieltä poimitaan näillä tietyillä kriteereillä, ensin*

automaattisesti ja sen jälkeen vielä ihmisten toiminnan kautta, niitä tiettyjä viranomaisia kiinnostavia seikkoja. Näistä kriteereistä nyt ainakin, et mistä liikenne tulee ja minne se menee, niin sen perusteella niitä kai suodatetaan ja, varmaan sitten on muitakin mutta niistä ei oo kauheesti julkisuudessa ollu. Sitten toinen on, eikös mun käsittääkseni nyt poliisi saanu myös tän oikeuden käyttää vakoiluohjelmia siten, että kansalaisten laitteita voidaan myös vakoilla suoraan." H1: MIES

Osallistuja H6 tulkitsee viranomaisten harjoittaman tiedonkeruun ja valvonnan luvanvaraiseksi hakusanaperustaiseksi tiedon massakeruuksi. Tiedustelulainsäädännön ja massamittaisen keruun kontekstissa hän puhuu ennen kaikkea puolustusvoimista, mitä oheinen sitaattikin kuvaa. Hän tunnistaa poliisin rikosperustaisen tiedonhankinnan kohdennetummaksi toiminnaksi kuin sotilas- ja siviilitiedustelu.

"En oo ihan varma, että mihin kaikkeen, tai missä tilanteessa se [puolustusvoimien tiedustelua koskeva] lupa on. Onko se tällä hetkellä yleisellä tasolla oleva lupa, että voi suodattaa kaikkea viestinvälitystä vai että pitääkö se yksilöidä erikseen, että missä se tieto kulkee. Mun käsitykseni puolustusvoimien tiedustelusta nojaa siihen massa..työhön, tai ainakin sen kaiken järjen mukaan pitäs nojata massatyöhön, jos muistelee niitä argumentteja, millä tiedustelulakeja Suomessa ajettiin läpi, ja se oli nimenomaan ehkäistä, mahdollisia turvallisuusuhkia, joita Suomeen kohdistuu. Jos niitä halutaan ehkäistä, tarkottaa sitä, et pitää silloin seuloa massasta mahdollisia osumia, joita sitten on syytä tarkastella lähempää." H6: MIES

8.3 Vakavien rikosten tutkinta oikeuttaa tiedonhankinnan

Viranomaisten harjoittaman tiedonhankinnan hyväksyttävyyttä käsiteltiin sekä haastatteluissa että kyselyssä. Haastatteluissa teema esitettiin yksityisyyden näkökulmasta, kun osallistujia pyydettiin esimerkiksi kertomaan, onko heidän mielestään olemassa tilanteita, joissa henkilö voi menettää oikeutensa yksityisyyteen verkossa. Kyselyssä vastaajat arvoivat tiedonhankinnan hyväksyttävyyttä skenaarioiden pohjalta eri tilanteissa. Esittelemme ensin haastattelujen ja sen jälkeen kyselyn tuloksia.

Kaikki haastatteluaineistomme vastaajat pitivät yksityisyyden rajoittamista verkossa hyväksyttävänä, jos sitä tarvitaan vakavimpien rikosten tutkimiseen tai yksilöidyn, jo tunnistetun vakavan rikoksen pysäyttämiseen. Vastaavasti mitä lievemmästä rikoksesta tai epäilystä oli kyse, sen kriittisemmiksi vastaajat pääsääntöisesti kävivät. Henkirikosten osalta vallitsi yksimielisyys, että ne ovat vakavia rikoksia, mutta muutoin se mitä yksi piti vakavana rikoksena, saattoi olla toiselle lievä. Seuraavaksi eritellään tilanteita, joissa vastaajat haarukoivat heidän mielestään tiedonhankinnan hyväksyttävyyden rajoja. Sitaatit on ryhmitelty jälleen sen perusteella, tunteeko vastaaja tiedustelulakeja vai ei.

Tämä luku osoittaa myös joitakin eroja vastaajien puhetavassa sen perusteella, tuntevatko he tiedustelulakeja vai eivät. Eroja on nähtävissä läpi haastattelujen. Tiedustelulakien etenemistä seuranneiden vastaajien puheesta on tunnistettavissa osin samaa retoriikkaa kuin tiedustelulakien ympärillä käydyssä julkisessa asiantuntijakeskustelussa. Sen sijaan tiedustelulakeja tuntemattomat haastateltavat eivät hallitse vastauksissaan asiantuntijatermistöä yhtä hyvin eivätkä sido vastauksiaan

voimassaoleviin lakeihin Suomessa. Vaikka käytetty kieli on analyysimme kannalta sivujuonne, johon ei ole keskitytty systemaattisesti, halusimme tuoda havaitsemiamme käsitteiden käyttöön liittyviä eroja esille, koska ne saattavat hämärtää osapuolten välisen viestinnän ymmärrettävyyttä ja johtaa väärinkäsityksiin.

Tiedustelulakeja tuntemattomat vastaajat

Vastaaja O5 kokee oikeusturvan parantuvan, jos viranomaisilla on mahdollisuus tutkia vakaviin rikoksiin liittyviä verkkojälkiä. Henkeen ja terveyteen liittyvien rikosten lisäksi hän pitää vakavina esimerkiksi talous- ja huumausainerikoksia. O5 on kuitenkin samalla huolissaan mahdollisista väärinkäytöksistä ja toiminnan laajenemisesta mielipiteiden valvontaan. Hän puhuu nimenomaan rikoksista, eikä mainitse esimerkiksi kansallista turvallisuutta koko haastattelun aikana, joten käsite ei ole hänelle todennäköisesti tuttu.

Ainakin sillon, jos on joku henkeen ja terveyteen liittyvä rikos, mitä tutkitaan. Tai joku muu vakava rikos, esim. joku huumausainerikos tai talousrikos. Niin kyllä mun mielestä sillon. Mut sitten, se on hyvin... sitte jossain vaiheessa mennään sille linjal, vähän semmoseen, että aletaan olee vähän, mun mielestä, hämärällä alueella, että onkohan tää enää oikein. Että jos, jotain tämmösiä, mielipidekysymyksiä aletaan verkkovalvonnalla ratkaisemaan. [...] Jos niitä [toimivaltuuksia] käytetään just niin kun sanotaan, käytetään just niiden rikosten tutkimiseen, niin todennäkösesti, mun mielestä, se parantaa ihmisten oikeusturvaa. Mahollisesti sen takii, koska rikoksia pystytään tutkimaan tehokkaammin, koska on tämmösiä toimivaltuuksia. Mutta sitten se, että jollakin on tämmöset toimivaltuudet, se saattaa jossain vaiheessa johtaa siihen, et niitä käytetään väärin. O5: MIES

Vastaaja O7 pitää tärkeänä, että viranomaisten harjoittama tiedonhankinta kohdistuu vain epäiltyihin vakaviin rikoksiin, kuten terrori-iskuihin eikä kerätystä tiedosta koidu merkintöjä tai ongelmia syyttömille. Hän peräänkuuluttaa kerättyjen tietojen poistamista, jos huomataan ettei henkilö ole syyllistynyt mihinkään.

> *”Kyllähän se nyt tietty, et jos on vahva epäilys siitä, että vaikka terrori-isku tulossa tai murha tai joku vakavampaa luokkaa oleva rikos, niin kyl mä nyt siinä sanoisin, että sais, tai ois oikeus kuunnella. [...] Sitten, jos nyt paljastuu et se olikin väärä hälytys, niin sitten ne tuhottais, eikä siitä sitten, jäis, tulis mitään. Tai sitten, jos todetaan, et se nyt oli ihan syytön tyyppi, että ei ollu mitään epäilystä niin sitten ne tuhottais. Mun mielestä joo [hyväksyttävää] [...] Jotku tollaset omaisuusvarkaudet, pienet huumerikokset, niin en mä nyt tiedä, niissä sitä pitäis hyväksyttävänä.” O7: MIES*

Osallistuja H10 sallisi verkkoliikenteen ja -viestinnän tarkkailun myös vakavien rikosten suunnittelussa, kunhan epäily suunnitteilla olevasta teosta on vahva. Hän kuitenkin pitää nuoria verkonkäyttäjiä haavoittuvana ryhmänä, mikä tulisi huomioida viranomaisvalvonnassa. Riskinä voi esimerkiksi olla, että nuori leimautuu syylliseksi kevyin perustein ja merkintä rekistereissä seuraa häntä pitkään heikentäen tulevaisuudennäkymiä. Niinpä tiedonhankintamenetelmien kohdentamisessa ja saadun materiaalin perusteella tehtävissä johtopäätöksissä tulisi olla varovainen erityisesti haavoittuvien ryhmien osalta.

”Ilman muuta sellaisissa tilanteissa, kun on vahva epäilys, että joku suunnittelee tai on tehnyt jonkun… vahva epäilys siitä, että on tekemässä jonkin tällaisen ison, esimerkiks ihmisten henkiä vaativan rikoksen tai muuten taloudellisessa mielessä, ison rikoksen. Näitä henkilöitä mun mielestä poliisilla pitää olla oikeus tarkkailla. [...] Nuorten tulevaisuuden osalta musta pitää… ei saa herättää joidenkin nuorten osalta turhia epäilyjä, et he olis syyllistyneet johonkin rikolliseen toimintaan. Pitää pitää se ovi avoinna aina nuorille, ettei he joudu tahtomattaan mustamaalatuiks tai sitten, ettei heille synny epäilystä siitä, että he on syyllistyneet johonkin. Siinä tapauksessakin, kun he ovat syyllistyneet johonkin, niin ettei rekisteriin jää sellaisia tahroja, etteikö he voi aloittaa niin sanotusti uudelleen alusta. Musta täytyy taata nuorille se mahollisuus, että he voivat selvitä niistä vaikeuksista, joita heillä on ollut ja, aloittaa niin sanotusti puhtaalta pöydältä.” H10: NAINEN

Vastaaja H2 kokee, että viranomaisille säädetyt toimivaltuudet itsessään eivät loukkaa ihmisten yksityisyyttä, vaan loukkaus tulee siitä, jos kansalaiset eivät tiedä toimivaltuuksista. Hän ajattelee, että valtio, joka ei kerro avoimesti toimivaltuuksistaan kerätä ja hyödyntää kansalaisten tieto- ja viestiliikennettä, loukkaa kansalaisten oikeuksia. Osallistuja hyväksyy yksityiseen viestintään puuttumisen, jos viranomaistoimien kohteeksi joutuneen on ollut tarkoitus vahingoittaa toista tai hänen omaisuuttaan. Huumausaineiden ostamisen hän perustelee lieväksi, koska kokee ettei se vahingoita muita.

”Toimivaltuus itsessään ei loukkaa kenenkään yksityisyyttä. Oikeuksien loukkaus tulee siitä, jos kansalaiset eivät tiedä. [...] Että oikeuksia ei loukattaisi, sen tahon, joka on vastuussa, tulee tehdä päivänselväksi, että he keräävät dataa ja valvovat. [...] Mielestäni yksilö menettää oikeutensa yksityisyyteen, jos on minkäänlainen epäilys, tai sanotaan vahva epäilys, että hän aikoo vahingoittaa muita. Murha, terroriteko tai vakava vahingoittaminen, jossa ja sitten ongelmaksi tuleekin, miten vakavuus määritellään. [...] Tää nyt vaan on esimerkki. Jos oisin esimerkiksi menossa hankkimaan amfetamiinia tai kannabista, en vahingoita ketään. Kenellekään ei käy huonosti. Sellaisissa tapauksissa se tulee mielestäni ehkä hyvin kiistanalaiseksi ja henkilön tulisi saada pitää oikeutensa. Mutta, jos ois viestintää jonkun kanssa, että mennään tänä yönä hakkaamaan X tai tuhoamaan sen auto tai jotain muuta vakaavaa tekoa suunnitteilla, silloin menettäisi oikeutensa.” H2: MIES

Osallistuja H4 pitää viranomaisvalvontaa verkossa hyvänä asiana, mutta rajaisi sen tilanteisiin, joissa henkilö tai ryhmä henkilöitä muodostaa uhkan toisten terveydelle. Toiminta tulisi hänen mukaansa kohdentaa mahdollisimman rajatusti vain epäiltyihin, jolloin esimerkiksi heidän ystäväpiirinsä tai sukulaiset tulisi jättää ulkopuolelle, jos heitä itseään ei ole aihetta epäillä. Poikkeuksen tähän voisi muodostaa esimerkiksi julistettu sotatila, jolloin hän sallisi laajemman valvonnan rajallisen pituuden ajan. Terrorismin uhkan nousua hän pitää liian yleisenä kriteerinä, sillä pahimmillaan se voisi jatkua vuosikymmeniä.

”Jos todetaan, et tää ihminen on jonkun sen ominaisuuden kannalta potentiaalisesti mahollisesti riski, niin se ei mun mielestä vielä esimerkiks oo peruste. Elikkä siis esimerkiks, jos sulla on sukulaisia tai tuttavia, jotka kuuluu johonkin äärijärjestöön, niin se ei välttämättä vielä oo peruste seurata sinun viestiliikennettä, ellet sä itte jollain tavalla oo osoittanut kiinnostusta tätä kohtaan. Mut tavallaan, mun mielestä siinä on kuitenkin se, että sen pitäis lähteä siitä, että pitäis nimenomaan olla aina se vahva peruste ja jos sitä vahvaa perustetta ei oo, niin silloin vois olla ihan harmaalla alueella ja siinä kohtaa ihmistä ei pitäis, tai sitä viestiliikennettä ei pitäis, seurata. [...] Ja tavallaan mun mielestä se on äärimäisen positiivista toimintaa. Mun mielestä siis viranomaisten läsnäolo verkossa ja viranomaisten seuraaminen verkossa, mikäli se ei ylitä niitä niitten toimivaltuuksia niin on kyllä äärimmäisen tärkee asia.” H4: MIES

Osallistuja H3 mielipide eroaa selvästi tyypillisistä vastauksista. Hänen mielestään rikoksen vakavuudella ei ole väliä, vaan hän hyväksyisi viranomaisten valvonnan verkossa rikostyypistä riippumatta, eikä ajattele sillä olevan haittoja.

”Minusta se on turvallisuutta lisäävä asia. Ei tule mieleen, että sitä pitäis jotenkin rajoittaa [rikosepäilyn vakavuuden perusteella]” H3: NAINEN

Tiedustelulakeja tuntevat vastaajat

Tiedustelulakeja tuntevat vastaajat käyttävät pääsääntöisesti erilaista kieltä ja osin monipuolisempia perusteluita kuin vastaajat, jotka eivät tunne tiedustelulakeja. Heidän tiedustelutoimivaltuuksiin liittämänsä kansallisen turvallisuuden retoriikka on samansuuntaista kuin Q-menetelmällä toteuttamissamme asiantuntijahaastatteluissa. Tarkoitamme tiedustelutoimivaltuuksiin liittyvällä kansallisen turvallisuuden retoriikalla termivalintoja ja puhetapaa, jotka esiintyivät tyypillisesti tiedustelulakipaketin ympärillä käydyssä julkisessa keskustelussa.

Vaikka osallistuja H1 kertoo suhtautuvansa tiedustelulakipakettiin kriittisesti, hän pitää tarpeellisena, että viranomaisilla on toimivaltuudet myös verkkoympäristössä. Hän hahmottaa eron rikosperustaisen tiedonhankinnan ja kansallisen turvallisuuden uhkiin perustuvan tiedustelutoiminnan välillä. Vastaaja osaa myös tarkentaa, että on olemassa verkossa tapahtuvia rikoksia, joita poliisi ei voi tutkia ilman sieltä saatavaa todistusaineistoa.

”Mulla ei oo sinänsä mitään periaatteellista ongelmaa sekä rikosperusteiseen seurantaan että sitten tällaiseen, löyhemmin perustein, kansalliseen turvallisuuteen perustuvaan seurantaan, jos on kyse tarpeeksi vakavista rikoksista, tai tarpeeksi vakavasta epäilystä johonkin kansalliseen turvallisuuteen liittyen. Niin ilman muuta, koska verkko ei sinänsä oo mikään erillinen elämänpiiri, että yhtä lailla kuin riittävillä perusteilla pystytään tosimaailmassakin kohdentamaan kaikenlaisia tutkimustoimia ihmisiin, niin samalla lailla pitäis pystyä verkossakin. Henkirikokset ilman muuta, riittävän isot talousrikokset, no terroristiseen toimintaan liittyvä kaikki, tän kaltaiset. Eli lähinnä henkeen tai terveyteen liittyvät, tai sitten sellaset, joita tehdään vaan verkossa, tietynlaiset talousrikokset esimerkiks, niin niissä tapauskohtaisesti pitäis myös

voida käyttää, vaikka ne ei sinänsä vakavia henkeen ja terveyteen kohdistuvia rikoksia oliskaan, mutta koska ne on verkkomaailman rikoksia, niin sillon sitä poliisin verkkotarkkailua ei voi korvata millään muulla tutkintatoimella. Sillon se ois myös järkevä." H1: MIES

Viestisisältöjen avaamisen vastaaja H1 kokee ongelmallisena, vaikka hän kertookin hyväksyvänsä sen *"periaatteessa"*. Hän epäilee, oikeat kohteet osaavat salata viestinsä, jolloin viranomaisten avattavaksi päätyy vain muiden viestintää. Eli hän samalla kyseenalaistaa tietoliikennetiedustelun tehokkuutta saavuttaa haluttu lopputulos, vaikka puhuukin seuraavassa sitaatissa poliisista.

"--siihen liittyy se ongelma, että ne ihmiset, jotka tekee sellasia rikoksia, et heidän viestinsä olis perusteltua avata, he luultavasti on suojannu ne niin hyvin, että siihen ei pystytä. Jotenka niiden oikeuksien antaminen poliisille mun mielestä kohdistaa sen riskin vaan sit niihin ihmisiin joiden viestejä ei olis oikein avata." H1: MIES

Osallistuja H6 tarkasteli rikoskontekstin lisäksi myös kansallisen turvallisuuden uhkien torjuntaa. Hänen mielestään viranomaisten tulee päästä käsiksi ihmisten väliseen verkkoviestintään rajatuissa tilanteissa, jotka voivat olla uhkia *"yksittäisille ihmisille tai suuremmille ihmisjoukoille"* tai aseellisen kriisin kohdalla kohdistua *"koko kansakuntaan"*. Hänelle viranomaistoiminnan hyväksyttävyys on seurausta ennen kaikkea siitä, että viranomaiset noudattavat toiminnassaan lakeja, joiden perusperiaatteet on esitetty avoimesti kansalaisille. Avoimuus on tärkeää, vaikka osallistuja epäileekin, ettei viranomaisten toimivaltuudet verkossa kiinnosta suurta yleisöä tai vaikuta heidän toimintaansa.

"Minun mielestä siitä tartutaan yksilön vapauteen sillä tavoin, että se on ihan OK, jos se tehdään, se on laissa hyväksytty, mutta siinä on kuitenkin hyvä olla läpinäkyvää sen toiminnan, nimenomaan periaatteiden suhteen, miksi sitä tehdään. Perusasiat tuoda esille yksinkertaisesti. [...] Se että, tekeekö joku siitä jotain johtopäätöksiä tai muuta toimintaansa niin, se on asia erikseen. Oletan, että keskivertoihminen ei enää hätkähdä yhtään mistään, mutta kuitenkin, reilu peli. H6: MIES

Osallistuja O8 sallisi viranomaisten harjoittaa tiedonhankintaa verkossa luvanvaraisesti, jos sen tarkoitus on estää vakava rikos tai suurelle joukolle muita ihmisiä koituva vaara. Viestintä on hänelle lähtökohtaisesti yksityistä, eikä sitä ole hyväksyttävää lähteä tarkastelemaan ilman riittävän painavaa syytä. Hän perustelee näkemyksensä sananvapauden ja yksityisyydensuojan kautta, mitkä ovat olleet tiedustelulainsäädännön valmistelun keskiössä.

"Jos on jokapäivästä, tavallista elämää, niin mul on aika liberaali näkemys siinä, että ihmiset saa toimia sananvapauden ja yksityisyyden suojan nimissä aika pitkälle. Mutta sitten ehkä siinäkin tulee uudestaan tää, et jos se toiminta on senlaatusta, että se voi sitten ottaa oikeuksia suurelta joukolta muita ihmisiä tai vaarantaa muita ihmisiä, niin sitten. [...] Lähtökohtasesti [yksityisen viestinnän] ei pitäis olla saatavilla, koska siinä mennään mun mielestä sitten

ihmisen yksityiselämän puolelle. Jos ei oo perusteltua syytä tutkia jotakin henkilöä niin, sillon pitäis olla oikeus myöskin yksityiseen kirjeenvaihtoon, sähköseen kirjeenvaihtoon. [...] Jos se on laadultaan semmonen rikos, että kenenkään henki tai terveys ei oo ollu vaarassa, ja siitä ei oo suurta taloudellista vahinkoa syntyny niin sit siinä tapauksessa [ei ainakaan ole hyväksyttävää]." O8: MIES

Vastaaja H5 kertoi perehtyneensä ennen haastattelua siviilitiedustelulainsäädäntöön. Tämä näkyy hyvin hänen haastattelussaan: hän käyttää monin paikoin samanlaista termistöä kuin tiedustelulainsäädäntöön perehtyneet asiantuntijat, mutta puheessa on myös samankaltaisuuksia ei-asiantuntijoiden kanssa. Hän puhuu esimerkiksi *"Suomen poliisista"*, kun julkisuudessa esillä ollut tiedustelulainsäädäntökeskustelu on rajattu selkeästi suojelupoliisiin ja puolustusvoimiin. Vastaaja hyväksyy, että turvallisuusviranomaiset tarvitsevat toimivaltuuksia verkossa, mutta pohtii valvontaa myös laajemmin yhteiskuntien tasolla. Hän sanoo miettineensä mahdollisuutta, jos turvallisuusuhkien torjuntaa varten perustettua tiedustelutoimintoa alettaisiin käyttää demokraattisen yhteiskunnan perusperiaatteiden vastaisesti.

"Niin, siis tässähän niin kun tämmöisenä yleisenä teemana tietenkin kulkee se kansallinen turvallisuus ja kaiken sellasen, turvallisuusuhkan tai uhkien, poistaminen. Että sen takia, tietenkin, se on ymmärrettävää kansalaisille, että niitä valtuuksia on ja pitääkin olla. Mä oon kyllä tietenkin ihan kansalaisena myös sitä mieltä. Mutta, sitten se raja menee jotenkin siinä, et niin kauan, kun mä vaikka nyt henkilökohtaisesti uskon ja luotan että Suomen poliisi toimii oikein ja käyttää sitä toimivaltuuttaan vastuullisesti niin että se ei halua mitään ylimääräistä haittaa ihmisille. Tai että ne henkilökohtaiset asiat ja verkkovalvonta, että se jotenkin kääntyis jossain vaiheessa ihmisiä, tai sanotaan syyttömiä, vastaan. Se on jotenkin näin, niin niin kauanhan se on tietenkin tosi ok. Mutta sit tulee ehkä semmosii isoja kysymyksiä, että missä vaiheessa siinä voi olla semmonen vaara, että se vaikka ruvetaan rajottamaan jotain tiettyä, kriittisiä ääniä, tai kontrolloimaan jotain sellaista, mikä periaatteessa kuuluu ihan tämmöseen avoimeen demokraattiseen yhteiskuntaan. Erilaisten, vaikka aktivistiryhmittymien toiminta ja niiden oppositiopolitiikan ajaminen ja muuta." H5: NAINEN

Missä tilanteissa tiedonhankinta voi olla hyväksyttävää?

Tiedonhankinnan edellytyksiä mitattiin englanninkielisessä kyselyssä kolmella kysymyskokonaisuudella, joissa vastaajilta kysyttiin millaisissa tilanteissa, olosuhteissa ja menetelmillä valtion viranomaisten harjoittama tiedustelutiedon kerääminen, tallentaminen ja hyödyntäminen verkossa (the collection/storing and use of online intelligence by the State) voisi olla heidän mielestään hyväksyttävää. Vastaajille annettiin arvioitavaksi kaksi skenaariota, joista ensimmäinen kuvasi mahdollisen terrori-iskun valmistelua ja toinen poliisin chat-alustalla tekemää tiedonhankintaa erilaisissa tilanteissa. Kolmas kysymyskokonaisuus puolestaan muodostui useista asenneväittämistä, jotka käsittelivät poliisin ja turvallisuuspalveluiden (police and security services) tiedonhankintaa verkossa.

Skenaario 1. *Pääkaupungin poliisi on saanut vihjeen mahdollisesta terrori-iskusta Pride-kulkueeseen. Saadakseen selville iskun suunnittelijat, tiedusteluviranomaiset alkavat kerätä tietoa verkkoliikenteestä erilaisilla hakusanoilla ja fraaseilla. Yksi sähköpostiviestisi päätyy turvallisuusviranomaisille, koska henkilö, jonka kanssa olet viestitellyt, oli käyttänyt viestissään hakuehtoja vastaavaa ilmausta.*

Vastaajilta kysyttiin, missä määrin he hyväksyvät erilaiset tavat, joilla tiedusteluviranomaiset mahdollisesti käsittelisivät skenaariossa esitettyä sähköpostiviestiä. Heille myös selvennettiin, etteivät kyseiset tavat ole mahdollisia Suomessa[11]. Kysely toteutettiin ennen kuin tiedustelulait olivat voimassa Suomessa ja lisäksi Skenaariossa 1 kuvattu hakusanaperusteinen suodatus ei vastannut Suomen lakiesityksessä kuvattua tietoliikennetiedustelun toteutustapaa. Kyselyssä kysyttiin: *"To what extent are you comfortable with the following possible treatments of your email"*. Esitettyjä menettelytapoja sähköpostiviestin käsittelyyn oli viisi, jotka on listattu Taulukossa 4. Vastausvaihtoehtojen äärimmäisinä arvoina olivat *"strongly disagree"* (1) ja *"strongly agree"* (7), jotka kirjaimellisesti kääntyvät suomen kielellä *"vahvasti eri mieltä"* ja *"vahvasti samaa mieltä"*. Käännämme ne tähän tavallisemmin käytetyillä ilmaisuilla *"täysin eri mieltä"* ja *"täysin samaa mieltä"*. Taulukossa 4 on ensin kuvattu suhteelliset jakaumat kaikille seitsemällä luokalle (1-7). Seitsemän luokkaa on supistettu kolmeen yhdistämällä kolme kielteistä ja kolme myönteistä arvoa yhteen kielteiseen ja yhteen myönteiseen luokkaan. Keskimmäinen luokka (4) jätettiin sellaisenaan. Kolmiluokkaista jakaumaa käytetään esiteltäessä tuloksia tekstissä ja yhteenlasketut arvot esitetään myös taulukossa. Yksikään vastaaja ei jättänyt vastaamatta ensimmäiseen skenaarioon, eikä kukaan valinnut vaihtoehtoa *"en osaa sanoa"*. Sähköpostin käsittelytavat etenevät kyselyssä ikään kuin vähiten yksityisyyteen tunkeutuvasta eniten yksityisyyteen tunkeutuvaan menettelyyn. Alkutarinaan sisältyvänä oletuksena on, ettei sähköpostiin vastannut henkilö, jonka asemaan kyselyyn osallistujaa pyydetään asettumaan, ole itse syyllistynyt mihinkään.

Taulukoissa 4-9 tulokset on esitetty käyttäen vastausluokkien koko arvosanajakaumaa 1-7. Tekstissä äärimmäiset vastausluokat 1-3 ja 5-7 on kuitenkin yhdistetty, jotta arvosanojen jakaumat on helpompi esittää. Lukija näkee taulukoista 4-9 tarkat arvosanajakaumat ja voi myös tarkistaa yhdistettyjen vastausluokkien jakaumien prosentit

11 Englanninkielisessä kyselylomakkeessa asia selvitettiin vastaajille seuraavalla tavalla. "In the UK, when data is collected in bulk (from more than a few targets), authorities can use a 'filtering' programme that automatically rejects items not relevant to that investigation before any human can set eyes on it. ALL non-relevant information should be discarded. [This type of collection is not done in Norway or Finland but please answer as if it does]"

*Taulukko 4 Skenaario 1 Missä määrin hyväksyt seuraavat mahdolliset sähköpostisi käsittelytavat, % (n = 236). 1 = täysin eri mieltä 7 = täysin samaa mieltä.**

Missä määrin hyväksyt seuraavat mahdolliset sähköpostisi käsittelytavat? (To what extent are you comfortable with the following possible treatments of your email?)	**Täysin eri mieltä**						**Täysin samaa mieltä**
	1	**2**	**3**	**4**	**5**	**6**	**7**
Tietokonealgoritmi poimii ja poistaa sähköpostin automaattisesti	14	11	17	10	18	17	14
Analyytikko tarkistaa kuka vastanotti ja lähetti sähköpostin	23	16	15	10	12	12	11
Analyytikko tarkistaa sen osan sähköpostia, joka sisälsi hakusanan tai -fraasin	25	14	15	9	13	15	9
Analyytikko lukee koko sähköpostikeskustelun	45	18	13	6	8	6	4
Analyytikko lukee sähköpostini ja tekee taustaselvityksen	50	12	14	6	7	8	4

* Pyöristyksistä johtuen prosenteista voi tulla yhteensä yli tai alle 100.

Taulukon 4 tuloksista havaitaan, että samaa mieltä väitteen kanssa olevia vastaajia on sitä vähemmän, mitä enemmän väitteissä kuvatuissa menettelytavoissa siirrytään sellaiseen sähköpostin käsittelyyn, joka kohdistuu yhä tarkemmin henkilötietoihin ja viestin sisältöön. Tietokonealgoritmin automaattisesti poimima ja poistama sähköpostiviestin käsittely ei haittaa (arvot 5–7) 49 % vastaajista. Toisaalta tietokonealgoritmin käyttö sähköpostin poiminnassa ja poistamisessa vaivaa (arvot 1–3) monia vastaajia (42 %). Jos analyytikko tarkistaa sähköpostin vastaanottajan ja lähettäjän, vaivaa se jo 54 % vastaajista, ja enää 35 % hyväksyy menettelyn. Samankaltainen jakauma (54 % vs. 37 %) havaitaan tilanteessa, jossa analyytikko tarkistaa sen osan sähköpostia, joka sisälsi algoritmin hakusanan tai -fraasin. Koko sähköpostikeskustelun lukemiseen ja viimeisessä vaihtoehdossa lukemiseen liitettävän taustaselvityksen tekemiseen suhtautuu ainakin jossain määrin kielteisesti 76 % vastaajista (arvot 1-3). Myönteisesti (arvot 5–7) kahteen viimeiseen menettelytapaan suhtautuu vajaa viidesosa, eli 18 % ja 19 % vastaajista. On myös huomionarvoista, että kaksi viimeistä menettelytapaa ovat sellaisia, joissa äärimmäisen *”täysin eri mieltä”* -vaihtoehdon (arvo 1) valitsi lähes puolet vastaajista eli 45 % ja 50 %.

Skenaario 2: *Sadat tuhannet maan rajojen sisä- ja ulkopuolella olevat ihmiset käyttävät suosittua chat-alustaa (chat server). Käyttäjät keskustelevat kaikenlaisista aiheista ruokaresepteistä seurusteluun. Poliisilla on todisteita siitä, että keskustelupalstalla käydään keskustelua laittomasta toiminnasta. Missä määrin olet samaa mieltä, että tämän maan poliisi tekee seuraavaa?*

Skenaariossa 2 vastaajilta kysyttiin, missä määrin he kokevat hyväksyttävänä, että maan poliisi pystyisi valvomaan chat-alustalla tapahtuvaa keskustelua erilaisissa tilanteissa *("How much do you agree with the police in this country doing the following?")*. Tilanteet käsittelivät esimerkiksi chat-alustan yksittäisen käyttäjän suoraa valvontaa, koko chat-alustan lokitietojen tallentamista ja poliisin osallistumista verkkokeskusteluun rikosepäilyissä, joiden vakavuus vaihteli vakavasta järjestäytyneestä rikollisuudesta mihin tahansa rikostyyppiin. Vastausvaihtoehtoja oli jälleen seitsemän, ääriarvojen ollessa *"täysin eri mieltä"* (1) ja *"täysin samaa mieltä"* (7). Kuten ensimmäisen skenaarion kohdalla, Taulukossa 5 esitetään koko seitsenluokkainen jakauma, mutta tekstissä luokat 1-3 ja 5-7 on yhdistetty. Myös kategoriat *"en tiedä"* ja *"ei vastausta"* on yhdistetty (arvo 0). Vastaajille ei selvennetty, olivatko taulukossa luetellut valvontamenetelmät arvioinnin kohteena olevassa maassa lainmukaisia vastausajankohtana.

*Taulukko 5 Skenaario 2: chat-alustan valvonta, % (n = 236). 1 = täysin eri mieltä 7 = täysin samaa mieltä, 0 = en osaa sanoa tai ei vastausta. **

Olen samaa mieltä, että tämän maan poliisin pitäisi kyetä… (I agree that the police in this country should be able to….)	**Täysin eri mieltä**							**Täysin samaa mieltä**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Valvoa suoraan chat-alustan käyttäjää, joka on maassa ja jota epäillään osallistumisesta vakavaan järjestäytyneeseen rikollisuuteen (kuten ihmiskauppa)	2	7	6	6	4	17	23	35
Valvoa suoraan chat-alustan käyttäjää, joka on ulkomailla ja jota epäillään osallistumisesta vakavaan järjestäytyneeseen rikollisuuteen (kuten ihmiskauppa)	3	8	11	6	10	17	20	23
Valvoa ja tallentaa kaikki chatin lokitiedot palvelimelta tukeakseen käynnissä olevaa tutkintaa, jonka kohteena vakava järjestäytynyt rikollisuus**	1	17	13	9	10	17	15	18
Valvoa ja tallentaa kaikki chatin lokitiedot palvelimelta tukeakseen minkä tahansa rikostyypin tutkintaa (kuten tekijänoikeuksien loukkaukset ja verkossa ostetut huumeet)	2	35	19	15	10	9	6	5

Olen samaa mieltä, että tämän maan poliisin pitäisi kyetä… (I agree that the police in this country should be able to….)	Täysin eri mieltä							Täysin samaa mieltä
	0	1	2	3	4	5	6	7
Osallistua avoimesti verkkokeskusteluihin, jotta voi estää rikoksia tai tukea minkä tahansa tyyppisen rikoksen tutkintaa	3	6	4	7	7	20	19	36
Osallistua verkkokeskusteluihin kertomatta olevansa poliisi, jotta voi estää rikoksia tai tukea minkä tahansa tyyppisen rikoksen rikostutkintaa	4	9	8	8	10	23	15	24

* Pyöristyksistä johtuen prosenteista voi tulla yhteensä yli tai alle 100.
** Tämän vaihtoehdon kohdalla oli yksi en osaa sanoa vastaus.

Kun kyseessä on epäily vakavasta järjestäytyneestä rikollisuudesta, poliisin kykyyn valvoa maassa oleskelevaa epäiltyä henkilöä chat-alustalla suhtautuu hyväksyvästi (arvot 5–7) 75 % vastaajista, kun taas 19 % (arvot 1-3) valitsi kielteisen kannan. Kykyä valvoa ulkomailla olevan epäiltyä piti hyväksyttävänä (arvot 5–7) 60 % vastaajista ja neljännes oli eri mieltä.

Puolet vastaajista hyväksyy (arvot 5-7) poliisin kyvykkyyden valvoa ja tallentaa chatin kaikki lokitiedot, jos kyse on vakavan järjestäytyneen rikollisuuden tutkinnasta. Minkä tahansa rikostyypin tutkinnan kohdalla myönteisesti suhtautuvia vastaajia on enää 20 % (arvot 5–7) ja kielteisen mielipiteen omaavien määrä kohosi jo 69 prosenttiin.

Toisen skenaarion neljän ensimmäisen väitelauseen perusteella voidaan sanoa, että vastaajien on helpompi hyväksyä verkkokeskustelun valvonta, jos se on kohdistettua henkilöön ja perusteena on vakava rikollisuus. Tosin pieni osa osallistujista vastustaa valvontaa voimakkaasti myös silloin.

Poliisin osallistumiseen verkkokeskusteluun suhtaudutaan pääosin myönteisesti. Avoimen läsnäolon verkkokeskusteluissa osana kaiken tyyppisten rikosten estämistä ja tutkintaa hyväksyy 75 % (arvot 5–7) osallistujista. Vain 17 % (arvot 1-3) suhtautuu siihen kielteisesti. Peiteltyyn osallistumiseen rikosten estämiseksi tai tutkimiseksi suhtautuu myönteisesti 62 % (arvot 5–7) ja kielteisesti 25 % (arvot 1–3) vastaajista.

Kyselyssä esitettiin myös yhdeksän väitelausetta, jotka ovat eri muodoissaan olleet viime vuosina esillä julkisessa keskustelussa poliisin ja turvallisuuspalveluiden toimivaltuuksista kerätä, säilyttää ja analysoida verkkoviestintää (Taulukko 6). Osa argumenteista on esitetty hiukan eri tavoin muotoiltuina myös asiantuntijoille suunnatussa Q-metodologisessa tutkimuksessamme. Tulokset esitellään taas Taulukossa 6 seitsenluokkaisen jakauman avulla, mutta raportoidaan tekstissä yhdistettyjen arvojen mukaan siten, että arvot 1–3 kuvaavat kielteistä ja arvot 5–7 myönteistä suhtautumista esitettyyn väitelauseeseen. Keskellä oleva arvo, 4, on neutraali.

*Taulukko 6 Asennoituminen julkisessa keskustelussa esitettyihin kannanottoihin poliisin ja turvallisuusviranomaisten valtuuksista kerätä, säilöä ja analysoida verkkoviestintää, % (n = 236). Arvoon 0 on yhdistetty puuttuva tieto ja "en osaa sanoa". 1 = täysin eri mieltä 7 = täysin samaa mieltä, 0 = en osaa sanoa tai ei vastausta. **

Väitelause	**Täysin eri mieltä**							**Täysin samaa mieltä**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Viranomaisten ei pitäisi kerätä millään tavalla, eikä missään tilanteessa tietoja käyttäytymisestäni internetissä, kun en ole epäilty.	0*	4	9	15	7	13	17	35
Verkossa tapahtuvan valvonnan (online surveillance) käyttäminen ei ole oikeutettua, kun toimitaan tavanomaista rikollisuutta vastaan.	3	4	6	15	9	17	16	31
Jos sinulla ei ole mitään piilotettavaa, sinun ei tarvitse olla huolissasi viranomaisten harjoittamasta valvonnasta.	0*	44	14	15	3	6	9	7
Meidän on rajoitettava viranomaisille myönnettäviä toimivaltuuksia nykyisyydessä, koska emme voi vaikuttaa siihen, kuinka tulevat hallinnot saattavat käyttää niitä.	5	1	5	4	5	17	19	44
Viranomaisten laajempi pääsy verkkoviestintään antaa minulle lisää turvaa.	4	23	17	15	10	20	7	3
Radikalisoituneet ihmiset, jotka ovat vaarassa muuttua väkivaltaiseksi, tulisi tunnistaa heidän verkkokäyttäytymisensä perusteella.	6	6	11	7	14	23	20	11
Nykyinen turvallisuus- ja rikollisuustilanne oikeuttaa laajemmat kyberympäristön valvontamenetelmät.	15	20	11	17	9	18	7	4
Uskon, että kaikille pitäisi ilmoittaa jälkikäteen, jos heidän verkkoviestintäänsä on avattu, tallennettu tai käytetty tutkinnassa.	3	3	4	6	7	14	19	46
On tärkeämpää valvoa viestintää, joka tulee ulkomailla olevilta ihmisiltä, kuin tässä maassa asuvilta.	10	20	17	20	21	5	5	3

* Pyöristyksistä johtuen prosenteista voi tulla yhteensä yli tai alle 100.
** Pieni desimaaliarvo pyöristyi nollaan.

Vastaajista 65 % katsoo, ettei viranomaisten pitäisi kerätä millään tavalla, eikä missään tilanteessa tietoja hänen käyttäytymisestään internetissä silloin, kun hän ei ole epäiltynä. Eri mieltä on 28 % osallistujista. Vastaajista 64 % ei pidä oikeutettuna verkossa tapahtuvan valvonnan käyttämistä tavanomaisen rikollisuuden vastatoimena. 25 % puolestaan kannattaa sitä. Julkisessa keskustelussa esillä ollut väite *"Jos sinulla ei ole mitään piilotettavaa, sinun ei tarvitse olla huolestunut viranomaisten harjoittamasta valvonnasta."* ei saavuttanut paljon kannatusta, sillä 73 % vastaajista on eri mieltä ja näistä 44 % valitsi kaikista jyrkimmän vaihtoehdon, *"täysin eri mieltä"*. Väitteen *"Meidän on rajoitettava viranomaisille myönnettäviä toimivaltuuksia nykyisyydessä, koska emme voi vaikuttaa siihen, kuinka tulevat hallinnot saattavat käyttää niitä."* kanssa samaa mieltä on 80 % vastaajista.

Viranomaisten laajemman pääsyn verkkoviestintään katsoo antavan lisää turvaa 30 % vastaajista. Väitteen kanssa eri mieltä on puolestaan enemmistö, 55 % vastaajista. Vaikka turvallisuusviranomaisten toimivaltuuksiin verkossa suhtauduttiin kriittisesti, niin silti väitteen *"Radikalisoituneet ihmiset, joilla on riski muuttua väkivaltaisiksi tulisi tunnistaa heidän verkkokäyttäytymisensä perusteella."* kanssa samaa mieltä on yli puolet (54 %) ja eri mieltä neljäsosa (25 %) vastaajista. Melkein puolet eli 48 % suhtautuu kielteisesti väitteeseen *"Nykyinen turvallisuus- ja rikollisuustilanne oikeuttaa laajemmat kyberympäristön valvontamenetelmät."*, mutta väitteen kanssa samaa mieltä oli lähes kolmasosa eli 29 % vastaajista. Kyseinen väite keräsi 9 % neutraaleja vastauksia (arvo 4). Vaihtoehtoon *"en osaa sanoa"* tai kokonaan vastaamatta päätyi yhteensä 15 % vastaajista. Toisin sanoen useiden vastaajien oli vaikea muodostaa väitteeseen mielipidettä.

Lähes neljä viidesosaa (79 %) vastaajista on samaa mieltä väittämän *"Uskon, että kaikille pitäisi ilmoittaa jälkikäteen, jos heidän verkkoviestintäänsä on avattu, tallennettu tai käytetty tutkinnassa."* kanssa, kun taas eri mieltä olevia on vain 13 %. Viimeinen väitelause *"On tärkeämpää valvoa viestintää, joka tulee ulkomailla olevilta ihmisiltä, kuin tässä maassa asuvilta."* saattoi olla vaikeasti hahmottuva kysymys, sillä neutraaleja (arvo 4) vastauksia oli yli viidennes (21 %) ja joka kymmenes (10 %) joko jätti vastaamatta tai valitsi vaihtoehdon "*en osaa sanoa*". Väitteen kanssa eri mieltä oli 57 % ja samaa mieltä 12 % vastaajista. Väite kuvastaa tietoliikennetiedustelun olennaista elementtiä, sillä tietoliikennetiedustelun saa kohdistaa vain sellaiseen viestintään, jota käydään Suomen rajan ylitse.

Edellä esitetyt skenaariot ja väitelauseet osoittavat, että suurin osa kyselyyn vastanneista suhtautuu viranomaisten toimivaltuuksiin verkossa melko kriittisesti tai varautuneesti, ellei kyse ole vakavan rikollisuuden tutkinnasta tai torjunnasta. Toisaalta, kuten edellisissä luvuissa esitetyistä haastattelutuloksista käy ilmi, lähes kään kaikki haastatellut, ja siten oletettavasti myös kyselyn vastaajat, eivät tunne kovinkaan hyvin viranomaisten tiedonhankintaväyliä tai -menetelmiä. Mielikuva viranomaisten harjoittamasta valvonnasta verkossa, sen ehdoista ja käytettävistä menetelmistä syntyy usein muuta kautta kuin lakien tuntemisen.

8.4 Kaupalliset tahot ja rikolliset huolestuttavat enemmän kuin viranomaiset

Kyselyssä kartoitettiin myös, missä määrin vastaajat ovat huolissaan eri tahojen suorittamasta verkkoaineistojen ja -käyttäytymisen (online data and behaviour) tietojen keräämisestä, säilyttämisestä ja analyysista (Taulukko 7). Kysyttyjä tahoja olivat *”tämän maan poliisi ja turvallisuuspalvelu”, ”ulkomainen poliisi tai turvallisuuspalvelu”, ”rikolliset”, ”yksityiset yritykset (esim. kohdennettu mainonta tai asiakkaiden profilointi)”, ”ystävät, omaiset ja kumppanit”* sekä *”työantaja tai koulutuksen järjestäjä”*.

*Taulukko 7 Missä määrin vastaajat ovat huolissaan eri tahojen suorittamasta verkkokäyttäytymisen tietojen keräämisestä, säilyttämisestä ja analysoinnista % (n = 236). 1 = vahvasti eri mieltä, 7 = vahvasti samaa mieltä, 0 = en osaa sanoa tai ei vastausta.**

Olen huolissani, että verkkoaineistoani ja -käyttäytymistäni kerää, säilyttää tai analysoi… (I am concerned about my online data and behaviour being collected, stored or analysed by…)	**Täysin eri mieltä**							**Täysin samaa mieltä**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Tämän maan poliisi tai turvallisuuspalvelu	3	17	21	20	7	13	10	9
Ulkomainen poliisi tai turvallisuuspalvelu	2	7	13	14	10	14	17	23
Rikolliset	-	3	8	9	8	23	21	28
Yksityiset yritykset	1	3	4	4	5	23	22	39
Ystävät, omaiset ja kumppanit	4	32	20	14	9	8	7	6
Työnantaja tai koulutuksen järjestäjä	1	17	15	17	11	17	10	13

* Pyöristyksistä johtuen prosenteista voi tulla yhteensä yli tai alle 100.

Taulukossa 7 esitetään tulokset seitsenluokkaisen jakauman mukaan, mutta tekstissä väitteen kanssa samaa mieltä (luokat 5–7) ja eri mieltä (1–3) olevat vastaajat on pääosin yhdistetty. Arvo 4 on neutraali ja kategoriaan 0 on yhdistetty puuttuvat vastaukset sekä *”en osaa sanoa”*-vastaukset. Vastaajista selkeä enemmistö eli 84 % (arvot 5-7) on huolissaan yksityisten yritysten harjoittamasta verkkoaineiston ja -käyttäytymisen keräämisestä, säilyttämisestä ja analysoinnista. Äärimmäisen luokan eli *”täysin samaa mieltä”* (7) valitsi 39 % vastaajista ja vain 11 % (arvot 1-3) ei ollut huolissaan yritysten harjoittamasta valvonnasta. Rikollisisista on huolissaan 72 % (arvot 5-7) osallistujista. Ulkomaisen poliisin tai turvallisuuspalvelun tiedonhankinnasta on huolissaan hiukan yli puolet (54 %, arvot 5-7), kun taas suomalaisen poliisin ja turvallisuuspalvelun kohdalla huolestuneita on noin kolmannes (32 %, arvot 5-7). Kotimaisen poliisin ja turvallisuuspalvelun kohdalla äärimmäisen luokan eli *”täysin samaa mieltä”* (7) valitsi 9 % vastaajista. Yli puolet (58 %, arvot 1-3) osallistujista ei kuitenkaan ollut huolissaan kotimaisista viranomaisista. Työantajan tai koulutuksen järjestäjän kohdalla huolestuneiden osuus on kotimaan poliisia ja turvallisuusviranomaisia hiukan suurempi, eli 40 % (arvot 5-7). Ystävien, omaisten ja kumppanien kohdalla huolestuneita oli vähiten eli vain 21 % (arvot 5-7) kaikista vastaajista. Vaikka lukema on pienempi kuin muut, ei kannata vähätellä havaintoa,

että kyselyn osallistujista noin viidennes kantaa huolta lähipiirinsä harjoittamasta verkkoaineistonsa ja -käyttäytymisensä mahdollisesta valvomisesta.

8.5 Mitä viranomaisten pitäisi kertoa tiedonhankinnastaan ja toimivaltuuksistaan?

Tässä luvussa tarkastellaan kyselyn ja haastattelujen tuloksia. Kyselyssä osallistujat saivat arvioida, millaisissa tilanteissa he toivoisivat saavansa ilmoituksen, jos viranomaisten haltuun päätyisi heidän viestintäänsä. Haastatteluista puolestaan poimittiin yleisemmän tason tiedontarpeita viranomaisten toimivaltuuksista verkossa.

Missä tilanteissa tiedonhankinnasta tulisi ilmoittaa?

Totesimme aiemmin (Taulukko 6), että kyselyssä esitetyn väittämän *"Uskon, että kaikille pitäisi ilmoittaa jälkikäteen, jos heidän verkkoviestintäänsä on avattu, tallennettu tai käytetty tutkinnassa"* kanssa samaa mieltä oli 78 % ja eri mieltä vain 12 % vastaajista. Eli kyselyn osallistujat vaikuttavat kannattavan laajaa ilmoitusvelvollisuutta. Kyselyn vastaajia pyydettiin ottamaan lisäksi kantaa kolmeen ilmoittamista tarkentavaan väitelauseeseen, jotka esitetään seuraavaksi (Taulukko 8). Väitelauseet kuvaavat erilaisia fiktiivisiä tilanteita, joissa viranomaiset saattoavat kerätä vastaajan verkkoviestintää tai -aineistoa. Lopuksi kysyttiin riittääkö, jos viranomaiset julkaisevat nimetöntä ja yleistä tietoa toiminnastaan. Kysymystä alustettiin toteamalla, että osa viranomaisten verkkoviestintään ja -aineistoon kohdistuvasta tiedonkeruusta, säilytyksestä ja analyysista voi poimia myös sellaisten henkilöiden tietoja, jotka eivät ole epäiltyjä. Taulukossa 8 esitetään tulokset seitsenluokkaisella jakaumalla, jotta vastauksissa esiintyvät ääripäät tulisivat paremmin esille. Tekstissä käytetään kuitenkin myös yhdistettyjä arvoja, jotta tulosten kokonaiskuva olisi helpompi raportoida. Tällöin arvot 1–3 kuvaavat kielteistä ja 5–7 myönteistä suhtautumista esitettyyn väitteeseen. Arvo 4 on neutraali ja kategoriaan 0 on yhdistetty puuttuvat sekä *"en osaa sanoa"* -vastaukset.

*Taulukko 8: Missä tilanteissa tiedonhankinnasta tulisi ilmoittaa % (n = 236). 1= vahvasti eri mieltä, 7 = vahvasti samaa mieltä, 0 = en osaa sanoa tai ei vastausta. % (n = 236). **

Minulle pitäisi ilmoittaa suoraan, jos verkkoviestintääni tai -aineistoani olisi kerätty, säilytetty tai analysoitu, jos (I should be directly informed if my online communications or other internet data had been collected, stored or examined, if…)	**Täysin eri mieltä**							**Täysin samaa mieltä**
	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Minä olisin epäiltynä	-	9	9	9	8	13	17	35
Olisin yhteydessä epäiltyyn	-	7	6	11	8	13	20	35
En liittyisi epäiltyyn, mutta aineistoani tallennettaisiin samanaikaisesti	-	5	3	5	9	13	20	46
Riittää kun viranomaiset julkaisevat nimetöntä ja yleistä tietoa toiminnastaan	6	15	9	14	34	10	7	6

* Pyöristyksistä johtuen prosenteista voi tulla yhteensä yli tai alle 100.

Selkeästi suurin osa vastaajista on sitä mieltä, että henkilölle tulisi ilmoittaa, jos hän joutuu tiedonhankinnan kohteeksi epäiltynä, olemalla yhteydessä epäiltyyn tai liittymättä epäiltyyn (Taulukko 8). Vastaajista 79 % (arvot 5-7) haluaa ilmoitettavan, jos hänen verkkoviestintäänsä kerätään, säilytetään tai tarkastellaan ilman liittymäpintaa epäiltyyn, toisin sanoen sivullisena. Lähemmäs puolet vastaajista (46 %) valitsi tähän väittämään vaihtoehdon 7, *"täysin samaa mieltä"*. Vain 13 % (arvot 1-3) ei kokenut tarvitsevansa suoraa ilmoitusta. Jos osallistuja liittyisi jollain lailla epäiltyyn henkilöön, niin ilmoittamisen kannalta on 68 % (arvot 5-7) vastaajista. Jos henkilö olisi itse epäiltynä rikoksesta, niin ilmoittamista toivoi 65 % (arvot 5-7) vastaajista ja 27 % (arvot 1-3) ei kokenut tarvitsevansa ilmoitusta. Neljäs väitelause, kansalaisten informointi nimettömästi, yleisellä tasolla, koettiin ilmeisesti epäselväksi, sillä kolmannes vastaajista valitsi keskimmäisen, neutraalin, arvon 4. Yleisellä tasolla tiedonkeruusta ilmoittamisen katsoo riittävän alle neljännes, 23 % (arvot 5-7).

Kyselyn vastaajat saattoivat myös kommentoida kysymystä tiedonhankinnan kohteeksi joutumisen ilmoittamisesta avovastauksessa. Avovastauksen antoi kaikkiaan 46 henkilöä. Useimmissa vastauksissa katsottiin, että poliisi ja turvallisuusviranomaiset tarvitsevat työssään myös verkkoaineistoja. Tiedonhankinnan kohteilla tulisi aina olla oikeus saada tietää joutumisestaan tiedonhankinnan kohteeksi ja mitä tietoja heistä on kerätty. Useimmat totesivat samalla, että ilmoittaminen olisi mahdollista ja järkevää vasta sen jälkeen, kun viranomaistoimet on saatettu päätökseen tai kun ilmoittaminen on muuten turvallista vaarantamatta tiedonhankinnan tarkoitusta. Useissa avovastauksissa korostettiin periaatetta, jonka mukaan viranomaisten kiinnostuksen kohteeksi joutuneella ihmisellä tulee olla tilaisuus selittää toimintaansa ja puolustaa itseään. Vain muutamassa avovastauksessa katsottiin, että yleinen ilmoittaminen kansalaisille on riittävä tapa kertoa viranomaisten harjoittamasta tiedonhankinnasta. Hyvin harva vastaaja ajatteli, ettei turvallisuusviranomaisille tulisi sallia minkään verkkoaineiston keräämistä.

Jotkut avovastaukset käsittelivät myös tilannetta, jossa henkilöstä kerätään tutkintaan liittymättömänä sivullisena tietoja tai hänestä on saatu tutkintaan liittymätöntä aineistoa. Tällaisissa tilanteissa suurin osa katsoi, että asiasta pitäisi myös aina ilmoittaa, jos se on tiedonkeruun tarkoitusta vaarantamatta mahdollista. Lisäksi moni vastaaja totesi, että kaikki tiedonkeruun kannalta ylimääräinen ja hyödytön tieto pitäisi tuhota välittömästi. Parissa vastauksessa yhdistettiin viranomaisten harjoittama tiedonkeruu ja kansalaisten heitä kohtaan tuntema luottamus: viranomaiset voivat kerätä toimivaltansa puitteissa tietoa myös verkosta niin kauan kuin heihin voidaan luottaa. Luottamus edellyttää, että viranomaisten tulee olla riittävän avoimia, vaarantamatta kuitenkaan tiedonhankinnan tarkoitusta. Luottamus pitää ansaita riittävän avoimuuden lisäksi toiminnalla saaduilla tuloksilla. Joissain vastauksissa nostettiin esiin toive viranomaisten toiminnan laillisuutta ja eettisyyttä valvovasta ulkopuolisesta järjestelmästä, joka voisi puuttua mahdollisiin viranomaistoiminnan väärinkäytöksiin.

Mitä toimivaltuuksista pitäisi kertoa ja miksi?

Haastattelujen vastaajat ajattelivat poikkeuksetta, että kansalaisten olisi hyvä olla perillä viranomaisten toimivaltuuksista ja niiden käytöstä. Osa oli hyvin kriittisiä viranomaisten nykyistä tiedotuslinjaa kohtaan ja ajatteli, että viranomaisten tulisi tiedottaa avoimemmin olemassa olevista toimivaltuuksista. Pääsääntöisesti kaivattiin

kansantajuista yleisluontoista tietoa siitä, mitkä viranomaiset tekevät, mitä ja missä tilanteissa. Kuitenkin samaan aikaan tiedustelulakeja huonosti tuntevien vastauksista oli havaittavissa, että useat eivät ole valmiita ottamaan asioista selvää, koska asiaa ei koettu riittävän kiinnostavaksi. Tyypillisiä itselle sopivia tiedonlähteitä, joita vastaajat mainitsivat, olivat esimerkiksi verkkosivut, sanomalehdet, koululaitos ja kampanjat. Haastateltavista on nostettava esiin tiedustelulakien etenemistä seuranneet haastateltavat, joka toivoivat yksityiskohtaisempaa tietoa tiedustelutoiminnan, erityisesti tietoliikennetiedustelun, tuloksista. Heillä oli myös muita selkeämpi kuva julkisuudessa käydystä keskustelusta. Seuraavaksi esitetään muutamia lainauksia haastateltujen puheesta, jaoteltuna jälleen tiedustelulakien tuntemuksen perusteella.

Tiedustelulakeja tuntemattomat vastaajat

Osallistuja O5 on epävarma, millaisia tiedonkeruuvaltuuksia suomalaisilla viranomaisilla on verkossa ja hän haluaisi niistä lisätietoa. Hän kaipaa tietoa erityisesti toimenpiteistä, joiden kohteeksi voi joutua kuka tahansa ilman rikosepäilyä. Henkilökohtaista ilmoitusta mahdollisesta tiedonkeruusta osallistuja ei niinkään kokenut tarvitsevansa.

> *”No, siis jos mun tietoja tutkitaan jotenki massatyylisesti, ilman että muhun kohdistuu mitään rikosepäilyä, niin kyllä mä haluaisin siitä tietää. Vaikka se oliskin joku semmonen, että siin ei oo mitään yksilöiviä tietoja, niin mä haluaisin kyllä tietää jos joku, analysoi mun tietoja. Ehdottomasti. [...] No, välttämättä en haluis henkilökohtasta ilmotusta. Mutta yleensäkin se, että esimerkiks Suomen valtio tekee terrorismin, terroristeja seuloakseen, tämmöstä massavalvontaa, jossa tutkitaan näitä ja näitä asioita ihmisistä. Semmonen olis erittäin kiva tietää. Ja sitten, se että kuka sitä tekee, mä haluaisin kyllä saada semmosesta enemmän lisätietoja.” O5: MIES*

Vastaaja O7 pitää tärkeänä, että kansalaiset tietävät viranomaisten toimivaltuuksista ja niiden käytöstä, koska se osaltaan estää järjestelmän väärinkäytöksiä. Sopiva tiedotustapa voisi olla hänen mukaansa kampanjatyylinen, joka antaisi perustiedot toiminnasta, koska *”kai se tieto on siellä niitten jossain hallinnon sivuilla, mutta se, että eksyykö sinne tai meneekö sinne muut, kun asiaan perehtyneet tai asiasta oikeesti kiinnostuneet, niin se on tietty toinen kysymys”.*

> *”No kyl mun mielestä se ois ihan tärkeetä, vaikka täytyy heti myöntää, etten ittekään oo ihan tarpeeks, kauheesti kärryillä näistä asioista. [...] Jos nyt näitä viimeisiä, Aarnion oikeudenkäynti ja sit siel on ollu näitä, Lardot ja muut, niitä poliisipäälliköitä siellä käräjillä. Ois kansalaisetkin perillä, että mitä ne tekee siellä, ettei oo, tuu tälläsiä seriffejä heilumaan.” O7: MIES*

Tietoisuuden lisääminen on vastaajien H9 ja O6 mielestä tärkeää, koska se voi vaikuttaa ihmisten verkkokäyttäytymiseen. Monet voivat jättää sallittuja asioita tekemättä, koska eivät ole varmoja ovatko ne laillisia vai eivät. Esimerkiksi H9 nostaa esiin tekijänoikeuskirjeet, joita yksityiset lakitoimistot ovat lähetelleet IP-osoitteen perusteella henkilöille, joiden on epäilty jakaneen oikeudetta tekijänoikeuksien alaista materiaalia, kuten musiikkia tai elokuvia. O6 kokee, että kansalaisilla

on myös rooli viranomaistoiminnan valvojina, etteivät viranomaiset kerää ja käytä tietoa tavoilla, joita kansalaiset eivät hyväksy, esimerkiksi tavallisten kansalaisten tarkkailuun. Tietämättömyys voi saada kansalaisen myös jakamaan tietojansa ymmärtämättä mihin niitä käytetään.

> *”Kyl sitä pitäis pikkasen valottaa siinä mielessä, että mä luulen, et monet ei tiedä, monet ehkä arkailee tehä juttuja, mitkä on kuitenkin täysin luvallisia ja kaikkee tällasta. Täs on ehkä osana tää tekijänoikeuskirje-pelottelu, mistä on ollut kauheesti juttua ja muuta tällasta. Ja se herättää sit ylimääräisii kysymyksii, joissain ihmisissä.” H9: MIES*

> *”Että sitten ei henkilö vahingossa tuu laittaneeks jotain tietoa johonkin silleen, et sitä käytetään johonkin mitä hän ei ois halunnu et sitä käytetään. [...] Ku mä aattelen, et jos sitä ei tiedä, niin ääritapauksissahan valtio voi käyttää tätä tietoa vähemmän hyviin tarkoituksiin. Emmä nyt usko et Suomessa tällaist tapahtuis, mut jos kattoo esim. mitä on Kiinassa tai Amerikassa tapahtunu, miten siviilien tietoja käytetään periaatteessa heidän valvomiseen. Siis että ei vaan valvota tiettyjä riskiryhmii, vaan ihan vaan tavallisii kansalaisii, niin kylhän se ois aika dystooppista, jos sellaist tapahtuis.” O6: NAINEN*

Osallistuja O4 kaipaa tietoa toimivaltuuksista siellä, missä mahdollinen laiton toiminta tapahtuu. Esimerkiksi keskustelufoorumeiden tulisi pyrkiä torjumaan vihapuhetta tiedottamalla, mitä vihapuheelle tapahtuu ja antamalla toimintaohjeita. Osallistuja kertoo, ettei tunne poliisin prosessia vihapuheen käsittelyyn, mutta toivoisi siitä lisätietoa.

> *”Et jos sä kirjotat jotain vihapuhetta jonneki, ni sit et miten siitä, jonkun pitää se jonneki ilmottaa, mut mitä se poliisi sit tekee ja voiks se päästä käsiks. Se esimerkiks on mun mielest tosi hämärää.” O4: NAINEN*

Vastaaja H7 pohtii tiedon luotettavuutta ja kokee, että faktatietoa on vaikea saada, vaikka se olisi tarpeellista. Hän myöntää, ettei tiedä itsekään tarpeeksi viranomaisten toimivaltuuksista verkossa ja kaipaisi lisää esimerkkejä viranomaisten mahdollisuuksista käytännön tilanteissa.

> *”Etenkin tällä hetkellä, ku tuntuu kaikenlainen disinformaatio ja misinformaatio lisääntyy, niin olis hyvä, että tietäis ne faktat. Tosin eihän se kaikkii oikeesti kiinnosta, mitkä ne faktat on, mutta et periaatteessa, se ois ehkä ihan kyllä kansalaisvelvollisuus tietää. Ja itse tiedän kyl valitettavan huonosti. [...] Siis ehkä esimerkit valasis sitä kaikkein parhaiten. Et mitä tää on ja miten tätä asiaa hoidetaan. Ja tää on ehkä musta just sen pullonkaula, joskus ehkä vähän arveluttavissakin lähteissä uutisoidaan jotaki asiaan liittyvää ja sitte se saattaa saada jotain ison painon, vaik ei se ois välttämättä tottakaan. Et faktoihin pohjautuva tieto tai faktoihin pohjautuvat uutiset tästä olis tosi tärkeitä.” H7: NAINEN*

Vastaaja H3 peräänkuuluttaa peruskoulun vastuuta varmistaa, että nuorille opetetaan viranomaisten toimivaltuuksista verkossa yleisellä tasolla, mutta *”kansalaisten*

ja maan turvallisuuden" takia tiedonkeruusta ei tulisi puhua liian yksityiskohtaisesti. Hänen mukaansa suomalaiset viranomaiset kertovat toiminnastaan *"aivan riittävästi"*. Vuosikertomuksiin tai omaehtoiseen tiedonhakuun hän ei sen sijaan usko.

> *"Minusta tää [toimivaltuudet verkossa] on tämmönen yleistiedollinen asia. Pitäis varmaan olla kansalaistaidonkursseja niin kun ennen vanhaan." [...] Ei minua kiinnostaisi lähteä mistään niitä [toimivaltuuksien käyttöä] tonkimaan, mutta luen kyllä mitä vastaan tulee. Vuosikertomuksia ei kukaan lue." H3: NAINEN*

Tiedustelulakeja tuntevat vastaajat

Osallistuja O9:n tiedot tiedustelulakipaketista ovat tämän haastattelututkimuksen parhaimmistoa, mutta siitä huolimatta hän arvioi, että toiminnasta on vaikea pysyä perillä ja viranomaisten tulisi tiedottaa enemmän. Hän kaipaa samankaltaista yksityiskohtiin menevää tietoa kuin Q-haastattelujen asiantuntijat. Häntä kiinnostaa esimerkiksi paljonko tietoa on kerätty, mihin valvontaa on kohdistettu ja minkälaisilla menetelmillä sitä on analysoitu. Kansalaiset voisivat hyödyntää tietoa sekä oman viestintänsä suojaamiseen, mutta myös toiminnan valvontaan. Vastaajan mukaan kansalaisvalvonnan tulisi olla aktiivista erityisesti Suomessa, jonka whistle blowing -kulttuurin hän kokee heikoksi.

> *"No sanoisin aika huonosti [viranomaiset kertovat toimivaltuuksistaan verkossa]. Se pitkälti muodostuu tällasen mediatiedon tai sitte tällasten isompien lakihankkeiden puolesta. Mutta väitän, että en itsekään ole täysin perillä siitä, että mitä tässä tapahtuu, vaikka kuitenkin koetan aktiivisesti seurata myös tätä aihepiiriä. [...] Ainakin siis tällaisia [tietoja tarvitaan] että, mikä on se tietomassan koko, jota vuosittain on käytetty, millä menetelmillä sitä on sit analysoitu vuosittain ja sit tosiaan näitä eri tekniikoita mahdollisimman tarkasti. Sekä myös ehkä se että, mihin erityisesti kohdistuu. Sinänsä kansalaisille olis myös hyvä tietää, jos esimerkiksi, pitkälti tätä tapahtuu sosiaalisen median, Facebookin sovelluksen vai onko se juuri se sähköposti jota, käytetään tässä myös sit, myös yritysten ja tutkimuksen puolella myös sen oman turvallisuuden vahvistamiseks." O9: MIES*

Osallistuja H6 pohti vastauksessaan erityisesti tiedustelulakipaketin mahdollistamaa tietoliikennetiedustelua ja koki, etteivät suomalaiset viranomaiset ole kertoneet toimivaltuuksista mitenkään. Hänen mielestään uutismediat eivät ole riittävä lähde, vaan viranomaiset voisivat lähestyä suoraan kotitalouksia ja koulujen tulisi päivittää opetussisältöjään vastaamaan uutta lainsäädäntöä.

> *"Minun mielestä tuo kuuluu, perustietona jokaiselle. Sanotaanko, että saavuttavin keino olis lähettää jokaiseen talouteen kirja, missä kerrotaan, että mistä on kysymys, millon se alkaa, ja niin edelleen, että ois perustietoja. Jos yksinkertasesti todetaan, että laki mahdollistaa tietynlaiset valvontamenetelmät ja siitä sitten uutisoidaan erilaisissa, esimerkiks printtimedioissa tai uutismedioissa yleensä, niin se ei mun mielestä oo kauhean… sillä saavuttaa osan väestöstä mutta ei läheskään kaikkia. Ja sitten myös koulussa,*

peruskoulussa, lukiossa, toisen asteen koulutuksessa tapahtuva, sanotaanko vallitsevan tilanteen päivitys, varmasti voisi olla ihan tarpeellinen ja paikallaan." H6: MIES

Vastaaja H1 ajattelee, että turvallisuusviranomaiset välttelevät kriittistä julkista keskustelua ja pyrkivät vähättelemään muiden tahojen asiantuntemusta. Asiasisältöjä enemmän hän korostaakin tarvetta asennemuutokselle.

"Aika huonosti mutta se liittyy ehkä yleensäkin turvallisuusviranomaisten tiedotuskulttuuriin, et mun mielestä Suomessa yleensäkin on tosi vahva tällainen, että kansalaisten ei tarvitse olla huolissaan tai tietää näistä, jatkakaa päivittäisiä toimianne, me huolehdimme. Tietysti turvallisuusorganisaatiot puhuu asioista niin kuin omalta kannaltaan parhain päin, mutta kyllä esimerkiksi tää keskustelu, mikä käytiin siitä, et onks tää uuden tiedustelulain mukainen valvonta massavalvontaa vai ei, niin kyllä siinä musta selkeesti viranomaisten käyttämä terminologia ei ollu kauheen rehellistä. [...] Kertomista tärkeempää olis se ehkä, et mitenkä kriittiseen julkiseen keskusteluun suhtaudutaan, että poliisilla ja muilla turvallisuusviranomaisilla on hyvin vahva pyrkimys monopolisoida se, et ainoastaan heillä on asiantuntemusta puhua näistä asioista ja mitkään muut tahot ja erilaisia intressejä esiin tuovat tahot eivät oo samalla lailla eksperttejä, joilla pitäis olla sit niin kuin auktoriteettia lausua näistä. Että se asenne on ehkä tärkeempi kuin se, mitä tuodaan, niin kuin teknisiä yksityiskohtia, tiedoksi." H1: MIES

Haastateltava H5 kokee viranomaisten nykyisen tiedotuslinjan huonoksi ja pohtii, että tietoa tarvitaan esimerkiksi siksi, ettei suomalaisen järjestelmän ajatella olevan pahempi kuin se todellisuudessa on. Hän kertoo etsineensä lisätietoa haastattelun aihepiiristä etukäteen ja tiivistää hyvin sen, mikä on tullut esille monissa tämän tutkimuksen haastatteluissa: toimivaltuuksien sisältöjen, kohdentamisen ja terminologian ymmärtäminen on haastavaa tavalliselle kansalaiselle. Lisäksi hän haluaa kiinnittää huomion erityisryhmiin, kuten maahanmuuttajiin, joille suomalaisten viranomaisten toiminnan ymmärtäminen voi olla vielä vaikeampaa, jos on kasvanut maassa, jossa viranomaisiin ei voi luottaa.

"Tavalliselle kansalaiselle tämmöisen tiedustelukentän ymmärtäminen, ylipäänsä että tarkoitetaanko tällä, että kuka tahansa viranomainen voi tai pääsee mihin tahansa tietoihin, kenen tahansa tietoihin, käsiksi ja kaikkea sitä, tarkastellaan tämmöstä massavalvontaa, vai että onko se tätä kohdennettua verkkovalvont- nää nyt on tämmöisiä, mä just äsken kattoin vähän tätä viimeisintä siviilitiedustelulakia, niin näitä termejä. En mä kansalaisena tämmöisiä termejä ees välttämättä osais yhtäkkiä heittää. Nää on tavallaan sellasii, aika ehkä vähän kaukaisia asioita tavalliselle kansalaiselle ymmärtää, mitä tarkoitetaan. [...] Ja voi olla ihmisiä jotka on eläny vaikka diktatuurin alaisuudessa, ihmisiä, joil on todella lähtökohtaisesti vähäinen luottamus minkäänlaista viranomaiskoneistoa tai valtiota kohtaan. Sellaset ihmisryhmät, että heille on erityisen tärkeä tai heitä kohtaan luoda molemminpuolisen luottamuksen ilmapiiriä ja siihen liittyen, tämmöset asiat on tärkeitä tietää." H5: NAINEN

8.6 Luottamus viranomaisiin

Haastattelun osallistujat luottivat pääsääntöisesti paljon suomalaisiin viranomaisiin, etenkin poliisiin. Luottamusta perusteltiin hyvillä omakohtaisilla kokemuksilla, yleisellä luottamuksella suomalaisessa yhteiskunnassa ja viranomaistoiminnan läpinäkyvyydellä. Toisaalta haastatellut olivat perillä myös Suomen poliisiin viime vuosina kohdistuneista julkisista skandaaleista ja väärinkäytöksistä, joiden arvioitiin heikentävän luottamusta ja omaa mielikuvaa poliisista, vaikka luottamus oli pysynyt monilla – ei kuitenkaan kaikilla – korkeana niistä huolimatta. Esimerkiksi Jari Aarnion tapaus sekä epäilty rasismi, puolueettomuuden vaarantuminen ja tietokantojen oikeudeton katselu mainittiin monissa vastauksissa asioina, jotka mietityttivät vastaajia poliisin toiminnassa.

Luottamus paitsi viranomaisiin yleisesti, myös poliisiin, tuntui olevan kaikille vastaajille suhteellisen helppo kysymys, johon saatiin kuvailevia, perusteltuja vastauksia. Tiedustelulakipaketin valmistelua seuranneille vastaajille vaikutti olevan luonnollisempaa arvioida luottamusta poliisin lisäksi myös tiedusteluviranomaisia kohtaan. Sen sijaan monelle tiedustelulakeja tuntemattomalle vastaajalle suojelupoliisin ja puolustusvoimien toteuttaman tiedustelun arviointi osoittautui haastavaksi, koska he kokivat, etteivät tiedä juurikaan organisaatioista ja niiden toiminnasta. Niinpä useat, joskin poikkeuksiakin oli, arvioivat tiedusteluviranomaisia kohtaan tuntemaa luottamustaan tutumpien viranomaisten kautta tai niukkasanaisesti, tarttumatta kysymykseen syvällisemmin. Kaikilta osallistujilta kuitenkin kysyttiin samat kysymykset.

Tiedustelulakeja tuntemattomat vastaajat

Osallistuja H3 kertoo vastaajille melko tyypillisesti kasvaneensa luottamaan poliisiin jo lapsuudesta alkaen. Luottamustaan tiedusteluviranomaisiin hän kuvaa varsin niukkasanaisesti. Hänen suhtautumisensa tiedusteluorganisaatioiden salamyhkäisyyteen on ymmärtäväinen, mikä näkyy läpi haastattelun.

> *”Hmm, kasvatuksestakin se tietenkin riippuu. Oon kasvanut maalla ja siellä on totuttu luottamaan kyllä poliisiin. Enkä ole saanut kyllä mitään sellaista tietoa mikä olisi vähentänyt uskoani poliiseihin, pois lukien nämä viimeaikaiset veikot, Aarniot plus muut. Mulla on erittäin korkea luottamus suomalaiseen poliisiin. [...] Puolustuslaitos on minun mielestäni yhtä luotettava kuin poliisi. Ja suojelupoliisi on hyvin salamyhkäinen. [Johtuen] Heidän omasta toiminnastaan. Ei paljon huudella, mutta onhan se tietysti aivan selvä, että ei pidäkään huudella.” H3: NAINEN*

Vastaaja O6 perustelee korkeaa luottamustansa poliisiin sillä, että ajattelee poliisin kohtelevan ihmisiä tasapuolisesti Suomessa. Luottamuksestaan suojelupoliisiin ja puolustusvoimiin hän ei osaa sanoa mitään yksilöivää, koska ei tunne niiden toimintaa, mutta kertoo luottavansa viranomaisiin yleisellä tasolla.

> *”Mä koen, et Suomessa on hyvin hyväksyväinen ilmapiiri. Jos vaikka mulle tapahtuu jotain ja mä soitan poliisin, niin mä pystyn luottaa siihen, että he*

eivät tule kohtelee minua mitenkään eri lailla esim. minun seksuaalisuuden tai uskonnollisten uskomusten takia. Mua kohdellaan ihan samal lailla ku kaikkia muita. [...] Emmä oikein tätä ennen ees tienny mitä suojelupoliisi on, niin ei oo mielipidettä. Yleisesti haluan vaan sanoo, et mä yritän luottaa Suomen viranomaisiin. Noin yleisesti, vaikka en paljoo tiedäkään, niin kuitenkin luotan." O6: NAINEN

Luottamus tuntuu kohdistuvan erityisesti instituutiotasolle, mutta ei ole sokea. Vastaajat pohtivat, että ihmiset, myös viranhaltijat, ovat persoonaltaan erilaisia, tekevät virheitä, ja toiset ovat rehellisempiä kuin toiset. Osallistuja H9:n luottamusta on vahvistanut omat hyvät kokemukset. Hän kertoo luottavansa myös tiedusteluviranomaisiin samalla tavalla kuin poliisiin, ja kokee, että mahdolliset väärinkäyttäjät ovat yksittäisiä viranhaltijoita.

"No sanotaan, että ei oo ollu tarvetta osoittaa epäluottamusta. Mun mielest ne harvat kerrat, kun oon viranomaisten kanssa ollut tekemisissä, niin asiat on järjestyny ihan puhumalla, että ei oo tarvinnu lähtee takkuaan yhtään mihinkään suuntaan. [...] Kyl mä luotan suomalaiseen poliisiin kuitenkin ja niitten arvostelukykyyn, suurimmaks osaks. Toki aina tulee, teet sä mitä tahansa, poliiseja on paljon, siel on yhtä monta persoonaa, kun niitä on. Ja kaikilla on joskus huono päivä. Kaikille sattuu joskus ylilyöntejä tai huteja. Mutta jos aatellaan sitä koko klönttiä niin, ei mul oo pahaa sanottavaa." H9: MIES

Vastaaja H7 on huolestunut poliisissa paljastuneista *"rasistisista seksistisistä piireistä"*, koska ajattelee sen olevan riski poliisiviranomaisen riippumattomuudelle ja sitä kautta demokratialle. Hän viittaa tutkittuun tietoon rodullistettujen ihmisryhmien kokemista poliisikohtaamisista, minkä mukaan esimerkiksi uhrin etnisellä taustalla on voinut olla vaikutusta rikosilmoituksen vastaanottamistilanteessa. Osallistuja luottaa suojelupoliisin ja puolustusvoimien harjoittamaan tiedusteluun samalla tavalla kuin poliisiin ja on huolissaan etnisestä profiloinnista myös siinä toiminnassa sekä pohtii, voidaanko sitä tehdä vähän tiedostamattomastikin.

"Kyllä mä noin yleisesti ottaen luotan, joo. Mutta siis on tosiaanki tällasta, et kaikkia rikoksia ei ehkä oteta aivan yhtä vakavasti ja kaikkiin ihmisiin ei suhtauduta ihan samalla tavalla. Tää on mun mielest todella huolestuttavaa. [...] Jos ilmeneeki suuria pahoja sidoksia, vaikkapa joihinki ääriryhmiin poliisissa tai esimerkiks hyvin rasistisia mielipiteitä, niin kyllähän se jotenki syö sitä uskottavuutta ja voi olla että... ja itse asias tutkimuksen perusteella, jotkut rodullistetut ihmisryhmät kokee, että he eivät poliisilta saa sitä apuu, mitä he tarvis." H7: NAINEN

Osallistujat O4 ja H10 luottavat viranomaisiin ja poliisiin Suomessa, mutta myöntävät, että viimeaikaiset skandaalit ovat horjuttaneet luottamusta. Osallistuja H10 uskoo, että Aarnion kaltaisia tapauksia voi paljastua poliisin lisäksi myös muista viranomaisista. Vastaaja O4 kokee vaikeaksi arvioida luottamustaan suojelupoliisin ja puolustusvoimien tekemää tiedustelua kohtaan. Esimerkiksi tiedustelutoiminnan lainmukaisuudesta hän tyytyy toteamaan *"Niin, lakihan on vähän erikoinen niille aina"*.

”Ei oo mitään muuta turvasysteemiäkään tässä maassa ja nyt johonki pitää luottaa. Ja valtioon on kuitenki jotenki optimistisempaa luottaa, ku ei luottaa. [...] No mä oon ollu varmaan enemmänki poliisipositiivinen ennen. No siis, onhan nää viimeaikaset poliisiskandaalit jotenki vaikuttanu siihen kokonaiskuvaan, ei silt voi välttyä.” O4: NAINEN

”Kyl mä oon luottanut viranomaisiin, mutta tietenkin... Uutiset joita tässä viime aikoina on tullut esille, esimerkiks tää Aarnio-tapaus. On tietenkin aika huolestuttavaa, että missä määrin, taustalla on tällaisia vastaavia, korruptioon ja rikollisuuteen sekaantuneita viranomaisia, joita ei oo paljastettu. Emmä usko, että niitä nyt kuitenkaan kovin paljon oo, mutta kyllä se Aarniotapaus osoittaa, että se on mahdollista suomalaisessa järjestelmässä. Että tällaiset henkilöt voi päästä hyvinkin pitkälle. Siinä mielessä musta on syytä olla varautunut siihen, että myös siellä viranomaisten puolella on tällaisia henkilöitä tai ryhmiä, jotka ei oo vielä paljastunut.” H10: NAINEN

Viranomaisten tekemät virheet voivat heijastua koettuun luottamukseen ja herättää kysymyksiä paitsi yksittäisten viranhaltijoiden moraalista, myös osaamisesta ja pätevyydestä organisaatiotasolla. Osallistuja O2 kertoo luottavansa poliisia enemmän suojelupoliisiin ja puolustusvoimiin, koska uskoo organisaatioiden valvonnan olevan paremmalla tasolla. Hänen kaverillaan on poliisista huonoja kokemuksia yksityiselämässään ja myös muiden viranomaisten virheet henkilötietojen käsittelyssä vaikuttavat hänen tuntemaansa luottamukseen.

”Kun ajattelee sitä, kun ajokortti- tai joku tämmönen autojen rekisteritietojen sivusto avattiin ja sitten sielt ihmiset onnistu aika nopeesti urkkii kaikenlaista henkilötietoo ja osotetta ihmisistä, ni tollaset jutut ei herätä sitä luottamusta siihen, et onko valtiolla tarpeeksi osaavia ihmisiä, jotka voi hoitaa ton ja suunnitella sen niin, että ei tapahdu sellasii virheitä. Ylipäätään ihan vaikka henkilötietojen käsittelynkin yhteydessä ja sit ehkä se luotto ei oo niin kova, varsinkaan poliisin suuntaan. Et ku niit juttuja on ollu. [...] Tämmönen tapaus, että kaveri oli menossa treffeille poliisin kans, ni se poliisi oli käyny katsomassa hänen, löytyykö mitään taustaa. Niin kävi ilmi, niin olin aika järkyttyny siitä, että tämmöstä. Tai sitten oliks se nyt Tony Halme tai joku vastaava, oli hoidossa, niin lääkärit oli käyneet urkkimassa sen tietoja. Ni tämmöset jutut jää sit mietityttää. [...] No siis, enemmän mä niihin [suojelupoliisiin ja puolustusvoimiin] luotan kuin ihan tavan poliisiin. Koen, että se on heidän erikoisalaa, ni enemmän luotan kyllä. Kyse niin vakavista asioist, et on itse niin avuton niiden edessä. Mä uskosin, että tuntuu hyvältä, et voi luottaa johonkin isompaan tahoon, joka sitten tekee sitä työkseen. Just ehkä se erikoisosaaminen. Että Supol on se oma erikoisvastuunsa ja sinne ei niin helposti pääse töihin, sinne tehään tarkat selvitykset, et kyl se luo must luottamusta. Ja sit, et sitä valvotaan myös.” O2: NAINEN

Kaikille luottamus ei ollut aivan selvä. Esimerkiksi osallistuja O5 mainitsee haastattelussa useaan kertaan poliisissa tapahtuneet tietokantojen väärinkäytökset ja on huolissaan, että uteliaat viranhaltijat voivat seuraamuksetta katsoa tietoja, jotka

heille eivät kuulu. Kysymykseen luottamuksesta hän vastaa *”Luotan ja en luota.”* ja taustoittaa asiaa paljastuneilla väärinkäytöksillä. Suojelupoliisin ja puolustusvoimien toimivaltuuksiin verkossa hän suhtautuu samalla tavalla ristiriitaisesti ja perustelee sitä tiedonpuutteen kautta *”Kyllä mä luotan, mutta ei mulla oo mitään syytä luottaa, koska en mä tiedä näistä paljoakaan mitään”*.

> *”Mä en ihan hirveesti siis luota siihen just [että poliisi toimisi lainmukaisesti verkkoliikenteen ja -viestinnän valvonnassa]. [...] Mää luulen, että siihen lainmukasuuteen on mahollisesti [vaikuttanut] just Aarnion tapaus. Sitten kun mä luin joskus, siit on varmaan monta vuotta jo, uutisen siitä, että tietyn poliisin tietoja oltiin urkittu poliisien arkistossa. Ja sitten siitä ei edes nostettu kellekään mitään syytteitä. Niin se vähän kyllä vei luottamusta tämmösissä asioissa ihmisiin.” O5: MIES*

Tiedustelulakeja tuntevat vastaajat

Vastaaja O8 luottaa vahvasti viranomaisiin, eikä ole huolissaan suomalaisten viranomaisten harjoittamasta tiedustelusta tai muusta valvonnasta verkossa. Luottamukseen vaikuttanee osaltaan se, että hän kertoo tavanneensa Supossa työskenteleviä ja mieltää kuulemansa perusteella tiedustelun arkiseksi, jopa vähän tylsäksi työksi.

> *”Suomen kohdalla mä en nää, et siin on mitään ongelmaa, koska jos me oltas maana korruptoituneempi, niin sitten varmaan syntys ongelmia. Mutta lähtökohtasesti, omakin luotto esimerkiks poliisiin ja pelastusviranomaisiin on kyllä vahva. [...] Supollakin on helposti, ehkä semmonen vähän mystinen kaapu, edelleen päällä. Mutta, mitä mä oon jonkin verran ihmisiä tavannu, jotka työskentelee siellä, niin on aika yllättävänkin tavallisia ja se työ on varmaan välillä jopa äärettömän tylsää, koska ei Supoa käsittääkseni kiinnosta, tai ainakin hyvin harvoin kiinnostaa, ihan yksittäiset henkilöt. Siinä pitää olla sitten joku laajempi kytkös ennen ku he kiinnostuu jostakin kansalaisesta. ” O8: MIES*

Vastaaja H1 näkee sotilastiedustelun ja poliisin toiminnassa selkeän eron, joka johtuu kohteista. Kansalaisiin kohdistuvan toiminnan tulee olla hänen mukaansa tarkemmin säädeltyä, kun taas vihollisiin kohdistuva sotilastiedustelu on hänen mielestään toimintaa, jonka ”*kuuluukin ehkä toimia myös sellaisella moraalisesti harmaalla alueella, että siihen vaan kuulu se, että silloin täytyy voida käyttää keinoja joustavammin”*. Hän luottaa poliisiin, mutta ei usko, että kaikista väärinkäytöksistä päästäisiin koskaan eroon. Tiedusteluviranomaisten hän arvelee toimivan lainmukaisemmin kuin poliisin, mutta myöntää pohtivansa myös tulevaisuudenskenaarioita, joissa suomalainen yhteiskunta olisi muuttunut toisenlaiseksi ja tieto- ja viestiliikenteen valvonta muodostaisi toisenlaisia riskejä.

> *”Luotan suomalaiseen poliisiin kyllä, mutta tiedostan sen, että aina siellä on näitä Aarnioita ja näitä, mikä tää yks nyt olikaan, mikä oli vasta uutisissa, kun oli vähän niin kuin tehny poliisihommaa, että maksa mulle vähän tai maksa isot sakot. Niitä keissejä ei oo monta, mutta kun niitä on, ja jos ne on*

jollain Aarnio-tasollakin... Sit jos niillä on työkalut, vaikka johonkin kunnon verkkotarkkailuun, niin ne riskit on isoja jo siinä suhteessa, ja varsinkin tiedustelupuolelta tulee vielä se, että ei koskaan voi ihan luottaa siihen, että suomalainen yhteiskunta toimis niin lakiperusteisesti ja demokraattisesti tulevaisuudessa kuin se toimii nykyään. [...] Luultavammin jos jotain rikkomuksia tulee, niin ne tulee nimenomaan tavallisen poliisin toimivaltuuksien ylityksestä, siis ihan siitä samanlaisista, melko pienistäkin jutuista, mistä poliisit säännöllisesti nykyään kärähtää jo kaikenlaisten rekisterien suhteen, että kun käydään katsomassa julkkisten kuolemasta tietoa, käydään katsomassa ex-vaimojen uusien puolisojen tietoja poliisirekisteristä. Sellasia rikkomuksia sieltä varmasti alkaa tulla. H1: MIES

Vastaaja O9 luottaa viranomaisiin ja että ne toimivat lainmukaisesti, vaikka hän suhtautuukin kriittisesti tiedustelulakipakettiin. Hän kertoo luottavansa enemmän viranomaistoimintaan yleensä kuin tiedusteluviranomaisten toimintaan verkossa. Tiedustelutoiminnan valvonta on hänen mielestään rakenteiltaan heikompi kuin rikosprosessi mahdollisen syntyvän sisäpiirin vuoksi ja toisaalta, pienempi määrä henkilöitä pääsee arvioimaan toimintaprosesseja sisältä käsin. Osallistuja pitää pienen maan riskinä esimerkiksi pyöröovi-ilmiötä, jossa samat henkilöt kiertävät vuorotellen tiedustelutehtävissä ja tiedustelutoimintaa valvovissa viroissa.

”Kyllä luotan. Ja sanoisinko että ehkä yleisesti luotan viranomaisiin enemmän, koska laajemmin nää Suomessa on, ehkä verrattuna tohon verkkopuoleen, ni kehitetty paremmin näitä erilaisia, valvontamekanismeja. [...] valvonta on tällä hetkellä Suomen kokoses valtiossa niin mahdottoman hankala toteuttaa, et siihen ei synny sellasta sisäpiiriä. Niin siihen se, ehkä kriittisyys näitä oikeuksia vastaan, suhteutuu. […] poliisin tapauksessa se liittyy rikostutkintaan, jossa herkemmin sit tulee oikeuskäsittely ja silloin esimerkiks erilaisilla asianajajilla on mahdollisuus siihen herkemmin puuttua.” O9: MIES

Osallistuja H6 luottaa kokonaisuutena suomalaisiin viranomaisiin, mutta nostaa esiin tuttuja esimerkkejä luottamusta horjuttavista tekijöistä, kuten viranhaltijoiden yksilölliset moraalierot ja etninen profilointi.

”Yleensä ottaen luotan suomalaisiin viranomaisiin, mut samalla luotan siihen, että siellä on ihmisiä, jotka tekee virheitä. Jossakin määrin luotan [poliisiin]. Mun käsitys poliisista on, että sieltä löytyy aika paljon... no esimerkiks tämä etninen kysymys ja siihen liittyvä ihmisten kohtelu. Ymmärrän kyllä, pystyn hyvin arvaamaan, että miksi saattaa poliisivoimista löytyä paljonkin suoranaisia rasisteja, mutta se kuitenkin aiheuttaa sen että, on pieni epäilys, että voiko kaikkeen poliisitoimintaan luottaa. [...] Mä luotan siihen, että molemmat organisaatiot [suojelupoliisi ja puolustusvoimat] toteuttaa niille asetettuja tehtäviä. Mä luotan siihen, että siellä on yksilöitä, jotka pääsääntöisesti toteuttaa varmasti tehtäviään hyvällä jämptillä tavalla ja samaan aikaan myös kyllä luotan siihen, että sieltä aina löytyy kaverit, jotka ei hoida hommiansa kunnolla, tai ne hoitaa hommiaan moraalisesti ja juridisesti kyseenalaisella tavalla. Kokonaisuutena luotan organisaatioihin.” H6: MIES

8.7 Yhteenveto ja pohdinta

Yliopisto-opiskelijoiden ja henkilökunnan haastattelut (n=20) osoittavat, että poliisin ja tiedusteluviranomaisten toimivaltuudet verkossa ovat monelle tuntematon alue, johon ei ole lähdetty erikseen perehtymään. Tiedonpalasia aiheesta tarttuu lähinnä uutisista, sosiaalisesta mediasta ja televisiosarjoista, mutta kokonaiskuvan luominen on vaivalloista ja yksityiskohdat voivat olla hämäriä. Myös ne henkilöt, jotka ovat perehtyneet aihepiiriin, pitävät toimivaltuuksiin ja tiedustelulainsäädäntöön liittyviä asioita vaikeaselkoisina. Osallistujat pitävät yhteiskunnan kannalta merkittävänä, että viranomaiset kertovat avoimesti toimivaltuuksistaan. Sääntöjen avoimuutta ja tietoista kansalaisten informointia kuvailtiin esimerkiksi *reiluksi peliksi* sekä *kansalaistaidoksi* ja tiedon koetaan mahdollistavan kansalaisten roolin valvoa viranomaistoimintaa. Osallistujat toivoivat pääasiassa perustietoa toimivaltuuksista, kuten mitkä viranomaiset voivat kerätä kansalaisten tieto- ja viestiliikennettä, minkälaisissa tilanteissa ja mihin tarkoituksiin. Sopiviksi viestintäkanaviksi he kokivat esimerkiksi koulut, tiedottamisen kotitalouksiin, kampanjat sekä verkkosivut. Kyselyn (n=236) vastaajat kannattivat laajasti ilmoittamista, jos henkilön tieto- ja viestiliikennettä oli kerätty tai hyödynnetty. Avovastauksissa monet myös kertoivat tiedostavansa, ettei ilmoittamisella pidä kuitenkaan vaarantaa esimerkiksi tutkinnan kulkua.

Haastattelujen perustella syntyy kuva, että tiedon puutteesta tai hataruudesta huolimatta osallistujilla on tyypillisesti oikeansuuntainen käsitys toimivaltuuksista: viranomaisten on mahdollista kerätä tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista tietoa ihmisten toiminnasta — kuten viestinnästä ja käytettyjen laitteiden sijainnista — rikosten selvittämistä tai estämistä varten, mutta toisaalta, käyttäjä voi suojata verkkoliikennettään, jolloin siihen käsiksi pääseminen on vaikeampaa. Yhdellekään haastatellulle ei tullut yllätyksenä, että suomalaiset viranomaiset voivat saada tieto- ja viestiliikenteeseen liittyviä tietoja. Suuri osa vastaajista ei kuitenkaan tiennyt, miten viranomaiset tiedot hankkivat ja että suomalainen lainsäädäntö on muuttunut tiedustelulakien myötä.

Viisitoista haastattelun osallistujaa tunsi kesäkuussa 2019 voimaan astuneita tiedustelulakeja heikosti tai hieman. Käytännössä se tarkoitti, että osa ei ollut kuullut lakimuutoksesta ollenkaan, jotkut vähän osaamatta yksilöidä mitään lain vaikutuksista ja muutama tiesi sanoa ympäripyöreästi, että viranomaisten toimivaltuudet verkossa ovat laajentuneet. Kahdenkymmenen haastattelun joukkoon mahtui lisäksi viisi vastaajaa, jotka olivat tutustuneet tiedustelulakeihin joko jo valmisteluprosessin aikana tai sen jälkeen.

Käytännössä tiedon puute tiedustelulainsäädännöstä näkyi siinä, että iso osa osallistujista rinnasti tiedonhankinnan poliisin rikostutkintaan ja rikosten estämiseen pohtimatta, miten suojelupoliisin tai puolustusvoimien suorittama tiedustelu eroaa tästä. Yksi keskeinen ero on tiedonhankinnan kohdentamisessa. Rikosperustainen tiedonhankinta edellyttää rikoslaissa tarkkarajaisesti määritellyn tunnusmerkistön täyttävää rikosepäilyä, joka käytännössä kohdistuu usein henkilöön tai laitteeseen, jonka uskotaan olevan epäillyn rikollisen hallussa. Vakavat kansallisen turvallisuuden uhkat esitetään sen sijaan laeissa listana tarkemmin määrittelemättömiä kohteita eikä tiedustelumenetelmän käyttö myöskään edellytä rikosepäilyä. Siksi tiedon hankkiminen vakavasti kansallista turvallisuutta uhkaavasta toiminnasta mahdollistaa myös vähemmän kohdennetun tiedonhankinnan kuin rikosperustainen.

Kaikki haastatellut hyväksyvät viranomaisten toimivaltuudet verkossa, kun kyse on vakavan rikoksen, kuten henkirikoksen, tutkinnasta tai epäillyn vakavan rikoksen

estämisestä. Sen sijaan lieväksi koettu rikollisuus piti osallistujien mukaan selvittää pääsääntöisesti muilla tavoin. Kyselytulokset ovat samoilla linjoilla, mutta vastaajien joukossa oli myös henkilöitä, jotka eivät olisi sallineet edes vakavasta rikoksesta epäillyn henkilön toimien seuraamista keskustelupalstalla. Kyselytuloksista piirtyi myös kuva, että tarkemmin rajattu tiedonhankinta on hyväksyttävämpää kuin tavat, joilla haaviin osuu myös sivullisten verkkoviestintää. Useimmat vastaajat odottivat, että jos viestintää seulottiin tietokoneavusteisesti laajemmasta massasta, tulisi epärelevantti viestintä kyetä sulkemaan pois mahdollisimman tarkasti, ennen kuin viestit päätyvät analyytikon pöydälle.

Tästä päästään kysymykseen ymmärtävätkö kansalaiset, että tiedustelulainsäädännön lähtökohtana ovat vakavat uhkat kansalliselle turvallisuudelle, mitkä voivat olla muutakin kuin rikollisuutta ja mitä se tarkoittaa käytännössä? Esimerkiksi tietoliikennetiedustelu menetelmänä perustuu tiedustelutehtävän kannalta olennaisten jälkien seulontaan laajasta määrästä tietoliikennettä, joten tiedusteluviranomaisten haaviin voi päätyä myös tavallisten kansalaisten viestiliikennettä, ei pelkästään turvallisuusuhkaksi tunnistettujen. Epärelevantti viestintä toki kuuluu lain mukaan poistaa, mutta se ei poista faktaa, että tieto voi kuitenkin tulla kerätyksi. Toisaalta on mahdollista, että asia ei ole monelle merkityksellinen legitimiteetin kannalta – sotilas- ja siviilitiedustelu tapahtuu piilossa ja suurin osa siviilitiedustelusta kohdistunee terrorismin torjuntaan, mikä rinnastunee vakavaan rikollisuuteen. Osallistujat eivät olleet erityisen huolestuneita suomalaisten turvallisuusviranomaisten tiedonhankinnasta verkossa, vaan huolet koskivat tyypillisimmin kaupallisten toimijoiden keräämää kuluttajadataa, rikollisuutta tai maita, joissa viranomaiset kontrolloivat tavallisia kansalaisia valvomalla heidän verkkokäyttäytymistään.

Kansalaiset tarvitsevat luotettavaa tietoa poliisin ja tiedusteluviranomaisten toimivaltuuksista Suomessa, jotta he pystyvät osallistumaan tiedonhankintaa koskevaan yhteiskunnalliseen keskusteluun, valvomaan viranomaistoimintaa demokraattisessa valtiossa sekä ymmärtämään millä perustein esimerkiksi heidän viestintäänsä voi päätyä viranomaisten haltuun ja miten viranomaiset huolehtivat, ettei syyttömille koidu harmia. Selkeä kansalaisille suunnattu tiedottaminen mahdollistaa hallitun viestinnän, verrattuna siihen, että jokin väärinkäytösskandaali tai tietovuoto toisi toimivaltuudet tapetille ja samalla paljastuisi, että moni suomalainen olisi luullut toimivaltuuksia edelleen vain rikosperustaiseksi.

Suomessa on korkea luottamus viranomaisiin, mikä näkyi myös tämän tutkimuksen haastatteluissa. Toisaalta joukossa oli myös henkilöitä, jotka luottivat vähemmän viranomaisiin. Monet osallistujat kertoivat kasvaneensa luottamaan yhteiskuntaan ja viranomaisiin jo lapsuudessa. Luottamusta on lisännyt myös omat hyvät kokemukset viranomaisista ja läpinäkyväksi koettu toiminta. Haastatellut tuntuvat kuitenkin muistavan hyvin uutiset viranomaisten tekemistä väärinkäytöksistä – esimerkiksi epäilyt rasismista ja etnisestä profiloinnista, tietokantojen väärinkäytökset sekä ylilyönnit voimankäytössä – merkittävimpänä yksittäisenä tapauksena Jari Aarnion vuosia kestänyt laiton toiminta korkeassa asemassa poliisiorganisaatiossa. Korkeaa luottamusta viranomaisiin ei voi pitää Suomessakaan itsestäänselvyytenä ja haastatellut mainitsivat edellä esitettyjen väärinkäytösten vaikuttavan heidän käsityksiinsä viranomaisista. Siksi viranomaisten on kyettävä vastaamaan kansalaisten huoliin ja osoittamaan konkreettisin keinoin, että organisaatiot tekevät parhaansa, ettei vastaavia väärinkäytöksiä enää tapahtuisi. Lisäksi Suomen muuttuessa monikulttuurisemmaksi ei voi olettaa, että monen haastatellun kuvaama kasvaminen luottamaan yhteiskuntaan ja viranomaisiin olisi jatkossa yhtä tavallista, koska ihmisten taustat poikkeavat toisistaan.

9 ASIANTUNTIJOIDEN JA MAALLIKKOJEN KÄSITYSTEN VERTAILU

Asiantuntijoiden ja maallikkojen haastatteluissa ensimmäinen selkeä ero oli kontekstissa, johon vastaajat asemoivat vastauksensa ja kielessä, jota he käyttivät puhuessaan haastattelun aihepiiristä. Sidosryhmäasiantuntijat, jotka olivat esimerkiksi aiheeseen perehtyneitä politikkoja, viranhaltijoita, kansalaisjärjestöjen tai yritysten edustajia, tutkijoita ja toimittajia, mielsivät poliisin ja tiedusteluviranomaisten toimivaltuudet verkossa erityisesti valmisteilla olleen tiedustelulakipaketin kautta ja he käyttivät tiedustelulakien valmistelusta tuttuja termejä sekä argumentteja tottuneesti. Esimerkiksi kansallinen turvallisuus, siviili- ja sotilastiedustelu, parlamentaarinen valvonta, tiedustelun kohde, rikosperustaisuus, yksityisyydensuoja ja perustuslain muutos olivat haastatteluissa tyypillisesti esiintyviä termejä ja aihealueita. Kutsumme käytettyä kieltä kansallisen turvallisuuden retoriikaksi, koska tiedustelulainsäädännön valmistelussa oli tarkoitus rakentaa suojelupoliisille ja puolustusvoimille tiedustelutoimivaltuudet kansallisen turvallisuuden turvaamiseksi. Sen sijaan yliopistojen opiskelijoilla ja henkilökunnalla, joita kutsumme poliisin ja tiedusteluviranomaisten tiedonhankinnan tuntemuksen osalta maallikoiksi, ei edellytetty olevan erityistä asiantuntemusta aihepiiristä eikä suurin osa heistä tuntenutkaan tiedustelulakeja. Tiedustelulakeja tuntemattomat vastaajat mielsivät viranomaisten toimivaltuudet verkossa suurimmaksi osaksi poliisin työkaluiksi, joita käytetään rikosten selvittämiseen ja estämiseen, eivätkä he puhuneet samalla tavalla kansallisesta turvallisuudesta tai käyttäneet samoja käsitteitä kuin sidosryhmäasiantuntijat. Tiedustelulakien valmistelua seuranneet yliopistolaiset sen sijaan pystyivät yhdistämään puheeseensa piirteitä, jotka ovat yhdistettävissä asiantuntijoiden puhetapaan.

Tutkimuksemme tunnisti kolme sidosryhmäasiantuntijoille tyypillistä näkemystä tarkastella viranomaisten toimivaltuuksia verkossa. Kaikki syntyneet näkökulmat rakentuivat tiedustelulakien ympärille ja kertovat osallistujien näkemyksen tiedustelulaeista. Päädyimme kutsumaan niitä seuraavilla nimillä: Yksityisyyden, vapauksien ja turvallisuuden tasapainoilijat (Tasapainoilijat), Ihmisoikeuksien korostajat (Korostajat) ja Valvontaoikeuksien laajentajat (Laajentajat). Tasapainoilijat ja Laajentajat pitivät valmisteltuja tiedustelulakiesityksiä suurelta osin onnistuneena ja kannattivat niitä sellaisinaan. Siitä huolimatta heidän vastauksissaan oli havaittavissa painopiste-ero. Laajentajat keskittyivät puheessaan tiedustelulainsäädännön edistämiseen ja perustelemaan lakien tarvetta turvallisemman yhteiskunnan näkökulmasta. Tasapainoilijat orientoituivat puolestaan enemmän tulevaisuuteen: miten lait ja niiden ympärille rakennetut tiedustelutoiminnan kontrollimekanismit, joiden tarkoitus on estää väärinkäytökset, tulevat toimimaan käytännössä? Korostajat suhtautuivat lakiesityksiin kriittisimmin. He kantoivat huolta yhteiskunnalle mahdollisesti koituvista kielteisistä seurauksista erityisesti ihmisoikeuksien ja vapauksien näkökulmasta sekä esittivät lakiesityksiin korjausehdotuksia.

Yliopistolaisten haastatteluissa Korostajien edustamat asiat, kuten ihmisoikeuksien turvaaminen, tuntuivat osallistujille tutuimmilta. Monet tunnistivat esimerkiksi, että mm. Kiinan ja Venäjän viranomaiset hyödyntävät ihmisten verkkojälkiä laajemmin kuin Suomi ja tiedonkeruuta voidaan käyttää poliittisia toisinajattelijoita vastaan. He pohtivatkin, voiko samankaltainen kehitys olla joskus mahdollista

Suomessa, vaikka tällä hetkellä se tuntuukin epätodennäköiseltä. Toisaalta haastatteluissa oli havaittavissa myös ymmärrystä myös Laajentajien ja Tasapainoilijoiden näkemykselle, että viranomaiset tarvitsevat toimivaltuuksia tietoverkoissa toimimiseen, jotta he voivat täyttää tehtävänsä kansalaisten ja valtion turvallisuuden ylläpitämisessä. Halusimme ryhmitellä yliopistolaisten haastattelujen analyysissa vastaajat ensisijaisesti heidän tietopohjansa perusteella tiedustelulakeja tunteviin ja tuntemattomiin vastaajiin, etteivät vastausten erilaiset kontekstit olisi vahingossa sekoittuneet ja johtaneet virheellisiin tulkintoihin esimerkiksi asennoitumisesta suomalaisiin tiedustelulakeihin, joita suurin osa ei edes tuntenut.

Kyselyn vastaajien mielipiteet puolestaan järjestäytyivät useimmille tiedonhankinnan perusteita, menettelytapoja ja kohteita mittaavissa kysymyksissä jatkumolle, joka vaihteli kielteisistä myönteisiin käsityksiin. Vastaajat suhtautuivat kriittisemmin viranomaisten toimivaltuuksiin verkossa, kun kyse on lievemmistä rikoksista tai jos tiedonhankinta on kohdentamatonta tai väärin kohdennettua, joka menee syvemmälle syyttömän henkilötietoihin ja viestinnän yksityisyyteen. Sen sijaan vakavan rikollisuuden kohdalla verkkojen valvonta ja verkkoviestinnän kerääminen ja analysoiminen sai enemmistön kannatuksen. Suurin osa vastaajista oli huolestuneempia yritysten ja rikollisten kuin kotimaisten tai edes ulkomaisten tiedusteluviranomaisten harjoittamasta tieto- ja viestiliikenteen keruusta, analyysista ja käyttämistä johonkin tarkoitukseen.

Vaikka yliopisto-opiskelijoiden ja henkilökunnan osalta ei ole suoraan tunnistettavissa jakoa kolmen sidosryhmäasiantuntijanäkökulman kannattajiin, voidaan kuitenkin todeta, että kaikkien aineistojen vastaajissa löytyy kriittisesti, melko neutraalisti sekä myönteisesti viranomaisten toimivaltuuksiin verkossa suhtautuvia vastaajia, mutta valittu analyysitapa vaikeuttaa ryhmien keskinäistä vertailua. On myös oletettavaa, että vastatessaan kysymyksiin kaikkien aineistotyyppien osallistujat hahmottivat erilaisia tiedonhankinnan menettelytapoja, kohteita ja tilanteita mielessään suhteessa moniin muihinkin arvoihin ja tavoitteisiin kuin turvallisuus. Tällaisia tärkeitä arvoja ja tavoitteita ovat esimerkiksi yksityisyys, kirjesalaisuus ja monet muut perustavanlaatuiset oikeudet, kuten mielipiteen vapaus ja syrjinnän kielto. Liiketoiminnallisista intresseistä ei kysytty kuin sidosryhmiltä, mutta niitä tuskin esiintyi samaan tapaan yliopistojen opiskelijoilla ja henkilökunnalla heidän taustansa takia. Lisäksi kaikista aineistoista välittyy vastaajien tarve pitää salaista tiedonhankintaa harjoittavat turvallisuusviranomaiset selontekovelvollisina ja avoimina toimintaperiaatteistaan. Tiedonhankinnan, silloin kun sitä on tarpeen käyttää, halutaan olevan vaikuttavaa ja valvottua sekä viranomaisten käyttämien keinojen tulee olla suhteessa torjuttuun uhkaan.

Puutteet lainsäädännön tuntemuksessa, esimerkiksi millä eri tavoin ja perustein sekä mitkä viranomaiset voivat kerätä, säilöä ja analysoida tieto- ja viestintäverkoista ja niihin kytketyistä laitteista saatavaa tietoa, heikentävät kansalaisten mahdollisuuksia osallistua keskusteluun tiedonhankinnan ja -käytön tulevaisuudesta. Asia on eittämättä laajempi kuin pelkät viranomaisten toimivaltuudet Suomessa ja se kytkeytyy vahvasti paitsi demokraattisen yhteiskunnan kenttään myös teknologioiden, kuten tekoälyn, kehitykseen tulevaisuudessa. Tiedustelulakien hyväksyminen edellytti perustuslain muutosta, mikä päädyttiin tekemään poikkeuksellisesti kiireelliseksi julistamalla. Siitäkin huolimatta, että monessa maassa uhka kansalliselle turvallisuudelle on hyvin tyypillinen peruste kerätä tiedustelutietoa, Suomessa sitä ei oltu kirjattu perustuslakiin kirjesalaisuutta rajoittavana tekijänä aiemmin ja sitä koskevan

asiantuntijakeskustelun aika oli vasta 2010-luvulla tiedustelulakipaketin valmistelun yhteydessä. Keskustelu käytiin pitkälti sidosryhmäasiantuntijoiden välillä ja sen anti tuntuu ainakin haastattelujemme perusteella jääneen vähäiseksi monille tavallisille kansalaisille siitäkin huolimatta, että haastattelemamme yliopistolaiset kokivat poikkeuksetta, että kansalaisten on tärkeä tietää viranomaisten toimivaltuuksista verkossa. Sidosryhmien haastattelut puolestaan osoittivat, että merkittävän lain viranomaisvalmistelussa on tärkeää tiedottaa hankkeen etenemisestä sekä pysähtyä kuuntelemaan ja kohdata eri tahojen näkemykset ja huolet ylenkatsomatta ja väheksymättä. Vuoropuhelun kautta pystytään lisäämään ymmärrystä miksi osapuolet ajattelevat niin kuin ajattelevat ja parhaassa tapauksessa löytämään osapuolten väliltä jotain yhteistä sekä muokkaamaan lakien sisällöt sellaisiksi, että osapuolten on mahdollista hyväksyä ne – siitäkin huolimatta, että kaikki toiveet eivät täyttyneet. Tuloksemme myös osoittavat, että viranomaisten työ avoimuuden edistämiseksi ei pääty lakien voimaan astumiseen. Tieto edistää mahdollisuuksia toimia demokraattisen yhteiskunnan aktiivisena osallistujana. Haastattelemamme yliopistolaiset kokevat, että tiedottamisen vastuu on viranomaisilla ja he toivovat nimenomaan perustietoja: mitkä tahot keräävät tietoja, millä perustein ja mistä syistä. Sidosryhmät ja asiantuntijat puolestaan toivovat yksityiskohtaisempaa tietoa tiedustelun hyödyistä ja kontrollimekanismien toiminnasta nyt kun lait ovat voimassa. Yhteistä molemmille ryhmille on se, että jos suomalaisten viranomaisten toiminnasta ei saada tietoa, käsitys toimivaltuuksista verkossa perustuu mielikuviin, joihin voivat vaikuttaa esimerkiksi tietovuodot, skandaalit ja ulkomaiset esimerkit – olivatpa esimerkit Suomen lain kanssa linjassa tai ei.

10 TOIMENPIDE-EHDOTUKSET

Tässä raportissa esitettyjen tulosten perustella ehdotamme seuraavia toimenpiteitä:

1. **Kansalaisten tietoisuuden lisääminen**: Esitutkinta- ja tiedusteluviranomaisten toimivaltuuksista verkossa järjestetään kansalaisille suunnattu tietoisuuskampanja ja kootaan aiheesta verkkoon pysyväluontoinen, päivittyvä tietopankki. Kampanjassa keskitytään toimivaltuuksien perusasioihin: mitkä tahot saavat kerätä tietoa, millä perusteella, minkälaisissa tilanteissa, mihin tarkoituksiin ja miksi. Myös kontrollimekanismien, kuten lupaprosessin, laillisuusvalvonnan ja parlamentaarisen valvonnan roolit ovat tärkeä oppia tunnistamaan ja ymmärtämään osana kokonaisuutta. Oikeusvaltiossa on annettava tietoa esimerkiksi sitä, kuinka henkilöt, jotka epäilevät joutuneensa tiedustelun kohteeksi, voivat hakea oikeuksiaan ja haastaa viranomaisten käsityksen asioista. Kansalaisten arkeen liittyvät esimerkit ja huolelliset sekä selitetyt termivalinnat auttavat viestin ymmärtämistä. Materiaalia voidaan hyödyntää esimerkiksi oppilaitoksissa, jotta opettajat pystyvät päivittämään opetussisältöjään helposti. Materiaalien suunnittelussa tulisi huomioida mahdollisuuksien mukaan myös erityisryhmät. Tietoisuuden lisääminen parantaa kansalaisten kykyä ottaa osaa koko yhteiskuntaa koskevaan keskusteluun yksityisyydestä ja heistä kerättyjen tietojen hyödyntämisestä niin viranomaisten kuin kaupallisten toimijoiden tarkoituksiin.

2. **Tietoliikennetiedustelun laillisuuden ja vaikuttavuuden seurannasta**: Sotilas- ja siviilitiedustelumenetelmistä sidosryhmiä kiinnosti selvästi eniten tietoliikennetiedustelu. Suojelupoliisin, puolustusvoimien, tiedusteluvalvontavaltuutetun sekä tiedusteluvalvontavaliokunnan kertomat kokemukset tietoliikennetiedustelun käynnistämisestä ja valvonnasta ovat tietoa, jota lakien valmisteluun osallistuneet sidosryhmät toivovat kuulevansa. Esimerkiksi miten tietoliikennetiedustelun valvonta on lähtenyt käyntiin, minkälaisia toimenpiteitä valvojat ovat tähän mennessä tehneet ja mitä operatiiviset toimijat aikovat raportoida paitsi valvojille myös julkisesti tiedustelutoiminnasta. Kunkin tahon toivoisi aidosti puntaroivan, minkälaista tietoa voidaan kertoa julkisuuteen. Vuosikertomukset ja vastaavat tuntuvat kiinnostavan enemmän aihepiiriin perehtyneitä sidosryhmiä kuin kansalaisia. Esimerkiksi kansanedustajista koostuvan tiedusteluvalvontavaliokunnan harjoittama parlamentaarinen valvonta edustaa suorimmin kansalaisia. Silti myös kansalaiset odottavat saavansa suoraa tietoa viranomaisilta siinä muodossa, jossa se on heille ymmärrettävää. Esimerkiksi kertomukset perusoikeuksien toteutumisesta, mahdollisista väärinkäytöksistä, tiedustelun valvonnan toiminnasta, havainnoista ja vaikuttavuudesta auttavat arvioimaan viranomaistoiminnan luotettavuutta.

Tiedon jakaminen on olennaisen tärkeää, jotta tiedon tarvetta ei täytä fiktiiviset tarinat, ulkomaiset esimerkit tai suoranaiset valheelliset käsitykset ja uutiset. Viranomaisten tulee myös käsittää, että nykyisen kaltaisessa viestintä- ja tiedotusmaailmassa jaetun tiedon on oltava oikeaa ja täsmällistä sekä saatavilla nopeasti. Monitulkintaisuudelle tai tietoaukkojen paikkaamiselle valheilla ja kuvitteellisilla ”totuuksilla” ei saa jättää tilaa. Samalla viestinnän ja tiedotuksen tulee olla rehellistä. Kaikki asiat eivät toimi aina täydellisesti, tulokset eivät ole välttämättä tavoitteiden mukaisia ja toiminnoissa löytyy jatkuvasti kehitettävää. Jälkikäteinen tietojen paikkailu ja korjaaminen syövät luottamusta. Riittävän avoin viestintä ja tiedottaminen myös ylläpitävät vahvaa yhteiskunnallista luottamusta.

11 LÄHTEET

ETS No. 005, European Convention on Human Rights [Euroopan ihmisoikeussopimus], as amended by Protocols Nos. 11 and 14 and supplemented by Protocols Nos. 1, 4, 6, 7, 12, 13 and 16. Council of Europe. Saatavilla: https://www.echr.coe.int/documents/convention_eng.pdf Luettu: 7.7.2021

FRA (2017). Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update. Saatavilla: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2017-surveillance-intelligence-services-vol-2_en.pdf Luettu: 1.2.2021

Honkanen, Kosti & Kim, Hanna (2017). Sotilastiedustelulainsäädäntö. Lausuntotiivistelmä. Puolustusministeriön julkaisuja 2017. Puolustusministeriö: Helsinki. Saatavilla: http://julkaisut.valtioneuvosto.fi/handle/10024/80631

Leppänen, Anna & Houtsonen, Jarmo (Hyväksytty julkaistavaksi). Key Stakeholders' Frames on the Police and Intelligence Agencies' Online Surveillance Capabilities in Finland. *Scandinavian Journal of Public Administration.*

Lyon, David (2007). *Surveillance Studies. An Overview*. Cambridge: Polity Press.

Meriniemi, Marko & Lohse, Mikael (2017). Siviilitiedustelulainsäädäntö. Lausuntotiivistelmä. Sisäministeriön julkaisu 21/2017. Sisäministeriö: Helsinki. Saatavilla: https://julkaisut.valtioneuvosto.fi/handle/10024/80630

Poliisihallitus (2019). Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta 2018. Raportti 8.3.2019. POL-2018-55595, ID-1948204.

Riekkinen Juhana (2019). *Sähköiset todisteet rikosprosessissa*. Alma Talent: Helsinki.

Scheinin, Martin (2017). Martin Scheinin: Avoin kirje Sosialidemokraattiselle eduskuntaryhmälle, Vihreälle eduskuntaryhmälle, Vasemmistoliiton eduskuntaryhmälle ja Ruotsalaiselle eduskuntaryhmälle. Perustuslakiblogi, 4.9.2017. Saatavilla: https://perustuslakiblogi.wordpress.com/2017/09/04/avoin-kirje-sosialidemokraattiselle-eduskuntaryhmalle-vihrealle-eduskuntaryhmalle-vasemmistoliiton-eduskuntaryhmalle-ja-ruotsalaiselle-eduskuntaryhmalle/

Sisäministeriön tiedote 043/2017. Parlamentaarinen seurantaryhmä tiedustelulainsäädännön valmistelulle ja perustuslain tarkastamiselle. Julkaistu: 5.5.2017 klo 13.00. Saatavilla: https://intermin.fi/-/parlamentaarinen-seurantaryhma-tiedustelulainsaadannon-valmistelulle-ja-perustuslain-tarkistamiselle Luettu: 19.4.2021

Valtioneuvoston periaatepäätös, 24.1.2013. Suomen Kyberturvallisuusstrategia ja taustamuistio. Saatavilla: https://www.defmin.fi/files/2368/Suomen_kyberturvallisuusstrategia_ja_taustamuistio.pdf Luettu: 2.3.2021

VNT 1/2015. Valtioneuvoston tiedonanto eduskunnalle 29.5.2015 nimetyn pääministeri Juha Sipilän hallituksen ohjelmasta. Saatavilla: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/VNT_1+2015.pdf

Watts, Simon & Stenner, Paul (2012). *Doing Q Methodological Research. Theory, Method and Interpretation*. London: Sage.

Risikko, Paula (2019). Yle-uutiset 2019. Risikko: ”Jos epäily herää, se myös perataan”, tiedustelulait vedettiin poikkeuksellisesti pois täysistunnosta. 13.2.2019 klo 11:21, päivitetty 13.2.2019 klo 16:46. Saatavilla: https://yle.fi/uutiset/3-10644331 Luettu: 26.2.2021

Lainvalmisteluasiakirjat ja työryhmäraportit

Eduskuntakäsittely HE202/2017 vp. Saatavilla: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_202+2017.aspx

Eduskuntakäsittely HE203/2017 vp. Saatavilla: https://www.eduskunta.fi/FI/vaski/KasittelytiedotValtiopaivaasia/Sivut/HE_203+2017.aspx

HE 203/2017 vp Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi. Saatavilla: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_203+2017.pdf

PeVM 4/2018 - HE 198/2017 vp. Valiokunnan mietintö. Perustuslakivaliokunta. Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta. Saatavilla: https://www.eduskunta.fi/FI/vaski/Mietinto/Sivut/PeVM_4+2018.aspx

PeVL 75/2018 vp - HE 202/2017 vp. Valiokunnan lausunto, Perustuslakivaliokunta. Hallintovaliokunnalle. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_75+2018.aspx

PeVL 76/2018 vp - HE 203/2017 vp. Valiokunnan lausunto, Perustuslakivaliokunta. Hallintovaliokunnalle. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. Saatavilla: https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_76+2018.aspx

PTK 94/2018vp Pöytäkirjan asiankohta. 3 Hallituksen esitys eduskunnalle laiksi Suomen perustuslain muuttamisesta. Täysistunto 3.10.2018 klo 14:01. Saatavilla: https://www.eduskunta.fi/FI/vaski/PoytakirjaAsiakohta/Sivut/PTK_94+2018+3.aspx

Siviilitiedustelulakityöryhmä ja siviilitiedustelulakityöryhmän sihteeristö (2017). Siviilitiedustelulainsäädäntö. Työryhmän mietintö. Sisäministeriön julkaisu 8/2017. Saatavilla: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79759/SM_08_2017_Siviilitiedostelulainsaadanto.pdf?sequence=1&isAllowed=y

Tiedonhankintalakityöryhmä (2015). Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän raportti. Puolustusministeriö 2015. Saatavilla: https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf

Työryhmä Nordström, H. et al. (2017). Ehdotus sotilastiedustelua koskevaksi lainsäädännöksi. Työryhmän mietintö. Puolustusministeriö 2017. Saatavilla: http://urn.fi/URN:ISBN:978-951-25-2899-8 Luettu 9.7.2021

Työryhmä Manninen S. et al. (2016). Luottamuksellisen viestin salaisuus. Perustuslakisääntelyn tarkistaminen. Oikeusministeriö. Mietintöjä ja lausuntoja 41/2016). Saatavilla: http://urn.fi/URN:ISBN:978-952-259-533-1

12 LIITTEET

Liite 1 Sidosryhmähaastattelun ohjeistus

Tässä tutkimuksessa kartoitetaan käsityksiä lainvalvonta- ja tiedusteluviranomaisten toimivaltuuksista valvoa verkkokäyttäytymistä ja -viestintää Suomessa, Norjassa ja Britanniassa.

Kuinka seuraavat väitelauseet vastaavat henkilökohtaista näkemystäsi Suomen tilanteesta?

Q-haastattelu vaiheittain

1) Lue nämä ohjeet.

2) Allekirjoita suostumuslomake osallistumisestasi tähän tutkimukseen ja täytä taustatietolomake.

3) Pidä mielessä tämän lomakkeen yläosassa esitetty tutkimustehtävämme: se on kysymyksemme sinulle.

4) Lue läpi väitelausekortit ja levitä ne pöydälle.

5) Järjestä väitelausekortit kolmeen pinoon:
   - olet samaa mieltä
   - olet eri mieltä
   - neutraali: väittämät joita kohtaan ajattelet neutraalisti TAI, jotka herättävät monia, ristiriitaisia tuntemuksia TAI et ole varma mitä asiasta ajattelet

6) Ota iso ruudukko ja väittämäpino "samaa mieltä". Levitä väittämät pöydälle. ***Vertaile väitelauseita suhteessa toisiinsa*** ja valitse kaksi, joiden kanssa olet eniten samaa mieltä ja aseta ne ruudukkoon arvon +5 alle. Valitse jäljelle jääneistä kolme väittämää, joiden kanssa olet eniten samaa mieltä. Ne saavat arvon +4. Asettele loput väittämät ruudukkoon edeten samaan tapaan arvo kerrallaan reunalta kohti ruudukon keskustaa. *Ilmoita tutkijalle, kun olet valmis.*

7) Ota väittämäpino "eri mieltä" ja levitä väittämät pöydälle. ***Vertaile väitelauseita suhteessa toisiinsa.*** Valitse kaksi, joiden kanssa olet eniten eri mieltä ja aseta ne ruudukkoon arvon -5 alle. Valitse jäljelle jääneistä kolme väittämää, joiden kanssa olet eniten eri mieltä. Ne saavat arvon -4. Asettele loput väittämät ruudukkoon edeten samaan tapaan arvo kerrallaan reunalta kohti ruudukon keskustaa. *Ilmoita tutkijalle, kun olet valmis.*

8) Ota väittämäpino "neutraali" ja levitä väittämät pöydälle. ***Vertaile väitelauseita suhteessa toisiinsa.*** Asettele väittämät jäljelle jääneisiin ruutuihin aloittaen väittämistä, joiden kanssa olet eniten samaa mieltä. *Ilmoita tutkijalle, kun olet valmis.*

9) Käy läpi tekemäsi lajittelu ja vaihda korttien paikkoja ruudukolla, jos haluat. Ilmoita, kun olet valmis.

10) Seuraavaksi tutkija kopioi kortin numerot pienempään ruudukkoon ja tallentaa näin tekemäsi järjestyksen.

11) Lopuksi tutkija esittää sinulle kysymyksiä, joiden avulla saat mahdollisuuden kertoa tekemästäsi lajittelusta ja mitä ajattelet esitetyistä väitelauseista. Tämä osuus haastattelusta nauhoitetaan.

Liite 2 Osallistujille esitetyt 45 väitelausetta.

1. Turvallinen internet on elintärkeä väline vapaassa ja demokraattisessa yhteiskunnassa. Tuotteita ja palveluita, jotka tukevat tätä turvallisuustavoitetta, ei tule vaarantaa luovuttamalla salausavaimia.

2. Esitutkinta- ja tiedusteluviranomaisten tietopyynnöt rasittavat kohtuuttomasti verkon palveluntarjoajia.

3. Verkkoja valvomalla saatu aineisto tulisi tuhota välittömästi kun juttu on päättynyt, eikä tietoa tulisi käyttää muuhun tarkoitukseen kuin se oli kerätty.

4. Koska uusia valvontamenetelmiä tuodaan lainsäädäntöön vaiheittain, hämärtyy kokonaiskuvan lainsäädännön laajuudesta.

5. Yksityisyyttä eniten loukkaavia verkkovalvontamenetelmiä, kuten teknisiin laitteisiin tunkeutumista, tulisi käyttää vain kaikkein vakavimmissa rikoksissa tai kansallisen turvallisuuden vakavissa uhkissa.

6. Saadaksemme arvokasta tietoa kansallisen turvallisuuden vakavista uhkista, meidän täytyy vahvistaa kansainvälistä yhteistyötämme.

7. Viranomaisten laajempi pääsy verkkoviestintään tulee parantamaan yhteiskunnan ja kansalaisten turvallisuutta.

8. Radikalisoituneet ihmiset, jotka ovat vaarassa muuttua väkivaltaiseksi, tulisi tunnistaa heidän verkkokäyttäytymisensä perusteella ja heidän viestintäänsä tulisi valvoa.

9. Tietoliikennetiedustelu on tehokas ja luotettava menetelmä paljastaa ennestään tuntemattomia kansallisen turvallisuuden uhkia.

10. Nykyinen turvallisuus- ja rikollisuustilanne oikeuttaa laajemmat kyberympäristön valvontamenetelmät.

11. Ihmisten joilla ei ole mitään salattavaa, ei tarvitse huolestua viranomaisvalvonnasta.

12. Tiedustelutietoa tulisi jakaa tai vastaanottaa vain sellaisten maiden kanssa, jotka noudattavat YK:n ihmisoikeussopimusta.

13. Perinteiset (offline) valvontamenetelmät ovat paljastaneet mitä ihmiset tekevät, mutta verkkoviestinnän valvonta paljastaa mitä ihmiset ajattelevat. Ero on perustavanlaatuinen yksityisyydensuojaan kajoamisen kannalta.

14. Tiedustelumenetelmien kohdentaminen ei saa olla syrjivää eli perustua ilman hyväksyttävää syytä esimerkiksi kohdehenkilön alkuperään, uskontoon, mielipiteeseen, yhteiskunnalliseen ryhmään kuulumiseen tai muuhun henkilöön liittyvään syyhyn.

15. Suojasta huolimatta tiedustelu on voitava kohdistaa myös arkaluontoisissa ammateissa työskentelevien, kuten lakimiesten, toimittajien tai lääkärien, viestintään, jos he viestivät kansallista turvallisuutta uhkaavan henkilön kanssa.

16. On elintärkeää, että ihmisillä on samat perusoikeudet tietoverkoissa kuin verkon ulkopuolella.

17. Jos lisäämme verkkojen valvontaa terrori-iskujen seurauksena, heikennämme juuri niitä arvoja, joita vastaan terroristit hyökkäävät.

18. Mahdollisuus valvonnan kohteeksi joutumisesta verkossa johtaa itsesensuuriin ja pelkoon sekä lopulta tukahduttaa demokraattisen keskustelun ja ajatuksen vapauden.

19. Meidän on rajoitettava viranomaisille myönnettäviä toimivaltuuksia nykyisyydessä, koska emme voi vaikuttaa siihen, kuinka tulevat hallinnot saattavat käyttää niitä.

20. Viranomaiset turvautuvat ja luottavat liikaa siihen, mitä digitaalisen viestinnän valvonnalla voidaan saavuttaa.

21. Maan rajat ylittävän verkkoviestinnän valvonta on hyväksyttävämpää kuin maan sisäisen viestinnän valvonta.

22. Maahamme suunniteltu, maamme rajat ylittävään verkkoliikenteeseen kohdistuva tietoliikennetiedustelu perustuisi tietoliikenteen suodattamiseen tiettyjen parametrien avulla ennen kuin data lähetetään analysoitavaksi. Kyseessä on siksi kohdennettu valvontakeino, ei massavalvonta.

23. Medialla on liikaa vaikutusvaltaa julkisen mielipiteen muodostumisessa verkkovalvonnasta.

24. Valtion viranomaiset saavat haluamansa käydystä julkisesta keskustelusta huolimatta.

25. Maani lainsäädäntö [arvioi myös hallituksen esitystä uudesta tiedustelulakipaketista] on tasapainossa turvallisuustavoitteiden ja yksityisyydensuojan osalta.

26. Yksityisyyden loukkaus tapahtuu jo kun tieto kerätään ja tallennetaan; se ei edellytä tiedon katsomista.

27. Rikolliset löytävät aina keinot kiertää viranomaisvalvonta verkossa, esimerkiksi siirtymällä käyttämään ulkomaisia verkkopalveluntarjoajia maissa, jotka loukkaavat yksityisyyttä vähemmän.

28. Teknologia kehittyy niin nopeasti, että viranomaisilla ja lainsäädännöllä on vaikeuksia pysyä kehityksessä mukana.

29. Jos kansalaiset hyväksyvät, että heidän yksityisyyttään loukataan turvallisuuden vuoksi, he eivät täysin ymmärrä, miksi yksityisyys on niin tärkeää digitaalisella aikakaudella.

30. Yksityisyyden loukkaamisen tasossa ei ole eroa, tarkasteltiinpa viestin sisältöä tai välitystietoja.

31. Kun kyseessä on kansallinen turvallisuus, verkkojen valvontaa koskevan lainsäädännön tulisi olla maamme hallinnon päätettävissä, ei ulkoisten tahojen, kuten EU:n.

32. Kansalaiselle tulisi kertoa jälkikäteen, jos hänen verkkoviestintäänsä on avattu, tallennettu tai käytetty tutkinnassa.

33. Verkkoviestinnän big data -analyysi tulee johtamaan virhearvioiden takia huonoihin yksilöitä koskeviin päätöksiin.

34. Verkon palveluntarjoajan tulisi säilyttää lainvalvontaviranomaisia varten tallentamia tietoja 12 kuukauden ajan, jotta tutkintamahdollisuuksia voitaisiin hyödyntää täysimääräisesti.

35. Kohdennetusta valvonnasta tulee massavalvontaa, jos sillä saadaan tietoa myös sellaisten henkilöiden viestinnästä, jotka eivät suoraan viesti epäillyn kanssa.

36. Verkkovalvontamenetelmien käytön laajuudesta ja tuloksista tulisi tiedottaa julkisuuteen riittävän usein ja riittävällä tarkkuudella, jotta kansalaisten luottamus esitutkinta- ja tiedusteluviranomaisiin säilyisi eikä heräisi epäilyksiä todellista laajemmista operaatioista.

37. Tietoliikennetiedustelun ennalta estävä vaikutus korvaa kaikki aiheutuvat taloudelliset ja yhteiskunnalliset kustannukset.

38. Täyden demokraattisen kontrollin mahdollistamiseksi taholla, joka vastaa tiedustelupalvelujen valvonnasta ja sääntelystä, tulee olla riittävä tieto ja tekninen ymmärrys valvottavan tahon valmiuksista ja toiminnasta.

39. Täysin itsenäiset valvontamekanismit ovat tehokkaampi tapa turvata oikeutemme kuin että yrittäisimme rajoittaa tai poistaa käytössä olevia viranomaisten toimivaltuuksia.

40. Esitetty tiedustelulainsäädäntö on verkkotiedustelumenetelmien osalta niin tulkinnanvarainen ja sirpaleinen, että sitä on vaikea ymmärtää ja se on avoin laajoille tulkinnoille.

41. Tuomioistuinten tulisi arvioida jokainen lupahakemus itsenäisesti ja täysimääräisesti, eikä tehdä päätöstä pelkkään luvanhakijan arvioon nojaten.

42. Maan rajat ylittävän verkkoliikenteen valvonnan (tietoliikennetiedustelun) lupaprosessissa tulisi olla mukana tuomarin ja tiedusteluviranomaisen lisäksi julkinen asiamies tai vastaava, joka valvoisi tiedustelun kohteeksi joutuvien oikeuksia ja etuja.

43. Vakoiluohjelmiin liittyviin tiedustelulupiin tulisi sisällyttää analyysi, mitä vahinkoa ohjelma voi aiheuttaa tietojärjestelmälle tai sen ohjaamalle prosessille, sekä uskottava kuvaus, miten ohjelmisto poistetaan vaaraa aiheuttamatta.

44. Salaisten tiedonhankintakeinojen väärinkäytösten ilmoittamiseen on taattava anonyymi, itsenäinen oikeudellinen kanava, jonne kaikilla tasoilla työskenteleviä kannustetaan ilmoittamaan epäilynsä ilman, että siitä aiheutuu vaaraa heille tai kansalliselle turvallisuudelle.

45. Verkkojen valvontaan liittyvät lupakäytännöt voivat aiheuttaa riskejä estämällä tai viivyttämällä tutkintaa kohtuuttomasti.

POLIISI
POLIISIAMMATTIKORKEAKOULU

Tässä raportissa paneudutaan poliisin ja tiedusteluviranomaisten toimivaltuuksiin hankkia tietoa tieto- ja viestintäverkoista sekä niihin kytketyistä laitteista. Aihepiiriä tarkastellaan kolmen empiirisen tutkimusaineiston avulla. Tutkimusaineistot antavat käsityksen millaisia ajatuksia, huolia ja tiedontarpeita toimivaltuudet herättävät Suomessa asuvissa sidosryhmäasiantuntijoissa, yliopisto-opiskelijoissa ja yliopistojen henkilökunnassa. Tuloksia pohjustetaan esittelemällä tiedustelulainsäädännön valmisteluprosessin keskeiset vaiheet sekä lyhyesti myös lainsäädäntöä, joka säätelee poliisin ja tiedusteluviranomaisten salaista tiedonhankintaa verkossa.

Raportti on kirjoitettu kaikille, jotka ovat kiinnostuneita poliisin ja tiedusteluviranomaisten toimivaltuuksista verkossa. Julkaisun tarkoitus on tarjota helposti lähestyttävää perustietoa, lisätä lukijoiden tietoisuutta tiedonhankinnasta sekä edistää keskustelua aihepiiristä. Raportti on hyvin ajankohtainen, koska sen keskiössä on kesäkuussa 2019 voimaan astunut tiedustelulainsäädäntö ja sen tuomat muutokset. Tulosten perusteella ehdotamme, että Suomeen tarvitaan tietoisuuskampanja viranomaisten toimivaltuuksista verkossa ja tietoa tiedustelumenetelmien, erityisesti tietoliikennetiedustelun, vaikuttavuudesta ja suojamekanismien toimivuudesta. Avoin viestintä ylläpitää vahvaa yhteiskunnallista luottamusta.

9 789518 153996 >

Poliisiammattikorkeakoulu • Vaajakatu 2, 33720 Tampere • puh. 0295 480 121 • www.polamk.fi