TIEDONHANKINTA VERKKOYMPÄRISTÖSTÄ – OIKEUDELLISIA NÄKÖKULMIA

Oikeustieteellinen tutkielma

Matti Raivikko

10/2017

POLIISIAMMATTIKORKEAKOULUN OPINNÄYTETYÖ / AMK

Tiivistelmä

Tekijä Matti Raivikko	Tutkinto Poliisi (AMK)
Julkaisun nimi Tiedonhankinta verkkoympäristöstä – Oikeudellisia näkökulmia	Julkisuusaste Julkinen
Ohjaaja Antti Jääskeläinen	Opinnäytetyön muoto Oikeusdogmaattinen tutkimus

Tiivistelmä

Poliisi suorittaa yleisvalvontaa ja tarkkailua verkkoympäristössä siinä missä reaalimaailmassakin, mutta verkkoympäristön osalta tekaistujen tietojen käyttö on korostuneessa roolissa. Tässä opinnäytetyössä selvitetään poliisin mahdollisuutta yleisvalvontaan ilman näkyviä poliisitunnuksia verkkoympäristön suljetuilla keskustelupalstoilla ja sosiaalisessa mediassa nykyisen lainsäädännön mukaan.

Sosiaalisen median käyttö on yleistynyt 2010-luvulla ja rikollisuus verkkoympäristössä lisääntynyt reilusti. Poliisin läsnäolo verkossa on täten perusteltua ja tarpeellista. Osa sosiaalisen median palveluista ja keskustelupalstoista vaatii kuitenkin kirjautumisen omalla nimellä, jotta viestejä pääsee lukemaan. Oman nimen käyttö ei valvonnan kannalta ole aina optimaalista.

Käytännön ohjeistusta valvonnan suorittamiseksi on ollut vähän tarjolla. Lainsäädännössä otetaan heikosti kantaa verkkoympäristön erityispiirteisiin ja lainsäätäjän tahto on vaikeasti tulkittavissa verkkoympäristön valvontaa koskien. Tästä syystä näkymättömän valvonnan laillisuutta oli tarve tutkia.

Tutkimusmenetelmänä tässä työssä on käytetty oikeusdogmatiikkaa eli lainoppia. Työssä esitellään aihepiiriä koskeva lainsäädäntö, lainsäädännön valmistelutöitä, oikeustieteellistä kirjallisuutta sekä aikaisempia tutkimuksia. Pohdinnat osiossa käydään vertailua oikeushyvien välillä ja haetaan tulkintoja aiheeseen esimerkkien ja käytännön kautta.

Opinnäytetyön lopputuloksena esitetään, että poliisi voi käyttää tekaistuja tietoja kirjautuessaan verkkoympäristöön valvontaa suorittaakseen. Tuloksista ilmenee kuitenkin se, että myös toisenlaista johtopäätöstä tukevia tekijöitä lainsäädännöstä löytyy. Lainsäädännöstä pitäisi saada selkeämpi ja siinä pitäisi huomioida reaalimaailman lisäksi myös verkkoympäristö nykyistä paremmin.

Sivumäärä 28 sivua	Tarkastuskuukausi ja vuosi marraskuu 2017	Opinnäytetyökoodi (OPS) mAmk2016ONT

Avainsanat

lainsäädäntö, oikeus, sosiaalinen media, tiedonhankinta, toimivalta, valvonta, verkkoympäristö

SISÄLLYS

1 JOHDANTO

Syksyllä 2015 kävin kuuntelemassa Henk Van Essin luentoa Keskusrikospoliisin tiloissa. Van Ess kertoi seikkaperäisesti, mitä kaikkea tietoa internetin avoimista lähteistä pystyy kaivamaan esiin. Tämä luento perustui tietysti sellaisiin menetelmiin, mitä käyttämällä ei syyllisty mihinkään rikokseen. Van Ess kertoi erityisesti Facebookista, jolla on tällä hetkellä noin kaksi miljardia käyttäjää maailmassa. Van Essin mukaan kaikki arkaluontoinenkin tieto, mitä hän sai kaivettua esiin muun muassa kurssiin osallistujista vaikka he olivat salanneet profiiliaan, löytyy internetistä. Ihmiset itse asiassa paljastavat yllättävän paljon tietoa itsestään muun muassa merkitsemällä osallistumisensa julkisiin tapahtumiin ja kirjoittaessaan viestejä julkisen profiilin omaavien ystäviensä Facebook-seinälle. Tieto, jota Van Ess esitteli, on saatavilla internetistä, mutta sen saadakseen täytyy olla itsekin kirjautuneena palveluihin, joista tietoa hakee.

Van Ess on luennoitsija, sosiaalisen median ja internettiedustelun opettaja, kirjailija ja paljon muuta, mutta ei virkamies. Henk Van Ess ei varsinkaan ole poliisi, jolle on laissa annettu toimivaltuudet ja tehtävät. Poliisilaissa määritellään, että yksi poliisin tehtävistä on valvoa yleistä järjestystä ja turvallisuutta. Valvonta internetissäkin eittämättä kuuluu poliisin tehtäviin, mutta lainsäädännössä ei sanota suoraan, miten tuota valvontaa tulee suorittaa. Van Ess sivusi luennollaan aihetta itsekin. Hän sanoi tiedon olevan saatavilla, mutta muistutti myös lainsäädännöstä ja vastuusta. Van Ess ei kuitenkaan ole Suomen lain asiantuntija, joten hän ei osannut sanoa, miten valvontaa Suomessa saa tehdä.

Asia jäi askarruttamaan myös minua. Sosiaalisen median käyttöä ei ole koulutettu valtaosalle poliisihenkilöistä ollenkaan. Itse asiassa suuri osa poliiseista on koulutettu jo ennen kuin internet vakinaisti asemansa päivittäisessä käytössä. Voimassaolevaa ohjeistusta asiaan ei myöskään löytynyt. Van Essin luentoon pohjautuen pidin tunnin mittaisen työpaikkakoulutuksen poliisilaitoksen työntekijöille avoimien tietolähteiden tiedonhankinnasta. Tässäkään vaiheessa en osannut sanoa miten valvontaa kuuluisi suorittaa ja mihin lakiin se pohjautuu. Perustuslaki kuitenkin edellyttää poliisilta lain tuntemista ja noudattamista. Perustuslain mukaan kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Keskusteluissa esimiesteni kanssa sain tietää, että ohjeita asiasta on pyydetty Poliisihallitukselta, mutta niitä ei ollut vielä saatu, kun opinnäytetyötäni aloitin tekemään alkukeväällä 2017.

Poliisihallitus esitti kannanottonsa verkkoympäristössä tapahtuvaan tiedonhankintaan poliisilaitoksille suunnatulla kirjeellä kesäkuussa 2017. Tämä osoittaa aiheen ajankohtaisuutta, mutta toisaalta asetti kyseenalaiseksi tutkimuksen tarpeellisuuden etenkin poliisilaitosten näkökulmasta, kun ohjeistusta oli nyt saatu. Tulin kuitenkin siihen tulokseen, että julkinen tutkimus aiheesta on tarpeellinen asian monimutkaisuuden vuoksi. Tarpeellisuuden puolesta puhuu myös se, että Poliisihallituskin on päätynyt lähestymään poliisilaitoksia pelkällä kirjeellä, varsinaisen valtakunnallisen ohjeen sijaan.

Kirjeessään Poliisihallitus kertoo näkemyksensä aiheesta ja antaa toimintamalleja poliisilaitoksille. Kirjeen suojaustasosta johtuen sitä ei käsitellä tässä työssä tämän enempää, sillä haluan opinnäytetyöni olevan avoin julkiselle tarkastelulle ja arvostelulle. En myöskään ota kantaa siihen vastaavatko tutkimukseni tulokset Poliisihallituksen näkemystä.

Suomen lainsäädännössä ei sanota saako virkamies perustaa työtään varten tilin sosiaalisen median palveluun. Suomen lainsäädännössä ei myöskään sanota, että saako poliisi käyttää omaa henkilökohtaista sosiaalisen median profiiliaan virkatehtäviensä tekemiseen. Valtion virkaehtosopimuksessa mainitaan kyllä, että pakottavista syistä voi virkamatkan, joka myös luetaan virkatehtäväksi, tehdä omalla autolla, mikäli yleisiä kulkuneuvoja ei kulje. Oman sosiaalisen median käyttäjäprofiilin käytöstä virkatehtävien tekemiseen ei kuitenkaan missään suoraan mainita. Ongelma vaatii siis useamman poliisin toimintaa ohjaavan lain tulkintaa ja näiden tulkintojen yhdistämistä yhtenäiseksi kokonaisuudeksi.

Poliisi on perustanut useita nettipoliisin virkoja Suomeen viimeisen vuoden aikana. Nettipoliisit valvovat internetissä yleisiä avoimia sivustoja, ennalta estävät rikollisuutta, etsivät rikollista toimintaa internetistä ja ovat tavoitettavissa. Myös jokaisen rikostutkijan täytyy osata käyttää internetiä tiedonhakuun. Ongelmatonta tiedonhankinta on, kun liikutaan yleisvalvonnan piirissä tai haetaan tietoa täysin avoimista internetlähteistä. Mutta miten poliisin tulee toimia, kun mennään niin sanotun rajatun avoimen datan äärelle, palveluihin, joihin täytyy kirjautua sisään luomalla käyttäjätunnukset? Voiko poliisi esiintyä väärällä nimellä esimerkiksi kirjautuessaan sosiaalisen median palveluihin? Voiko poliisi yrittää hankkia tavoitettavuutta koskevaa tietoa henkilöistä sosiaalisen median palveluista edes virallisella profiilillaan? Missä kulkevat salaisen tiedonhankinnan mukaisen tarkkailun ja suunnitelmallisen tarkkailun taikka peitellyn tiedonhankinnan rajat? Näihin kysymyksiin on tarkoitus tässä tutkimuksessa löytää vastaus.

1.1 Tutkimuksen tausta

Avoimien tietolähteiden käyttö rikostorjunnassa lisääntyy koko ajan. Perinteiset, viranomaisrekistereihin perustuvat tiedonhankintakeinot eivät ole enää riittäviä, kun tietoa on internetistä vapaasti saatavissa enemmän kuin suljetuissa viranomaisrekistereissä. Ihmisten tavoitettavuuskin voi olla helpompaa internetin välityksellä kuin perinteisesti puhelimitse tai kirjeitse.

Nettipoliisin virkoja on perustettu poliisiin viimeisen vuoden aikana lukuisia ja valvontaa internetissä tehostetaan (Mäntymaa 2017). Resurssien vähentyessä (Kari 2017, 13-21) ennaltaehkäisevää työtä on pyritty tekemään internetissä, jossa tavoitetaankin huomattavasti suurempi määrä ihmisiä kuin esimerkiksi perinteisellä lähipoliisitoiminnalla. Nettipoliisitoiminta perustuukin poliisin ja kansalaisten avoimeen kanssakäymiseen. Rikostutkijat puolestaan tarvitsevat toisenlaista tietoa selvittäessään rikoksia. Nettipoliisit eivät ehdi kaikkien rikostutkijoiden tiedonjanoa täyttämään, vaan on jokaisen rikostutkijan oma tehtävä kaivaa esiin tarvitsemansa tieto tarjolla olevista tietolähteistä. Rikostutkijoille

ei ole kuitenkaan tehty vielä selväksi, mitä internetissä saa poliisina lain mukaan tehdä eikä sitä miten internettiedustelussa tulee toimia.

1.2 Tutkimusongelma ja tavoitteet

Opinnäytetyöni on lainopillinen tutkimus. Tutkimuksessa on tarkoitus selvittää poliisin keinoja tiedonhankintaan internetin palveluissa, jotka vaativat sisäänkirjautumisen. Tutkimuksen ongelman voi kiteyttää yhteen kysymykseen: Onko internetin rajattu avoin tieto avointa myös poliisille ja miten poliisin tulee toimia verkkoympäristössä? Poliisin toimintaa määrittävät lait ja asetukset, joista lainopillisin keinoin haetaan vastaus siihen, mikä on viranomaisen rooli suhteessa verkossa sijaitsevaan vapaasti saatavaan informaatioon. Käsittelen tutkimuksessa pääosin Facebook-palvelua, joka on suosituin sosiaalisen median kanava yli kahdella miljardilla rekisteröityneellä käyttäjällä (Kallas 2017). Samat lainalaisuudet pätevät pääasiassa myös muihin sosiaalisen median palveluihin sekä keskustelufoorumeihin, joihin käyttäjät kirjaavat tietoja itsestään ja käyttäjät ovat yksilöitävissä.

Aiheen tutkiminen on tärkeää, jotta saadaan selkeät ohjeet peruspoliisitoiminnassa tehtävään tietojen hankintaan. Tiedän kokemuksesta, että tällä hetkellä muun muassa sosiaalista mediaa käydään läpi poliisin virkatehtäviin liittyen rikostutkijoiden omilla henkilökohtaisilla profiileilla tai vaihtoehtoisesti tekaistuilla profiilitiedoilla. Käyttäjien profiilit sisältävät mahdollisesti paljon tietoa heistä ja näiden tietojen hankinta voi olla todella on nopeaa ja helppoa. Tieto voi olla houkuttelevasti vain yhden klikkauksen päässä. Laillisuusnäkökulmasta tarkasteltuna tuon klikkauksen tekeminen saattaa kuitenkin vaatia esimerkiksi päätöksen pakkokeinosta. Se, mitä jokainen siviili voi tehdä internetissä rikkomatta lakia, ei aina vastaa sitä mitä poliisi voi tehdä. Reaalimaailman esimerkki: Kun kerrostaloyhtiössä asukas A-portaasta vahtii B-portaan asukkaan tekemisiä ja liikkumista jopa tallentamalla kuvamateriaalia naapuristaan, ei hän välttämättä riko mitään lakia. Jos poliisi tekee tuon saman, puhutaan salaisista tiedonhankintakeinoista. Jos poliisi ei itse selvitä sääntöjä ja tee rajanvetoja hyvissä ajoin, voi edessä olla tilanne, että poliisin täytyy oppia ulos lainvastaisista keinoista.

1.3 Työn rajaus

Tässä tutkimuksessa ei käydä läpi poliisin näkyvää toimintaa internetissä eli niin sanottua kansalaisia palvelevaa nettipoliisitoimintaa. Tutkimuksessa ei käsitellä verkossa tapahtuvaa niin sanottua kyberrikollisuutta, vaan poliisin valvontaa ja tietojenhankintaa internetin rajatuista avoimista lähteistä muusta kuin verkossa tapahtuneesta rikoksesta johtuen. Tutkimuksen tarkoituksena on selvittää voiko tai milloin poliisi voi laillisesti hakea tietoa internetin rajatuista avoimista lähteistä.

1.4 Tutkimusasetelma ja menetelmät

Pyrin työssäni selvittämään lain ja oikeuden suhdetta poliisin tiedonhankintaan internetin rajatuissa avoimissa tietolähteissä. Poliisin toimintaa internetissä ei ohjaa erityinen lainsäädäntö. Tästä syystä tutkimuksessa pyritään tuomaan esiin ne lainkohdat, jotka vaikuttavat poliisin internetiä koskevaan tiedonhankintaan. Lainkohdat analysoidaan ja niiden sisältöä tulkitaan muita oikeuslähteitä hyväksikäyttäen. Lopulta pohdintaosiossa mietitään miten säännöksiä tulisi tulkita normaalissa päivittäisessä poliisitoiminnassa. Tutkimusmenetelmänä käytän oikeustieteiden lainoppia.

Oikeustiede tutkii oikeutta tutkimustieteenä. Sille ei ole selkeää yhtä määrittelyä. Oikeustieteen tutkimuksella pyritään tukemaan oikeudellista ratkaisutoimintaa. Oikeustieteellisen tutkimuksen tavoitteena on oikeudellisen tiedon systematisointi ja tulkinta. Oikeustieteellisessä tutkimuksessa käytetään perusaineiston säädöksiä, hallituksen esityksiä ja eduskuntakäsittelyissä syntyneitä asiakirja-aineistoja riippuen siitä, mitä halutaan tietää. (Miettinen 2016, 79.)

Lainoppi eli oikeusdogmatiikka on puolestaan oikeustieteen tutkimusmenetelmä, joka tutkii oikeudellisia tekstejä. Lainoppi tulkitsee oikeusnormeja, niiden ajatussisältöjä sekä sanojen ja tekstien merkityksiä. Lainopillinen tutkimus pyrkii siis selvittämään tutkimuskysymykseen vastauksen. Sen mitä laki sanoo ja miten tuota sanomaa tulkitaan. (Hirvonen 2011, 36.)

Tässä opinnäytetyössä on tarkoitus nimenomaan tulkita lainopillisesti tutkimuskysymystä. Selkeää oikeusnormia tutkittavaan aiheeseen ei ole, joten opinnäytetyössä täytyy tulkita useampaa lakia ja koostaa käsitys lainsäätäjän tahdosta.

1.5 Aihealueen aikaisemmat tutkimukset

Virtuaalista poliisitoimintaa on tutkittu aikaisemmin muutamissa tutkimuksissa. Poliisin toimintaan sosiaalisessa mediassa liittyviä opinnäytetöitä tai päättötöitä on tehty Poliisikoulussa ja nykyisessä Poliisiammattikorkeakoulussa useita. Kuitenkaan yhdessäkään tutkimuksessa ei oteta kantaa laillisuusnäkökulmaan poliisin toimiessa virkatehtävissään tietoa hankkiessaan avoimessa internetissä. Internet ja sosiaalinen media on aiemmin koettu hyväksi paikaksi lähipoliisitoiminnalle. Siellä on helppo kohdata poliisi lähes anonyymisti ja vaikeisiinkin asioihin saa apua.

Sosiaalisen median suuren käyttäjämäärän ja käsittämättömän suuren datamäärän on havaittu antavan paljon informaatiota myös poliisin tiedonhankintaan. Kuitenkaan laillisuuskysymystä ei ole vielä herätetty siitä, miten paljon poliisi voi seurata eri henkilöiden toimintaa internetissä.

2 TEOREETTINEN VIITEKEHYS

Tutkimus on oikeustieteellinen tutkimus, jonka teoriapohja tulee sen tarkastelusta, miten Suomen lait, hallituksen esitykset ja oikeustieteellinen kirjallisuus ohjaavat poliisin toimintaa tiedonhankinnan suhteen. Tutkimuksella pyrin selvittämään mitä ovat ne lait, jotka ohjaavat poliisin kyseistä toimintaa ja löytyykö täsmentävää tietoa kyseisten lakien valmistelutöistä tai kirjallisuudesta.

Tässä luvussa kerron mitä tutkimuksessa käytetyt käsitteet tarkoittavat. Keskeiset käsitteet liittyvät sosiaaliseen mediaan, tiedonhankintaan ja tietolähteeseen.

Omassa kappaleessaan esittelen yhden sosiaalisen median sovelluksen, Facebookin, toimintaperiaatteen. Koska tutkimus käsittelee yksinomaan datan hankintaa sellaisista kaikille avoimista lähteistä, jotka vaativat sisäänkirjautumisen, on toimintaperiaatteen ymmärtäminen keskeistä koko tutkimuksen kannalta. Toimintaperiaatteet tiedon jakamisen kannalta pätevät moniin muihinkin sosiaalisiin medioihin, keskustelupalstoihin ja muuhun vastaavaan dataan internetissä, mutta Facebookin esittely on valittu siitä syystä, että se on niistä suurin.

2.1 Keskeiset käsitteet

2.1.1 Tiedonhankinta

Reijo Savolainen (2010, 91-92) määrittelee tiedonhankinnan olevan yleisesti ymmärrettynä näkö ja kuuloaistiin pohjautuvaa tiedontarpeesta johtuvaa toimintaa, jonka tarkoituksena on tunnistaa merkityksellisiä tiedonlähteitä ja kanavia, hakeutua niille ja hyödyntää niitä. Tiedonhankinta ei ole Savolaisen mukaan itsearvoinen prosessi vaan se palvelee jotakin muuta päämäärää, esimerkiksi opiskelua, suunnittelua tai työtehtävää. Tiedonhankinta on siis Savolainen mukaan väline jonkin muun asian suorittamiseksi. Tietoa tarvitseva hankkii Savolaisen mukaan tietoa erilaisia kanavia hyödyntäen.

Tiedonhankinnalla tässä tutkimuksessa tarkoitetaan ammatillisessa mielessä tarvittavaa tiedon etsintää tiedonhankintakanavan ollessa internetin rajattu avoin tietolähde. Tiedonhankinta voi olla esimerkiksi yhteystietojen etsintää tällaisesta palvelusta.

2.1.2 Rajattu avoin tietolähde

Rajatulle avoimelle tietolähteelle ei ole varsinaista määritelmää olemassa. Termi sinällään on uusi, koska internetissä olevat sosiaalisen median palvelut on tarkoitettu lähtökohtaisesti avoimiksi eikä niitä pidetä varsinaisessa mielessä tietolähteinä vaan sosiaalisen median alustoina. Tässä tutkimuksessa käytän termiä ”rajattu avoin tietolähde” kuvaamaan kaikkia sellaisia internetin palveluita, joihin täytyy kirjautua sisään päästäkseen palvelun sisältämään dataan käsiksi. Palveluissa ei kuitenkaan yleensä ole sellaista ominaisuutta, että ne tarkastaisivat kirjautujan henkilöllisyyden, joten käytännössä

kirjautuja voi olla kuka tahansa. Rajatuissa avoimissa tietolähteissä saattaa olla myös osioita, joihin pääsee osallistumaan vain saamalla hyväksynnän toiselta käyttäjältä.

2.1.3 Sosiaalinen media

Ei ole aina täysin selvää mitä termillä ”sosiaalinen media” tarkoitetaan. Sosiaaliselle medialle ei ole olemassa yhtä ainoaa tarkoitusta. Termin tarkoitus on myös muuttunut ajan myötä. Nykyään sosiaalinen media on vakiintunut tarkoittamaan internetin käyttäjän roolin uudistumista aktiivisempaan suuntaan. Käyttäjä ei ole enää ainoastaan tiedon vastaanottaja vaan myös tiedon jakaja sekä tuottaja. (Suominen 2013, 15-16). Poliisihallituksen ohjeen (Poliisihallitus 2017) mukaan sosiaalinen media on verkkoviestintäympäristö, jossa jokaisella on mahdollisuus olla aktiivinen viestijä ja sisällöntuottaja vastaanottajana olemisen lisäksi.

Tällä tavalla sosiaalinen media on todella laaja käsite sisältäen keskustelupalstat, videotoistopalvelut ja sosiaaliset verkostoitumispalvelut. Kallialan ja Toikkasen (2012, 18) mukaan sosiaaliseen mediaan liittyy sisällön tuottamisen ja sisällön käyttämisen sekoittuminen.

Sosiaalinen media on siis uudenaikainen media-alusta, jossa käyttäjä pystyy osallistumaan palvelun tai sovelluksen tarjoamaan sisältöön tuottamalla sinne omaa materiaaliaan ja kirjoittamalla viestejä muille käyttäjille, esimerkiksi jakamalla sinne lehtiartikkeleita ja kommentoimalla niitä, lataamalla ottamiaan kuvia, luomalla tapahtumia, ja monella muulla tavalla. Toiminnalle onkin ominaista verkostoituminen, yhteisöllisyys ja nopea omaksuminen.

Poliisin toiminta sosiaalisessa mediassa sai alkunsa vuonna 2008, kun Helsingin poliisilaitoksen ylikonstaapeli Marko Forss loi IRC-Galleria -palveluun poliisiprofiilin nimeltään -fobba- (Pönkä 2014, 79). Nykyään poliisi on liittynyt sosiaaliseen mediaan useilla käyttäjätileillä moneen eri palveluun, jotka löytyvät poliisin internet-sivuilta: www.poliisi.fi/some.

2.2 Facebook

Päätin avata Facebookin toimintaperiaatetta, koska tämä tutkimus perustuu juuri Facebookin kaltaiseen sosiaalisen median ympäristöön, johon täytyy kirjautua sisään saadakseen informaatiota. Facebook on selkeästi suurin sosiaalisen median palvelu 2,01 miljardilla käyttäjällään (Kallas 2017). Sen toimintaperiaatteen esittely antaa hyvän kuvan siitä, mistä aiheessa on kysymys.

Facebook on sosiaalinen verkosto. Se on perustettu vuonna 2004 alun perin Harvardin yliopiston opiskelijoille. Palvelu avautui 26.9.2006 käytettäväksi kenelle tahansa, jolla on toimiva sähköpostiosoite. (Kalliala & Toikkanen 2014, 113.) Facebookilla oli kesäkuun lopussa 2017 yli kaksikymmentätuhatta työtekijää, 1,32 miljardia aktiivista käyttäjää päivittäin ja 2,01 miljardia kuukausittaista käyttäjää (Company info 2017).

Facebook luotiin sivustoksi, jossa voi ilmaista itseään internetissä ja olla yhteydessä tosielämän ystäviin monella tavalla. Siellä voi katsoa, mitä ystävät meinaavat tehdä tulevaisuudessa, suunnitella tapahtumia ystävien kesken, näyttää ottamiaan kuvia ystävilleen, ja monella muulla tavalla olla sosiaalisessa kanssakäymisessä ihmisten kanssa. Kaikki sosiaalisen median alustat tarjoavat palveluita hieman eri tavalla asioita painottaen. Facebook on suurin, koska se pyrkii tarjoamaan kaiken sen, mitä muut sosiaalisen median palvelut tarjoavat yhteensä. (Abram 2016, 8-18.)

Facebookiin käyttäminen edellyttää kirjautumista palveluun henkilökohtainen käyttäjätunnus luomalla. Palveluun tulee syöttää etunimi, sukunimi, toimiva sähköpostiosoite tai puhelinnumero sekä syntymäaika ja sukupuoli. Facebook edellyttää käyttöehdoissaan, että palvelussa käytetään oikeita tietoja. Tätä perustellaan sillä, että ystävien ja kontaktien löytäminen on näin helpointa. Salanimien käyttäminen on kiellettyä ja käyttäjällä voi olla vain yksi käyttäjätunnus. (Abram 2016, 23-35; Pönkä 2014, 84-90.)

Facebookin yhtenä merkittävänä ominaisuutena on erilaisten keskusteluryhmien luominen. Ryhmät voivat olla ammattialojen tai harrastuksiin liittyviä ryhmiä taikka naapurustoryhmiä tai kirpputoripalstoja. Osalle Facebookin käyttäjistä juuri ryhmät ovat tärkein ominaisuus Facebookiin kuulumiselle. Ryhmiä voi luoda kuka tahansa käyttäjä ja lisätä omista kontakteistaan ryhmään perustamisvaiheessa liitettävät jäsenet. Ryhmän perustajasta tulee alussa myös ryhmän ylläpitäjä. Ylläpitäjiä voi valita ryhmään useampiakin ja niitä pystyy myöhemmin muuttamaan. (Pönkä 2014, 94.)

Facebookin ryhmät voivat olla joko täysin julkisia, suljettuja tai salaisia. Täysin julkisen ryhmän keskustelun näkevät kaikki Facebookin käyttäjät ja täysin julkisiin ryhmiin voivat kaikki liittyä halutessaan, esimerkiksi saadakseen ryhmään kirjoitetut viestit helpommin näkyviin tai vain ideologisista syistä. Suljettujen ryhmien käyttäjät näkyvät kaikille Facebookin käyttäjille, mutta ryhmän sisällä julkaistu materiaali näkyy vain jäsenille. Täysin salaisien ryhmien olemassa olosta eivät tiedä kuin ryhmän jäsenet ja ryhmään kutsut henkilöt. Suljettuihin ja salaisiin ryhmiin sisään pääsyyn on myös valittavissa useita käytäntöjä. Salaisiin ryhmiin pääsee ainoastaan jo ryhmässä olevan jäsenen kutsun kautta ja ryhmän säännöt voivat vaatia vielä ylläpitäjän vahvistusta liittymiselle. Suljettuihin ryhmiin puolestaan voi itse pyytää sisäänpääsyä. Sisäänpääsyn hyväksyy ryhmän säännöistä riippuen joko joku ryhmän jäsenistä tai ylläpitäjä. (Abram 2016, 225-226.)

Ryhmät eivät ole ainoastaan Facebookissa käytössä. Muissakin sosiaalisen median alustoissa on vastaavanlaisia avoimuuden asteita. Pönkä (2014, 166-167) listaa avoimuuden asteita yhteensä kuusi, joista tulee valita jokin taso kulloisenkin käyttötarkoituksen mukaan.

3 LAINSÄÄDÄNTÖ

Maailman nopea kehittyminen digitaaliseen suuntaan asettaa lainsäädännön kehitykselle kovia haasteita. Lainsäätäjä joutuu huomioimaan aivan uudentyyppisiä tilanteita nopealla

aikataululla. Ennen kirjoitettu laki saattoi säilyä ajankohtaisena vuosikymmeniä. Nykyinen uusien innovaatioiden kehittymisen tahti ja nopeat muutokset digitaalisessa maailmassa eivät enää suo tämänkaltaisia tilanteita.

Sosiaalisen median vaikutukset arkipäivään lisääntyvät koko ajan ja sen huomioiminen lainsäädännössä on vasta alkutekijöissä. Vaikka samat lait periaatteessa pätevätkin sekä todellisessa että digitaalisessa elämässä, ovat digitaalisen maailman erityispiirteet haastavia tulkita lain kannalta. Myös mahdollisuus anonymiteettiin verkossa asettaa haasteita lainsäädännön kannalta.

Poliisin toiminnan on oltava avointa tarkastelulle ja poliisin on kaikessa toiminnassaan noudatettava lakia ja annettuja asetuksia sekä määräyksiä. Nämä vaatimukset asettavat poliisin toiminnalle rajoitteita myös sosiaalisessa mediassa. Kaikki, mikä on mahdollista tehdä, ei ole välttämättä lain mukaan sallittua. Viranomaisen toimintaa säädellään useassa laissa, mutta niissä ei oteta kantaa erikseen internetin erityispiirteisiin. Kunnes asiasta säädetään täsmällisesti laissa tai asetuksessa, joudutaan asiaa tarkastelemaan voimassa olevaa lainsäädäntöä ja lainsäätäjän tahtoa tulkiten.

3.1 Julkinen valta

Termi julkinen valta tarkoittaa yksityisen oikeudesta, velvollisuudesta tai edusta määräämistä, kun siitä ei ole sopimuksin sovittu ja se tapahtuu yksipuolisesti. Sen käyttäminen on lain nojalla tehtävien päätösten tekemistä, joka vaikuttaa yksityiseen oikeushyvään. Tämän kaltaisen julkisen vallan käyttö voi olla esimerkiksi hallintopäätösten ja määräysten antamista. (Husa & Pohjolainen, 74-75.)

Suomen perustuslaki (1999/731 §2) määrää, että kaiken julkisen vallan tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Nämä vaatimukset pitävät sisällään sekä lainalaisuusperiaatteen että lakisidonnaisuuden vaatimuksen. Lainalaisuusperiaate tarkoittaa toisaalta sitä, että ainoastaan ne tahot voivat käyttää julkista valtaa, joille lainsäädännössä annetaan oikeus siihen, ja toisaalta sitä, että tuon julkisen vallan käytön on perustuttava eduskunnan hyväksymään lakiin. Viranomainen voi näin toimia ainoastaan niillä valtuuksilla, jotka laki hänelle antaa. Lainalaisuusperiaatteen piiriin kuuluu kaikki yksipuolinen viranomaistoiminta ja lainalaisuusperiaatteen voi katsoa niin suojaavan yksityisiä oikeussubjekteja julkisen vallan mielivaltaiselta käytöltä kuin antavan oikeuden yksityisille oikeussubjekteille laista ilmeneviin etuihin. (Mäenpää 2008, 60-61.)

Lakisidonnaisuuden vaatimus syntyy Perustuslain 2 pykälän 3 momentin jälkimmäisestä osasta. Sen mukaan julkisessa toiminnassa on noudatettava tarkoin lakia. Lakisidonnaisuuden vaatimus sisältää lainalaisuusperiaatteesta poiketen kuitenkin myös lain perusteella annetut alemman asteiset säädökset ja muun voimassa olevan oikeuden. Lakisidonnaisuuden vaatimuksen mukaan viranomaisella on velvollisuus noudattaa lakia. Tämä tarkoittaa sitä, että viranomaisen on toteutettava sille määrätyt tehtävät ja yksityisellä on oikeus odottaa näin tapahtuvan. (Mäenpää 2008. 61-62.)

Lakisidonnaisuuden vaatimus tai lainalaisuusperiaate ei kuitenkaan poista sitä faktaa, että virkamiehen eteen voi tulla tilanne, jossa lainsäädäntö ei ole aivan täydellistä. Myös joustavien oikeusnormien soveltamisessa on harkinnanvaraa. Tällöin tulee huomioida, että päätökset ovat yleisen edun kannalta tarkoituksenmukaisia ja toimenpiteiden toteuttaminen ei tuota huomattavaa haittaa. Tämän kaltaisissa tilanteissa korostuu yleisen ja yksityisen edun välinen punninta. Lakisidonnaisuuden vaatimus on erityisen ongelmallinen, kun jotain julkisen vallan käyttöön liittyvää toimintaa ei ole laissa säädetty ollenkaan tai sitä on säädelty ristiriitaisesti. Näissä tapauksissa on erityisen tärkeää ottaa huomioon perusoikeudet, hallinnon oikeusperiaatteet ja vakiintunut laintulkintaa ohjaava säännöstö. (Mäenpää 2011, 52-53.)

Poliisi käyttää toiminnassaan myös julkista valtaa. Suurelta osin poliisin toiminnassaan käyttämä julkinen valta on tosiasiallista julkisen vallan käyttöä, jossa yksityiseen oikeushyvään puututaan välittömästi ja suoraan. Tosiasiallista julkisen vallan käyttöä on tässä tapauksessa erilaisten käskyjen ja määräysten antaminen. (Husa & Pohjolainen, 35-36). Esimerkki tällaisesta julkisen vallan käytöstä voi olla poistumiskäskyn antaminen yleistä järjestystä ja turvallisuutta häiritsevälle henkilölle.

3.2 Perustuslaki

Vaikka lakisidonnaisuuden piiriin kuuluu koko oikeusjärjestys, oikeusnormien hierarkia määrittää niiden sitovuuteen vaikuttavan etusijajärjestyksen. Alemmanasteinen normi ei siis ole velvoittava siltä osin, kun se on ristiriidassa ylemmän normin kanssa. Suomen Perustuslaki (1999/731 §107) kieltää viranomaista soveltamasta lakia alempiasteisia säännöksiä, jos ne ovat ristiriidassa perustuslain tai muun lain kanssa. Saman lain 106§ puolestaan määrittelee perustuslain etusijan. Perustuslain kanssa ristiriidassa olevia lakeja ei saa soveltaa. (Mäenpää 2011, 53-54.)

Vaatimukset julkisen toiminnan perustumisesta lakiin tarkoittaa sitä, että julkisen vallan käyttäjän toimivaltaperuste pitää aina löytyä laista. Esimerkiksi viranomaisella ei voi olla sellaista toimivaltaa, joka ei perustu lakiin. (HE 1/1998 vp, 74.)

Perustuslain toinen luku käsittelee perusoikeuksia, joita ovat muun muassa yksityisen elämän suoja sekä sananvapaus. Yksityisen elämän suoja turvaa myös kirjeiden, puheluiden ja muiden luottamuksellisten viestien salaisuuden. Yksityiselämän suojan lähtökohta on, että yksilöllä on ilman valtion tai muiden mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä, oikeus elää omaa elämäänsä. Yksityiselämän suojaan kuuluu niin oikeus solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön kuin perhe-elämäkin. Yksityiselämän suojan ylläpitämiseksi on valtiolta vaadittu pidättäytymistä yksityiselämän loukkaamiseen sekä aktiivisia toimia, jotta muutkaan tahot eivät pääse loukkaamaan ihmisen yksityisyyttä. (HE 309/1993 vp, 53.)

Suomen Perustuslain 10 pykälän mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Kyseinen laki siis turvaa oikeuden luottamukselliseen

viestintään. Viestin luottamuksellisuus tarkoittaa sitä, että kukaan muu kuin lähettäjän tarkoittama vastaanottaja ei saa ottaa viestin tunnistetiedoista tai sisällöstä selvää eikä estää viestin perille menoa. Luottamuksellisen viestin suoja koskee kaikkea niin sanottua kohdeviestintää ja on voimassa myös sosiaalisen median palveluissa, jossa viestit voivat olla luottamuksellisia tai julkisia. Verkkoviestinnässä viestintä voi tapahtua joko yhdeltä yhdelle, yhdeltä usealle tai yhdeltä kaikille halukkaille. Luottamuksellisuutta rajaa se, kenelle viesti on tarkoitettu luettavaksi. Kahdenkeskeiset sekä rajatulle joukolle lähetetyt viestit ovat luottamuksellisia. Kaikille avoimet viestit eivät puolestaan ole luottamuksellisia. (Pesonen 2013, 99-104.)

3.3 Viestintää koskeva lainsäädäntö

Sähköisen viestinnän tietosuojalain (516/2004) mukaan viesti, tunnistamistiedot ja paikkatiedot ovat luottamuksellisia, jos muualla laissa ei toisin säädetä. Kyseinen laki on kumottu Tietoyhteiskuntakaarella (917/2014), mutta tämän lain hallituksen esityksessä (HE 221/2013 vp, 153) sanotaan lain pykälän vastaavan vanhan lain pykälää. Hallituksen esityksen (HE 123/2003, 51) mukaan viesti ei ole luottamuksellinen, jos se on saatettu yleisesti vastaanotettavaksi. Luottamuksellisuutta arvioitaessa keskeistä on se, onko viesti saatettu julkiseksi esimerkiksi keskustelupalstalle. Saman hallituksen esityksen mukaan vastaanottajien lukumäärällä ei ole väliä arvioitaessa luottamuksellisuutta, jos viestiä ei ole saatettu yleisesti vastaanotettavaksi.

Sosiaalisen median julkaisujen sisältöön vaikuttaa myös sananvapauslaki (Laki sananvapauden käyttämisestä joukkoviestinnässä 460/2003). Sananvapauslaki antaa tarkempia säännöksiä Suomen perustuslain 12 pykälän kohtaan, johon kuuluu oikeus ilmaista ja vastaanottaa tietoja, mielipiteitä ja muita viestejä sekä välittää niitä kenenkään ennakolta estämättä. Sananvapauslaki koskee ainoastaan yleisölle, eli vapaasti valikoituneelle vastaanottajakunnalle, tarkoitettua joukkoviestintää. Tällaisia ovat myös verkkoviestit, joita ovat esimerkiksi sähköisen viestintäverkon kautta lähetettävät yleisön saataville tarkoitetut viestit. Sananvapauslaki ei siis koske kohdeviestintää, joka ei ole tarkoitettu yleisölle. Lain valmistelutöissä yleisön määritelmää ei pystytä avaamaan kokonaan, vaan se jää tapauskohtaisesti arvioitavaksi. Arvioinnissa tulee kiinnittää huomiota vastaanottajamäärään, siihen kuinka suljettu ryhmä on ja miten vapaasti siihen voi liittyä. Hallituksen esityksen mukaan muutaman henkilön välinen postitusryhmä ei muodosta yleisöä. Yleisöä ei myöskään muodosta yhden työpaikan sisäiset tiedotteet. (HE 54/2002 vp, 42-43.)

Pirkko Pesonen (2013, 119) ottaa kirjassaan kantaa sosiaalisen median osalta yleisön koon määritelmään. Pesosen mukaan viestin ollessa suunnattu vain kavereille tai osalle heistä, eivät he vielä muodosta yleisöä, sillä edellytyksellä, että kavereita on vain muutama. Kaveripiirin ollessa laaja, esimerkiksi satoja henkilöitä, muodostaa joukko Pesosen mukaan yleisön.

3.3.1 Viestinnän vaikutukset verkkoympäristössä tapahtuvaan tiedonhankintaan

Perustuslailliset oikeudet kirjesalaisuuteen ja sananvapauteen tulee ottaa huomioon verkkoympäristössä valvontaa suoritettaessa. Kohdennettu viestintä verkossakin on kirjesalaisuuden piirissä ja siihen eivät vaikuta sananvapauslain säädökset. Aikaisemmin sähköpostiviestinnässä koettiin jo muutos aiempaan kirjeviestintään verrattuna, kun kohdennettua viestintää pystyikin lähettämään useammalle henkilölle samalla kirjeellä. Sosiaalinen median asettaa uusia ulottuvuuksia myös kohdennetulle viestinnälle, kun viestinnän alustoja on tullut moninkertainen määrä lisää aiempaan verrattuna.

On huomioitava, että perustuslailliseen oikeuteen kuuluu vapaus mielipiteen ilmaisuun ja yksityisyyden suojaan ja viesti nauttii luottamuksen suojaa, vaikka se olisi toimitettu yhteisöpalvelussa (Pesonen 2013, 104). Ainoastaan viestit, jotka on asetettu yleisesti vastaanotettavaksi tai yleisölle saataville, voidaan katsoa olevan edellytys monen rikoslaissa mainitun rikoksen tunnusmerkistön täyttymiselle. Tällaisia ovat esimerkiksi kiihottaminen kansanryhmää vastaan (RL 10:11) ja yksityiselämää loukkaavan tiedon levittäminen (RL 24:8). Sosiaalisen median monenlaiset alustat vaikeuttavat tulkintaa siitä, onko kyseessä kohdennettu viesti vai yleisölle suunnattu tieto. Viestin lähettäjän tarkoitus viestiä lähettäessään vaikuttaa tuohon asiaan. Esimerkiksi pieneen suljettuun Facebook-ryhmään lähetetty viesti voi olla tietyille henkilöille tarkoitettu kohdennettu viesti. Viesti jää kuitenkin näkyviin ryhmän sisälle. Ryhmän koon kasvaessa myöhemmin suuremmaksi joudutaan tarkastelemaan sitä, kuka viestin sisällön on tosiasiassa tuonut yleisön saataville, alkuperäinen viestin kirjoittaja vai kenties ryhmän ylläpitäjä, joka on myöhemmin päästänyt ryhmään lisää jäseniä.

3.4 Rikoslaki

Rikoslaki sisältää useita sellaisia säännöksiä, jotka voivat tulla kyseeseen poliisin toimiessa verkkoympäristössä salaa. Lähdemateriaalia tällaisista tilanteista ei paljoa ole tarjolla, sillä asiaa ei ole käsitelty kirjallisuudessa juurikaan viranomaisen tekemien rikosten kannalta. Lakitekstistä ja hallituksen esityksistä selviää lainsäätäjän tahto parhaiten.

Rikoslain 38 luvun 3 pykälä on rangaistuspykälä edellisessä kappaleessa käsiteltyyn luottamuksellisen viestin avaamiseen oikeudetta. Jos henkilö avaa toiselle osoitetun kirjeen tai viestin taikka purkaa tällaisen viestin salaisuuden, syyllistyy hän rikokseen.

Rikoslain 40 luku käsittelee virkarikoksia. Kyseisen luvun yhdennentoista pykälän mukaan virkamies on muun muassa virka- tai siihen rinnastettavassa suhteessa valtioon oleva henkilö. Tämä määritelmä kuvastaa poliisihenkilöä. Poliisin käyttäessä sosiaalista mediaa virkatehtäviensä hoitamiseen, voi kyseeseen käytännössä tulla kyseisen luvun pykälät yhdeksän ja kymmenen. Rikoslain 40 luvun yhdeksännen pykälän tekstissä sanotaan, että virkamiehen virkaansa toimittaessaan tahallaan rikkoessa virkatoiminnassa noudatettaviin säännöksiin tai määräyksiin perustuvan virkavelvollisuutensa, muuten kuin vähäisesti, on hänet tuomittava. Pykälien erona on tahallisuus ja huolimattomuus. Muuten pykälät käsittävät samat asiat rangaistusasteikon ollessa kuitenkin huolimattomuudessa pienempi.

Rikoslain 38 lukuun lisättiin 9a pykälä, identiteettivarkaus, vuonna 2015. Kyseisellä pykälällä kriminalisoitiin toisen henkilötietojen tai muiden tunnistetietojen taikka yksilöivien tietojen käyttö. Kyseisessä pykälässä vaaditaan lisäksi sitä, että teolla on tarkoitus erehdyttää kolmatta osapuolta ja aiheutetaan joko taloudellista tai muuten vähäistä merkittävämpää haittaa. Hallituksen esityksessä (HE 232/2014 vp, 36-37) sanotaan, että kolmas osapuoli voi myös olla henkilöiden luoma tai ylläpitämä tietojärjestelmä. Erehdyttämisessä olennaista on nimenomaan se, että erehdytetään henkilöllisyyden tai identiteetin osalta ja syntyy selkeä erehtymisen vaara. Edellytyksesi rangaistukselle hallituksen esitys mainitsee sen, että toimitaan oikeudettomasti.

Identiteettivarkaus on asianomistajarikos. Asianomistajan selvittäminen olla vaikeaa käytettäessä pelkästään nimitietoa. Tällöin ei välttämättä anasteta kenenkään tietyn henkilön identiteettiä. Rangaistavuutta harkittaessa oleellista on hallituksen esityksen mukaan (HE 232/2014 vp, 37) myös se, että erehdytetään kolmatta osapuolta luulemaan tietojen käyttäjää tietyksi toiseksi henkilöksi. Vähäistä suuremmasta haitasta edellä mainittu hallituksen esitys mainitsee juurikin internetin sosiaaliseen mediaa luodun valeprofiilin toisen henkilötiedoilla. Tällaisen profiilin ja siihen syötettyjen tietojen poistaminen voi olla vaikeaa.

3.4.1 Rikoslain vaikutus verkkoympäristössä tapahtuvaan tiedonhankintaan

Kuten aiemmin todettu, Facebookin kirjautumiseen tarvitsee sähköpostiosoitteen ja etunimen sekä sukunimen. Poliisin suorittaessa ei näkyvää valvontaa internetissä, tarvitsee palveluihin sisään kirjautua jollakin anonyymillä nimellä, jottei nimestä voi päätellä sen käyttäjän olevan valvontaa suorittava virkamies. Tällaista ongelmaa ei tietysti ole, jos suoritetaan näkyvää valvontaa ja toimitaan omalla nimellä tai jollakin selkeällä henkilöprofiililla. Tällaisia ovat esimerkiksi poliisin käyttämät nettipoliisien nimimerkit. Nimen kehittämisessä täytyy olla tarkkana, jottei tule sekoitetuksi keneenkään oikeaan henkilöön. Tällöin jouduttaisiin vakavasti punnitsemaan erehdyttämisen tarkoituksellisuutta. Liikuttaisiin siis hyvin lähellä kriminalisoitua identiteettivarkauden teonkuvausta. Vaikka virkamiehellä ei olisikaan aktiivisesti tarkoitus, että kolmas osapuoli erehtyy luulemaan häntä keneksikään tietyksi toiseksi, voi kolmannen osapuolen erehtyminen kuitenkin aiheuttaa merkittävääkin haittaa henkilölle, jonka nimeä on käytetty. Risto Heinosen mukaan (2001, 202) identiteettiin kohdistuva varkaus on paljon merkittävämpi kuin johonkin fyysiseen omaisuuteen kohdistuva varkaus, sillä se aiheuttaa paljon arvokkaamman, hyvän nimen, identiteetin ja yksityisyyden, menetyksen. Hyvän niemen ja identiteetin palauttaminen on Heinosen mukaan aina vaikeaa.

Identiteettivarkaus ei Marko Forssin (2014, 86) mukaan ollut vähään aikaan kriminalisoitu Suomen laissa. Identiteettivarkauteen liittyvä kriminalisointisäännös, yksityishenkilön erehdyttäminen poistettiin laista vuonna 1999 (Forss 2014, 86). Muuksi henkilöksi tekeytyminen olisi ollut hyvin kyseenalaista poliisilta ilman uutta kriminalisointiakin, sillä siitä saattaa koitua huomattavaa haittaa yksityiselle edulle. Tämä olisi ristiriidassa myös poliisin eettisen säännöstön ja arvojen kanssa, jotka sanovat poliisin olevan luotettava ja

tarjoavan perusturvallisuutta kaikille kansalaisille (Poliisin arvot, luettu 10.10.2017). Perusturvallisuuden ja luotettavuuden tunne varmasti heikkenisi ainakin itselläni, jos huomaisin viranomaisen käyttävän henkilötietojani rikostorjunnassa ilman lupaani.

Virkarikospykäliä poliisihenkilö voi rikkoa tekemällä virkatoimia vastoin ohjeita tai määräyksiä. Poliisihallitus on linjannut omaa kantaansa verkossa tapahtuvaan tiedonhankintaan. Tähän salassa pidettävään asiakirjaan ja sen perusteella annettuihin ohjeisiin jokaisen poliisimiehen tulisikin perehtyä, sillä annetuista ohjeista täytyy itse ottaa selvää. Tietysti ohjaavat asiakirjat ovat vielä hyvin tuoreita, joka saattaa osaltaan lieventää rangaistavuutta väärin toimittaessa.

Viestintäsalaisuuden rajanvetoa kohdennetun viestin osalta käytiin perustuslakia käsittelevässä kappaleessa. Rikoslain 38:3 pykälästä löytyy siis rangaistus laittomaan kirjeen tai muun viestin avaamiseen. Kuten kappaleessa mainittiin, on rajanveto sosiaalisessa mediassa toimittaessa hankalaa ja usein täysin tapauskohtaista. Selkeästi yhdelle henkilölle osoitetun viestin avaaminen ilman oikeutusta menee kuitenkin varmasti rangaistavuuden piiriin. Toki tällainenkin viesti pitää olla lähetetty esimerkiksi yksityisviestinä siten, että sitä ei lähtökohtaisesti pääse lukemaan kuin se henkilö, jolle se on osoitettu, muuten kuin murtamalla viestin suojaus. Väärällä identiteetillä toimiessa voi saada tällaisenkin viestin haltuunsa, jolloin sen avaaminen ei ole rikoslain 38:3 pykälän mukaan rikos, sillä valeprofiilin haltija on viestinnän osapuoli (Forss 2014, 248). Tällöin ollaan tietysti lähellä edellä mainittua identiteettivarkauden määritelmää.

Sosiaaliselle medialle ominaiset ryhmät ja niiden sisällä lähetetyt viestit tekevätkin lain tulkinnasta huomattavasti hankalampaa. Lain esitöissä ei ole käsitelty tällaisia tilanteita. Selvää on, että yksityisviestien lähettämiseen millä tahansa alustalla pätee luottamuksellisuus riippuen toki hieman siitä, miten monelle viesti lähetetään. Aikaisemmin käsitelty yleisö-käsitteen muodostuminen tulee esille, kun vastaanottajia on satoja. Suljettuihin ja salaisiin ryhmiin lähetetyt viestit ovatkin tulkinnanvaraisempi kokonaisuus. Toisaalta, koska tällaiset ryhmät vaativat aina jonkun jo ryhmän jäsenenä olevan hyväksynnän ryhmään pääsyyn, näkisin niin, että vaikka viesti ei alun perin olisi ollut tarkoitettu ryhmään uutena hyväksytylle, esimerkiksi poliisihenkilölle, on hänet ryhmään hyväksynyt jäsen hyväksymisen yhteydessä samalla jakanut myös kaikki ryhmän sisällä jo aiemmin olleet viestit eteenpäin uudelle jäsenelle. Näin poliisihenkilöstä muodostuu viestinnän osapuoli, sillä viestin vastaanottaja saa välittää viestin eteenpäin (Pesonen 2013, 104).

3.5 Poliisilaki

Aiemmin tässä luvussa käsiteltiin perustuslakia, jonka mukaan kaiken viranomaistoiminnan tulee perustua lakiin. Poliisilain 1 luvun ensimmäinen pykälä määrittelee poliisin tehtävän. Poliisin tehtäväksi sanotaan muun muassa yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen ja paljastaminen. Pykälän ei kuitenkaan määrittele miten poliisin tulee määrätty tehtävänsä hoitaa.

Kansankielellä sanottuna poliisi valvoo. Poliisi valvoo nykyään myös internetissä, kuten se valvoo liikennettä tai yleistä järjestystä ja turvallisuutta. Internetissä valvotaan useamman yksikön voimin, sillä Marko Forssin (2014, 14) mukaan poliisilaitosten ohella myös Keskusrikospoliisi, joka vastaa internetin yleisvalvonnasta, ja Suojelupoliisi valvovat internetiä. Lisäksi poliisin jokaiseen yksikköön on Ylen uutisten mukaan (Mäntymaa 2017) rekrytoitu vuonna 2017 nettipoliiseja, yhteensä 25 kappaletta. Valvonta internetissä on perusteltua, sillä rikosmäärät internetissä ovat lisääntyneet reilusti koko 2010-luvun ajan (Forss & Keinänen 2017, 4-5). Poliisilaissa ei edellä mainittua yleisvalvontaa kuitenkaan säädellä.

Perinteistä valvontaa on pidetty poliisin ennalta estävän toiminnan perustana. Valvonta tarkoittaa normaalein aistihavainnoin tehtävää seurantaa, joka kohdistuu ennalta määräämättömään ihmisjoukkoon. Valvonnasta, joka kohdistuu vain hetkellisesti henkilöön tai henkilöihin, on perinteisesti käytetty termiä yleisvalvonta. Valvonnan ja tarkkailun erona nähdään juuri se, että tarkkailu, toisin kuin valvonta, on tiedonhankintatarkoituksessa tehtävää tiettyyn henkilöön kohdistuvaa seurantaa. (Helminen ym. 2012, 220-221, 392.)

Hallituksen esityksessä (HE 224/2010 vp) on useita viitteitä valvonnasta ja jopa valvonnasta verkkoympäristössä. Poliisi siis valvoo internetissä tapahtuvaa keskustelua yleisvalvonnan näkökulmalla. Joskus valvonta voi johtaa tarkkailuun ja tarkkailun jatkuessa pidempään mennään salaisten tiedonhankintakeinojen piiriin.

Poliisilain ja pakkokeinolain uudistusten yhteydessä Poliisilaki 5 luvun salaiset tiedonhankintakeinot ja Pakkokeinolaki 10 luvun salaiset pakkokeinot kirjoitettiin vastaamaan sanallisesti toisiaan niin hyvin kuin mahdollista. Erona näillä on se, että Poliisilain pykäliä käytetään esimerkiksi rikosten ennalta ehkäisemiseen ja edellä mainittuun valvontaan. Pakkokeinolain pykälässä käsitellään puolestaan toimivaltuuksia jo tapahtuneen rikoksen selvittämiseksi. (Hankilanoja 2014, 72-73.) Tässä työssä käsitellään poliisin toimivaltuuksia poliisilain näkökulmasta, sillä työn rajauksessa on työn ulkopuolelle jätetty tilanteet, joissa tutkitaan jo tapahtunutta rikosta.

Poliisi on käyttänyt salaisia tiedonhankintakeinoja tiettävästi niin kauan kuin on instituutiona ollut olemassa. Salaisista tiedonhankintakeinoista säädettiin laissa kuitenkin ensimmäisen kerran vasta uuden poliisilain voimaan tullessa vuonna 1995. Sitä ennen poliisi käytti salaisia tiedonhankintakeinoja niin sanotun tavanomaisen oikeuden eli yleisvaltuutuksen perusteella. Entisen käsityksen mukaan poliisilla oli oikeus käyttää niitä keinoja, joita ei erikseen laissa kielletä. Oikeusasiamies otti jo vuonna 1984 kantaa sääntelyn puutteeseen, todeten, että poliisi ei voi käyttää kaikkia niitä tiedustelutoimenpiteitä tarkoituksenmukaisuussyihin vedoten, mitä laki ei erikseen kiellä. Oikeudellinen ajattelu onkin mennyt viime vuosikymmeninä siihen suuntaan, että kaiken viranomaisen toiminnan pitää perustua lakitasoiseen säädökseen. (Hankilanoja 2014, 69-71.)

Tarkkailu

Tarkkailun määritelmä tulee Poliisilain 5:13,1 pykälästä. Pykälän mukaan tarkkailulla tarkoitetaan tiettyyn henkilöön salaa kohdistettavaa havaintojen tekemistä tiedonhankintatarkoituksessa. Tarkkailu on ollut aikaisemmin eräänlainen perussäännös ja, vaikka se nyt on kirjattuna lakiin, ei se Helmisen ym. (2012, 392) mukaan ole toimivaltasäännös vaan määritelmäsäännös, joka mainitaan suunnitelmallisen tarkkailun selkeyttämiseksi. Tarkkailu on siis kuitenkin sallittu tutkintamenetelmä. Tarkkailu nähdään oikeuskirjallisuudessa kuitenkin myös toimivaltasäännöksenä, kuten Metsäranta (2015, 172-176) sen näkee väitöskirjassaan. Lainvalmistelutyöt eivät anna suoraa vastausta siihen kummasta on kysymys. Poliisilain 5:1,1 pykälä, joka määrittää, mitä tiedonhankintakeinoja voidaan käyttää kohteelta salassa, ei sisällä mainintaa tarkkailusta. Myös lakivaliokunta lausunnossaan (LaVL 21/2010 vp, 2) listaa uuden poliisilain mukaiset salaiset tiedonhankintakeinot eikä tarkkailu siltäkään listalta löydy. Tämä tukisi sitä käsitystä, ettei tarkkailu ole Poliisilain tarkoittaman salaisen tiedonhankinnan piirissä.

Hallituksen esityksessä (HE 224/2010 vp, 102) todetaan erikseen, että tarkkailu on mahdollista myös tietoverkossa, ilman että sitä pidetään teknisenä tarkkailuna vaikkakin siinä käytetään tietokonetta. Hallituksen esityksen mukaan kyse on ainoastaan toimintaympäristön erityispiirteestä, jossa tietokonetta käytetään muiden käyttäjien tavoin.

Tarkkailun rooli salaisena tiedonhankintakeinona on tärkeä mietittäessä poliisin toimintaa sosiaalisessa mediassa. Jos tarkkailu ei ole salainen tiedonhankintakeino, ei poliisin ole mahdollista suorittaa tarkkailua verkossa peiteprofiilin turvin, sillä poliisi saa käyttää vääriä, harhauttavia tai peiteltyjä tietoja vain salaista tiedonhankintakeinoa käytettäessä, kuten Poliisilaki 5:46 pykälä sanoo. Tätä mieltä asiasta on myös Helminen ym. (2012, 394) korostaessaan erityisesti sitä, että verkkoympäristö ei perusta sellaisenaan laajempia oikeuksia tiedustelun suorittamiseen esimerkiksi nimimerkin takaa, vaan tällöin kyseeseen tulee tietoverkossa suoritettava peitetoiminta.

Vanhassa poliisilaissa tarkkailun edellytyksistä (PolL 7.4.1995/493, 30§) oli säädetty erikseen. Tarkkailu kuului myös saman lain 33a pykälässä säädettyyn tiedonhankinnan paljastumisen estämiseen, joka vastaa pitkälti nykyistä salaisten tiedonhankintakeinojen suojaamisen pykälää (PolL 5:46). Hallituksen esityksessä (224/2010 vp, 131) otetaan kantaa noihin vanhoihin pykäliin. Esityksessä sanotaan, että aikaisemmin tiedonhankinnan paljastumisen estämistä voitiin käyttää vain tietyissä salaisen tiedonhankinnan pykälissä, joihin tarkkailukin kuului, mutta suojaustarve koskee kaikkia salaisia tiedonhankintakeinoja. Hallitus halusi siis lisätä salaisen tiedonhankinnan suojaamista, mutta tulikin poistaneeksi tarkkailun listalta. Hallituksen esityksestä jää siis puuttumaan selvä kannanotto siihen, että onko hallitus tarkoittanut tarkkailun edelleen sisältyvän salaisen tiedonhankinnan piiriin vai ei. Tällä hetkellä poliisilain mukaan se ei sinne enää kuulu.

Tarkkailu verkkoympäristössä tarkoittaa siis tiettyyn henkilöön kohdistuvaa tiedonhankintatarkoituksessa tehtävää havainnointia. Tarkkailu tulee tehdä ilman vuorovaikutusta kohteen kanssa. Havainnot voidaan taltioida tarkkailun yhteydessä.

Tarkkailulle ominaista on, että sitä tehdään salassa tiedonhankinnan kohteelta ja sillä pyritään rikoksen estämiseen tai paljastamiseen. (Helminen ym. 2012, 388-393.)

Suunnitelmallinen tarkkailu ja muut salaiset tiedonhankintakeinot

Salaiset tiedonhankintakeinot käsitellään tässä yhteydessä lyhyesti siitä syystä, että niillä tehdään vain rajaa siihen, mitä poliisi voi tehdä verkossa ennen kuin puhutaan salaisesta tiedonhankinnasta.

Suunnitelmallinen tarkkailu löytyy samasta lakipykälästä (PolL 5:13) tarkkailun määritelmän kanssa. Se eroaa perusmuotoisesta tarkkailusta siten, että se ei ole lyhytaikaista ja kohdistuu henkilöön, jonka voidaan perustellusti olettaa syyllistyvän rikokseen. Vähimmäisaikaa ei lainvalmistelutöissä mainita, vaan se on tapauskohtaista. Aikarajoitteen lisäksi tarkkailu voidaan katsoa suunnitelmalliseksi, jos se toistetaan jonkin ajan kuluessa. Suunnitelmallista tarkkailua saadaan kohdistaa henkilöön, jonka voidaan perustellusti olettaa syyllistyvän rikokseen, josta säädetty rangaistus on vähintään kaksi vuotta vankeutta, taikka varkauteen tai kätkemisrikokseen. Suunnitelmallisen tarkkailun piirteenä on myös se, ettei tarkkailtavaan kohteeseen oteta kontaktia (Metsäranta 2015, 173).

Sosiaalisessa mediassa tapahtuvan valvonnan kannalta kaikki tähän lain kohtaan osuvat tai tämän törkeysasteeltaan ylittävät perustellut epäilyt rikoksista ovat selkeästi myös salaisten tiedonhankintakeinojen suojauksen (PolL 5:46) piirissä, jolloin voidaan verkkoympäristössä toimia esimerkiksi peitenimillä. Kahden vuoden rangaistumaksimi antaa mahdollisuuden tietyissä tapauksissa myös muun muassa peitellylle tiedonhankinnalle (PolL 5:16), peitetoiminnalle verkossa (PolL 5:28) ja valeostolle (PolL 5:35). Kahteen jälkimmäiseen liittyy vaatimus siitä, että niiden suorittaminen on välttämätöntä rikoksen estämiseksi tai paljastamiseksi. Näille salaisille tiedonhankintakeinoille ominaista on vuorovaikutus kohteen kanssa. Peitetoiminnan käytön osalta rangaistusmaksimia on alennettu verkkoympäristössä tapahtuvan peitetoiminnan osalta jopa peiteltyä tiedonhankintaa alemmalle tasolle, sen normaalissa kanssakäymisessä ollessa neljä vuotta.

3.5.1 Poliisilain vaikutus verkkoympäristössä tapahtuvaan tiedonhankintaan

Poliisilain salaiset tiedonhankintakeinot ovat keskiössä, kun mietitään poliisin tiedonhankintaa verkkoympäristössä. Vaikka osa verkossa olevista sosiaalisen median alustoista ja keskustelupalstoista on luettavissa kirjautumatta sisään, on suurin osa sisällöstä luettavissa ainoastaan kirjautumalla palveluun. Poliisin suorittaa valvontaa sekä selkeästi erottuvilla, esimerkiksi nettipoliisin tunnuksilla, että palveluihin varta vasten tehdyillä anonyymeillä tai peitetunnuksilla (Forss & Keinänen 2017, 22).

Kuten aiemmin todettu, internetissä tapahtuvan rikollisuuden lisäännyttyä koko 2010-luvun, on poliisinkin järkevää olla paikalla siellä missä rikollisuutta esiintyy. Poliisin valvonta internetissä on perusteltua ja lainsäädäntö antaa siihen mahdollisuuden.

Ongelmaksi muodostuu se, että lainsäädäntö ei anna siihen juurikaan keinoja. Suuri osa keskusteluista sosiaalisessa mediassa käydään sellaisten ryhmien sisällä, jotka eivät ole kaikille täysin avoimia (Pönkä 2014, 166). Poliisin on tätä verkkokeskustelua hankala valvoa. Tällaiseen ryhmään sisään pääseminen nettipoliisin tunnuksilla on täysin kiinni ylläpitäjästä. Ylläpitäjä tuskin haluaa valvovaa silmää keskusteluja seuraamaan, jos keskustelut koskevat jotakin laitonta. Sillä, valvontaanko suurempaa ryhmää vai tiettyä henkilöä, jonka valvominen on lain mukaan tarkkailua, ei ole merkitystä sivustojen sisältöön kiinni pääsemiseksi. Tällä hetkellä niin valvonta kuin tarkkailukin jäävät peiteltyjen tietojen käytön mahdollisuuden ulkopuolelle.

Mainittakoon vielä, että selkeä epäily tietyn henkilön valmistelemasta tai tekemästä vakavasta rikoksesta antaa poliisille monia mahdollisuuksia myös verkkoympäristössä salaisten tiedonhankintakeinojen käyttöön.

3.6 Muut ohjeet ja oleelliset asiat

Poliisihallitus on antanut ohjeen poliisin toiminnasta sosiaalisessa mediassa kesäkuussa 2017. Sosiaalisen median ohje on julkinen ja käsittelee sosiaalisen median käyttöä poliisin työtehtävissä. Ohjeen mukaan poliisin ennalta estävä toiminta kuuluu kaikkeen poliisitoimintaan, mukaan lukien sosiaalinen media. Lisäksi sosiaalisen median mahdollisuuksia tulee ohjeen mukaan hyödyntää mahdollisimman laajasti kaikessa poliisitoiminnassa. Ohjeen mukaan sosiaalista mediaa voidaan hyödyntää myös tiedonhankinnassa. (Poliisihallitus 2017.)

Poliisihallituksen ohjeessa käsitellään myös julkisten virkaprofiilien perustamista sosiaaliseen mediaan ja niiden julkaisua poliisi.fi -verkkopalvelussa (Poliisihallitus 2017). Poliisihallituksen ohje ei kuitenkaan ota kantaa muuhun kuin julkisen virkaprofiilin luontiin sosiaalisessa mediassa. Ei julkisten virkaprofiilien luomista ei ohjeisteta.

Aiemmin tutkimuksessa käsitelty Facebook kieltää käyttöehdoissaan (Pönkä 2014, 90) muun muassa useamman kuin yhden käyttäjätilin käytön. Facebookin käyttöehdoissa mainitaan Pöngän (2014, 90) mukaan, että käyttöehtojen noudattamatta jättäminen voi johtaa käyttäjätilin poistamiseen. Poliisi.fi -verkkosivustoilla julkaistuilla julkisilla virkaprofiileilla toimivilla poliisihenkilöillä on useilla myös oma, poliisitoimintaan viittaamaton käyttäjätunnus. Tähän epäkohtaan Poliisihallitus ei ota ohjeessaan kantaa.

4 POHDINNAT

4.1 Sääntely

Uuden poliisilain sääntelyssä otetaan hyvin vähän kantaa verkkoympäristöön. Asia on valvontaa suorittavan tahon osalta hankala, sillä suuri määrä tietoa löytyy nykyään internetin syövereistä ja selvää sääntelyä sen tiedon hankkimiseksi ei ole. Salaisen tiedonhankinnan osalta Hankilanoja (2014, 106) kirjoittaa, että salaisen tiedonhankinnan toimivaltuuksien käytön sääntely tietoverkkoympäristössä on sivuutettu merkittäviltä osin

uudessa poliisi- ja pakkokeinolakien sääntelyssä. Hankilanojan mukaan toimivaltuuksien käytön edellytykset reaalimaailmassa ja tietoverkossa ovat osin epäloogisia ja niihin pitäisi saada lisää pykälätasoista sääntelyä. Hankilanoja jatkaa teoksessaan, että uusi laki ei ole tuonut helpotusta vaikeaselkoiseen, osin tulkinnanvaraiseen ja puutteelliseen sääntelyyn. Se on Hankilanojan mukaan osin poistanut epäkohtia sääntelystä, mutta luonut samalla uusia ongelmakohtia.

Tuoreessa tutkimuksessaan Forss ja Keinänen (2017, 11) kritisoivat sitä, että sosiaaliseen mediaan liittyvissä rikoksissa ollaan jouduttu soveltamaan lainsäädäntöä, joka on ajalta ennen kuin sosiaalinen media on yleistynyt. Kritiikkiä herätti myös se, että lainvalmisteluohjeissa ei huomioida sosiaalista mediaa lainkaan (Forss & Keinänen 2017, 4). Lisäksi tutkimuksen johtopäätöksissä tuodaan esiin se, että pakkokeinojen tulisi seurata paremmin tekniikan kehitystä ja sosiaalisen median arkipäiväistyminen tulisi erityisesti huomioida (Forss & Keinänen 2017, 24).

Näyttääkin siltä, että lainsäätäjä ei ole tuonut tahtoaan poliisitoiminnan suorittamisesta internetissä ja sosiaalisessa mediassa riittävän hyvin esille. Sosiaalinen media eroaa tosielämästä merkittävästi ja nykyisen lain laajempi tulkinta alueelle, jota lainsäätäjä ei ole huomioinut tarpeeksi, on haasteellista. Lakiin pitäisi saada selkeämmät pykälät toiminnasta verkkoympäristössä tai vähintään niihin pitäisi ottaa kantaa asetuksien tasolla.

4.2 Väärällä identiteetillä kirjautuminen

Syitä väärän identiteetin käyttöön valvonnassa tulee mieleeni ainoastaan kaksi: oikealla identiteetillä ei saada sitä tietoa haltuun mitä ollaan hakemassa tai ei haluta tiedonhankinnan kohteen tietävän poliisin mielenkiinnosta. Niinpä väärällä identiteetillä kirjautumista tulisikin tarkastella sekä valvonnan että tarkkailun näkökulmista.

Lainsäätäjän tahtoa on vaikea tulkita verkkoympäristössä tapahtuvan valvonnan suhteen. Jos lakia tulkitaan hyvin tiukasti, ei poliisille löydy toimivaltaa esiintyä väärillä tiedoilla internetissä normaalia valvontaa suorittaessaan. Poliisi voi käyttää harhaanjohtavia tietoja ainoastaan salaisessa tiedonhankinnassa. Salaisen tiedonhankinnan säännöstö, vaikka onkin verrattain uusi, on kuitenkin tehty reaalimaailmaa silmällä pitäen. Sosiaalisen median ja tosielämän eroavaisuudet ovat merkittävät. Sosiaalisessa mediassa esiinnytään hyvin yleisesti eri identiteetin turvin kuin reaalimaailmassa. Tosielämässä tekaistun identiteetin luominen valvontatarkoituksessa on poliisille mahdotonta. Väärien, harhauttavien tai peiteltyjen tietojen käytössä on kysymys salaisesta tiedonhankintakeinosta, jonka käyttöä ohjaavat selkeät säännöt ja rajoitukset. Lisäksi väärän identiteetin antaminen rikkoo usein palveluntarjoajan sääntöjä. Toimivaltaa noiden sääntöjen rikkomiseen on vaikea löytää, jollei asiasta ole erikseen sovittu palveluntarjoajan kanssa. Nämä asiat silmällä pitäen verkkoympäristössä väärän identiteetin käyttäminen olisi poliisille kiellettyä yleisvalvontaa suorittaessa.

Tarkkailu verkkoympäristössä voi tarkoittaa esimerkiksi tietyn henkilön profiilitietojen katselua, hänen kirjottamiensa tekstien johdonmukaista lukemista tai hänen kontaktien tai

niiden ryhmien, joihin hän on liittynyt, läpi käymistä. Kuten aikaisemmin todettu, kaikki mikä on sallittua yksityiselle kansalaiselle, ei välttämättä ole sallittua poliisille. Niin ihmisen seuraaminen kadulla kuin verkkoympäristössäkin on sallittua yksityiselle henkilölle. Viranomaisen tehdessä samaa puututaan henkilön yksityisyyteen jo sen verran, että puhutaan tarkkailusta. Jos tarkkailu on jatkuvaa, puhutaan suunnitelmallisesta tarkkailusta.

Tarkkailulle ei ole annettu mitään määrämuotoisia vaatimuksia eikä tarkkailun suorittamiseen ole annettu poliisille mitään erillisoikeuksiakaan. Edellisessä lainsäädäntöä koskevassa osiossa tuotiin ilmi, ettei tarkkailu ole salainen tiedonhankintakeino enää nykylainsäädännön mukaan. Väärien tietojen käyttöä tarkkailun yhteydessä koskevat pääasiassa samat säännöt kuin valvonnassakin.

Poliisiin pitäisi pystyä kirjautumaan verkon palveluihin väärillä tiedoilla saadakseen valvontaa suoritettua täysipainoisesti. Vaikka kirjautumista väärillä tiedoilla voisikin perustella normaalilla siviiliasussa suoritettavalla valvonnalla, eroaa reaalimaailma anonymiteetti verkkomaailmasta oleellisesti. Reaalimaailmassa ei tarvitse keksiä tekaistuja henkilötietoja tuon valvonnan toteuttamiseksi. Verkkomaailmassa jonkinasteisten identifioimistietojen antaminen on usein välttämätöntä valvonnan suorittamiseksi. Tällainen väärien tai tekaistujen tietojen käyttö ei lakia tiukasti tulkiten sovellu valvontaan. Se onnistuu lain mukaan ainoastaan salaista tiedonhankintakeinoa käytettäessä.

Reaalimaailmassa poliisi voi valvoa nimettömänä siviilivaatteet päällä yleistä järjestystä ja turvallisuutta, varsinkin siinä tapauksessa, kun poliisille annetaan vinkki rikollisesta toiminnasta, voi poliisi mennä paikan päälle siviilivaatteissa tarkastamaan tilanteen taikka tarkkailemaan mahdollista epäiltyä. Tällöin ei tarvitse kenellekään antaa vääriä tietoja. Lainsäätäjä tuskin on tarkoittanut, että tällaista valvontaa ei voisi tehdä verkkoympäristössä.

On täysin eri asia erehdyttää tietojärjestelmää kuin ihmistä. Yleisvalvontaa internetissä suorittaessaan, ottamatta kontaktia kehenkään henkilöön, poliisi esiintyy ainoastaan palveluntarjoajalle väärillä tiedoilla suorittaakseen näkymätöntä valvontaa. Näin siis riippumatta siitä liikutaanko sosiaalisessa mediassa virallisella nettipoliisin tunnuksella vai tekaistulla tunnuksella. Tietojärjestelmään väärän tiedon syöttämisen ei voi katsoa erehdyttävän ketään samalla tavalla kuin henkilökohtaisessa kanssakäymisessä ihmisen kanssa kerrottava valhe. Väärän tiedon käyttöä voikin nähdä olevan vasta se, kun ihmistä erehdytetään tai luodaan vääriä rekisteritietoja virallisiin järjestelmiin.

Väärän tiedon käyttäminen jättää vastuuta mielestäni myös kuulijalle. Verkkoympäristössä esimerkiksi Facebookiin voi syöttää mitä tahansa nimensä kohdalle. Se ei ymmärrä satiiria samalla tavalla kuin ihminen. Jos tietojärjestelmälle kerrot olevasi esimerkiksi Super Mies, ei tietojärjestelmä kyseenalaista nimeäsi. Tätä nimitietoa ei myöskään millään tavalla tarvitse varmentaa. Ihminen puolestaan ymmärtää välittömästi, ettei kyseessä ole todellinen nimesi. Selvä satiiri ei voi olla sitä väärän tiedon käyttöä, mitä lainsäätäjä on tarkoittanut säätäessään salaisia tiedonhankintakeinoja koskevaa lakia.

4.3 Avoimuuden asteen vaikutukset valvontaan

Suuri osa keskustelusta sosiaalisessa mediassa tapahtuu ryhmien sisällä (Pönkä 2014, 166). Poliisilla voi tiedonhankinnallisista syistä olla tarvetta joskus pyytää pääsyä sellaisen verkkoryhmän jäseneksi, johon pääsyä on rajattu jollakin tavoin. Tällaisia eri avoimuuden asteita on verkkoympäristössä Pöngän (2014, 166-167) mukaan kuusi. Näistä osa on sen tyylisiä, että niihin tarvitsee saada ylläpitäjältä hyväksyntä, jotta sisältöä pääsee tarkastelemaan.

Poliisin saadessa vinkin jonkin verkkoympäristön ryhmän sisällä tapahtuvasta yleistä järjestystä ja turvallisuutta vaarantavasta asiasta tai rikoksen suunnittelusta, ei poliisi voi tarkistaa asiaa, jos mahdollisuutta kirjautua verkkoympäristöön väärillä tiedoilla ei ole. Tällainen tilanne, jossa poliisilla on ainoastaan kansalaiselta tullut epäily tai tarkistuspyyntö, ei vielä lähtökohtaisesti täytä salaisen tiedonhankinnan edellytyksiä. Salaisten tiedonhankintakeinojen käyttö asettaa vaatimuksen rikoksen vakavuudesta ja tiedonhankinnan odotetavissa olevasta tuloksellisuudesta (Helminen ym. 2012, 400-401).

Verkkoympäristön koolla on merkitystä harkittaessa sitä, voiko poliisi suorittaa valvontaa ryhmän keskusteluihin. Muutaman hengen ryhmään kohdistuva valvonta täyttää helposti tarkkailun määritelmän, kun tarkkailu kohdistuu käytännössä yksittäisiin henkilöihin. Verkkoympäristön koon lisäksi on merkitystä sillä, minkä tyyppinen ryhmä on kyseessä. Jos ryhmä sisältää esimerkiksi ainoastaan saman lasten hoitopaikan vanhempia, ryhmään kirjoitettavat viestit on myös luokiteltava ainoastaan sen ryhmän sisäisiksi viesteiksi, ei näin välttämättä julkisiksi. Ryhmän sisällä lähetetyt viestit on tarkoitettu ainoastaan ryhmän jäsenille eli tässä tapauksessa lasten vanhemmille. Tällöin mielestäni poliisi ei myöskään voi liittyä ryhmään valvontaa suorittaakseen yksityisyyden suoja huomioiden. Tällaiseen ryhmään pyrkimisen tulkitsisin jo peitetoiminnaksi, sillä siinä luodaan jo valheellista identiteettiä pidemmälle kuin pelkkä nimi tekaisemalla. On myös oletettavaa, että tällaiseen ryhmään pyrkimisen yhteydessä joutuu kanssakäymiseen vähintään ryhmän ylläpitäjän kanssa. Hän todennäköisesti tiedustelee ryhmään pyrkijältä vähintään, että kenen lapsen vanhempi ryhmään pyrkijä on. Lyhyenkin kontaktin ottaminen ja henkilön erehdyttäminen ovat tulkittavissa vähintään peitellyksi tiedonhankinnaksi tai vaihtoehtoisesti peitetoiminnaksi. Kontaktin ottaminen ei kuulu suunnitelmallisen tarkkailuun sen enempää kuin tarkkailun tai valvonnankaan piiriin (HE 224/2010 vp, 101-103).

Jos suljettu ryhmä on sellainen, mihin kuka tahansa pääsee sisään, siellä esimerkiksi käydään huutokauppaa, ovat siellä julkaistavat viestit myös avoimen datan piirissä. Tällaiseen ryhmään liityttäessä ei sinänsä erehdytetä ketään, eikä oteta kontaktia kehenkään. Ryhmään liittymispyyntö menee kyllä yksittäiselle henkilölle, mutta hän hyvin suurella todennäköisyydellä hyväksyy kaikki ryhmään pyrkijät kiinnittämättä huomioita siihen, kuka ryhmään on pyrkimässä. Tällaiseen ryhmään liittyminen ja siellä valvonnan suorittaminen kuuluisi näin tulkittuna yleisvalvonnan piiriin.

Valvontaa suorittavan poliisihenkilön nimimerkillä on myös merkitystä valvontaa suorittaessaan. Varmin tapa välttää ihmisten erehdyttäminen vahingossa, on käyttää täysin satiirista nimimerkkiä. Tällaisella nimimerkillä pyrkiminen johonkin suljettuun ryhmään ei mielestäni erehdytä ylläpitäjänä olevaa henkilöä. Hyväksyessään täysin satiirisen tunnuksen ryhmän jäseneksi, hyväksyy ryhmä sen, että nimimerkin takana voi olla kuka tahansa, poliisikin.

Eri nimen käyttämistä voi perustella myös virtuaalisen identiteetin ja todellisen identiteetin erolla. Virtuaalinen identiteetti voi Heinosen (2001, 65) mukaan olla täysin vastakkainen sille mitä esittäjä todellisessa elämässä on. Nimi voi olla mitä vain, sukupuolta pystyy vaihtamaan laittamalla rastin eri ruutuun kuin missä se on aikaisemmin ollut ja omaa historiaansa voi halutessaan vääristellä. Vaikka osa sosiaalisen median alustoista vaatiikin käyttäjää syöttämään todellista henkilöllisyyttä vastaavia tietoja, on tietojen väärin syöttäminen todella yleistä. Kun sosiaalisessa mediassa kuka tahansa voi rakentaa identiteettiään minkälaiseksi tahansa haluaa, herää kysymys, onko poliisilla ainoana toimijana velvollisuus syöttää todelliset henkilötietonsa tällaisiin palveluihin suorittaessaan valvontaa?

4.4 Pohdintaa valvonnan tarpeesta verkkoympäristössä.

Poliisin resurssit eivät tule ikinä riittämään totaalivalvontaan reaalimaailmassa eikä varsinkaan verkkoympäristössä. Poliisi tulee aina tarvitsemaan kansalaisilta ilmoituksia epäillyistä rikoksista ja reagoi niihin parhaan kykynsä mukaan. Poliisilla ei ole resursseja istua kahviloissa virkavaatteet päällä kaitsemassa siellä käytävää keskustelua. Myöskään siviilivaatteet päällä poliiseja harvoin istuu tällaisissa paikoissa suorittamassa valvontaa. Verkkoympäristön laajuus tekee verkkovalvonnan jopa reaalimaailmaa haastavammaksi. Aktiivisia kansalaisia tullaan siis tarvitsemaan aina.

Kysymys ei olekaan verkon totaalivalvonnasta, vaan usein muuhun analyysiin perustuvasta kohdennetusta valvonnasta tai lisätiedonhankinnasta. Poliisi ei voi luottaa siihen, että kaikki tarpeellinen tieto tulee kansalaisten ilmoituksina. Poliisin täytyy aktiivisesti kaivaa itsekin tietoa pystyäkseen reagoimaan erilaisiin yleistä järjestystä ja turvallisuutta uhkaaviin tilanteisiin. Esimerkiksi poliisin saadessa vinkin laittomasta mielenosoituksesta tai yleistä järjestystä ja turvallisuutta uhkaavasta käyttäytymisestä, on valvonnan suorittaminen verkossa välttämätöntä tarkemman tiedon saamiseksi. Tällaisen tiedon saaminen vaatii usein toimimista anonyyminä.

5 TUTKIMUKSEN TULOKSET

5.1 Johtopäätökset

Tiedonhankinta verkkoympäristöstä poliisin toiminnassa ei ole oikeudellisesti aivan yksinkertainen asia. Asiaa arvioitaessa tulee huomioida useita lakeja ja tulkita niiden sanomaa, koska tiedonhankintaa verkkoympäristössä ei ole laissa säädelty erikseen. Lainsäädännössä ei ole huomioitu verkkoympäristön erityispiirteitä ja sosiaalista mediaa

hyvin. Sosiaalinen media ilmiönä on tuore ja nopeasti muuttuva, joka asettaa lainsäädännön ajantasaisuudelle kovan haasteen.

Tutkimukseni alussa määritin tutkimusongelmaksi internetin rajatun avoimen tiedon saatavuuden poliisille. Lähdin tarkastelemaan sitä, mikä tieto on poliisin hyödynnettävissä ja mikä tieto puolestaan on poliisin ulottumattomissa normaalin valvonnan osalta. Mielestäni olen onnistunut tutkimuksessa tuomaan esiin tutkimuksen kannalta olennaiset asiat.

Poliisin toimintaa ohjaa useampi laki. Lähdin tulkitsemaan poliisin tiedonhankintaa ensin perustuslain näkökulmasta. Julkisen vallan käytön tulee aina perustua lakiin ja julkisen vallan käyttö rajoittaa usein ihmisten oikeuksia. Poliisin tiedonhankinta verkkoympäristössä ei tulkintani mukaan aiheuta sellaisia perustuslaillisia ongelmia, jotka estäisivät sen. Poliisin yleisvalvonta ei loukkaa kenenkään perusoikeuksia. Poliisi voi perustuslain ja siitä johdettujen alempiasteisten lakien mukaan valvoa yleistä keskustelua ilman, että se loukkaisi kenenkään sananvapautta tai kirjesalaisuutta. Sosiaaliseen mediaan jaetut kirjoitukset ovat pääosin julkisia ja poliisikin voi niitä seurata.

Rikoslain näkökulmasta poliisin on mahdollista syyllistyä joihinkin rikoksiin valvontaa suorittaessaan. Poliisin tuleekin valvonnassaan kiinnittää huomiota valvontatapaan, jottei oikeudenloukkauksia pääse tapahtumaan. Poliisihallitus on antanut tuoreen ohjeistuksen valvonnan käytännöistä sekä poliisin toiminnasta sosiaalisessa mediassa. Näiden ohjeiden noudattaminen on rikosvastuun poistumisen kannalta tärkeää.

Poliisilaki säätelee poliisin toimintaa merkittävimmin. Poliisilaki määrää poliisin tehtävän ja antaa poliisille toimivallan. Poliisin oikeudesta yleisvalvontaan internetissä ei ole epäselvyyttä, mutta valvonnan toteutustapaan poliisilaki ei annan selkeitä ohjeita. Poliisilaki on kirjoitettu reaalimaailmaa silmällä pitäen ja samat säännöt eivät päde verkkoympäristöön. Poliisi voi suorittaa yleisvalvontaa internetissä ja kirjautua järjestelmiin poliisitunnuksilla. Tällä tavalla valvomalla poliisilta jää kuitenkin suuri osa sosiaalisen median sisältämästä tiedosta saamatta.

Lainsäätäjä ei ole ottanut riittävällä tavalla kantaa siihen miten poliisin tulisi toimia verkkoympäristössä. Nyt voimassa oleva lainsäädäntö jättää tulkinnanvaraiseksi sen miten poliisi tulee valvontaa suorittaa sosiaalisessa mediassa.

Lainsäädäntöä tulkittaessa on mahdollista päätyä kahteen täysin vastakkaiseen johtopäätökseen väärällä nimellä kirjautumista koskien. Ensimmäisen tulkinnan mukaan sosiaaliseen mediaan kirjautuminen ei ole väärien henkilötietojen käyttöä, vaan valvonnan suorittamista oikeaa identiteettiä paljastamatta. Tällöin ei puhuta perinteisessä mielessä väärien tai harhauttavien tietojen antamisesta. Käytännössä tiedot annetaan ainoastaan verkkoympäristöön. Kun ketään yksittäistä henkilöä ei harhauteta, ei näin toimimista voida käsittää myöskään väärien tai harhauttavien tietojen käyttämiseksi. Näin toimimalla mahdollistetaan ainoastaan anonyymi sisäänpääsy verkkoympäristöön ja valvonnan suorittaminen siellä. Näin toimimalla rikotaan ainoastaan verkkoympäristön käyttöohjeita.

Näin vähäisen käyttöohjeiden rikkomisen ei voida katsoa loukkaavan kenenkään oikeuksia merkittävästi. Asiasta olisi hyvä kuitenkin sopia verkkoympäristön oikeuksien hallitsijan kanssa.

Toisenlainen tulkinta olisi, että poliisi voi käyttää vain niitä valtuuksia, joita lainsäätäjä sille erikseen antaa eikä ylläkuvatun kaltainen laajentava poliisioikeuksien käyttämien olisi mahdollista. Perustuslain määräämien lainalaisuusperiaatteen ja lakisidonnaisuuden vaatimuksen mukaisesti julkisen vallan käytön tulee perustua lakiin ja viranomainen ei voi toimia ilman lakiperustaa. Tästä johtuen poliisi ei voisi suorittaa tiedonhankintaa ja valvontaa kirjautumalla anonyymisti verkkopalveluihin, sen ollessa ainoastaan salaisena tiedonhankintakeinona käytettävissä. Tämäkin argumentti on käypä, sillä perusoikeuksiin puuttuva toiminta tulisi olla perusoikeusmyönteistä eli viranomaistoimintaa rajoittavaa. Myöskään tarkkailun suorittamiseksi ei olisi näin mahdollista käyttää tekaistuja tunnuksia, sillä lainsäätäjä otti tuon mahdollisuuden pois tarkkailun osalta poliisilain uudistuksessa vuonna 2014.

Lainsäätäjän selkeän tahdon osoittamattomuus jättää paljon harkinnanvaraa valvovalle viranomaiselle. Nyt valvontaa suorittava taho voi käyttää kumpaa tahansa tulkintaa asiassa, lain väljemmän tulkinnan varmasti ollessa toiminnallisesti sopivampi. Kun kaksi täysin vastakkaista tulkintaa on mahdollista tehdä, voidaan tulla siihen johtopäätökseen, että poliisi voi kirjautua verkkoympäristöihin anonyymillä tunnuksella. Poliisihallituksen ohjeistuksen mukaan toiminnan sosiaalisessa mediassa tulee kuitenkin olla selkeästi johdettua ja yhdenmukaista, jolloin jonkinlainen johtamis- ja seurantajärjestelmä sosiaalisen median valvonnassa on oltava olemassa. Selkeä ohjeistus toiminnasta sosiaalisessa mediassa tiedonhankinnan osalta on luotava. Ohjeistuksen olisi syytä olla valtakunnallinen, jotta poliisitoiminta verkkoympäristössä olisi poliisihallituksen ohjeen mukaisesti yhdenmukaista, verkostomaista ja valtakunnallista.

Mainittakoon vielä, että vaikka sosiaaliseen mediaan voi väljemmän tulkinnan mukaan luoda nimimerkin, joka ei vastaa poliisimiehen todellista identiteettiä, täytyy poliisin ottaa huomioon salaisen tiedonhankinnan rajoitukset. Näin luotuja tunnuksia voi siis käyttää vain valvontaan ja tarkkailuun. Tarkkailu ei kuulu salaisen tiedonhankinnan keinoihin, jolloin muu kuin pitkäaikainen ja jatkuva tiettyyn henkilöön kohdistuva tarkkailu ottamatta kontaktia yksittäisiin ihmisiin, on mahdollista nimimerkin tai väärän nimitiedon avulla samalla tavalla kuin valvontakin. Otettaessa kontaktia yksittäiseen ihmiseen vääriä tietoja käyttäen, mennään jo salaisen tiedonhankinnan sääntelyn alueelle.

Johtopäätökseni mukaan valvonta on mahdollista myös sellaisissa suljetummissa verkkoympäristöissä, jotka vaativat erillisen hyväksynnän ryhmän ylläpitäjältä sisällön yleisvalvontaa varten. Tämä siinä tapauksessa, että ylläpitäjään ei tarvitse ottaa muuta kontaktia, kuin laittaa pelkkä liittymispyyntö. Myöskään tällainen yksittäiselle ylläpitäjälle lähetetty pyyntö yleisvalvonnan suorittamiseksi ei ole nähtävissä väärän tiedon antamiseksi, suljetun ympäristön ollessa sellainen, minne hyväksytään kaikki halukkaat enempää kyselemättä. Nimimerkin on kuitenkin oltava sellainen, ettei ylläpitäjä voi erehtyä luulemaan poliisia joksikin toiseksi henkilöksi. Lisäksi kontaktin on rajoituttava

ainoastaan liittymispyyntöön, sillä lainsäädäntömme ei anna tällä hetkellä mahdollisuutta minkäänlaiseen peitetoimintaan yleisvalvonnan suorittamiseksi. Sellaisessa tapauksessa, että ylläpitäjä esittää tiedusteluja liittymispyynnön lähettäneelle poliisille, on poliisin harkittava toiminnallisen tarpeen mukaan, kertooko hän ylläpitäjälle millä asialla on vai vetäytyykö hän tilanteesta.

On myös huomioitava, että lainsäätäjä on ottanut selkeästi kantaa myös verkkoympäristössä tapahtuvaan salaiseen tiettyyn henkilöön kohdistuvaan peiteltyyn tiedonhankintaan ja peitetoimintaan verkkoympäristössä. Tämä lainsäädäntö tulee huomioida, jos vääriä tietoja käytetään yksittäisen henkilön seurantaan.

Työni toisena tarkoituksenani oli selvittää, voiko poliisihenkilö käyttää omaa henkilökohtaista profiiliaan tiedonhankinta- tai valvontatarkoituksessa sosiaalisessa mediassa. Poliisihallituksen antaman poliisin sosiaalisen median ohjeen mukaan toiminnan verkkoviestintäympäristössä on oltava selkeäasti johdettua, avointa sekä yhdenmukaista. Varsinaiseen virkatehtävään liittyen oman profiilin käyttö on täten kyseenalaista ja aiemmat johtopäätökset huomioon ottaen, myös tarpeetonta. Poliisihenkilöt liikkuvat tietenkin sosiaalisen median maailmassa vapaa-ajallaan aivan kuten reaalimaailmassakin. Poliisin velvollisuus vapaa-ajallaankin ilmoittaa vakavasta rikoksesta koskee myös sosiaalista mediaa.

Työni osoittaa todeksi väittämän siitä, että asiaa ei ole yksiselitteisesti säädetty laissa. Verkkoympäristö muuttuu nopeaan tahtiin ja lainsäätäjä ei aina pysy mukana kehityksessä. Lakiviittauksia sosiaalisen median ympäristöön on hyvin vähän. Lainsäätäjän tahto verkkoympäristöön kohdistuvaa valvontaa kohtaan ei tule riittävän hyvin selville nykyisestä lainsäädännöstä.

Poliisitoiminnan perusasioita ovat tiedonhankinta ja tiedon analysointi. Johtopäätöstäni tukee myös se, että poliisitoiminnan kannalta olisi erikoista, että poliisi ei pääsisi käsiksi sellaiseen tietoon, joka on hyvin helposti kaikkien muidenkin saatavilla.

5.2 Tutkimuksen luotettavuus ja pätevyys

Oikeustieteellisen tutkimuksen metodien tulee olla sellaisia, joita tiedeyhteisö voi arvioida ja kontrolloida. Käytettävät metodit eivät voi olla itse luotuja tai intuitiivisesti valittuja vaan niillä täytyy olla tiedeyhteisön hyväksyntä. Hyvänä oikeustieteenä ei voida pitää sitä, että ainoastaan kirjataan voimassaolevia normeja, tulkintoja ja teorioita. Tutkielmassa pitää olla ja näkyä tutkijan oma panos, on esitettävä uutta materiaalia ja kysyttävä jotain uutta aiheesta. (Hirvonen 2011, 18.)

Olen käyttänyt tutkimuksessani oikeusdogmatiikkaa eli lainoppia. Se on oikeustieteissä vakiintunut tutkimusmenetelmä lain tulkinnasta, joka jäsentää voimassa olevaa oikeutta ja tulkitsee oikeuden sisältöä. (Hirvonen 2011, 21-23.) Tutkimuksen lähdemateriaalina olen käyttänyt lainsäädäntöä, lakien esitöitä, oikeustieteellistä kirjallisuutta ja tieteellisiä julkaisuja. Lainoppia olen käyttänyt lähdemateriaalia tulkitessani ja systematisoidessani.

Tutkimuksen validius eli pätevyys tarkoittaa sitä, että tutkimus on perusteellisesti tehty, saadut tulokset ja tehdyt päätelmät ovat oikeita. Pätevyys voidaankin ymmärtää uskottavuutena ja vakuuttavuutena, että tutkijan päätelmät tuodaan ymmärrettävästi esille myös muille. Reliabiliteetti tarkoittaa tutkimuksen johdonmukaisuutta ja luotettavuutta. Reliabiliteettia arvioitaessa pyritään miettimään, pystytäänkö tutkimustulokset toistamaan vai ovatko saadut tulokset vain sattumaa. (Saaranen-Kauppinen & Puusniekka 2006, kohdat 3.3.1 ja 3.3.2.)

Pidän tutkimustani validina, sillä olen käyttänyt tutkimusmenetelmänä oikeustieteen vakiintunutta tutkimusmenetelmää. Olen myös käyttänyt lähteinä alan tärkeimpiä lähteitä, joista olen perustellusti koostanut johtopäätökseni. Johtopäätökseni vastaavat tutkimusongelmaan ja ratkaisevat kysymyksiä, joita tutkimuksessa on asetettu. Tutkimuksen luonteeseen kuuluu se, että johtopäätöksissä ei ole yhtä ainoaa oikeaa vastausta, mutta olen tuonut selkeästi ja ymmärrettävästi esiin sen, miksi kyseisiin johtopäätöksiin on päädytty. Tutkimuksen toistettavuuden arviointia en pidä mielekkäänä, sillä tutkimuksessa ei ole käytetty mitään määrää mittaavia tuloksia, joita voisi verrata keskenään. Pidän tutkimusta kuitenkin reliaabelina, sillä se seuraa johdonmukaisesti valittua tutkimusmetodia oikeustieteen vakiintuneen käytännön mukaisesti.

5.3 Jatkotutkimus

Tutkimuksessani käsiteltiin pääasiassa yhtä sosiaalisen median alustaa ja sen toiminnallisuuksia. Pyrkimyksenä oli kuitenkin selvittää mahdollisimman kattavasti yleisellä tasolla sosiaalisessa mediassa vastaan tulevia tilanteita. Perehtyminen sosiaalisen median eri alustoihin ja niiden vertailu sen selvittämiseksi, onko niissä sellaisia toiminnallisuuksia, joihin tämä tutkimus ei anna vastausta, olisi tarpeellinen jatkotutkimuksen kohde. Tutkimuksessani esitetään myös väite poliisin toimimisesta anonyyminä internetissä. Määrällinen tutkimus polisiin anonyymistä toiminnasta verkkoympäristössä olisi tarpeellinen sen mittaamiseksi, miten suurestä ilmiöstä on kysymys.

LÄHTEET

Abram, Carolyn 2016: Facebook for dummies. 6th edition. Hoboken, New Jersey. John Wiley & Sons, Inc.

Company info 2017.
Luettavissa: https://newsroom.fb.com/company-info/
Luettu 19.9.2017

Forss, Marko 2014: Fobban sosiaalisen median selviytymisopas. Helsinki, Crime time.

Forss, Marko & Keinänen, Anssi 2017: Rikoslakia koskeva lainvalmistelu – miten internet ja erityisesti sosiaalinen media huomioitiin vuosina 2009–2016 annetuissa hallituksen esityksissä.
Edilex-sarja 2017/38. Edita Publishing Oy.
Luettavissa: https://www-edilex-fi.polamk.idm.oclc.org/artikkelit/18068.pdf
Luettu: 15.10.2017

Hankilanoja, Arto 2014: Poliisin salainen tiedonhankinta. Helsinki, Alma Talent Oy.

HE 1/1998 vp. Hallituksen esitys Eduskunnalle uudeksi Suomen Hallitusmuodoksi.

HE 54/2002 vp. Hallituksen esitys Eduskunnalle laiksi sananvapauden käyttämisestä joukkoviestinnässä ja eräiksi siihen liittyviksi laeiksi.

HE 125/2003 vp. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 224/2010 vp. Hallituksen esitys Eduskunnalle poliisilaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 232/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkko-rikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

Helminen, Klaus & Kuusimäki, Matti & Rantaeskola, Satu 2012: Poliisilaki. Helsinki, Alma Talent Oy.

Heinonen, Risto 2001: Digitaalinen minä. Helsinki, Edita.

Hirvonen, Ari 2011: Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki.
Luettavissa:
https://www.helsinki.fi/sites/default/files/atoms/files/hirvonen_mitka_metodit.pdf
Luettu: 15.10.2017

Husa, Jaakko ja Pohjolainen, Teuvo 2014: Julkisen vallan oikeudelliset perusteet. Johdatus julkisoikeuteen. Helsinki, Talentum.

Kallas, Priit 2017: Top 15 Most Popular Social Networking Sites and Apps [October 2017].
Luettavissa: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/

Luettu: 19.9.2017

Kalliala, Eija & Toikkanen, Tarmo, 2012: Sosiaalinen media opetuksessa. Helsinki, Finn Lectura.

Kari, Matti 2017: Tarkastelu sisäministeriön ja poliisin resurssien ja poliisitoimen palvelujen laadun tasosta ja kehityksestä. Raportteja 35. Helsinki, Palkansaajien tutkimuslaitos
Luettavissa: http://www.labour.fi/?wpfb_dl=4483
Luettu 16.10.2017

LaVL 21/2010 vp. Lakivaliokunnan lausunto 21/2010. Hallituksen esitys poliisilaiksi ja eräiksi siihen liittyviksi laeiksi.

Miettinen, Tarmo 2016: Oikeustieteellinen opinnäyte - artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edilex.
Luettavissa: www.edilex.fi/kirjat/16170
Luettu: 19.9.2017

Mäenpää, Olli 2008: Hallintolaki ja hyvän hallinnon takeet. 2. uudistettu painos. Helsinki, Edita

Mäenpää, Olli 2011: Oikeus hyvään hallintoon. Helsinki, Helsingin yliopiston oikeustieteellinen tiedekunta.

Mäntymää, Eero 2017: Poliisi rekrytoi 25 uutta nettipoliisia – "kyse ei ole sananvapauden rajoittamisesta". Luettavissa: https://yle.fi/uutiset/3-9437958
Luettu: 19.9.2017

Pesonen, Pirkko 2013: Sosiaalisen median lait. Helsinki. Lakimiesliiton kustannus.

Poliisihallitus 2017: Poliisin toiminta sosiaalisessa mediassa. Poliisihallituksen ohje POL-2017-8358.

Poliisin arvot: Luettavissa: http://www.poliisi.fi/tietoa_poliisista/poliisin_arvot
Luettu 10.10.2017

Pönkä, Harto 2014: Sosiaalisen median käsikirja. Jyväskylä, Docendo.

Savolainen, Reijo 2010: Tiedonhankintatutkimuksen lähtökohtia
Teoksessa: Ote informaatiosta: Johdatus informaatiotutkimukseen ja interaktiiviseen mediaan. Serola, Sami (toim.). Helsinki, BTJ, 75-115.

Suominen, Jaakko 2013: Sosiaalisen median aika.
Teoksessa: Sosiaalisen median lyhyt historia. Saarikoski, Petri & Suominen, Jaakko & Turtiainen, Riikka & Östman, Sari. Helsinki, Gaudeamus, 9-27.

Saaranen-Kauppinen, Anita & Puusniekka, Anna 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. Luettavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali.
Luettu 15.10.2017