# Salaiset tiedonhankinta- ja pakkokeinot poliisi- ja peiteprofiileilla

Itä-Suomen yliopisto
Yhteiskunta- ja kauppatieteiden tiedekunta
Pro gradu -tutkielma
10.5.2019
Tekijä: Marko Forss 246741
Ohjaaja: Mika Launiala

# TIIVISTELMÄ

ITÄ-SUOMEN YLIOPISTO

| Tiedekunta | Yksikkö |
|---|---|
| **Yhteiskuntatieteiden ja kauppatieteiden tiedekunta** | **Oikeustieteiden laitos** |
| Tekijä<br>**Marko Forss** | Ohjaaja<br>**Mika Launiala** |

| Työn nimi |
|---|
| **Salaiset tiedonhankinta- ja pakkokeinot poliisi- ja peiteprofiileilla** |

| Pääaine | Työn laji | Aika | Sivuja |
|---|---|---|---|
| **Rikos- ja prosessioikeus ja rikollisuuden tutkimus** | **Pro gradu -tutkielma** | **10.5.2019** | **XXIV+160** |

Tiivistelmä

Poliisin salaiset tiedonhankinta- ja pakkokeinot pitävät sisällään laajat mahdollisuudet suorittaa tiedonhankintaa salassa kohteilta rikosten estämiseksi, paljastamiseksi ja selvittämiseksi. Tämän tutkimuksen tarkoituksena on esitellä poliisi- ja peiteprofiileilla mahdolliset salaiset tiedonhankinta- ja pakkokeinot tietoverkoissa sekä tulkita profiileilla mahdollisten toimivaltuuksien keskinäistä suhdetta toisiinsa.

Perus- ja ihmisoikeusnäkökulma on korostuneessa roolissa salaisissa tiedonhankinta- ja pakkokeinoissa. Tietoverkoissa kotirauhan suoja ei ole merkittävässä roolissa, mutta luottamuksellisen viestinnän suoja vaikuttaa poliisi- ja peiteprofiilien toimintaan jo jonkin verran. Laajimmin tutkimuksessa käsitellään yleisesti yksityiselämän suojan eroja reaalimaailmassa ja tietoverkoissa, jossa problematiikka on jaettu viiteen eri alakohtaan.

Tutkimus esittelee poliisi- ja peiteprofiilit, mutta myös poliisimiehen siviiliprofiiliin käyttöön liittyvät tulkintaongelmat. Poliisiprofiilien kohdalla on kyse poliisin näkyvästä toiminnasta tietoverkoissa, jolla on kuitenkin liittymäpinta salaiseen tiedonhankintaan. Peiteprofiileihin liittyen tuodaan esille suojaamissääntelyn merkitys peiteprofiilin luomiseen sekä tarkastellaan sen mahdollisuutta yleisvalvonnan ja tarkkailun osalta.

Avainsanat: poliisiprofiili, peiteprofiili, tietoverkot, internet, sosiaalinen media, salaiset tiedonhankintakeinot, salaiset pakkokeinot

# SISÄLLYS

TIIVISTELMÄ....II

LÄHTEET....V

LYHENNELUETTELO....XXIII

KUVIOT JA TAULUKOT....XXV

1 JOHDANTO....1

1.1 Salaisten tiedonhankinta- ja pakkokeinojen toimivaltuussääntelykehityksestä erityisesti tietoverkkojen näkökulmasta....1

1.2 Salaisten tiedonhankinta- ja pakkokeinojen jaottelu sekä rikoksen estäminen, paljastaminen ja selvittäminen....4

1.3 Tutkimuskysymykset ja tutkimuksen rajaukset....7

1.4 Tutkimusmetodi ja tutkimuksen rakenne....14

2 SALAISIA TIEDONHANKINTA- JA PAKKOKEINOJA KOSKEVAT IHMISOIKEUSSOPIMUKSET JA EU-LAINSÄÄDÄNTÖ....21

2.1 Ihmisoikeussopimukset....21

2.2 Euroopan unionin lainsäädäntö....23

3 SALAISIA TIEDONHANKINTA- JA PAKKOKEINOJA KOSKEVAT PERUSOIKEUDET ERITYISESTI TIETOVERKKOJEN NÄKÖKULMASTA....26

3.1 Salaisiin tiedonhankinta ja -pakkokeinoihin vaikuttavat perusoikeudet....26

3.2 Kotirauhan suoja....27

3.3 Luottamuksellisen viestin suoja....31

3.4 Yksityiselämän suoja....40

3.4.1 Yleistä yksityiselämän suojasta....41

3.4.2 Tiedon syntymistapa....42

3.4.3 Henkilön yksilöiminen ja tunnistaminen....44

3.4.4 Tiedonhankinnan kohde....49

3.4.5 Tiedon keräämistapa, reaaliaikaisuus ja laajuus....52

3.4.6 Tiedon laatu ja luotettavuus....56

3.5 Yhteenveto perus- ja ihmisoikeussuojan eroista reaalimaailmassa ja tietoverkoissa....59

4 PERUS- JA IHMISOIKEUKSIEN VAIKUTUS SALAISIA TIEDONHANKINTA- JA PAKKOKEINOJA KOSKEVIIN TOIMIVALTUUKSIIN....62
4.1 Poliisin toimintaa ohjaavat yleiset periaatteet....62
4.2 Yleiset edellytykset....64
4.3 Erityiset edellytykset....68
4.4 Muut oikeusturvatakeet....74
5 POLIISIN NÄKYVÄT PROFIILIT TIETOVERKOISSA....79
5.1 Nettipoliisitoiminta ja muu poliisin näkyvä toiminta tietoverkoissa....79
5.2 Näkyvän poliisiprofiilin luominen ja suhde salaisiin tiedonhankinta- ja pakkokeinoihin....81
5.3 Siviiliprofiilin käyttö poliisin työtehtävissä....81
6 POLIISIN PEITEPROFIILIT TIETOVERKOISSA....86
6.1 Salaisten tiedonhankinta- ja pakkokeinojen suojaaminen....86
6.2 Peiteprofiilien luomismahdollisuudet yleisvalvontaa ja tarkkailua varten....96
6.3 Peiteprofiililla toimivan velvollisuudet puuttua havaittuihin rikoksiin....101
7 POLIISI- JA PEITEPROFIILEJA KOSKEVAT SALAISET TIEDONHANKINTA- JA PAKKOKEINOT TIETOVERKOISSA....105
7.1 Yleisvalvonta....105
7.2 Tarkkailu....108
7.3 Suunnitelmallinen tarkkailu....115
7.4 Peitelty tiedonhankinta....120
7.5 Peitetoiminta....124
7.6 Valeosto....132
7.7 Tietolähdetoiminta....139
8 JOHTOPÄÄTÖKSET....149

# LÄHTEET

## KIRJALLISUUS

Aarnio, Aulis:

- Laintulkinnan teoriaa. Yleisen oikeustieteen oppikirja. Juva 1989.
- Tulkinnan taito. Ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. Vantaa 2006.
- Luentoja lainopillisen tutkimuksen teoriasta. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut. Helsinki 2011.

Aalto, Tuija – Uusisaari, Marylka Yoe: Löydy – Brändää itsesi verkossa. Vantaa 2010.

Ammar, Jamil – Xu, Songhua: When Jihadi Ideology Meets Social Media. Palgrave Macmillan 2018.

Awan, Imran: Cyber Threats and Cyber Terrorism: The Internet as a tool for Extremism, s. 21–38 teoksessa Awan, I,ran – Blakemore, Brian, Policing Cyber Hate, Cyber Threats and Cyber Terrorism. MPG Books Group UK 2012.

Bazzell, Michael: Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information. Third Edition. CCI Publishing 2014.

Bright, David A.: Disrupting and Dismantling Dark Networks: Lessons from Social Network Analysis and Law Enforcement Simulations, s. 39–52 teoksessa Gerdes, Luke M. (toim.), Illuminating Dark Networks. The Study of Clandestine Groups and Organisations.

Bosk, Daniel – Rodriguez-Cano, Guillermo – Greschbach, Bemjamin – Buchegger, Sonja: Applying privacy-enchancing technologies: one alternative future of protests, s. 73–94 teoksessa Melgaço, Lucas – Monaghan, Jeffrey (toim.), Protests in the Information Age. Routledge 2018.

Burattin, Andrea – Cascavilla, Giuseppe – Conti, Mauro: SocialSpy: Browsing (Supposedly) Hidden Information in Online Social Networks, s. 83–99 teoksessa Springer, Charm (toim.), International Conference on Risks and Security of Internet and Systems. CRiSIS Confrence paper 27.8.2014.

Calcara, Giulio – Forss, Marko – Tolvanen, Matti – Sund, Peter: The Finnish Internet Police (Nettipoliisi): towards the developement of a real cyber police. European Journal of Law and Technology, Vol 6, No 2, 2015.

Cascavilla, Giuseppe – Conti, Mauro – Scwartz, David G. – Yahav, Inbal: Revealing Censored Information Throgh Comments and Commenters in Online Social Networks, s.

675–680 teoksessa Pei, Jian – Silvestri, Fabricio – Tang, Jie (toim.), Proceedings of the 2015 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining.

Erbschloe, Michael: Extremist Propaganda in Social Media. CRC Press Taylor & Francis Group 2019.

Euroopan unionin neuvosto: The Network of National Wxperts on Joint Investigation Teams. Yhteiset tutkintaryhmät - Käytännön opas. 6128/1/17 REV 1. 14.2.2017.

Europol: Internet Organised Crime Assessment (IOCTA) 2018. EC3 European Cybercrime Centre.

Forss, Marko:

- Kuolemanjälkeinen kunnia ja yksityiselämä - mitä tietoja kansalainen saa julkaista kuolleesta henkilöstä erityisesti sosiaalisessa mediassa? Teoksessa: Korpisaari, Päivi: Viestintäoikeuden vuosikirja 2016. Viestinnän muuttuva sääntely. Helsinki 2017.
- Fobban sosiaalisen median selviytymisopas. GPD Group 2014.
- Lähipoliisi tavoittaa virtuaalimaailmassakin, s. 244–259 teoksessa Aaltonen-Ogbeide, Terhi – Saastamoinen, Pentti – Rainio, Heikki – Vartiainen, Heikki, Silmät auki sosiaaliseen mediaan. 2. painos. Eduskunnan tulevaisuusvaliokunnan julkaisu 3/2011. Eduskunnan monistamo 2011.

Forss, Marko – Keinänen, Anssi: Rikoslakia koskeva lainvalmistelu - miten internet ja erityisesti sosiaalinen media huomioitiin vuosina 2009–20016 annetuissa hallituksen esityksissä. Edilex 21.9.2017. [https://www-edilex-fi.ezproxy.uef.fi:2443/artikkelit/18068.pdf]

Froomkin, Michael A.: Pseudonyms by Another Name: Identity Management in a Time of Surveillance, s. 61–69 teoksessa Rotenberg, Marc – Horwitz, Julia – Scott Jeramie: Privacy in the Modern Age, The Search for Solutions. New York 2015.

Frände, Dan: Näkökohtia todiste- ja rikosprovokaatiosta. Lakimies 3/2004, s. 404–411.

Fuchs, Christian: Social media surveillance, s. 395–414 teoksessa Coleman, Stephen – Freelon Deen (toim.), Handbook of Digital Politics. Edward Elgar Puplishing Inc 2015.

Gillen, Martina: Lawyers and Cyberspace: Seeing the Elephant?. ScriptED, Volume 9, Issue 2, August 2012.

Gravelle, James: Knowledge Magement and Cyber Terrorism, s. 111–128 teoksessa: Teoksessa: Awan, I,ran – Blakemore, Brian: Policing Cyber Hate, Cyber Threats and Cyber Terrorism. MPG Books Group UK 2012.

Gullans, Monica: Luku VII artikla 8: Teoksessa: Pellonpää, Matti – Gullans, Monica – Pölönen, Pasi – Tapanila, Antti: Euroopan ihmisoikeussopimus. 6., uudistettu painos. Helsinki 2018.

Haapamäki, Juha: Poliisin salaisen tiedonhankinnan valvonnasta, s. 191–201 teoksessa Eduskunnan oikeusasiamies 90v. Sastamala 2010.

Hankilanoja, Arto: Poliisin salainen tiedonhankinta. Helsinki 2014.

Hirvelä, Päivi – Heikkilä, Satu: Ihmisoikeudet – Käsikirja EIT:n oikeuskäytäntöön. 2., uudistettu painos. Alma Talent 2017.

Hirvonen, Ari: Oikeuden ja lainkäytön teoria. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki 2012.

Heinonen, Risto: Digitaalinen minä. Helsinki 2001.

Heinonen, Risto – Hannula, Ilari: Valvonta tietoyhteiskunnassa. Helsinki 1999.

Helminen, Klaus – Fredman, Markku – Kanerva, Janne – Tolvanen, Matti – Viitanen, Marko: Esitutkinta ja pakkokeinot. Helsinki 2014.

Helminen, Klaus – Kuusimäki, Matti – Rantaeskola, Satu: Poliisilaki. Helsinki 2012.

Helminen, Klaus – Kuusimäki, Matti – Salminen, Markku: Poliisioikeus. Jyväskylä 1999.

Innanen, Antti – Saarimäki, Jarkko: Internetoikeus. 2., uudistettu painos. Porvoo 2012.

Kenney, Michael – Coulthart, Stephen: The Methodological Challenges of Extracting Dark Networks: Minimizing False Positives through Ethnography, s. 52–70 teoksessa Gerdes, Luke M. (toim.), Illuminating Dark Networks. The Study of Clandestine Groups and Organisations. Cambridge University Press 2015.

Kim, KiDeuk – Oglesby-Neal, Ashlin – Mohr, Edward: 2016 Law Enforcement Use of Social Media Survey. A Joint Publication by the International Association of Chiefs of Police and the Urban Institute. Washington, February 2017.

Kolehmainen, Antti, Tutkimusongelma ja metodi lainopillisessa työssä, s. 105–134 teoksessa, Tarmo Miettinen (toim.): Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edilex Kirjat 16.2.2016. [www.edilex.fi/kirjat/16170]

Korja, Juhani: Biometrinen tunnistaminen ja henkilötietojen suoja. Väitöskirjatutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta. Turenki 2016.

Kosinski, Michal – Stillwell, David, Graepel, Thore: Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences (PNAS), vol. 110, no. 15, April 9, 2013. s. 5802–5805.

Koulu, Riikka: Jokakodin laajakaista – pääsy internetiin perusoikeutena. Lakimies 2/2012, s. 280–302.

Kurenmaa, Tero: Rikostorjunnan tila. Selvityshankkeen loppuraportti 1/2018. Poliisihallituksen julkaisusarja 31.8.2018.

Lappi-Seppälä, Tapio: Rikosoikeustutkimus, kriminaalipoliittinen orientaatio – ja metodi, s. 189–218 teoksessa Häyhä, Juha (toim.), Minun metodini. Porvoo 1997,

Lessig, Lawrence: Code and Other Laws of Cyberspace. Basic Books. New York 1999.

Malkki, Leena – Pohjonen, Matti: Jihadistinen verkkoviestintä ja Suomi. Sisäministeriön julkaisuja 2019:15. Helsinki 2019.

Martellozzo, Elena: Policing online child sexual abuse – the British experience. European Journal of policing Studies. Volume 3, Issue 1, 6.10.2015. s. 32–52.

McKeown, Sean – Maxwell, David – Azzopardi, Leif – Glisson, Willian Bradley: Investigating People: A Qualitative Analysis of the Search Behaviours of Open-Source Intelligence Analysts, s. 175–184 teoksessa, XXiX ’14 Proceedings of the 5th Information Interaction in Context Symposium. Regensburg, Germany 2014.

Metsäranta, Tuomas: Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja. Väitöskirja. Turku 2015.

Miller, Seumas – Gordon, A. Ian: Investigative Ethics. Ethics for Police Detectives and Criminal Investigators.Wiley Blackwell 2014.

Mitnick, Kevin: The Art of Invisibility. Little, Brown and Company. New York, February 2017.

Mäkipää, Leena: Tietolähteiden käyttäminen poliisin tiedonhankinnassa. Lakimies 4/2009. s. 575–596.

Määttä, Ari: Luottamuksellisen viestin suoja erityisesti tietoverkoissa. Poliisiammattikorkeakoulun tiedotteita 18. Helsinki 2002.

Niskakangas, Hanna – Lahtinen, Hanna – Tolvanen, Matti: Tuomareiden tietämys silminnäkijätunnistamisen luotettavuuteen vaikuttavista tekijöistä todistajapsykologisen tutkimustiedon valossa. Defensor Legis N:o 6/2017, s. 867–884.

Nuotio, Kimmo:

- Oikeuslähteet, ”supernormistot” ja ratkaisujen perustelu. Teoksessa: Tala, Jyrki – Wikström, Kauko: Oikeus – kulttuuria ja teoriaa. Juhlakirja Hannu Tolonen 2005. Turun yliopisto, Oikeustieteellinen tiedekunta 2005.
- Oikeuslähteet ja yleiset opit. Lakimies 7–8/2004, s. 1267–1291.

Pellonpää, Matti: Luku II. Teoksessa: Pellonpää, Matti – Gullans, Monica – Pölönen, Pasi – Tapanila, Antti: Euroopan ihmisoikeussopimus. 6., uudistettu painos. Helsinki 2018.

Pesonen, Pirkko:

- Viestinnän lait. Keuruu 2017.
- Sosiaalisen median lait. Viro 2013.

Piispanen, Kirsi: Välttämätön paha? Näkökohtia poliisin preventiivisestä epäkonventionaalisesta tiedonhankinnasta, s. 179–193 teoksessa Länsineva, Pekka – Viljanen Veli-Pekka (toim.): Perusoikeuspuheenvuoroja. Turku 1998.

Pitkänen, Olli – Tiilikka, Päivi – Warma, Eija: Henkilötietojen suoja. Helsinki 2013.

Police Executive Research Forum: Future Trends in Policing. Office of Community Oriented Policing Services. Washington D.C. 2014.

Procter, Rob – Crump, Jeremy – Karstedt, Susanne – Voss, Alex – Cantijoch, Marta: Reading the riots: what were the police doing on Twitter?, s. 5–28 teoksessa Wall, Davis S. – Williams, Matthew L.: Policing Cybercrime. Networked and Social Media Technologies and the Challenges for Policing. Routledge 2014.

Pölönen, Pasi: Salaiset pakkokeinot. Vammala 1997.

Pölönen, Pasi – Tapanila, Antti: Todistelu oikeudenkäynnissä. Helsinki 2015.

Pönkä, Harto: Sosiaalisen median käsikirja. Saarijärven Offset Oy 2014.

Rainiala, Petri: Tiedottajan käyttö poliisin tiedonhankintamenetelmänä. Poliisiammattikorkeakoulun tutkimuksia 36/2009. Tampere 2009.

Rouhiainen, Lasse: Artificial Intelligence. 101 things you must know today about our future. Columbia, SC 2018.

Sajama, Seppo: Argumentaatio oikeustieteellisessä tutkimuksessa, s. 24–50 teoksessa: Tarmo Miettinen (toim.): Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Edilex Kirjat 16.2.2016. [www.edilex.fi/kirjat/16170]

Salminen, Markku: Poliisin tiedonsaantioikeus poliisilain kannalta. Poliisin oppikirjasarja 4/1995. Helsinki 1995.

Saraviita, Ilkka: Perustuslaki. Toinen, uudistettu painos. Helsinki 2011.

Savola, Pekka: Sähköisen viestinnän luottamuksellisuuden rajoitusten oikeasuhtaisuuden arvioimisesta. Edilex 13.9.2017 [https://www-edilex-fi.ezproxy.uef.fi:2443/artikkelit/18057.pdf]

Semenov, Alexander: Principles of Socila Media Monitoring and Analysis Software. Academic dissertation. Faculty of Information Tachnology of the University of Jyväskylä. Jyväskylä Studies in Computing 168. Jyväskylä 2013.

Seppälä, Pauliina – Mikkola, Tomi: Huumeet Internetissä ja nuorisokulttuureissa. Havaintoja huumeiden merkityksistä ja riskikäsityksistä käyttäjäpiireissä. Sosiaali- ja terveysalan tutkimus- ja kehittämiskeskus. Raportteja 287. Saarijärvi 2004.

Shipley Todd G. – Bowker, Art: Investigating Internet Crimes. An Introduction to Solving Crimes in Cyberspace. Syngress 2014.

Siljander, Raymond P. – Fredrickson, Darin D: Fundamentals of Physical Surveillance: A Guide for Uniformed and Plainclothes Personnel. Third Edition. Springfield, Illinois 2016.

Siltala, Raimo:

- Oikeustieteen tieteenteoria. Vammala 2003.
- Johdatus oikeusteoriaan. Helsinki 2001.

Sinisalo, Kari:

- Poliisi. Poliisioikeuden perusteet. Helsinki 1973.
- Poliisin toimivallan määräytyminen. Tutkimus poliisin vallasta ylläpitää yleistä järjestystä ja turvallisuutta. Vammala 1971.

SPJL: Poliisi & Oikeus 1/2019. Suomen poliisijärjestöjen liiton jäsenlehti.

Stratcom: NATO Strategic Communications Centre of Excellence. Robotrolling. Issue 1/2019. [https://www.stratcomcoe.org/robotrolling-20191]

Suojelupoliisi: Suojelupoliisi juhlavuosikirja 70 vuotta. Julkaistu 21.3.2019.

Svantesson Dan Jerker B: The Characteristics Making Internet Communication Challenge Traditional Models of Regulation – What Every International Jurist Should Know About the Internet. International Journal of Law and Information Technology (IJLIT). Spring 2005, s. 39–69.

Tapanila, Antti: Luku VII. Teoksessa: Pellonpää, Matti – Gullans, Monica – Pölönen, Pasi – Tapanila, Antti: Euroopan ihmisoikeussopimus. 6., uudistettu painos. Helsinki 2018.

Terenius, Markus: Poliisin voimankäyttö. Rikosoikeudellinen tutkimus sallitun voimankäytön rajoista. Sastamala 2013.

Tolonen, Hannu: Oikeuslähdeoppi. Helsinki 2003.

Trottier, Daniel: Social Media as Surveillance. Rethinking Visibility in a Converging World. Ashgate Publishing Ltd 2012.

Tuori, Kaarlo: Oikeusjärjestys ja oikeudelliset käytännöt. Helsinki 2013.

Uldam, Julie: Between visibility and surveillance: challenges to anti-corporate activism in social media, s. 115–134 teoksessa: Melgaço, Lucas – Monaghan Jeffrey: Protests in the Information Age. Social Movements, Digital Practices and Surveillance. Routledge 2018.

Viljanen, Veli-Pekka: Yksityiselämän suoja (PL 10 §), s. 389–411 teoksessa Hallberg, Pekka – Karapuu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka, Perusoikeudet. Helsinki 2011.

Voigt, Sebastian – Hinz, Oliver – Jansen, Nora: Law Enforcement 2.0 – The Potential And The (Legal) Restrictions Of Facebook Data For Police Tracing And Investigation. Association. ECIS 2013 Completed Research. 5.

Voutilainen, Tomi:

- Oikeus tietoon. Informaatioikeuden perusteet. Porvoo 2012.
- ICT-oikeus sähköisessä hallinnossa. ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely. Helsinki 2009.

Wells, Douglas – Gibson, Helen: OSINT from a UK perspective: considerations from the law enforcement and military domains, s. 84–113 teoksessa, Estonian Academy of Security Sciences. From Research to Security Union. Number 16, Tallinna 2017.

Wilhemsson, Thomas: Sosiaalisen siviilioikeuden metodiset lähtökohdat, s. 339–358 teoksessa, Häyhä, Juha (toim.): Minun metodini. Werner Söderström Lakitieto Oy 1997,

Willner-Mäenpää, Daniela: TOR-verkkoa hyödyntävä rikollisuus. Poliisiammattikorkeakoulun opinnäytetyö. 11/2018.

Ylösjoki, Pentti:

- Poliisioikeus I. Hämeenlinna 1963.
- Poliisioikeus II. Hämeenlinna 1966.

**VIRALLISLÄHTEET**

HaVL 5/1994 vp. Hallintovaliokunnan lausunto liittyen hallituksen esitykseen (HE 135/1994 vp eduskunnalle Suomen liittymisestä Euroopan unioniin tehdyn sopimuksen eräiden määräysten hyväksymisestä (nide I) Sopimus Norjan, Itävallan, Suomen ja Ruotsin liittymisestä Euroopan unioniin (nide II) Sopimus Euroopan unionista ja Euroopan talousyhteisön perustamissopimus (nide III) Euroopan atomienergiayhteisön perustamissopimus ja Euroopan hiili- ja teräsyhteisön perustamissopimus (nide IV) Euroopan yhteisöjen perustamissopimuksia muuttavat sopimukset ja asiakirjat (nide V).

HaVM 50/2010 vp. Hallintovaliokunnan mietintö liittyen hallituksen esitykseen (HE 185/2010 vp) laiksi kotoutumisen edistämisestä ja eräiden siihen liittyvien lakien muuttamisesta.

HaVM 42/2010 vp. Hallintovaliokunnan mietintö liittyen hallituksen esitykseen (224/2010 vp) poliisilaiksi ja eräiksi siihen liittyviksi laeiksi.

HaVM 10/2005 vp. Hallintovaliokunnan mietintö liittyen hallituksen esitykseen (266/2004 vp) laiksi poliisilain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

HE 242/2018 vp. Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä poliisitoimessa sekä eräiksi siihen liittyviksi laeiksi.

HE 203/2017 vp. Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi.

HE 202/2017 vp. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.

HE 198/2017 vp. Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.

HE 41/2017 vp. Hallituksen esitys eduskunnalle laiksi rikostorjunnasta Rajavartiolaitoksessa ja eräiksi siihen liittyviksi laeiksi.

HE 286/2014 vp. Hallituksen esitys eduskunnalle ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen kuudennentoista pöytäkirjan hyväksymisestä ja laiksi pöytäkirjan lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

HE 174/2014 vp. Hallituksen esitys eduskunnalle laiksi rikostorjunnasta Tullissa ja eräiksi siihen liittyviksi laeiksi.

HE 65/2014 vp. Hallituksen esitys eduskunnalle laiksi todistajansuojeluohjelmasta ja eräiksi siihen liittyviksi laeiksi.

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

HE 19/2013 vp. Hallituksen esitys eduskunnalle laeiksi rikoslain, pakkokeinolain 10 luvun 7 §:n ja poliisilain 5 luvun 9 §:n muuttamisesta.

HE 16/2013 vp. Hallituksen esitys eduskunnalle laeiksi poliisilain sekä eräiden siihen liittyvien lakien muuttamisesta.

HE 14/2013 vp. Hallituksen esitys eduskunnalle laeiksi esitutkintalain ja pakkokeinolain muuttamisesta sekä eräiksi niihin liittyviksi laeiksi.

HE 282/2010 vp. Hallituksen esitys Eduskunnalle lasten suojelemista seksuaalista riistoa ja seksuaalista hyväksikäyttöä vastaan koskevan Euroopan neuvoston yleissopimuksen hyväksymiseksi ja siihen liittyviksi laeiksi.

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

HE 222/2010 vp. Hallituksen esitys Eduskunnalle esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi.

HE 48/2008 vp. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta.

HE 266/2004 vp. Hallituksen esitys eduskunnalle laiksi poliisilain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

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

HE 52/2002 vp. Hallituksen esitys eduskunnalle laeiksi esitutkintalain ja pakkokeinolain sekä eräiden näihin liittyvien lakien muuttamisesta.

HE 75/2000 vp. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi.

HE 34/1999 vp. Hallituksen esitys eduskunnalle laiksi poliisilain muuttamisesta.

HE 6/1997 vp. Hallituksen esitys Eduskunnalle oikeudenkäyttöä, viranomaisia ja yleistä järjestystä vastaan kohdistuvia rikoksia sekä seksuaalirikoksia koskevien säännösten uudistamiseksi.

HE 57/1994 vp. Hallituksen esitys poliisilaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 22/1994 vp. Hallituksen esitys Eduskunnalle telekuuntelua ja -valvontaa sekä teknistä tarkkailua koskevaksi lainsäädännöksi.

HE 309/1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

HE 94/1993 vp. Hallituksen esitys Eduskunnalle rikoslainsäädännön kokonaisuudistuksen toisen vaiheen käsittäviksi rikoslain ja eräiden muiden lakien muutoksiksi.

Keskusrikospoliisi: Keskusrikospoliisin lausunto esitutkinta- ja pakkokeinotoimikunnan mietinnöstä, 10.9.2009, 493/52/09.

LaVM 44/2010 vp. Lakivaliokunnan mietintö liittyen hallituksen esitykseen (HE 222/2010 vp) esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi.

LaVL 16/2017 vp. Lakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 41/2017 vp) eduskunnalle laiksi rikostorjunnasta Rajavartiolaitoksessa ja eräiksi siihen liittyviksi laeiksi.

LaVL 6/2005 vp. Lakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 266/2004 vp) laiksi poliisilain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

LaVL 7/2000 vp. Lakivaliokunnan lausunto liittyen hallitukseen esitykseen (HE 34/1999 vp) poliisilain muuttamiseksi.

Oikeusministeriö: Identiteettivarkaus. Lausuntotiivistelmä. Oikeusministeriön mietintöjä ja lausuntoja 47/2013.

PeVL 36/2017 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 41/2017 vp) eduskunnalle laiksi rikostorjunnasta Rajavartiolaitoksessa ja eräiksi siihen liittyviksi laeiksi.

PeVL 49/2014 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 174/2014 vp) eduskunnalle laiksi rikostorjunnasta Tullissa ja eräiksi siihen liittyviksi laeiksi.

PeVL 18/2014 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 221/2013 vp) eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

PeVL 33/2013 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 16/2013 vp) eduskunnalle laeiksi poliisilain sekä eräiden siihen liittyvien lakien muuttamisesta.

PeVL 6/2012 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 144/2011 vp) eduskunnalle laeiksi viestintämarkkinalain muuttamisesta ja väliaikaisesta muuttamisesta sekä sähköisen viestinnän tietosuojalain 10 ja 24 §:n muuttamisesta.

PeVL 67/2010 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 224/2010 vp) poliisilaiksi ja eräiksi siihen liittyviksi laeiksi.

PeVL 66/2010 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 222/2010 vp) esitutkinta- ja pakkokeinolainsäädännön uudistamiseksi.

PeVL 62/2010 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 204/2010 vp) turvallisuustutkintalaiksi, laiksi sotilasilmailuonnettomuuksien tutkinnasta ja laeiksi eräiden niihin liittyvien lakien muuttamisesta sekä ihmishengen turvallisuudesta merellä vuonna 1974 tehdyn kansainvälisen yleissopimuksen liitteen XI-1 lukuun tehdyn muutoksen hyväksymisestä ja laiksi muutoksen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

PeVL 56/2010 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 216/2010 vp) postilaiksi sekä Maailman postiliiton yleissopimuksen hyväksymiseksi ja laiksi sen lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

PeVL 18/2010 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 106/2009 vp) laiksi ampuma-aselain ja eräiden siihen liittyvien lakien muuttamisesta sekä kansainvälisen järjestäytyneen rikollisuuden vastaisten Yhdistyneiden Kansakuntien yleissopimuksen ampuma-aseiden, niiden osien ja komponenttien sekä ampumatarvikkeiden laittoman valmistuksen ja kaupan torjumista koskevan lisäpöytäkirjan hyväksymisestä ja laiksi lisäpöytäkirjan lainsäädännön alaan kuuluvien määräysten voimaansaattamisesta.

PeVL 5/2010 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 263/2009) valmisteverotuslaiksi ja laiksi Ahvenanmaan maakuntaa koskevista poikkeuksista arvonlisäveron- ja valmisteverolainsäädäntöön annetun lain 27 §:n muuttamisesta.

PeVL 34/2009 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 188/2009 vp) laeiksi eläintunnistusjärjestelmästä ja eläintautilain muuttamisesta.

PeVL 23/2006 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 31/2006 vp) laeiksi ulkomaalaislain ja ulkomaalaisrekisteristä annetun lain 8 §:n muuttamisesta.

PeVL 18/2006 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 34/2006 vp) laeiksi maatalouden harjoittamisesta luopumisen tukemisesta ja luopumisjärjestelmiä koskevien lakien muuttamisesta.

PeVL 11/2005 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 266/2004 vp) laiksi poliisilain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

PeVL 9/2004 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 125/2003 vp) sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi.

PeVL 13/2003 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 26/2003 vp) konkurssilainsäädännön uudistamiseksi.

PeVL 69/2002 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 157/2002 vp) laiksi maaseutuelinkeinojen rahoituslain muuttamisesta.

PeVL 51/2002 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 93/2002 vp) laiksi henkilötietojen käsittelystä poliisitoimessa ja eräiksi siihen liittyviksi laeiksi.

PeVL 40/2002 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 141/2002 vp) ajoneuvolaiksi ja siihen liittyviksi laeiksi.

PeVL 5/1999 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 3/1999 vp) laiksi poliisilain muuttamisesta.

PeVL 36/1998 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 239/1997 vp) yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi.

PeVL 31/1998 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esityksen (HE 76/1998 vp) pelastustoimilaiksi.

PeVL 17/1998 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 42/1998 vp) laiksi rajavartiolaitoksesta.

PeVL 12/1998 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 10/1998 vp) laeiksi rangaistusten täytäntöönpanosta annetun lain, tutkintavankeudesta annetun lain, pakkokeinolain ja kansanterveyslain muuttamisesta.

PeVL 23/1997 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 6/1997 vp) oikeudenkäyttöä, viranomaisia ja yleistä järjestystä vastaan kohdistuvia rikoksia sekä seksuaalirikoksia koskevien säännösten uudistamiseksi.

PeVL 2/1996 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 178/1995 vp) Eduskunnalle laeiksi tullilain ja valmisteluverotuslain 21 §:n muuttamisesta.

PeVL 8/1994 vp. Perustuslakivaliokunnan lausunto liittyen hallituksen esitykseen (HE 22/1994 vp) eduskunnalle telekuuntelua ja -valvontaa sekä teknistä tarkkailua koskevaksi lainsäädännöksi.

PeVM 4/2018 vp. Perustuslakivaliokunnan mietintö liittyen hallituksen esitykseen (HE 198/2017 vp) eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.

PeVM 25/1994 vp. Perustuslakivaliokunnan mietintö liittyen hallituksen esitykseen (HE 309/1993 vp) perustuslakien perusoikeussäännösten muuttamisesta.

Poliisihallitus:

- Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2018.
- Poliisin salaisen tiedonhankinnan järjestäminen, käyttö ja valvonta. POL-2018-11889. Voimassaoloaika 1.8.2018–31.7.2023. Julkaistu 13.07.2018. (Poliisihallitus 2018a)

- Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2017. Poliisihallitus 2018. (Poliisihallitus 2018c)
- Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2016. Poliisihallitus 2017. (Poliisihallitus 2017a)
- Poliisin toiminta sosiaalisessa mediassa ohje. POL-2017-8358. Voimassaoloaika 23.1.2017 – 22.10.2022. Julkaistu 23.10.2017. (Poliisihallitus 2017b)
- Poliisihallituksen kirje verkkoympäristössä tapahtuvaan tiedonhankintaan liittyen. Julkinen versio. POL-2017-11225. 16.6.2017. (Poliisihallitus 2017c)
- Selvitys haalarikameroiden käyttöönotosta poliisissa. Työryhmän loppuraportti 2/2017. Poliisihallituksen julkaisusarja. (Poliisihallitus 2017d)
- Vihapuheiden ja -rikosten torjuntaan liittyvän toimintasuunnitelman valmistelua koskevan työryhmän loppuraportti 14.11.2016. (Poliisihallitus 2016a)
- Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2015. Poliisihallitus 2016. (Poliisihallitus 2016b)
- Tietojen käsittely epäiltyjen tietojärjestelmässä. POL-2016-3510. 30.3.2016. (Poliisihallitus 2016c)
- Poliisihallituksen kertomus sisäministeriölle poliisin salaisesta tiedonhankinnasta ja sen valvonnasta vuonna 2014. Poliisihallitus 20.5.2015.
- Poliisihallituksen selvitys sisäasiainministeriölle poliisin tiedonhankinnasta ja valvonnasta vuonna 2012. Poliisihallitus 1.3.2013.
- Poliisin näkyvä toiminta sosiaalisessa mediassa. Työryhmän loppuraportti 21.5.2012. Poliisihallituksen julkaisusarja 2/2012.
- Poliisihallituksen selvitys sisäasiainministeriölle poliisin tiedonhankinnasta ja valvonnasta vuonna 2010. Poliisihallitus 7.3.2010.

Sisäministeriö:

- Kansallinen riskiarvio 2018. Sisäministeriön julkaisuja 2019:5. Helsinki 2019.
- Tietoverkkorikollisuuden torjuntaa koskeva selvitys. Sisäministeriön julkaisu 14/2017. Helsinki 2017.
- Henkilöllisyyden luomista koskeva hanke (identiteettiohjelma). Työryhmän loppuraportti. Sisäasiainministeriön julkaisuja 32/2010.

- Esitutkinta, pakkokeinolain ja poliisilain kokonaisuudistus. Esitutkinta- ja pakkokeinotoimikunnan mietintö. Komiteamietintö 2009:2. Helsinki 2009. (Sisäministeriö 2009a)
- Esitutkinta- ja pakkokeinotoimikunnan mietintö KM 2009:2. Tiivistelmä lausunnoista. Sisäasiainministeriö julkaisuja 34/2009. (Sisäministeriö 2009b)

**INTERNET-LÄHTEET**

American City & County: Huntington Beach police use social media to keep the peace. Julkaistu 31.8.2015. [https://www.americancityandcounty.com/2015/08/31/huntington-beach-police-use-social-media-to-keep-the-peace/] (17.2.2019)

BuzzFeed: How To Spot A Deepfake Like The Barack Obama–Jordan Peele Video. Julkaistu 17.4.2018. [https://www.buzzfeed.com/craigsilverman/obama-jordan-peele-deepfake-video-debunk-buzzfeed?utm_source=dynamic&utm_campaign=bfshareemail&utm_term=.xyEB6pDKRR] (6.11.2018)

Campus Safety: Social Media Monitoring: Beneficial or Big Brother? Julkaistu 12.3.2018. [https://www.campussafetymagazine.com/university/social-media-monitoring/] (26.2.2019)

ESS: Poliisi kertoo tarinan, kuinka neuvokas nuori tyttö sai varastetun pyöränsä takaisin. Julkaistu 26.11.2016. (6.4.2019)

Europol:

- xDedic Marketplace Shut Down in International Operation. Press release 28.1.2019. [https://www.europol.europa.eu/newsroom/news/xdedic-marketplace-shut-down-in-international-operation] (10.3.2019)
- More than 200 children identified and rescued in worldwide police operation. Press release 16.3.2011. [https://www.europol.europa.eu/newsroom/news/more-200-children-identified-and-rescued-in-worldwide-police-operation] (3.3.2019)

Facebook:

- Ryhmät. [https://www.facebook.com/help/1629740080681586/?helpref=hc_fnav] (18.2.2019) (Facebook 2019a)
- Mistä ihmiset, jotka saatat tuntea -ehdotukset tulevat? [https://www.facebook.com/help/163810437015615?helpref=faq_content] (18.2.2019) (Facebook 2019b)

FamilyTreeDNA: Press release: Connectin Families and Saving Lives. Julkaistu 1.2.2019. [https://blog.familytreedna.com/press-release-connecting-families-and-saving-lives/] (10.2.2019)

Helsingin poliisilaitos: Kaksi henkilöä on vangittu kuluvalla viikolla ryöstörikoksista epäiltyinä Helsingissä – molemmat tapaukset liittyvät netin huumekauppaan. Tiedote 3.4.2019. [https://www.poliisi.fi/tietoa_poliisista/tiedotteet/1/1/kaksi_henkiloa_on_vangittu_kuluvalla_viikolla_ryostorikoksista_epailtyina_helsingissa_molemmat_tapaukset_liittyvat_netin_huumekauppaan_79489] (6.4.2019)

Helsingin Sanomat (HS):

- Suljetun Sihteeriopisto-sivuston ylläpitäjä on ollut mysteeri: taustalla suomalainen bordelli-motelleja pyörittänyt liikemies. Julkaistu 27.3.2019. (6.4.2019) (HS 2019a)
- Yhdysvalloissa rakennettiin tekoälyllä toimiva tekstigeneraattori, joka voi olla liian vaarallinen julkaistavaksi, ohjelman kehittäjät sanovat. Julkaistu 14.2.2019. [https://www.hs.fi/ulkomaat/art-2000006001926.html] (17.2.2019) (HS 2019b)

Iltalehti:

- Onko sinulla tämä laite? Google neuvoo vaihtamaan salasanan – taustalla vakoilua ja kiusaamista. Julkaistu 12.2.2019 [https://www.is.fi/digitoday/art-2000005997614.html?cs] (12.2.2019)
- Huumeita hankitaan nyt härskin uutuusjuonen varjolla – tarkkaile kutsumattomia vieraita postilaatikollasi. Julkaistu 11.11.2018. [https://www.iltalehti.fi/kotimaa/a/ce7775e3-a0e8-4f16-9cb2-ef703a2a2683] (6.4.2019)
- Kuvaa jopa suomalaisesta makuuhuoneesta - tuhannet suojaamattomat valvontakamerat netissä. Julkaistu 5.6.2017. [https://www.iltalehti.fi/digi/201706052200186842_du.shtml] (3.11.2018)

Keskusrikospoliisi:

- KRP on saanut valmiiksi laajan seksuaalirikoskokonaisuuden - epäilyn mukaan Suomessa tuotettu väkivaltaista lasten hyväksikäyttömateriaalia. Tiedote julkaistu 27.3.2019.
- Huumausainerikosten määrä jatkaa kasvuaan – nettikaupasta tullut tärkeä välityskanava. Tiedote 27.4.2018. POL-2018-10127. [https://www.poliisi.fi/instancedata/prime_product_julkaisu/intermin/embeds/

poliisiwwwstructure/69911_Tilannekatsaus_huumaus-_ja_dopingainerikollisuudesta.pdf] (8.4.2019)

NBS News: Undercover cops break Facebook rules to track protesters, ensnare criminals. Julkaistu 5.10.2018. [https://www.nbcnews.com/news/us-news/undercover-cops-break-facebook-rules-track-protesters-ensnare-criminals-n916796] (21.2.2019)

Poliisihallitus: Poliisi panostaa rikosten ehkäisemiseen ja paljastamiseen. Tiedote 19.12.2018. [https://www.poliisi.fi/poliisihallitus/tiedotteet/1/0/poliisi_panostaa_rikosten_ehkaisemiseen_ja_paljastamiseen_76737] (10.3.2019) (Poliisihallitus 2018b)

Sisäministeriö: Lisätalousarviossa rahaa nettipoliiseille, turvapaikkahakemusten käsittelyyn ja Oulun säilöönottoyksikön perustamiseen. Tiedote 13/2019. Julkaistu 22.2.2019.

Terre des Hommes: Webcam Child Sex Tourism. Becoming Sweetie: a novel approach to stopping the global rise of Webcam Child Sex Tourism. 4.11.2013. [https://www.terre-deshommes.nl/en/publications/webcam-child-sex-tourism]. Katsottu 17.2.2019.

The New York Times: As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. Julkaistu 18.12.2018. [https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html] (18.2.2019)

The Press: Gunman Thomas Thislethwaite threatened to shoot policeman in siege. Julkaistu 26.2.2019. [https://www.yorkpress.co.uk/news/17457716.gunman-thomas-thistlethwaite-threatened-to-shoot-policeman-in-siege/] (27.2.2019)

Yle:

- Onko lapsesi kuulunut tähän Whatsapp-ryhmään? Poliisi paljasti satojen lasten suosiman ryhmän, jossa on jaettu raakoja ja rivoja kuvia. Julkaistu 21.2.2019. [https://yle.fi/uutiset/3-10657015] (21.2.2019)
- Facebookin ohjelmistovirhe muutti miljoonien käyttäjien yksityisyysasetuksia. Julkaistu 8.6.2018. [https://yle.fi/uutiset/3-10244006] (14.1.2019)

**OIKEUSTAPAUKSET**

**Euroopan ihmisoikeustuomioistuin**

*Big Brother Watch and Others v. Yhdistynyt kuningaskunta*, 58170/13, 62322/14 ja 24960/15, 13.9.2018.

*Allan v. Yhdistynyt kuningaskunta*, 25424/09, 12.7.2013.

*Michaud v. Ranska*, 12323/11, 6.12.2012.

*Bannikova v. Venäjä*, 18757/06, 4.11.2010.

*Uzun v. Saksa*, 35623/05, 2.9.2010.

*Sequeira v. Portugali*, 18545/06, 20.10.2009.

*S. ja Marper v. Yhdistynyt kuningaskunta*, 30562/04 ja 30566/04, 4.12.2008.

*Ramanauskas v. Liettua*, 74420/01, 5.2.2008.

*Copland v. Yhdistynyt kuningaskunta*, 62617/00, 3.4.2007.

*van Vondel v. Alankomaat*, 38258/03, 25.10.2007.

*Weber ja Saravia v. Saksa*, 54934/00, 29.6.2006.

*Vanyan v. Venäjä*, 53203/99, 15.12.2005.

*Shannon v. Yhdistynyt kuningaskunta*, 6563/03, 4.10.2005.

*Rajcoomar v. Yhdistynyt kuningaskunta*, 59457/00, 14.12.2004.

*M.M v. Alankomaat*, 39339/98, 24.9.2003.

*Perry v. Yhdistynyt kuningaskunta*, 63737/00, 17.7.2003.

*Teixeira de Castro c. Portugali*, 25829/94, 9.6.1998.

*Halford v. Yhdistynyt kuningaskunta, 20605/92,* 25.6.1997.

*Klass ym. v. Saksa*, 5029/71, 6.9.1978.

**Euroopan unionin tuomioistuin**

Asia C 582/14, *Patrick Breyer v Saksan liittotasavalta* (2016) EUVCL:C:475.

Asia C-131/12, *Google Spain SL ja Google Inc. v. Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* (2014) EUVL:C:212.

Yhdistetty ratkaisu C-293/*12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Irlanti ja Attorney General ja* C-594/12 *Kärtner Landesregierung, Michael Seitlinger ja Christof Tschohl ym* (2013) EU:C:2013:845.

Ennakkoratkaisupyyntö C-623/17 *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs ym* (2017) EUVL:C:22.

**Korkein oikeus**

KKO 2018:77

KKO 2016:92

KKO 2012:54

KKO 2011:11

KKO 2009:54

KKO 1981-II-182

**Korkein hallinto-oikeus**

KHO 2018:112

**Hovioikeudet**

Helsingin HO 14.11.1996 R 96/1503

Helsingin HO 8.2.2000 R 98/1662

Turun HO 25.10.2018 R 17/1974

**Käräjäoikeudet**

Helsingin KO 22.3.2019 R 19/1572

Helsingin KO 1.8.1995 R 95/2808

Itä-Uudenmaan KO 11.2.2019 R 18/3115/766

Länsi-Uudenmaan KO 26.09.2013 R 13/1208

**Eduskunnan oikeusasiamiehen päätökset**

AOA 2.7.2015 Dnro 87/4/15

AOA 29.11.2013 Dnrot 1870/4/13, 2061/4/13, 2186/4/13, 2187/4/13 ja 2189/4/13

AOA 29.11.2010 Dnro 686/4/09

AOA 7.9.2010 Dnro 571/2/08

EOA 14.11.1989 Dnro 1255/4/87

**MUUT LÄHTEET**

Esitutkintapöytäkirja 2400/R/239/18 11.2.2019.

KK 468/2017 vp. Kirjallinen kysymys yhdenvertaisuusvaltuutetun harjoittamasta vaaliehdokkaiden kirjoitusten tarkkailusta.

KK 262/2016 vp. Kirjallinen kysymys mobiilitunnistautumisesta viranomaispalveluihin prepaid-liittymällä.

KK 353/2012 vp. Kirjallinen kysymys Prepaid-liittymien väärinkäytösten kitkemisestä.

KK 557/2007 vp. Kirjallinen kysymys Prepaid-korttirekisterin perustamiseksi.

KK 172/2007 vp. Kirjallinen kysymys Prepaid-liittymien rekisteröinnistä.

KK 33/2007 vp. Kirjallinen kysymys Prepaid-liittymän ottajan pakollisesta rekisteröitymisestä.

KKV 468/2017 vp. Vastaus kirjalliseen kysymykseen yhdenvertaisuusvaltuutetun harjoittamasta vaaliehdokkaiden kirjoitusten tarkkailusta.

## LYHENNELUETTELO

| | |
|---|---|
| AOA | Eduskunnan apulaisoikeusasiamies |
| EIS | Euroopan ihmisoikeussopimus |
| EIT | Euroopan ihmisoikeustuomioistuin |
| EOA | Eduskunnan oikeusasiamies |
| EPSA | Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta (122/2014) |
| ESPA | estävän ja paljastavan toiminnan tietoryhmä |
| ETL | esitutkintalaki (805/2011) |
| EU | Euroopan unioni |
| EUT | Euroopan unionin tuomioistuin |
| EUVL | Euroopan unionin virallinen lehti |
| HaVL | hallintovaliokunnan lausunto |
| HaVM | hallintovaliokunnan mietintö |
| HE | hallituksen esitys |
| IMEI | International Mobile Equipment Identity |
| IP | Internet Protocol |
| JIT | Joint Investigation Team |
| KK | kirjallinen kysymys |
| KHO | korkein hallinto-oikeus |
| KKO | korkein oikeus |
| KO | käräjäoikeus |
| LaVL | lakivaliokunnan lausunto |
| LaVM | lakivaliokunnan mietintö |
| LSVP | laki sähköisen viestinnän palveluista (917/2014) |
| OK | oikeudenkäymiskaari (4/1734) |
| OSINT | Open Source Intelligence |
| PKL | pakkokeinolaki (806/2011) |
| PL | perustuslaki (731/1999) |
| PolL | poliisilaki (872/2011) |

| | |
|---|---|
| PolHalL | laki poliisin hallinnosta (110/1992) |
| PeVL | perustuslakivaliokunnan lausunto |
| PeVM | perustuslakivaliokunnan mietintö |
| POTI | poliisin tiedustelujärjestelmä |
| POV | pidättämiseen oikeutettu virkamies |
| RL | rikoslaki (39/1889) |
| RSS | Really Simple Syndication |
| Salpa | salaisten pakkokeinojen asiankäsittelyjärjestelmä |
| STEKPOV | salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu virkamies |
| SVL | laki sananvapauden käyttämisestä joukkoviestinnässä (460/2003) |
| YK | Yhdistyneet kansakunnat |

# KUVIOT JA TAULUKOT

Kuvio 1. Salaisten tiedonhankinta- ja pakkokeinojen ryhmittely, jossa tummennettuina poliisi- ja peiteprofiileilla mahdolliset keinot.

Kuvio 2. Tietoverkkojen luottamukselliseen viestintään liittyvät suojaamistarpeen tasot.

Kuvio 3. Yksityiselämän suojan jaottelua reaalimaailman ja tietoverkkojen välillä.

Kuvio 4. Salaisten tiedonhankinta- ja pakkokeinojen yleisten edellytysten kolmiportainen järjestelmä poliisi- ja peiteprofiilien osalta.

Kuvio 5. Salaisten tiedonhankinta- ja pakkokeinojen suojaamiskeinot.

# 1 JOHDANTO

## 1.1 Salaisten tiedonhankinta- ja pakkokeinojen toimivaltuussääntelykehityksestä erityisesti tietoverkkojen näkökulmasta

Tietoverkkojen käyttö vaikuttaa jo miltei jokaisen suomalaisen arkeen hyvässä ja pahassa. Internet ja erityisesti sosiaalinen media on yhtäältä paikka hakea tietoa, tehdä kauppaa, verkostoitua ja ilmaista itseään, mutta myös ympäristö, jossa syyllistytään yhä enemmän rikoksiin ja erilaiseen negatiiviseksi ilmiöksi tulkittavaan vaikuttamiseen.[1] Erityisesti sosiaalisen median palvelujen yleistymisen myötä tietoverkoista on tullut yhä tärkeämpi foorumi sekä ennalta estävän poliisitoiminnan että rikosten paljastamiseen ja selvittämiseen liittyvän tiedonhankinnan näkökulmasta.[2] Tekninen kehitys on mahdollistanut vaihtoehtoisia viestintätapoja, jonka takia perinteiset tiedonhankintamenetelmät eivät enää välttämättä toimi.[3] Salaisia tiedonhankinta- ja pakkokeinoja koskeva toimivaltuussääntely onkin kohdannut haasteita pysyä teknisen kehityksen perässä rikoslain sääntelyn tapaan, vaikka ongelma on tunnistettu lainvalmistelussa jo vuosia.[4]

Poliisin toimivaltuussääntelyn perustui vielä 1960-luvulla yleisvaltuusajatteluun, mutta vuoden 1966 poliisilaki (84/66) antoi jo suuntaa säännösperustaiseen toimivaltuussääntelyyn.[5] Sittemmin ajattelumallista ”kaikki mikä ei ole kiellettyä, on poliisille sallittua” on siirrytty PL 2.3 §:n mukaiseen viranomaistoimintaan, jossa julkisen vallan tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia.[6]

---

[1] Sosiaaliseen mediaan liittyvästä yleisimmästä rikollisuudesta ks. kokonaisuudessaan Forss 2014 ja erityisesti erilaisista rikosnimikkeistä s. 187–288. Ks. myös Forss – Keinänen 2017, s. 5–6, jossa tilastotietoa eri sosiaalisen median palvelujen esiintymisyleisyydestä poliisin tietojärjestelmiin kirjatuissa ilmoituksissa. Ks. digitaalisen yhteiskunnan kehityksestä ja haasteista yleisesti esimerkiksi tekoälyn, esineiden internetin ja massadatan hyödyntämisen osalta Sisäministeriö 2019, s. 17–18. Negatiiviseksi koettuun tai laittomaan vaikuttamiseen liittyen ks. Suojelupoliisi 2019, s. 16, jossa todetaan tietoverkkojen olevan alusta kyberhyökkäyksille, valeuutisille ja tietovuotoihin, joilla pyritään vaikuttamaan kohdevaltion yhteiskunnalliseen ilmapiiriin ja päätöksentekoon.

[2] Poliisihallitus 2018c, s. 40.

[3] Ks. esimerkiksi Poliisihallitus 2018c, s. 2, jonka mukaan telekuuntelujen määrä oli vuonna 2017 jo 300 pienempi kuin huippuvuonna 2013. Tämän katsottiin ainakin osittain johtuvan siitä, että viestintä oli yhä enenevissä määrin siirtynyt vaihtoehtoisiin viestintätapoihin.

[4] Ks. teknisen kehityksen haasteiden ottamisesta huomioon salaisia tiedonhankinta- ja pakkokeinoja koskien HE 22/1994 vp, s. 12; HE 57/1994 vp, s. 4; HE 266/2004 vp, s. 4; HE 224/2010 vp, s. 31; HE 222/2010 vp, s. 12–13. Ks. myös lainvalmistelun heikkouksista tietoverkkoihin liittyen kokonaisuudessaan Forss – Keinänen 2017.

[5] Ks. yleistoimivallan käsitteestä Ylösjoki 1965, s. 34–52; Ylösjoki 1966, s. 33–45.

[6] Ks. lakisidonnaisuuteen siirtymisen historiasta tarkemmin Terenius 2013, s. 163–171.

Tämän takia tavanomaisoikeudellisen, eli maan tapaan, perustuvan toimivallan käyttöala on nykyään erittäin kapea. Yleisvaltuusajattelusta 1970-luvulla irrottautunut *Sinisalo* katsoi tosin jo silloisen vuoden 1966 poliisilain normien jättävän vain poikkeuksellisesti tilaa tavanomaiselle oikeudelle, vaikka käytännössä ero nykypäivän sääntelyn määrään ja tarkkuuteen oli vielä huomattava.[7] Käytännössä salaisia tiedonhankintakeinoja on käytetty niin kauan eri muodoissaan kuin poliisitoimintaa on ollut olemassa, mutta vuosien myötä yhä useampi keino on tullut sääntelyn piiriin.[8] Esimerkkinä voidaan mainita nykyistä peitetoimintaa vastaava piilopoliisitoiminta ja valeostot, joita suoritettiin jo ennen varsinaista sääntelyä. Sama koskee myös tiedustelu- ja tarkkailutoimintaa yleisesti.[9] *Hankilanoja* toteaakin, että vaikka poliisin lisääntyvää toimivaltuuksien määrää on kritisoitu, käytännössä yleisvaltuusajoista lisääntynyt sääntely on pikemminkin rajoittanut entistä enemmän poliisin mahdollisuuksia toimia salaisen tiedonhankinnan alueella kuin lisännyt niitä.[10]

Salaisten tiedonhankinta- ja pakkokeinojen osalta poliisin toiminta tietoverkoissa on huomioitu lainsäädännössä vasta viime vuosina, koska yleensäkin salaisiin toimivaltuuksiin liittyvää sääntelyä alkoi ilmestyä vasta 1990-luvulla.[11] Poliisi- ja pakkokeinolakiin salaiseen tiedonhankintaan liittyviä säännöksiä saatiin vasta vuoden 1995 kokonaisuudistuksessa, jolloin tietoverkkojen rooli oli ihmisten arjessa vielä suhteellisen vähäinen.[12] Vuosien varrella aikaisemmin voimassa olleita poliisilakia (493/1995) ja pakkokeinolakia (450/1987) täydennettiin useilla osauudistuksilla, joilla pyrittiin parantamaan rikostorjunnan tehokkuutta.[13] Osauudistukset johtivat kuitenkin siihen, että poliisi- ja pakkokeinolaista tuli

---

[7] Poliisin toimivallasta Sinisalo 1971, s. 223–227 ja tavanomaisen oikeuden ulottuvuudesta Sinisalo 1973, s. 41–42. Ks. Hankilanoja 2014, s. 238, jonka mukaan salaisia tiedonhankinta- ja pakkokeinoja koskevien säännösten määrä vuosina 1992–2013 kasvoi yli 60-kertaiseksi ja valtaosaan (88%:iin) alkuperäisistä säännöksistä on tullut muutoksia. Näiden säännösten määrä kolminkertaistui vuosina 1995–2013 ja vuoden 2014 alussa säännösmäärä edelleen kolminkertaistui aiempaan verrattuna.

[8] Hankilanoja 2014, s. 69.

[9] Ks. esimerkiksi valeostoon rinnastettavasta ansoituksesta KKO 2000:112 ja peitetoiminnasta sekä valeostosta HE 34/1999 vp, s. 12. Ks. myös Salminen 1995, s. 21–23; Piispanen 1998, s. 183 ja 192. Tiedustelusta ja tarkkailusta HE 57/1994 vp, s. 16.

[10] Hankilanoja 2014, s. 239.

[11] Hankilanojan mukaan ensimmäinen salaista tiedonhankintaa koskeva säännös oli vuonna 1992 silloiseen teletoimintalakiin (676/1992) säädetty oikeus saada teleyritykseltä puheluliikenteen tunnistetietoja rikoksen selvittämiseksi. Ks. Hankilanoja 2014, s. 70–71. Vrt. kuitenkin Määttä 2002, s. 35, jossa hän viittaa jo aikaisempaan vuonna 1987 säädettyyn teletoimintalakiin (183/1987). Kyseisen lain 29 §:n 2 momentissa säädettiin poliisin oikeudesta saada silloisen RL 24:3 a §:ssä mainitun rikoksen selvittämiseksi tarpeellisia tunnistamistietoja.

[12] Tuolloin poliisilakiin otettiin säännökset tarkkailusta ja teknisestä tarkkailusta. Pakkokeinolakiin lisättiin uusi 5a luku, jossa säädettiin telekuuntelusta, televalvonnasta ja teknisestä tarkkailusta.

[13] Ks. esimerkiksi HE 266/2004 vp, s. 4, jossa todetaan, että se että järjestäytyneen rikollisuuden jäsenet olivat ottaneet käyttöön tiedonvaihdon internetin avustuksella ja siten heikentäneet telekuuntelun käyttömahdollisuuksia. Tämän takia poliisin tuli tiedonhankinnassa ja vakavan rikollisuuden torjunnassa ottaa käyttöön entistä tehokkaampia toimintamuotoja.

epäyhtenäinen ja sekava kokonaisuus.[14] Tätä tilannetta pyrittiin korjaamaan poliisi-, pakkokeino- ja esitutkintalakien kokonaisuudistuksessa, joka astui voimaan vuonna 2014.[15] Kokonaisuudistus onnistuikin selkeyttämään sääntelyn rakennetta ja erityisesti poliisi- ja pakkokeinolakien tarpeettomia sääntelyeroja.

Vaikka sosiaalinen media oli mullistanut ihmisten tietoverkoissa toimimisen jo ennen tätä, ja vaikka esimerkiksi nettipoliisitoiminta alkoi jo vuonna 2008, jäi tietoverkkojen rooli kokonaisuudistuksessa taka-alalle. Vuoden 2014 poliisilaissa (872/2011, PolL) ja pakkokeinolaissa (806/2011, PKL) sääntely ja esityöt perustuivat edelleen hyvin pitkälti reaalimaailman problematiikkaan.[16] Tietoverkot otettiin huomioon lähinnä sivulauseissa tai jätettiin kokonaan huomioimatta, vaikka samaa toimivaltuussäännöstä oli tarkoitus käyttää molemmissa ympäristöissä. Tietyllä tapaa ironisena esimerkkinä tietoverkkojen suppeasta ja tarkemman sekä täsmällisemmän käsittelyn sivuuttavasta tavasta voidaan mainita hallituksen esityksistä 224/2010 vp ja 222/2010 vp löytyvä tarkkailua koskeva lause: ”Selvyyden vuoksi on mainittava, että tarkkailu on mahdollista myös tietoverkossa.”.[17] Käytännössä esityöt eivät tuoneet juurikaan ”selvyyttä”, saati että niissä olisi arvioitu laajemmin tietoverkkojen ja reaalimaailman eroja.[18] Hankilanoja on todennut, että ristiriidat kokonaisuudistuksen lainvalmistelussa johtivat siihen, että ongelmat joihin ei löytynyt ratkaisuja, jäivät suorittavan portaan käytännön varaan.[19] Tämä onkin luultavasti johtanut osaltaan siihen, että vuoden 2014 uudistuksessa tietoverkkoja koskeva toimivaltuussääntely on merkittäviltä osin sivuutettu ja tilanne on lain toimeenpanijoiden kannalta epätyydyttävä.[20] Salaisten

[14] Ks. poliisin toimivaltuuskehityksestä laajemmin Hankilanoja 2014, s. 109–121.

[15] Vuoden 2014 kokonaisuudistusta edeltävästä poliisi- ja pakkokeinolain kehityksestä salaiseen tiedonhankintaan liittyen ks. Hankilanoja 2014, s. 69–75. Viimeisimpänä voidaan mainita tietoliikennetiedusteluun liittyvät uudistukset. Ks. siihen liittyen siviilitiedusteluun liittyen hallituksen esitys 202/2017 vp ja sotilastiedusteluun liittyen 203/2017 vp. Ks. myös tiedustelulainsäädännön takia muutettuun perustuslain 10 §:ään liittyen HE 198/2017 vp. Ks. myös yleisesti teknologiakehityksen vaikutuksesta poliisin eri valvontamuotoihin Heinonen – Hannula 1999, s. 82–95.

[16] Ks. Sisäministeriö 2009a, jossa tietoverkkojen rooli oli huomioitu vuoden 2014 kokonaisuudistusta koskevassa mietintövaiheessa. Huomiointi jäi tosin suhteellisen vaatimattomaksi niin kuin koko vuoden 2014 uudistuksessakin, vaikka vuosia kestäneen valmistelun aikana asiaan olisi ehtinyt kiinnittämään halutessaan huomiota. Ks. myös Poliisihallituksen Salpa-määräykseen liittyen Poliisihallitus 2013, s. 43, jossa tietoverkkojen osuus on huomioitu ensimmäisen kerran.

[17] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.

[18] Lause oli samassa muodossa esillä jo komiteamietintövaiheessa vuotta aiemmin. Ks. Sisäministeriö 2009a, s. 462.

[19] Tämä tosin koski myös reaalimaailmaan liittyvää problematiikkaa. Ks. tähän liittyen AOA Dnro 571/02/08, jossa oli kyse valeostoon liittyvistä tulkintaongelmista jo ennen 2014 muutoksia. AOA otti kantaa valeostoa koskevan lainsäädännön niukkuuteen ja tulkinnanvaraisuuteen. AOA kritisoi silloisen lainsäädännön oikeussuojatakeita ja totesi toimintakentän olevan monin tavoin vaativa, jossa rajanvedot oli jätetty suorittavan tason vastuulle. Näyttää siltä, että sama tilanne vallitsee tietoverkkojen osalta tällä hetkellä useiden toimivaltuussäännösten kohdalla.

[20] Hankilanoja 2014, s. 105–106. Hankilanoja kiinnittää huomiota myös siihen, että lainvalmistelussa ei ollut lakitoimikunnassa mukana varsinaisena jäsenenä yhtään esitutkintaviranomaisen operatiivisen toiminnan

tiedonhankinta- ja pakkokeinojen monimuotoisuuden ja käytön hankaluuden takia niiden käyttöä on jopa vältelty.[21] Kritiikkiin on helppo yhtyä, vaikka toisaalta positiivisena esimerkkinä voidaan mainita peitetoiminnan tietoverkkoja koskeva sääntely, jonka osalta reaalimaailman ja tietoverkkojen erilaisuus tunnistettiin ja sillä oli selkeä vaikutus toimivaltuuden käytön erityisiin edellytyksiin.[22] Vaikka näitä tulkintahaasteita oli havaittu tietoverkkojen osalta jo ennen kuin vuoden 2014 uudistus ehti tulla edes voimaan, ei niihin ole jostain syystä kiinnitetty huomiota uudemmissa Tullia ja Rajavartiolaitosta koskevissakaan salaisten tiedonhankinta- ja pakkokeinojen lainvalmisteluissa. Näitä koskevat esityöt ovat hyvin pitkälti poliisi- ja pakkokeinolain toisintamista.[23] Lainvalmistelun heikkoudet tietoverkkojen huomioimisessa muodostavatkin erityisen haasteen tämän tutkimuksen toteuttamiselle.

### 1.2 Salaisten tiedonhankinta- ja pakkokeinojen jaottelu sekä rikoksen estäminen, paljastaminen ja selvittäminen

Salaisista tiedonhankintakeinoista säädetään poliisilain 5 luvussa ja salaisista pakkokeinoista pakkokeinolain 10 luvussa.[24] Lisäksi salaisia tiedonhankinta- ja pakkokeinoja koskee Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta (122/2014, EPSA) 3 luku. Tässä tutkimuksessa salaiset tiedonhankinta- ja pakkokeinot jaotellaan seuraavasti: 1) teletoimivaltuudet, 2) tarkkailutoimivaltuudet ja 3) erityiset toimivaltuudet.[25]

---

lainsoveltajaa. Sama koski lakitoimikunnan kuulemia henkilöitä. Ks. myös vuoden 2014 uudistukseen liittyvä keskusrikospoliisin lausunto esitutkinta- ja pakkokeinotoimikunnan mietinnöstä KRP 2009, s. 1–18, jossa tietoverkkoihin liittyvää problematiikkaa käsitellään kattavasti. Lainvalmisteluaineistossa se on otettu kuitenkin vain osittain huomioon.

[21] Ks. tarkemmin Kurenmaa 2018, s. 35.

[22] Peitetoiminnan erityisiä edellytyksiä koskevaa rangaistusmaksimirajaa laskettiin reaalimaailmasta poiketen. Ks. perusteluista tarkemmin HE 224/2010 vp, s. 45–46; HE 222/2010 vp, s. 129.

[23] Ks. Tullin salaisiin tiedonhankinta- ja pakkokeinoihin liittyen HE 174/2014 ja Rajavartiolaitoksen osalta HE 41/2017 vp. Lainvalmistelun laatuun liittyvistä ongelmista voidaan mainita esimerkkinä myös Rajavartiolaitoksen lainsäädännöstä unohdettu tietolähdetoimintaa koskeva säännös. Ks. LaVL 16/2017 vp, s. 6–7, jossa lakivaliokunta piti valitettavana, että tietolähdetoimintaa koskevan sääntelyn tarve tuotiin esille vasta esityksen eduskuntakäsittelyssä. Perustellumpaa olisi lakivaliokunnan mielestä ollut todeta sääntelyn tarve hallituksen esityksen perusteluissa ja asianmukaiseen valmistelutyöhön nojautuen. Käytännössä kyseinen säännös oli unohtunut lainvalmistelussa.

[24] Määritelmäluettelot ovat poliisi- ja pakkokeinolain osalta miltei identtiset (PolL 5:1.1 ja PKL 10:1.1).

[25] Jaottelu on tehty oikeuskirjallisuudessa yleensä hieman eri termein. Ks. Helminen ym. 2014, s. 1105; Helminen – Kuusimäki - Rantaeskola 2012, s. 272. Ensimmäisestä kohdasta käytetään yleensä termiä ”telepakkokeinot”, mutta koska tässä tutkimuksessa jaottelu sisältää myös poliisilain mukaiset salaiset tiedonhankintakeinot, ei kyseinen termi kata mielestäni poliisilain mukaisia toimivaltuuksia. Sama koskee myös erityisiä salaisia pakkokeinoja, jotka määritellään tässä tutkimuksessa erityisiksi toimivaltuuksiksi.

- *Teletoimivaltuuksia* ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella, sijaintitietojen hankkiminen epäillyn ja tuomitun tavoittamiseksi, tukiasematietojen hankkiminen ja tietoliikennetiedustelu[26]
- *Tarkkailutoimivaltuuksia* ovat suunnitelmallinen tarkkailu, tekninen tarkkailu eri muodoissaan sekä teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkiminen
- *Erityisiä toimivaltuuksia* ovat peitelty tiedonhankinta, peitetoiminta, valeosto, tietolähteen ohjattu käyttö ja valvottu läpilasku[27]

Toimivaltuuksien käyttömahdollisuudet eroavat sen mukaan, onko rikos jo tapahtunut ja millainen varmuus poliisilla on mahdollisen rikoksen tapahtumisesta. Tämän perusteella poliisi- ja pakkokeinolain mukaiset toimenpiteet jaetaan 1) rikoksen estämiseen, 2) paljastamiseen ja 3) selvittämiseen.[28]

> Tietoliikennetiedustelua koskevalla lakimuutoksella aineellista ja alueellista soveltamisalaa ollaan laajentamassa tiedusteluperusteiseksi.[29] Siten rikostorjuntatoimivaltuuksien käytön lisäksi mahdollistetaan tiedustelutoimivaltuudet, joilla on mahdollista hankkia tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. [30] Tämän takia myös perustuslakia muutettiin luottamukselliseen viestintään liittyen.[31] Lisäksi esitutkintalain (805/2011, ETL) 2 luvun 1 §:stä tullaan muuttaman siten, että suojelupoliisi ei ole enää esitutkintaviranomainen.

*Rikoksen estämisellä* tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa

[26] Aikaisemmin mainitussa oikeuskirjallisuudessa ei ole otettu huomioon vielä tietoliikennetiedustelua, mutta sen voidaan katsoa kuuluvan teletoimivaltuuksien piiriin.
[27] Peitelty tiedonhankinta on jostain syystä sijoitettu lainsäädännössä tarkkailutyyppisiin keinoihin. Tässä tutkimuksessa sitä pidetään kuitenkin erityisenä toimivaltuutena, koska toiminta perustuu vuorovaikutukseen, joka ei ole ominaista tarkkailutyyppisille keinoille. Lisäksi kyseessä on tietynlainen peitetoiminnan lievempi muoto, joten jaottelussa se sopii selvästi paremmin erityisiin toimivaltuuksiin. Ks. suhteesta peitetoimintaan HE 224/2010 vp, s. 36–37 ja 103–104; HE 222/2010 vp, s. 119 ja 327. Kyseinen jaottelu on myös tutkimuksen kannalta järkevämpi, koska tarkkailutyyppisistä keinoista puhuttaessa ei viitata vuorovaikutuksen sisältäviin tilanteisiin.
[28] Tietoliikennetiedustelun osalta voidaan puhua tiedustelusta, mutta asiaa ei käsitellä tässä tutkimuksessa tarkemmin. Ks. rikostorjuntatoimivaltuuksien käyttöalan laajentamisesta HE 202/2017 vp, s. 111–114.
[29] Tiedusteluvaltuuksissa erityiset edellytykset on määritelty rikosten ja niiden vakavuuden sijasta uhkalähtöisesti. Ks. tästä tarkemmin HE 202/2017 vp, s. 74.
[30] Ks. tarkemmin HE 202/2017 vp, s. 111–114.
[31] Ks. tarkemmin perustuslain muutostarpeesta HE 198/2017 vp, s. 28–29. Lisäksi esitutkintalakiin

(PolL 5:1.2).[32] Rikoksen estämisestä on kysymys silloin, kun teko kyetään estämään ennen kuin tunnusmerkistön mukaiseen täytäntöönpanotoimeen tai sen yritykseen on ryhdytty. Valmistelun estämisellä taas tarkoitetaan rangaistavan teon valmistelua, vaikka itse teon valmistelua ei olisikaan kriminalisoitu. Valmistelun estämiseen tosin kuuluu myös rangaistavan valmistelun estäminen. Rikoksen keskeyttämiseen liittyvissä tapauksissa rikoksen tunnusmerkistö on saattanut edetä jo yrityksen asteelle, mutta tällöin tapaus luetaan edelleen rikoksen estämiseksi. Sama koskee myös rikoksesta aiheutuvan vahingon tai vaaran rajoittamista, jossa teko voi olla jo tehty, mutta seuraus ei ole vielä ilmennyt tai sitä pystytään vielä rajoittamaan.[33]

*Rikoksen paljastamisella* tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty (PolL 5:1.3). Rikoksen paljastamisella tarkoitetaan rikoksen estämisen ja selvittämisen väliin jäävää harmaata aluetta, josta esimerkkinä voidaan mainita tilanne, jossa vihjetiedon mukaan rikos olisi jo tehty, mutta syytä epäillä -kynnys ei ole vielä ylittynyt. Rikoksen paljastamisessa on tarkoituksena saada selville esitutkinnan aloittamisen perustaksi jo tehdyn rikoksen välittömästi merkityksellisiä seikkoja, kuten rikostunnusmerkistöön kuuluvat elementit sekä tekijä, tekoaika ja -paikka. Kyse ei siis ole rikoksen selvittämistä, koska ei ole syytä epäillä rikosta, mutta ei myöskään rikoksen estämisestä, koska rikos oletetaan jo tehdyksi.[34] Salainen tiedonhankinta on rikoksen paljastamiseksi erittäin rajattua ja tuleekin kyseeseen vain PolL 5:3:n mukaisissa tapauksissa, jotka koskevat lähinnä suojelupoliisin toimialaan kuuluvia maanpetos-, vakoilu- ja terrorismirikoksia.

Oli kyse rikoksen estämisestä tai paljastamisesta, tulkitaan havaintotietojen ja muutoin saatujen tietojen määritelmiä samoin. Henkilön toiminnasta tulee siis olla havaintoja tai muuten saatuja tietoja, ennen kuin salaisia tiedonhankintakeinoja voidaan käyttää. Näihin tietoihin kuuluvat rikostiedustelutiedot, tarkkailuhavainnot, vihjetiedot ja rikosanalyysillä tehdyt johtopäätökset. Edellytyksenä rikoksen estämisen osalta on, että tällaisten tietojen perusteella muodostuu perusteltu oletus henkilön syyllistymisestä rikokseen. Paljastamisen

[32] Poliisin lisäksi osaa salaisista tiedonhankintakeinoista on mahdollista käyttää rajavartio-, tulli- ja sotilasviranomaisten toimesta (PolL 5:1.4).
[33] HE 224/2010 vp, s. 89.
[34] HE 224/2010 vp, s. 90.

osalta taas riittää syytä olettaa -kynnys, joka on matalampi kuin esitutkintalain syytä epäillä -kynnys.[35] Jos syytä epäillä -kynnys täyttyy, siirrytään käyttämään pakkokeinolain mukaisia salaisia pakkokeinoja.[36] Pakkokeinolain mukaisissa salaisissa pakkokeinoissa on kyse jo tapahtuneen rikoksen esitutkinnasta.[37] Pakkokeinolain toimivaltuuksien käyttö tulee kysymykseen vasta siinä vaiheessa, kun poliisin on syytä epäillä rikosta ja poliisi aloittaa esitutkinnan, eli *rikoksen selvittämisen*. Suoritettaessa esitutkintalain 3:3.2:n mukaisia alustavia tutkintatoimia, ei PKL:n mukaiset pakkokeinot ole vielä mahdollisia.[38]

### 1.3 Tutkimuskysymykset ja tutkimuksen rajaukset

Tutkimus keskittyy tietoverkoissa tapahtuvaan poliisitoimintaan ja vaikka tietoverkoissa tapahtuva toiminta on sinänsä myös reaalimaailmassa tapahtuvaa toimintaa, on tutkimuksessa erotettu nämä käsitteet toisistaan. *Reaalimaailman* toiminnalla tarkoitetaan fyysiseen ja tosiasialliseen toimintaan perustuvia toimia, joita kohdehenkilö tekee tietoverkkojen ulkopuolella. *Tietoverkoilla* tarkoitetaan tässä tutkimuksessa laitteiden välisten tietoliikenneyhteyksien välille muodostuvaa järjestelmää, joka mahdollistaa datan välittämisen. Tietoverkon käsitteen alle lukeutuu internet, joka voidaan karkeasti jakaa näkyvyyden mukaan: 1) normaaliin internetiin (clearnet), 2) syvään internetiin (deep web) ja 3) pimeään internetiin (darknet). Internetin avoimet palvelut, kuten useimmat sosiaalisen media palvelut, lukeutuvat normaaliin internetiin. Keskimmäiseen liittyvät erilaiset verkkopankit ja valtiolliset tietokannat sekä maksumuurin takana olevat sivustot. Viimeisimmän joukon muodostavat erilaiset piilossa olevat palvelut, joihin pääsemiseen tarvitsee erillisen ohjelmiston.[39] Näitä ovat esimerkiksi TOR-ohjelmisto, mutta myös I2P ja Freenet.[40]

---

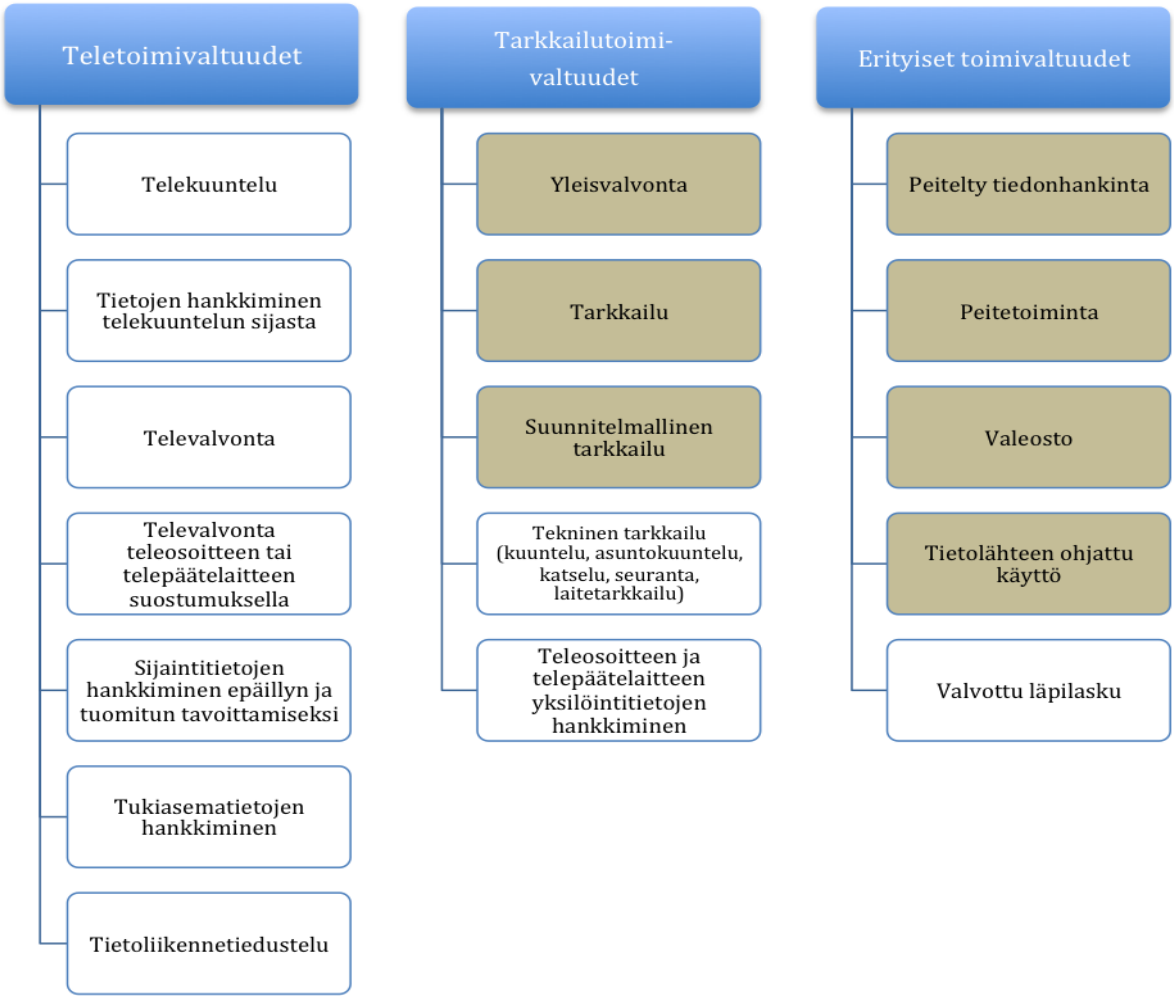
[35] HE 224/2010 vp, s. 89.
[36] Rikoksen estämiseksi tai paljastamiseksi aloitettua salaista tiedonhankintaa saadaan kuitenkin jatkaa enintään kolme vuorokautta tai enintään luvan voimassaoloaikaan asti, vaikka on syytä epäillä rikos jo tehdyksi. Tuon määräajan jälkeen tulee käyttää pakkokeinolain mukaisia salaisia pakkokeinoja ja saattaa asia toimivaltaisen viranomaisen ratkaistavaksi (PolL 5:4).
[37] Erona voidaan mainita esimerkiksi vain pakkokeinolain puolelta löytyvä sijaintitietojen hankkiminen epäillyn ja tuomitun tavoittamiseksi sekä asuntokuuntelu. Lisäksi eroja on esimerkiksi erityisten edellytysten osalta.
[38] Ks. rajanvedosta tarkemmin Helminen ym. 2014, s. 34–36.
[39] Käytännössä myös darknettiin pääsee avoimien tietoverkkojen kautta, mutta niihin vain tarvitsee kyseisen erillisen ohjelmiston.
[40] Ks. internetin datan näkyvyyden tasoista tarkemmin Willner-Mäenpää 2018, s. 16–17.

Jotta tutkimuskysymykset voidaan esittää ymmärrettävästi, tulee lukijan ymmärtää myös tietoverkkoihin liittyvät keskeiset telepäätelaitteen ja teleosoitteen määritelmät. *Telepäätelaitteella* tarkoitetaan laitetta, joka viestien lähettämiseksi, käsittelemiseksi tai vastaanottamiseksi on tarkoitettu johtimella, sähkömagneettisella tavalla liitettäväksi joko suoraan yleisen viestintäverkon liittymään tai toimimaan yleisen viestintäverkon yhteydessä kytkettynä suoraan tai epäsuorasti yleisen viestintäverkon liittymään.[41] Näitä ovat esimerkiksi pöytätietokoneet, älypuhelimet ja erilaiset tablettitietokoneet. *Teleosoite* on yläkäsite, joka kattaa kaikki tiedot, jonka perusteella tele- tai datayhteyden osapuolet voidaan yksilöidä. Näitä ovat esimerkiksi IP-osoite, sähköpostiosoite, käyttäjätunnus ja profiili.[42] Olennainen käsite tutkimuksen kannalta on juuri teleosoitteen määritelmän piiriin kuuluva *profiili*, joka on tietyssä palvelussa oleva käyttäjätili tai nimimerkki. Profiilin käsitteen alla tässä tutkimuksessa ymmärretään erilaiset sosiaalisen median profiilit, keskustelupalstan nimimerkit ja muut vastaavat tunnukset salasanoineen.

Tietoverkkojen globaalissa ja yleensä anonyymissä ympäristössä toimivaan poliisimieheen pätevät oikeudet ja velvollisuudet siinä missä reaalimaailmassakin, riippumatta siitä missä päin Suomea poliisimies suorittaa työtehtäväänsä.[43] Vaikka poliisin toimivalta sekä yksittäisten toimivaltuuksien ulottuvuus on sinänsä selvä, on reaalimaailmaan luotujen toimivaltuuksien soveltaminen tietoverkoissa tapahtuvassa toiminnassa monin paikoin vaikeaa.[44] On täysin eri asia tehdä havaintoja kohdehenkilöstä reaalimaailmassa tai olla hänen kanssaan fyysisessä vuorovaikutuksessa, verrattuna tietoverkkojen digitaaliseen ympäristöön. Ero konkretisoituu selvästi poliisilain 2 luvun yleisiä toimivaltuuksia tarkasteltaessa. Poliisilain 2 luvun 1 §:n mukaan poliisimiehellä on yksittäisen tehtävän suorittamiseksi oikeus saada jokaiselta tiedot tämän nimestä, henkilötunnuksesta tai sen puutteessa syntymäajasta ja kansalaisuudesta sekä paikasta, josta hän on tavoitettavissa. Jos henkilö kieltäytyy antamasta näitä tietoja, voidaan henkilöllisyys selvittää henkilötuntomerkkien perusteella tai ottaa henkilö jopa kiinni 24 tunnin ajaksi, jos se on välttämätöntä henkilöllisyyden selvittämiseksi. Sanomattakin on selvää, että kyseinen toimivaltuus ei ole toimiva tietoverkoissa.[45]

[41] HE 224/2010 vp, s. 93; HE 222/2010 vp, s. 316–317.
[42] HE 224/2010 vp, s. 32 ja 93; HE 222/2010 vp, s. 114–115.
[43] Poliisin hallinnosta annetun lain (110/1992, PolHalL) 15 a §:n 1 momentin mukaan poliisimiehellä on tehtäväänsä suorittaessaan koko maassa poliisilaissa tai muussa laissa säädetyt valtuudet.
[44] Ks. kansallisen sääntelyn haasteista globaalissa ympäristössä erityisesti tietoverkkojen näkökulmasta Forss – Keinänen 2017, s. 8–11.
[45] Yhtä selvää on, että poliisi ei voi eristää tiettyä paikkaa (PolL 2:8), hajottaa väkijoukkoa (PolL 2:9) tai käyttää voimakeinoja (PolL 2:17) tietoverkoissa. Ks. nettipoliisin ns. virtuaalisista huomautuksista ja toimivaltuuksiin tietoverkoissa liittyvästä problematiikasta tarkemmin Calcara ym. 2015, s. 10–15.

Poliisi- ja peiteprofiileilla toimiminen on teknisesti mahdollista vain tiettyjen salaisten tiedonhankinta- ja pakkokeinojen kohdalla. Näissä tapauksissa toimivaltuus löytyy aina sekä poliisi- että pakkokeinolain puolelta. Oheisesta kuviosta selviää, miten poliisi- ja peiteprofiileilla mahdolliset salaiset tiedonhankinta- ja pakkokeinot sijoittuvat eri tyyppisten toimivaltuuksien joukkoon. Todettakoon lisäksi, että yleisvalvonta (PolL 1:1) tai perusmuotoinen tarkkailu (PolL 5:13.1 ja PKL 10:12.1) eivät ole PolL 5:2:n tai PKL 10:2:n mukaisia salaisia tiedonhankinta- ja pakkokeinoja, mutta ovat tutkimuksen kannalta oleellisessa roolissa eri toimivaltuuksia määriteltäessä. Tämän takia ne esitetään mukana oheisessa kuviossa.




Kuvio 1. Salaisten tiedonhankinta- ja pakkokeinojen ryhmittely, jossa tummennettuina poliisi- ja peiteprofiileilla mahdolliset keinot.

Tässä tutkimuksessa on tarkoitus käsitellä edellisessä kuviossa tummennettuja poliisi- ja peiteprofiileilla tietoverkoissa teknisesti mahdollisia salaisia tiedonhankinta- ja pakkokeinoja. Tutkimus tulee kuvaamaan kyseisten toimivaltuuksien ulottuvuudet ja erot tietoverkoissa mahdollisimman tarkkarajaisesti ja täsmällisesti. Tutkimus ottaa kantaa poliisi- ja peiteprofiilien lisäksi myös siihen voiko poliisimies käyttää omaa siviiliprofiiliaan salaisessa tiedonhankinnassa. Toimintaympäristöjen erilaisuuden hahmottamiseksi tutkimuksessa käsitellään ensin kattavasti perus- ja ihmisoikeuksien suojan eroja reaalimaailman ja tietoverkkojen välillä poliisi- ja peiteprofiileihin liittyen. Jotta poliisi- ja peiteprofiileilla mahdollisia toimivaltuuksia voitaisiin kuvata, tuodaan esille miten profiilit luodaan ja mitä niillä toimiminen käytännössä tarkoittaa. Tähän liittyy peiteprofiilien kohdalla kysymys toiminnan suojaamisesta tietoverkoissa. Yksinkertaistettuna tutkimusongelman voi tiivistää kysymyksiin miten reaalimaailman tilanteita varten luotuja perus- ja ihmisoikeuksia tulisi tulkita tietoverkoissa ja miten poliisi- ja peiteprofiilit liittyvät salaisiin tiedonhankinta- ja pakkokeinoihin? Tarkemmin tutkimuskysymykset voidaan esittää seuraavasti:

1) Miten salaisiin tiedonhankinta- ja pakkokeinoihin liittyvät perus- ja ihmisoikeussuojatarpeet eroavat reaalimaailmassa ja tietoverkoissa sekä millainen vaikutus eroilla tulisi olla toimivaltuussäännöksiin?

2) Mikä on poliisiprofiili ja miten se liittyy salaisiin tiedonhankinta- ja pakkokeinoihin?

3) Onko poliisimiehellä mahdollisuus käyttää omaa siviiliprofiiliaan salaisessa tiedonhankinnassa?

4) Mikä on peiteprofiili ja miten suojaamissääntely liittyy sen luomiseen sekä käyttöön?

5) Miten tulisi tulkita poliisi- ja peiteprofiileilla mahdollisten salaisten tiedonhankinta- ja pakkokeinojen ulottuvuuksia sekä eroja tietoverkoissa?

Tutkimus keskittyy pääosin clearnetiä ja darknetiä koskeviin poliisin tiedonhankintamenetelmiin, joihin pääsy on lähtökohtaisesti kaikilla kansalaisilla.[46] Avoimissa tietoverkoissa tapahtuvaa tiedonhankintaa kutsutaan yleisesti *OSINT-toiminnaksi*

[46] Tutkimus rajataan poliisin tiedonhankintamenetelmiin, vaikka ne sopivat monilta osin identtisinä myös Tullin ja Rajavartiolaitoksen toimintaan.

(Open Source Intelligence), jolla tarkoitetaan tiedon keräämistä avoimista lähteistä.[47] Myös TOR-verkko kuuluu OSINT-toiminnan piiriin, vaikka kyse onkin sinänsä suljetusta ja internetistä osittain irrallisesta tietoverkosta. Syvät tietoverkot, kuten esimerkiksi työyhteisön sisäinen tietoverkko, jäävät tutkimuksen ulkopuolelle.[48]

Selkeimmin tutkimuksesta rajautuvat pois teletoimivaltuudet, koska niiden käyttö ei ole teknisesti mahdollista minkään toimivaltuuden kohdalla poliisi- tai peiteprofiileilla. Teletoimivaltuuksissa tiedonhankinta kohdistuu yleensä televerkkoihin ja kyselyt tehdään teleoperaattoreille.[49] Kyselyjä voi kohdentaa myös sosiaalisen median palveluntarjoajille, mutta myöskään näissä tapauksissa tiedonhankintaan ei voi käyttää poliisi- tai peiteprofiileja, vaan tiedonhankinta tapahtuu yleensä poliisin Salpa-järjestelmän kautta.[50] Erikseen voidaan vielä mainita tietoliikennetiedustelu, joka ei ole mahdollinen poliisi- ja peiteprofiileilla. Tietoliikennetiedustelu perustuu menetelmällisesti tietoliikenteen automatisoituun erotteluun, jossa viestimassasta suodatetaan haluttua tietoa erilaisin hakuehdoin.[51] Tietoliikennetiedusteluun liittyviä poliisilain 5 luvun ja pakkokeinolain 10 luvun lakimuutoksia sivutaan tutkimuksessa soveltuvin osin, mutta ne eivät ole vielä tutkimushetkellä astuneet voimaan.[52]

Tarkkailutyyppisistä tiedonhankinta- ja pakkokeinoista on poliisi- ja peiteprofiililla mahdollinen vain suunnitelmallinen tarkkailu (PolL 5:13 ja PKL 10:12). Vaikka yleisvalvonta (PolL 1:1) tai perusmuotoinen tarkkailu (PolL 5:13.1 ja PKL 10:12.1) eivät ole PolL 5:2:n tai PKL 10:2:n mukaan salaisia tiedonhankinta- tai pakkokeinoja, käsitellään niitä kattavasti tässä tutkimuksessa. Tämä sen takia, että niillä on oleellinen merkitys toimivaltuuksien rajojen hahmottamiselle sekä poliisin tiedonhankinnalle yleisesti tietoverkoissa. Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen (PolL 5:25 ja PKL 10:25) sekä teknisen tarkkailun eri muodot (PolL 5:17–24 ja PKL 16–24) rajautuvat pois. Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisessa käytetään teknistä

[47] Ks. OSINT-toiminnasta tarkemmin Bazzell 2014, s. 387–394.
[48] Tarkastelua ei lähtökohtaisesti uloteta myöskään muihin tiedonhankintatapoihin, kuten tietoliikennetiedusteluun tai Snowdenin paljastamaan National Security Agency (NSA) tiedusteluohjelmaan nimeltä PRISM, jolla pystyttiin systemaattisesti hakemaan tietoa palveluista kuten Facebook, Google ja Microsoft. Ks. tästä esimerkiksi Bosk ym. 2018, s. 79.
[49] Teleoperaattoreita ovat esimerkiksi Elisa ja Telia.
[50] Ks. Salpa-järjestelmästä tarkemmin esimerkiksi Poliisihallitus 2018c, s. 37.
[51] Ks. tarkemmin HE 202/2017 vp, s. 122.
[52] Poliisi- ja peiteprofiileihin liittyen muutokset koskivat päätöksentekijää, jossa useisiin säännöksiin lisättiin suojelupoliisin päällystöön kuuluva esimies. Lisäksi vaikutusta oli tietolähdetoimintaan. Tutkimushetkellä muutettiin myös poliisin henkilötietolainsäädäntöä, jonka vaikutus huomioidaan myös vain osittain tässä tutkimuksessa.

laitetta, joita poliisi- ja peiteprofiilit eivät ole. Teknisessä tarkkailussa on edellisen tapaan kyse erilaisten teknisten laitteiden käytöstä, eikä kyseiset tarkkailun muodot sovellu toimintaan poliisi- tai peiteprofiileilla. Esitöissä on nimenomaisesti todettu, että vaikka tietoverkoissa tapahtuvassa tarkkailussa käytetään teknistä laitetta, on se toimintaympäristöön liittyvä erityispiirre, jossa tietokonetta käytetään muiden käyttäjien tavoin.[53] Teoriassa teknisessä laitetarkkailussa (PolL 5:23 ja PKL 10:23) voitaisiin käyttää apuna poliisi- tai peiteprofiilia tilanteessa, jossa profiilista lähetetään haittaohjelman sisältämä viesti kohteelle.[54] Koska itse tiedonhankinta- tai pakkokeino kuitenkin suoritetaan muulla kuin poliisi- tai peiteprofiililla, en katso teknisen laitetarkkailun kuuluvan poliisi- ja peiteprofiililla tapahtuvan toiminnan piiriin.

Erityisistä toimivaltuuksista kyseeseen tulevat peitelty tiedonhankinta (PolL 5:15 ja PKL 10:14), peitetoiminta (PolL 5:28 ja PKL 10:27), valeosto (PolL 5:35 ja PKL 10:34) ja tietolähteen ohjattu käyttö (PolL 5:40 ja PKL 10:39). Näistä peitetoimintaa ja valeostoa koskevassa sääntelyssä tietoverkoissa tapahtuva toiminta on huomioitu.[55] Myös peitelty tiedonhankinta on mahdollista poliisi- ja peiteprofiileilla, mutta jostain syystä lainsäätäjä ei ole käsitellyt sitä tietoverkkojen näkökulmasta lainkaan. Tietolähdetoimintaa voidaan suorittaa tietoverkkojen kautta siinä missä reaalimaailmassakin, vaikka asiaa ei ole laissa tai esitöissä tarkemmin avattu. Lisäksi kyseeseen tulee välillisesti valvottu läpilasku (PolL 5:43 ja PKL 10:41), mutta en laske sitä suoraan poliisi- ja peiteprofiililla mahdolliseksi keinoksi. Valvotun läpilaskun osalta tilanne on osittain monimutkainen, koska yksinomaan tietoverkossa sitä ei voi käytännössä suorittaa.[56] Tämä johtuu erityisesti siitä syystä, että valvottua läpilaskua tulisi pystyä valvomaan ja tarvittaessa puuttua siihen, joka ei ole pelkästään tietoverkoissa toimien mahdollista.[57] Tullin salaisen tiedonhankinnan peitetoimintaa koskevien esitöiden mukaan yksinomaan tietoverkossa peitetoimintaa suorittava tullimies saisi varsinaisen peitetoiminnan lisäksi osallistua myös valvotun

[53] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.
[54] Haittaohjelmaa kutsutaan näissä tapauksissa yleensä nimellä kaksoiskäyttöohjelma.
[55] Tietoverkoissa tapahtuvan peitetoiminnan erityiset edellytykset ovat alhaisemmat kuin reaalimaailmassa (PolL 5:28.3 ja PKL 10:27.3) ja valeostossa tietoverkoissa julkisten myyntitarjouksien osalta päätöksentekijätaso on alhaisempi (PolL 5:36.1 ja PKL 10:35.1)
[56] Valvotun läpilaskun kohdalla on yleensä kyse laittomien tai laittomaksi epäiltyjen lähetysten kulku eri valtioiden rajojen yli. Ks. tästä tarkemmin HE 224/2010 vp, s. 37–38; HE 222/2010 vp, s. 120–121. Teoriassa kyse voisi olla myös datasta, mutta kyisestä seikkaa ei mainita säännöksessä. Käytännössä olisi myös melko vaikeaa valvoa datan liikkumista tietoverkoissa säännöksen tarkoittamalla tavalla.
[57] Valvotun läpilaskun tulisi olla koko ajan poliisin kontrollissa, koska lähetykseen tulee puuttua, jos se aiheuttaa säännöksessä määriteltyä vaaraa taikka esimerkiksi oikeusapupyynnön esittänyt ulkomaan esitutkintaviranomainen pyytää keskeyttämään toimituksen. Ks. tarkemmin HE 224/2010 vp, s. 128; HE 222/2010 vp, s. 350.

läpilaskun kohteena olevan toimituksen järjestämiseen, jos osallistuminen edistäisi merkittävästi läpilaskun tavoitteen saavuttamista.[58] Kyse on kuitenkin vain osittaisesta toimintaan osallistumisesta, jossa kyse on lähinnä peitetoimintaan liittyvästä sivujuonteesta. Vaikka valvottuun läpilaskuun voi liittyä peiteprofiili, pidän sitä samantyylisenä apuvälineenä kuin teknisessä laitetarkkailussa kaksoiskäyttöohjelmaa linkkaavaa profiilia, jonka takia valvotun läpilaskun tarkempi tarkastelu jää tästä tutkimuksesta pois.[59]

Koska tutkimus on jo muutoinkin normaalia laajempi, joudutaan erityisesti salaisten tiedonhankinta- ja pakkokeinoja koskevien yhteisten säännösten osalta tekemään laajoja rajauksia.[60] Toisaalta esimerkiksi kuuntelu- ja katselukiellot sekä ylimääräisen tiedon käyttö eivät koske poliisi- ja peiteprofiililla mahdollisia salaisia tiedonhankinta- ja pakkokeinoja, joten ne rajautuvat jo tällä perusteella tutkimuksesta pois.[61] Lisäksi voidaan mainita, että tuomioistuinkäsittelyyn liittyvät eroavaisuudet koskevat lähinnä telepakkokeinoja (PolL 5:45.3–4 ja PKL 10:43.3–4). Maininnan ansaitsee tässä yhteydessä erikseen salaisia tiedonhankinta- ja pakkokeinojen käytöstä ilmoittamista koskevat säännökset PolL 5:58 ja PKL 10:60, joilla on merkitystä myös tietoverkoissa tapahtuvalle toiminnalle. Tästä tutkimuksesta ne rajataan kuitenkin pois, koska ilmoitusvelvollisuuden osalta ei ole havaittavissa eroja reaalimaailman ja tietoverkoissa tapahtuvan toiminnan välillä.[62] Yhteisistä säännöksissä käsitellään kuitenkin kattavasti suojaamissäännöstä (PolL 5:46 ja PKL 10:47), koska se on erityisen tärkeässä roolissa juuri tietoverkkojen osalta. Tämä koskee sekä peiteprofiilien luomista että rikoksiin puuttumisen siirtämistä.

[58] HE 174/2014 vp, s. 105.

[59] Lisäksi voidaan huomioida se seikka, että valvottua läpilaskua ei juuri käytetä Suomessa. Esimerkiksi vuoden 2017 salaisesta tiedonhankinnasta ja sen valvonnasta annetun selvityksen mukaan poliisi oli tehnyt muutaman valvotun läpilaskun päätöksen, joskaan ei yhtään esimerkiksi vuonna 2017. Ks. tarkemmin Poliisihallitus 2018c, s. 30.

[60] Tästä tutkimuksesta pois rajattuihin kysymyksiin voi tutustua esimerkiksi Metsärannan 2015 väitöskirjasta s. 237–329, jossa Metsäranta kutsuu näitä säännöksiä minimointi- ja kontrollointimekanismeiksi. Ks. myös Helminen ym. 2014, s. 1219–1264; Helminen – Kuusimäki – Rantaeskola 2012, s. 421–430.

[61] Ylimääräisen tiedon käyttö koskee vain telekuuntelun, televalvonnan, tukiasematietojen hankkimisella ja teknisellä tarkkailulla saatua tietoa (PolL 5:53 ja PKL 10:55). Vrt. kuitenkin Poliisihallitus 2017a, s. 32, jonka mukaan suunnitelmallisessa tarkkailussa ylimääräisen tiedon käyttö oli merkitty jostain syystä kahteen pöytäkirjaan.

[62] Kyseinen ilmoitusvelvollisuus on saanut kritiikkiä poliisilta erityisesti niiden keinojen osalta, joissa käytetään jotain peitettä tai kyse on tietolähteen ohjatusta käytöstä. Ilmoittamisvelvollisuudella laukaistaan sekä hengen että terveyden vaara toimijalle. Lisäksi ilmoittamisella aiheutetaan salassa pidettävän poliisin taktisen ja teknisen menetelmän paljastumisvaara. Ks. kritiikistä tarkemmin esimerkiksi Poliisihallitus 2015, s. 39–40 ja 46.

### 1.4 Tutkimusmetodi ja tutkimuksen rakenne

Tutkimus on oikeusdogmaattinen, eli lainopillinen tutkimus, jonka tarkoituksena on tulkita ja systematisoida poliisi- ja peiteprofiileilla mahdollisten salaisten tiedonhankinta- ja pakkokeinojen toimivaltuussäännösten sisältöä sekä niihin vaikuttavia perus- ja ihmisoikeuksia. Lainopillisessa tutkimuksessa perustehtävänä on lain sisällön selventäminen, eli tulkinta, mutta myös oikeussäännösten systematisointi.[63] Lainopillinen metodi on oikeudellista päättelyä määrätyistä oikeustosiseikoista oikeusseuraamuksiin sekä toisaalta oikeusnormien keskinäistä suhteiden määrittämistä ohjaavien metatason sääntöjen ja periaatteiden kokonaisuus.[64] Tulkintasuosituksilla oikeustiede palvelee ensisijaisesti lainkäyttöä.[65] Tulkintaperusteita ryhmitellään eri tavoin riippuen siitä, onko tarkoitus tulkita esimerkiksi lainsäädäntöä tai oikeusperiaatteita.[66] Lainsäädännölle ominaisia tulkintaperusteita ovat *Siltalan* mukaan säännöksen sanamuodon mukainen tulkinta, systemaattinen tulkinta, lainsäätäjän tarkoitus, oikeuskäytännössä vakiintunut tulkinta, teleologinen tulkinta sekä perus- ja ihmisoikeusmyönteinen tulkinta.[67]

Systematisointi on yksi tekijä, joka tekee lainopista tiedettä ja joka voidaan nähdä lainsäätäjän systematisointityön jatkamisena.[68] Systematisoinnille on annettu oikeuskirjallisuudessa useita erilaisia määritelmiä. Systematisoinnin tehtävänä on saattaa oikeudellinen aines helpommin hallittavaan yleiskatsauksellisempaan, mutta samalla yksityiskohdissaan tarkempaan ja käytännössä soveltumiskelpoisempaan muotoon.[69] Lisäksi oikeustieteellisen systematisoinnin voidaan katsoa kehittävän yleisiä oppeja, mutta myös tarjoavan ratkaisuohjeita konkreettisissa soveltamistilanteissa oikeusperiaatteiden perusteella sekä oikeuskysymyksen paikan oikeusjärjestelmässä osoittavia oikeuskäsitteitä.[70] *Sajama* pyrkii kuvaamaan systematisointia kääntämisen, tulkitsemisen ja tiivistelmän käsitteiden kautta. Systematisoinnissa on mukana kääntämisen elementti, koska lähtötekstin ilmauksia käännetään selvemmiksi. Tulkinnan elementin mukaisesti systematisoinnissa joudutaan pohtimaan mitä lähtöteksti oikeasti merkitsee. Tiivistämisen elementin mukaisesti systematisoinnin tarkoitus on tiivistää lähtöteksti tiiviimpään muotoon. Lyhyesti Sajama

[63] Aarnio 1989, s. 304; Aarnio 2011, s. 13.
[64] Siltala 2003, s. 328.
[65] Tuori 2013, s. 22.
[66] Siltala 2003, s. 331 ja 363–367.
[67] Siltala 2003, s. 364. Ks. lainsäädännön eri tulkintaperusteista tarkemmin Siltala 2003, s. 334–340; Tuori 2013; s. 50–55. Ks. myös Kolehmainen 2016, s. 10–17.
[68] Kolehmainen 2016, s. 17.
[69] Lappi-Seppälä 1997, s. 192. Ks. myös Wilhelmsson 1997, s. 341.
[70] Kolehmainen 2016, s. 17.

toteaa systematisoinnin olevan informaatiokäsittelyprosessi, jossa lähtöteksti muuntuu kohdetekstiksi.[71]

Oikeuslähdeopin tärkein tehtävä on olla apuna voimassa olevan oikeuden määrittelyssä, joka edellyttää tulkinnan perustumista oikeudellisiin normeihin. Oikeuslähdeoppi rajaakin oikeuden ei-oikeudesta.[72] Oikeuslähdeoppi vastaa siihen, mikä on eri normilähteiden välinen hierarkia tai tärkeysjärjestys ja sen avulla voi konkreettisessa soveltamis- ja tulkintatilanteessa ottaa rationaalisesti kantaa eri normilähteiden keskinäisiin suhteisiin ja määrittää niiden painoarvoja.[73] Oikeuslähdeopillisesti tutkimus tukeutuu *Aarnion* ja *Peczenikin* oikeuslähdeoppiin, joka perustuu oikeuslähteiden velvoittavuuteen.[74] Oikeuslähteet jaotellaan vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin.[75] Kyseisen oikeuslähdeopin mukaisia vahvasti velvoittavia lähteitä ovat kansallisen tason normit perustuslaissa, eduskuntalaeissa sekä lakien nojalla annetut alemmantasoiset normit. Vahvasti velvoittaviin lähteisiin kuuluuvat myös eurooppaoikeuden suoraan sovellettavat osat, Euroopan ihmisoikeussopimuksen (EIS) normit sekä EU-tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen (EIT) prejudikaatit.[76] Heikosti velvoittavia oikeuslähteitä ovat lainvalmisteluaineisto ja ne tuomioistuinten ratkaisut, joilla voidaan katsoa olevan prejudikaattiarvoa. Sallittuja oikeuslähteitä ovat esimerkiksi laillisuusvalvojien ratkaisut, oikeuskirjallisuuden argumentit, lainoppi, yleiset oikeusperiaatteet ja vertailevat sekä käytännölliset argumentit.[77] Vaikka kyseinen kolmijakoinen staattinen oikeuslähdeoppi ei täysin tavoita dynaamisempaa eurooppaoikeuden vaikutusta, antaa se kiinteämmän ja ennakoitavamman perustan oikeudelliselle ratkaisutoiminnalle.[78]

Vahvasti velvoittavina lähteinä tutkimuksessa käytetään pääosin voimassa olevia poliisi- ja pakkokeinolakeja, mutta myös erityisesti perustuslakia ja sen 10 §:n mukaisen yksityiselämän suojan sisältöä.[79] Perus- ja ihmisoikeuksien vaikutus on muutoinkin vahvasti

[71] Sajama 2016, s. 40–41.
[72] Nuotio 2005, s. 128–129.
[73] Nuotio 2004, s. 1267–1268.
[74] Ks. vaihtoehtoisesta oikeuslähdeoppinäkemyksestä esimerkiksi Tolonen 2003, s. 22 ss.
[75] Aarnio 1989, s. 220–221. Ks. myös Hirvonen 2012, s. 153–154. Korostuneessa asemassa oikeuslähteiden velvoittavuus on erityisesti tutkimuksen osassa, jossa käsitellään sitä, onko tarkkailua salainen tiedonhankinta- tai pakkokeino.
[76] Aarnio 2006, s. 292.
[77] Aarnio 2006, s. 293.
[78] Kolehmainen 2016, s. 9–10.
[79] Poliisi- ja pakkokeinolakien kohdalla käytetään myös jo kumottuja säännöksiä tulkinta-apuna. Esimerkkinä tästä voidaan mainita tarkkailu.

läsnä salaisia tiedonhankinta- ja pakkokeinoja koskevassa sääntelyssä, koska lainsäätäjä on systematisoinut toimivaltuuksien käytön yleisten ja erityisten edellytysten yhteisvaikutuksen kautta.[80] Tutkimuksessa systematisoidaan erityisiä edellytyksiä selvemmin hahmotettavaksi kokonaisuudeksi, joka on jäänyt lainvalmisteluaineistossa ja oikeuskirjallisuudessa melko vähälle huomiolle. Lisäksi toimivaltuuksien käyttöön vaikuttavat poliisi-, pakkokeino- ja esitutkintalain yleiset periaatteet, joilla voi olla myös merkittävä vaikutus yksittäisessä toimivaltuuden käyttötilanteessa.[81] Poliisi- ja peiteprofiileihin liittyen perusoikeuksiin liittyvää tulkintaa ja systematisointia tehdään merkittävissä määrin reaalimaailman ja tietoverkkojen yksityiselämän suojan tarpeen eroista.[82] Vaikka suojan tason tarpeissa osoitetaan olevan selkeitä eroja, tulee jokaisen toimivaltuuden kohdalla joka tapauksessa valita perus- ja ihmisoikeuksia parhaiten edistävä tulkinta.[83] Vahvasti velvoittavana oikeuslähteenä pidetään myös tavanomaista oikeutta, eli maantapaa. Vaikka sen merkityksen on voitu katsoa jäävän modernin lainsäädännön jalkoihin, voidaan etenkin informaatioteknologian nopean kehityksen katsoa lisänneen tavanomaisen oikeuden merkitystä. Tämä sen takia, että jo muutaman vuoden ikäinen lainsäädäntö voi olla teknisen kehityksen takia vanhaa.[84] Vahvasti velvoittavista oikeuslähteistä voidaan mainita myös EIS 8 artiklan sisältö ja Euroopan ihmisoikeustuomioistuimen (EIT) ratkaisut, joilla on ollut yleisesti suuri vaikutus salaisten tiedonhankinta- ja pakkokeinojen sääntelyn kehitykseen.[85] Toisaalta näissä ratkaisuissa tietoverkkojen osuutta ei ole juurikaan käsitelty ja ne toimivatkin tutkimuksessa lähinnä erilaisten tulkintojen tukena.[86]

Heikosti velvoittavina oikeuslähteinä tukeudutaan pääosin salaisia tiedonhankinta- ja pakkokeinoja koskevaan lainvalmisteluaineistoon. Esitöiden merkitys perustuu ajatukseen, jonka mukaan tulee pyrkiä lainsäätäjän alkuperäisen tahdon tai tavoitteiden toteuttamiseen. Painoarvoon vaikuttaa myös esitöiden tuoreus ja kuinka kattavasti esitöissä on kyetty ennakoimaan tulevaisuudessa toteutuvia laintulkintatilanteita.[87] Tutkimuksessa tullaan

[80] Ks. perus- ja ihmisoikeuksien haasteista oikeuslähdeopille tarkemmin Metsäranta 2015, s. 134–139.
[81] Tällä tarkoitetaan sitä, että lakiin perustuvien yleisten ja erityisten edellytysten osalta tietyn toimivaltuuden käyttäminen voisi olla sinänsä mahdollista, mutta suhteellisuusperiaatteen vaikutuksesta voi seurata se, ettei säännöstä voida soveltaa kyseessä olevaan tapaukseen lainkaan. Ks. esimerkiksi HE 16/2013 vp, s. 10. Ks. myös LaVL 7/2000 vp, s. 5.
[82] Myös perusoikeusjärjestelmä voi olla lainopillisen systematisoinnin kohteena. Ks. tähän liittyen Siltala 2003, s. 571.
[83] PeVM 25/1994 vp, s. 4. Ks. myös Nuotio 2005, s. 131–132.
[84] Siltala 2001, s. 94.
[85] Ks. esimerkiksi HE 224/2010 vp, s. 15; HE 222/2010 vp, s. 12.
[86] Tämän takia EIT:n ja laillisuusvalvojien ratkaisujen määrä on tässä tutkimuksessa luultavasti hieman suppeampi kuin muutoin salaisia tiedonhankinta- ja pakkokeinoja käsiteltäessä, eikä ratkaisujen sisältöä käydä kovinkaan kattavasti läpi.
[87] Siltala 2001, s. 95.

käyttämään uusien poliisi- ja pakkokeinolakien lainvalmisteluaineiston lisäksi myös jo kumottujen säännösten lainvalmisteluaineistoa.[88] Sallittujen oikeuslähteiden osalta on viitattu muutamiin laillisuusvalvojan ratkaisuihin, mutta tietoverkkojen osuus on myös näiden ratkaisujen kohdalla heikko. Oikeuskirjallisuudesta on yritetty käydä taustoituksessa läpi kattavasti aihealueeseen liittyvää kotimaista ja ulkomaalaista oikeuskirjallisuutta, mutta salaisiin tiedonhankinta- ja pakkokeinoihin tietoverkoissa liittyvää materiaalia löytyi äärimmäisen vähän.[89] Esimerkkinä voidaan mainita *Metsärannan* väitöskirja, jossa hän käsitteli poliisin salaisia tiedonhankintakeinoja ja yksityiselämän suojaa valtiosääntöoikeudellisesta näkökulmasta.[90] Käytännössä Metsäranta ei kuitenkaan ole käsitellyt tutkimuksessaan tietoverkkojen erilaista roolin reaalimaailmaan verrattuna kuin sääntelystä ja lainvalmisteluaineistosta löytyvien niukkojen esimerkkien kautta.[91]

Salaisia tiedonhankinta- ja pakkokeinoja pidettiin jo ennen vuoden 2014 kokonaisuudistusta sekavana ja vaikeasti hallittavana kokonaisuutena, jossa lukujen välillä määritelmät ja menetelmien käyttöedellytykset poikkesivat monin paikoin ja perusteettomasti toisistaan.[92] Vaikka erityisesti sääntelyn rakennetta ja yhtäläisyyksiä poliisi- ja pakkokeinolain välillä selvennettiin, jouduttiin sääntelyä kuitenkin korjaamaan jo ennen sen voimaantuloa.[93] Toisaalta kokonaisuudistuksen jälkeenkin muutoin tarkkarajaiseen ja täsmälliseen sääntelyyn pyrkinyt uudistus on ollut erityisesti tietoverkkojen osalta epäselvä ja tulkinnanvarainen kokonaisuus, jossa reaalimaailman tilanteista tulisi johtaa tulkintoja tietoverkkojen selvästi erilaiseen ympäristöön.[94] Tässä tutkimuksessa tulkinta ja systematisointi ei välttämättä jatkakaan suoraan lainsäätäjän työtä, vaan alkaa tietoverkkojen kohdalla paikoin miltei lähtöpisteestä. Tämän takia myös lainsäädännölle ominaisten tulkintaperusteiden käyttäminen ei välttämättä onnistu. Esimerkiksi säännöksen

[88] Vaikka vanhemmalla lainvalmisteluaineistolla ei välttämättä ole niin suurta painoarvo kuin voimassa olevan lainsäädännön osalta, voidaan yhtenä tutkimukseen liittyvänä esimerkkinä mainita vuoden 1995 poliisilain yleisvalvontaa käsittelevä osio, jossa kyseisen keinon sisältöä on avattu kattavammin.

[89] Muutamissa tapauksissa tulen esittämään myös omaa kokemusperäistä tietoa poliisin salaisiin tiedonhankinta- ja pakkokeinoihin liittyen. Tämän pyrin kuitenkin tekemään lähinnä esimerkkien kautta, enkä niinkään tietyn normin tulkinta-apuna.

[90] Metsäranta 2015.

[91] Muusta peruskirjallisuudesta voidaan mainita Helminen ym. 2014 sekä Helminen –Kuusimäki – Rantaeskola 2012, joissa on perusesitykset poliisi- ja pakkokeinolain salaisista tiedonhankinta- ja pakkokeinoista. Myöskään näissä tietoverkkojen roolia ei ole otettu tarkempaan tarkasteluun.

[92] HE 224/2010 vp, s. 31–32; HE 222/2010 vp, s. 12. Vaikeaselkoisuus ja soveltamisongelmat olivat tulleet ilmi useissa laki- ja perustuslakivaliokuntalausunnoissa sekä ylimpien laillisuusvalvojien ratkaisuissa.

[93] Ks. HE 16/2013 vp, s. 5; HE 14/2013 vp, s. 6. Tällä hetkellä poliisi- ja pakkokeinolain väliset sääntelyerot ovat suhteellisen vähäisiä.

[94] Ks. esimerkiksi Poliisihallitus 2016a, s. 37 ja jo aikaisemmin mainittu Hankilanojan kritiikki erityisesti tietoverkkoja koskevan sääntelyn suhteen Hankilanoja 2014, s. 105–106. Esimerkkinä voidaan mainita myös paljon julkisuudessa ollut oikeudenkäynti tietolähdetoimintaan liittyen, josta ei kirjoitushetkellä ole vielä saatu tuomiota.

sananmukainen tulkinta ei välttämättä onnistu, jos lainvalmisteluaineisto koskee vain reaalimaailmaa. Myös lainsäätäjän tarkoitus jää monin paikoin epäselväksi. Juuri näiden erinäisten tulkintahaasteiden takia tutkimus sisältää *de lege lata* tulkintasuositusten lisäksi runsaahkosti myös *de lege ferenda* -tutkimukseen liittyvää lainsäädäntökritiikkiä ja suosituksia sääntelyn jatkokehittämisen suhteen. Tämän takia toivon tutkimuksen toimivan ainakin keskustelunavauksena sille, miten lainsäätäjän tulisi säännellä tulevaisuudessa salaisia tiedonhankinta- ja pakkokeinoja tietoverkoissa.

Tutkimuksen johdannon jälkeen käydään läpi pääluvussa kaksi ihmisoikeussopimusten ja EU-oikeuden vaikutusta salaisiin tiedonhankinta- ja pakkokeinoihin. Erityisesti kiinnitetään huomiota Euroopan ihmisoikeussopimukseen. EU-oikeuden merkitystä sivutaan vain lyhyesti, koska vaikutus salaisiin tiedonhankinta- ja pakkokeinoihin on ainakin toistaiseksi vain välillinen. Kolmannessa pääluvussa käsitellään perustuslain 10 §:n yksityiselämän suojan sisältöä ja käydään läpi eroja reaalimaailman ja tietoverkkojen välillä.[95] Kotirauhan suojan käsittely jää vähemmälle, mutta luottamuksellisen viestin suojan kohdalla tietoverkkojen merkitys alkaa jo näkyä. Yksityiselämän suojan kohdalla erot on jo selvästi havaittavissa ja problematiikka on jaoteltu viiteen eri alalukuun. Jaottelu on osittain päällekkäinen, joten jaottelua ei tule tulkita siten, että jokainen alaluku olisi selvästi erotettavissa toisistaan. Kyseinen suojien päällekkäisyys on muutoinkin tyypillistä PL 10 §:n sääntelylle. Kolmannen luvun päättää alaluku, jossa tuodaan koottuna esille reaalimaailman ja tietoverkkojen erot.[96]

Neljännessä pääluvussa käsitellään perus- ja ihmisoikeuksien vaikutusta poliisi- ja pakkokeinolain yksittäisiin säännöksiin. Luvussa käydään ensin läpi poliisilain 1 luvun ja pakkokeinolain 1 luvun yleisiä periaatteita.[97] Sen jälkeen avataan salaisia tiedonhankinta- ja pakkokeinoja koskevien yleisten ja erityisten edellytysten vaikutusta eri toimivaltuuksien käyttöön. Yleisten edellytysten käsittely jää melko yleiselle tasolle, mutta erityisten edellytysten osalta on pyritty systematisoimaan niitä koko salaisia tiedonhankinta- ja pakkokeinoja koskeva sääntely silmällä pitäen. Lopuksi käsitellään vielä salaisten tiedonhankinta- ja pakkokeinojen päätöksentekijätasoa.

[95] Salaisten tiedonhankinta- ja pakkokeinojen osalta oleellisten kotirauhan ja luottamuksellisen viestin suojan osalta tilanne on suhteellisen selkeä tietoverkoissa, mutta myös niitä käsitellään mahdollisimman kattavasti tietoverkkojen näkökulmasta.

[96] Erityisesti yksityiselämän suojan laaja käsittely on vaikuttanut tutkimukseen siten, että sitä voidaan pitää normaalia pro gradu -tutkielmaa laajempana. Pidän kuitenkin kyseistä osiota niin tärkeänä, että sen poisjättäminen olisi vaikeuttanut selvästi tutkimuksen muiden osioiden ja erityisesti yksittäisten toimivaltuuksien tarkempaa käsittelyä.

[97] Lisäksi sivutaan esitutkintalain periaatteita.

Pääluvussa viisi esitellään näkyvään toimintaan tarkoitettu poliisiprofiili, eli tuttavallisemmin nettipoliisitoiminta, ja mitkä sen liittymäpinnat ovat salaisiin tiedonhankinta- ja pakkokeinoihin. Samasta luvusta löytyy myös tulkintaa siitä, millä edellytyksillä poliisimies voi käyttää siviiliprofiiliaan omassa työssä. Pääluvussa kuusi käsitellään poliisin käyttämiä peiteprofiileja ja erityisesti profiilin luomiseen liittyvää problematiikkaa. Suojaamissääntelyn kohdalla voidaan havaita tulkintaongelmia erityisesti tiedon, asiakirjan ja rekisterin käsitteiden osalta, mutta myös problematiikka sen suhteen, voidaanko suojaamissääntelyä käyttää yleensäkään yleisvalvontaan tai tarkkailuun. Tämän takia avataan kattavasti myös tarkkailun toimivaltuusluonnetta. Luvussa kuusi käsitellään lisäksi suojaamissääntelyyn liittyvää peiteprofiilin velvollisuutta puuttua havaitsemiinsa rikoksiin.

Pääluvussa seitsemän käsitellään kattavasti kaikkia poliisi- ja peiteprofiileilla mahdollisia salaisia tiedonhankinta- ja pakkokeinotoimivaltuuksia. Mukana on myös yleisvalvonta ja tarkkailu, vaikka ne eivät olekaan PolL 5:2:n tai PKL 10:2:n mukaisia salaisia tiedonhankinta- tai pakkokeinoja. Jokainen toimivaltuus on esitelty erityisesti tietoverkkojen näkökulmasta. Viimeisessä kahdeksannessa pääluvussa käydään läpi johtopäätökset tutkimuskysymyksiin.

# 2 SALAISIA TIEDONHANKINTA- JA PAKKOKEINOJA KOSKEVAT IHMISOIKEUSSOPIMUKSET JA EU-LAINSÄÄDÄNTÖ

## 2.1 Ihmisoikeussopimukset

Suomen perustuslaki vastaa hyvin pitkälti kansainvälisten sopimusten velvoitteita, koska vuoden 1995 perusoikeusjärjestelmä integroitiin ihmisoikeusjärjestelmiin. Merkittävämpänä salaisiin tiedonhankinta- ja pakkokeinoihin vaikuttavana sopimuksen voidaan mainita Euroopan ihmisoikeussopimus, joka on saatettu Suomessa voimaan eduskuntalailla (SopS 18–19/1990).[98] Muina merkittävinä sopimuksina voidaan mainita Yhdistyneiden kansakuntien (YK) kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (KP-sopimus), joka on myös saatettu voimaan eduskuntalailla (SopsS 7–8/1976). Sen merkitys on kuitenkin jäänyt selvästi EIS:n ja EIT:n ratkaisukäytännön varjoon. [99] Selkeimmin salaisiin tiedonhankinta- ja pakkokeinoihin vaikuttaa EIS:n yksityiselämän suojaa koskeva 8 artikla.[100] Vaikka EIT:n käyttämät käsitteet eivät välttämättä ole samansisältöisiä kuin valtioiden sisäisessä lainsäädännössä, tulee Suomen perustuslain säännösten antaa vähintään samansisältöistä ja -asteista suojaa.[101]

EIS:n yksityiselämän suojaa antava 8 artikla on seuraavanlainen: 1.) Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. 2.) Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.[102] EIS:n 8 artiklan mukaisen yksityiselämän suojan voidaan katsoa kattavan

[98] EIS ja erityisesti EIT:n tulkintakäytäntö on vaikuttanut selvästi viimeisimpään poliisi- ja pakkokeinolain kokonaisuudistukseen. Ks. HE 224/2010 vp, s. 7 ja HE 222/2010 vp, s. 12.

[99] EIS:n roolia tärkeimpänä ihmisoikeussopimuksena on korostettu sen tiukemman valvontajärjestelmän ja EIT:n ratkaisukäytännön yksityiskohtaisuuden merkityksellä. Ks. Pölönen 1997, s. 19–20; Helminen ym. 2014, s. 56; Metsäranta 2015, s. 23.

[100] Lisäksi salaisia tiedonhankinta- ja pakkokeinoja on käsitelty EIS:n 6 artiklan oikeudenmukaisen oikeudenkäyntiin liittyen ja erityisesti equality of arms -periaatteen kautta. Ks. kyseisestä periaatteesta ja siihen liittyvästä ratkaisukäytännöstä tarkemmin Tapanila 2018, s. 674–683.

[101] Helminen ym. 2014, s. 57. Ks. laajasti EIS:n valtiolle asettamien velvoitteiden yleisestä luonteesta ja ulottuvuudesta sekä niihin liittymistä varaumista Pellonpää 2018, s. 12–40.

[102] KP-sopimuksen 17 artiklassa on turvattu yksityiselämän suoja seuraavasti: ”1.) Kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. 2.) Jokaisella on oikeus lain suojaan tällaista puuttumista tai

lähes koko elämän kirjon. Se on usein päällekkäinen muiden 8 artiklan suojan kohteisiin eli perhe-elämään, kotiin ja kirjeenvaihtoon. EIT tarkastelee 8 artiklan suojan tarvetta negatiivisesta (pidättäytymisvelvollisuus) tai positiivisesta (toimimisvelvollisuus) näkökulmasta. Negatiivisen velvollisuuden analyysissä arvioidaan onko puuttuminen ollut lakiin perustuvaa ja lainmukaista, onko puuttumisella ollut oikeutettu tarkoitus ja onko se ollut välttämätöntä demokraattisessa yhteiskunnassa. Positiivisen velvollisuuden näkökulmasta EIT ei arvioi kyseisiä asioita, vaan kohtuullista tasapainoa yleisen edun vaatimusten ja yksilön edun välillä.[103]

EIT on todennut, että jo pelkkä salaisen tiedonhankinnan mahdollistava lainsäädäntö on yksityiselämän suojaan puuttumista.[104] Yleisesti salaisia tiedonhankinta- ja pakkokeinoja koskien EIT on asettanut vähimmäisvaatimukset salaisia tiedonhankinta- ja pakkokeinoja koskevalle lainsäädännölle, jotka voivat tosin vaihdella toimivaltuuksittain.[105] Siten esimerkiksi telekuuntelua varten asetetut vaatimukset eivät välttämättä sovellu sellaisenaan avoimessa tietoverkossa tapahtuvaan salaiseen tiedonhankintaan. EIT:n ratkaisukäytännössä on noussut esille ainakin vaatimukset, että 1) puuttumisella on oltava oikeudellinen perusta, 2) tieto tilanteeseen sopivista oikeudellisista säännöistä on oltava saatavilla, 3) ennustettavuusvaatimus, jonka perusteella normien tulee olla riittävän tarkkarajaisia, jotta yksilö voisi päätellä tekojensa seuraukset sekä 4) vallan väärinkäytön estäminen.[106] Nimenomaan väärinkäytösten estämiseksi EIT on määritellyt vähimmäistakeita, joita lainsäännöstä tulisi löytyä. Näitä ovat 1) toimivaltuuden keston rajoittaminen, 2) saadun aineiston tutkimista, käyttämistä ja säilyttämistä koskeva sääntely, 3) varokeinot tietojen ilmoittamisessa muille osapuolille ja 4) olosuhteet, joissa tallenteet voi tai tulee poistaa.[107]

EIT:n lainkäytöllä voidaan katsoa olevan dynaaminen eli oikeutta kehittävä vaikutus. Esimerkkinä dynaamisuudesta voidaan mainita 8 artiklan kirjeenvaihdon käsitteen laajentuminen teknisen kehityksen myötä koskemaan myös sähköistä viestintää.[108] Toisaalta EIT:n ratkaisukäytännöstä ei ole löydettävissä tulkintaa siitä, miten yksityiselämän suojan eroja tulisi arvioida reaalimaailman ja tietoverkkojen välillä. Ratkaisut painottuvat

tällaisia hyökkäyksiä vastaan.”

[103] Ks. tarkemmin tapausten analyysin rakenteesta Hirvelä – Heikkilä 2017, s. 629–630.

[104] Ks. tähän liittyen esim. Klass ym. v. Saksa (1978), kohdat 30–38; Halford v. Yhdistynyt Kuningaskunta (1997), kohta 56.

[105] Uzun v. Saksa (2010), kohta 66. Ks. myös laajemmin Metsäranta 2015, s. 120–121.

[106] Ks. aiheesta tarkemmin ratkaisuineen HE 198/2017 vp, s. 19–21; Metsäranta 2015, s. 116–123.

[107] Ks. *Weber ja Saravia v. Saksa* (2006), kohta 95.

[108] Ks. esimerkiksi *Copland v. Yhdistynyt Kuningaskunta* (2007), kohdat 41–42. Ks. tarkemmin erityisesti 8 artiklan kehittyvästä luonteesta EIT:n ratkaisukäytännön seurauksena Hirvelä – Heikkilä 2017, s. 628.

tietoverkkojen kohdalla enemmän julkaisutoimintaan ja nimenomaan luottamuksellisen viestinnän suojaan liittyviin teletoimivaltuuksiin.[109] EIT:n ratkaisuilla tullee joka tapauksessa olemaan merkittävä rooli tulevaisuudessa myös avoimia tietoverkkoja koskevien salaisten tiedonhankinta- ja pakkokeinojen sääntelykehityksessä dyynaamisen luonteensa takia.[110]

EIT:n valvontajärjestelmää ollaan uudistettu vuosien varrella esimerkiksi järjestelmän ruuhkautumisen takia.[111] Tällä hetkellä EIT käsittelee valitusasioita yhden tuomarin kokoonpanossa, kolmesta tuomarista koostuvissa komiteoissa, seitsemästä tuomarista koostuvissa jaostoissa sekä seitsemästätoista tuomarista koostuvassa suuressa jaostossa.[112] Elokuussa 2018 astui Suomessa voimaan EIS:n kuudennentoista pöytäkirjan lainsäädännön alaan kuuluvat määräykset (SopS 52/2018), jonka 1 artiklan 1 kohdan perusteella sopimusvaltion ylimmät tuomioistuimet voivat pyytää EIT:ltä neuvoa-antavan lausunnon.[113] Euroopan neuvoston ihmisoikeusvaltuutettu ja neuvoa-antavaa lausuntoa pyytävän tuomioistuimen sopimusosapuolella on 3 artiklan mukaan oikeus esittää kirjallisia huomioita ja osallistua suulliseen käsittelyyn. Neuvoa-antavan lausunnon pyytäminen on vapaaehtoista, eikä se 5 artiklan mukaan sido kansallista tuomio-istuinta. Lausunnon antaa 2 artiklan 2 kohdan mukaan suuri jaosto, joten sen painoarvoa voidaan kuitenkin pitää merkittävänä.[114]

## 2.2 Euroopan unionin lainsäädäntö

Euroopan unionin perusoikeuskirjan (2012/C 326/02, 26.10.2012) artiklassa 7 turvataan yksityis- ja perhe-elämän kunnioittaminen. Kyseisen artiklan mukaan ”Jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan.”. Euroopan unionin perusoikeuskirja perustuu hyvin pitkälti EIS:n sisältöön, mutta siinä on käytetty nykyaikaisempaa muotoiltua ja suojeltujen etujen ala on laajempi.[115] EIS 8 artiklan

[109] Esimerkiksi niin sanottuun massavalvontaan liittyen löytyy useita ratkaisuja. Ks. esimerkiksi Snowdenin paljastuksiin liittyen *Big Brother Watch and Others v. Yhdistynyt kuningaskunta* (2018).
[110] Ks. nykyisiin poliisi- ja pakkokeinolakeihin liittyvästä vaikutuksesta HE 224/2010 vp, s. 15; HE 222/2010 vp, s. 12.
[111] Ks. valvontajärjestelmän muutoksista ja valitusmääristä tarkemmin HE 286/2014 vp, s. 3–5.
[112] Ks. EIT:n eri kokoonpanoista tarkemmin Hirvelä – Heikkilä 2017, s. 30–37.
[113] Suomessa näitä tuomioistuimia ovat korkein oikeus, korkein hallinto-oikeus, työtuomioistuin ja vakuutusoikeus.
[114] Tutkimuksentekohetkellä EIT on jo antanut ensimmäisen ennakkopäätöksensä, mutta tämä ei koskenut salaisia tiedonhankinta- ja pakkokeinoja.
[115] Ks. perusoikeuskirjan soveltamisesta yleisesti esitutkintaan Helminen ym. 2014, s. 51–54.

sisällön on katsottu vastaavaan perusoikeuskirjan 7 artiklaa, koska perusoikeuskirjan oikeudet perustuvat EIS:een, mutta myös EIT:n ratkaisukäytäntöön.[116]

Euroopan unionin perusoikeuskirjan soveltamisen merkitys salaisten tiedonhankinta- ja pakkokeinojen osalta on jäänyt vähäiseksi.[117] Suurin syy tähän on perusoikeuskirjan 51 artikla, jonka mukaan määräykset koskevat jäsenvaltioita ainoastaan silloin, kun sovelletaan unionin oikeutta. Lisäksi vaikutusta heikentävänä seikkana voidaan mainita Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoidun toisinnon (C 326/47, 26.10.2012) 276 artikla, jonka mukaan Euroopan unionin tuomioistuimella ei ole toimivaltaa tutkia jäsenvaltion poliisiviranomaisen tai muiden lainvalvontaviranomaisten toteuttamien toimien pätevyyttä tai oikeasuhtaisuutta taikka antaa ratkaisua niiden velvollisuuksien suorittamisesta, joita jäsenvaltioilla on yleisen järjestyksen ylläpitämiseksi ja sisäisen turvallisuuden suojaamiseksi. EUT:lla on kuitenkin ratkaisuvaltaa erityisesti sähköistä viestintää ja henkilötietoja koskevissa asioissa ja siten EU-oikeudella on ainakin välillistä merkitystä myös salaisten tiedonhankinta- ja pakkokeinojen suhteen.[118]

EU-oikeuden suhteellisen vähäisestä merkityksestä huolimatta salaisia tiedonhankinta- ja pakkokeinoja koskevaa sääntelyä on pyritty harmonisoimaan EU-tasolla jo 1990-luvulta lähtien.[119] Vaikutusta salaisiin tiedonhankinta- ja pakkokeinoihin on myös muutoin välillisesti Europolin kautta tapahtuvan tiedonvaihdon ja yhteisten tutkintaryhmien (Joint Investigation Team, JIT) takia.[120] Kyseisiä ryhmiä perustetaan tilanteissa, joissa kyse on vaativasta rajat ylittävästä tutkinnasta tai kyseessä on toisiinsa liittyvä tutkinta, joka vaatii koordinointia.[121] Kansainvälinen yhteistyö on myös mahdollistanut esimerkiksi peitepoliisitoiminnassa siten, että vieraan valtion virkamies suorittaa peitetoimintaa Suomessa Suomen poliisin tekemän kansainvälisen oikeusapupyynnön perusteella.[122] EU:n liittyvästä yhteistyöstä voidaan mainita esimerkkinä myös PolL 5:27:ssä vieraan valtion

[116] HE 202/2017 vp, s. 65.
[117] Savola 2015, s. 60–64; Metsäranta 2015, s. 25–26.
[118] Ks. tarkemmin EUT:n ratkaisukäytännöstä ja EU-oikeuden vaikutuksesta luottamuksellisen viestinnän suojaan HE 202/2017 vp, s. 65–68; HE 198/2017 vp, s. 23–26. Ks. myös vireillä oleva ennakkoratkaisupyyntö C-623/17 *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs ym.* (2017) EUVL:C:22 tietoliikennetiedusteluun liittyen.
[119] Ks. esimerkiksi HE 34/1999 vp, s. 16; HE 266/2004 vp, s. 23.
[120] Ks. poliisin kansainvälisestä yhteistoiminnasta Helminen – Kuusimäki – Rantaeskola 2012, s. 45–56.
[121] Euroopan unionin neuvosto 2017, s. 6. Ks. myös tiedote Europol 2019. Tiedotteessa kerrottiin JIT-operaatiosta, jossa xDedic Marketplace-niminen sivusto ja sen palvelimet suljettiin usean maan yhteistyössä. Kyseinen sivusto toimi avoimen internetin lisäksi darknetissä ja sitä kautta pystyi ostamaan pääsyn hakkeroituihin tietokoneisiin sekä erilaisiin anastettuihin henkilötietoihin.
[122] HE 266/2004 vp, s. 26.

virkamiehen suorittamaa tarkkailua ja teknistä tarkkailua koskeva sääntely. Lisäksi poliisilain 9 luvusta löytyy Prüm- ja Atlas-yhteistyöhön liittyvä sääntelyä.

# 3 SALAISIA TIEDONHANKINTA- JA PAKKOKEINOJA KOSKEVAT PERUSOIKEUDET ERITYISESTI TIETOVERKKOJEN NÄKÖKULMASTA

## 3.1 Salaisiin tiedonhankinta ja -pakkokeinoihin vaikuttavat perusoikeudet

Salaisilla tiedonhankinta- ja pakkokeinoilla puututaan erityisesti PL 10.1 §:ssä mainittuihin yksityiselämän ja kotirauhan suojaan sekä PL 10.2 §:n mukaiseen luottamuksellisen viestin suojaan.[123] Yksityiselämän suoja voidaan ymmärtää henkilön yksityistä piiriä koskevaksi yleiskäsitteeksi, eikä PL 10 §:llä suojattavat oikeushyvät ole kaikissa tilanteissa täysin muutenkaan erotettavissa toisistaan.[124] PL 10.1 §:ssä mainitaan myös henkilötietojen suoja, josta todetaan säädettävän tarkemmin lailla.[125] Henkilötietoja koskeva lainsäädäntö liitetään yleensä määritelmiin yksityisyyden suoja ja tietosuoja.[126] Yksityisyyden käsitettä suhteessa yksityiselämän suojaan on käsitelty lainvalmisteluaineistossa ja oikeuskirjallisuudessa eri tavoin. Yksityisyyden ja yksityiselämän käsitteitä on esimerkiksi pidetty osittain päällekkäisiä tai toistensa alle kuuluvina.[127] Vaikka henkilötietojen suoja liittyy salaisiin tiedonhankinta- ja pakkokeinoihin ainakin tietojen keräämisen osalta, on sen merkitys toimivaltuuksia arvioitaessa jäänyt taka-alalle.[128] Salaisten tiedonhankinta- ja pakkokeinojen

[123] HE 224/2010 vp, s. 31; HE 222/2010 vp, s. 113.
[124] HE 309/1993 vp, s. 53.
[125] Perustuslain viittaus henkilötietojen suojasta lailla säätämiseen viittaa tarpeeseen turvata lainsäädännöllisesti yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä. Säännös edellyttää lainsäädännöllisiä järjestelyjä henkilötietojen suojasta, eli tietosuojasta. Ks. HE 309/1993 vp, s. 53.
[126] EU:ssa astui voimaan tietosuoja-asetus (2016/679) keväällä 2018, jonka lisäksi tietosuojaan vaikuttaa erityisesti poliisin osalta rikosasioiden tietosuojadirektiivi (2016/680). Kyseisen direktiivin perusteella säädettiin laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018). Lisäksi eduskunta hyväksyi tutkimushetkellä uuden poliisia koskevan henkilötietolain, jonka on tarkoitus tulla voimaan mahdollisimman pian. Lain tarkoituksena on täydentää tietosuojadirektiivin yleistä täytäntöönpanolainsäädäntöä ja EU:n tietosuoja-asetusta siltä osin, kuin tarvittavat täytäntöönpanosäännökset eivät sisälly mainittuihin säännöksiin. Rikosasioihin liittyen uudistuksella on vaikutusta erityisesti henkilötietojen vaihdossa jäsenvaltioiden kesken.
[127] Ks. HE 75/2000 vp, s. 13, jonka mukaan yksityisyyden suojaan kuuluu yksityiselämän suoja, josta säädetään PL 10 §:ssä; Viljanen 2011, s. 392; Piispanen 1998, s. 179; Korja 2016, s. 114. Ks. myös Pitkänen – Tiilikka – Warma 2013, s. 15.
[128] Henkilötietojen suojan kannalta tärkeitä sääntelykohteita ovat ainakin rekisteröinnin tavoite, rekisteröitävien henkilötietojen sisältö, niiden sallitut käyttötarkoitukset, tietojen luovutettavuus, tietojen säilytysaika henkilörekistereissä ja rekisteröidyn oikeusturva. Sääntelyn tulee olla lain tasolla riittävän kattavaa ja yksityiskohtaista. Ks. PeVL 51/2002 vp, s. 2. Ks. myös Viljanen 2011, s. 397–398.

toimivaltuuksia arvioitaessa henkilötietojen suojan voidaankin katsoa olevan toissijainen kotirauhan, luottamuksellisen viestin ja yksityiselämän suojaan nähden.[129]

Perustuslain 10 §:n suoja ei ole ehdoton, koska kyseiseen säännökseen sisältyy niin sanotut kvalifioidut lakivaraukset. Ensinnäkin PL 10.3 §:n mukaan voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Toiseksi PL 10.4 §:n mukaan voidaan lailla 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 vahvasti uhkaa kansallista turvallisuutta.[130] Perusoikeustulkinnan osalta tärkeimpänä asiakirjana pidetään perustuslakivaliokunnan mietintöä 25/1994 vp, jossa on tiivistettynä perusoikeusteorian keskeisimmät osat. Näitä ovat perusoikeussäännösten luonne, lakivaraus- ja viittaustekniikka, säännöt perusoikeuksien rajoittamisesta tai yleisestä sääntelystä tavallisen lain tasoisesti sekä delegointiproblematiikka.[131] Mietinnöstä löytyvät myös perusoikeuksien yleiset rajoitusedellytykset, joita ovat 1) lailla säätämisen vaatimus, 2) tarkkarajaisuus- ja täsmällisyysvaatimus, 3) rajoitusperusteen hyväksyttävyys, 4) ydinalueen suoja, 5) suhteellisuusvaatimus, 6) oikeusturvajärjestelyvaatimus ja 7) ihmisoikeusvelvoitteiden noudattamisvaatimus.[132]

### 3.2 Kotirauhan suoja

Kotirauhan suojan ydinalueena on henkilön asunto, vaikka suoja sinänsä ulottuu laveammalle.[133] Kotirauhan piiri kattaa lähtökohtaisesti kaikenlaiset pysyväisluonteiseen asumiseen käytetyt tilat.[134] Esimerkiksi tuotanto- tai talousrakennukseen sisältyvä tila, joka on asumisen tarkoitettu, voidaan lukea pysyväisluonteiseksi asunnoksi.[135] Liikehuoneistot

[129] Ks. tähän liittyen uutta poliisin henkilötietolakia koskeva HE 242/2018 vp, s. 59. Siinä todetaan nimenomaisesti, että poliisin tiedonhankinnasta säädetään erikseen. Ks. myös Metsäranta 2015, s. 12, jossa hän toteaa, että henkilötietojen saaminen tapahtuu siten, että tiedonhankintakeinoilla puututaan muihin yksityiselämän suojan alueisiin. Tämän takia kyse on yksilön oikeuksien kannalta ensisijaisesti siitä, millä ehdoilla keinojen käyttö on mahdollista näiden muiden oikeuksien näkökulmasta.
[130] PL 10 §:ä muokattiin vuonna 2018 tietoliikennetiedusteluun liittyen.
[131] Ks. esimerkiksi Saraviita 2011, s. 116–117.
[132] PeVM 25/1994 vp, s. 4–5.
[133] HE 309/1993 vp, s. 53.
[134] PeVL 18/2010 vp, s. 7.
[135] PeVL 18/2006 vp, s. 4.

sinällään eivät kuitenkaan nauti kotirauhan suojaa, mutta ne voivat kuulua yksityiselämän suojan piiriin.[136] Myös yleensä lyhytaikaiseen asumiseen käytetyt tilat, kuten asuntovaunut, aluksen asumiseen käytettävät tilat, hotellit ja matkustajakodit voivat kuulua kotirauhan piiriin, jos niitä käytetään pitkäaikaiseen asumiseen. Varsinaiseen asuttuun asuntoon nähden niiden on katsottu kuitenkin kuuluvan kotirauhan suojan reuna-alueelle. Siten niistä on voinut säätää tavallisen lain säätämisjärjestyksessä, vaikka PL 10.3 §:n rajoitusedellytykset eivät ole täyttyneet.[137]

Kotirauhan piirin ulottuvuus ei ole sama kuin rikoslain 24 luvun 11 §:n määrittelyllä.[138] Kyseisen säännöksen suoja on laajempi kuin valtiosääntöoikeudellisen kotirauhan suojan.[139] Kotirauhan piiriin ulottuvista toimenpiteistä tulee säätää lailla ja niiden tulee olla välttämättömiä. Lakivaraus koskee vain perusoikeuksien turvaamista tai rikoksen selvittämistä (PL 10.3 §).[140] Vaikka säännöksessä mainitaan lakivarauksena rikosten selvittäminen, on sen katsottu kattavan laajassa mielessä myös rikosten estäminen ja paljastaminen.[141] Rikoksia ei ole erikseen rajattu, mutta on katsottu, että yleensä vain sakolla rangaistavien vähäisten rikkomusten selvittämiseksi ei suhteellisuusperiaatteen mukaisesti ole mahdollista puuttua kotirauhan suojaan.[142] Tällaisena on kuitenkin aikaisemmin pidetty rikoslain (39/1889) 17 luvun 19 §:n mukaista sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapitoa, jonka rangaistusasteikko ei säätämisaikanaan oikeuttanut kotietsinnän suorittamiseen.[143] Perusoikeuksien turvaamiseksi suoritettavia toimenpiteitä

[136] Ks. tarkemmin Metsäranta 2015, s. 40–41 ja siinä mainittu EIT:n ratkaisukäytäntö ja PeVL 5/2010 vp, s. 2–3. Ks. vakituisen ja tilapäisen asumisen rajanvedosta niin sanotun piilokonttorin osalta ratkaisusta KKO 2009:54.
[137] PeVL 8/1994 vp, s. 3; PeVL 17/1998 vp, s. 4.
[138] Kyseisen säännöksen mukaan kotirauhan suojaamia paikkoja ovat asunnot, loma-asunnot ja muut asumiseen tarkoitetut tilat, kuten hotellihuoneet, teltat, asuntovaunut ja asuttavat alukset, sekä asuintalojen porraskäytävät ja asukkaiden yksityisaluetta olevat pihat niihin välittömästi liittyvine rakennuksineen.
[139] PeVL 36/1998 vp, s. 2. Ks. myös Metsäranta 2015, s. 41–42.
[140] Perustuslakivaliokunta väljensi mietinnössään hallituksen esityksessä olleen sanamuodon ”tarkastuksia” muotoon ”toimenpiteitä”, mutta korosti samalla vastapainona välttämättömyysedellytystä, jotta asiasta voidaan säätää tavallisella lailla. Ks. PeVM 25/1994 vp, s. 8. Ks. välttämättömyysvaatimuksesta tarkemmin Viljanen 2011, s. 404–405.
[141] Perustuslakivaliokunta on pitänyt rikosten selvittämisenä myös sellaisia toimenpiteitä, joihin ryhdytään jonkin konkreettisen ja yksilöidyn rikosepäilyn johdosta, vaikka rikos ei olisi vielä ehtinyt toteutuneen teon asteelle. Ks. esimerkiksi PeVL 2/1996 vp, s. 2; PeVL 66/2010 vp, s. 7.
[142] PeVL 40/2002 vp, s. 2.
[143] Perustuslakivaliokunta katsoi hallussapitorikoksen luonteen vaativan kotietsinnän mahdollisuutta, jotta rangaistussäännöstä on mahdollista edes jollakin vaikuttavuudella valvoa, jonka takia välttämättömyysedellytys täyttyi. Ks. PeVL 23/1997 vp, s. 4. Ks. myös PeVL 69/2002 vp, s. 2–3, jossa kotirauhan piiriin ulottuva toimenpide katsottiin mahdolliseksi myös pelkän sakkorangaistusuhkaisen rikkomuksen osalta.

voivat olla esimerkiksi palotarkastuksen suorittamiseen, onnettomuustutkintaan tai ampuma-aseiden säilyttämiseen liittyvät tarkastukset.[144]

Vaikka kotirauhan suoja on yleisesti merkittävässä roolissa salaisten tiedonhankinta- ja pakkokeinoja koskevassa sääntelyssä, ei sen vaikutus ulotu juurikaan tietoverkkoihin. Kotirauhan suoja on alun perinkin muodostettu palvelemaan muita tarkoitusperiä kuin antamaan suojaa modernin tekniikan muodostamia uhkia vastaan.[145] Tietoverkoissa voi syntyä tilanteita, joissa poliisi- tai peiteprofiililla päästään seuraamaan kohteen toimintaa kotirauhan piiriin kuuluvalla alueella tai asutussa asunnossa. Selkeimpänä esimerkkinä toimii webkamera-yhteys kohdehenkilöön, joka oleskelee asunnossaan kyseisellä hetkellä. Lisäksi tietoverkkoihin liittyvät nykyään erilaiset kodinkoneet ja laitteet, joiden kautta on mahdollista kuunnella, katsella ja kerätä tietoja henkilöistä. Esimerkiksi Googlen on tiedetty kuuntelevan älypuhelimen kautta käyttäjiä, mutta kyseisenlaisia laitteita voivat olla myös televisio, tietokoneen webkamera ja muut tietoverkkoihin liitetyt laitteet.[146]

Esimerkkinä kotirauhan suojaan ja tietoverkkoihin liittyen voidaan mainita tilanne, jossa suunnitelmallista tarkkailua suorittava poliisimies pääsee sattumalta seuraamaan kohdehenkilön itsensä asunnosta lähettämää reaaliaikaista striimausta.[147] Tällaisen toiminnan mahdollistava palvelu on esimerkiksi Periscope, jossa käyttäjillä on mahdollisuus lähettää suoraa videokuvaa käyttäjille ympäri maailmaa.[148] Koska kyseinen suoratoisto voi tapahtua tarkkailtavan asunnosta käsin, voisi poliisimiehen toiminta teoriassa rinnastua teknistä tarkkailua koskeviin säännöksiin, jossa vain pakkokeinolain osalta on mahdollista suorittaa asuntokuuntelua (PKL 10:17). Lisäksi on huomioitava, että vakituiseen asumiseen käytettävään tilaan ei voi kohdistaa teknistä katselua lainkaan (PKL 10:19.2). Jos analogiaa tulkintaan yrittää hakea reaalimaailman puolelta, ei esimerkiksi verhojen aukaisulla ja siten paremman näkyvyyden mahdollistamisella asuntoon ole merkitystä toimivaltuuden käytölle. Poliisimies ei saa tällöinkään kohdistaa tarkkailua vakituiseen asumiseen käytettävään tilaan (PolL 5:13.4 ja PKL 10:12.4).

---

[144] PeVL 31/1998 vp, s. 2.; PeVL 18/2010 vp, s. 7–8. Ks. myös PeVL 34/2009 vp, s. 3, jossa eläinten hyvinvoinnin vaarantamista ei voitu pitää PL 10.3 §;n mukaisena perusoikeuksien turvaamisena.
[145] HaVL 5/1994 vp, s.5.
[146] Ks. tarkemmin Mitnick 2017, s. 203–214.
[147] Striimauksella tarkoitetaan suoratoistoa, jossa käyttäjä lähettää videokuvaa muille käyttäjille. Kyseessä voi olla live-striimaus, jossa videokuvaa lähetetään reaaliaikaisesti. Vaihtoehtoisesti kyseessä voi olla tallenne, joka rinnastuu normaaliin videotallenteeseen.
[148] Samanlainen mahdollisuus on myös useissa muissa palveluissa, kuten Facebook, YouTube ja pelaajien suosima Twich, jossa lähetetään monesti videokuvaa omasta pelaamisesta.

On kuitenkin käytännössä eri asia lähettää omasta asunnosta koko maailmalle julkista videokuvaa, kuin pitää esimerkin mukaisesti verhoja auki. Tämä sen takia, että tieto perustuu kohdehenkilön tietoiseen julkaisupäätökseen. Reaalimaailman ja tietoverkkojen osalta tuleekin erottaa julkisuus ja julkaiseminen. Kotirauhan suojan alueella tapahtuvan julkaisutoiminnan voidaan tämän takia katsoa rinnastuvan ennemminkin toimintaan julkisella paikalla, kuin kotirauhan suojaamalla alueella. Näissä tilanteissa kohdehenkilön tulee sovittaa oma käyttäytymisensä vallitseviin olosuhteisiin.[149] Poliisin tiedonhankintaa ei olekaan pidettävä kotirauhan suojaan puuttuvana keinona, vaikka poliisin on mahdollista kuulla ja nähdä mitä asunnossa tapahtuu, jos tarkkailu perustuu kohdehenkilön omaan julkaisupäätökseen.

Tätä tulkintaa tukee myös poliisi- ja pakkokeinolaissa ilmi tuotu linjaus siitä, että henkilön tarkkailu tietoverkossa tietokoneen avulla ei ole teknistä tarkkailua, vaan kysymys on kyseiseen toimintaympäristöön liittyvästä erityispiirteestä, jossa tietokonetta käytetään muiden käyttäjien tavoin.[150] Jos tulkinta olisi vastakkainen, tulisi myös asunnossa kuvatun ja televisiossa lähetetyn ohjelman seuraamista pitää kotirauhan suojaan puuttuvana. Sama koskisi myös asunnossa otettuja valokuvia, joita julkaistaan tietoverkoissa. Tämä ei ole ollut lainsäätäjän tarkoitus kotirauhan suojaa säädettäessä. Myöskään muun kuin asunnon haltijan kohteesta lähettämä videokuvan seuraamista ei voida katsoa kotirauhan suojaan puuttuvaksi toiminnaksi, jos se tapahtuu ilman poliisin ohjausta.[151] Joka tapauksessa näissä tilanteissa kohdehenkilön toiminta nauttii yksityiselämän suojaa, koska jo tiedon keräämisen on katsottu puuttuvan yksityiselämän suojaan.[152]

Poikkeuksen yllä esitettyyn tulkintaan muodostavat tilanteet, joissa tietoverkoissa toimiva poliisimies yllyttää kohdetta tai muuta asunnossa oleskelevaa henkilöä avaamaan

[149] Ks. HE 22/1994 vp, s. 15, jonka mukaan yleisellä paikalla oleskelevan tulee ottaa huomioon se, että hän voi olla kanssaihmisten jatkuvan tarkkailun alla, jonka takia myös salaisia tiedonhankinta- ja paikkokeinojen käyttö on kyseisillä alueilla sallitumpaa.

[150] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.

[151] Ks. tähän liittyen *Shannon v. Yhdistynyt kuningaskunta* (2005), jossa toimittaja oli nauhoittanut ja videoinut salaa hotellihuoneessa huumausainekauppaan liittyvät tapahtuvat ja luovuttanut nämä poliisille. Koska toimittaja ei ollut toiminut poliisin toimeksiannosta tai muutoinkaan poliisin ohjaamana, sai poliisi käyttää aineistoa näyttönä. Sama tulkinta koskee tilannetta, jossa kodin valvontajärjestelmä on hakkeroitu ja siitä lähetetään kuvaa julkisesti internetissä jonkun muun toimesta. Ks. Iltalehti 2017, jossa uutisen mukaan yhdelle sivustolle oli kerätty tuhansien suojaamattomien valvontakameroiden suoraa videokuvaa, joista osa lähetti kuvaa julkisilta paikoilta, mutta osa myös asunnoista. Mukana oli myös useita suomalaisia kohteita.

[152] Jo pelkkä tietojen keruu voidaan katsoa yksityiselämän suojaan puuttumiseksi. Ks. tiedon keräämisen ja sen tallentamisen vaikutuksesta yksityiselämän suojaan esimerkiksi HE 57/1994 vp, s. 15 ja 56. Ks. myös Helminen – Kuusimäki – Salminen 1999, s. 45. Ks. myös PeVL 11/2005 vp, s. 5, jonka mukaan yksityiselämän suojan lähtökohtana on se, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten ja ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista siihen.

videoyhteyden asuntoon, jotta poliisilla olisi mahdollista seurata tapahtumia asunnossa.[153] Poliisimies ei saa kiertää toimivaltuuksia pyytämällä toista henkilöä tekemään toimia, joihin poliisilla tulisi olla toimivaltuus, joten tällainen yllytys tai pyytäminen ei ole käytännössä mahdollista.[154] Samaan kielletyn toiminnan kategoriaan menevät myös tilanteet, joissa poliisimies asentaa PolL 5:26:n tai PKL 10:26:n mukaisesti ohjelmiston kohteen pöytätietokoneelle tai muuhun laitteeseen, ja ottaa sen hallintaansa siten, että poliisimies voi kuunnella ja katsella webkameran kautta asunnon tapahtumia.[155]

### 3.3 Luottamuksellisen viestin suoja

Perustuslain 10.2 §:n suojaa luottamuksellista viestintää väline- ja teknologianeutraalisti. Ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta, mutta säännös antaa suojaa muillekin viestiä koskeville tiedoille, joilla voi olla merkitystä viestin säilymiselle luottamuksellisena. Näitä ovat esimerkiksi puhelujen tunnistamistiedot.[156] Toisaalta perustuslakivaliokunta ei ole pitänyt luottamuksellisena viestintänä toiminnan luonteen ja viestien taltiointia koskevan tietoisuuden takia esimerkiksi kulkuneuvon ohjaajan ja liikenteenohjauksen välistä viestinliikennettä.[157] Säännös ei myöskään suojaa tavallisella kuuloetäisyydellä käytävän keskustelun sisältöä ulkopuolisilta, mutta luottamukselliseksi tarkoitetun keskustelun kuunteleminen teknisin apuvälinein on puuttumista säännöksessä turvattuihin oikeushyviin. Säännös ei suojaa pelkästään viestin lähettäjää, vaan kyseessä on molempien viestinnän osapuolten perusoikeus. Toisaalta viestinnän osapuoli voi julkistaa luottamuksellisen viestin ja kyseiset tilanteet jäävät muilla perusteilla ratkaistavaksi.[158]

---

[153] Lain mukaan poliisilla ei ole mahdollista suorittaa teknistä katselua tai edes normaalein näköhavainnoin asunnon sisälle, joten tähän yllyttäessään poliisi voisi syyllistyä virkarikokseen.
[154] Ks. HE 57/1994 vp, s. 61–62, jossa nimenomaan kielletään tekninen tarkkailu toisen henkilön myötävaikutuksella. Ks. myös *van Vondel v. Alankomaat* (2007), kohta 49, jossa poliisin opastuksella ja heidän antamilla laitteilla tapahtunut keskustelun nauhoitus tulkittiin EIS:n 8 artiklan vastaiseksi toiminnaksi.
[155] Ks. esimerkiksi Ilta-Sanomat 2019, jossa kerrotaan Googlen Nest-kameraa käyttäville asiakkailleen lähettämästä viestistä, jossa se kehottaa vaihtamaan laitteiden salasanat ja ottamaan käyttöön kaksivaiheisen tunnistautumisen. Esille oli tullut tapauksia, joissa valvontakameroihin oli päästy käsiksi ulkopuolisen tahon toimesta ja saatu katseltua toimintaa asunnossa. Yhdessä tapauksessa Nest-kameran kaiuttimesta oli alkanut kuulua kovaääninen varoitus ydinohjushyökkäyksestä Yhdysvaltoihin, joka oli luonnollisesti paljastunut myöhemmin pilaksi.
[156] HE 309/1993 vp, s. 53.
[157] Tämä siitäkin riippumatta, että myös tällaisessa viestinnässä voidaan sinänsä välittää myös luottamuksellisia viestejä henkilöiden välillä. Ks. tarkemmin PeVL 62/2010 vp, s. 5.
[158] HE 309/1993 vp, s. 53–54.

Luottamuksellisen viestin salaisuutta voidaan rajoittaa oikeudenkäynnissä, yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana. Vuonna 2018 uutena rajoittamisperusteena säännöksen tuli tietoliikennetiedusteluun liittyen tiedon hankkiminen sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vahvasti uhkaa kansallista turvallisuutta.[159] Oikeudenkäynnissä luottamuksellista viestintää voidaan rajoittaa esimerkiksi oikeudenkäymiskaaren (4/1734) 17 luvun sääntelyyn liittyen velvollisuudesta esittää yksityinen asiakirja tai tallenne oikeudenkäynnissä.[160] Yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten piiriin kuuluvat esimerkiksi huumausainerikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetosrikokset.[161] Turvallisuustarkastukset voivat tulla kyseeseen esimerkiksi kansainvälisten kokousten järjestelyjen yhteydessä.[162] Vapaudenmenetyksen aikana tapahtuvalla luottamuksellisen viestinnän rajoituksena tarkoitetaan pidätyksen, tutkintavankeuden tai vankeusrangaistuksen aikana puuttumista luottamukselliseen viestintään. Lisäksi määritelmän alle sisältyy mielisairaalassa tai muussa vastaavassa laitoksessa hoidettavana olevat sekä lastensuojeluun liittyvän lainsäädännön perusteella huostaan otetut. Kaikkia näitä rajoituksia koskee välttämättömyysedellytys ja rajoituksesta on säädettävä lailla.[163]

Sotilaallisella toiminnalla tarkoitetaan sotilaallisesti järjestäytyneiden joukkojen toimintaa tai sotilaallisin voimakeinoin, kuten aseistukseen ja sotatarvikkeisiin liittyvää toimintaa taikka muuta näihin rinnastuvaa, sotavoimaa käyttävien joukkojen toimintaa. Sillä ei ole väliä, onko kyse valtiollisesta toiminnasta vai ei.[164] Valtiollisella toiminnalla tarkoitetaan vieraan valtion asevoimien toimintaa tai siihen rinnastuvaa kansainvälisen, sotilaallisen liittouman tai järjestön toimintaa, kun taas ei-valtiollinen toiminta on sellaista sotilaallisesti

[159] Samalla käsite ”rikosten tutkinta” oli tarkoitus muuttaa muotoon ”rikosten torjunta”. Perustuslakivaliokunta ei pitänyt käsitteen muutosta tarpeellisena. Sanamuoto ”rikosten torjunta” viittasi entistä enemmän painopisteen siirtymisen ennalta estävään toimintaan, eikä tämä ollut tarkoitus. Lisäksi kotirauhan suojan rajoitusperusteeseen liittyvää rikoksen selvittäminen -käsitettäkään ei olisi muutettu, vaikka sen osalta problematiikka oli samanlainen. Ks. tarkemmin PeVM 4/2018 vp, s. 5–6 ja siinä mainitut perustuslakivaliokunnan lausunnot.

[160] HE 309/1993 vp, s.55. Ks. myös PeVL 13/2003 vp, s. 4–5, jossa luottamuksellisen viestinnän salaisuutta katsottiin voivan rajoittaa konkurssimenettelyssä osana oikeudenkäyntiä, vaikka kyse oli konkurssipesän pesänhoitajan oikeudesta avata velalliselle osoitetut pesän selvittämiseen liittyvät viestit.

[161] Tällaisia rikoksia ovat myös useimpien rikosten törkeät tekomuodot, vapauteen kohdistuvat rikokset ja petosrikokset. Ks. tarkemmin HE 198/2017 vp, s. 6–7.

[162] HE 309/1993 vp, s. 55. Ks. myös PeVL 56/2010 vp, s. 4, jonka mukaan postilähetys voidaan avata, jos se saattaa aiheuttaa vaaraa terveydelle tai omaisuudelle. Lisäksi PeVL 36/2017 vp, s. 4 mukaan niin sanotun rynnäkkötarkkailun katsotaan kuuluvan turvallisuustarkastuksen piiriin.

[163] HE 309/1993 vp, s. 54–55.

[164] Kyseessä on myös itsenäinen rajoitussäännös suhteessa vakavaan uhkaan kansalliselle turvallisuudelle. Kyseistä asiaa perustellaan sillä, että sotilaallista toimintaa on usein tarpeen seurata pitkäjänteisesti ja systemaattisesti ilman, että seurattavan toiminnan tarvitsisi olla välittömästi uhkaavaa seurannan aikana.

järjestettyä, aseistettua tai varustettua toimintaa, jolla ei ole edellä tarkoitettua valtiollista alkuperää tai sitä ei voida tunnistaa.[165] Muulla toiminnalla, joka vakavasti uhkaa kansallista turvallisuutta, tarkoitetaan suppeasti kuvattuna kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä taikka kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Lisäedellytyksen on se, että toiminnalla on joku kytkentä Suomeen ja että se uhkaa nimenomaan Suomen kansallista turvallisuutta, vaikka toiminta tapahtuisi Suomen rajojen ulkopuolella.[166]

Perustuslain 10.2 §:ssä on mainittu vain kirje, puhelu ja muu luottamuksellinen viesti suojan piiriin kuuluvina. Lähtökohtana on kuitenkin se, että säännöksellä turvataan yleisesti kaikenlaisen luottamuksellisen viestinnän salaisuutta väline- ja teknologianeutraalisti myös tietoverkoissa.[167] Tietoverkkoihin liittyvä sähköinen viesti määritellään sähköisen viestinnän palveluista annetun lain (917/2014, LSVP) 3.1,22 §:n mukaan tiedoksi, joka välitetään tai jaetaan sähköisesti. Luottamuksellista viestiä tietoverkoissa voidaan pitää verkkoviestin vastakohtana. Verkkoviestin määritelmästä säädetään sananvapauden käyttämisestä joukkoviestinnässä annetun lain (460/2004, SVL) 2 §:n 1 momentin 2 kohdassa, jonka mukaan verkkoviestillä tarkoitetaan radioaaltojen, sähköisen viestintäverkon tai muun vastaavan teknisen järjestelyn avulla yleisön saataville toimitettua tietoa, mielipidettä tai muuta viestiä. Yleisöllä tarkoitetaan SVL 2.1,1 §:n mukaan vapaasti valikoituvaa viestin vastaanottajien joukkoa. Viestin sisällölle ei ole lainsäädännössä vakiintunutta määritelmää, mutta yleensä kyse on sen semanttisesta sisällöstä.[168] Kyse voi olla esimerkiksi puheesta, kirjoituksesta tai kuvista.[169]

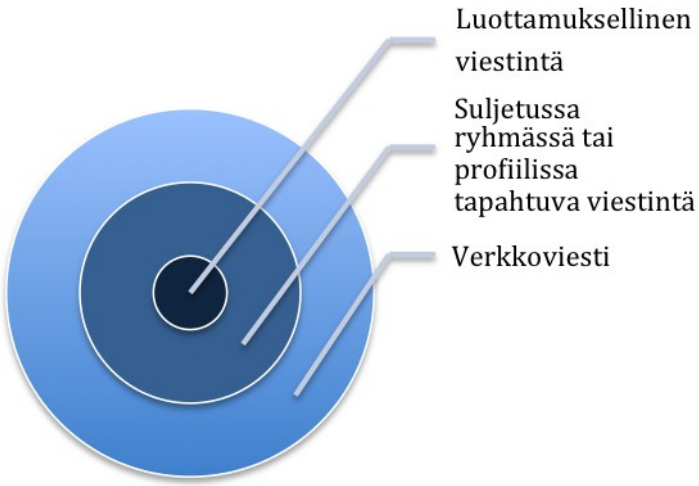
Luottamuksellisen viestin ja verkkoviestin eroa on arvioitu ennen sosiaalisen median yleistymistä hallituksen esityksessä 125/2003 vp. Kyseisten esitöiden mukaan keskeisintä arvioidessa viestin luottamuksellisuutta on se, onko viestin lähettäjä saattanut viestin yleisesti vastaanotettavaksi, esimerkiksi keskustelupalstalle tai mielipidepalstalle. Jos lähettäjä ei ole saattanut viestiä yleisesti vastaanotettavaksi, viestin oletetaan olevan

[165] HE 198/2017 vp, s. 34–35.
[166] Ks. tarkemmin kyseisen käsitteen sisällöstä HE 198/2017 vp, s. 35–37.
[167] Tekninen kehitys oli huomioitu jo perustuslakiuudistuksessa HE 309/1993 vp, s. 53, jolloin sosiaalisen median käsite oli vielä kaukana tulevaisuudessa. Teknologianeutraalius on todettu myös tietoliikennetiedustelua koskevassa perutuslain 10 §:n muutosta koskevassa hallituksen esityksessä 198/2017 vp, s. 5. Ks. myös telekuuntelun mahdollistanut hallituksen esitys HE 22/1994 vp, s. 4, jossa mainitaan tietokoneiden välinen datasiirto luottamuksellisen viestinnnän suojaan liittyen. Ks. myös rikoslaissa säädetyn viestintäsalaisuuden loukkauksen kohdalla tietokoneiden välisen sähköisen viestinnän suojaamisesta HE 94/1993 vp, s. 149.
[168] HE 202/2017 vp, s. 241.
[169] HE 309/1993 vp, s. 53.

luottamuksellinen. Myöskään vastaanottajien lukumäärällä ei katsottu olevan merkitystä arvioitaessa viestin luottamuksellisuutta, joten esimerkiksi useammalle henkilölle lähetetty sähköposti olisi luottamuksellinen, jos sitä ei ole saatettu yleisesti vastaanotettavaksi.[170] Kyseinen linjaus on tehty ennen sosiaalisen median käytön yleistymistä ja onkin erityisesti sosiaalisen median kannalta ongelmallinen, koska viestinnän avoimuudella on useita eri tasoja ja viestejä on helppo lähettää useille sadoille henkilöille yhdellä kertaa.[171]

Erityisesti sosiaalisen median viestintämahdollisuuksien monimuotoisuus on ainakin osittain hämärtänyt luottamuksellisen viestin suojan rajoja, koska luottamuksellisen viestin ja verkkoviestin väliin jää tietty harmaa alue. Lainsäätäjä ei ole käsitellyt asiaa kuin lyhyesti välitystietoihin liittyen.[172] Oikeuskirjallisuudessa sosiaalisen median ryhmissä tapahtuva viestintä on yleensä jaettu suhteellisen mustavalkoisesti luottamuksellisen ja kaikille avoimen viestinnän välillä, jossa ryhmissä tapahtuvan viestinnän ei ole yleensä katsottu olevan luottamuksellista.[173] Sähköisen viestinnän vertaaminen perinteiseen viestintään on katsottu myös muutoin haastavaksi, koska analogioiden löytäminen reaalimaailman ja tietoverkkojen välillä on ongelmallista myös julkaisutoiminnan osalta.[174] Viestinnän luottamuksellisuuden problematiikka tietoverkoissa poliisi- ja peiteprofiilien osalta voidaankin karkeasti jakaa 1) luottamukselliseen viestintään, 2) suljetussa ryhmässä tai profiilissa tapahtuvaan viestintään ja 3) verkkoviestiin, jota voidaan havainnollistaa yksityiselämän suojan tarpeen näkökulmasta seuraavalla kuviolla.

[170] HE 125/2003 vp, s. 51.
[171] Suomessa ensimmäinen sosiaalisen median palvelu oli IRC-Galleria, joka perustettiin vuonna 2000. Facebook perustettiin vuonna 2004, mutta meni vielä useampi vuosi, ennen kuin siitä tuli globaalisti suosittu palvelu. Palvelut ovat myös koko ajan muuttaneet muotoaan, joka on vaikuttanut myös viestintäominaisuuksiin.
[172] Ks. välitystietojen käsittelymahdollisuuksien liittyen hallituksen esitys 221/2013 vp, s. 153, jossa todetaan Facebookin tarjoavan käyttäjilleen rajatulle piirille tapahtuvan viestinnän lisäksi kaikille avoimen viestinnän mahdollisuutta, jonka takia palveluntarjoajan suhde viestintätapahtumaan tulisi arvioida tapauskohtaisesti. Esitöissä ei avattu tarkemmin erilaisten ryhmien luottamuksellisen viestinnän tasoja, jotka vaikuttavat kyseiseen tulkintaan.
[173] Ks. esimerkiksi Pesonen 2017, s. 74–75, jossa hän jakaa viestinnän suljetussa piirissä, yhdeltä yhdelle, yhdeltä monelle ja yhdeltä koko verkkomaailmalle viestimiseen. Ks. myös Voutilainen 2012, s. 338.
[174] Ks. tarkemmin Innanen – Saarimäki 2012, s. 32–33.




Kuvio 2. Tietoverkkojen luottamukselliseen viestintään liittyvät suojaamistarpeen tasot

*Luottamuksellisia viestejä* ovat selvimmin kaikki yksittäisille tai muutamille käyttäjille lähetetyt yksityisviestit erilaisissa sosiaalisen median palveluissa, koska lähettäjä on tarkoittanut viestin vain kyseisille henkilöille. Suojaa saa anonyymi viestintä siinä missä omalla nimellä ja kasvoilla tapahtuva viestintä.[175] Mahdollisella viestin salaamisella ei ole myöskään vaikutusta viestinnän luottamuksellisuuteen tai salaisten tiedonhankinta- tai pakkokeinojen käyttöön.[176] Viestin sisällöllä ja viestijällä voi kuitenkin olla merkitystä luottamuksellisen viestinnän suojan tasoon, niin kuin alussa tuotiin jo ilmi. Lainsäätäjä ei ole toiminnan ammattimaisen luonteen ja viestin taltiointia koskevan tietoisuuden takia pitänyt luottamuksellisena viestintänä kulkuneuvon ohjaajan ja liikenteenohjauksen välisestä viestinliikennettä.[177] Erityisesti viestien taltiointi on ominaista tietoverkoille, jossa sosiaalisen median palveluilla on hallussa suuria määriä tietoja käyttäjien viestinnästä. Merkitystä perusoikeussuojan kannalta on katsottu olevan myös sillä, että viestijänä on vieras valtiotoimija tai siihen rinnastuva taho taikka haittaohjelmaliikenne.[178] Lisäksi voidaan mainita viestintäsalaisuuden loukkausta (RL 38:3) koskeva sääntely, jossa mainos- ja massakirjeillä on katsottu olevan heikompi suojan tarve.[179] Vahvempaa suojaa taas on katsottu nauttivan kirjeenvaihto asianajajan kanssa, joka sekään ei ole rajoittamaton.[180]

[175] Ks. esimerkiksi PeVL 9/2004 vp, s. 7.
[176] HE 224/2010 vp, s. 93–94; HE 222/2010 vp, s. 317.
[177] Tämä siitäkin riippumatta, että myös tällaisessa viestinnässä voidaan sinänsä välittää myös luottamuksellisia viestejä henkilöiden välillä. Ks. tarkemmin PeVL 62/2010 vp, s. 5. Ks. myös HE 198/2017 vp, s. 5.
[178] Ks. tarkemmin tietoliikennetiedusteluun liittyen HE 202/2017 vp, s. 239–240.
[179] HE 94/1993 vp, s. 149.
[180] Ks. *Michaud v. Ranska* (2012), kohta 118. Ks. myös vankien kirjeenvaihdon rajoittamisesta ja siihen liittyvästä EIT:n ratkaisukäytännöstä tarkemmin Gullans 2018, s. 836–838.

*Pönkä* on jakanut avoimuuden asteet sosiaalisessa mediassa seuraavasti: 1) täysin avoin, 2) osittain avoin, 3) suljettu, vaatii rekisteröinnin, 4) suljettu, vaatii ylläpitäjän hyväksynnän, 5) suljettu, vaatii ylläpitäjän kutsun sekä 6) suljettu ja salainen.[181] Ensimmäisen kohdan tilanteessa kyse on ryhmästä tai keskustelupalstasta, jossa kaikki käyttäjät voivat lukea, muokata ja lisätä sisältöä. Toisessa kohdassa vain jäseneksi hyväksytyt voivat lisätä sisältöä, mutta muut pääsevät lukemaan toisten viestejä. Kolmannen ominaisuuden kohdalla kuka tahansa voi liittyä rekisteröitymällä verkkoympäristöön, jonka jälkeen heille aukeaa mahdollisuus lukea, muokata ja lisätä sisältöä. Tällaisia ovat yleensä erilaiset keskustelupalstat, joissa voi olla ykköskohdan mukaisten kaikille avoimien palstojen lisäksi rekisteröitymistä vaativia palstoja, joihin kaikilla on kuitenkin mahdollisuus rekisteröityä. Neljäs kohta vastaa kolmoskohtaa sillä erotuksella, että liittyminen vaatii ylläpitäjän hyväksynnän. Viides kohta taas vastaa neloskohtaa, mutta kutsun ryhmään liittymiseen tulee tapahtua ylläpitäjän toimesta.[182] Viimeisen kohdan mukaisia ovat suljetut ja salaiset ryhmät, jotka eivät ole löydettävissä erilaisilla hakukoneilla ja edellisen kohdan tapaan vaativat kutsun ryhmään liittymiseksi ylläpitäjältä.[183] Näitä ovat esimerkiksi Facebookin salaiset ryhmät ja whatsapp-ryhmät. Lisäksi voidaan mainita palvelut, joissa 7) ryhmään pääsy perustuu paikkatietoon. Tällainen on muun muassa anonyymi keskustelupalvelu Jodel, jossa voi lähettää viestejä muun muassa 10 kilometrin säteellä oleville käyttäjille.[184]

Pöngän jaottelussa on kyse lähinnä yleisestä mahdollisuudesta lukea, muokata ja lisätä tietoa tiettyyn ryhmään. Jos viestit ovat suoraan kaikkien nähtävillä, on kyse luonnollisesti *verkkoviestistä*. Sama tulkinta koskee myös tilanteita, joissa ei ole mahdollista muokata sisältöä, mutta kuitenkin mahdollisuus lukea viestit. Ensimmäinen epäselvyys viestinnän luottamuksellisuudessa syntyy Pöngän luokittelun kolmoskohdan mukaisissa tilanteissa, joissa vasta ryhmään liittymällä saadaan mahdollisuus lukea viestit. Jos kaikilla on mahdollisuus liittyä ryhmään ja jos aikaisemmin julkaistut viestit ovat nähtävissä myöhemmin liittyvien toimesta, voidaan kyseinen viestintä rinnastaa julkisessa tilassa kuuloetäisyydellä käytävään keskusteluun tai kovaääniseen puheluun. Viestinnän vastaanottajien voidaan katsoa määräytyvän satunnaisin syistä, riippuen siitä kuka sattuu

[181] Pönkä jaottelee avoimuuden asteet myös yksinkertaisemmalla tavalla, jossa erotetaan 1) täysin julkinen tila, 2) yhteisöön liittyneiden jäsenten suljettu tila sekä 3) yhteisön sisäpiiriläisten tai ylläpitäjien suljettu ja salainen tila.

[182] Ryhmä voi kuitenkin olla julkisesti löydettävissä, vaikka viestintä ryhmässä ei välttämättä näy ulkopuolisille.

[183] Pönkä 2014, s. 166–167.

[184] Myös deittisovellus Tinder perustuu paikkatietoon, jossa treffikumppaneita voidaan etsiä tietyllä säteellä omasta sijainnista. Aikaisemmin sovelluksessa oli myös mahdollista ryhmäkeskusteluihin.

liittymään ryhmään tai poistumaan sieltä. Kyseisenlainen viestintä ei nauti luottamuksellisen viestinnän suojaa, koska kyse on verkkoviestistä.[185] Samanlainen problematiikka koskee osittain myös yksittäistä profiilia. Jos palvelun ominaisuuksiin kuuluu se, että profiilissa julkaistut tiedot ovat kaikkien myös myöhemmin kaverilistalle hyväksyttyjen nähtävissä, on kyse lähtökohtaisesti verkkoviestistä.[186]

Pöngän jaottelun kohtien 3–6 mukaisissa tilanteissa tulkinta tulisi tehdä ensinnäkin sillä perusteella, 1) onko aikaisempi viestintä nähtävissä ryhmään tai profiilin kaverilistalle uutena hyväksytyille. Merkitystä on myös sillä, 2) kuinka laajasta ryhmästä tai kaverilistasta on kyse ja 3) mitä tarkoitusta varten ryhmä tai profiili on luotu. Lisäksi ryhmän tai kaverilistan 4) hyväksymisprosessilla voidaan katsoa olevan merkitystä viestinnän luottamuksellisuudelle. Kyseistä problematiikkaa voidaan luonnehtia *suljetussa ryhmässä tai profiilissa tapahtuvaksi viestinnäksi*, joka jää luottamuksellisen viestinnän ja verkkoviestin välimaastoon. Vaikka viestintää ei tulkittaisi näissä tilanteissa luottamuksellisen viestin suojan piiriin kuuluvaksi, voidaan viestinnän katsoa vähintään nauttivan vahvempaa yksityiselämän suojaa kuin verkkoviestin.

Jos viesti ei ole nähtävissä muille kuin sen lähetyshetkellä valikoituneille vastaanottajille, voidaan tämän katsoa tukevan vahvasti viestinnän luottamuksellisuutta.[187] Sillä, että viestiä voi olla helppo jakaa eteenpäin kuvakaappauksin, ei ole merkitystä. Myös sähköpostiviestiä tai muuta luottamuksellista viestiä on viestinnän osapuolen toimesta mahdollisuus välittää joko normaalein palvelun välitystoiminnoin tai kuvakaappauksin LSVP 136.1 §:n perusteella eteenpäin, mutta tällöin kyse on jo uudesta viestistä. Jos viestintä tapahtuu profiilissa tai ryhmässä jossa on tuhansia vastaanottajia, voidaan tällä katsoa olevan heikentävä vaikutus viestinnän luottamuksellisuuteen, vaikka viestijä sinänsä tarkoittaisikin viestinsä vain kyseisille henkilöille.[188] Ryhmän tai profiilin osallisten lukumäärällä on suora vaikutus siihen, miten sen jäsenet luottavat toisiinsa ja tämä näkyy myös viestinnässä.[189]

Ryhmän tai profiilin luomisen tarkoituksella viittaan siihen, onko kyseessä esimerkiksi perheen sisäiseen käyttöön luotu ryhmä, tietty luokkakavereiden keskusteluryhmä,

[185] Ks. HE 309/1993 vp, s. 53; HE 224/2010 vp, s. 105 ja 95; HE 222/2010 vp, s. 319 ja 329.
[186] Tähän voi tehdä poikkeuksen tilanteet, joissa ryhmä tai erityisesti yksittäisen profiililin kaverilista on erittäin suppea. Aiheeseen palataan tarkemmin vielä myöhemmin.
[187] Ks. HE 125/2003 vp, s. 51.
[188] Toiminta menee tällöin lähemmäs aikaisemmin mainittua HE 309/1993 vp, s. 53 liittyvää mainos- ja massakirjemäistä toimintaa, joiden luottamuksellisen viestinnän suoja on lähtökohtaisesti heikompi.
[189] Pönkä 2014, s. 167.

harrastuksiin liittyvä ryhmä tai poliittisen keskustelun alusta. Tämä määrittää yleensä sen, kuinka arkaluontoisia tietoja ryhmässä tai profiilissa jaetaan.[190] Viestinnän luottamuksellisuuden ja yksityiselämän suojan näkökulma korostuu erityisesti tilanteissa, joissa ryhmässä on vain toisensa tuntevia jäseniä, jotka ovat luoneet alustan nimenomaan keskinäistä vuorovaikutusta varten. Suojan ydinalueelta kauemmas taas menevät tilanteet, joissa kyse on satunnaisten henkilöiden tietyn aihepiiriin ympärille luodusta keskustelualustasta. Profiilien kohdalla kyseessä voi olla normaalin kansalaisen yksityiskäyttöön luotu profiili, mutta myös työkäyttöön, julkisuuden henkilön tai vaikka poliitikon yleistä viestintää varten luoma profiili, joka on kuitenkin rajoitettu nähtäväksi vain kaverilistalla oleville.[191] Mitä selvemmin profiili liittyy perhe-elämään ja läheisten kanssa tapahtuvaan vuorovaikutukseen, sitä selvemmin se kuuluu yksityiselämän suojan ydinalueelle.

Hyväksymisprosessin näkökulmasta yksityiselämän suojan nökökulma on yleensä vahvimmin käsillä yksittäisessä profiilissa tapahtuvan ja kavereille suunnatun viestinnän osalta. Suojan tarvetta puoltaa nimenomaan tietyille henkilöille kohdistettu viestintä, jossa viestin lähettäjällä on ainoana vastaanottajien valikoitumiseen liittyvä vaikutusvalta. Ryhmien osalta hyväksymisprosessi on yhteydessä ryhmän tarkoitukseen. Jos ryhmä on esimerkiksi tarkoitettu tiettyyn harrastukseen liittyvään keskusteluun, on oletettavaa, että ryhmään hyväksytään kaikki halukkaat. Tästä taas poikkeaa esimerkiksi tietyn työvuoron ryhmään hyväksytä, johon pääsee vain kaikki kyseisen työvuoron henkilöt.[192] Kärjistettynä esimerkkinä voidaan mainita tilanne, jossa viestin lähettäjän on tarkoitus kommentoida tiettyä asiaa ryhmässä kahdella eri viestillä. Ensimmäisen ja toisen viestin välissä ryhmän ylläpitäjä voi hyväksyä ryhmään uusia henkilöitä, joten viestinnän vastaanottajat

[190] Ks. tietoverkkojen sosiaalisten verkostojen perusteista ja syntymistavoista tarkemmin Pönkä 2014, s. 170–175.

[191] Ks. esimerkiksi Heinonen – Hannula 1999, s. 25, jotka erottavat tietoverkoissa roolit kansalaisena, työntekijänä ja kuluttajana. Esimerkkinä työprofiilista voidaan mainita nettipoliisi, jonka päivitykset Facebookissa on voitu sulkea vain kaverilistalla olevien nähtäväksi. Lähtökohtaisesti kyseisellä seinällä tapahtuvan viestinnän luottamuksellisuuden tai yksityiselämän suojan tarve ei ole niin vahva kuin yksittäisen kansalaisen profiilissa käydyn keskustelun kohdalla.

[192] Myös ryhmän salaisuudella voidaan katsoa olevan vaikutusta viestinnän luottamuksellisuuteen, koska se vaikeuttaa ryhmän löytymistä ja vaatii yleensä kutsun ryhmässä jo olevalta henkilöltä. Ryhmän salaisuus tulee erottaa viestinnän salaamisesta, joka ei vaikuta viestinnän luottamuksellisuuteen. Ks. HE 224/2010 vp, s. 93–94; HE 222/2010 vp, s. 317.

valikoituvat satunnaisista syistä.[193] Tällöin viestintä vaikuttaa enemmän siltä, ettei sitä ole tarkoitettu vain tietyn vastaanottajaryhmän nähtäville HE 125/2003 vp mukaisesti.[194]

Niin kuin edellä esitetystä käy ilmi, ei suljetuissa ryhmissä tai profiileissa tapahtuvaa viestintää voi luonnehtia yksiselitteisesti luottamukselliseksi tai julkiseksi. Jokainen tapaus tulisikin tulkita erikseen salaisia tiedonhankinta- ja pakkokeinoja koskevia toimivaltuuksia käytettäessä ja arvioida millainen vaikutus sillä on yksityiselämän suojan kannalta. Käytännössä tämä tarkoittaa suojan tarpeen erojen hahmottamista tilanteissa, joissa erilaisten ryhmien jäseniksi hakeudutaan tai pyritään tietyn profiilin kaverilistalle.[195] Siinä vaiheessa kun liittyminen on tapahtunut, ei kyse ole enää luottamukselliseen viestintään puuttumisesta, jos poliisi- tai peiteprofiili on yksi viestinnän osapuolista.

Niin kuin alussa todettiin, liittyy viestinnän luottamuksellisuuteen kiinteästi myös tunnistamistiedon ja välitystiedon käsitteet, joiden tärkeys perusoikeusnäkökulmasta on ollut muutoksessa viestinnän digitalisoituessa.[196] Tunnistamistiedolla tarkoitetaan PolL 5:8.1:n ja PKL 10:6.1:n mukaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Viittaus koskee jo kumottua sähköisen viestinnän tietosuojalain (516/2004) määritelmää, joka on sittemmin korvattu LSVP 3.1,40:n välitystiedon käsitteellä.[197] Käsitteet eivät ole identtisiä, mutta kyseisellä seikalla ei ole katsottu olevan juurikaan olennaista merkitystä.[198]

> Jatkossa tietoliikennetiedustelua koskevien lainsäädäntömuutosten myötä PolL 5:8.1:n ja PKL 10:6.1:n tulee muuttumaan. Muutoksen jälkeen tunnistamistiedolla tarkoitetaan sähköisen viestinnän palveluista annetun lain 3 §:n 7 kohdassa tarkoitettuun käyttäjään tai mainitun pykälän 30 kohdassa tarkoitettuun tilaajaan

[193] Ylläpitäjän ja moderaattorin osalta, jotka hyväksyvät ryhmän jäsenet, viestintä rinnastuu enemmän yksittäisessä profiilissa tapahtuvaan viestintään viestinnän vastaanottajien näkökulmasta, koska heillä on valta valita vastaanottajat.
[194] HE 125/2003 vp, s. 51.
[195] Asiaan palataan yksittäisiä toimivaltuuksia tarkasteltaessa.
[196] Tunnistamistietojen merkitys reaalimaailman puolella on vähäinen, koska perinteiseen postitoimintaan verrattaessa sähköisen viestinnän tiedot ovat HE 48/2008 vp, s. 3 mukaan rinnastettavissa kirjeen tai postipaketin osoite- ja postileimatietoihin sekä kirjeen tai paketin kokoon ja muotoon.
[197] Sen mukaan välitystiedolla tarkoitetaan oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi sekä tietoa radioaseman tunnisteesta ja radiolähettimen käyttäjästä sekä tietoa radiolähetyksen alkamisajankohdasta, kestosta ja lähetyspaikasta.
[198] Asialla ei katsottu olevan suurta merkitystä tietoliikennetiedusteluun liittyen, joskin esitöissä todettiin vain se, että molempien käsitteiden katsottiin kuuluvan ehdotetun säännöksen piiriin. Ks. tarkemmin HE 202/2017 vp, s. 241.

> yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Aiemmin tunnistamistietojen on katsottu jäävän luottamuksellisen viestinnän suojan ydinalueen ulkopuolelle, jonka takia PL 10.3 §:n lakivarausta ei ole sovellettu, vaan sääntelyn on tullut täyttää vain perusoikeuksien yleiset rajoitusedellytykset.[199] Tämän takia tunnistamistietojen saamista ei ole sidottu tiettyihin rikostyyppeihin, niin kuin kvalifioitu lakivaraus edellyttäisi.[200] Tilanteeseen on kuitenkin vaikuttanut EUT:n ratkaisukäytäntö ja erityisesti Digital Rights Ireland -tapaus[201], jonka perusteella tunnistamistietojen kuuluminen luottamuksellisen viestinnän reuna-alueelle voidaan kyseenalaistaa.[202] EUT:n ratkaisujen jälkeen perustuslakivaliokunta onkin todennut, että käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot ja mahdollisuus niiden kokoamiseen ja yhdistämiseen voi olla yksityiselämän suojan näkökulmasta ongelmallista. Kategorinen erottelu suojan reuna- ja ydinalueeseen ei ole aina perusteltua, vaan huomiota on kiinnitettävä myös rajoitusten merkittävyyteen.[203] Lausuntokäytännöstä ei ole ollut selvästi pääteltävissä, miten tällainen uudelleenarviointi muuttaa aiempaa perusoikeuksien yleisiin rajoittamisedellytyksiin perustuvaa tulkintaa.[204] Lausuntojen jälkeen ei ole esimerkiksi ollut havaittavissa sitä, että teletoimivaltuuksia olisi muutettu jollakin tapaa tunnistamistietoihin liittyen. Tällä ei sinänsä ole vaikutusta tälle tutkimukselle, koska tunnistamistietojen osalta merkitys poliisi- ja peiteprofiileilla mahdollisissa salaisissa tiedonhankinta- ja pakkokeinoissa on käytännössä melko vähäinen. Tämä sen takia, että viestinnän tunnistamistiedot liittyvät luottamuksellisen viestinnän tapaan lähinnä erilaisiin teletoimivaltuuksiin.

### 3.4 Yksityiselämän suoja

[199] Ks. tarkemmin tunnistamistiedoista PeVL 33/2013 vp, s. 3; PeVL 6/2012 vp, s. 3–4 ja perusoikeuksien yleisiin rajoitusedellytyksiin liittyen PeVL 62/2010 vp, s. 4–5; PeVL 23/2006 vp, s. 3.
[200] Ks. esimerkiksi PeVL 33/2013 vp; PeVL 67/2010 vp.
[201] Asia C-293/12 ja C-549/12 Digital Rights Ireland (2013) EU:C:2013:845.
[202] Ks. laajasti EUT:n ratkaisukäytännöstä ja sen vaikutuksesta luottamuksellisen viestinnän suojaan HE 198/2017 vp, s. 23–26.
[203] PeVL 18/2014 vp, s. 6. Tuomio tarkoittaa käytännössä myös sitä, että kansallisessa lainsäädännössä on otettava huomioon tuomion vaatimukset täsmällisemmistä rajoituksista tietojen säilyttämiseen ja käyttöön. Käytännössä tämä tarkoittaa, että oikeasuhtaisuusvaatimuksen vastaisina on pidettävä ainakin sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin.
[204] HE 198/2017 vp, s. 8.

### *3.4.1 Yleistä yksityiselämän suojasta*

Perustuslain 10.1 §:n mukaisen yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä.[205] Yksityiselämän piiriä ei ole määritelty tarkasti ja se voidaan ymmärtää henkilön yksityistä piiriä koskevaksi yleiskäsitteeksi.[206] Siihen kuuluu muun muassa yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään ja ruumiistaan.[207] Lisäksi yksityiselämän käsitteeseen katsotaan kuuluvan kansainvälisissä ihmisoikeussopimuksissa mainittu perhe-elämän suoja.[208] Yksityiselämän yleiskäsitteestä johtuen se pitää sisällään usein kotirauhan tai luottamuksellisen viestin suojan, mutta peittää myös sellaisia aukkoja, joita kyseiset perusoikeudet eivät suojaa.[209] Salaisten tiedonhankinta- ja pakkokeinojen osalta esimerkiksi tiedot henkilön sijainnista ovat tällaisia.[210] Toisena esimerkkinä voidaan mainita vankisellissä olevan henkilön oleskelun tarkkailu, jonka katsotaan olevan merkityksellistä yksityiselämän suojan kannalta, koska selliä ei pidetä kotirauhan suojaamana alueena.[211]

Yksityiselämän suoja ei sisällä kvalifioitua lakivarausta kotirauhan ja luottamuksellisen viestin suojan tapaan, jonka takia kyseisiä rajoituksia tulee peilata perusoikeuksien yleisten rajoitusedellytysten avulla.[212] Tällöin tulee kiinnittää huomiota erityisesti lailla säätämisen vaatimukseen, rajoituksen täsmällisyys- ja tarkkarajaisuusvaatimukseen, rajoitusperusteiden hyväksyttävyysvaatimukseen ja suhteellisuusvaatimukseen. Lisäksi vaikutusta on EIS:n 8 artiklan 2 kappaleen tyhjentävällä luettelolla yksityiselämän suojaan puuttumisen perusteiksi.[213]

---

[205] Suoja koskee siten yhtäältä viranomaisten puuttumista yksityiselämään, mutta myös aktiivisia toimenpiteitä yksityiselämän suojelemiseksi toisten yksilöiden loukkauksia vastaan. Perutuslaki 22 §:n sääntely velvoittaa julkisen vallan turvaamaan perus- ja ihmisoikeudet ja rikoslainsäädännössä yksityiselämää suojataan esimerkiksi 24 ja 27 lukujen sääntelyllä.

[206] Lisäksi yksityiselämän liittyy läheisesti myös muihin perusoikeuksiin, kuten perustuslain 7 §:n mukaisen oikeuteen elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen. Ks. tästä tarkemmin HE 309/1993 vp, s. 47,

[207] Ks. yksityiselämän suojasta moraalisena oikeutena tarkemmin Miller – Gordon 2014, s. 243–246, jossa he jakavat yksityiselämän suojan moraalisen oikeutuksen kymmeneen eri kohtaan.

[208] HE 309/1993 vp, s. 53. Ks. myös KKO 2011:11, jossa käsitellään perhe-elämän suojan sisältymistä yksityiselämän suojaan.

[209] HE 309/1993 vp, s. 53.

[210] Metsäranta 2015, s. 20.

[211] PeVL 12/1998 vp, s. 5

[212] Jos yksityiselämän suojan katsotaan sisältävän muita perusoikeuksia, tulee rajoitusten luonnollisesti täyttää myös kyseisten perusoikeuksien kvalifioidut lakivaraukset.

[213] Viljanen 2011, s. 395.

Tietoverkkojen roolia yksityiselämän suojan näkökulmasta ei ole käsitelty erikseen perustuslaissa tai sen esitöissä tarkemmin, joka johtuu pitkälti siitä, että esityöt ovat viime vuosituhannelta.[214] Jostain syystä myöskään oikeuskirjallisuudessa ja aikaisemmassa tutkimuksessa ei ole käyty tarkemmin läpi yksityiselämän suojan eroja reaalimaailman ja tietoverkkojen välillä, vaikka näitä eroja on selvästi havaittavissa. Tästä huolimatta eroilla on ollut vaikutusta salaisiin tiedonhankinta- ja pakkokeinoihinkin esimerkiksi peitetoiminnan erityisten edellytysten kohdalla. Lainsäätäjä ei ole kuitenkaan arvioinut reaalimaailman ja tietoverkkojen eroja yksityiselämän suojan kannalta kokonaisvaltaisesti, vaan juurikin yksittäisten säännösten kohdalla ja silloinkin suppeasti.[215] Tässä tutkimuksessa yksityiselämän suojan erot reaalimaailman ja tietoverkkojen välillä jaetaan seuraavien alaotsikoiden alle: 1) tiedon syntymistapa, 2) henkilön yksilöiminen ja tunnistaminen, 3) tiedonhankinnan kohde, 4) tiedon keräämistapa, reaaliaikaisuus ja laajuus sekä 5) tiedon laatu ja luotettavuus. Kohtien voidaan katsoa olevan osittain päällekkäisiä, joka on omaista muutoinkin yksityiselämän suojalle.

### *3.4.2 Tiedon syntymistapa*

Julkisella paikalla oleskellessa ihmiset ovat jatkuvasti muiden nähtävinä ja he joutuvat sen vuoksi ottamaan huomioon sen, että kanssaihmiset voivat tarkkailla heitä. Asunnossa tilanne on toinen.[216] Reaalimaailmassa tapahtuvassa toiminnassa henkilö voi liikkua julkisilla paikoilla eri tarkoituksin ja tavata julkisilla paikoilla toisia ihmisiä, vaikka hänellä ei ole välttämättä minkäänlaista tarkoitusta saattaa kyseistä tietoa muutoin julkiseksi.[217] Myös henkilön omat odotukset toiminnan julkisuudesta voidaan ottaa huomioon arvioinnissa yksityiselämän suojan tason tarpeesta.[218] On katsottu, että pelkkä viranomaisen

[214] Perustuslakia on sittemmin muutettu tietoliikennetiedusteluun liittyen vuonna 2018, mutta tämä muutos käsitteli lähemmin luottamuksellisen viestin suojaa, joten siinä ei paneuduttu yksityiselämän suojan tasoihin avoimissa tietoverkoissa.
[215] Ks. HE 224/2010 vp, s.116; HE 222/2010 vp, s. 339, jossa peitetoimintaan liittyen perusteet erityisten edellytysten reaalimaailmaan poikkeavasta tasosta. Esitöissä tietoverkkojen anonyymi luonne, dokumentoinnin helppous ja tarkkuus sekä vähäisempien turvallisuusriskien katsottiin vaikuttavan sääntelytarpeisiin. Ks. myös Sisäministeriö 2009a, s. 204, jossa ihmisten vuorovaikutukselle tietoverkoissa kuvattiin olevan luonteenomaista tietynlainen epäluottamus ja lähtökohtana pidettiin sitä, ettei henkilöt esiinny tietoverkoissa omalla identiteetillään, vaan käytetään esimerkiksi nimimerkkejä tai muita vastaavia tunnisteita.
[216] HE 22/1994 vp, s. 15.
[217] Kyseinen tieto voidaan luokitella yksityiselämän suojaan kuuluvaksi arkaluontoiseksi tiedoksi esimerkiksi sukupuolitautipoliklinikalla käynnin takia. Kyseistä tietoa ei ole mahdollista julkaista toisten toimesta ilman, että mahdollisesti syyllistyisi RL 24:8:n mukaiseen yksityiselämää loukkaavan tiedon levittämiseen.
[218] Ks. *Perry v. Yhdistynyt kuningaskunta* (2003), kohta 37.

henkilöön kohdistama seuraaminen on suojattu PL 10.1 §:n perusteella. Tämä sen takia, että jo pelkän tiedon kerääminen puuttuu kohdehenkilön yksityiselämän suojaan.[219] Reaalimaailmassa julkisten sekä eriasteisesti suojattujen tilojen ja alueiden erot näkyvät selvästi teknisen tarkkailun eri muodoissa. Toimivaltuuksissa erotetaan seuraavia eri tasoisesti suojattuja paikkoja: 1) vakituiseen asumiseen käytettävä tila, 2) kotirauhan suojaama paikka, 3) tila tai muu paikka, jossa perustellusti rikokseen syyllistyväksi oletettu tai rikoksesta epäilty oleskelee ja 4) julkinen alue (PolL 5:17–24 ja PKL 10:16–24).[220] Eriasteiseen suojaamiseen liittyvää ja lähinnä kotirauhan suojaan liittyvää sääntelyä on havaittavissa myös muissa tarkkailutyyppisissä ja erityisissä toimivaltuuksissa.[221]

Tietoverkkojen osalta ei ole olemassa samanlaista jaottelua, koska ”tietoverkkojen kotirauha” perustuu hyvin pitkälti edellä käsiteltyyn luottamuksellisen viestinnän suojaan.[222] On kuitenkin selvää, että henkilön toiminta reaalimaailmassa julkisilla paikoilla muodostaa perustavanlaatuisen eron yksityiselämän suojan näkökulmasta tietoverkkoihin erityisesti tarkkailutyyppisten keinojen osalta, koska reaalimaailmassa tiedon syntymistapa perustuu oleskelun sijasta julkaisemiseen. Julkaiseminen taas liittyy vahvasti PL 12.1 §:n mukaiseen sananvapauteen ja kohdehenkilön tiedolliseen itsemääräämisoikeuteen siitä, mitä hän haluaa julkaista kaikkien nähtäville.[223] Esimerkkinä voidaan mainita tilanne, jossa poliisi tarkkailee avioliitossa olevaa henkilöä, joka tapaa julkisella paikalla salarakkaansa. Tarkkailtava suutelee häntä julkisella paikalla ”salaa”, eikä tarkoituksena ole saattaa asiaa kaikkien ihmisten, saati puolison tietoon. Jos sama tapahtuma tuodaan esille kohdehenkilön toimesta julkisesti tietoverkossa esimerkiksi julkaisemalla valokuva suutelusta, voidaan tietoa pitää yksityiselämän suojan kannalta selkeästi heikomman suojan tarpeessa olevana. Kyseistä esimerkkiä voidaan toisintaa useista muistakin arkaluontoisista asioista ja sama pätee myös yleisesti muiden ihmisten tapaamiseen ja vuorovaikutukseen heidän kanssa.[224] Tukea

[219] Ks. tiedon keräämisen ja sen tallentamisen vaikutuksesta yksityiselämän suojaan esimerkiksi HE 57/1994 vp, s. 15. Ks. myös Helminen – Kuusimäki – Salminen 1999, s. 45. Esityöt erottavat myös poliisin viranomaisena kansalaisesta, jossa poliisin järjestelmällinen tiedonhankinta jonkun yksityiselämästä voidakseen harkita häneen myöhemmin kohdistettavia virkatoimia, saattaa tämä merkitä yksilön vapauspiiriin puuttumista. Ks. HE 57/1994 vp, s. 56. Ks. tiedon tallentamisen ja sen poliisin rekistereissä säilyttämisen vaikutuksesta henkilön yksityiselämän suojaan *S. ja Marper v. Yhdistynyt kuningaskunta* (2008), kohta 67.

[220] Ks. teknisen tarkkailun eri asteisesta puuttumisesta yksityiselämän suojaan tarkemmin HE 57/1994 vp, s. 62.

[221] Esimerkkinä voidaan mainita myös suunnitelmallinen tarkkailu (PolL 5:13.4 ja PKL 10:12.4) ja peitelty tiedonhankinta (PolL 5:14.3 ja PKL 10:14.4), joissa asutussa asunnossa oleskelevan henkilöön kohdistuva toiminta ei ole mahdollista.

[222] Tietoverkoissa ei myöskään jaotella erikseen kuuntelua tai katselua, vaan puuttuminen katsotaan yksityiselämän suojan näkökulmasta samanasteiseksi.

[223] Perustuslain 12.1 §:n mukaan jokaisella on sananvapaus. Sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä.

[224] Ks. HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325, jonka mukaan suunnitelmallisen tarkkailulle on tyypillistä sen seuraaminen, mitä kohdehenkilö tekee ja keitä henkilöitä hän tapaa.

julkisella paikalla tapahtuvan toiminnan ja julkaisemisen eroihin voidaan hakea myös rikoslain yksityiselämää loukkaavan tiedon levittämistä (RL 24:8) koskevan säännöksen avulla, vaikka rikoslain säännökset eivät olekaan suoraan verrannollisia salaisiin tiedonhankinta- ja pakkokeinoihin.[225] Jos kohdehenkilö paljastaa itse arkaluontoista tietoa julkisesti tietoverkoissa, ei kyseisen tiedon katsotaan enää yleensä nauttivan yksityiselämän suojaa siinä määrin kuin ennen tiedon julkistamista.[226]

Tiedon syntymistapaan liittyy myös jo edellä käsitelty luottamuksellisen viestin suojan taso, jonka avulla voidaan kuvata reaalimaailman julkisuuden ja tietoverkkojen julkisuuden käsitteiden eroja. Jos kyse on verkkoviestistä, on julkisuuden asteen ero reaalimaailmaan selkeä. Jos henkilö julkaisee tietoverkoissa avoimesti tietoja kaikkien nähtäville, ei se rinnastu reaalimaailman osalta julkisella paikalla huutamiseen, kaupan ilmoitustauluun, tai edes useita tuhansia osallistujia keräävässä tilaisuudessa puhumiseen. Tämä sen takia, että tietoverkoissa avoimesti saatavilla olevilla tiedoilla on globaali yleisö ja viesti on jatkuvasti saatavilla.[227] Vaikka sekä reaalimaailman ja tietoverkkojen tilanteita voidaan sinänsä molempia luonnehtia julkisesti luonteen omaaviksi toimiksi, on viestinnän kattavuus tietoverkoissa täysin eri luokkaa. Poikkeuksen tekevät kuitenkin tilanteet, joissa kyse on jo aikaisemmin käsitellyistä suljetuista ryhmistä tai profiileista.

### *3.4.3 Henkilön yksilöiminen ja tunnistaminen*

Henkilön yksilöinti reaalimaailmassa on helppoa, koska vaikka kohdehenkilö voi käyttää erilaisia valeasuja tai muita harhauttavia keinoja, poliisimies pystyy yksilöimään, että kyseessä on yksittäinen luonnollinen henkilö. Reaalimaailmassa henkilön yksilöiminen perustuu fyysisiin ja tosiasiallisiin aistihavaintoihin kohteesta tai myöhemmin tekniseen tarkkailuun liittyvistä tallenteista tapahtuvaan tunnistamiseen.[228] Tunnistaminen voi tapahtua

[225] Ks. rikoslain suhteesta salaisiin tiedonhankinta- ja pakkokeinoihin HE 22/1994 vp, s. 5 ja 11, jossa verrataan yksityiselämää loukkaavaa tiedon levittämistä sekä salakuuntelua salaisiin tiedonhankinta- ja pakkokeinoihin. Ks. suhteesta myös Terenius, s. 316–322. Voidaan myös huomioida se seikka, että vainoamisen (RL 25:7a) tunnusmerkistö täyttyy reaalimaailmassa seuraamisesta, mutta tietoverkoissa ei. Ks. tähän liittyen HE 19/2013 vp, s. 24.

[226] Ks. HE 19/2013 vp, s. 41, jonka mukaan henkilön itsensä julkisuuteen tuoman tiedon ajallisesti läheinen toistaminen esimerkiksi toisessa tiedotusvälineessä ei ole oikeudetonta.

[227] Ks. Trottier 2012, s. 74–76, jossa tuodaan esille, että suurin osa ihmisistä yleensä ymmärtää mahdollisuuden käyttää erilaisia yksityisyysasetuksia sekä sen, että julkinen toiminta sosiaalisessa mediassa voi tulla kenen tahansa tietoon. Ks. tähän liittyen myös Fuchs 2015, s. 408, joka toteaa, että vaikka kansalaiset olisivat sinänsä huolissaan yksityisyydestään, voidaan omat tiedot jättää joka tapauksessa avoimiksi.

[228] Keskeisin tapa tunnistaa ihminen reaalimaailmassa ilman vuorovaikutusta on hänen kasvonsa, mutta myös ääni, ulkomuoto ja yleinen olemus vaikuttavat tähän. Ks. identiteetin käsitteestä laajasti Korja 2016, s. 120–

myös kohteen hallussa olevista tunnistamisasiakirjoista tai muulla vastaavalla tavalla, vaikka tähän tuskin salaista keinoa käytettäessä päädytään, koska tiedonhankinta voi paljastua. [229] Muita tapoja ovat esimerkiksi rekisterikyselyjen, asiakirjojen, sormenjälkien, ääninäytteen, kasvojen tai DNA:n avulla tapahtuva tunnistaminen.[230] Näitä tietoja voidaan kerätä myös ilman kohdehenkilön tietoa salaisen tiedonhankinnan aikana.

Henkilön yksilöiminen ja tunnistaminen tietoverkoissa eroaa oleellisesti reaalimaailman tilanteesta, koska yksilöiminen sekä tunnistaminen perustuu tietoverkkoihin lisättyyn dataan (henkilötietoihin).[231] Vaikka kyse on ihmisen identiteettiin liittyvästä tiedosta, ei sitä ole yleensä sidottu fyysisiin ominaisuuksiin. Henkilö voi esimerkiksi esiintyä vastakkaisen sukupuolen edustajana tai muutoin keksiä erilaisia fyysisiä ominaisuuksia selvästi reaalimaailmaa helpommin, jos kyse ei ole webkamerayhteydestä. [232] Jos tarkasteluun otetaan kansalaisen eri tasoisesti suojattujen tietoverkkojen osista löytyvät tiedot yleisellä tasolla, voidaan viitata *Korjan* kolmijakoon verkkoidentiteetistä. Yläkäsitteenä toimii 1) yksilön tiedollinen identiteetti, joka muodostuu yksilöstä eri lähteistä saatavissa olevasta informaatiosta, joiden pohjalta yksilö on tunnistettavissa. Osana kyseistä tiedollista identiteettiä on 2) digitaalinen identiteetti, joka on digitaalisessa muodossa ja yksilöön liitettävissä olevaa informaatiota. Kyseinen digitaalinen identiteetti voidaan jakaa kolmeen eri osaan: 2a) tunnistautumiseen liittyvä informaatioon, 2b) dataan ja 2c) digitaaliseen jälkeen. Ensimmäiseen liittyvät IP-osoite, sähköpostiosoite, käyttäjätunnukset ja aliakset. Datalla Korja tarkoittaa pankkitietoja ja sosiaalista dataa.[233] Digitaalisiin jälkiin liittyvät

128. Ks. myös Sisäministeriö 2010, s. 18.

[229] Poliisi ei välttämättä halua ottaa tuntematontakaan kohdehenkilöä käsittelyyn ja selvittää hänen henkilöllisyyttään. Henkilöä voidaan seurata esimerkiksi asuntoon tai ottaa valokuvia hänestä, jonka perusteella henkilöllisyys voi selvitä myöhemmin. Toisaalta eteen voi tulla myös tilanteita, jossa salaisten tiedonhankinta- ja pakkokeinojen kohteeksi valittu tuntematon henkilö kadotetaan, eikä hänen todellinen henkilöllisyytensä selviä.

[230] Ihmisen keho on mahdollista muuntaa biometrisen tunnistamiseen liittyen digitaaliseksi koodiksi useilla eri tavoin ja tätä kautta tunnistaa yksittäinen henkilö. Tulevaisuudessa erilainen biometrinen tunnistaminen tulee lisääntymään. Ks. aiheesta tarkemmin Korja 2016, s. 87–89.

[231] Ks. oman identiteetin hallinnoimisesta tietoverkoissa yleisesti Froomkin 2015, s. 61–69.

[232] Henkilön ei yleensä tarvitse tunnistautua luotettavalla tavalla sosiaalista mediaa käyttäessään. Ks. tunnistautumisen käsitteestä tarkemmin Sisäministeriö 2010, s. 18. Poikkeuksen tilanteeseen tekevät biometriset tunnisteet, joiden avulla henkilö voi todentaa henkilöllisyyden älylaitteiden, mutta myös tietoverkoista löytyvien palveluiden osalta. Esimerkkinä tästä sormenjälkitunnistus. Ks. virtuaalisesta identiteetistä verrattuna reaalimaailman identiteettiin Heinonen 2001, s. 63–66. Ks. myös identiteetistä kokonaisuudessaan Lessig 1999, s. 30–31, jonka mukaan identiteetti kattaa myös kaikki tietoverkoista saatavissa olevat tiedot.

[233] Sosiaalisella datalla Korja tarkoittaa henkilön perhettä kuvaavia tietoja, toimintaa koskevia tietoja, yhteistietoja sekä erillisinä yksikköinä hänen rooliaan, asemaansa ja valtuuttaan kuvaavia tietoja tietyssä tilanteessa ja toiminnassa. Kyseisiä tietoja löytyy esimerkiksi väestötietojärjestelmästä, kaupparekisteristä, yhdistysrekisteristä, säätiörekisteristä, holhousasioiden rekisteristä sekä muista yksittäisistä viranomaisten rekistereistä.

linkit, blogikommentit jne. Identiteetin syvimmän osan tietoverkoissa muodostaa 3) sähköinen identiteetti, joka on johonkin luonnolliseen henkilöön teknisesti ja oikeudellisesti luotettavalla tavalla liittyvää informaatiota, jonka perusteella henkilö on tunnistettavissa sähköisessä toimintaympäristössä. Kyseessä on siten henkilön tunnistamisen ydinalueelle kuuluvasta informaatiosta, joka voi olla esimerkiksi henkilötunnus tai biometrinen tunniste, joka on liitettävissä vain yhteen henkilöön.[234] Sähköisellä identiteetillä on mahdollisuus toimia tietoverkoissa oikeudellisesti luotettavalla tavalla esimerkiksi erilaisissa viranomaisen palveluissa.[235] Yksityiselämän suojan näkökulmasta Korjan jaottelu ei ole täysin toimiva. Digitaalisen identiteetin käsitteessä sekoittuu julkista luotettavuutta nauttivat viranomaisen rekisterit sosiaaliseen mediaan, jossa henkilön yksilöiminen ja tunnistaminen ei ole yhtä luotettava. [236] Sosiaalisen median palveluja ei suojata RL 16:7:n rekisterimerkintärikosta koskevalla säännöksellä, vaan niihin voi vapaasti luoda erilaisia identiteettejä.[237] Näiden osalta käyttäjätilin perustamiseen tarvitsee internet-yhteyden lisäksi yleensä vain sähköpostiosoitteen, joiden todentamismahdollisuus tiettyyn henkilöön on helpohkosti peitettävissä.[238]

Tietoverkoissa problematiikka henkilön yksilöinnin ja tunnistamisen kannalta voidaan jakaa esiintymiseen 1) *todellisilla tiedoilla*, 2) *pseudonyyminä* tai 3) *anonyyminä*. Henkilöt voivat esiintyä palveluista riippuen täysin oikeilla tiedoilla ja omana itsenään, jolloin tiedonhankinnassa on mahdollisuus saada laajasti tietoa tietystä henkilöstä.[239] Pseudonyymeillä tarkoitan profiileja, joissa on sekoitettuna paikkansa pitäviä tietoja keksittyjen tai väärien tietojen seassa, eikä henkilö ole välttämättä suoraan tunnistettavissa profiilin tietojen perusteella.[240] Anonyyminä taas voidaan pitää profiilia, jossa ei välttämättä

[234] Harvinaisena poikkeuksena voidaan mainita identtiset kaksoset, joilla on sama DNA.
[235] Korja 2015, s. 173–175. Ks. myös Oikeusministeriö 2013, s. 24, jossa tietosuojavaltuutettu jakaa henkilöä koskevat tiedot konventionaalisiin henkilötunnisteisiin, erilaisiin laitteisiin ja palveluihin liittyviin tunnisteisiin sekä henkilökohtaisiin tunnisteisiin.
[236] Tämä koskee erityisesti datan käsitettä, jota Korjan mukaan löytyy erilaisista viranomaisen ylläpitämistä rekistereistä. Näissä tiedot ovat yleensä saatu luotettavalla tavalla, esimerkiksi fyysistä vuorovaikutusta ja asiakirjoja apuna käyttäen, toisin kuin sosiaaliseen mediaan lisättyjen tietojen osalta. Esimerkkinä voidaan mainita tilanne, jossa väestörekisteristä löytyy tieto yhdestä veljestä, mutta sosiaalisessa mediassa henkilö väittää, että hänellä on kaksi siskoa. Sosiaalisen median palvelut ovat tosin alkaneet ottamaan biometrisiä tunnisteita käyttöön, mutta toistaiseksi niiden käyttö on vielä rajoittunutta tunnistautumisen suhteen.
[237] Tilannetta ei muuta se, että palvelun käyttöehdoissa mainitaan siitä, että henkilön tulee esiintyä omalla nimellään. On yleinen käytäntö, että omia tietoja muutellaan tilanteen mukaan, eikä sosiaalisen median palvelut juuri puutu tähän.
[238] Sähköpostiosoitteen luomiseksi ei tarvitse antaa oikeita tietojaan ja tarjolla on erilaisia anonymisointiin perustuvia sähköpostiosoitteen tarjoajia, kuten Protonmail.
[239] Esimerkkinä palvelusta, jossa esiinnytään yleensä omilla tiedoilla voidaan mainita LinkedIn. Tämä johtuu erityisesti siitä, että palvelu on tietynlainen oma ammatillinen CV.
[240] Ks. pseudonyymin käsitteeseen liittyen tietosuoja-asetuksen (2016/679) 4 artiklan 5 kohdan pseudonymisointia koskeva määritelmä.

mikään tieto viittaa yksittäiseen tunnistettavaan henkilöön. Kyse voi olla pelkästä nimimerkistä.

Lisäksi voidaan tunnistaa esiintyminen 4) *toisena henkilönä* tai 5) *yhteiskäyttöroolissa*. Toisena henkilönä esiintymisen osalta on kyse identiteettivarkauden kaltaisesta tilanteesta, jossa esiinnytään RL 38:9 a §:n mukaisesti toisen henkilötiedoilla, tunnistamistiedoilla tai muilla vastaavilla tiedoilla erehdyttääkseen kolmatta henkilöä.[241] Yhteiskäyttöroolissa olevalla käyttäjätilillä voi toimia syystä tai toisesta useita henkilöitä, joita ei välttämättä pystytä yksilöimään.[242] Yhä kiihtyvän teknologisen kehityksen myötä omaksi kohdakseen voidaan laskea myös 6) *keinoälyyn* perustuva toiminta, jossa toimijana ei ole luonnollinen henkilö.[243] Toiminnan takana voi olla automaattisesti ohjautuva robotti ja asia liittyä esimerkiksi informaatiovaikuttamiseen.[244] Nykyteknologialla on myös mahdollista tehdä uskottavia ääniklooneja, kuvamuokkauksia tai keksittyjä videoita toisista henkilöistä niin sanotulla deepfake-tekniikalla.[245] Kyseinen asia on otettu huomioon jo rikoslainsäädännössä, jossa puhutaan todenmukaisesta kuvasta tai kuvatallenteesta lapsen hyväksikäyttömateriaaliin liittyen.[246] Todenmukaisella kuvalla tai kuvatallenteella tarkoitetaan tilanteita, joissa kuvasta tai kuvatallenteesta ei voida päätellä, kuvaako se todellisia henkilöitä tai todellisia tapahtumia.[247]

Jos henkilö ei esiinny omilla tiedoillaan – ja vaikka esiintyisikin – on henkilöllisyyden todentaminen reaalimaailmaan verrattuna selvästi epäluotettavampaa. Poliisin mahdollisuudet todentaa profiilin henkilöllisyys, voidaan karkeasti jakaa 1) *poliisimiehen manuaalisesti suorittamaan tunnistamiseen* ja 2) *nimenomaiseen toimivaltuuteen perustuvaan tunnistamiseen*. Kummassakaan ei päästä reaalimaailman todentamisen tasolle.

[241] Identiteettivarkaus voidaan toteuttaa joko esiintymällä erehdyttävästi toisena henkilönä tai kaappaamalla toisen käyttäjätili, jota varsinainen kohdehenkilö on käyttänyt. Ks. identiteetin anastamistavoista sosiaalisessa mediassa tarkemmin Forss 2014, s. 89– 94.
[242] Näitä ovat yleensä yritysten tai yhteisöjen profiilit. Myös yksittäistä profiilia voi käyttää useampi henkilö.
[243] Vrt. Heinonen 2001, s. 64; Korja 2016, s. 121, jossa he toteavat digitaalisen identiteetin takaa löytyvän aina tosiasiallisesti yksilöitävissä olevan luonnollisen henkilön. Näin ei nykyteknologian takia enää välttämättä ole.
[244] Keinoälyllä toimivat esimerkiksi erilaiset botit, jotka voivat olla ihmisten koodaamia profiileja esimerkiksi Twitterissä. Ne voivat twiittailla ihmisestä riippumatta. Ks. keinoälyn käyttömahdollisuuksista erityisesti chatbottien osalta laajasti Rouhiainen 2018, s. 91–118. Ks. informaatiovaikuttamiseen liittyen ks. kokonaisuudessaan esimerkiksi Stratcom 2019, jossa Naton strategisen viestinnän osaamiskeskus Stratcom antaa katsauksen niin sanottuun ”robotrollaukseen” venäjän Facebook-vastineessa VK:ssa. Ks. myös HS 2019b, jossa uutisoitiin tekoälyllä toimivasta tekstigeneraattorista, joka olisi ohjelman kehittäjien mielestä liian vaarallinen julkaistavaksi, koska sitä voisi käyttää valeuutisten ja identiteettivarkauksien tekemiseen.
[245] Ks. ääniklooneista esimerkiksi www.lyrebird.ai ja deepfake-tekniikasta esimerkkinä BuzzFeed 2018, jossa Yhdysvaltojen entinen presidentti Barack Obama saatiin haukkumaan videolla nykyistä presidenttiä Donald Trumpia.
[246] Sääntely koskee RL 17:18:n, RL 17:18a:n ja RL 17:19:n tunnusmerkistöjä.
[247] Ks. tarkemmin HE 282/2010 vp, s. 103.

Käytännössä ensimmäinen kohta tarkoittaa OSINT-toiminnassa kerättyä tietoa. Yksinkertaisimmillaan tunnistaminen tarkoittaa sitä, että tietty henkilö esiintyy profiilissa omalla nimellä sekä kuvalla ja hänen voidaan erilaisten profiilista löytyvien tietojen mukaan olettaa olevan juuri kyseinen henkilö. [248] Jos poliisilla on kohdehenkilöstä vain jokin yksittäinen tieto, kuten nimimerkki, on tunnistaminen vaikeampaa. *Bazzell* jakaa OSINT-tiedonhankinnan viiteen tärkeimpään seikkaan tietoa etsittäessä. Nämä ovat 1) sähköpostiosoite, 2) käyttäjänimi (eli yleensä samalla myös nimimerkki), 3) oikea nimi, 4) puhelinnumero ja 5) verkkotunnus. Riippuen saatavilla olevista yksittäisistä tiedosta, etsitään eri tietoverkkolähteistä lisätietoja kyseisiä alkutietoja hyödyntäen. Kyseinen menetelmä on tarkoitettu yleisesti tiedonkeruuseen kohteesta, mutta kattaa samalla myös tämän yksilöimiseen ja tunnistamiseen liittyvän toiminnan.[249]

Jos tunnistaminen ei onnistu profiilista löytyvän nimen, kuvan tai muun kohdehenkilöön yhdistettävän henkilötiedon avulla, pitää turvautua toimivaltuuteen, jolla henkilöllisyyden voi mahdollisesti selvittää.[250] Yleisin tapa tunnistaa profiili tietoverkoissa on hankkia IP-osoite televalvonnan (PolL 5:8 ja PKL 10:6) avulla. Käytännössä riippuu paljon rikoksen vakavuudesta ja palvelun ylläpitäjästä onko tietoja mahdollista saada, vaikka teoriassa toimivaltuus tämän mahdollistaisi.[251] Jos IP-osoite saadaan, tulee kyseisen IP-osoitteen haltijan tiedot pyytää operaattorilta PolL 4:3.2:n perusteella. Tämäkään ei yksilöi tiettyä käyttäjää, vaan pelkästään liittymän tilaajan. IP-osoite voi olla esimerkiksi kirjaston, kahvilan tai asiaan liittymättömän henkilön.[252] Jos IP-osoite ei ole kotimaisen operaattorin hallinnoima, tunnistaminen muodostuu melko mahdottomaksi. Sama koskee myös darknetin kautta tapahtuvaa tai muuten anonymisoitua viestintää. Käytännössä onkin mahdotonta sanoa, onko henkilön tunnistaminen helpompaa manuaalisesti vai toimivaltuuden perusteella, koska tämä on täysin tapauskohtaista.[253] Lisäksi voidaan mainita, että poliisilain

[248] Ks. OSINT-toimintaan liittyvästä henkilöllisyyden varmentamisesta ja siihen liittyvästä taktiikasta tarkemmin McKeown – Maxwell - Azzopardi 2014, s. 5.
[249] Ks. tarkemmin OSINT-toiminnan prosesseista ja tiedonhankintametodeista Bazzell 2014, s. 387–394.
[250] Niin kuin aikaisemmin on jo tuotu ilmi, ei PolL 2:1:n henkilöllisyyden selvittämistä koskevalla toimivaltuudella ole käyttöä tietoverkoissa. Poliisi- ja pakkokeinolaista löytyy kuitenkin muuta sääntelyä, jolla henkilöllisyyden selvittäminen voi olla mahdollista.
[251] Suomen ulkopuolella toimivat palvelut eivät ole velvollisia noudattamaan Suomen poliisi- tai pakkokeinolakia. Teoriassa tiedot voisi saada kansainvälisen oikeusavun kautta, mutta sen käyttö on erittäin harvinaista esimerkiksi erilaisten sosiaalisen median palvelujen osalta. Yleisempää on poliisin suora yhteys palveluntarjoajaan. Ks. tarkemmin tietoverkkoon liittyvien pakkokeinojen problematiikasta Forss – Keinänen 2017, s. 20–21. Lisäksi sananvapausrikoksiin liittyen on mahdollista hakea tunnistamistietoja sananvapaudesta käyttämisestä joukkoviestinnässä annetun lain (460/2003) 17 §:n perusteella.
[252] Useissa paikoissa on avoimia wlan-liittymiä, eikä yksityisen henkilöiden avoimien langattomien verkkojen käyttö ei ole kriminalisoitu (RL 28:7.3).
[253] Ks. liittymän käyttäjän tunnistamiseen liittyvästä problematiikasta Savola 2013, s. 887 ja siinä mainitut tuomiot, joiden perusteella pelkän internet-liittymän haltijalla ei myöskään ole legaalista vastuuta liittymää

4 luvun 3 §:n 2 momentin säännöksellä on mahdollista saada profiilin rekisteröitymistiedot, joista voi selvitä henkilöllisyys.[254]

### *3.4.4 Tiedonhankinnan kohde*

Reaalimaailmassa poliisimies tekee salaisessa tiedonhankinnassa havaintoja esimerkiksi siitä, mitä kohdehenkilö puhuu, keitä hän tapaa ja missä hän liikkuu.[255] Sama koskee tarkkailutyyppisten keinojen lisäksi erityisiä toimivaltuuksia, mutta niissä havaintojen tekeminen tapahtuu vuorovaikutuksessa kohteen kanssa. Reaalimaailman puolella toimintaa on eroteltu yksityiselämän suojan näkökulmasta tarkkailutyyppisissä keinoissa siten, että toiminta voi kohdistua kohdehenkilön lisäksi myös asuntoon tai tilaan taikka paikkaan, jossa hänen voidaan olettaa todennäköisesti oleskelevan tai käyvän (PolL 5:17–22 ja PKL 10:16–22). Lisäksi teknistä tarkkailua voidaan kohdistaa esineeseen, aineeseen tai omaisuuteen (PolL 5:21–22 ja PKL 10:21–22). [256] Erottelu koskee myös teknistä laitetarkkailua, joka kohdistuu tietokoneeseen, muuhun vastaavaan tekniseen laitteeseen taikka sen ohjelmiston toimintaan, sen sisältämiin tietoihin tai yksilöintitietoihin (PolL 5:23–24 ja PKL 10:23–24). On havaittavissa, että reaalimaailmassa on vahvimmin suojattu kohdehenkilön fyysinen toiminta. Tämä ilmenee esimerkiksi teknisen seurannan edellytyksistä, jossa henkilön teknisen seurannan erityiset edellytykset ovat korkeammat muihin seurattaviin kohteisiin verrattuna (PolL 5:21.3 ja PKL 10:21.3).

Tietoverkoissa kyseisenlaista jaottelua ei ole tehty, eikä tietoverkoista saatavan datan lähdettä ole eroteltu yksityiselämän suojan näkökulmasta. Vaikuttaakin siltä, että yksityiselämän suojan kannalta ei olisi merkitystä mistä tietoverkon lähteestä tieto on peräisin. *Fuchs* on jakanut Facebook-profiilin sisältämän tiedon henkilökohtaiseen tietoon, kommunikatiiviseen tietoon ja sosiaalisen verkoston tietoihin. Fuchs toteaa, että reaalimaailmasta poiketen erityisesti viimeisen kohdan osalta henkilön eri roolit läheisten tai tuntemattomien kesken taikka yleisesti yhteiskunnassa sekoittuvat monimutkaiseksi

käyttäen muiden tekemistä teoista.

[254] Kyseistä säännöstä käydään läpi tarkemmin tiedon keräämistä, reaaliaikaisuutta ja laajuutta koskevassa kohdassa.

[255] Tämä voi tapahtua joko suoraan kohdehenkilöön kohdistetulla tarkkailulla tai esimerkiksi myöhemmin tallenteelta teknisen tarkkailun toimivaltuuksien kohdalla.

[256] Teknisessä tarkkailussa tietoa kerätään esimerkiksi ajoneuvoon asennetun seurantalaitteen avulla tai kohdistetaan teknistä katselua varastorakennukseen.

tietojoukoksi.[257] Tietoverkoissa tiedonhankinnan kohteeseen liittyvää problematiikkaa voidaankin jaotella Fuchsin jaottelua osittain mukaillen seuraavasti: 1) kohdehenkilön oma toiminta, 2) muiden tuottama tieto ja 3) muu tietotoverkoista saatava tieto.

Reaalimaailman tapaan tiedonhankinnan kohteena tietoverkoissa voi olla *kohdehenkilön oma toiminta*, joka käsittää erilaiset sosiaalisen median profiileilla kirjoitetut viestit, kuvat, videot ja striimaukset sekä blogit, keskustelupalstakirjoitukset ja muut vastaavat viestit. Kohdehenkilö voi jättää myös paikkatietoja joko merkitsemällä itsensä tiettyyn paikkaan tai paikkatieto voi olla havaittavissa taikka löydettävissä esimerkiksi valokuvasta.[258] Tähän luokkaan kuuluvat myös profiilista löytyvät kaverilistat, merkinnät sukulaissuhteista, harrastuksista sekä erilaiset tykkäykset urheiluseuroista, artisteista, järjestöistä ja muista vastaavista tahoista. Näissä kaikissa tilanteissa tieto on yleensä kohdehenkilön itsensä tuottamaa ja löytyy hänen profiilista tai tietyltä sivustolta.

Kohdehenkilöstä voidaan saada yksityiselämän suojan kannalta merkittävää tietoa myös *muiden tuottamana*. Tieto voi olla syntynyt joko siten, että joku 2a) muu henkilö on ollut vuorovaikutuksessa kohdehenkilön kanssa, tai kyse on 2b) ilman kohdehenkilön vuorovaikutusta syntyneestä tiedosta. Vuorovaikutukseen liittyvissä tilanteissa yksi tai useampi henkilö viestii kohdehenkilön kanssa, jonka perusteella muu kuin kohdehenkilö tuottaa tietoja kohdehenkilöstä. Yleisenä esimerkkeinä voidaan mainita kohdehenkilön Facebook- tai Instagram-profiiliin lähetetty kommentti. Tilanteessa poliisi saa ensinnäkin tiedon vuorovaikutuksesta kohteen kanssa, mutta esille voi tulla myös muuta kohdehenkilöä koskevaa tietoa.[259]

---

[257] Fuchs 2015, s. 402. Ks. myös Heinonen – Hannula 1999, s. 25, jotka erottavat tietoverkoissa roolit kansalaisena, työntekijänä ja kuluttajana sekä Aalto – Uusisaari 2010, s. 21–34, jossa he erottelevat roolit tietoverkoissa seuraavasti: yksityinen henkilökohtainen, ei-julkinen ammatillinen, julkinen ammatillinen ja julkinen henkilökohtainen. Tässä yhteydessä voidaan todeta, että kohdehenkilön yhteiskunnallisella asemalla tai roolilla ei ole vaikutusta salaisten tiedonhankinta- ja pakkokeinojen käytölle. Esimerkiksi tarkkailun kohteena voi olla putkimies, julkisuuden henkilö, poliitikko tai vaikka poliisi, eikä tämä vaikuta heidän yksityiselämän suojan tasoon. Tältä osin voidaan viitata RL 24:8.2:n sääntelyyn, jossa politiikassa, elinkeinoelämässä tai julkisessa virassa tai tehtävässä taikka näihin rinnastettavassa tehtävässä toimivien suoja on yksityiselämän kannalta erilainen kuin normaalin kansalaisen. Kyseinen sääntely korostaa myös edellä käsiteltyä julkisuuden ja julkaisemisen eroa. Ks. myös Copland v. Yhdistynyt kuningaskunta (2007), kohta 41. Ratkaisussa oli kyse sähköpostin valvonnasta työpaikalla ja EIT totesi, että myös työpaikalta soitetut puhelut, sähköpostit ja internet-yhteyden käyttö nauttii EIS 8 artiklan suojaa.

[258] Valokuvasta on mahdollista havaita kohdehenkilön sijainti, mutta myös saada jossain tapauksissa paljon muuta tietoa. Valokuvan metatietoja, joita kutsutaan EXIF-dataksi, voivat olla esimerkiksi GPS-paikkatieto, kuvan ottamishetki ja kuvan ottamiseen käytetty laite. Ks. EXIF-datasta tarkemmin Bazzell 2014, s. 217–219.

[259] Tällainen tieto voi olla esimerkiksi syntymäpäiväonnittelu, jonka perusteella poliisi voi saada tietoonsa kohdehenkilön syntymäpäivän. Ks. Trottier 2012, s. 22, jossa hän nostaa esille erityisesti sen, että muut ihmiset voivat tuottaa sosiaaliseen mediaan avoimesti tietoa henkilöstä, joka pitää itse yksityisyysasetukset tiukkoina.

Tällöin tilanteen voidaan ainakin osittain katsoa rinnastuvan reaalimaailman tilanteeseen, jossa kohdehenkilöä tarkkaillaan tai hänen kanssaan ollaan vuorovaikutuksessa tilanteessa, jossa kohdehenkilö keskustelee jonkun muun kanssa. Reaalimaailmasta poiketen tietoverkoissa kyseisenlaista tietoa voidaan kuitenkin kerätä selvästi laajemmin ja helpommin, koska kaikki keskustelut ovat koko ajan saatavilla, eikä kyse ole yksittäisen pistemäisen tilanteen seuraamisesta. Tietoverkoissa kyseessä voi tämän lisäksi olla toiminta, jossa viestintä tapahtuu ilman kohdehenkilön tietoa tai vaikutusta. Esimerkkeinä voidaan mainita erilaisissa blogeissa, ryhmissä ja keskustelupalstoilla tapahtuva kohdehenkilöön liittyvä viestintä, joissa kohdehenkilö ei ole osallisena.[260] Yleisen sosiaalisen median viestinnän ja vuorovaikutuksen lisäksi voidaan mainita esimerkkeinä erilaisten huomiota herättäviin rikoksiin, mielenosoituksiin tai terroristi-iskuhin liittyvä viestintä, joiden yhteydessä kansalaiset voivat itse aktivoitua etsimään ja yhdistelemään tietoja mahdollisista tekijöistä. Tällöin voi syntyä poliisia hyödyttävää tietoa, koska kansalaisten oman aktiivisuuden perusteella tuottamat tiedot ovat monesti avoimesti myös poliisin saatavilla.[261]

Kohdehenkilön oman ja muiden toiminnan lisäksi voidaan erottaa omaksi kohdakseen *muu tietoverkoista saatava tieto*. Kohteena on osittain kahden edellisen kohdan yhdistelmä, jossa tieto saadaan esille palvelun teknisten ominaisuuksien tai poliisin käytössä olevien ohjelmien avulla.[262] Esimerkkinä tällaisesta toiminnasta voidaan mainita tilanne, jossa kohdehenkilö on asettanut yksityisyysasetuksensa Facebookissa siten, ettei hänen kaverilistansa näy. Joko käymällä läpi oletettuja kavereita tai käyttämällä erilaisia apuohjelmia voidaan kuitenkin paljastaa ainakin osa hänen kaverilistalla olijoista muiden avointen kaverilistojen avulla.[263] Tähän luokkaan voidaan lukea myös palvelun teknisten haavoittuvuuksien takia saadut tiedot, jotka perustuvat tosin satunnaisiin tilanteisiin.[264]

### *3.4.5 Tiedon keräämistapa, reaaliaikaisuus ja laajuus*

[260] Ks. esimerkiksi Cascavilla ym. 2015, s. 667, jossa he esittelevät israelilaisen sotilaan nimeltä ”Corporal S.” -tapausta. Kyseistä nimitystä käyttäen hänestä oli julkaistu kasvojen kohdalta peitetty kuva Facebook-sivulla, jossa häntä ylistettiin terroristin tappamisesta. Sivuston kommenteista löytyi tieto, jossa kuvassa esiintyvän kehuttiin olevan hänen hyvän ystävän tytär ja mistä hän on kotoisin. Muutamalla klikkauksella pystyttiin selvittämään kyseisen sotilaan henkilöllisyys.
[261] Ks. kyseisestä toiminnasta tarkemmin esimerkiksi Procter ym. 2014, s. 11.
[262] Siten kyseessä on vain osittain poliisi- ja peiteprofiileihin liittyvä toiminta. Asiaa avataan tarkemmin tiedon keräämistä koskevassa osiossa.
[263] Ks. aiheesta tarkemmin Burattin – Cascavilla – Conti 2014, s. 3, jossa tutkijat saivat paljastettua keskimäärin 25 prosenttia piilotetun kaverilistan sisällöstä ja joidenkin osalta jopa 70 prosenttia.
[264] Ks. palvelujen haavoittuvuuksista esimerkiksi Yle 2018, jossa Facebookin ohjelmistovirheen takia miljoonat käyttäjät julkaisivat tietämättä päivityksiä pelkän kaverilistan sijasta julkisesti.

Reaalimaailmassa tietoa kerätään tarkkailutyylisissä keinoissa yleensä seuraamalla kohdehenkilön toimintaa reaaliaikaisesti. Tietoa kerätään fyysisin ja tosiasiallisin aistihavainnoin, mutta teknisessä tarkkailussa myös esimerkiksi tallentaen videokuvaa tietystä tilasta tai seuraamalla teknisesti henkilön sijaintia.[265] Laajuudeltaan tieto on reaalimaailmassa yleensä pistemäistä, jossa saadaan tietoa vain tietystä ajankohdasta ja paikasta.[266] Toisaalta teknisen laitetarkkailun (PolL 5:23 ja PKL 10:23) yhteydessä tietoja voi saada myös laajasti. Tällöin kyse on tietokoneesta tai muusta vastaavasta teknisestä laitteesta taikka sen ohjelmiston toiminnasta, sen sisältämistä tiedoista tai yksilöintitiedoista tehdyistä havainnoista. Kohteena on nimenomaan kohdehenkilön laitteet, joista ei kuitenkaan saa hankkia tietoa viestin sisällöstä tai tunnistamistiedoista. Erityisten salaisten tiedonhankinta- ja pakkokeinojen osalta vuorovaikutus reaalimaailmassa tapahtuu yleensä kasvotusten. Myös näissä keinoissa tiedon keräämistapa, reaaliaikaisuus ja laajuus ilmenevät samanlaisena pistemäisenä tietona kuin tarkkailutyylissä keinoissa.[267]

Tarkkailutyyppisissä keinoissa tiedon kerääminen poliisi- tai peiteprofiileilla perustuu sivustoja ja sen eri käyttäjiä selatessa tehtyihin havaintoihin sekä erilaisiin hakutoimintoihin.[268] Reaaliaikaiseksi ja siten lähimmäksi reaalimaailman pistemäistä tiedonhankintatilannetta voidaan lukea viestintätavat, joissa kohdehenkilö striimaa suoraa videokuvaa toiminnastaan tietoverkkoon. Sama pätee viestintään, jota voidaan muutoin seurata reaaliaikaisesti. Tällainen on esimerkiksi chat- tai webkamerakeskustelu. Tällöin saatu tieto on pistemäistä, niin kuin reaalimaailmassakin. Tietoverkoista kohdehenkilöä koskevaa tietoa voidaan kuitenkin kerätä reaalimaailman reaaliaikaisesta ja pistemäisestä luonteesta poiketen vuosienkin ajalta erittäin laajasti. Useilla sosiaalisen median palveluilla on omia järjestelmän sisään rakennettuja hakutoimintoja, joilla ihmisiä voi olla helpompi löytää eri hakuehdoin esimerkiksi asuinpaikan perusteella. Facebookista löytyi aikaisemmin erittäin tehokas ja yksityiselämän suojan kannalta kritiikkiä herättänyt hakukone Graph Search. Kyseisellä hakuominaisuudella pystyi tekemään erittäin monipuolisia hakuja, ja palvelun itsensä lisäksi se yhdisteli tietoja myös Bing-hakukonetta hyväksikäyttäen.[269]

[265] Tällöin tieto voi tulla poliisin tietoon myös viiveellä, mutta PolL 5:51:n ja PKL 10:53:n mukainen velvollisuus tarkastaa tallenteet ilman aiheetonta viivytystä pitää tiedonhankinnan lähellä reaaliaikaista.

[266] Kerätyn tiedon laajuus onkin reaalimaailman osalta selvässä yhteydessä tiedonhankinnan reaaliaikaisuuteen.

[267] Ks. laajasti erilaisista reaalimaailman tarkkailun muodoista Siljander – Fredrickson 2016, s. 23–56.

[268] Tiedon keräämisestä käytetään tietoverkoissa usein muotoa tiedonlouhinta, mutta tässä tutkimuksessa puhutaan tiedon keräämisestä, koska määritelmänä se sopii paremmin profiileilla tapahtuvaan toimintaan. Lisäksi voidaan todeta, että tiedon keräämistapa on yhteydessä poliisimiehen ammattitaitoon ja kokemukseen, koska siinä missä reaalimaailmassakin, myös tietoverkoissa silmä harjaantuu havaitsemiaan erinäisiä seikkoja. Ks. tiedonkerääjän ammattitaidon merkityksestä yleisesti esimerkiksi Gravelle 2012 s. 114–120.

[269] Kyseinen hakukone on nykyään vain osittain käytössä. Ks. esimerkiksi tarkemmin Twitteriä ja Facebookia koskevista tiedonhankintatekniikoista Bazzell 2014, s. 39–90.

Omanlainen profiileihin liittyvä hakumahdollisuus on myös #:n, eli risuaitamerkin (hashtag) käyttäminen, jolla haetaan tietoa yleensä erilaisiin teemoihin tai tapahtumiin liittyvää tietoa esimerkiksi Twitterissä. Näitä voivat olla muun muassa mielenosoituksiin tai muihin poliisia kiinnostaviin tapahtumiin liittyvät tiedot.[270]

Tietoverkkoihin kohdistuvassa tarkkailussa voidaan käyttää avuksi myös perinteisiä hakukoneita, kuten Googlea.[271] Kaikkien saatavilla on lisäksi erilaisia ilmaisia sivustoja ja sovelluksia, joiden avulla voidaan hakea tietoa tietoverkoista.[272] Yleensä hakuja voidaan suorittaa usean sanallisen hakukriteerin avulla, mutta myös esimerkiksi kohdehenkilön ottamalla tai hänestä otetulla valokuvalla.[273] Lisäksi tietoa voidaan hakea sijaintitiedon perusteella.[274] Vaikka kyseiset hakumahdollisuudet eivät välttämättä tarvitse profiilia tai muuta erillistä käyttäjätiliä, voidaan ne lähtökohtaisesti laskea mukaan luontevaksi osaksi poliisi- ja peiteprofiileilla tapahtuvaan toimintaan.[275] Profiileja voi käyttää lisäksi välillisesti erilaisten hakurobottien (web crawler) avulla tapahtuvassa tiedonhankinnassa, joilla voidaan hakea laajoja datamassoja analysoitavaksi.[276] Oma haaste laajemman tiedonkeruun kannalta on darknet, koska perinteiset tiedonkeräämistavat esimerkiksi terroristisoluihin liittyen eivät välttämättä toimi darknetissa samalla tavalla erilaisen toimintaympäristön takia.[277]

---

[270] Erilaisia mielenosoituksia ja aktivisteja seuraavat myös jotkut isot yritykset sosiaalisessa mediassa tarkoituksenaan estää kritiikin leviäminen laajemmalle. Ks. aiheesta tarkemmin Uldam 2018, s. 130.

[271] Nykypäivänä kansalaisilla on myös mahdollisuus saada tiettyjä hakutuloksia estettyä ja puhutaan niin sanotusta oikeudesta tulla unohdetuksi. Ks. tähän liittyen EUT:n ratkaisu C-131/12 *Google Spain SL ja Google Inc. v. Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* (2014) EUVL:C:212. Ks. myös KHO 2018:112. Tieto ei tosin poistu sivulta, jolla se on julkaistu ja voi näkyä muilla hakukoneilla, joista sitä ei ole pyydetty poistamaan.

[272] Näistä voidaan mainita esimerkkeinä www.pipl.com, joka kerää tietoja useista eri sosiaalisen median lähteistä ja voi kertoa esimerkiksi suoraan henkilön iän, jos se on jostain palvelusta saatavilla.

[273] Valokuvalla hakeminen on mahdollista esimerkiksi Googlen hakukoneella, mutta myös erillisiä sivustoja löytyy. Näistä voidaan mainita esimerkkinä www.tineye.com.

[274] Tällaisesta toimii esimerkkinä palvelu nimeltä Geofeedia, jota esimerkiksi poliisi käytti Yhdysvalloissa hyväkseen valvoessaan suurta U.S. Open of Surfing -kilpailua, johon saapuu joka vuosi puoli miljoonaa vierasta. Poliisi käytti paikkaperustaisen haun lisäksi hakusanoja kuten ”gun”, ”fight”, ”shoot” ja ”riot” valvoessaan tapahtumaa. Kyseinen toiminta osoittautui toimivaksi ja poliisi sai esimerkiksi sitä kautta näyttöä tapahtumassa puhjenneeseen mellakkaan. Ks. tapauksesta tarkemmin Amecian City & County 2015.

[275] Sosiaalisen median osalta taas on yleistä, että jos palvelussa on oma profiili, on myös hakumahdollisuudet laajemmat.

[276] Ks. tarkemmin hakurobotin käsitteestä ja toiminnasta Semenov 2013, s. 46–50. Sosiaalisen median osalta voidaan käyttää myös määritelmää ”profile crawlers”, jossa tietoja kerätään tietyn sosiaalisen median palvelun sisällä. Ks. tästä tarkemmin Voigt – Hinz – Jansen 2013, s. 7. Ks. tarkemmin sosiaaliseen mediaan liittyvistä tiedonkeräämisohjelmista Erbschloe 2019 s. 85–87. Käytännössä profiilien käyttö voisi tapahtua esimerkiksi siten, että luodaan useita peiteprofiileja ja pyritään hakeutumaan laajasti erilaisten henkilöiden kaverilistoille, joiden perusteella voidaan hakea hakurobottiin yhdistettynä tietoa.

[277] Voidaan esimerkiksi vaatia laajemmin tietoteknisen tutkijan ja etnografiikon yhteistyötä. Ks. tarkemmin Kenney – Coulthart 2015, 68–70.

Erityisten toimivaltuuksien kohdalla tiedon kerääminen poliisi- ja peiteprofiileilla perustuu vuorovaikutukseen siinä missä reaalimaailmassakin. Niin kuin tarkkailutyyppisissä keinoissakin, voi myös erityisillä toimivaltuuksilla saada kerättyä tietoa laajemmin kuin pistemäisessä reaalimaailman vuorovaikutuksessa. Vuorovaikutuksessa voidaan esimerkiksi saada näkyvyys kohdehenkilön profiilin yksityisyysasetuksin suljettuihin osiin ja vuorovaikutustilanteen lisäksi poliisimies voi löytää profiilista paljon laajemmin sellaista tietoa, jota ei välttämättä käydä läpi reaalimaailmassa tapahtuvan vuorovaikutuksen aikana.[278] Tietoverkoissa tapahtuvaan vuorovaikutukseen perustuvaa tiedonkeruuta voidaan pitää poliisin näkökulmasta helpompana toteuttaa, koska vuorovaikutukseen liittyy suurempi anonymiteetin mahdollisuus. Jatkossa tekninen kehitys voi mahdollistaa myös erilaiset tekoälyyn liittyvät ratkaisut vuorovaikutuksen toteuttamiseen, mutta toistaiseksi poliisi- ja peiteprofiileilla tulee olla luonnollinen henkilö taustalla ohjaamassa toimintaa.[279]

Oli kyse reaalimaailmassa tai tietoverkoissa tapahtuvasta toiminnasta, voi poliisi kerätä tietoa kohdehenkilöstä 1) useista eri käytössään olevista rekistereistä ennen varsinaisen salaisen toimivaltuuden käyttämistä, mutta myös 2) suorittaa PolL 4:2–3:ään perustuvia tiedonsaantipyyntöjä. Poliisin käytössä olevista rekistereistä voidaan mainita esimerkkeinä Poliisin tiedustelujärjestelmä (POTI), Patja, aseluparekisteri, henkilökortti- ja passirekisteri, ulkomaalaisrekisteri, väestötietojärjestelmä.[280] Lisäksi kohdehenkilöstä voidaan kerätä tietoja POV:n päätöksellä muilta viranomaisilta sekä yksityiseltä yhteisöltä tai henkilöltä PolL 4:2:n ja 4:3:n tiedonsaantioikeussäännöksiin liittyen.[281] Rekisterikyselyt tai tiedonsaantipyynnöt eivät ole salaisia tiedonhankinta- tai pakkokeinoja. Siten niitä ei

[278] Esimerkkinä voidaan mainita tilanne, jossa peitetoimintaa suorittava poliisimies hakeutuu kohdehenkilön kaverilistalle, jonka seurauksena hänelle voi avautua suuri määrä tietoa kohdehenkilöön liittyen. Ks. esimerkkinä tällaisesta tilanteesta Forss 2014, s. 100, jossa lehtitietojen mukaan Facebookissa oli esiinnytty Naton Euroopan joukkojen komentajana ja saatu useita Iso-Britannian armeijan ja virkamieskoneiston henkilöitä hyväksymään kyseinen valeprofiili kaverilistalleen. Tiedotusvälineissä tekijäksi arveltiin vierasta valtiota. Todettakoon tässä yhteydessä, että Suomessa voimassa olevan lain mukaan poliisi ei voi esiintyä kyseiseen tapaan toisena luonnollisena henkilönä, koska kyseessä olisi identiteettivarkaus (RL 38:9a).

[279] Ks. esimerkiksi Terre des Hommes 2013, s. 54, jossa kerrotaan Sweetiestä. Sweetie oli digitaalisesti luotu 10-vuotias tyttö, jota käytettiin webkameran kautta peiteoperaatiossa lasten seksuaaliseen hyväksikäyttöön liittyen. Vaikka kyse oli digitaalisesti luodusta hahmosta, varsinainen vuorovaikutus tapahtui kuitenkin ihmisten toimesta kyseistä digitaalista hahmoa ohjaamalla.

[280] POTI kattaa esimerkiksi entisen epäiltyjen tietojärjestelmän EPRI:n, jonka osalta POTI:ssa on estävän ja paljastavan toiminnan tietoryhmä (ESPA). POTI:n käyttö alkoi vuoden 2018 lopussa ja kyseiseen järjestelmään kirjataan havaintotietoja ja niiden jatkojalostamiseen liittyviä tiedustelun asia -tietoja. Ks. POTI:n sisällöstä tarkemmin tiedote Poliisihallitus 2018b. Väestötietojärjestelmästä selviää sukulaissuhteet, asuinpaikan, siviilisäädyn, kansalaisuuden, mahdollisesti ammatin ja huostaanottoasiat.

[281] PolL 4:2:n koskee viranomaisilta saatavaa tietoa. PolL 4:3.1:n mukaiset pyynnöt tehdään rikoksen estämiseksi tai selvittämiseksi ja PolL 4:3.2:n mukaiset pyynnöt teleosoitteen omistajan tai käyttäjän selvittämiseksi.

myöskään sido erilaiset salaisiin tiedonhankinta- ja pakkokeinoihin liittyvät kattavat oikeusturvatakeet.[282]

Sosiaalisen median palveluista ja erilaisilta internet-sivustoilta voi saada muutoin piilotettuja asiakas- ja rekisteröitymistietoja PolL 4:3.2:n perusteella, jolloin voi selvitä esimerkiksi käyttäjän sähköpostiosoite, puhelinnumero ja rekisteröitymisessä käytetty IP-osoite. [283] Kyseinen mahdollisuus onkin saanut kritiikkiä osakseen erityisesti rekisteröitymiseen käytetyn IP-osoitteen hankkimismahdollisuudesta, koska sillä voi olla mahdollista tunnistaa käyttäjä siinä missä televalvonnallakin. Edellytykseksi riittää kuitenkin pelkkä POV:n päätös ja tarve yksittäisen tehtävän hoitamiseen liittyen.[284] Lisäksi poliisi voi PolL 4:3.1:n perusteella saada tietoja useista eri lähteistä. Näitä ovat esimerkiksi joukkoliikenteen käyttäminen, laivan matkustajatiedot, Kansaneläkelaitoksen sekä pankkien asiointi- sekä tilitiedot.[285]

> OSINT-tietoa tai muutoin esimerkiksi kaverilistalla olemisen perusteena saatavaa tietoa ei pidä sekoittaa sosiaalisen median palveluiden sisäisiin tietoihin, joita palvelut voivat kerätä käyttäjän suostumukseen perustuen suuria määriä. Tieto ei välttämättä edes pysy tietyssä yhdessä palvelussa, vaan yhtiöt voivat kaupata tietoja toisilleen joko laillisesti tai ainakin lain rajamailla. Näitä tietoja ei yleensä jaeta viranomaisille.[286]

Rekisterikyselyjen voidaan katsoa olevan ei-reaaliaikaista tietoa ja esimerkiksi POTI-järjestelmässä voi olla laajasti aikaisemman tarkkailutoiminnan havaintotietoja. Myöskään PolL 4:2–3:n sääntelyn mukaiset tiedot eivät yleensä ole reaaliaikaisia, mutta niillä voidaan kerätä erittäin kattavasti tietoa kohdehenkilöstä. Herääkin kysymys miksi ei-reaaliaikaisten tietojen kerääminen avoimesta profiilista, jossa yleensä kohdehenkilö on tehnyt julkaisupäätöksen, on suojattu kattavammin kuin poliisin käyttäjästä eri tahoilta saatavat

[282] Yhtenä oleellisena esimerkkinä voidaan mainita kohteelle ilmoittaminen (PolL 5:58 ja PKL 10:60).
[283] Poliisilla voi kuitenkin olla vaikeuksia saada tietoa esimerkiksi sosiaalisen median palveluntarjoajilta suoraan, koska ulkomaalaisia palveluntarjoajia ei velvoita Suomen lainsäädäntö. Ks. esimerkiksi Facebookille toimitettaviin tietopyyntöihin liittyvistä haasteista Voigt – Hinz – Jansen 2013, s. 8 Tietoverkoista voi saada tietopyyntöihin liittyen yllättävääkin tietoa. Esimerkiksi Yhdysvaltalainen sukulaissuhteita DNA:n perusteella selvittelevä sivusto www.familytreedna.com on antanut sikäläiselle poliisille tietoja tietokannastaan, jotta esimerkiksi väkivaltarikoksen tehnyt tai tuntematon kuollut henkilö voitaisiin tunnistaa. Ks. yrityksen tiedote asiasta FamilyTreeDNA 2019.
[284] Ks. kritiikistä Savola 2013, s. 902–904. Ks. myös Metsäranta 2013, s. 10.
[285] Ks. myös HE 202/2017 vp, s. 223, jossa todetaan, että PolL 4:3.1:stä vastaavan siviilitiedustelua koskevan PolL 5a:50:n perusteella voi saada tietoa kohdehenkilön tunnistamiseksi ja tavoittamiseksi sekä hänen yhteystiedoista, liikkumisesta ja taloudellisesta toiminnasta.
[286] Ks. esimerkiksi The New York Times 2018, jossa kerrotaan Facebookia kohdanneesta skandaalista, jossa se antoi esimerkiksi hakupalvelu Bingille näkyvyyden salaisiin kaverilistoihin, Netflixille ja Spotifylle mahdollisuuden lukea yksityisviestejä ja Amazonin saada käyttäjien yhteystietoja.

julkisuudesta ainakin osittain salassa pidettävät tiedot? Etenkin kun tätä toimintaa ei koske salaisia tiedonhankinta- ja pakkokeinoja koskevat oikeusturvatakeet. Käytännössä tietoa voidaankin hankkia laajasti kohteelta salassa jo ennen varsinaisen salaisen tiedonhankinta- tai pakkokeinon aloittamista. Keräämistapa ei ole tietoverkoissa muutoinkaan yleensä reaaliaikaiseen fyysiseen seurantaan rinnastuvaa, vaan tarkkailutoiminta rinnastuu mieluummin esimerkiksi henkilön kirjoittaman päiväkirjan, avatun kirjeen, kirjan, kaupan ilmoitustauluilmoituksen, sanomalehden mielipidekirjoituksen tai muun vastaavan julkaisun havainnointiin. Tällaisten julkaisujen seuraaminen ei ole vielä reaalimaailmassa tarkkailua, koska se ei kohdistu fyysisesti henkilön toimintaan, joten miksi se olisi sitä tietoverkoissa? Tällä hetkellä tulkinta lähtee kuitenkin siitä, että tietoverkoista tapahtuva ei-reaaliaikainenkin tiedonhankinta tulkintaan tarkkailutyyppiseksi toiminnaksi, vaikka ääritapauksessa tarkkailtava henkilö voi olla jopa jo kuollut.[287]

### *3.4.6 Tiedon laatu ja luotettavuus*

Reaalimaailmassa tiedon laadulle on tehty selvät erot teknistä tarkkailua koskevassa sääntelyssä, jossa on erotettu kuuntelu (PolL 5:17 ja PKL 10:16), katselu (PolL 5:19 ja PKL 10:19), seuranta (PolL 5:21 ja PKL 10:21) ja teknisen laitteen tarkkailu (PolL 5:23 ja PKL 10:23). Esimerkiksi kuuntelussa ja katselussa erot ovat selvästi havaittavissa, koska laadullisesti ääntä pidetään heikommin suojattuna kuin kuvaa. Tämä käy hyvin ilmi asuntokuuntelussa (PKL 10:17), joka on mahdollista vain pakkokeinolain osalta, eikä asutun asunnon tekninen katselu ole lainkaan mahdollista. Lisäksi pelkän sijainnin määrittämisen katsotaan puuttuvan vähemmän yksityiselämän suojaan kuin kuvan tai äänen, koska niillä saadaan laajemmin tietoa henkilön käyttäytymisestä, mielipiteistä ja tunteista.[288] Laatuun kiinteästi sidoksissa olevan luotettavuuden osalta ei reaalimaailmassa ole yleensä ongelmaa. Tieto perustuu poliisimiehen omiin aistihavaintoihin, joten problematiikka koskee lähinnä väärin tulkittuja tai kirjattuja havaintoja.[289]

---

[287] Tietoverkkoihin on luonnollisesti jäänyt paljon jo kuolleidenkin henkilöiden tuottamaa materiaalia ja esimerkiksi Facebookin osalta on käytössä niin sanottu muistotiliominaisuus, jossa jo menehtyneen henkilön sosiaalisen median käyttäjätili voidaan jättää tietoverkkoon saataville. Ks. kuolleen henkilön perus- ja ihmisoikeussuojasta Forss 2017, s. 172. Läheskään aina henkilön kuolemasta kertovaa tietoa ei ole saatavilla ja tietoverkoista löytyy jo nyt valtavat määrät tietoa, jonka sinne on lisännyt jo menehtynyt henkilö.

[288] Ks. *Uzun v. Saksa* (2010), kohta 52.

[289] Vaikka poliisimiestä voidaan pitää oman alansa ammattilaisena esimerkiksi tarkkailutoimintaan liittyen, ei poliisimieskään ole immuuni havaintovirheille. Ks. esimerkiksi silminnäkijätunnistamisen luotettavuuden virhelähteistä todistajapsykologian näkökulmasta Niskakangas – Lahtinen – Tolvanen 2017, s. 868–869.

Tietoverkkojen osalta suojan tasoja voitaisiin jaotella reaalimaailman tapaan sen perusteella, onko kerätty tieto kirjoitusta, kuvia, ääntä, videokuvaa tai onko kyse sijaintitiedosta. Tietoverkoissa ei ole olemassa teknisen tarkkailun kaltaista laadullista jaottelua, eikä se olisi järkevääkään, koska tietoverkkoon tuotettu tieto perustuu lähtökohtaisesti aikaisemmin käsitellyn mukaisesti kohdehenkilön tekemään julkaisupäätökseen.[290] Tietoverkkoihin liittyen tulisi ottaa huomioon mahdollisuudet analysoida laajaa datamassaa reaalimaailman yleensä pistemäiseen tiedonhankintaan verrattuna. Laajat tietomassat voivat mahdollistaa henkilön käyttäytymiseen ja ominaisuuksiin perustuvan analyysin aivan eri tehokkuudella kuin reaalimaailmassa, jolloin saadaan yleensä laadullisestikin hyödyllisempää tietoa kohteesta. Esimerkiksi Facebook-tykkäyksien perusteella voidaan päätellä ikä, seksuaalinen suuntautuminen, etnisyys, uskonto, poliittiset näkemykset, persoonallisuuden piirteet, älykkyys, onnellisuus ja addiktoivien aineiden käyttö melko tarkasti. [291] Tämä ei ole yleensä mahdollista reaalimaailmassa kuin pitkään jatkuneella suunnitelmallisella tarkkailulla tai soluttautumisella.[292] Toisaalta myös tietoverkoissa tämä voi edellyttää soluttautumista, jos henkilö on sulkenut tietonsa yksityisyysasetuksin.[293]

Tietoverkoista avoimesti saatavan tiedon laatuun vaikuttaa olennaisesti tiedon luotettavuus. Vaikka tietoa olisikin saatavilla laajasti, ei kerätyllä tiedolla ole välttämättä mitään käyttöä poliisille, jos tiedon todenperäisyyttä ei pystytä varmistamaan. Kerätyn tiedon laatua voidaan arvioida luotettavuuden näkökulmasta joko 1) poliisin toiminnan tai 2) kohdehenkilön toiminnan perusteella. Tietoverkoissa tapahtuvassa toiminnassa dokumentoinnin toteuttamisen helppous ja tarkkuus ovat esimerkiksi vaikuttaneet siihen, että peitetoiminnan erityisten edellytysten raja on tietoverkoissa alempi kuin reaalimaailmassa.[294] Tämä on yhteydessä siihen, että poliisin tietoverkoista dokumentoituja havaintoja voidaan pitää lähtökohtaisesti luotettavampia, kuin jälkikäteen poliisimiehen

[290] Tiedon laatu on yhteydessä myös aikaisemmin puheena olleeseen tiedon keräämisen kohteeseen, jossa tietoa voidaan saada laajasti myös muilta kuin kohdehenkilöltä itseltään.
[291] Ks. aiheeseen liittyvästä tutkimuksesta kokonaisuudessaan Kosinski – Stillwell – Graepel 2013, jossa analysointiin aineistoa yhteensä 58 000 vapaaehtoisen Facebook-tykkäysten perusteella.
[292] Tulee tosin ottaa huomioon, että osa näistä tiedoista voidaan kerätä suoraan erilaisista rekistereistä ja edellä käsiteltyjen PolL 4:2–3:n sääntelyyn liittyen.
[293] Siten tulee myös ottaa huomioon se, että kyse on lähtökohtaisesti henkilön omasta valinnasta sen suhteen, mitä tietoa hän haluaa asettaa avoimesti esille itsestään. On tosin otettava huomioon, että kohdehenkilöstä voidaan julkaista tietoa muidenkin toimesta tai kyse voi olla esimerkiksi järjestelmän häiriöstä, niin kuin on jo aikaisemmin esitetty.
[294] Ks. HE 224/2010 vp, s. 116; HE 222/2010 vp, s. 339.

reaalimaailman toiminnasta tehtyjen havaintojen kirjaamista.[295] Jostain syystä tämä tulkinta ei kuitenkaan ole vaikuttanut muihin säännöksiin.

Arvioidessa tiedon luotettavuutta kohteen toiminnasta tehtyjen havaintojen näkökulmasta, voidaan reaalimaailmassa tehtyjä havaintoja luonnehtia luotettaviksi. Tietoverkkojen osalta tilanne on kuitenkin päinvastainen, koska kyse on julkaistusta materiaalista, joka on voitu keksiä tai sitä on voitu muokata ja vääristellä halutulla tavalla.[296] Tietoverkoissa henkilö voi merkata itsensä toiselle puolelle maapalloa, vaikka samaan aikaan istuisikin kotisohvalla. Samaan tapaan kohdehenkilö voi viestiä tavanneensa jonkun toisen henkilön jossain tietyssä paikassa, vaikka näin ei ole oikeasti tapahtunut. Kohdehenkilö voi myös keksiä itselleen erilaisia ominaisuuksia, joita hänellä ei tosiasiallisesti ole. Tiedon luotettavuuden heikkouden takia OSINT-tieto määritelläänkin yleensä laajasti saatavilla olevaksi, mutta ei välttämättä tarkaksi, luotettavaksi tai päteväksi.[297] Poliisi jakaa havaintotiedot tiettyjen luotettavuusmääritteiden mukaisesti ja jos arvioidaan tietoverkon avoimista lähteistä saatua tietoa, on sen luotettavuus lähtökohtaisesti heikko.[298] Tiedon oikeellisuutta voidaan tosin arvioida erilaisin keinoin ja mitä ammattitaitoisempi sekä kokeneempi poliisimies on, sitä paremmin poliisimies pystyy arvioimaan tietoverkoista löydetyn tiedon luotettavuutta.[299]

Arvioitaessa tiedon laadun ja luotettavuuden vaikutusta yksityiselämän suojaan, voidaan mainita myös PKL 8:20:n mukainen laite-etsintä. Kyseisellä tiedonhankintatavalla saadaan rikoksesta epäillyltä esimerkiksi koko älypuhelimen tai pöytätietokoneen data, jossa voi olla vuosienkin ajalta erilaisia arkaluontoisia viestejä, kuvia ja kuvatallenteita, jonka takia puuttuminen yksityiselämän suojaan voi olla erittäin tuntuva.[300] Tiedon kerääminen laite-etsinnässä ei kuitenkaan tapahdu kohdehenkilöltä salassa, joka taas vaikuttaa vahvasti salaisten tiedonhankinta- ja pakkokeinojen sääntelyyn, koska kansalaisella on heikompi

[295] Teknisen tarkkailuun liittyvien katselun ja kuuntelun taas voidaan katsoa rinnastuvan tietoverkoihin dokumentoinnin luotettavuuden osalta, mutta lainsäätäjä ei ole arvioinut tämän vaikutusta erityisiin edellytyksiin.

[296] Koska netissä ei ole ilmeitä, eleitä ja äänensävyjä, voi pelkkä teksti olla myös suhteellisen harhaanjohtavaa reaalimaailmaan verrattuna. Tähän liittyvät myös aikaisemmin käsitelty deepfake-tekniikan käyttäminen ja erilaiset RL 17:18.4:ssä mainitut todenmukaiset kuvat tai kuvatallenteet.

[297] Wells – Gibson 2017, s. 94.

[298] Ks. tähän liittyen Poliisihallitus 2016c, s. 10, josta ilmenee poliisin käyttämä neliasteiden tiedon oikeellisuuden luokittelu. Luokittelua tarkastellaan tarkemmin tietolähdetoimintaa koskevassa osiossa.

[299] Ks. esimerkiksi Forss 2014, s. 103–104, jossa käydään läpi erilaisia seikkoja, joista voi tunnistaa valeprofiilin.

[300] Ks. KKO 2018:77. Korkein oikeus totesi, että kotietsinnän yhteydessä toimitettu laite-etsintä oli omiaan lisäämään luottamukselliselle viestinnälle ja yksityiselämän suojalle aiheutetun loukkauksen tuntuvuutta. Laite-etsintä voidaan toimittaa PKL 8:27:n mukaisesti myös etäetsintänä, joka voi koskea esimerkiksi pilvipalveluja.

mahdollisuus kontrolloida poliisin toimintaa.[301] Ottaen kuitenkin huomioon erityisesti kerätyn tiedon laajuus, laatu ja luotettavuus, voidaan yksityiselämään puuttumisen katsoa olevan selvästi tuntuvampi kuin esimerkiksi poliisi- tai peiteprofiililla tapahtuvassa suunnitelmallisessa tarkkailussa.[302] Laite-etsinnässä erityisenä edellytyksenä on kuuden kuukauden rangaistusmaksimi (PKL 8:21), kun suunnitelmallisen tarkkailun osalta se on kaksi vuotta (PolL 5:13.3 ja PKL 10:12.3). On vaikea perustella eroa pelkästään suunnitelmallisen tarkkailun salavihkaisella luonteella. Etenkin kun suunnitelmallisesta tarkkailusta ja salaisista tiedonhankinta- ja pakkokeinoista yleensä joka tapauksessa ilmoitetaan kohteelle.[303]

### 3.5 Yhteenveto perus- ja ihmisoikeussuojan eroista reaalimaailmassa ja tietoverkoissa

Edellä on käsitelty kotirauhan suojaa, luottamuksellisen viestin suojaa ja yleisesti yksityiselämän suojaa salaisten tiedonhankinta- ja pakkokeinojen näkökulmasta. Tarkastelua on tehty lähinnä tarkkailutyyppisiä keinoja sekä erityisiä toimivaltuuksia koskien. Kotirauhan suojan merkitys tietoverkoissa voidaan katsoa olevan minimaalinen, eikä juuri aiheuta tulkintaongelmia. Luottamuksellisen viestinnän näkökulmasta voi syntyä tulkintaongelmia tilanteissa, joissa kyse on suljetuissa ryhmissä tai profiilissa tapahtuvasta viestinnästä. Selvästi vaikeimmin hahmotettavissa ovat yleisesti yksityiselämän suojaa koskevat erot reaalimaailman ja tietoverkkojen välillä. *Koulu* kuvaa reaalimaailman ja tietoverkkojen eroja yleisellä tasolla siten, että tietoverkoissa on mahdollisuus irtautua ajasta ja paikasta, identiteetin pysyvyydestä ja aineellisesta materiasta, joiden lisäksi keskeisiä piirteitä ovat vuorovaikutteisuus sekä kommunikatiivisuus. Oikeudellisesti tietoverkkoihin liittyvä toiminta ei ole Koulun mukaan tällä hetkellä kaikilta osin ennakollisesti ratkaistavissa, vaan tarve erityispiirteiden huomioimiselle ja analogiatulkinnan tehokkuus on ratkaistava jokaisessa tulkintatilanteessa erikseen.[304]

---

[301] Toisaalta huomioon tulee ottaa PKL 8:24:n mukainen datan säilyttämismääräys, jossa datan säilyttämismääräyksen saanut on velvollinen pitämään toiminnan PKL 8:26:n perusteella salassa.

[302] Ks. myös laajemmin intresseistä suojata yksityiselämää salaisiin tiedonhankinta- ja pakkokeinoihin liittyen Metsäranta 2015, s. 26–31.

[303] Ks. salaisten tiedonhankinta- ja pakkokeinojen epätasapainosta muihin toimivaltuuksiin nähden KRP 2009, s. 7–10, jossa verrattiin silloisia salaisia keinoja PKL 8 lukuun sekä muiden viranomaisten toimivaltuuksiin. Ks. salavihkaisuuteen liittyen Poliisihallitus 2018c, s. 11, 16 ja 28. Salaisia tiedonhankinta- ja pakkokeinoja koskevan kertomuksen mukaan on erittäin harvinaista, ettei kohteelle ilmoitettaisi toimivaltuuden käytöstä, jonka lisäksi ilmoituksen siirtämisiä on vähän.

[304] Koulu 2012, s. 284–285. Ks. tietoverkkojen ja reaalimaailman oikeudellisen sääntelyn eroista yleisellä tasolla lisäksi kokonaisuudessaan artikkelit Gillen 2012 ja Svantesson 2005. Svantesson katsoo reaalimaailman ja tietoverkkojen analysoimisen välttämättömäksi oikeudellisten erojen hahmottamisessa ja Gillen taas tarjoaa välineeksi niin sanotun autopoeeisen teorian, joka ottaisi paremmin huomioon tietoverkot omana entiteettinään.

Tilanteen ei pitäisi luonnollisesti olla etenkään salaisten tiedonhankinta- ja pakkokeinojen osalta tällainen, joilla puututaan merkittävissä määrin ihmisten oikeuksiin. Sääntelyn perusteella ei ole kuitenkaan saatavissa selviä tulkintaperiaatteita siitä, miten reaalimaailman ja tietoverkkojen erojen tulisi vaikuttaa sääntelyyn. Toisaalta perus- ja ihmisoikeusnormit ovat muutoinkin väljiä ja sisältävät harkintavaltaa.[305] On kuitenkin ongelmallista määritellä perus- ja ihmisoikeuksien vaikutusta yksittäiseen toimivaltuuteen, jos eroja ei ole huomioitu riittävällä tavalla. Koulun linjauksen mukaan, jokainen tilanne tulee tulkita tapauskohtaisesti, jos selvää tarkkarajaista ja täsmällistä sääntelyä ei ole. Poliisilla ei kuitenkaan ole mahdollisuutta tehdä toimivaltuuksista laajentavia tulkintoja. Tämä sen takia, että perus- ja ihmisoikeusargumenteilla ei voida heikentää kohdehenkilön oikeusasemaa, vaan pelkästään supistava tulkinta on mahdollinen.[306] Lainsäätäjän tulisikin *de lege ferenda* arvioida reaalimaailman ja tietoverkkojen vaikutusten eroja kokonaisvaltaisesti salaisia tiedonhankinta- ja pakkokeinoja koskevaan sääntelyyn. Kyseisten erojen hahmottamiseen yksityiselämän suojan eroja reaalimaailmassa ja tietoverkoissa voidaan yrittää selventää vielä kyseisellä kuviolla.

[305] Tolonen 2003, s. 136.
[306] Ks. perus- ja ihmisoikeusnormien vaikutuksesta poliisin toimivaltuuksia koskevissa harkintatilanteissa Metsäranta 2015, s. 140–144.

| | REAALIMAAILMA | TIETOVERKKO |
|---|---|---|
| **Tiedon syntymistapa** | Oleskelu | Julkaiseminen |
| **Yksilöiminen** | Yksilöitävissä | Ei yleensä yksilöitävissä |
| **Tunnistaminen** | Yleensä tunnistettavissa | Ei yleensä tunnistettavissa |
| **Kohde** | Kohdehenkilön fyysinen toiminta | Data |
| **Keräämistapa** | Aistihavainnot ja tekniset laitteet | Aistihavainnot ja haku- sekä tiedonkeräämisohjelmat |
| **Reaaliaikaisuus** | Reaaliaikaista | Ei yleensä sidottu aikaan tai paikkaan |
| **Laajuus** | Pistemäistä | Laajaa |
| **Laatu** | Äänen, kuvan ja sijaintitiedon erot | Analysointimahdollisuudet |
| **Luotettavuus** | Luotettavaa | Yleensä epäluotettavaa |

Kuvio 3. Yksityiselämän suojan jaottelua reaalimaailman ja tietoverkkojen välillä.

# 4 PERUS- JA IHMISOIKEUKSIEN VAIKUTUS SALAISIA TIEDONHANKINTA- JA PAKKOKEINOJA KOSKEVIIN TOIMIVALTUUKSIIN

## 4.1 Poliisin toimintaa ohjaavat yleiset periaatteet

Periaatteet on otettu lainsäädäntöön perus- ja ihmisoikeuksien korostumisen sekä niiden tärkeän merkityksen vuoksi, jonka takia periaatteiden noudattamiseen tulee kiinnittää erityistä huomiota.[307] Poliisia ohjaavista yleisistä periaatteista säädetään poliisilain 1 luvussa, jonka lisäksi pakkokeinojen käytön kannalta merkittävimmät periaatteet on otettu mukaan pakkokeinolain 1 lukuun, jotka ovat osittain päällekkäiset poliisilain periaatteiden kanssa. Oma vaikutuksensa on myös esitutkintalain 4 luvun periaatteilla, jos kyseessä on pakkokeinolain mukaiset toimenpiteet. Näistä nousee selkeimmin esille salaisiin tiedonhankinta- ja pakkokeinoihin liittyen ETL 4:1:n mukainen tasapuolisuuden periaate. Jos salaisilla tiedonhankinta- ja pakkokeinoilla saadaan rikoksesta epäiltyä puolesta puhuvia tietoja, myös nämä on otettava esitutkinnassa huomioon.[308] Kaikilla näillä periaatteilla on merkitystä poliisin salaisten tiedonhankinta- ja pakkokeinojen käytölle.[309] Poliisilain yleisiä periaatteita ovat perusoikeuksien ja ihmisoikeuksien kunnioittamisen periaate (PolL 1:2), suhteellisuusperiaate (PolL 1:3), vähimmän haitan periaate (PolL 1:4), tarkoitussidonnaisuuden periaate (PolL 1:5) sekä tehtävien hoito ja tärkeysjärjestys (PolL 1:6). Pakkokeinolain yleisiä periaatteita ovat suhteellisuusperiaate (PKL 1:2), vähimmän haitan periaate (PKL 1:3) ja hienotunteisuusperiaate (PKL 1:4)

Poliisilain 1 luvun 2 §:n mukaan poliisin on kunnioitettava perusoikeuksia ja ihmisoikeuksia sekä toimivaltuuksia käyttäessään valittava perusteltavissa olevista vaihtoehdoista se, joka parhaiten edistää näiden oikeuksien toteutumista. Säännös koskee kaikkea poliisitoimintaa, joten se ulottuu myös pakkokeinolain mukaisten toimivaltuuksien soveltamiseen.[310] Poliisilain 1 luvun 3 §:n mukaan poliisin toimenpiteiden on oltava puolustettavia suhteessa

[307] HE 224/2010 vp, s. 17; HE 220/2010 vp, s. 72.
[308] Säätämisvaiheessa kyseistä periaatetta, eikä muitakaan esitutkintalain periaatteita katsottu tarpeelliseksi ottaa pakkokeinolakiin, vaikka kaikki esitutkintalain periaatteetkin tulee ottaa huomioon pakkokeinoja käytettäessä. Ks. tarkemmin HE 222/2010 vp, s. 72.
[309] Ks. poliisilain periaatteiden osalta HE 198/2017 vp, s. 9; Helminen – Kuusimäki - Rantaeskola 2012, s. 203–204 ja pakkokeinolain osalta HE 222/2010 vp, s. 46–47 ja 72. Ks. myös Metsäranta 2015, s. 197 ja 144–146, jossa myös yhteydestä hallinto-oikeudellisiin periaatteisiin.
[310] HE 224/2010 vp, s. 72.

tehtävän tärkeyteen, vaarallisuuteen ja kiireellisyyteen, tavoiteltavaan päämäärään, toimenpiteen kohteena olevan henkilön käyttäytymiseen, ikään, terveyteen ja muihin vastaaviin häneen liittyviin seikkoihin sekä muihin tilanteen kokonaisarviointiin vaikuttaviin seikkoihin.[311] Pakkokeinolain 1 luvun 2 §:n suhteellisuusperiaatetta koskeva sääntely toteaa, että pakkokeinoja saadaan käyttää vain, jos pakkokeinon käyttöä voidaan pitää puolustettavana ottaen huomioon tutkittavana olevan rikoksen törkeys, rikoksen selvittämisen tärkeys sekä rikoksesta epäillylle tai muille pakkokeinon käytöstä aiheutuva oikeuksien loukkaaminen ja muut asiat vaikuttavat seikat.[312] Suhteellisuusperiaate velvoittaa ottamaan huomioon myös ne näkökohdat, jotka puhuvat pakkokeinon käyttö vastaan, jolloin pakkokeinoa ei voida käyttää, tai sen käyttöä on rajoitettava.[313]

Myös vähimmän haitan periaatteen osalta poliisi- ja pakkokeinolain säännökset ovat miltei identtiset. Poliisilain 1 luvun 4 §:n mukaan poliisin toimenpiteillä ei kenenkään oikeuksiin saa puuttua enempää eikä kenelläkään saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Pakkokeinolain 1 luvun 3 §:ssä taas säädetään, että pakkokeinojen käytöllä ei kenenkään oikeuksiin saa puuttua enempää kuin on välttämätöntä käytön tarkoituksen saavuttamiseksi. Pakkokeinon käytöllä ei myöskään saa aiheuttaa kenellekään tarpeettomasti vahinkoa tai haittaa.[314]

Poliisilain 1 luvun 5 §:n mukaan poliisi saa käyttää toimivaltuuttaan vain säädettyyn tarkoitukseen. Pakkokeinolain puolelta kyseistä periaatetta ei löydy.[315] Toisaalta tarkoitussidonnaisuuden periaate koskee myös pakkokeinojen käyttämistä ja esitutkintaa yleisesti. Poliisin puuttuessa yksilön oikeuksiin tai velvollisuuksiin, tulee toimivaltuussäännöksen löytyä laista.[316] Poliisilain 1 luvun 6 §:n mukaan poliisin on toimittava asiallisesti ja puolueettomasti sekä yhdenvertaista kohtelua ja sovinnollisuutta

[311] Lakivaliokunta on todennut valeostoa koskevan lausuntonsa 7/2000 vp, s. 5 yhteydessä, että suhteellisuusperiaate voi rajoittaa valeoston käyttämistä silloin, kun epäilty rikos on vähäinen, vaikka sen lain mukainen enimmäisrangaistus olisikin valeoston edellytykset täyttävä.

[312] Vaikka periaatteet ovat kirjoitettu eri tavoin, voidaan niiden katsoa vastaavan toisiaan suurimmilta osin. Poliisilain suhteellisuusperiaatteessa on kuitenkin huomioitu paremmin se, että poliisimies saattaa joutua tilanteisiin, joissa merkitystä on myös tehtävän vaarallisuudella ja toimenpiteen kohteena olevan henkilön käyttäytymisellä. Ks. tarkemmin HE 224/2010 vp, s. 17. Esitutkintalain 4 luvun 4 §:ssa olevassa suhteellisuusperiaatteessa on poliisi- ja pakkokeinolain periaatteiden sisältö yhdistettynä.

[313] Tällainen voi olla esimerkiksi pakkokeinon keston rajaaminen. Ks. tarkemmin HE 22/1994 vp, s. 35. Ks. myös Metsäranta 2015, s. 146–147.

[314] Esitutkintalain 4 luvun 5 §:n mukainen sääntely on myös samanlainen poliisi- ja pakkokeinolain vähimmän haitan periaatteen kanssa.

[315] Ei myöskään esitutkintalain puolelta.

[316] Tarkoitussidonnaisuuden periaate on johdettavissa PL 2.3 §:stä, jonka mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Ks. tarkemmin HE 224/2010 vp, s. 18 ja 73.

edistäen. Poliisin tulee ensisijaisesti neuvoin, kehotuksin ja käskyin pyrkiä ylläpitämään yleistä järjestystä ja turvallisuutta. Poliisin tehtävät on hoidettava tehokkaasti ja tarkoituksenmukaisesti. Olosuhteiden vaatiessa tehtävät on asetettava tärkeysjärjestykseen. Pakkokeino- tai esitutkintalain puolelta vastaavaa säännöstä ei löydy. Vaikka säännöstä ei yleensä mainita salaisten tiedonhankinta- ja pakkokeinojen yhteydessä, on sillä vaikutusta niidenkin osalta, koska esimerkiksi yhdenvertaisen kohtelun edistäminen liittyy kiinteästi PL 6 §:ään, eikä kehenkään saa kohdistaa kyseisiä keinoja esimerkiksi kielen, uskonnon tai alkuperän takia.[317]

Pakkokeinolain 1 luvun 4 §:n mukaan pakkokeinoja käytettäessä on vältettävä aiheettoman huomion herättämistä ja toimittava muutenkin hienotunteisesti. Poliisilain puolelta kyseistä säännöstä ei löydy.[318] Hienotunteisuusperiaatteella tarkoitetaan sitä, että pakkokeinoja käytettäessä on vältettävä aiheettoman huomion herättämistä ja toimittava muutenkin hienotunteisesti.[319] Käytännössä kyseisen periaatteen merkitys salaisten pakkokeinojen osalta on vähäinen.[320]

### 4.2 Yleiset edellytykset

Salaisten tiedonhankinta- ja pakkokeinojen kaikkia toimivaltuuksia yhteisesti koskevat yleiset edellytykset on jaettu kolmiportaisesti 1) tuloksellisuusodotukseen, 2) erittäin tärkeä merkitys -edellytykseen ja 3) välttämättömyysvaatimukseen.[321] Yleiset edellytykset ovat poliisi- ja pakkokeinolain osalta identtiset (PolL 5:2 ja PKL 10:2). Yleisten edellytysten rinnalla on myös huomioitava PolL 5:2.3:n ja PKL 10:2.3:n sääntely, jonka mukaan salaisen tiedonhankinta- tai pakkokeinon käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Mitä tuntuvammin tiedonhankinta- tai pakkokeino puuttuu henkilön oikeuksiin, sitä vahvemmat vaatimukset toimivaltasäännöksen yleisillä edellytyksillä on.[322]

---

[317] HE 224/2010 vp, s. 73. Tällainen kielletty tilanne voisi tulla kyseeseen esimerkiksi tapauksessa, jossa terrorismin torjuntaa toteutettaisiin sen perusteella, mitä uskontokuntaa hän edustaa.
[318] Esitutkintalain 4 luvun 6 §:stä löytyy kuitenkin vastaava periaate.
[319] HE 222/2010 vp, s. 72.
[320] Salaisia pakkokeinoja käytetään nimensä mukaisesti salassa, joten mahdollisuudet siihen että pakkokeinojen kohdatta esimerkiksi leimattaisiin julkisesti ovat vähäiset.
[321] Helminen ym. 2014, s. 1116–1118. Vielä komiteamietintövaiheessa yleisistä edellytyksistä puhuttiin erityisinä edellytyksinä. Ks. Sisäministeriö 2009a, s. 190 ja 447. Ks. myös Sisäministeriö 2009b, s. 148. Hallituksen esityksiin liittyen ks. HE 222/2010 vp, s. 172; HE 222/2010 vp, s. 315.
[322] HE 224/2010 vp, s. 39; HE 222/2010 vp, s. 122.

Yleinen *tuloksellisuusodotus* koskee kaikkia salaisia tiedonhankinta- ja pakkokeinoja.[323] Poliisilain toimivaltuuksissa kaikkien salaisten tiedonhankintakeinojen käytön yleisenä edellytyksenä on, että sillä voidaan olettaa saatavan rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi tarvittavia tietoja (PolL 5:2.1). Pakkokeinolaissa sääntely on muutoin samanlainen, mutta käytöllä tulee voida olettaa saatavan rikoksen selvittämiseksi tarvittavia tietoja (PKL 10:2.1).[324] Näillä keinoilla ei puututa tiedonhankinnan kohteen perus- ja ihmisoikeuksiin yhtä tuntuvasti, kuin erittäin tärkeä merkitys -edellytyksen osalta. Käytännössä tämä tarkoittaa sitä, että sääntely on jätetty kutakin toimivaltuutta koskevan erityisen edellytyksen varaan ja edellytys on lähinnä informatiivinen.[325] Pelkkä tuloksellisuusodotus koskee poliisi- ja peiteprofiileilla mahdollisista salaisista tiedonhankinta- ja pakkokeinoista vain peiteltyä tiedonhankintaa (PolL 5:15 ja PKL 10:14).[326]

Poliisilain 5 luvun 2 §:n 2 momentin mukaan sen lisäksi mitä 1 momentin tuloksellisuusodotuksessa todetaan, saadaan tiettyjä salaisia tiedonhankintakeinoja käyttää vain, jos niillä voidaan olettaa olevan *erittäin tärkeä merkitys* rikoksen estämiselle tai paljastamiselle. Pakkokeinolaissa sääntely on muutoin samanlainen, mutta kyse on rikoksen selvittämisestä (PKL 10:2.2). Kyseisillä menetelmillä voidaan puuttua perus- ja ihmisoikeuksiin siinä määrin, että niiden käytölle on katsottu olevan perusteltua asettaa kyseinen edellytys.[327] Poliisi- ja pakkokeinolain esitöissä viitataan telekuuntelua koskevaan hallituksen esitykseen 22/1994 vp, jossa määriteltiin tarkemmin erittäin tärkeä merkitys -edellytystä.[328] Edellytyksellä ei tarkoiteta sitä, että lupa salaiseen pakkokeinoon voitaisiin myöntää vain, jos rikos muuten jäisi selvittämättä. Toisaalta lupaa ei voi myöntää vielä sillä perusteella, että pakkokeino helpottaisi asian selvittämistä. Sama koskee tilannetta, jossa näyttö voitaisiin hankkia muilla keinoin. Erittäin tärkeä merkitys -edellytyksen täyttyminen vaatii, että ilman pakkokeinoa rikoksen selvittäminen aiheuttaisi kohtuuttomia kustannuksia tai muuten olisi hyvin työlästä, ja esimerkiksi tutkinnan pitkittymisestä aiheutuu erityistä vaaraa. Jos esitutkinnassa on kertynyt niin paljon näyttöä, että se riittää syytteen

[323] HE 224/2010 vp, s. 172.
[324] Näyttökynnyksen tason riittävyydestä on käyty keskustelua oikeuskirjallisuudessa. Ks. tästä tarkemmin Metsäranta 2015, s. 192–193.
[325] HE 224/2010 vp, s. 91; HE 222/2010 vp, s. 315. Ks. myös Metsäranta 2015, s. 194.
[326] Muita tähän luokkaan kuuluvia salaisia tiedonhankinta- ja pakkokeinoja ovat televalvonta, tukiasematietojen hankkiminen, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen ja muu kuin henkilöön kohdistuva tekninen seuranta,
[327] HE 224/2010 vp, s. 91; HE 222/2010 vp, s. 315.
[328] HE 224/2010 vp, s. 39; HE 222/2010 vp, s. 122.

nostamiseen, pakkokeinoa ei saa käyttää. Luvan myöntämisessä tuomioistuimen tulee ottaa lisäksi huomioon kokonaisharkinta suhteellisuusperiaate huomioiden.[329] Edellytys tulee täyttyä poliisi- ja peiteprofiileilla mahdollisten salaisten tiedonhankinta- ja pakkokeinojen kohdalla suunnitelmallisen tarkkailun (PolL 5:13 ja PKL 10:12) ja tietolähteen ohjatun käytön osalta (PolL 5:39 ja PKL 10:40).[330]

Lainsäätäjän on katsonut, että salaisten tiedonhankinta- ja pakkokeinojen joukossa on sellaisia keinoja, jotka on tarkoitettu viimesijaisiksi suhteessa muihin salaisiin keinoihin. Kyseinen viimesijaisuuden vaatimus on kuvattu *välttämättömyysvaatimuksen* avulla. Näiden keinojen tulee täyttää ensinnäkin PolL 5:2.2:n ja PKL 10:2.2:n erittäin tärkeä merkitys -edellytys, mutta niiden tulee myös olla välttämättömiä rikoksen estämiseksi, paljastamiseksi tai selvittämiseksi.[331] Välttämättömyysvaatimuksen osalta poliisi- ja pakkokeinolain esitöissä viitataan vanhaan pakkokeinolakiin ja niiden asuntokuuntelua koskevaan sääntelyyn.[332] Asuntokuuntelua koskevissa esitöissä välttämättömyyttä avattiin siten, että rikoksen selvittäminen ei olisi mahdollista tai olisi olennaisesti vaikeampaa käyttämällä epäillyn tai muiden henkilöiden perusoikeuksia vähemmän rajoittavia pakkokeinoja. Pakkokeinoa voitaisiin käyttää vain silloin, jos poliisi osoittaa että rikoksen selvittäminen perinteisillä keinoilla ja esitutkintamenetelmillä, kuten kotietsinnällä ja takavarikolla tai televalvonnan tai -kuuntelun avulla ei ole mahdollista, tai ainakin vaatisi oleellisesti enemmän voimavaroja taikka viivyttäisi rikoksen selvittämistä kohtuuttomasti.[333] Kyseinen edellytys koskee poliisi- ja peiteprofiileilla mahdollisista keinoista peitetoimintaa (PolL 5:28 PKL 10:27 ja valeostoa (PolL 5:35 PKL 10:34).[334]

---

[329] HE 22/1994 vp, s. 27. Kyseinen linjaus syytekynnyksen ylittymisestä liittyy esitöissä telekuunteluun ja pidän sitä osittain ongelmallisena. Jos poliisin esitutkinnassa keräämä näyttö ei riitä tuomioon ja salaisella tiedonhankinta- ja pakkokeinoilla voitaisiin saada tuomitsemiskynnykseen ylittävä näyttö, tulisi toimivaltuutta olla mahdollisuus käyttää. Riippumatta siitä, että kyse olisi erittäin tärkeä merkitys -edellytystä vaativasta toimivaltuudesta.

[330] Edellytys ei koske niin sanottua passiivista PolL 5:40.1:n ja PKL 10:39.1:n mukaista tietolähdetoimintaa. Ks. tarkemmin Helminen ym. 2014, s. 1117.

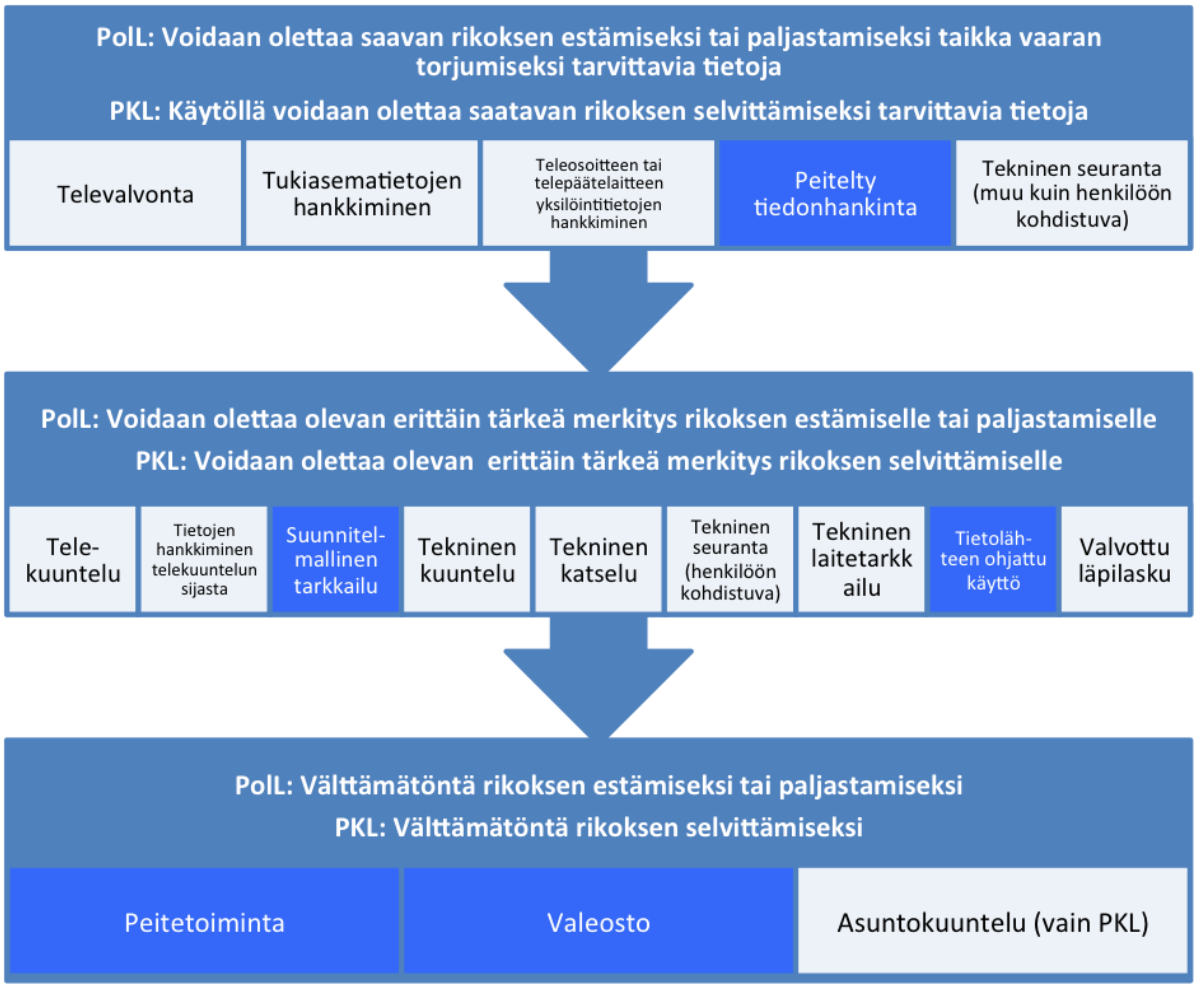
[331] HE 224/2010 vp, s. 91; HE 222/2010 vp, s. 315–316.

[332] HE 224/2010 vp, s. 39; HE 222/2010 vp, s. 122.

[333] HE 52/2002 vp, s. 70–71.

[334] Lisäksi vain pakkokeinolain mukainen asuntokuuntelu kuuluu tähän luokkaan. Poliisilain osalta asuntokuuntelu ei ole mahdollista muuta kuin ns. rynnäkkökatseluna. Ks. tästä tarkemmin HE 224/2010 vp, s. 109.

Salaisten tiedonhankinta- ja pakkokeinojen kolmiporrastusta voidaan kuvata toimivaltuuskohtaisesti seuraavalla taulukolla, jossa poliisi- ja peiteprofiileilla mahdolliset toimivaltuudet on tummennettu.[335]




Kuvio 4. salaisten tiedonhankinta- ja pakkokeinojen yleisten edellytysten kolmiportaisesta järjestelmästä.

*Metsäranta* on kritisoinut erittäin tärkeän merkitys -edellytyksen ja välttämättömyysvaatimuksen eron epäselvyyttä, jonka lisäksi hän kyseenalaistaa tuloksellisuusodotuksen pelkän informatiiviseen vaikutuksen. Metsärannan mukaan vähimmän haitan periaatteen ja suhteellisuusperiaatteen takia kaikkien salaisten tiedonhankintakeinojen käytön tulisi olla välttämätöntä.[336] Kokonaisharkintaa käytettäessä merkitystä tulee joka tapauksessa antaa suhteellisuusperiaatteelle, jonka perusteella

[335] Mukaan on otettu myös muut kuin poliisi- ja peiteprofiileilla mahdolliset salaiset tiedonhankinta- ja pakkokeinot, jotta porrastus ja erot perus- ja ihmisoikeuksien vaikutuksista olisi helpommin havaittavissa.
[336] Ks. tarkemmin Metsäranta 2015, s. 194–197.

toimivaltuutta ei pitäisi käyttää, vaikka erityiset edellytykset sinänsä täyttyisivätkin.[337] Käytännössä toimivaltuuksien käyttöön vaikuttavatkin ennemminkin toimivaltuuskohtaiset erityiset edellytykset. Yleisiä edellytyksiä voidaan pitää lisäksi osittain epäloogisesti järjestettynä suhteessa erityisiin edellytyksiin ja muihin oikeusturvatakeisiin. Tämä koskee erityisesti tietoverkkoja, joita lainsäätäjä ei ole huomioinut yleisiä edellytyksiä säätäessään, vaikka perus- ja ihmisoikeusnäkökulma on vaikuttanut tietoverkkojen osalta erityisiin edellytyksiin ja muihin oikeusturvatakeisiin.[338] Erityisesti tulisi ottaa huomioon aikaisemmin tutkimuksessa esitetyt erot yksityiselämän suojan tarpeessa. Yleiset edellytykset jäävätkin käytännössä melko abstraktille tasolle, eivätkä ne tunnu olevan loogisessa yhteydessä erityisten edellytysten kanssa. Yleisiä edellytyksiä tulisikin arvioida lainsäätäjän toimesta selvemmin loogisena kokonaisuutena erityisten edellytysten ja muiden oikeusturvatakeiden kanssa, jossa tietoverkkojen roolia tarkastellaan reaalimaailmasta irrallisena.

### 4.3 Erityiset edellytykset

Yleisten edellytysten vaatimusten lisäksi jokaisen salainen tiedonhankinta- ja pakkokeinon tulee täyttää tiettyjä erityisiä edellytyksiä, jotta toimivaltuutta voidaan käyttää.[339] Erityisten edellytysten vaatimuksiin vaikuttaa oleellisesti se, onko kyse rikoksen paljastamisesta, estämisestä vai selvittämisestä.[340] Rikosten paljastamisen osalta erityiset edellytykset ovat tiukimmat. Rikosten estämisessä on käytössä jo laajempi keinovalikoima ja jo tapahtuneiden rikosepäilyjen osalta laajin.[341]

Erityisiä edellytyksiä ei eritellä tai määritellä poliisi- ja pakkokeinolaissa yleisten edellytysten tapaan, vaan jokaiseen toimivaltuuteen on määritelty omat erityiset edellytykset. Poliisi- ja pakkokeinolakeja koskevien esitöiden mukaan lauseella ”mitä salaisten pakkokeinojen erityisistä edellytyksistä jäljempänä säädetään” tarkoitetaan sitä,

[337] HE 22/1994 vp, s. 27; HE 224/2010 vp, s. 39; HE 222/2010 vp, s. 121.
[338] Esimerkkinä tästä voidaan mainita peitetoiminta tietoverkossa, jossa erityiset edellytykset ovat lievemmät kuin reaalimaailman peitetoiminnassa, mutta yleiset edellytykset ovat samat. Voidaan mainita myös peitelty tiedonhankinta, jonka yleisenä edellytyksenä on pelkkä tuloksellisuusodotus, mutta käytännössä erityiset edellytykset rajaavat sen käytön käytännössä pois kokonaan, eikä poikkeuksia tietoverkkojen osalta tunneta.
[339] Yleiset ja erityiset edellytykset liittyvät myös muihin kuin salaisiin tiedonhankinta- ja pakkokeinoihin, kuten vangitsemisen yleisiin ja erityisiin edellytyksiin. Ks. yleisesti pakkokeinojen edellytyksistä Helminen – Kuusimäki – Rantaeskola 2012, s. 276–278.
[340] Tämä korostuu erityisesti siinä, millaisten rikosten osalta salaisia tiedonhankinta- ja pakkokeinoja voidaan käyttää.
[341] Ks. rikosten estämisen, paljastamisen ja selvittämisen eroista perus- ja ihmisoikeuksien näkökulmasta Metsäranta 2015, s. 60–61.

että kutakin pakkokeinoa koskevassa säännöksessä asetetaan sitä keinoa koskevia käytön edellytyksiä. Esimerkiksi se, että tutkittavana olevan rikoksen täytyy olla tiettyä vakavuustasoa, tai että paikkokeinoa saadaan käyttää vain tiettyyn tilaan taikka paikkaan kohdistuvana.[342] Tietoliikennetiedustelua koskevissa esitöissä on mainittu erityisinä edellytyksinä ennen kaikkea yksilöidyt rikokset, jonka lisäksi on mainittu kohdehenkilön roolin vaikutus toimivaltuuksien käyttöön.[343] Salaisia tiedonhankinta- ja pakkokeinoja koskeva erityisten edellytysten laajempi systematisointi oikeuskirjallisuudessa on ollut harvinaista. Oikeuskirjallisuudessa toimivaltuuden käyttöön vaikuttavat erityiset edellytykset on jaoteltu yleensä suppeasti rikosnimikkeen, rangaistusmaksimin ja edellisten yhdistelmän avulla.[344] Lisäksi tulee huomioida, että erityiset edellytykset tulee erottaa erilaisista oikeusturvatakeista, joita ovat esimerkiksi päätöksentekijätason määräytyminen, toimivaltuuden kestoon liittyvät kysymykset ja kohteelle ilmoittaminen.

Erityisten edellytysten sisältö voidaan kuvata yleisesti käytettyjä 1) rikosnimikettä ja 2) rangaistusmaksimia laajemmin, koska erityisinä edellytyksinä tulisi käsittää kaikki toimivaltuussäännöksessä esitetyt edellytykset. Edellä mainittujen lisäksi voidaan erottaa salaisia tiedonhankinta- ja pakkokeinoja koskevista toimivaltuussäännöksistä seuraavia edellytyksiä: 3) kohdehenkilön asema, 4) kohteen laatu ja sijainti, 5) suostumus 6) henkeä ja terveyttä välittömästi uhkaava vaara ja 7) erityisten edellytysten säännöskohtaiset rajoitukset.[345] Poliisi- ja peiteprofiileilla koskevaa tiedonhankintaa näistä koskee vain osa.

Rikosten paljastamiseksi erityiset edellytykset on säädetty tiukoiksi *rikosnimikkeiden* ja *rangaistusmaksimin* osalta. Salaista tiedonhankintaa saa käyttää vain rikoslain 11–13 luvun sota-, maanpetos- ja valtiopetosrikoksissa, jonka lisäksi myös rikoslain 34 a luvun terrorismirikokset ovat luettu erityisiin edellytyksiin. On kuitenkin huomioitava, että tällöin käytössä on poliisilain 5 luvun 3 §:n mukaisesti kaikki poliisilain 5 luvussa säädetyt salaiset tiedonhankinta keinot. Rikoksen estämiseksi salaisia tiedonhankintamenetelmiä on käytössä selkeästi enemmän, mutta kuitenkin suppeammin kuin pakkokeinolain puolella. Yleisvalvonnan ja tarkkailun tapaan, myöskään tietolähteen ohjatun käytön osalta ei ole säädetty rikoksen rangaistusasteikkoon tai rikosnimikkeisiin liittyviä erityisiä edellytyksiä.

[342] HE 224/2010 vp, s. 90–91; HE 222/2010 vp, s. 315.
[343] HE 202/2017 vp, s. 72.
[344] Ks. esimerkiksi Helminen ym. 2014, s. 751–754. Ks. myös Metsäranta 2015, s. 202 ja 231. Määrittelyä sekoittaa osaksi se, että yleisiä edellytyksiä kutsuttiin vielä komitean mietintövaiheessa erityisiksi edellytyksiksi. Ks. Sisäministeriö 2009a, s. 190 ja 447.
[345] Oikeuskirjallisuudessa kyllä käsitellään myös näitä seikkoja säännöskohtaisissa edellytyksissä, mutta yleensä niihin ei viitata nimenomaan erityisinä edellytyksinä.

Poliisilain osalta on mainittu 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottaminen (PolL 5:40.1), joten käytännössä kyse voi olla mistä vain poliisin tehtäväpiiriin kuuluvasta asiasta.[346] Pakkokeinolain puolella puhutaan rikoksen selvittämiselle merkityksellisten tietojen vastaanottamisesta (PKL 10:39.1), joten edellytyksenä on vain se, että kyse on rikoksesta. Suunnitelmallisen tarkkailun osalta poliisi- ja pakkokeinolaissa on edellytyksenä kahden vuoden rangaistusmaksimi, varkaus tai kätkemisrikos (PolL 5:13.3 ja PKL 10:12.3). Kynnykseen vaikuttaa se, että koska keinolla puututaan henkilön yksityiselämän suojaan hänen elämäänsä seuraamalla, suhteellisuusperiaate edellyttää että suunnitelmallista tarkkailua ei saa käyttää vähäisten rikosten paljastamisessa, estämisessä tai selvittämisessä.[347] Myös valeostolle on asetettu kahden vuoden rangaistusmaksimiraja (PolL 5:35.2 ja PKL 10:34.2). Peitellyn tiedonhankinnan osalta erityisenä edellytyksenä on poliisi- ja pakkokeinolain osalta neljän vuoden rangaistusmaksimi, mutta lisäksi säännöksissä on luetteloitu myös muita mahdollisia rikoksia. Pakkokeinolakiin on otettu mukaan panttivangin ottamisen ja törkeän ryöstön valmistelu mukaan poliisilain edellytyksistä poiketen (PolL 5:15.2 ja PKL 10:14.2).[348] Peitetoiminnan erityisten edellytysten osalta viitataan pakkokeinolain 10 luvun 3 §:ssä tarkoitettuihin telekuuntelun edellytyksiin. Molempien lakien osalta säännös kuitenkin rajaa pois törkeän laittoman maahantulon järjestämisen.[349] Toisaalta lisäedellytyksenä mainitaan rikoslain 17 luvun 18 §:n 1 momentin 1 kohdan mukainen sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittäminen, jota ei löydy telekuuntelun edellytyksistä.

Tietoverkkojen osuus rikosnimikettä ja rangaistusmaksimia koskevissa erityisissä edellytyksissä on otettu huomioon vain peitetoiminnan osalta. Tietoverkoissa peitetoiminnan raja on säädetty kahteen vuoteen, jonka lisäksi edellytyksenä mainitaan rikoslain 17 luvun 19 §:n mukainen sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapito (PolL 5:28.3 ja PKL 10:27.3). Syyksi tähän on mainittu esitöissä tietoverkkojen 1) anonyymi luonne, 2) dokumentoinnin helppous ja tarkkuus sekä 3) vähäisemmät turvallisuusriskit.[350] Kun katsoo kyseisiä perusteita, soveltuvat ne muihinkin salaisiin tiedonhankinta- ja

[346] HE 224/2010 vp, s. 124. Esimerkkinä mainitaan lupahallintoon kuuluvat asiat, jossa tietolähteeltä saadaan aseharrastajan terveydentilaa koskeva tieto, joka voisi johtaa viranomaisen taholta esimerkiksi lääkärintodistuksen pyytämiseen ja edelleen ampuma-aseluvan peruuttamiseen.
[347] HE 224/2010 vp s. 42 ja 103; HE 222/2010 vp, s. 126 ja 326.
[348] Lisäksi pakkokeinolain puolelta löytyy Tullia koskevaa sääntelyä (PKL 10:14.3).
[349] Tullin osalta rajataan pois myös törkeä tulliselvitysrikos.
[350] HE 224/2010 vp, s.116; HE 222/2010 vp, s. 339. Jo komiteamietintövaiheessa ihmisten vuorovaikutukseen tietoverkoissa kuvattiin olevan luonteenomaista tietynlainen epäluottamus ja lähtökohtana pidettiin sitä, ettei henkilöt esiinny tietoverkoissa omalla identiteetillään, vaan käytetään esimerkiksi nimimerkkejä tai muita vastaavia tunnisteita. Ks. Sisäministeriö 2009a, s. 204.

pakkokeinoihin ainakin osittain. Herääkin kysymys, miksei suunnitelmallisen tarkkailun, peitellyn tiedonhankinnan ja valeoston erityisissä edellytyksissä ole otettu kyseistä seikkaa huomioon? Etenkin kun kahden viimeisen toimivaltuuden osalta kyse on vuorovaikutukseen perustuvasta toiminnasta peitetoiminnan tapaan. Toisaalta valeoston raja on muutoinkin jo suhteellisen alhainen, mutta erityisesti peitellyn tiedonhankinnan lähtökohtainen neljän vuoden maksimirangaistuksen raja tietoverkoissa ei ole perusteltu suhteessa peitetoimintaan.[351] Etenkin kun peiteltyä tiedonhankintaa pidetään peitetoiminnasta poiketen yksittäisenä ja lyhytaikaisena toimenpiteenä, joka ei puutu henkilön yksityiselämän suojaan niin syvällisesti kuin peitetoiminta.[352] Voidaan lisäksi kysyä, miksei RL 17:19:ää ole lisätty muihin tietoverkoissa mahdollisten toimivaltuuksien edellytyksiin?[353]

*Henkilön aseman* vaikutuksen lähtökohtana on, että salaisia tiedonhankinta- ja pakkokeinoja kohdistetaan yleensä henkilöön, jonka voidaan perustellusti olettaa syyllistyvän rikokseen tai hän on rikoksesta epäiltynä. Osaa keinoista on kuitenkin mahdollista käyttää myös muissa asemissa oleviin henkilöihin.[354] Tietolähteen ohjatun käytön kohdalla kyseessä on monesti rikollisten kanssa tekemisissä olevat henkilöt, jotka ovat itsekin saattaneet syyllistyä erilaisiin rikoksiin. Tietolähde voi teoriassa olla kuka vain, mutta poliisi- ja pakkokeinolain mukaan hänen tulee olla tähän tehtävään henkilökohtaisilta ominaisuuksiltaan sopiva (PolL 5:40.2 ja PKL 10:39.2). Sopivuudella tarkoitetaan tietolähteen motiiveja toimia tehtävässä, koska tarkoituksena ei tule olla esimerkiksi taloudellisen hyödyn tai muun edun tavoittelu taikka kosto.[355] Myöskään pelkän tarkkailun osalta ei ole määritelty henkilön asemaa, joten se voi kohdistua lyhytaikaisesti kehenkä vain.[356] Poliisi- ja peiteprofiileilla mahdollisten salaisten tiedonhankinta- ja pakkokeinojen osalta rikokseen oletettavasti syyllistyvän tai rikoksesta epäillyn edellytys koskee suunnitelmallista tarkkailua (PolL 5:13.3 ja PKL 10:12.3) ja peitetoimintaa (PolL 5:28.2 ja PKL 10:27.2). Suunnitelmallisen tarkkailun osalta

[351] Toisaalta peitellyn tiedon hankinnan yleisenä edellytyksenä on vain tuloksellisuusodotus, joten se kompensoi osaltaan tilannetta. Niin kuin yleisiä edellytyksiä koskevassa kohdassa on todettu, on erityisillä edellytyksillä käytännössä selvästi konkreettisempi vaikutus toimivaltuuksien käyttöön.
[352] Ks. tarkemmin HE 224/2010 vp, s. 177–178; HE 222/2010 vp, s. 386.
[353] Tätä perustelen esimerkiksi sillä, että kyseistä materiaalia hallussa pitäviä olisi mahdollisuus seurata pidempään tai vaihtoehtoisesti kohdistaa epäiltyyn materiaalin hallussapitäjään peiteltyä tiedonhankintaa yksittäisenä toimenpiteenä yrittäen tiedustella esimerkiksi sitä, olisiko hänellä mahdollisesti vaihtaa materiaalia, joka on yleistä kyseiseen rikollisuuden muotoon liittyen. Ks. pedofiilirinkien materiaalinvaihdosta Europol 2018, s. 33
[354] HE 224/2010 vp, s. 34. Toimivaltuudet myös eroavat yleisvalvonnasta, joka ei kohdistu kehenkään tiettyyn henkilöön, vaan esimerkiksi pelkkään rakennukseen, tilaan, paikkaan, keskustelupalstaan tai muuhun vastaavaan kohteeseen.
[355] Ks. HE 224/2010 vp, s. 125; HE 222/2010 vp, s. 347–348.
[356] Lisähuomiona henkilön asemasta voidaan mainita vapautensa menettänyt, jonka osalta löytyy sääntelyä teknisen kuuntelun (PolL 5:17.3 ja PKL 10:16.2) ja katselun (PolL 5:19.3 ja PKL 10:19.3) osalta.

pakkokeinolain esitöissä on täsmennetty, että muihin kuin rikoksesta epäiltyihin kohdistuva tarkkailu on mahdollista vain lyhytkestoisena ja yksitäisenä toimenpiteenä lähinnä oikean tarkkailukohteen varmistamiseksi, jolloin käytännössä joudutaan kohdistamaan havaintojen tekemistä myös muihin ihmisiin.[357] Käytännössä on kuitenkin harvinaista, että olisi tarpeellista tai järkevää seurata esimerkiksi asianomistajan, todistajan tai muun asemassa olevia henkilöitä. Toisaalta niin kuin toimivaltuuksia käsitellessä tuodaan myöhemmin ilmi, tarkkailun kriteerit täyttyvät tietoverkoissa käytännössä heti kun yksittäistä profiilia tarkastellaan tarkemmin. Tämän takia tietoverkkojen puolella muissa asemissa olevien henkilöiden tarkkailu on yleisempää kuin reaalimaailmassa. Peitellyssä tiedonhankinnassa henkilön asemaa ei ole rajattu, koska sen tulee vain kohdistua tiettyyn henkilöön (PolL 5:15.1 ja PKL 10:14.1). Esimerkkinä voidaan mainita tilanne, jossa rikollisryhmä tilaa taksin, jota tosiasiallisesti kuljettaa poliisimies ja rikolliseen tekoon oletetusti syyllistyvä tai rikoksesta epäilty on ryhmän mukana.[358] Myöskään valeostoa ei ole rajoitettu vain rikoksesta epäiltyyn tai rikokseen perustellusti syyllistyväksi oletettuun, vaan osapuolena voi olla myös muu tietty henkilö.[359] Valeoston kohteena oleva henkilö tulee pystyä joka tapauksessa yksilöimään (PolL 5:36.3,2 ja PKL 10:35.3,2).

Tietoverkoissa tapahtuvan toiminnan kohdalla henkilön asemaan ei ole kiinnitetty lainvalmistelussa erityistä huomiota, eikä asian suhteen ole sinänsä havaittavissa ongelmia. Haasteita tosin tuottaa reaalimaailmaa enemmän se, että henkilön yksilöiminen ja tunnistaminen on haastavampaa tietoverkoissa, niin kuin tutkimuksessa on tuotu ilmi. Voidaan myös todeta tietoverkkoihin liittyen, että tietoliikennetiedustelua koskevassa lakimuutoksessa käyttöalaa laajennettiin siten, että salaisen tiedonhankintakeinon kohdetta ei tarvitse enää pystyä yksilöimään. Tätä perusteltiin sillä, että tiedustelutoiminnan olennaisena tarkoituksena on nimenomaan löytää henkilöitä. Tämän takia tiedustelutoimivaltuuksien kohdalla katsottiin tarpeelliseksi irtaantua perinteisestä toimivaltuuksien rikos- ja henkilöperustaisuudesta.[360] Toisaalta aikaisemminkaan yksilöinti ei ole tarkoittanut sitä, että kohteen henkilöllisyys olisi tullut olla tiedossa, koska esimerkiksi

[357] HE 222/2010 vp, s. 325–326. Esimerkkinä mainitaan tilanne, jossa tiedetään tietyn henkilön toimittavan pakoilua varten varoja esitutkintaa karttavalle rikoksesta epäillylle. Tällaista henkilöä voidaan tarkkailun puitteissa seurata piilopaikkaan epäillyn tavoittamiseksi esitutkintaan.
[358] Toimivaltuuden piiriin kuuluu myös esimerkiksi tietyn kohdehenkilölle tarkoitetun lähetyksen toimittaminen perille lähettinä esiintyen, jolloin on mahdollista, että lähetyksen ottaa vastaan joku muu kuin rikokseen oletettavasti syyllistyvä tai rikoksesta epäilty. Sama tilanne voi tulla eteen myös silloin, jos poliisimies on esimerkiksi tarjoilijaksi tekeytyneenä ravintolassa ja harjoittaa tiedonhankintaa kohteen läheisyydessä. Ks. HE 224/2010 vp, s. 103–104; HE 222/2010 vp, s. 327.
[359] Esimerkkinä voidaan mainita henkilö, joka myy anastettua polkupyörää, jonka hän on kuitenkin voinut laillisesti vilpittömässä mielessä ostaa aikaisemmin itselleen.
[360] HE 202/2017 vp, s. 73–74.

pelkkä IP-osoite tai IMEI-koodi on ollut riittävä yksilöintitieto. Koska samaa IP-osoitetta on voinut käyttää useampi henkilö, ei yksilöinti ole välttämättä ollut tiettyyn henkilöön kohdistuvaa. Sama koskee myös sosiaaliseen mediaan luotua valeprofiilia, jolla voi olla useita eri käyttäjiä. Kyseinen taso on kuitenkin ollut riittävä yksilöimään salaisen tiedonhankinta- ja pakkokeinon kohteen.[361]

Kohteen *laadulla ja sijainnilla* tarkoitan sitä, kohdistuuko toimivaltuus henkilöön, viestiin, tunnistamistietoon, tilaan, paikkaan, esineeseen, aineeseen, omaisuuteen tai laitteeseen. Lisäksi määrittelyllä viitataan siihen, missä paikassa kohdehenkilö on sillä hetkellä, kun häneen kohdistetaan poliisin tiedonhankintaa. Näillä kaikilla voi olla vaikutusta erilaisten salaisten tiedonhankinta- ja pakkokeinojen erityisille edellytyksille, mutta vain osa koskee poliisi- ja peiteprofiileilla mahdollisia toimivaltuuksia. Poliisi- ja peiteprofiileilla mahdolliset toimivaltuudet kohdistuvat tietoverkoissa kaikki tiettyyn henkilöön, eikä hänen sijainnillaan ole merkitystä keinon käytölle. Viestin ja tunnistamistiedon osalta erot vaikuttava vain teletoimivaltuuksissa. *Suostumuksella* on merkitystä salaisten pakkokeinojen osalta televalvonnan eri muodoissa, joten myöskään se ei koske poliisi- ja peiteprofiileja.[362] *Henkeä ja terveyttä uhkaavaa vakavaa vaaraa* koskeva erityinen edellytys koskee poliisilainmukaisia toimia, joissa voi olla kyse telekuuntelusta (PolL 5:5.3), televalvonnasta (PolL 5:8.3–4), tukiasematietojen hankkimisesta (PolL 5:11.3) tai teknisen tarkkailun ”rynnäkköluontoisista” toimenpiteistä (PolL 5:17.5, 5:19.5, 5:21.4). Siten myöskään nämä erityiset edellytykset eivät koske poliisi- ja peiteprofiileilla mahdollisia toimivaltuuksia.

Salaisten tiedonhankinta- ja pakkokeinojen erityisiin edellytyksiin on sisällytetty erilaisia *säännöskohtaisia lisärajoituksia*. Erityisiä edellytyksiä koskevilla lisärajoituksilla suojataan erityisesti kotirauhaa ja sen ydinaluetta, asuttua asuntoa. Vaikka poliisi- ja peiteprofiileilla mahdollisista salaisista tiedonhankinta- ja pakkokeinoista löytyy näitä rajoituksia, ei niillä kuitenkaan ole juuri merkitystä tietoverkoissa tapahtuvan toiminnan osalta.[363] Tietoverkoissa

[361] Ks. esimerkiksi telekuunteluun liittyen HE 224/2010 vp, s. 94; HE 222/2010 vp, s. 318. Telekuuntelun kohde voidaan yksilöidä teleosoitteen tai telepäätelaitteen perusteella, eikä poliisilla välttämättä tarvitse olla tietoa kohteen henkilöllisyydestä.

[362] Ks. suostumusperusteisen televalvonnan erityisistä edellytyksistä tarkemmin Metsäranta 2015, s. 211–214 ja 233. Ks. suostumuksen vaikutuksesta yleisesti erilaisiin pakkokeinoihin Helminen – Kuusimäki – Rantaeskola 2012, s. 181–182.

[363] Poliisi- ja peiteprofiileilla mahdollista suunnitelmallista tarkkailua ei saa kohdistaa vakituiseen asumiseen käytettävään tilaan, eikä teknisellä laitteella tapahtuvaa toimintaa saa kohdistaa RL 24:11:ssä tarkoitettuun kotirauhan suojaamaan paikkaan. Sama koskee myös pelkkää tarkkailua (PolL 5:13.4 ja PKL 10:12.4). Peitellyn tiedonhankinta on mahdollista kotirauhan suojaamalla alueella, mutta asunnossa ei edes asunnonhaltijan myötävaikutuksella (PolL 5:15.3 ja PKL 10:14.4). Peitetoiminnan osalta toimivaltuus on mahdollistettu myös asunnossa, mutta sisäänkäynnin ja oleskelun tulee tapahtua asuntoa käyttävän aktiivisella

ei ole määritelty samanlaista ”tietoverkkojen kotirauhaan” kuuluvaan aluetta, jossa esimerkiksi suunnitelmallinen tarkkailu ei olisi mahdollista. Käytännössä erilaisen luottamuksellisen viestinnän ja ryhmäominaisuuksien takia asiaa olisi kuitenkin voitu arvioida lainvalmistelussa laajemmin erityisesti suppeiden suljettujen ryhmien osalta.[364] Eli vaatisiko esimerkiksi suppean suljetun ryhmän suunnitelmallinen tarkkailu jotain rajoituksia, joissa suunnitelmallista tarkkailua ei enää saisi toteuttaa. tai kyse olisi vaihtoehtoisesti jo peitetoiminnasta.[365] Valeostoa koskevan toimivaltuuden rajoitukseksi voidaan tulkita PolL 5:35.3:stä ja PKL 10:34.3:stä koskevat säännökset tiedonhankinnan rajaamisesta vain valeostolle välttämättömään ja lähtökohtaisesti vain näyte-erän mahdollistavan valeoston. Myös tietolähteen ohjatussa käytössä on rajoituksia, vaikka erityisten edellytysten osalta vaatimukset ovat muutoin kevyet. Tietolähteen ohjatussa käytössä tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä tai joka vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden (PolL 5:40.3 ja PKL 10:39.3).[366]

### 4.4 Muut oikeusturvatakeet

Yleisten ja erityisten edellytysten lisäksi salaisten tiedonhankinta- ja pakkokeinojen käyttöön liittyy muitakin toimivaltuuksien käyttömahdollisuuksiin liittyviä kysymyksiä. Yksi olennaisimmista yksittäisen toimivaltuuden käyttöön vaikuttavana seikkana on päätöksentekijätasoa koskeva säännös. Kyseinen säännös on yleensä sijoitettu toimivaltuuden edellytyksiä seuraavaan pykälään. Lisäksi toimenpidekohtaisista edellytyksistä on erotettu niin sanotut yhteiset säännökset, jotka vaikuttavat toimivaltuuksien käyttöön.[367] Käsittelen näistä tarkemmin tässä kohtaa vain päätöksentekijätasoa.

---

myötävaikutuksella (PolL 5:28.4 ja PKL 10:27.4). Sama rajoitussääntely koskee myös valeostoa (PolL 5:35.4) ja PKL 10:34.4).

[364] Tällä viittaa luottamuksellista viestintää käsiteltäessä esille tuotuihin viestinnän luottamuksellisuuden eroihin erilaisissa ryhmissä ja sen vaikutuksesta suojan tarpeeseen.

[365] Toisaalta ryhmän suppeuden takia voi kyseeseen tulla myös peitelty tiedonhankinta tai peitetoiminta.

[366] Lisäksi säännöksistä löytyy rajoituksilta vaikuttavia edellytyksiä, mutta käytännössä niillä on toimivaltuutta laajentava luonne. Peitetoimintaa on rajattu rikoksentekokieltosäännöksellä, jonka mukaan peitetoimintaa suorittava poliisimies ei saa syyllistyä kuin vähäisiin rikkomuksiin (PolL 5:29 ja PKL 10:28). Käytännössä kyseessä ei kuitenkaan ole rajoitussäännös, vaan ennemminkin vähäiset rikkomukset peitepoliisille salliva toimivaltuussäännös. Lisäksi poliisimiehelle on PolL 5:30:ä ja PKL 10:29 koskevalla sääntelyllä annettu oikeus osallistua järjestäytyneen rikollisryhmän toimintaan ja valvottuun läpilaskuun.

[367] Metsäranta kutsuu näitä salaisia tiedonhankinta- ja pakkokeinoja koskeviksi minimointi- ja kontrollimekanismeiksi. Ks. Metsäranta 2015, s. 237 ja 288. Yhteisiä säännöksiä ovat esimerkiksi menettely tuomioistuimessa (PolL 5:45 ja PKL 10:43), kuuntelu- ja katselukiellot (PolL 5:50 ja PKL 10:52), salaisen tiedonhankintakeinon käytöstä ilmoittaminen (PolL 5:58 ja PKL 10:60) ja salaisen tiedonhankinnan valvonta (PolL 5:63 ja PKL 10:65). Kaikki yhteiset säännökset eivät tosin koske kaikkia toimivaltuuksia, josta

Perus- ja ihmisoikeuksilla on suora vaikutus salaisten tiedonhankinta- ja pakkokeinojen päätöksentekijätasoon, koska mitä tuntuvampi puuttuminen kyseisiin oikeuksiin on, sitä korkeammalle taholle päätöksentekovalta on annettu.[368] Päätöksentekijätasot voidaan jakaa viiteen eri tasoon: 1) tuomioistuintaso, 2) päällikkötaso, 3) salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu virkamies (STEKPOV), 4) pidättämiseen oikeutettu virkamies (POV) ja 5) poliisimies.[369] Tuomioistuimilla tarkoitetaan jokaista tuomiovaltaista yleistä tuomioistuinta. Päällikkötasolla tarkoitan keskusrikospoliisin, suojelupoliisin ja poliisilaitoksen päälliköitä.[370] STEKPOV:lla taas tarkoitetaan POV:a, joka on suorittanut erillisen koulutuksen salaisten tiedonhankinta- ja pakkokeinojen osalta.[371] Siten jokainen STEKPOV on myös POV, joka määritellään erikseen PKL 2:9:ssä.[372] Poliisimiehiä on valtioneuvoston asetuksella tarkemmin säädettävät päällystöön, alipäällystöön ja miehistöön kuuluvat virkamiehet (PolL 1:12).

*Tuomioistuimen* päätettäväksi on annettu merkittävimmin perus- ja ihmisoikeuksiin puuttuvien salaisten tiedonhankinta- ja pakkokeinojen käyttäminen.[373] Se ei tee sitä koskaan omatoimisesti, vaan yleensä POV:n aloitteesta.[374] Tuomioistuin tekee päätöksen poliisi- ja peiteprofiilien osalta päätöksen vain peitetoiminnan edellytyksistä (PolL 5:33 ja PKL 10:32).[375] *Päällikkötason* osalta päätöksenteko koskee lähinnä erityisiä toimivaltuuksia. Lisäksi päällikkötasolle on annettu toimivaltaa salaisen tiedonhankinta- ja pakkokeinon suojaamisesta päättämiseen liittyen (PolL 5:47.1 ja PKL 10:48.1), joka ei kuitenkaan ole

esimerkkinä voidaan mainita ylimääräisen tiedon käyttö, joka ei koske yhtäkään poliisi- ja peiteprofiililla mahdollista toimivaltuutta (PolL 5:53 ja PKL 10:55).

[368] HE 224/2010 vp, s. 51–53; HE 222/2010 vp, s. 136–137. Kyseiseen jaotteluun vaikuttaa myös kiire-elementti. Lisäksi vaikutusta on pakkokeinojen keskinäistä suhteiden hahmottamisella ja oikeusturvaseikoilla, niin kuin jälkeen päin käy ilmi.

[369] Suojelupoliisin tiedusteluorganisaatioksi muuttumisen jälkeen oma heidän osalta POV:a vastaa suojelupoliisin päällystöön kuuluva poliisimies.

[370] Päällikkötason toimivaltaa on tosin kavennettu siten, että paikallispoliisin päällikölle on annettu toimivalta päätöksen tekemiseen vain osittain.

[371] Ks. Poliisihallitus 2018a, s. 3. Ks. myös HE 202/2017 vp, s. 184. Tietoliikennetiedusteluun liittävän lakimuutoksen myötä sääntelyyn tullaan lisäämään suojelupoliisin päällystöön kuuluva poliisimies, jolla on lähtökohtaisesti samat oikeudet kuin STEKPOV:lla.

[372] Kyseisen säännöksen mukaan POV:n oikeudet on myös poliisiylijohtajalla, poliisipäälliköllä ja kaikilla tästä komisarioon asti alempiarvoisilla.

[373] HE 224/2010 vp, s. 51–53; HE 220/2010 vp, s. 136–137.

[374] Salaisen tiedonhankinta- ja pakkokeinon käyttö tulee lopettaa ennen määräaikaa, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole (PolL 5:2.3 ja PKL 10:2.3). Yleensä päätöksentekijä vastaa tästä, mutta tuomioistuimen ratkaisua koskevissa tapauksissa vastuussa on yleensä pakkokeinoa tuomioistuimessa hakenut POV.

[375] Poliisilain osalta edellytykset tulee tutkia vain siinä tapauksessa, että peitetoiminnalla saatua tietoa on tarkoitus käyttää oikeudenkäynnissä syyllisyyttä tukevana selvityksenä. Peitetoiminnan edellytykset käsitellään keskitetysti Helsingin käräjäoikeudessa (PolL 5:45.1 ja PKL 10:43).

toimivaltuus.[376] Päällikkötaso voi päättää poliisi- ja peiteprofiileilla mahdollisista salaisista tiedonhankinta- ja pakkokeinoista peitellystä tiedonhankinnasta (PolL 5:16.1 ja PKL 10:15.1), peitetoiminnasta (PolL 5:32.1 ja PKL 10:31.1), valeostosta (PolL 5:36.1 ja PKL 10:35.1) ja tietolähteen ohjatusta käytöstä (PolL 5:42 ja PKL 10:40.1). Peitetoimintaan liittyen päällikkötason päätöksentekoa on kavennettu siten, että poliisilaitoksen päällikkö saa tehdä päätöksen vain tietoverkoissa tapahtuvasta peitetoiminnasta.[377] Jos peitetoiminta edellyttää myös soluttautumista reaalimaailmassa, ei poliisilaitoksen päällikön tekemää päätöksentekomenettelyä voi käyttää.[378] Valeoston osalta sääntely on samansuuntainen, koska jos kyseessä on yksinomaan yleisön saataville toimitettu myyntitarjous, päätöksen voi tehdä päällikkötason lisäksi STEKPOV. Muutoin päätösvalta on kohdennettu vain keskusrikospoliisin ja suojelupoliisin päällikölle (PolL 5:36.1 ja PKL 10:35.1).[379]

Päällikkötason osalta voidaan todeta, että päällikkö ei ole välttämättä käynyt STEKPOV-koulutusta, joten heidän liittäminen osaksi päätöksentekijätasoa vaikuttaa osin tarpeettomalta. Vaikka tarkoituksena on ollut perus- ja ihmisoikeusnäkökulman korostaminen, ei ratkaisua voida pitää kovin onnistuneena, koska joka tapauksessa PolL 5:63:n ja PKL 10:65:n perusteella päälliköillä on toimivaltuuksista valvontavastuu, eikä päällikkö käytännössä osallistu operatiiviseen päätöksentekoon muuta kuin allekirjoittamalla päätöksen.[380] Perus- ja ihmisoikeuksien kannalta toimivampi vaihtoehto olisi määritellä tarkemmin STEKPOV-tason koulutusvaatimukset erityisesti tietoverkkojen osalta ja jättää koko päällikkötaso pois päätöksentekoportaikosta.[381]

---

[376] HE 266/2004 vp, s. 31.

[377] Varsinaisessa hallituksen esityksessä myös reaalimaailman peitetoiminnasta päättämistä esitettiin mahdolliseksi muillekin kuin keskusrikospoliisin ja suojelupoliisin päälliköille, mutta perustuslakivaliokunta esitti hallintovaliokunnalle peitetoiminnan päätösvallan siirtämistä tuomioistuimille. Lisäksi perustuslakivaliokunta katsoi ongelmalliseksi, ettei toimivaltaa oltu määritelty lain tasoisesti, vaan viitattu pelkästään valtioneuvoston asetuksella säädetyn poliisiyksikön päällikköön. Tämän takia päätösvalta jäi pelkästään keskusrikospoliisin ja suojelupoliisin päälliköille. Ks. aiheesta tarkemmin PeVL 67/2010 vp, s. 5 ja PeVL 66/2010 vp, s. 9 sekä HaVM 42/2010 vp, s. 6 ja HaVM 50/2010 vp, s. 9.

[378] HE 224/2010 vp, s. 119; HE 222/2010 vp, s. 342.

[379] Jostain syystä poliisilaitoksen päällikkötaso on jätetty kokonaan pois päätöksentekijöistä, joten jos päällikkö ei ole STEKPOV, ei hän voi myöskään tehdä päätöstä kyseisestä yleisön saataville toimitettuun myyntitarjoukseen kohdistuvasta valeostosta.

[380] Vaikuttaakin siltä, että lainsäätäjä ei ole miettinyt päällikkötason osalta osaamista, vaan mieluumminkin näennäistä päätöksentekotason korostamista.

[381] Sama koulutusvaatimus tulisi koskea myös tuomioistuimessa asioita ratkaisevia tuomareita. Ks. esimerkiksi Haapamäki 2010, s. 196, jonka mukaan poliisi oli tuonut esille huolensa tuomioistuimen osaamiseen. Matkapuhelimiin kohdistuvan telekuuntelun osalta tilanne oli hyvä, mutta jos asia liittyi tietoverkkoihin, asetti se erityisvaatimuksia tuomarin asiantuntemukselle. Haapamäki totesi saman haasteen koskevan myös laillisuusvalvontaa.

*STEKPOV* voi tehdä päätöksen poliisi- ja peiteprofiilitoimintaan liittyen peitellystä tiedonhankinnasta (PolL 5:16.1 ja PKL 10:15.1), yksinomaan tietoverkossa toteutettavasta peitetoiminnasta (PolL 5:32.1 ja PKL 10:31.1), yksinomaan yleisön saataville toimitettua myyntitarjousta koskevasta valeostosta (PolL 5:36.1 ja PKL 10:35.1) ja tietolähteen ohjatusta käytöstä (PolL 5:42 ja PKL 10:40.1).[382] Esitöissä ohjatun tietolähdetoiminnan todetaan vastaavan riskeiltään suunnilleen valeostoa, joten myös päätöksentekijätaso on sama ja STEKPOV:n tekemä päätös mahdollinen.[383] Riskien sisältöä ei avata tarkemmin. Vertaus on siinä mielessä mielenkiintoinen, että tietolähdetoiminnassa kyse on kouluttamattomasta siviilistä, joka mahdollisesti omaa rikollisen taustan. Valeostossa kyse on nimenomaan vale- ja peitetoimintaan koulutetusta poliisimiehestä, joten riskitason voisi katsoa olevan lähtökohtaisesti alhaisempi. *POV:n* päätettävissä oleva ainoa poliisi- ja peiteprofiililla mahdollinen keino on suunnitelmallinen tarkkailu (PolL 5:14.1 ja PKL 10:13.1).[384] *Poliisimiehellä* ei ole itsenäistä päätäntävaltaa minkään salaisen tiedonhankinta- tai pakkokeinon osalta. Siten poliisi- ja peiteprofiileilla mahdollisten keinojen osalta poliisimiehen päätettäväksi jää yleisvalvonta ja tarkkailu, joita ei kuitenkaan pidetä salaisina tiedonhankinta- tai pakkokeinoina.[385] Poliisimies voi lisäksi tehdä salaisiin tiedonhankinta- ja pakkokeinoihin liittyen väliaikaisen päätöksen peitetoiminnan laajentamisesta (PolL 5:34 ja PKL 10:33). Esimerkkinä voidaan mainita tilanne, jossa törkeän lapsen seksuaalisen hyväksikäytön epäilyn osalta on syytä epäillä kohdetta tai muuta henkilöä myös törkeää sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittämisestä.[386]

Selkeimmin tietoverkkojen erilainen rooli reaalimaailmaan ja tietoverkkojen välillä on päätöksentekovallassa huomioitu peitetoimintaa ja valeostoa koskevassa sääntelyssä.[387] Lainsäätäjä on katsonut, että POV:n päätettävissä oleviin keinoihin ei lähtökohtaisesti sisälly

[382] Lisäksi STEKPOV voi tehdä päätöksen valvotusta läpilaskusta.
[383] HE 224/2010 vp, s. 123 ja 126; HE 222/2010 vp, s. 346 ja 349.
[384] POV:n päätettäväksi on annettu poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa ja valeostossa, vaikka varsinaista päätösvaltaa näiden suorittamiseen sillä ei ole (PolL 5:39 ja PKL 10:38). Turvaamiskeinot koskevat kuitenkin vain reaalimaailman toimintaan. POV:n on mahdollista aloittaa jossain kiiretapauksissa toiminta omalla päätöksellään Näissä tapauksissa asia tulee saattaa tuomioistuimen ratkaistavaksi heti kun se on mahdollista, mutta viimeistään 24 tunnin kuluttua keinon aloittamisesta Kyseisiä toimivaltuuksia ovat esimerkiksi tietyt televalvonnan ja teknisen seurannan tyypit, joten nämä eivät liity poliisi- ja peiteprofiileilla mahdollisiin salaisiin tiedonhankinta- ja pakkokeinoihin. Lisäksi POV voi tehdä päätöksen tietyistä televalvonnan muodoista, tietyistä teknisen tarkkailun muodoista ja teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta.
[385] Näidenkin osalta kyse on yleensä esimiehen ohjaamasta toiminnasta, vaikka poliisimies voikin yleisvalvonnan yhteydessä havaita kohteen, jota hän päättää ryhtyä tarkkailemaan. Ks. salaisen tiedonhankinnan esimiesohjaamisesta Poliisihallitus 2017c, s. 4.
[386] HE 222/2010 vp, s. 343.
[387] Käytännössä STEKPOV:n päätäntävalta valeostossa ulottuu myös tietoverkkojen ulkopuolelle, koska valeostossa puhutaan yleisön saataville toimitetusta myyntitarjouksesta, joka pitää sisällään esimerkiksi sanomalehtien tai ilmoitustaulujen myyntitarjoukset.

erityisiä oikeusturvariskejä, esimerkiksi rikosprovokaatiovaaraa, eikä toimivaltuuksilla puututa syvällisesti toimenpiteen kohteena olevan henkilön perus- ja ihmisoikeuksiin.[388] Peiteltyyn tiedonhankintaan liittyen vähimmäisvaatimuksena oleva STEKPOV-taso johtuu siitä, että on erityisen tärkeää tiedostaa peitellyn tiedonhankinnan ja peitetoiminnan raja, jotta toimivaltuutta ei käytettäisi siten, että kysymys on tosiasiallisesti peitetoiminnasta. [389] Kyseinen erojen hahmottamisen tärkeys koskee mielestäni korostuneesti tietoverkkoja ja vielä enemmän esimerkiksi tarkkailun ja suunnitelmallisen tarkkailun eroja, jotka ovat erityisesti tietoverkoissa selvästi vaikeampi hahmottaa kuin peitellyn tiedonhankinnan ja peitetoiminnan erot.[390] Tätä ei kuitenkaan ole esitöissä käsitelty. Edelleen peiteltyä tiedonhankintaa koskevien esitöiden osalta todetaan, että STEKPOV-koulutuksella pyritään vähentämään rikosprovokaatiota, tiedonhankinnan paljastumisen riskiä ja edistämään toiminnan tuloksellisuutta.[391] Valeostossa todetaan yleisön saataville toimitetun myyntitarjouksen olevan rikosprovokaatioriskiltään lähtökohtaisesti vähäisempi, jonka takia päätöksentekijätasoa on laskettu. Asiaa ei avata tarkemmin, mutta on sinänsä ymmärrettävää, että jos tiettyä tuotetta on jo tarjottu myytäväksi, rikosprovokaation riski voi olla matalampi.[392]

[388] HE 224/2010 vp, s. 53; HE 222/2010 vp, s. 137.
[389] HE 224/2010 vp, s. 104; HE 222/2010 vp, s. 327–328.
[390] Tätä eron hahmottamisen problematiikkaa tarkastellaan myöhemmin toimivaltuusosiossa.
[391] Näistä kaksi viimeistä liittyy myös suunnitelmalliseen tarkkailuun.
[392] Asia ei kuitenkaan ole näin yksinkertainen, jos myyntikohde on esimerkiksi huumausaine, eikä ole tiedossa kuinka paljon epäillyllä on huumausainetta myyntihetkellä hallussa. Tähän problematiikkaan palataan tarkemmin toimivaltuutta käsiteltäessä.

# 5 POLIISIN NÄKYVÄT PROFIILIT TIETOVERKOISSA

## 5.1 Nettipoliisitoiminta ja muu poliisin näkyvä toiminta tietoverkoissa

Poliisin toiminta sosiaalisessa mediassa voidaan karkeasti jaotella siten, että yhtäältä poliisi jakaa sosiaalisen median kautta omaan viestiään, mutta myös kerää tietoa sieltä.[393] Tietoverkkojen yleistyneen käytön ja siihen liittyvän rikollisuuden takia poliisi on ollut yhä enemmän näkyvästi läsnä erityisesti sosiaalisessa mediassa. Suomessa poliisin näkyvä toiminta sosiaalisessa mediassa alkoi syyskuussa 2008 suomalaisesta sosiaalisen median palvelusta IRC-Galleriasta ja on jatkunut eri palveluissa eri muodoissaan tähän päivään asti.[394] Jo ennen tätä poliisi oli toiminut internetissä ja sosiaalisessa mediassa, mutta lähinnä peitteen avulla. Näkyviä poliisiprofiileja voidaan käyttää laaja-alaisesti, esimerkiksi neuvontaan, rikoksiin puuttumiseen ja henkilöiden tavoitteluun.[395] Nykyään poliisi hyödyntääkin sosiaalista mediaa sekä poliisitoiminnallisesti että viestinnällisesti kaikessa toiminnassa ja kanssakäymisessä kansalaisten kanssa.[396]

Poliisi toimii sosiaalisessa mediassa poliisin strategian ja arvojen mukaisesti.[397] Poliisilla ja sen henkilöstöllä on sosiaalisessa mediassa erilaisia rooleja, joita ovat esimerkiksi poliisitoiminnalliset, viestinnälliset ja maineenhallinnalliset roolit. Poliisin strategian ja arvojen lisäksi toiminnassa on huomioitava myös poliisitoiminnan yleiset periaatteet, joista korostuu tasapuolisuuden ja puolueettomuuden vaatimus sekä poliisilain edellyttämä sovinnollisuuden edistäminen.[398] Poliisin toiminta sosiaalisessa mediassa tulee olla selkeästi johdettua, luotettavaa, avointa ja suunnitelmallista sekä tilanteen edellyttämällä tavalla vuorovaikutteista ja reagoivaa.[399] Toiminnassa tulee myös huomioida vaatimus yksityisyyden turvaamiseen sekä muut tietosuojan vaatimukset käsiteltäessä henkilötietoja

[393] Ks. esimerkiksi Police Executive Reasearch Forum 2014, s. 27–28; Kim – Oglesby-Neal – Mohr 2017, s. 2.
[394] Forss 2011, s. 244–245. Ks. myös Poliisihallitus 2012, s. 15.
[395] Henkilön tavoittelulla voidaan tarkoittaa esimerkiksi kadonneen henkilön kuvan julkaisemista tai vaihtoehtoisesti rikoksesta epäillyn kuvan julkaisua tunnistamista varten.
[396] Poliisihallitus 2017b, s. 1.
[397] Poliisin strategiset tavoitteet ovat turvallisuuden edistäminen, rikollisuuden torjuminen, hyvät palvelut sekä avoin toiminta ja vaikuttavuuden edistäminen. Poliisin arvoja ovat palvelu, oikeudenmukaisuus, osaaminen ja henkilöstön hyvinvointi.
[398] Poliisihallitus 2017b, s. 2. Ks. myös Poliisihallitus 2017b, s. 5–6, jossa tarkemmin poliisin käyttäytymisvelvoitteesta sosiaalisessa mediassa.
[399] Ks. tarkemmin sosiaalisen median toiminnan organisoinnista ja vastuukysymyksistä Poliisihallitus 2017b, s. 3.

sosiaalisessa mediassa. Erityisesti tulee kiinnittää huomiota henkilötietojen käsittelyn lainmukaisuuteen ja siihen, ettei tarpeettomia henkilötietoja levitetä tai muutoin käsitellä.[400]

Nettipoliisitoiminnaksi kutsutaan lähtökohtaisesti toimintaa, jossa poliisimies tekee työtä sosiaalisessa mediassa joko täysipäiväisesti, tai käyttää sosiaalista mediaa työkaluna omassa työssään. Näkyvät poliisiprofiilit ovat nykyään vahvasti sidoksissa poliisin ennalta estävään toimintaan ja yleisesti organisaatiotason viestintään. Poliisin näkyvää toimintaa sosiaalisessa mediassa ei kuitenkaan rajoiteta pelkästään näihin toimintoihin, vaan sosiaalisen median mahdollisuuksia hyödynnetään mahdollisimman laajasti kaikessa poliisitoiminnassa. Eli valvonta- ja hälytystoiminnan, rikostorjunnan ja liikenneturvallisuuden sekä lupahallinnon prosessien yhteisvaikuttavuus kattavasti ja tehokkaasti sekä tuottavasti huomioiden. Lisäksi sidosryhmäyhteistyö huomioidaan myös sosiaalisessa mediassa.[401]

Aikaisemmin Helsingissä toimi kolme kokopäiväistä nettipoliisia, jotka työskentelivät päätoimisesti näkyvillä poliisiprofiileilla eri sosiaalisen median palvelussa.[402] Tällä hetkellä sosiaalisesta mediasta löytyy pääsääntöisesti oman työnsä ohella toimivia näkyviä poliisiprofiileja.[403] Näkyvä poliisiprofiili voi olla esimerkiksi valvonta- ja hälytystehtävissä toimivalla poliisilla, joka kertoo yleisesti poliisin työstä tai Poliisiammattikorkeakoulun opiskelija, joka kertoo ajankohtaisia asioita opiskelustaan. Heillä toiminnan tarkoitus ja työajan käyttö sosiaaliseen mediassa vaihtelevat suuresti.[404] Lisäksi sosiaalisesta mediasta löytyy poliisilaitoskohtaisia, asiantuntijakohtaisia ja erilaisia toimintoja koskevia käyttäjätilejä, joita ei yleensä kutsuta nettipoliiseiksi.[405]

[400] Poliisihallitus 2017b, s. 2.
[401] Poliisihallitus 2017b, s. 3–4.
[402] Helsingissä toiminut kolmen nettipoliisin ryhmä oli keskittynyt enemmän rikoksiin puuttumiseen ja niiden selvittämiseen tähtääviin toimenpiteisiin, mutta ryhmää ei ole enää olemassa. Toiminta loppui maaliskuussa 2017. Näkyvät profiilit olivat myös tiedonkeräämismielessä hyviä, koska profiilit saivat suuren määrän viestejä päivittäin erityisesti sosiaaliseen mediaan liittyvästä rikollisuudesta. Ks. poliisitoiminnallisesta luonteesta tarkemmin Forss 2011, s. 249–252.
[403] Vuoden 2019 vaihteessa Suomessa levisi laajasti uutisointi Oulun seksuaalirikoksista, joissa oli epäiltynä useita maahanmuuttajataustaisia miehiä. Tähän liittyen hallitus päätti lisätalousarviossaan vahvistaa poliisin resursseja torjua ja ennalta ehkäistä seksuaalirikoksia internetissä. Tähän liittyen tarkoituksena oli palkata kaksi nettipoliisia jokaiselle poliisilaitokselle. Ks. Sisäministeriö 2019b.
[404] Poliisihallitus 2012, s. 32–33; Poliisihallitus 2016a, s. 12.
[405] Ks. näistä tarkemmin poliisilaitoskohtaisilta internetisivuilta. Jokaisen poliisilaitoksen sosiaalisen median profiilit löytyvät sivun www.poliisi.fi/some kautta. Mukana on asiantuntijoina esimerkiksi poliisipäälliköitä ja erilaisissa päällystötehtävissä toimivia henkilöitä ja toimintokohtaisista käyttäjätileistä voidaan mainita esimerkkinä Helsingin ratsupoliisi.

## 5.2 Näkyvän poliisiprofiilin luominen ja suhde salaisiin tiedonhankinta- ja pakkokeinoihin

Näkyvä poliisiprofiili perustetaan sosiaaliseen mediaan poliisimiehen henkilökohtaista poliisi.fi -päätteistä sähköpostiosoitetta käyttäen ja profiilin tiedoista käy selkeästi ilmi, että kyseessä on poliisi. Profiilissa esiinnytään omalla nimellä ja kuvalla. Kyseisen profiilin tiedot tulee myös lisätä poliisin kotisivuille, jotta kansalainen pystyy varmistumaan profiilin aitoudesta.[406] Jos profiilin käyttäjän virkasuhde päättyy, virkamies vaihtaa tehtävää, tai profiilia ei enää käytetä, on kyseinen profiili lakkautettava. Profiilia ei voi muuttaa siviilikäyttöön käytön loputtua.[407]

Vaikka kyse on näkyvästä poliisitoiminnasta, voi myös näkyvän poliisiprofiilin käyttö tulla kyseeseen salaisten tiedonhankinta- ja pakkokeinojen käytössä. Tämä pitää kuitenkin erottaa näkyvän poliisiprofiilin jo itsessään rikoksista tietoa tuottavasta ja paljastavasta luonteesta.[408] Poliisiprofiilien pelkkä läsnäolo tuottaa yhteydenottoja esimerkiksi rikosten asianomistajilta ja yleisesti vihjetietoa rikoksista.[409] Esimerkkinä voidaan mainita lapsen seksuaalinen hyväksikäyttö ja nettikiusaaminen, josta tuli aikaisemmin useita ilmoituksia suoraan asianomistajilta silloiselle Helsingin nettipoliisille.[410] Salaisista tiedonhankinta- ja pakkokeinoista tulee näkyvällä poliisiprofiililla kyseeseen suunnitelmallinen tarkkailu (PolL 5:13.2 ja PKL 10:12.2) ja tietolähteen ohjattu käyttö (PolL 5:40.2 ja PKL 10:39.2). Tarkemmin näiden toimivaltuuksiin käyttöön palataan kyseisiä toimivaltuuksia käsiteltäessä.

## 5.3 Siviiliprofiilin käyttö poliisin työtehtävissä

Poliisimiehet käyttävät sosiaalista mediaa siinä missä muutkin kansalaiset, joten useimmilta poliiseilta löytyy siviiliprofiileja erilaisista sosiaalisen median palveluista. Etenkin pienemmillä paikkakunnilla poliisit tunnetaan, joten ei ole sinänsä väliä, onko

[406] Poliisin näkyvään toimintaan liittyvät tiedot on koottu sivustolle www.poliisi.fi/some. Tietyissä sosiaalisen median palveluissa on myös mahdollisuus verifioida profiili.
[407] Poliisihallitus 2017b, s. 7.
[408] Poliisin toiminta sosiaalisessa mediassa rikosten paljastamiseksi ei siten ole sama asia kuin salaisten tiedonhankintakeinojen käyttö rikoksen paljastamiseksi. Näkyvien poliisiprofiilien rikoksia paljastavalla luonteella tarkoitetaan esimerkiksi sosiaalista mediaa yleisesti seuraamalla havaittavia rikoksia, joita voivat olla yleensä erilaiset sananvapausrikokset. Ks. tarkemmin Poliisihallitus 2016a, s. 18.
[409] Poliisihallitus 2016a, s. 13. Lisäksi voidaan mainita keskusrikospoliisin ylläpitämä Nettivikki, jonka kautta kansalaiset voivat lähettää vihjeitä lähinnä internetiin liittyvistä rikoksista. Vinkin voi lähettää sivuilta www.poliisi.fi/nettivinkki.
[410] Poliisihallitus 2012, s. 72.

siviiliprofiilissa tietoja ammatista. Toisaalta monesti profiilista voi käydä tavalla tai toisella ilmi poliisin ammatti, jolloin se rinnastuu selkeämmin poliisiprofiiliin. On myös selvää, että siinä missä muutoinkin vapaa-ajalla, voi poliisi havaita rikoksen myös sosiaalisessa mediassa. Poliisimiehen joko voi, tai hänen tulee reagoida rikokseen.[411] Poliisilla on luonnollisesti normaalin kansalaisen tapaan lähettää eteenpäin havaitsemiaan tietoja.[412] Käytännössä siviiliprofiililla tulee harvemmin eteen tilanteita, joissa poliisimiehen tulisi reagoida välittömästi tilanteeseen muutoin kuin ilmoittamalla asiasta eteenpäin, oli kyse rikoksista tai tiedustelutiedosta.[413]

Lainsäädännössä ei oteta erikseen kantaa siihen, voiko poliisimies toimia tietoverkoissa siviilikäyttöön tarkoitetulla profiililla salaisia tiedonhankinta- ja pakkokeinoja käyttäessä. Sama koskee myös muita siviilikäyttöön tarkoitettuja telepäätelaitteita tai teleosoitteita. Ei ole esimerkiksi sääntelyä siitä, voiko poliisimies soittaa asiakkaalle omalla puhelimellaan tai toimia omalla tietokoneella, jonka IP-osoite on hänen siviilikäyttöön liittyvä. Poliisin sosiaalisen median ohjeen mukaan poliisin sosiaalisen median toimintaan liittyvät yksikkö- ja muut virkaprofiilit tulee erottaa selvästi yksityisistä siviiliprofiileista. Tältä osin kyse on vain erottelusta, eikä käytöstä. Erikseen on kielletty sosiaalisen median yksityisessä käytössä salassa pidettävien virka- ja työasioiden käsittely, poliisin sähköpostiosoitteiden tai muiden työhön liittyvien tunnusten käyttö.[414] Tämä puoltaisi sitä tulkintaa, ettei työasioita voi käsitellä siviiliprofiilissa. Tulee kuitenkin ottaa huomioon, että poliisin sosiaalisen median ohje on tarkoitettu lähinnä poliisin näkyvän toiminnan ohjeistukseksi, vaikka se onkin soveltuvin osin voimassa myös tiedonhankinnassa, koska myös näkyvillä poliisiprofiileilla voi suorittaa salaista tiedonhankintaa.[415]

---

[411] Velvollisuuteen reagoida rikoksiin koko valtakunnan alueella voidaan viitata PolHalL 15 c §:n 3 momenttiin, jonka mukaan poliisimiehen on ilman eri määräystä velvollinen ryhtymään kiireellisiin toimiin koko maassa myös toimialueensa ulkopuolella ja vapaa-aikanaan, jos se on välttämätöntä vakavan rikoksen estämiseksi, tällaista rikosta koskevan tutkinnan aloittamiseksi tai yleistä järjestystä ja turvallisuutta uhkaavan vakavan vaaran torjumiseksi taikka jos se näihin rinnastettavan muun erityisen syyn vuoksi on tarpeen.

[412] Vihjetiedon välittämiseen eteenpäin ei poliisimiehellä ole erikseen velvollisuutta vapaa-aikanaan, jos kyseessä ei ole PolHalL 15 c §:n 3 momentin mukainen tilanne.

[413] Tietoverkoissa puuttuminen rikoksiin rajoittuu lähinnä sananvapausrikoksiin, mutta näiden osalta on harvemmin kyse sellaisesta vakavasta rikoksesta, johon poliisimiehen tulisi konkreettisesti puuttua esimerkiksi viestimällä kohteelle. Vakavien tapausten osalta poliisimiehellä on kuitenkin velvollisuus toimia, joten esimerkiksi vapaa-ajalla havaittuun vakavasti otettavaan koulu-uhkaukseen sosiaalisessa mediassa tulee reagoida.

[414] Poliisihallitus 2017b, s. 4 ja 6. Kielto käsitellä virka- ja työasioita koskee lähinnä tilanteita, jossa omissa sosiaalisen median profiileissa esimerkiksi keskustellaan salassa pidettävistä virka- ja työasioista, eikä niinkään siitä, että poliisimies suorittaa jotain tehtävää tai käyttää jotain toimivaltuutta siviiliprofiilillaan.

[415] Ks. Poliisihallitus 2017b, s. 2.

Poliisimies voi luonnollisesti toimia tietoverkoissa myös yksityishenkilönä, mutta tällöin tulee arvioida, onko kyseessä työtehtävä vai vapaa-ajantoiminta. Eroja työtehtävän ja vapaa-ajan toiminnan välillä voidaan arvioida seuraavin kriteerein: 1) *mitä tarkoitusta varten ja millä tiedoilla siviiliprofiili on luotu*, 2) *onko kyseessä salainen tiedonhankinta- tai pakkokeino*, 3) *onko poliisilla vireillä toimintaa tiedonhankinnan kohteena olevaan henkilöön liittyen*, 4) *missä, milloin ja millä laitteella tiedonhankinta tapahtuu* ja 5) *tapahtuuko tiedonhankinta esimiehen ohjauksessa*.

Jos poliisimies on luonut profiilin omalla kuvallaan ja muutoinkin omilla henkilötiedoillaan sekä käyttää profiilia vapaa-ajallaan esimerkiksi yhteydenpitoon läheisten kanssa, kaupantekoon, harrastuksiin tai muutoin työn ulkopuolisiin asioihin liittyen, on kyse selvästi siviilitarkoitukseen luodusta profiilista. Tähän ei vaikuta se, millaista tietoa hän voi sattumalta saada sen käytön yhteydessä. Jos poliisimies alkaa käyttää tätä täysin siviilikäyttöön luotua profiilia salaisessa tiedonhankinnassa, tulisi sitä arvioida samoista lähtökohdista kuin muutenkin poliisin työtä. Esimerkkinä voidaan mainita *Ramanauskas* -tapaus, jossa poliisi oli alkanut valmistelemaan peitetoimintaa yksityishenkilönä. EIT totesi, etteivät viranomaiset voi vapautua virkavastuustaan kyseisellä tavalla.[416] Poliisimiestä koskeekin profiilista riippumatta PolL 5 luvun ja PKL 10 luvun toimivaltuusedellytykset ja muotomääräykset.[417]

Jos siviiliprofiili on luotu vääriä, harhauttavia tai peiteltyjä tietoja käyttäen, on sillä vaikutusta salaisten tiedonhankinta- ja pakkokeinojen suojaamista koskevan sääntelyn kannalta. Jos vääriä, harhauttavia tai peiteltyjä tietoja sisältävää siviiliprofiilia käytetään työtehtävässä salaiseen tiedonhankintaan, tulisi lähtökohtaisesti noudattaa PolL 5:46:n ja PKL 10:47:n mukaista sääntelyä. Tällöin suojaamisen käytöstä tulisi myös olla PolL 5:47.2:n tai PKL 10:48.2:n mukaisesti STEKPOV:n päätös.[418] Vapaa-ajankäyttöön tällaisen vääriä, harhauttavia tai peiteltyjä sisältävän siviiliprofiilin tekeminen on kuitenkin sallittua myös poliisimiehelle, esimerkiksi kanavaksi käydä kansalaiskeskustelua ilman taustansa paljastamista.[419] Pelkkä poliisiaiheisista asioista keskustelu näkyvästi poliisina tai

[416] *Ramanauskas* v. Venäjä (2008), kohta 63.
[417] Luonnollisesti myös esitutkintaa koskevat ETL 4 luvun mukaiset periaatteet sekä muu poliisin esitutkintaa yleisesti ohjaava sääntely tulee huomioida.
[418] Jos poliisimies esiintyy omilla tiedoillaan, ei kyseistä suojaamissääntelyä luonnollisesti tarvitse soveltaa.
[419] Sosiaalista mediaa käytetään paljon yhteiskunnalliseen keskusteluun, vaikka se ei aina olekaan välttämättä aina kovin tasokasta. Erityisesti anonymiteetin tarve voi korostua aiheissa, joissa keskustelu onnistuu keskimääräistä heikommin tai on muutoin omiaan leimaamaan poliisin tietyn ideologian kannattajaksi.

anonyymisti ei kuitenkaan vielä tarkoita sitä, että kyseessä olisi työtehtävään liittyvä toimi.[420]

On normaalia, että sosiaalista mediaa selaillaan käyttäjien toimesta siten, että se on rinnastettavissa poliisin suorittamaan yleisvalvontaan. Käytännössä yleisvalvonnassa toiminnan luonteen ratkaisee se, onko poliisimiehelle annettu tehtäväksi seurata tiettyä keskustelupalstaa tai sosiaalisen median ryhmää. Sama koskee myös tilannetta, jossa poliisimies voi olla tutkijana rikoksessa, johon liittyen hän alkaa suorittamaan toimenpiteitä siviiliprofiilillaan rikoksesta epäiltyyn liittyen. Tällöin ollaan selvästi työtehtävän puolella ja siten PKL 10 luvun sääntely tulee ottaa huomioon.[421] Erityisesti tämä korostuu silloin, jos poliisimies suorittaa toimenpiteitä siviiliprofiilillaan työpaikalla, työaikana ja työnantajan laitteilla.[422]

Suunnitelmallisen tarkkailun (PolL 5:13 ja PKL 10:12) kohdalla voi syntyä haastavia rajanvetotilanteita, jos poliisimies on seurannut vapaa-ajallaan siviiliprofiililla henkilöitä, jotka tulevatkin osaksi hänen työtehtäväänsä.[423] Tällöin poliisimiehen normaali toiminta vapaa-ajalla voi sinänsä jatkua, mutta jos kyseisen toiminnan perusteella alkaa muodostua työssä hyödynnettävää tietoa, siirtyy toiminta enemmän työtehtävän puolelle.[424] Sama rajanveto-ongelma voi koskea myös tilannetta, jossa poliisimies kuuluu vapaa-ajallaan sosiaalisen median suljettuun ryhmään, johon liittyen poliisimiehelle muodostuu työtehtävä. Tällöin voi herätä kysymys onko kyse peitellystä tiedonhankinnasta tai peitetoiminnasta, jos poliisimies osallistuu aktiivisesti ryhmän keskusteluihin myös sen jälkeen, kun tiedonhankintatarve työtehtävään liittyen on alkanut. Poliisimiehen toiminnan jatkaminen ilman nimenomaisen toimivaltuuden käyttämistä tulisi linjata kaikissa tapauksissa vähintään

[420] Sinänsä ei ole kuitenkaan täysin poissuljettua, etteikö jossain tapauksissa esimerkiksi peitetoimintaa suorittava poliisimies voisi käyttää vääriä, peiteltyjä tai harhauttavia tietoja myös siten, että hän esiintyy vapaa-ajalla olevana poliisina. Kysymykseen voi tulla esimerkiksi tilanne, jossa henkilö yrittää soluttautua poliisina viharikoksiin syyllistyneeseen ryhmään. Poliisimies voisi esimerkiksi kertoa olevansa hallituksen ja virkamiesten turvapaikanhakijoita suosivaan toimintaan läpeensä kyllästynyt poliisimies, joka haluaa tuoda esille erilaisia työssään esille tulleita vääryyksiä viharikoksiin syyllistyneen ryhmän kautta.

[421] Tätä korostaa erityisesti perustuslain 2.3 §:ä, jonka mukaan julkisen vallankäytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava lakia.

[422] Tällöin korostuu myös salassapitoa koskeva sääntely. On ongelmallista, mutta myös poliisin sosiaalisen median ohjeen vastaista, että poliisimies käsittelisi työhönsä liittyvää salassa pidettävää tietoa siviiliprofiilissaan. Toisaalta osittain ongelmallista se on myös näkyvillä poliisiprofiileilla, joissa sosiaalisen median kanavissa voi yksityisviestein liikkua hyvinkin arkaluontoisia tietoja.

[423] Etenkin kun otetaan huomioon se, että jos viranomainen hankkii järjestelmällisesti tietoa jonkun yksityiselämästä, tiedonhankinta saattaa merkitä henkilö yksityiselämän suojaan puuttumista. Ks. HE 57/1994 vp s. 56.

[424] Reaalimaailmassa tämän eron hahmottaminen on selvästi helpompaa, koska poliisimiehet eivät lähtökohtaisesti seuraile ja tarkkaile työhönsä liittyviä henkilöitä vapaa-ajallaan.

STEKPOV:n tasoisen henkilön toimesta, koska hänen tulisi olla riittävällä tavalla perehtynyt salaisia tiedonhankinta- ja pakkokeinoja koskevaan sääntelyyn. Käytännössä aktiivista ja vuorovaikutteista tiedonhankintaa voidaan tuskin jatkaa ilman toimivaltuussäännösten ja muotomääräysten noudattamista.

Sama päätöksentekijätasoon liittyvä problematiikka koskee myös muita toimivaltuuksia. Yleensä tiedonhankintaa suorittava poliisimies on miehistöön kuuluva, eikä omaa päätöksenteko-oikeutta salaisten tiedonhankinta- tai pakkokeinon käyttöön kuin hätätilanteessa. Ainoastaan yleisvalvontaan tai tarkkailuun ei tarvita vähintään POV:n tasoista päättäjää. Lisäksi voidaan mainita peitetoiminnan ja valeostojen koulutusvaatimukset (EPSA 3:9.3 ja 3:11.3), joita suorittamaton ei voi toimia kyseisissä tehtävissä. Vaikka poliisimiehellä on sinänsä oikeus tehdä yleisvalvontaa ja tarkkailla oman päätöksensä nojalla, tulee huomioida, että myös tietoverkoissa tapahtuva tiedonhankinta on johdettua toimintaa.[425] Työnantajan tulisikin tarjota sopivat työkalut tietoverkoissa toimimiseen kaikissa tilanteissa, eikä toiminnan tulisi perustua siviiliprofiilien käyttöön.

[425] Poliisihallitus 2017c, s. 4. Ks. esimiestyön merkityksestä yleisesti salaisten tiedonhankinta- ja pakkokeinojen osalta Hankilanoja 2014, s. 37–39.

# 6 POLIISIN PEITEPROFIILIT TIETOVERKOISSA

## 6.1 Salaisten tiedonhankinta- ja pakkokeinojen suojaaminen

Suojaamisesta säädetään samansuuntaisesti poliisi- ja pakkokeinolaissa ja sääntely jakautuu suojaamisen osalta kahteen eri tapaan (PolL 5:46 ja PKL 10:47).[426] PolL 5:46.1:ssä ja PKL 10:47.1:ssä on kyse poliisin mahdollisuudesta siirtää puuttumista rikokseen, kun taas PolL 5:46.2:ssä ja PKL 10:47.2:ssä on kyse erilaisista tavoista estää poliisin paljastuminen.[427] PolL 5:46.2:n ja PKL 10:47.2:n mukaan poliisi saa käyttää vääriä, harhauttavia tai peiteltyjä tietoja, tehdä ja käyttää vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä sekä valmistaa ja käyttää vääriä asiakirjoja. Toiminnan tulee olla välttämätöntä jo toteutetun, käynnissä olevan tai tulevaisuudessa toteutettavan salaisen tiedonhankinta- tai pakkokeinon käytön suojaamiseksi. PolL 5:46.3:n ja PKL 10:47.3:n mukaan rekisterimerkintä on oikaistava sen jälkeen, kun edellytyksiä sen käyttämiseen ei enää ole.

Suojaamissäännöksessä ei kyse ole poliisin toimivaltuudesta, vaan sillä pyritään turvaamaan jo olemassa olevien keinojen tehokas käyttäminen niiden erityisluonne huomioon ottaen.[428] Lisäksi on huomioitava, että suojaamistoimilla voidaan suojata vain poliisia. Tämä on huomioitava esimerkiksi tietolähdetoiminnassa, koska säännöksellä ei voida suojata itse tietolähdettä.[429] Suojaamisen päätöksentekijätaso riippuu siitä, onko kyse tiedosta, rekisterimerkinnästä vai asiakirjasta. Rekisterimerkinnästä ja asiakirjan valmistamisesta päättää keskusrikospoliisin tai suojelupoliisin päällikkö (PolL 5:47.1 ja PKL 10:48.1).[430] STEKPOV päättää näiden ulkopuolelle jäävästä tiedonhankinnan suojaamisesta (PolL 5:47.2 ja PKL 10:48.2).[431] Rekisterimerkintöjen tekemisestä sekä asiakirjojen valmistamisesta

[426] Poikkeuksena pakkokeinolakiin myöhemmin lisätyt Tullille ja Rajavartiolaitokselle kuuluvat oikeudet.
[427] Ensimmäisen momentin osuutta käsitellään myöhemmin omassa kohdassaan.
[428] HE 266/2004 vp, s. 31. Vaikka suojaamissäännös ei ole toimivaltuussäännös, puoltaa erityisesti vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä koskeva tekeminen ja käyttö toimivaltuusluonnetta. Jos kyseistä toimivaltuutta ei olisi, syyllistyisi poliisi rikokseen tehdessään tekaistuja rekisterimerkintöjä.
[429] HE 224/2010 vp, s. 131; HE 222/2010 vp, s. 354. Poikkeuksen tähän tekee laki todistajansuojelunohjelmasta (88/2015), johon liittyen myös suojellulle voidaan 5.1 §:n mukaan tehdä ja valmistaa toista henkilöllisyyttä tukevia vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä ja asiakirjoja, jos se on välttämätöntä todistajansuojeluohjelman toteuttamiseksi. Tämän toiminnan osalta ei kuitenkaan ole kyse salaisesta tiedonhankinta- tai pakkokeinosta.
[430] Jos poliisilaitos haluaa käyttää rekisterimerkintöjä tai asiakirjoja, tulee poliisilaitoksen tehdä esitys rekisterimerkinnän tekemisestä ja väärän asiakirjan valmistamisesta keskusrikospoliisille (EPSA 3:20.2).
[431] Keskusrikospoliisin päällikkö, suojelupoliisin päällikkö ja poliisilaitoksen päällikkö määräävät kukin yksikössään harhauttavien tai peiteltyjen rekisterimerkintöjen ja väärien asiakirjojen käyttämisestä vastaavan STEKPOV:n (EPSA 3:19).

päättäneen viranomaisen on pidettävä luetteloa merkinnöistä ja asiakirjoista, valvottava niiden käyttöä sekä huolehdittava merkintöjen oikaisemisesta (PolL 5:47.3 ja PKL 10:48.3).[432] Rekisterien, asiakirjojen ja tietojen käyttämistä salaisten tiedonhankinta- ja pakkokeinojen suojaamisessa voidaan selventää seuraavalla kuviolla.

| SUOJAAMISTYYPPI | SUOJAAMISTAPA | PÄÄTÖKSENTEKIJÄ |
|---|---|---|
| REKISTERI | Väärien, harhauttavien tai peiteltyjen rekisterimerkintöjen tekeminen ja käyttö | KRP:n tai supon päällikkö |
| ASIAKIRJA | Väärien asiakirjojen valmistaminen ja käyttäminen | KRP:n tai supon päällikkö valmistamisesta ja käyttämisestä STEKPOV |
| TIETO | Väärien, harhauttavien tai peiteltyjen tietojen käyttäminen | STEKPOV |

Kuvio 5. Salaisten tiedonhankinta- ja pakkokeinojen suojaamiskeinot.

Tiedon, asiakirjan tai rekisterin määritelmiä ei ole avattu tarkemmin poliisi- tai pakkokeinolaissa taikka niiden esitöissä.[433] Sama koskee osittain myös määritelmiä väärä, harhauttava ja peitelty, joiden osalta tietoverkkojen roolia ei ole käsitelty lainvalmistelussa lainkaan.[434] Salaisiin tiedonhankinta- ja pakkokeinoihin liittyen ensimmäisen kerran erilaisia

[432] Kyseisten tahojen tulee myös sopia erikseen PolL 5:46.2:n ja PKL 10:47.2:ssä tarkoitettujen rekisterien rekisterinpitäjien kanssa harhauttavien tai peiteltyjen rekisterimerkintöjen tekemisestä sekä niiden oikaisemisen yksityiskohtaisista menettelytavoista (EPSA 3:20.1).

[433] Rekisterin ja asiakirjan määritelmiä löytyy erilaisista laeista, vaikka niihin ei ole nimenomaisesti viitattu salaisten tiedonhankinta- ja pakkokeinojen osalta.

[434] Pakkokeinolain esitöissä tyydytään vain toteamaan, että erot näiden kolmen määritelmän välillä ovat vähäisiä ja ne ovat tältä osin toisiinsa rinnastettavia. Ks. HE 222/2010 vp, s. 140. Peitetoiminnan alkuperäisissä esitöissä ilmaisulla ”harhauttavia tai peiteltyjä” tarkoitettiin vääriä tai puutteellisia tietoja, jotka annetaan paljastumisen estämiseksi. Ks. HE 34/1999 vp, 27. Poliisi on kuitenkin soveltanut suojaamistoimia myös tietoverkoissa jo vuosia. Poliisihallituksen vuotta 2016 koskevassa kertomuksessa salaisten tiedonhankintakeinojen käytöstä todetaan, että vuonna 2016 suojaamispäätöksiä oli toteutettu useita kymmeniä suoritettaessa peitetoimintaa ja valeostoja tietoverkossa. Ks. Poliisihallitus 2017a, s. 34.

poliisin paljastumisen estämiskeinoja on käsitelty lain tasolla peitetoiminnan poliisilakiin tuoneessa hallituksen esityksessä 34/1999 vp. Tämän jälkeen määritelmiä on avattu varsinaista suojaamissääntelyä koskevassa alkuperäisissä hallituksen esityksessä 266/2004 vp. Kyseisessä esityksessä puhuttiin vielä tiedonhankinnan paljastumisen estämisestä ja määritelmiä on avattu jonkin verran esimerkkien avulla.[435]

*Rekisterin* määritelmä voi koskea poliisi- ja pakkokeinolain sekä niitä koskevien esitöiden perusteella teoriassa millaista rekisteriä tahansa. Oli se sitten viranomaisen tai yksityisen ylläpitämä rekisteri. Tätä tulkintaa tukee EU:n tietosuoja-asetuksen (2016/679) 4 artiklan 1 kohdan henkilötiedon määritelmää koskeva erittäin laaja kattavuus, jonka takia tietoja rekisteriin tallennettaessa muodostuu miltei aina henkilörekisteri, jossa tiedot ovat yhdistettävissä joko suoraan tai epäsuorasti johonkin luonnolliseen henkilöön.[436] Selvimpänä rekisterin määritelmänä voidaankin pitää EU:n tietosuoja-asetuksen 4 artiklan määritelmää.[437] Rekistereihin kohdistuvina yleisimpinä suojaamistapoina voidaan pitää viranomaisen ylläpitämiin rekistereihin kohdistuvia väärien, peiteltyjen tai harhauttavien rekisterimerkintöjen tekemistä sekä niiden käyttöä. Viranomaisen rekistereitä on Suomessa tuhansia ja osaa näistä nimitetään niin sanotuiksi perusrekistereiksi. Näille on ominaista lakisääteisyys, valtakunnallinen tiedollinen kattavuus, luotettavuus, monikäyttöisyys ja tietojen suojaus. [438] Esimerkkejä viranomaisen perusrekistereistä ovat väestötietojärjestelmä, kiinteistötietojärjestelmä sekä yritys- ja yhteisötietojärjestelmä.[439]

Rekistereiden luotettavuutta suojataan lähtökohtaisesti RL 16:7:n rekisterimerkintärikosta koskevalla sääntelyllä. Säännöksessä puhutaan viranomaisen ylläpitämästä yleisestä

---

[435] Tuolloin tiedonhankinnan paljastumisen estämisen piiriin otettiin silloinen tarkkailu, tekninen tarkkailu, valeosto, peitetoiminta ja tietolähdetoiminta. Nykyään suojaamissääntely kattaa kaikki salaiset tiedonhankinta- ja pakkokeinot. Lisäksi tukea suojaamissäännöksen tulkintaan voi yrittää hakea todistajansuojeluohjelmaa koskevan lain (88/2015) 5 §:ää koskevan säännöksen esitöistä, jossa käsitellään vääriä, harhaanjohtavia tai peiteltyjä tietoja, rekisterimerkintöjä ja asiakirjoja. Näitä keinoja on mahdollista käyttää poliisimiehen suojaamisen lisäksi todistajansuojeluohjelman toteuttamiseen.

[436] Tietosuoja-asetuksen johdannon 26 kohdan mukaan henkilötiedon käsite koskee myös pseudonymisoituja tietoja, jotka voidaan yhdistää luonnollisiin henkilöihin lisätietoja käyttämällä. Henkilötiedon käsitteen on katsottu pitävän sisällään esimerkiksi ajoneuvon IP-osoitteen, valokuvan Ks. IP-osoitteesta tarkemmin EUT:n C 582/14 *Patrick Breyer v Saksan liittotasavalta* EUVCL:C:475. ja Tietosuojalautakunta 4.4.2006 1/2006. Ks. myös valokuvasta henkilötietona Tietosuojalautakunta 25.2.2002 1/2002.

[437] Rekisterillä tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu.

[438] Voutilainen 2009, s. 90–91.

[439] Peitetoimintaa koskevassa hallituksen esityksessä rekistereiden todetaan olevan passi-, ajokortti- tai väestön keskusrekisteri. Myös ajoneuvon sekä omaisuuden omistaja- ja haltijatiedot mainitaan. Ks. HE 34/1999 vp, s. 27–28. Peitetoiminnan salaamiseksi voitiin siten merkitä esineen, ajoneuvon tai muun varusteen haltijaksi jokin muu kuin poliisiorganisaatio. Lisäksi poliisille voitiin luoda uusi henkilöllisyys.

rekisteristä. Rekisterimerkintärikosta koskevissa esitöissä viitataan silloisiin väestö-, kauppa-, moottoriajoneuvo- ajokortti-, yhdistys-, säätiö-, lainhuuto-, kiinnitys-, maa- tai patenttirekisteriin. Vaikka viranomaisen rekisterin käsitettä ei ole määritelty tarkemmin, tulee yleisen rekisterin sisältämillä tiedoilla olla esitöiden mukaan ainakin jonkinlaista merkitystä todisteena oikeuselämässä. Viranomaisen rekisterin yleisyydellä viitataan silloiseen asiakirjain julkisuudesta annettuun lakiin, joka on sittemmin kumottu ja korvattu lailla viranomaisen julkisuudesta (621/1999, JulkL tai julkisuuslaki). Viranomaisen rekisterin ei kuitenkaan tarvitse olla julkinen.[440]

Suojaamistoimien kohteena olevien rekisterien on mahdollista olla myös muita kuin viranomaisen ylläpitämiä rekistereitä, mutta asiaa ei ole sivuttu esitöissä kuin todistajansuojelua koskevan lainsäädännön esitöissä.[441] Poliisihallituksen määräyksessä suojaamistoimenpiteiden kohteena olevat mahdolliset rekisterit kuvataan viranomaisen ylläpitämiksi ja julkista luotettavuutta omaaviksi rekistereiksi.[442] Voimassa olevassa määräyksessä ei ole kuitenkaan tarkemmin määritelty, mitkä kaikki rekisterit voivat olla julkista luotettavuutta nauttivia rekistereitä. Tällaisia voisivat käytännössä olla esimerkiksi pankkien asiakasrekisterit. Muiksi enemmän ja vähemmän luotettavuutta nauttiviksi rekistereiksi voidaan mainita kaupallisten toimijoiden asiakasetuusjärjestelmiin liittyvät rekisterit, puhelinoperaattorien asiakasrekisterit, mutta myös erilaisia virtuaalivaluuttoja säilyttävien kryptovaluuttatiliyritysten rekisterit.[443] Rajanveto ei ole siis selkeä julkisen luotettavuuden osalta. Tulee myös huomioida, että jos poliisi haluaa tehdä merkintöjä muun kuin viranomaisen ylläpitämiin rekistereihin, jää yksityisen rekisterinpitäjän harkintaan haluaako kyseinen taho tehdä vääriä rekisterimerkintöjä.[444] Lisäksi yksityisten rekisterinpitäjien osalta voidaan joutua arvioimaan kattavammin poliisin toiminnan paljastumisvaaraa.

---

[440] HE 6/1997, s. 72. Tällaisesta toimii esimerkkinä esitöiden mukaan Oikeusrekisterikeskuksen ylläpitämä rikosrekisteri. Poliisiviranomaisten rikostutkintaa liittyvistä syistä ylläpitämät tekotapa- tai muut sellaiset rekisterit, jotka on tarkoitettu yksinomaan viranomaisen sisäiseen käyttöön, eivät voi kuitenkaan olla rekisterimerkintärikoksen kohteena. Kyseisen säätämisajan jälkeen on luonnollisesti tullut muutoksia erilaisiin rekistereihin ja esimerkiksi ratkaisussa KKO 2016:92 ulkomaalaisrekisteri on katsottu viranomaisen rekisteriksi.

[441] HE 65/2014 vp, s. 39.

[442] Poliisihallitus 2018a, s. 8–9.

[443] Näitä voisi olla esimerkiksi Kesko Oyj:n ylläpitämä K-Plussan asiakasrekisteri ja S-ryhmän asiakasrekisteri. asiakasrekisteriin. Virtuaalivaluutan osalta voidaan mainita Coinmotion ja Coinbase. Myös näiden rekisterien kohdalla tulee muistaa välttämättömyysvaatimus, joten vääriä rekisterimerkintöjä ei tule tehdä yksityisiinkään rekistereihin ilman ilmeistä tarvetta.

[444] Myös yksityisen rekisterinpitäjän kanssa tulee soveltaa EPSA 3:20:n sääntelyä yksityiskohtaisten menettelytapojen sopimisesta rekisterimerkintöjen tekemisen ja oikaisemisen osalta.

Tietoverkkoihin liittyen jää esitöissä selventämättä se seikka, onko peiteprofiilia pidettävä suojaamissääntelyn mukaisena rekisteriin tehtynä vääränä, peiteltynä tai harhauttavana rekisterimerkintöjen tekemisenä ja käyttönä. Sosiaalisen median palveluja ja muita tietoverkkojen sivustoja on pidetty erityisesti tietosuoja-asetuksen säätämisen jälkeen yksiselitteisesti henkilörekistereinä.[445] Siten esimerkiksi Facebook, Instagram, Whatsapp, YouTube, Google, Snapchat ja Twitter ovat palveluja, joiden tulee noudattaa tietosuoja-asetuksen sääntelyä. Sama koskee myös erilaisia internetin kauppa- ja keskustelupaikkoja, kuten tori.fi, nettiauto.com, huuto.net, Amazon, Suomi24.fi ja vauva.fi.[446] On yleisesti tiedossa, että tietoverkoissa mahdollisuus esiintyä anonyyminä on selvästi reaalimaailmaa helpompaa. Tämän takia useimpien palvelujen muodostamia rekistereitä ei voida pitää julkisesti luotettavina. Tämän takia ne eivät yleensä täytä Poliisihallituksen määräyksen mukaista määritelmää julkisesti luotettavasta rekisteristä.[447] Poliisihallituksen määräyksen linjausta vain viranomaisen ja julkista luotettavuutta omaavaan rekisteriin voidaan kuitenkin pitää perus- ja ihmisoikeussuojamyönteisen tulkinnan kannalta ongelmallisena, koska sillä rajataan tietoverkkoja koskevat palvelut pois rekisterin määritelmästä ja siten muutetaan päätöksentekijätasoa alemmaksi.[448] Jos sosiaalisen median palvelut tulkitaan suojaamissääntelyn mukaisiksi rekistereiksi, tulisi päätös peiteprofiilin luomisesta tehdä PolL 5:47.1:n tai PKL 10:48.1:n mukaisesti aina keskusrikospoliisin tai suojelupoliisin päällikön toimesta. Poliisihallituksen tulkinnalla päätöksentekijätaso alennetaan vastaamaan pelkkää väärää, peiteltyä ja harhauttavaa koskevaa tietoa, jonka osalta päätöksen tekee STEKPOV.

Asiaan kiinnitettiin huomiota jo komiteamietintöä koskevassa lausuntotiivistelmässä, jossa keskusrikospoliisi tuo esille päätöksentekijätason porrastamistarpeen viranomaisen sekä yksityisen rekisterien ja asiakirjojen välillä.[449] Lausunnossaan keskusrikospoliisi kritisoi eron tekemättä jättämistä PKL 10:46:ssä, koska viranomaisen ylläpitämä rekisteri ja sen myöntämät asiakirjat nauttivat huomattavasti suurempaa luottamusta kuin yksityisen ylläpitämät rekisterit. Keskusrikospoliisi ehdottikin, että viranomaisen rekisterien kohdalla

[445] Myös aikaisemman henkilötietoja koskevan lainsäädännön aikana sosiaalisen median palvelut olivat osittain sääntelyn piirissä. Ks. tästä tarkemmin Pesonen 2013, s. 75–78.
[446] Tietosuoja-asetuksen 3 artiklassa säännellään siitä, että samoja sääntöjä sovelletaan kaikkiin rekisterinpitäjiin, jotka tarjoavat palveluja EU:n sisällä, mutta myös niihin, jotka ovat sijoittuneet EU:n ulkopuolelle ja tarjoavat palveluja EU:n sisällä.
[447] Ks. julkisesti luotettavien rekisterien suhteesta tietoverkoissa olevaan tietoon Pitkänen – Tiilikka – Warma 2013, s. 93.
[448] Päätöksentekijätaso on yhteydessä perus- ja ihmisoikeuksiin. Ks. tarkemmin HE 224/2010 vp, s. 51–53; HE 222/2010 vp, s. 136–137.
[449] Sisäministeriö 2009b, s. 182.

päätöksen voisi tehdä poliisiyksikön päällikkö ja yksityisen rekisterin osalta tietty päällystöön kuuluva poliisimies.[450] Tämä olisi myös ollut osittain linjassa vanhan lain aikana voimassa olleen ja salaisia tiedonhankinta- ja pakkokeinoja koskevan määräyksen kanssa.[451]

> Aikaisemmin voimassa olleeseen ja salassa pidettävään määräykseen on viitattu vanhemmissa salaisia tiedonhankinta- ja pakkokeinoja koskevissa vuosikertomuksissa ja niiden osalta tiedonhankintamenetelmien suojaukset on jaettu kolmeen eri suojausluokkaan, joita kaikkia koski erilliset menettelyprosessit. Suojausluokkia olivat: I) Viranomaisen ylläpitämään rekisteriin tehtävä harhauttava tai peitelty rekisterimerkintä ja viranomaisen antaman väärän asiakirjan (tms.) valmistaminen, joista päättää keskusrikospoliisin tai suojelupoliisin päällikkö, II) muuhun kuin viranomaisen ylläpitämään rekisteriin tehtävä harhauttava tai peitelty rekisterimerkintä ja muun kuin viranomaisen antaman väärän asiakirjan valmistaminen, joista päättää poliisilaitoksen päällikkö tai hänen määräämänsä ja III) muu harhauttava tai peitelty tieto, joista päättää poliisipäällikön nimeämä tiedonhankinnan suojauksesta vastaava päällystöön kuuluva poliisimies.[452]

Esitöistä tai valiokuntien lausunnoista ei käy ilmi, että suojaamissääntelyn päätöksentekijätasosta olisi käyty keskustelua. On myös todennäköistä, ettei lainsäätäjä ole ottanut huomioon peiteprofiilien osuutta lainvalmistelussa lainkaan. *De lege ferenda* rekisterin määritelmää ja päätöksentekijätasoa tulisikin tarkentaa keskusrikospoliisin ehdotuksen suuntaan. Perus- ja ihmisoikeusnäkökulman kannalta perusteltu vaihtoehto olisi, että rekisteriä koskeva suojaamissääntely koskisi vain viranomaisen ylläpitämiä rekistereitä ja yksityisten rekisterien osalta kyse olisi väärän, peitellyn tai harhauttavan tiedon käytöstä. Tätä tulkintaa voidaan katsoa tukevan rikoslain 16 luvun 7 §:n sääntely rekisterimerkintärikoksesta, jolla suojataan vain viranomaisen ylläpitämiä yleisiä rekistereitä. Lisäksi tietoverkkojen kohdalla kyse on yleisesti vähäistä luottamusta nauttivista henkilörekistereistä.[453] Lisäksi voidaan mainita, että väärien rekisterimerkintöjen

[450] Keskusrikospoliisi 2009, s. 46.
[451] Kyseinen määräys oli salassa pidettävä, joten siihen ei voida viitata suoraan. Kyseinen luokittelu oli kuitenkin otettu salaisia tiedonhankinta- ja pakkokeinoja koskevaan vuosikertomukseen.
[452] Poliisihallitus 2011, s. 37.
[453] Pelkkä peiteprofiilin tekeminen sosiaalisen median palveluun ilman rekisterinpitäjän lupaa ei ole rikos. Lisäksi profiilin poistaminen palvelusta ei vaadi yhteistyötä rekisterinpitäjän kanssa, vaan profiilin saa helposti itse poistettua. Viranomaisten ylläpitämien rekisterien osalta kyseeseen tulee rekisterimerkintärikos (RL 16:7) ja asiakirjojen osalta voi tulla kyseeseen esimerkiksi väärennys (RL 33:1) tai laittoman maahantulon järjestäminen (RL 17:8).

tekeminen ja oikaisu yhteistyössä EPSA 3:20.1:n mukaisesti ulkomailla sijaitsevien sosiaalisen median palvelujen yritysten kanssa olisi haastavaa.[454]

*Asiakirjojen* valmistus ja käyttäminen ovat tiiviisti yhteydessä rekistereitä koskeviin suojaamistoimenpiteisiin, koska asiakirjat luodaan yleensä vääriin rekisterimerkintöihin liittyen. Tämä käy ilmi poliisihallituksen määräyksestä, jossa asiakirjojen valmistus kytketään viranomaisten ylläpitämiin ja julkista luotettavuutta nauttiviin rekistereihin.[455] Tähän liittyy osaltaan myös se, että päätöksen rekisterimerkinnöistä ja asiakirjojen valmistamisesta tekee PolL 5:47.1:n tai PKL 10:48.1:n mukaisesti keskusrikospoliisin tai suojelupoliisin päällikkö, kun taas asiakirjojen käytöstä voi päättää STEKPOV. Peitetoimintaa koskevissa esitöissä mahdollisina rekistereitä koskevina muutoksina mainittiin passi-, ajokortti ja väestötietojärjestelmän muutokset. Mukana oli myös ajoneuvojen sekä omaisuuden omistaja- ja haltijatiedot.[456] Tällä perusteella yleisiä suojaamissääntelyn perusteella valmistettavia asiakirjoja olisivat erityisesti passilain (671/2006) mukainen passi[457], henkilökorttilain (663/2016) mukainen henkilökortti[458], ajokorttilain (386/2011) mukainen ajokortti sekä ulkomaalaislain (301/2004) mukainen oleskelulupakortti. Omistaja- ja haltijatiedot voivat liittyä ajoneuvojen omistajatietoihin, jolloin asiakirja voi olla esimerkiksi rekisteröintitodistus, joka on nykyään lähinnä sähköinen.[459] Asiakirjan määritelmä ei siis rajaa ulkopuolelle sähköisiä asiakirjoja.[460] Niin kuin rekistereitä käsiteltäessä on jo käyty läpi, ei lainsäädännössä tai sen esitöissä oteta kantaa rekisterien julkiseen luotettavuuteen. Sama koskee myös asiakirjan määritelmää, joten teoriassa se voisi olla millainen asiakirja tahansa. Myös asiakirjan kohdalla sääntelyä tulisi tarkistaa viranomaisen ja yksityisen tahon myöntämän asiakirjan välillä rekisterien määritelmän tapaan. Tietoverkoissa väärien asiakirjojen valmistamisella ja käyttämisellä ei ole kovinkaan suurta merkitystä. Toisaalta myös tietoverkkojen kautta voi esittää erilaisia

---

[454] Esimerkiksi Facebook on ilmoittanut poistavansa havaitsemansa sääntöjen vastaiset profiilit, vaikka niiden tekijä olisi virkatehtävässä toimiva poliisi. Ks. esimerkiksi NBC News 2018. Peitetoimintaa koskevissa alkuperäisissä esitöissä todettiin, että poliisitoiminnan paljastumisen ja paljastumisen aiheuttamien ilmeisten vaarojen vuoksi ei ole aina mahdollista, että rekisterinpitäjälle tiedotettaisiin peiterekisteröinnistä. Ks. HE 34/1999 vp, s. 27. Tätä tosin rajoittaa nykyään EPSA 3:20.1:n mukainen velvoite.

[455] Poliisihallitus 2018a, s. 7–8.

[456] HE 34/1999 vp, s. 27.

[457] Varsinaisen passin lisäksi kyseeseen voi tulla myös merimiespassi, diplomaattipassi, virkapassi ja varsinaisen passin erilaiset väliaikaiset muodot.

[458] Henkilökorttilaissa säädetään myös ulkomaalaisen ja alaikäisen henkilökortista sekä väliaikaisesta henkilökortista.

[459] Muuta omaisuutta koskeva asiakirja voi olla esimerkiksi kiinteistön omistusta osoittava lainhuutotodistus.

[460] Ks. viranomaisen sähköisistä asiakirjoista tarkemmin Voutilainen 2012, s. 90–91.

asiakirjoja peitetoiminnan sekä valeostojen yhteydessä, jotta toisen osapuolen luottamus saavutetaan paremmin.[461]

Väärät, harhauttavat tai peitellyt *tiedot* pitävät sisällään laajan joukon erilaisia mahdollisuuksia suojata poliisimiestä ja poliisin toimintaa. Peitetoimintaa koskevissa esitöissä on mainittu esimerkkeinä tilanteet, joissa poliisi esiintyy autonkuljettajana, putkimiehenä, isännöitsijänä tai tarjoilijana.[462] Tällöin poliisilla voi olla vaatteissa ja ajoneuvoissa kyseiseen toimintaan viittaavia tietoja. Varsinaista suojaamissäännöstä koskevissa esitöissä 266/2004 vp mainittiin tarkkailutoimintaan ja suojaamistietoihin liittyen, että ensisijaisesti kyse on välineistön suojaamisesta, mutta jossain tilanteissa saattaa myös muodostua tarve suojata tehtävää suorittavaa poliisimiestä.[463] Nykyisen poliisi- ja pakkokeinolain esitöissä peiteltyä tiedonhankintaa koskevassa osiossa suojaamisesimerkkeinä mainittiin kuljetustoimintaa harjoittavan yhtiön haalareiden ja nimikylttien käyttäminen.[464] Jos poliisi käyttää salaisessa tiedonhankinnassa normaalia siviilivaatetusta, ei tätä ole lähtökohtaisesti tulkittu PolL 5:46:n ja PKL 10:47:n mukaiseksi väärien, peiteltyjen tai peiteltyjen tietojen käyttämisenä.[465] Sama tulkinta koskee myös poliisilaitoksen omistamia siviilimallisia ajoneuvoja, mutta myös leasing-ajoneuvoja, joita ei pysty jäljittämään suoraan Trafin tietokannasta poliisilaitoksen ajoneuvoiksi.[466] Kyseinen toiminta on verrattavissa tavanomaiseen kansalaisen toimintaan.[467]

Väärien, harhauttavien ja peiteltyjen tietojen käyttöä tietoverkoissa ei ole avattu lainvalmisteluaineistossa lainkaan. Peitetoimintaa koskevissa esitöissä tosin viitattiin jo vuonna 1999 tekniseen kehitykseen, jonka takia ei ole mahdollista ennalta määritellä, minkälaisia harhaanjohtavia tai puutteellisia tietoja on paljastumisen estämiseksi

---

[461] Esimerkkinä voidaan mainita tilanne, jossa toinen osapuoli pyytää syystä tai toisesta varmistamaan henkilöllisyyden esimerkiksi lähettämällä kuvan henkilökortista tai muusta vastaavasta tunnistamisasiakirjasta. Mainittakoon kuitenkin tässä yhteydessä, että esitöiden mukaan valeostossa käytettäviä suojaamissääntelyyn perustuvia rekisterimerkintöjä tai asiakirjoja ei ole tarkoitettu käytettäväksi peitetoiminnan tapaan, vaan ainoastaan sellaisissa yksittäisissä tilanteissa, joissa valeostajan turvallisuus ja valeoston paljastumisen estäminen välttämättömästi edellyttävät suojaamisen käyttämistä. Ks. HE 224/2010 vp, s. 55; HE 222/2010 vp, s. 139

[462] HE 34/1999 vp, s. 26.

[463] HE 266/2004 vp, s. 31–32.

[464] HE 224/2010 vp, s. 104; HE 222/2010 vp, s. 327.

[465] Raja suojaamissäännöksen osalta voi tulla vastaan pukeutumisen osalta tilanteessa, jossa poliisimies osallistuu mielenosoitukseen ja kantaa jonkin tietyn ryhmittymän tunnuksia vaatteissaan.

[466] Ks. Poliisihallitus 2017c, s. 5. Jos leasing-sopimuksessa on käytetty jotain muita kuin poliisilaitoksen tietoja, siirrytään PolL 5:46:n ja PKL 10:47:n sääntelyn piiriin.

[467] Tulee myös huomioida, että kyseessä ei ole lähtökohtaisesti toimivaltasäännös, vaan tarkoituksena on salata toimivaltuuksien käyttö. Ks. HE 266/2004 vp, s. 31.

välttämätöntä antaa.[468] Suojaamiskeinon käyttäminen on lähtökohtaisesti helpommin toteutettavissa kuin reaalimaailman puolella, koska erilaisia paljastumisen estäviä tietoja on helpompi luoda tietoverkkoihin. Jotta poliisimies pystyy luomaan palveluun profiilin, tulee tätä varten luonnollisesti hankkia telepäätelaite, jolla saa internet-yhteyden. Käytännössä kyseessä on tietokone tai älylaite, joiden hankkimisessa ei ole tarvetta soveltaa suojaamissääntelyä.[469] Telepäätelaitteen lisäksi poliisimiehen tulee hankkia tietoliikenteen mahdollistava liittymä (teleosoite), jolla saa yhteyden internetiin. Jos poliisi hankkii tekaistuilla tiedoilla liittymän, ollaan jo lähellä väärän rekisterimerkinnän tekemistä, koska asiakastieto tallennetaan operaattorin rekistereihin. Poliisilla on tosin mahdollisuus käyttää prepaid-puhelinliittymää siinä missä kansalaisillakin, joka mahdollistaa suhteellisen anonyymin yhteyden.[470] Katson tämän rinnastuvan leasing-auton käyttöön, eikä itse prepaid-liittymän hankkiminen ole siten suojaamissääntelyn piiriin kuuluva asia. Tietoverkoissa poliisin on mahdollista luoda peiteprofiileja useisiin eri palveluihin, joissa sisäänkirjautumiseen vaadittavat tiedot vaihtelevat. Esimerkiksi Google-tilin luomiseen ja siten gmail-sähköpostiosoitteen käyttöön ei tarvitse ilmoittaa kuin nimi ja keksiä käyttäjätunnus sekä salasana. Käyttäjätunnus määrittää sähköpostiosoitteen alkuosan ja voi olla mikä tahansa käyttäjän valitsema yhdistelmä kirjaimia, numeroita ja pisteitä. Google tai yleensä mikään muukaan sosiaalisen median palvelu ei varmista kirjautujan henkilöllisyyttä. Jos poliisimies kirjautuu erilaisiin sosiaalisen median palveluihin, voidaan kirjautumiseen käyttää myös pelkkää sähköpostiosoitetta, eikä erillistä puhelinnumeroa tarvita.[471] Palveluissa voidaan esiintyä nimellä, mutta yleisiä ovat myös erilaiset nimimerkit. Tällaisia yleensä nimimerkillä käytettäviä palveluita ovat esimerkiksi Instagram ja Snapchat, kun taas Facebook vaatii kirjautumaan palveluun nimellä jota henkilö ”käyttää arkielämässä”.

---

[468] HE 34/1999 vp, s. 26–28. Tämän osalta sääntelyn voidaan todeta olevan teknologianeutraalia, jossa tietoverkkoihinkin liittyvä kehitys on otettu sinänsä huomioon, vaikka uudemmissa esitöissä asian käsittely on sivuutettu.

[469] Tietokone voi olla pöytätietokone tai kannettava tietokone. Älylaitteena taas pidetään yleensä tietoliikenneyhteyden mahdollistavaa matkapuhelinta tai tablettia. Mahdollista on myös muuttaa telepäätelaitteen IMEI-koodia. Ks. suojaamissääntelyn tarpeesta tähän liittyen KKO 2012:54, jossa oli kyse IMEI-koodin väärentämisestä Flasher box -laitteella.

[470] Prepaid-liittymien käytön anonyymiys siinä missä internetinkin anonyymi käyttö on herättänyt huolta päättäjissä. Ks. esimerkiksi KK 33/2007 vp, KK 172/2007 vp, KK 557/2007 vp ja KK 353/2012 vp, joissa on vaadittu toimenpiteitä prepaid-liittymillä tapahtuvan anonyymin toiminnan lopettamiseksi erityisesti häiriköintitilanteissa. Ks. myös KK 262/2016 vp, jossa taas tietyllä tapaa paradoksaalisesti prepaid-liittymille haluttiin laajempaa mahdollisuutta mobiilitunnistautumiselle viranomaispalveluihin.

[471] Osaan palveluista voidaan kirjautua myös jo olemassa olevalla sosiaalisen median palvelun käyttäjätilillä. Tällainen on esimerkiksi Uuden Suomen Puheenvuoro-palsta, johon voi kirjautua Facebookin tai Googlen käyttäjätilillä. Puheenvuoron blogit ja kommentit tosin näkyvät muutoinkin, joten rekisteröinti ei ole tarpeen.

Käytännössä sosiaalisen median palvelulle pystyy valehtelemaan helposti esimerkiksi nimensä, ikänsä ja muut tietonsa.[472]

Näkyvässä poliisitoiminnassa poliisi esiintyy sosiaalisessa mediassa yleensä omalla nimellä ja omilla kasvoilla.[473] Peitetoiminnassa tilanne ei luonnollisesti ole näin, vaan poliisin tarkoituksena on häivyttää yhteys poliisiin mahdollisimman kauas. Poliisin tietoverkoissa mahdolliset peiteprofiilit voidaan jakaa karkeasti 1) kevyen peitteen peiteprofiileihin ja 2) vahvan peitteen peiteprofiileihin.[474] Tarkkailutyylisiä keinoja varten peiteprofiilin kuviin, ulkoasuun tai muihin tietoihin ei juurikaan tarvitse kiinnittää huomiota, koska tarkoituksena ei ole paljastua tiedonhankinnan kohteelle.[475] Yleensä tällaisetkaan profiilit eivät kiinnitä käyttäjien erityistä huomiota, vaikka käynnistä kohdehenkilön profiilin jäisi jonkinlainen tieto, koska anonyymi esiintyminen ja toisten profiilien selailu on tyypillistä sosiaalisessa mediassa.[476] Kevyt peite on rinnastettavissa poliisimiehen toimimiseen siviilivaatetuksessa ja leasing-ajoneuvon käyttöön, jossa ei vielä sovelleta suojaamissääntelyä. Toisaalta esimerkiksi TOR-verkossa voi luoda uskottavan profiilin keskustelupalstalle hyvin vähäisin tiedoin huumausaineisiin liittyvässä valeostossa, koska toimintaympäristöön kuuluu vielä vahvemmin anonyymi luonne kuin sosiaaliseen median yhteisöpalveluissa. Suojaamisen vahvuuden tarve riippuukin siitä, missä ympäristössä ja millaisesta toimivaltuudesta on kyse. Vahvan peitteen osalta tietojen tulee olla siinä määrin vääriä, harhauttavia tai peiteltyjä, että kohde ei tiedä toisena osapuolena olevan poliisi. Erityisesti tämä korostuu tilanteissa, joissa on kyse pidempiaikaisemmasta ja syvällisemmästä vuorovaikutuksesta.[477] Tällöin suuressa

[472] Tietojen valehtelemista palveluille ei ole kriminalisoitu, mutta ne ovat yleensä palvelun omien sääntöjen vastaisia. Vaikka poliisin tekeminen peiteprofiilien osalta sosiaalisen median palveluun tapahtuu lain rajoissa, ei palvelut itse välttämättä halua hyväksyä poliisin peiteprofiileja palveluissa. Ks. tästä esimerkiksi NBC News 2018. Tällöin peiteprofiilien tulkinta rekisterimerkinnöiksi myös vaikeuttaisi huomattavasti peiteprofiilitoimintaa, koska EPSA 3:20:n mukaan merkinnöistä tulisi sopia rekisterinpitäjien kanssa.

[473] Esimerkiksi ensimmäisen näkyvän poliisiprofiilin nimimerkki IRC-Galleriassa oli -fobba-, mutta profiilista löytyi tunnistettavissa oleva kuva ja siitä kävi ilmi virkamiehen oikea nimi. Vrt. virkamiehen velvollisuudesta käyttää virantoimituksessa omaa nimeään esimerkiksi AOA 29.11.2010 Dnro 686/4/09, jossa apulaisoikeusasiamiehen mukaan silloisen Pohjois-Karjalan Prikaatin komentajan tuli käyttää virallista etunimeä Viljo hänen käyttämänsä Ville-nimen sijaan. Omalla nimellä esiintymiseen liittyen SPJL on vaatinut RL 16 lukuun niin sanottua maalittamista rangaistavaksi, johon liittyen poliisilla tulisi olla oikeus esiintyä ilman omaa nimeä ja sen sijaan käytettäisiin numero- tai kirjaintunnisteita. Ks. tarkemmin SPJL 2019, s. 10–15.

[474] Jako ei perustu lakiin tai poliisin määräyksiin, vaan on pelkästään tätä tutkimusta varten luotu jaottelu.

[475] Itse tieto ei kuitenkaan voi olla sellaista, jolla poliisi esimerkiksi syyllistyisi identiteettivarkauteen (RL 38:9a) esiintymällä jonain toisena tunnistettavana henkilönä tai käyttäisin materiaalia, jonka osalta voisi syyllistyä aineettomia oikeuksia koskeviin tekijänoikeus- ja teollisuusoikeusrikoksiin (RL 49:1–2).

[476] Ks. esimerkiksi HE 224/2010 vp, s.116; HE 222/2010 vp, s. 339, jossa tietoverkkojen anonyymin luonteella katsottiin olevan merkitystä peitetoiminnan erityisiin edellytyksiin.

[477] Erityisesti peitetoiminnan kohteella voi esimerkiksi olla kaverilistalle ottamisen takia laajempi katseluoikeus peiteprofiilin sisältöön kuin ulkopuolisella, jolloin kohteelle näkyvät tiedot tulee olla riittävällä tavalla suojattuja.

roolissa ovat myös peiteprofiilin historiatiedot, joilla on suuri merkitys profiilin luotettavuuden arvioinnissa.[478] Tietoverkoissa tapahtuvassa peitetoiminnassa on mahdollisuus käyttää myös edellä käsiteltyjä rekisterimerkintöjä ja asiakirjoja, etenkin jos peitetoimintaa suoritetaan tietoverkkojen lisäksi samanaikaisesti myös reaalimaailmassa.[479]

Vahvaan peitteeseen liittyy olennaisesti kysymys siitä, missä vaiheessa profiili voidaan luoda ja tuleeko tuossa vaiheessa olla jo tieto tulevasta salaisesta tiedonhankinta- ja pakkokeinon käytöstä. Niin kuin on jo todettu, tulee toiminnan olla välttämätöntä jo toteutetun, käynnissä olevan tai tulevaisuudessa toteutettavan salaisen tiedonhankinta- tai pakkokeinon käytön suojaamiseksi (PolL 5:46.2 ja PKL 10:47.2). Uusissa esitöissä viitataan hallituksen esitykseen 266/2004 vp, jossa asiaa käsiteltiin jo aikaisemmin säädetyn peitetoiminnan suojaamiseen liittyen.[480] Vaikka peitetoimintavaltuuteen katsottiin liittyvän mahdollisuus käyttää poliisitaustan häivyttämisen mahdollistamia keinoja rekisterien, asiakirjojen ja tietojen avulla, katsottiin suojaamissäännöksen olevan tarpeellista sisällyttää myös peitetoiminnan suojaaminen. Syyksi mainittiin se, että peitetoiminta tuli nähdä kokonaisuutena, johon sisältyi yksittäiseen juttuun liittyvän toiminnan lisäksi myös sitä ylläpitävää toimintaa. Voimaan tullut suojaamista koskeva lainsäädäntö mahdollisti täten toiminnan suojaamisen muutenkin kuin varsinaisen operatiivisen peitetoiminnan aikana. Siten peitettä käyttävälle henkilölle pystytään luomaan historia- eli taustatieto, joka ei liity yksittäiseen poliisioperaatioon ja joka voi jäädä olemaan myös operaation jälkeen.[481] Tällä toiminnalla mahdollistetaan paitsi peitetoimintaa suorittavan poliisimiehen luonteva soluttautuminen rikollisten keskuuteen, mutta myös hänen turvallinen irtautuminen jutusta.[482] Käytännössä tämä tarkoittaa sitä, että tietoverkkoihin voidaan alkaa luomaan vahvoja peitteitä jo ennen kuin tietty salainen tiedonhankinta- tai pakkokeino on edes tiedossa. Vaikka suoja voidaan rakentaa jo hyvissä ajoin ennen yksittäisen operaation alkamista, ei peiteprofiililla ole mahdollista suorittaa ennen operatiivista vaihetta tai sen jälkeen aktiivista tiettyyn toimivaltuuteen perustuvaa tiedonhankintaa.[483] Tietoverkoissa toiminta kuitenkin eroaa reaalimaailman operatiivisesta toiminnasta siten, että tiedot ovat

[478] Ks. valeprofiilin tunnistamisesta tarkemmin Forss 2014, s. 103–104.
[479] Kyseeseen voisi tulla esimerkiksi terroristiverkostoon soluttautuva poliisi, joka pyrkii tapaamaan kohteita kasvotusten, mutta myös sosiaalisen median kanavia käyttäen. Tätä tarkoitusta varten hänelle on voitu luoda henkilöllisyys viranomaisen rekistereihin, vääriä tietoja sisältäviä asiakirjoja, mutta myös profiili sosiaalisen mediaan.
[480] HE 224/2010 vp, s. 55; HE 222/2010 vp, s. 139.
[481] Myös rekisterimerkinnän oikaisun osalta viitattiin tähän ja todettiin, että oikaisu voidaan tehdä esimerkiksi vasta siinä tilanteessa, kun poliisimies ei enää toimi näissä tehtävissä. Ks. HE 266/2004 vp, s. 34.
[482] HE 266/2004 vp, s. 31. Rekisterimerkintöjen lisäksi peitteen ylläpitäminen koskee myös asiakirjoja. Ks. HE 266/2004 vp, s. 32.
[483] Ks. HE 266/2004 vp, s. 31–32.

globaalisti ja jatkuvasti saatavilla. Tämän takia peiteprofiililla tulee olla tavalla tai toisella aktiivinen myös operatiivisen vaiheen ulkopuolella, jotta sen uskottavuus säilyisi. Tämä taas vaikeuttaa oleellisesti profiilin uskottavuuden, eli ”legendan rakentamista”.[484]

## 6.2 Peiteprofiilien luomismahdollisuudet yleisvalvontaa ja tarkkailua varten

Peiteprofiilin luominen perustuu lähtökohtaisesti PolL 5:46.2:n ja PKL 10:47.2:n suojaamissääntelyyn, joka on mahdollista vain silloin, kun se on välttämätöntä jo toteutetun, käynnissä olevan tai tulevaisuudessa toteutettavan salaisen tiedonhankinta- tai pakkokeinon käytön suojaamiseksi. Esitöissä on yleisellä tasolla huomioitu yleisvalvonta ja tarkkailu tietoverkoissa, mutta ei tarkasteltu asiaa suojaamissääntelyn näkökulmasta.[485] On kuitenkin selvää, että poliisilla tulee olla mahdollisuus reaalimaailman tapaan suorittaa yleisvalvontaa ja tarkkailua ”ilman virkapukua” myös tietoverkoissa. Yleisvalvontaa tai tarkkailua ei ole mainittu PolL 5:1.1:n tai PKL 10:1.1:n toimivaltuusluetteloissa, joten herää kysymys voiko niissä soveltaa suojaamissääntelyä. Yleisvalvonnan kohdalla tilanne on selvä, kyseessä ei ole toimivaltuus, eikä suojaamissääntelyä voida soveltaa.[486] Tarkkailun osalta kysymys on kuitenkin haastavampi ja on herättänyt epätietoisuutta myös lainsoveltajien keskuudessa.[487]

Poliisi- ja pakkokeinolaissa tarkkailulla tarkoitetaan tiettyyn henkilöön salaa kohdistettavaa havaintojen tekemistä tiedonhankintatarkoituksessa (PolL 5:13.1 ja PKL 10:12.1). Esitöiden mukaan tarkkailun määritelmällä on välineellistä merkitystä useiden salaisten tiedonhankinta- ja pakkokeinojen määritelmien kannalta. Erityisesti mainitaan erilaiset teknisen tarkkailun muodot. Kyseisenlaisen hetkellisen havaintojen tekemisen ei katsota

---

[484] Ks. ”legendan rakentamiseen” liittyen ETP 2400/R/239/18, s. 129. Esitutkintapöytäkirjasta käy ilmi, että peitetoiminnan kohteena ollut henkilö oli epäillyt kyseessä olevan poliisi esimerkiksi sillä perusteella, ettei peitepoliisin Playstation-pelitilillä ollut saatu niin sanottuja ”trophyjä” miltei kahteen vuoteen. Kyseisiä ”trophyjä”, eli tietynlaisia saavutusmerkintöjä, saadaan pelaamiseen perustuen ja koska peitepoliisin oli luultavasti kertonut pelaavansa paljon, ei tämä sopinut peitepoliisin kertomukseen.

[485] Ks. yleisvalvonnasta keskustelupalstoilla HE 224/2010 vp, s. 34 ja tarkkailun toteuttamisesta tietoverkoissa katselemalla henkilön keskustelupalstalla käymää keskustelua HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.

[486] Ks. yleisvalvonnasta poliisin perustoimintona esimerkiksi Helminen – Kuusimäki – Rantaeskola 2012, s. 388–391. Ks. myös HE 57/1994 vp, s. 57, jossa valvonta määriteltiin ennalta määräämättömään ihmisryhmään kohdistuvaksi seurannaksi. Yleisvalvonnan määritelmää ja sen sisältöä tarkastellaan tässä tutkimuksessa myöhemmin omassa kohdassaan.

[487] Ks. tarkemmin Poliisihallitus 2018c, s. 40, jossa todetaan, että STEKPOV-koulutuspäivillä keskusteltiin ongelmalliseksi koetuista kysymyksistä, joiden perusteella Poliisihallitus laati asiasta kirjeen poliisiyksiköille. Ks. kyseisestä kirjeestä Poliisihallitus 2017c, s. 1, jossa esitetään kysymykset suojaamissäännökset soveltumisesta yleisvalvontaan ja tarkkailuun.

edellyttävän toimivaltuussääntelyä.[488] Lisäksi tarkkailua kuvataan eräänlaiseksi poliisin keinovalikoimaan kuuluvaksi perustoimenpiteeksi, jonka takia sen edellytyksistä ei ole tarpeen säätää erikseen.[489] Lakivaliokunnan pakkokeinolakia koskevassa mietinnössä 44/2010 vp pitäydyttiin hallituksen esityksen kannassa ja todettiin, että valiokunnan käsityksen mukaan kyse ei ole toimivaltuussäännöksestä vaan määritelmäsäännöksestä, joka on otettu pykälään apukäsitteeksi ennen kaikkea tarkentamaan ehdotetun suunnitelmallisen tarkkailun määrittelyä.[490] Toisaalta tilannetta sekoittaa se, että pöytäkirjaamista koskevissa säännöksissä PolL 5:59 ja PKL 10:61 todetaan: ”Muun salaisen tiedonhankintakeinon kuin tarkkailun käytön lopettamisen jälkeen on laadittava ilman aiheetonta viivytystä pöytäkirja”. Säännöksestä saa kuvan, että tarkkailu on salainen tiedonhankinta- tai pakkokeino, mutta siitä ei muista toimivaltuuksista poiketen tarvitse laatia pöytäkirjaa. Esitöiden mukaan tarkkailusta olisi kuitenkin tarvittaessa tehtävä merkintä muuhun asiakirjaan, esimerkiksi tehtävänsuorituslomakkeeseen.[491]

Oikeuskirjallisuudessa on hyväksytty esitöiden käsitys tarkkailusta määritelmäsäännöksenä, mutta myös poikkeavia näkökulmia löytyy.[492] Tarkkailun on katsottu olevan toimivaltuussäännös erityisesti sillä perusteella, että siinä saadaan käyttää kameraa ja muita teknisiä laitteita, joiden käyttäminen olisi muutoin rangaistavaa.[493] Onkin epäselvää, miksi lainsäätäjä ei ole pitänyt tarkkailua tällä perustella toimivaltuutena, koska ilman nimenomaista toimivaltuussäännöstä kyseeseen voisi tulla salakatselu (RL 24:6), joka on vielä erikseen tarkkailun määritelmäsäännöksessä mainittu (PolL 5:13,1 ja PKL 10.12,1).[494] Kyseinen muutoin rangaistavan teon oikeuttamisperuste tarkkailusäännöksessä puoltaa vahvasti toimivaltuussäännösmäistä luonnetta. Toimivaltuusnäkökulmaa puoltavana

[488] HE 224/2010 vp, s. 34; HE 222/2010 vp, s.117.
[489] HE 224/2010 vp, s. 177. Ennen vuoden 2014 lakimuutosta, tarkkailusta ei oltu säädetty pakkokeinolaissa lainkaan, vaan esitutkinnan aikana tarkkailu oli sallittua tavanomaisen oikeuden nojalla.
[490] LaVM 44/2010 vp, s. 26.
[491] HE 224/2010 vp, s. 139; HE 222/2010 vp, s. 363.
[492] Ks. Helminen – Kuusimäki – Rantaeskola 2012, s. 392, jossa PolL 5:13.1:n mukaisen tarkkailun todetaan olevan vain määritelmä, eikä toimivaltuussäännös.
[493] Metsäranta 2015, s. 172–173; Helminen ym. 2014, s. 1152. Vrt. kuitenkin saman teoksen Helminen ym. 2014, s. 1117, jossa viitataan lakivaliokunnan mietintöön ja todetaan tulkinta siitä, että tarkkailu ei ole salainen pakkokeino. Ks. kriminalisointien vaikutuksesta toimivaltanormien tulkintaan Terenius 2013, s. 284–322 siinä mainittuine esitöineen. Ks. myös PeVL 5/1999 vp, s. 5, jossa todetaan erityisten salaisten tiedonhankinta- ja pakkokeinoja luonnehditaan sellaisiksi, että ne merkitsevät poliisin oikeutta toimia vastoin jotain rikosoikeudellisia kieltoja ilman virkavastuuta.
[494] Ks. poliisin oikeudesta kuvata ja hankkia tietoa haalarikameralla Poliisihallitus 2017d, s. 12–14. Kyseisen loppuraportin mukaan jo näkyvästi poliisina tapahtuvassa yleisvalvontatyyppisessä kuvaamisessa tulisi käyttää harkintaa ja ottaa korostuneesti huomioon millä edellytyksillä ja mihin tarkoitukseen laitetta käytetään. Kuvaaminen voi muuttua yksityiselämän suojaan puuttuvaksi, jos kuvaamisen ajallinen kesto kasvaa, valvonta kohdistuu selkeästi yksittäiseen henkilöön, eikä poliisilla ole toimivaltaperusteista tehtävään, johon tiedonhankinta kiinteästi liittyy. Lisäksi merkitystä katsotaan olevan myös sillä, jos laitteella pystytään tallentamaan havaintoja, joita laitteen käyttäjä ei voi havaita normaalein näkö- tai kuuloaistein.

seikkana voidaan pitää myös sitä, että vaikka tarkkailu on vain lyhytaikaista toimintaa, voi jo sen yhteydessä kertyä poliisin tietojärjestelmiin kohteesta tallennettavaa tietoa.[495] Erityisesti siinä tapauksessa, että hyväksytään myöhemmin tarkemmin käsiteltävä Poliisihallituksen kanta viiden eri tarkkailukerran tai vähintään vuorokauden yhtämittaisesti jatkuvan tarkkailun rajasta suunnitelmalliseen tarkkailuun verrattuna.[496]

Jos asiaa tarkastelee pelkästään oikeuslähdeopillisesti, on haastavaa tulkita tarkkailun olevan toimivaltuussäännös, koska tarkkailu on jätetty pois PolL 5:1.1:n ja PKL 10:1.1:n luettelosta. Lisäksi esitöissä tarkkailun on nimenomaisesti todettu olevan vain määritelmäsäännös. Oikeuskirjallisuudessa mainittu peruste kameran ja muiden teknisten laitteiden käytön mahdollistamisesta tarkkailussa salakatselun rangaistavuuden poistavana seikkana on kuitenkin jo yksistään perusteena sellainen, että tarkkailua tulisi pitää toimivaltuutena, koska poliisille annetaan oikeus tehdä jotain, joka olisi muutoin rangaistavaa.[497] Tämä ei kuitenkaan päde tietoverkoissa tapahtuvaan tarkkailuun, koska näissä tapauksissa teknisillä laitteilla ei ole merkitystä toimivaltuuden käyttämiselle. Vaikka tietoverkoissa tapahtuvassa tarkkailussa käytetään esimerkiksi tietokonetta tai älypuhelinta, on kyse tähän toimintaympäristöön liittyvästä erityispiirteestä, eikä teknisen laitteen käyttämisestä.[498] Arvioitaessa kysymystä tarkkailun yksityiselämään puuttuvasta luonteesta, on lainsäätäjä nimenomaisesti todennut, että puuttuminen ei ole lyhytaikaisessa toiminnassa niin kattavaa, että se edellyttäisi toimivaltuussääntelyä.[499] Reaalimaailman osalta tilanne on varmasti näin, mutta tietoverkoissa jo lyhytaikaisella tarkkailulla voidaan saada tallennettua suuri määrä tietoa esimerkiksi kohdehenkilö profiilista. Ottaen kuitenkin huomioon tutkimuksessa esitellyt erot yksityiselämän suojaan puuttumisen osalta tietoverkkojen ja reaalimaailman välillä, ei kyseisen seikan voida välttämättä katsoa puoltavan tarkkailun toimivaltuussäännösluonnetta. Lisäksi tallennettua tietoa suojataan kattavasti henkilötietojen käsittelyyn liittyvällä lainsäädännöllä.[500] Kyseisillä perusteilla perusmuotoinen *tarkkailu*

[495] Ks. tiedon keräämisen ja sen tallentamisen vaikutuksesta yksityiselämän suojaan esimerkiksi HE 57/1994 vp, s. 15 ja 56. Ks. myös Helminen – Kuusimäki – Salminen 1999, s. 45. Tähän palataan vielä tarkemmin toimivaltuuksia erikseen käsiteltäessä.

[496] Ks. Poliisihallitus 2017c, s. 4. Ks. myös Sisäministeriö 2009b, s. 61, jossa komiteamietintövaiheessa puhuttiin vielä muutaman kymmenen minuutin ajanjaksosta. Eroon palataan vielä tarkemmin suunnitelmallista tarkkailua toimivaltuutena käsiteltäessä.

[497] Ennen uuden poliisi- ja pakkokeinolain muutosta poliisilaki muutettiin vielä hallituksen esityksiin 16/2013 liittyen vastaamaan pakkokeinolakia. Siinä kameran ja muun teknisen laitteen käyttäminen sidottiin nimenomaan tarkkailuun, eikä pelkästään suunnitelmalliseen tarkkailuun, jonka takia maininta lisättiin ensimmäiseen momenttiin. Ks. HE 16/2013 vp, s. 22.

[498] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.

[499] HE 224/2010 vp, s. 34; HE 222/2010 vp, s.117.

[500] Huomioon voidaan ottaa myös se, että jos poliisi pystyy tallentamaan kerrallaan suuren määrän tietoa henkilöstä tietoverkoista esimerkiksi erilaisia sovelluksia käyttämällä, tulisi tätä ennemminkin arvioida

*tietoverkoissa ei ole toimivaltuussäännös*, vaan pelkkä suunnitelmalliseen tarkkailuun liittyvä määritelmäsäännös.

Poliisihallitus on kuitenkin salaisia tiedonhankinta- ja pakkokeinoja koskevassa määräyksessään todennut, että vaikka tarkkailua ei mainita erikseen salaisten tiedonhankinta- ja pakkokeinojen soveltamisalaan kuuluvana, on se kuitenkin kuulunut aiemman lainsäädännön mukaan keinoihin, joissa voidaan käyttää tiedonhankinnan suojausta. Poliisihallitus katsoi, että esitöiden perusteella ei ole nähtävissä, että lainsäätäjän tarkoituksena olisi ollut rajata perusmuotoista tarkkailua pois. Tällä perusteella Poliisihallitus totesi tarkkailun kuuluvan suojaamissääntelyn piiriin.[501] Olen Poliisihallituksen kanssa samaa mieltä siitä, että lainsäätäjän tarkoitus on tuskin ollut rajata pois suojaamissäätelyä nykyisestä tarkkailusta, koska koko suojaamissäännös on yleensäkin luotu enemmän mahdollistamis- kuin rajoitusmielessä.[502] Perustelu tarkkailun aikaisemmasta sisältymisestä suojaamissääntelyn piiriin ei kuitenkaan ole toimiva, koska vuoden 1995 poliisilain aikaan voimassa ollut tarkkailu vastaa mieluumminkin nykyistä suunnitelmallista tarkkailua (PolL 5:13,2 ja PKL 10.12,2).[503]

Yleisvalvonnasta Poliisihallitus on todennut, ettei poliisi- tai pakkokeinolain mukainen suojaaminen ole mahdollista. Poliisihallitus kuitenkin katsoo, ettei tämä tarkoita suoraan sitä, etteikö poliisi voisi toimia yleisvalvontaa tehdessään anonyyminä ja ilman poliisin tunnuksia. Siten tilanne rinnastuu jossakin määrin reaalimaailmassa tapahtuvaan yleisvalvontaan, jossa poliisi suorittaa valvontaa näkyvästi virkapuvussa tai tilanteen niin vaatiessa siviilivaatetuksessa. Valvonnassa voidaan käyttää niin ikään tunnuksellisia poliisiajoneuvoja tai poliisin käytössä olevia siviilimallisia ajoneuvoja. Siviiliajoneuvot voivat olla joko poliisille rekisteröityjä leasing-ajoneuvoja, joissa jälkimmäisissä virnaomaiskäyttö ei ilmene esimerkiksi Trafin rekisterikyselyssä. Poliisihallituksen näkemyksen mukaan tietoverkossa tapahtuvalla laajempaan joukkoon kohdistuvalla yleisvalvonnalla ei puututa yksittäisen henkilöiden oikeushyviin tai perusoikeuksiin niin,

---

suunnitelmallisena tarkkailua. Tähän palataan myöhemmin toimivaltuuksia käsiteltäessä.

[501] Poliisihallitus 2018a, s. 7. Ks. myös Poliisihallitus 2017c, s. 4.

[502] Ks. HE 266/2004 vp, s. 31, jossa todetaan, että säännöksen tarkoitus ei ole säätää poliisille uusia toimivaltuuksia, vaan sillä pyritään turvaamaan jo olemassa olevien keinojen tehokas käyttäminen niiden erityisluonne huomioon ottaen.

[503] Vuoden 1995 poliisilain 3:28.1,1:n mukaan tarkkailulla tarkoitettiin jatkuvaa tai toistuvaa tiettyyn henkilöön tai hänen toimintaansa kohdistuvaa tiedonhankintaa. Lisäksi esitöissä mainittiin, että yksittäiseen henkilön jatkuva ja suunnitelmallinen tarkkailu kajoaa hänen yksityiselämän suojaansa silloinkin, kun toimenpiteellä ei puututa hänen muihin perusoikeuksiin. Ks. HE 57/1994 vp, s. 60.

että poliisin tulisi esiintyä valvontaa tehdessään aina näkyvillä poliisitunnuksilla.[504] Edellä esitetyn perusteella Poliisihallitus tuleekin siihen tulokseen, että yleisvalvonnassa voi käyttää anonyymejä peiteprofiileja.[505] Suojaamistapaa kirjeessä ei kuitenkaan avata tarkemmin, koska kyseinen osio on salassa pidettävä.[506]

Tietoverkoissa tapahtuvan yleisvalvonnan, mutta Poliisihallituksen kannasta poiketen myös tarkkailun kohdalla voidaan lähteä siitä tulkinnasta, että tietoverkoissa kevyen peitteen ”siviilivaatteisiin pukeutuminen” on tavanomaisoikeuteen perustuvaa poliisin perustoimintaa samaan tapaan kuin poliisin mahdollisuus liikkua siviilivaatteissa tai leasing-ajoneuvolla yleisvalvonta- ja tarkkailutehtävissä reaalimaailman puolella. Edellisessä alaluvussa on käyty läpi eroja kevyen ja vahvan peitteen välillä tietoverkoissa, joiden perusteella voidaan helpommin hahmottaa mahdollisuuksia käyttää peiteprofiilia yleisvalvontaan ja tarkkailuun ilman suojaamissääntelyä. Kevyen peitteen osalta voi olla kyse hyvin vähäisestä määrästä tietoa, jonka perusteella profiili voidaan luoda palveluun. Kyseessä voi olla esimerkiksi nimimerkki ja joku satunnainen kuva, jota ei ole pidettävä yhtään sen harhauttavampana tai peiteltynä kuin siviilivaatteita, prepaid-liittymiä tai leasing-ajoneuvojakaan. Lisäksi tietoverkoissa kevyellä peitteellä toimiminen siviilivaatetukseen rinnastuen on toimintaympäristöön liittyvä erityispiirre.[507] Kyseisellä toiminnalla ei puututa kenenkään oikeusasemaan sillä tavalla, että asiasta tulisi nimenomaisesti säännellä, jonka takia profiilin luominen voidaan perustaa tavanomaiseen oikeuteen.[508] *De lege ferenda* olisi kuitenkin selvempää, jos poliisi- ja pakkokeinolaissa määriteltäisiin suojaussäännös siten, että tietoverkoissa väärien, peiteltyjen ja harhauttavien tietojen käyttö olisi mahdollista yleisvalvonnassa ja tarkkailussa.[509]

[504] Asiassa ratkaisevaa on toiminnallinen tarve ja tämä tulee arvioida tapauskohtaisesti toiminnan tavoitteet huomioiden. Esimerkkinä mainitaan tulossa oleva mielenosoitus, jossa poliisilla on tarve suorittaa tiedonhankintaa tietyillä keskustelupalstoilla, mutta myös pidempiaikainen seuraaminen, joka voi kohdistua vihapuheeseen, radikalisoitumiseen tai muuhun perinteisempään rikolliseen toimintaan viittaavaan keskusteluun.

[505] Poliisihallitus toteaa, että päätöksen tekeminen perustuu puheena olevaan kirjeeseen. Mikäli tiedonhankinta muuttuu tarkkailuksi tai suunnitelmalliseksi tarkkailuksi, tulee tästä tehdä poliisi- tai pakkokeinolain mukainen päätös tiedonhankinnan suojaamisesta.

[506] Poliisihallitus 2017c, s. 4–6.

[507] Ks. HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325, jossa käsitellään teknisen tarkkailun suhdetta tarkkailuun tietoverkoissa. Voidaan myös todeta, että valeprofiilien tekeminen on lisäksi tavanomaista kansalaistenkin kohdalla sosiaalisen median palveluissa, joista löytyy laajasti profiileja eri tarkoitusperin.

[508] Näin myös Terenius 2013, s. 169–170, jossa hän katsoo salanimellä tietoverkossa tapahtuvan toiminnan soveltuvan tavanomaisen oikeuden alaan. Tämän sen takia, että poliisin toiminta ei kohdistu kriminalisointien alueelle eikä toiminnalla juurikaan puututa kenenkään oikeusasemaan. Tulee kuitenkin huomioida, että kyseisenlaisia profiileja ei voida käyttää suunnitelmalliseen tarkkailuun tai muihin toimivaltuuksiin liittyen ilman suojaamissääntelyä.

[509] Tämän osalta päätöksentekovalta voitaisiin antaa STEKPOV:lle, jolla olisi riittävä ymmärrys asiasta. Lisäksi edellytykseksi voitaisiin asettaa jonkinlainen koulutusvaatimus myös kyseistä työtä suorittavalle poliisimiehelle ja ottaa huomioon se, että lähtökohtaisesti kaiken toiminnan tulee perustua esimiesjohdettuun

### 6.3 Peiteprofiililla toimivan velvollisuudet puuttua havaittuihin rikoksiin

Poliisilla on salaista tiedonhankinta- tai pakkokeinoa käyttäessään oikeus siirtää puuttumista rikokseen, jos puuttumisen siirtämisestä ei aiheudu merkittävää vaaraa kenenkään hengelle, terveydelle tai vapaudelle eikä merkittävää huomattavan ympäristö-, omaisuus- tai varallisuusvahingon vaaraa.[510] Lisäedellytyksenä on se, että puuttumisen siirtäminen on välttämätöntä pakkokeinon käytön paljastumisen estämiseksi tai toiminnan tavoitteen turvaamiseksi (PolL 5:46.1 ja PKL 10:47.1).[511] Säännös ei edellytä, että poliisimies itse puuttuu tilanteeseen, vaan hän voi torjua vaaran myös ulkopuolisen avun turvin, jolloin myös esimerkiksi peitetoiminnan käyttäminen pysyy salassa.[512] Todettakoon tässä yhteydessä, että näkyvää poliisiprofiilia käyttävä on velvollinen puuttumaan normaaliin tapaan tietoonsa tulleisiin rikoksiin.[513]

> Rikokseen puuttumatta jättäminen on yhteydessä esitutkintalain 3 luvun 12 §:ään, jossa säädetään esitutkintatoimenpiteiden siirtämisestä.[514] Esitutkinnan siirtämisessä on kuitenkin kyse jo kirjatusta rikosilmoituksesta, joten asia ei lähtökohtaisesti koske peiteprofiililla toimivaa, koska tällöin kyse on yleensä ensikertaa havaittavasta rikoksesta.[515] Peiteprofiileja ei myöskään käytännössä koske ETL 3:9.1:n tarkoitettu toimenpiteistä luopumista koskeva säännös.[516] Toiminnan suojaamista koskevat säännökset PolL 5:46.1 ja PKL 10:47.1 liittyvät myös PolL 1:9:ään, jossa säädetään toimenpiteestä luopumisesta ja sen siirtämismahdollisuuksista.[517] Käytännössä

toimintaan. Lisäksi voidaan mainita jo aikaisemmin esille tuotu tilanne, jossa vahvan peitteen peiteprofiililla voitaisiin suorittaa yleisvalvontaa ja tarkkailua operatiivisen vaiheen ulkopuolella, joka ei kuitenkaan pitäisi olla lähtökohtatilanne yleisvalvonnan ja tarkkailun osalta.

[510] Merkittävää vaaraa aiheuttavien ja kiireellisten tehtävien osalta voidaan viitata myös PolHalL 15 c §:n 3 momenttiin, joka koskee rikoksiin puuttumista vapaa-ajalla. Ks. myös vuoden 1995 poliisilakia koskeva hallituksen esitys 57/1994 vp, s. 38, jonka mukaan velvollisuuden syntymiselle on asetettu edellytykseksi kiireellisyys ja välttämättömyys. Huomioon tulee ottaa rikoksen vakavuuden lisäksi myös teon kohdistuminen suojauskyvyttömään henkilöön, aineelliset vahingot, loukatun oikeustilan palauttamisintressi ja mahdollisuudet estää teosta aiheutuvia toissijaisia vahinkoja. Ks. myös poliisimiehen toimivaltuuksista yleisesti Helminen – Kuusimäki – Rantaeskola 2012, s. 104–106.

[511] Oma merkityksensä on luonnollisesti myös sillä, onko asiassa ylipäätään syytä epäillä rikosta. Ks. syytä epäillä -kynnyksestä tarkemmin HE 222/2010 vp, s. 177–178.

[512] HE 224/2010 vp, s. 130–131 ja HE 222/2010 vp, s. 352.

[513] Ks. esimerkiksi Poliisihallitus 2017b, s. 6.

[514] HE 222/2010 vp, s. 139 ja 190.

[515] Tilanne on verrattavissa poliisin valvontatoimintaan poliisiautolla partioidessa, jossa poliisi havaitsee esimerkiksi akuutin tappelun tai liikennerikoksen.

[516] Tätä tulkintaa tukee esimerkiksi HE 222/2010 vp, s. 185 linjaus, että ratkaisua ei tule tehdä puutteellisen selvityksen perusteella. Pelkkä havainto tietoverkoissa ei ole siten riittävä ja asiaa tulisi selvittää laajemmin, joka taas käytännössä tarkoittaa rikosilmoituksen kirjaamista.

[517] Säännöksessä on myös viittaus PolL 5:46.1:n suojaamissäännökseen.

> toimenpiteistä luopumisen raja on erittäin korkea ja onkin hyvin epätodennäköistä, että tietoverkoissa peitepoliisitoimintaa suorittavan kohdalla voisi tulla kyseeseen toimenpiteistä luopuminen.[518]

Poliisi- tai pakkokeinolaissa ei ole eroteltu tietoverkkoja reaalimaailmasta puuttumisen siirtämistä koskevien PolL 5:46.1:n ja PKL 10:47.1:n osalta, joten lähtökohtaisesti rajaa on pidettävä samana. Puuttumista voidaan siirtää yleensä kaikissa internetissä havaittavissa yleisimmissä sananvapausrikoksissa, koska ne eivät yleensä muodosta merkittävää varaa kenenkään hengelle, terveydelle tai vapaudelle eikä merkittävää huomattavan ympäristö-, omaisuus- tai varallisuusvahingon vaaraa. Peiteprofiililla toimiva olisi kuitenkin velvollinen puuttumaan tavalla tai toisella myöhemmin erityisesti virallisen syytteen alaisiin sananvapausrikoksiin, kuten kiihottaminen kansanryhmää vastaan (RL 11:10).[519] Poikkeuksen voivat muodostaa asianomistajarikokset, joilloin peiteprofiililla toimivan ei välttämättä tarvitsisi siirtää puuttumista, vaan jättää asia kokonaan huomioimatta.[520] Jos peiteprofiililla toimiva poliisi havaitsee esimerkiksi kunnianloukkauksen tunnusmerkistön mukaisen teon sosiaalisessa mediassa, ei tähän tarvitse puuttua, jos asianomistaja on itse ollut mukana keskustelussa ja selkeästi tietoinen mahdollisesta rikoksesta. Tässä tapauksessa rikosilmoituksen tekeminen voidaan jättää asianomistajan omaan harkintaan.[521]

Käytännössä lainsäädäntö vaikuttaa tietoverkoissa osassa tapauksista vähintäänkin haastavalta. Haasteet voidaan jakaa 1) välittömään puuttumiseen ja 2) havaittujen rikosepäilyjen suureen määrään liittyvään problematiikkaan. Selkeimmin *välitöntä puuttumista* vaativana rikoksena internetissä voidaan mainita lapsen seksuaalinen

[518] Toimenpidettä suorittava poliisimies tai toiminnasta päättävä esimies voisivat yksittäistapauksessa harkita, onko toimenpiteestä luovuttava sen aiheuttamien ennakoitavissa olevien seurausten takia. Toimenpiteestä luopuminen edellyttää myös vaihtoehtoisten keinojen puuttumista. Tyyppitapauksena voidaan mainita tilanteet, joissa poliisin toiminta ristiriitatilanteessa saattaisi provosoida laajoja tai vakavia väkivaltaisuuksia. Kyseessä voisi olla myös provokaatiotilanne, jossa ei ole yhteiskunnan edun mukaista, että poliisi toimisi asiassa. Tällöin yleisön luottamus poliisin toimintaan taikka poliisin yleiset toimintamahdollisuudet saattaisivat kärsiä toisarvoisten etujen vuoksi. Ks. HE 57/1994 vp, s. 35.

[519] Käytännössä tämä voisi tarkoittaa sitä, että peiteprofiililla toimiva poliisimiehen tulisi joko toimittaa tieto rikoksesta eteenpäin ja ottaa mahdollisesti myös kuvakaappaukset kyseisestä materiaalista, jottei materiaalia poisteta siihen mennessä kun joko konkreettisesti alkaa selvittelemään asiaa tarkemmin.

[520] Asianomistajarikoksissa esitutkinta saadaan aloittaa ETL 3:4.2:n mukaisesti, vaikkei rangaistusvaatimusta olekaan tehty, jos asianomistaja ei ilmeisesti vielä tiedä rikoksesta eikä tutkintaa voida siirtää rikoksen selvittämistä vaarantamatta. Tutkinnan aloittamisesta olisi tällöin viipymättä ilmoitettava asianomistajalle, mutta tutkinta lopetettava, jos asianomistajalla ei ole asiassa rangaistusvaatimusta.

[521] Jos kyseinen teko tapahtuu ilman asianomistajan tietoisuutta, tulisi asiaan puuttua tai siirtää puuttumista. Oma erityisryhmänsä ovat myös ETL 3:4.3:n tapaukset, joissa syyttäjällä voi olla oikeus nostaa syyte asianomistajarikoksessa, vaikka asianomistajalla ei olekaan asiassa vaatimuksia. Näitä ovat esimerkiksi rikoslain 24 luvun kunnianloukkaus ja yksityiselämää loukkaava tiedon levittäminen, jos teko on tapahtunut julkisesti internetissä. Lähtökohta kuitenkin on, että myös näissä tapauksissa asianomistaja tekee itse rikosilmoituksen.

hyväksikäyttö (RL 20:6). Kyse voi olla esimerkiksi tilanteesta, jossa peiteprofiili saa tiedon tulevasta lapsen seksuaalisesta hyväksikäytöstä, joka mahdollisesti striimataan tietoverkossa.[522] Toisena esimerkkinä voidaan mainita törkeä henkeen tai terveyteen kohdistuvan rikoksen valmistelu (RL 21:6a), jossa teko etenee tilanteeseen, jossa on jo kyse merkittävän vaaran aiheutumisesta jonkun hengelle, terveydelle tai vapaudelle. Esimerkiksi ratkaisussa Helsingin KO 22.3.2019 R 19/1572, oli kyse törkeän henkeen tai terveyteen kohdistuvan rikoksen valmistelusta, jonka esitutkinnassa oli käytetty peiteprofiilia. Tuomittu oli syytteen mukaan suunnitellut aseliikkeeseen menemistä, aseiden anastamista, liikkeen myyjien tappamista ja sen jälkeen yleisesti ihmisten tappamista kyseisillä aseilla.[523] Jos tilanne olisi johtanut suunnitellun teon suorittamisen aloittamiseen, olisi poliisin tullut puuttua tilanteeseen.

*Rikosepäilyjen suureen määrään* liittyvästä problematiikasta voidaan mainita esimerkkinä tilanne, jossa kyse on valeostoja darknetissä suorittavasta poliisimiehestä. Valeostoja peiteprofiililla toimivan tietoon voi tulla useita tietyllä kauppapaikalla huumeita tarjoavia profiileja, jolloin puuttumisen siirtäminen tulee sinänsä kyseeseen.[524] Säännös ei kuitenkaan mahdollista kuin siirtämisen, joten käytännössä poliisin tulisi reagoida tilanteeseen esimerkiksi kirjaamalla asiasta rikosilmoitus. Ei ole kuitenkaan tarkoituksenmukaista kirjata rikosilmoitusta kaikista kauppapaikalta löytyvistä myyntitarjouksista, jos näitä ei pystyä alkaa heti selvittämään valeoston keinoin. Jos kaikista kymmenistä myynti-ilmoituksista kirjattaisiin rikosilmoitus huumausainerikoksesta, tutkinta vain myöhemmin keskeytettäisiin, koska tekijän selvittäminen ei olisi muutoin mahdollista. Oli kyseessä välittömään tai suureen määrään puuttumisen problematiikasta, on poliisin mahdotonta pysäyttää tai selvittää mahdollista rikosta, jos kohteen henkilöllisyys ja tapahtumapaikka ei ole tiedossa. Siten poliisi voi olla reaalimaailmaa useammin siinä tilanteessa, että uhkiin tai rikoksiin ei pystytä tosiasiallisesti puuttumaan.

---

[522] Ks. esimerkiksi Keskusrikospoliisi 2019. Tiedotteessa kerrotaan esitutkinnasta, jossa lapsiin oli kohdistettu useita erilaisia törkeitä seksuaalirikoksia. Osa hyväksikäyttötilanteista oli kuvattu niin sanottuihin livelähetyksiin, jossa hyväksikäyttöä oli pystynyt seuraamaan reaaliajassa tietoverkon välityksellä. Ks. tähän osittain liittyvästä webkamera-seksiturismi-ilmiöstä tarkemmin Forss 2014, s. 137–139.Esimerkiksi pelkkä RL 17:18:n mukainen sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan levittäminen olisi rikos, johon puuttumista voitaisiin siirtää, jos siihen ei liittyisi akuuttia hyväksikäyttötilannetta ja puuttumisen siirtäminen on välttämätöntä.

[523] Tuomio tuli kuitenkin törkeän ryöstön valmistelusta.

[524] Poikkeuksen voisi tehdä tilanne, jossa erittäin vaarallista huumausainetta oltaisiin kaupittelemassa alaikäisille ja tämä muodostaisi merkittävän vaaran heidän hengelle ja terveydelle. Käytännössä tällaisen tiedon saamista voidaan kuitenkin pitää äärimmäisen harvinaisena, koska kaupanteko tapahtuu monesti anonyymisti.

# 7 POLIISI- JA PEITEPROFIILEJA KOSKEVAT SALAISET TIEDONHANKINTA- JA PAKKOKEINOT TIETOVERKOISSA

## 7.1 Yleisvalvonta

Poliisi on yleensä suorittanut henkilöihin, ajoneuvoihin ja paikkoihin kohdistuvaa valvontaa, voidakseen ennalta estää rikoksia ja häiriötä sekä saada selville rikoksia ja tunnistaakseen rikoksesta epäiltyjä.[525] Yleisvalvonnasta ei löydy nimenomaista säännöstä, eikä se ole salainen tiedonhankinta- tai pakkokeino. Se on kuitenkin tärkeä määritellä erityisesti tietoverkoissa, jotta muita toimivaltuuksia voidaan arvioida suhteessa siihen.[526] Sääntelyssä voidaan lähimmin tukeutua PolL 1:1:n poliisin tehtäviä koskevaan säännökseen.[527] Yleisvalvonta onkin tietynlainen yläkäsite poliisin toiminnalle, jolla tarkoitetaan ennalta määräämättömään ihmisryhmään kohdistuvaa seurantaa, joka ei kohdistu kehenkään tiettyyn henkilöön. Yleisvalvonnan tarkoituksena on mahdollisimman nopea ja tehokas puuttuminen mahdollisesti tapahtuviin rikoksiin tai esiintyviin häiriöihin sekä niihin syyllistyneiden välitön kiinniottaminen. Lisäksi yleisvalvonnan yhteydessä voidaan saada tietoja, joita voidaan käyttää hyväksi rikosten ennalta estämisessä ja selvittämisessä.[528] Tietoverkoissa erilaiset keskustelupalstat rinnastuvat reaalimaailmassa tietyn rakennuksen, tilan tai paikan yleisvalvontaan.[529] Eli jos kohteena ei ole tietty henkilö, on keskustelupalstan tai muun vastaavaan tietoverkoissa olevan sivuston seuraaminen yleisvalvontaa.[530]

Poliisilain esitöiden perusteella jää epäselväksi, miten yleisvalvonnan määritelmä pitäisi hahmottaa erilaisissa rakenteeltaan monimutkaisemmissa sosiaalisen median palveluissa. Asiaa voidaan arvioida luottamukselliseen viestintään liittyvän suljetun ryhmän ja profiilin problematiikan avulla. Tulkintaan vaikuttavat 1) ryhmän tai kaverilistan laajuus, 2) mitä

[525] Helminen – Kuusimäki – Rantaeskola 2012, s. 388.
[526] Yleisvalvonnasta käytetään esitöissä myös määritelmää valvonta, mutta ne tarkoittavat samaa. Tässä tutkimuksessa käytetään yleisvalvonnan käsitettä, joka kuvaa sen yleistä luonnetta paremmin. Ks. termeistä myös Helminen – Kuusimäki – Rantaeskola 2012, s. 388.
[527] Vaikka kyseessä ei ole toimivaltuussäännös, velvoittaa kyseinen säännös poliisin suorittamaan valvontaa yleisen järjestyksen ja turvallisuuden ylläpitämiseksi. Ks. valvonnan suhteesta toimivaltuuteen esimerkiksi AOA 29.11.2013 Dnrot 1870/4/13, 2061/4/13, 2186/4/13, 2187/4/13 ja 2189/4/13, s. 11, jossa oli kyse koiran käyttömahdollisuudesta tarkistaa sattumanvaraisesti vastaantulevia ihmisiä.
[528] HE 57/1994 vp, s. 57.
[529] Näitä ovat esimerkiksi tienristeys tai aukio. Ks. HE 22/1994 vp, s. 26.
[530] HE 224/2010 vp, s. 34.

tarkoitusta varten ryhmä tai profiili on luotu ja 3) millainen hyväksymisprosessi on.[531] Esimerkiksi muutaman kymmenen hengen mielenosoittajaryhmän seuraaminen reaalimaailmassa on vielä yleisvalvontaa, jos se ei kohdistu tiettyyn henkilöön. Tietoverkkojen puolella tämä voidaan tulkita siten, että jos poliisi seuraa samankokoisen ryhmän keskusteluja, eikä tarkkailu kohdistu kehenkään tiettyyn henkilöön, on kyse vielä yleisvalvonnasta. Tarkkailuksi toiminta muuttuu, jos ryhmästä aletaan yksilöimään tarkkailun kohteeksi tiettyjä henkilöitä. Poliisihallitus katsoo, että jos kyseessä on suppea muutaman hengen ryhmä, tiedonhankinnan toteuttaminen kohdistuu käytännössä tiettyihin henkilöihin ja tämä edellyttää erityisten tarkkaa harkintaa siitä, onko kyseessä jo tarkkailu tai suunnitelmallinen tarkkailu.[532] Olen Poliisihallituksen kanssa siitä samaa mieltä, että ryhmän koolla on merkitystä arvioitaessa yleisvalvonnan soveltuvuutta. Jos kuitenkin kyseessä on muutaman hengen ryhmään soluttautuminen, on kyse pikemminkin jo peitetoiminnasta.[533] Sama koskee myös yksittäisen profiilin kaveriksi hakeutumista, vaikka profiililla olisikin useita kavereita. Tämä sen takia, että tiedonhankinnan voidaan katsoa kohdistuvan kyseiseen profiiliin. Ryhmän tai profiilin tarkoitus on monesti yhteydessä ryhmän laajuuteen, joten sen itsenäinen merkitys on vähäisempi. Jos ryhmä tai profiili on luotu vain läheisten kesken tapahtuvaa viestintää varten, on yleensä henkilöiden määräkin suppeampi ja siten lähempänä edellä mainittua peitetoimintaa.

Ryhmään liittymisen ja sen viestinnän näkemisestä esimerkkeinä voidaan käyttää Facebookin ryhmärakennetta, jossa ryhmät jaetaan julkisiin, suljettuihin ja salaisiin.[534] Liittymispyynnön voi kahteen ensimmäiseen lähettää kuka vain Facebook-käyttäjä, mutta salatun ryhmän osalta liittymisen tulee tapahtua kutsusta. Ryhmään liittyminen taas riippuu siitä, millaiset asetukset ryhmän ylläpitäjä/ylläpitäjät ovat asettaneet ryhmälle.[535] Julkisten ja suljettujen ryhmien kohdalla käyttäjä voi itse liittyä suoraan ryhmään, mutta asetuksilla voidaan asettaa hyväksyntä ryhmän jäsenen, moderaattorin tai ylläpitäjän tehtäväksi.[536]

---

[531] Keskustelupalstan ja yleisesti verkkoviesteiksi tulkittavien tilanteiden kohdalla tilanne on helpompi tulkita, koska ne ovat avoimesti kaikkien saatavilla.

[532] Poliisihallitus 2017c, s. 5.

[533] Tilanteessa soluttaudutaan muutaman hengen ryhmään, jossa oletettavasti käydään suhteellisen luottamuksellisia keskusteluja ja viestintä nauttii luottamuksellisen viestin suojaa heidän kesken.

[534] Facebookista löytyy myös useita osto- ja myyntiryhmiä. Ne ovat sinänsä tavallisia ryhmiä, mutta niissä on mahdollista asettaa tuotteita myytäväksi, merkitä tuotteita myydyksi ja hakea ostettavia tuotteita.

[535] Ryhmän ylläpitäjä on voinut esimerkiksi antaa tiettyjen muiden ryhmien jäsenille automaattisen oikeuden liittyä ryhmään halutessaan. Sama koskee tilannetta, jossa ylläpitäjä on voinut ladata sähköpostiosoitelistan palveluun, jolloin kaikki nuo käyttäjät pääsevät ryhmään halutessaan.

[536] Ylläpitäjät ja moderaattorit erotetaan yli 50 hengen ryhmissä erillisellä merkillä. Ylläpitäjän ja moderaattorin erot perustuvat lähinnä siihen, kuinka laajaa joukkoa ryhmän asetuksia he voivat hallita. Moderaattorilla on samat oikeudet jäsenten lisäämiseen ja poistamiseen kuin ylläpitäjälläkin.

Lisäksi liittymisen yhteyteen voidaan lisätä enintään kolme kysymystä, joihin tulee vastata, ennen kuin ryhmään hyväksytään.[537] Salattujen ryhmien osalta käyttäjä ei voi itse löytää ryhmää lainkaan, vaan hänet tulee kutsua sinne. [538]

Näkyvällä poliisiprofiililla yleisvalvontaa suorittavan profiilin liittyessä ryhmään, ryhmän jäsenet, moderaattorit ja ylläpitäjät tietävät ryhmään liittyvän olevan poliisi. He voivat halutessaan estää liittymisen tai poistaa poliisiprofiilin ryhmästä.[539] Salaisten tiedonhankinta- ja pakkokeinojen näkökulmasta yleisvalvontaan ryhmässä tähtäävä toiminta ei aiheuta tulkintaongelmia, koska poliisin toiminta ei tapahdu salaa, vaan näkyvästi poliisina. Ongelmaton on myös tilanne, jossa peiteprofiili pystyy liittymään ryhmään ilman kenenkään hyväksymistä, koska tällöin tilanne rinnastuu siihen, että siviilivaatetuksessa oleva poliisimies kävelee suoraan johonkin avoimeen tilaisuuteen.[540] Tilanne on kuitenkin monimutkaisempi, jos ryhmään liittyminen yleisvalvontatarkoituksessa tapahtuu peiteprofiililla ja vaatii jonkun ryhmäläisen reagointia.[541] Herää kysymys, vaatiiko vuorovaikutukseen perustuva ryhmään liittyminen jonkin nimenomaisen toimivaltuuden, kuten peitellyn tiedonhankinnan (PolL 5:15 ja PKL 10:14) edellytysten täyttymisen?

Poliisihallitus on linjannut, että ryhmään liittyminen on mahdollista vielä yleisvalvonnan rajoissa, jos sisäänpääsy ei edellytä laajaa vuorovaikutusta sivuston ylläpitäjän tai muun ”portinvartijan” kanssa. Jos kyse on laajemmasta vuorovaikutuksesta, kyseessä olisi peitelty tiedonhankinta.[542] Olen tästä samaa mieltä, joskin huomioon tulee ottaa aikaisemmin mainittu ryhmän koko toimivaltuuskysymystä arvioitaessa.[543] Vaikka PL 2:3 §:n mukaan julkisen vallan käytön tulee perustua lakiin ja poliisin salaisten tiedonhankinta- ja pakkokeinojen osalta PolL 5 ja PKL 10 luvun toimivaltuuksiin, on poliisimiehellä edelleen

[537] Käyttäjä voidaan myös kutsua julkiseen tai suljettuun ryhmään, jolloin käyttäjä voi itse päättää liittyykö hän siihen vai ei.
[538] Ks. tarkemmin Facebook 2019a, jossa tietoa ryhmistä ja niiden hallinnoimisesta.
[539] Poliisilla ei ole olemassa mitään toimivaltuutta tai edes teknistä mahdollisuutta liittyä ”väkisin” ryhmään.
[540] Tietoverkojen osalta voidaan mainita Facebook-ryhmien lisäksi myös avoimeksi tarkoitetut Whatsapp-ryhmät. Ks. esimerkiksi Yle 2019, jossa poliisi oli yleisvalvonnan kautta saanut tiedon noin 250:n 9–13-vuotiaan käyttäjän ryhmästä, jossa oli ollut kuvia ja videoita, jotka olivat äärimmäisen väkivaltaisia ja pornografisia. Kyseistä ryhmää oli mainostettu Instagram-profiilissa linkillä. Asiaa tutkittiin sukupuolisiveellisyyttä loukkaavan kuvan levittämisenä.
[541] Tämä koskee lähinnä suljettuja ja salaisia ryhmiä, koska julkisissa ryhmissä ryhmän keskustelut ovat kaikkien Facebook-käyttäjien nähtävissä.
[542] Poliisihallitus 2017c, s. 5.
[543] Myös reaalimaailmassa poliisi voi suorittaa yleisvalvontaa esimerkiksi liikenteenvalvontaan, mielenosoituksiin tai erilaisiin tilaisuuksiin liittyen. Jos poliisi haluaa esimerkiksi mennä suorittamaan yleisvalvontaa musiikkitapahtumaan, voivat poliisimiehet siirtyä festarialueelle muiden osallistujien tapaan. Siirtymällä festarialueelle he ovat samanlaisen ”portinvartija” problematiikan edessä kuin Facebook-ryhmien osalta, jossa liittyvän peiteprofiilin tulee olla vuorovaikutuksessa ylläpitäjän tai moderaattorin kanssa, joka päättää sisäänpääsystä.

virkatehtäviin liittyvien erityisvaltuuksien ohella pääsääntöisesti oikeus kaikkiin sellaisiin toimenpiteisiin jotka lainsäädäntö sallii kenelle tahansa kansalaiselle. [544] Tämän takia ei ole tarpeen säännellä sellaisesta toiminnasta, joka liittyy tiedonhankintaan kuuluviin normaaleihin keskusteluihin.[545] Yleisvalvontatarkoituksessa ryhmään liittymiseen liittyvää vuorovaikutusta ylläpitäjään tai moderaattoriin voidaankin pitää normaalina tiedonhankintaan liittyvänä keskusteluna, eikä ryhmään liittyminen peiteprofiililla vaadi lähtökohtaisesti mitään nimenomaista toimivaltuutta. Saman voidaan katsoa myös tilannetta, jossa peiteprofiililla toimiva poliisi osallistuu ryhmän keskusteluun ja esimerkiksi tykkää jonkun päivityksestä. Kyseessä on lähtökohtaisesti vain normaali tiedusteluun liittyvä keskustelu, jos keskustelua ei käydä profiilin kanssa, johon on tarkoitus kohdistaa tiedonhankintaa. Sama pätee myös tarkkailuun ja suunnitelmalliseen tarkkailuun. Peiteprofiililla toimiva ja tiettyä ryhmäläistä tarkkaileva poliisimies voi siis kommentoida tai tykätä toisten henkilöiden päivityksistä, mutta kohdehenkilön kanssa tämä ei ole mahdollista ilman vuorovaikutuksen mahdollistavaa toimivaltuutta.[546] Kyseinen toimivaltuuksien ulkopuolelle jäävä toimintatapa on myös oleellisessa roolissa vahvan peitteen peiteprofiilin ”legendan rakentamismahdollisuuksien” osalta, jossa operatiivisen vaiheen ulkopuolella peiteprofiili pidetään eri tavoin aktiivisen näköisenä.[547]

### 7.2 Tarkkailu

Poliisi- ja pakkokeinolain määritelmä tarkkailusta on samanlainen.[548] Tarkkailulla tarkoitetaan tiettyyn henkilöön salaa kohdistettavaa havaintojen tekemistä tiedonhankintatarkoituksessa (PolL 5:13.1 ja PKL 10:12.1). Poliisilain mukaisessa

[544] HE 57/1994 vp, s. 56. Poikkeuksen tekevät yksityiselämän suojan näkökulmasta kuitenkin tilanteet, joissa poliisi viranomaisena hankkii järjestelmällisesti tietoja jonkun yksityiselämästä, josta yleisvalvonnan osalta ei kuitenkaan ole kyse. Lainsäätäjä ei ole katsonut olevan tarpeellista säätää tarkkailun edellytyksistäkään tarkemmin, koska se voidaan katsoa eräänlaiseksi poliisin keinovalikoimaan kuuluvaksi perustoimenpiteeksi. Ks. HE 224/2010 vp, s. 177; HE 222/2010 vp, s.

[545] HE 57/1994 vp, s. 15.

[546] Reaalimaailmassa tämä rinnastuu tilanteeseen, jossa poliisimies keskustelee toisen henkilön kanssa kahvilassa ja tarkkailtava kohdehenkilö kuulee poliisimiehen keskustelun. Jos kohdehenkilö jostain syystä kommentoi tai reagoi poliisimiehen toimintaan, on siitä mahdollista vetäytyä vuorovaikutuksen keinoin. Ks. vetäytymismahdollisuudesta HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.

[547] Tämä voidaan erottaa peitetoiminnan operatiivisen vaiheen osalta siitä, että luonnollista vuorovaikutusta voi olla myös muiden kuin itse kohdehenkilön kanssa, eikä tämän osalta ole tarvetta erillisille toimivaltuussääntelylle, ellei peitetoimintaa nimenomaisesti laajenneta koskemaan kyseistä henkilöä. Ks. tarkemmin HE 224/2010 vp, s. 115; HE 222/2010 vp, s. 338.

[548] Tarkkailusta oli säännelty ennen vuoden 2014 lakimuutoksia vain poliisilain puolella ja esitutkinnan osalta tarkkailu oli sallittua tavanomaisen oikeuden perusteella. Ks. HE 222/2010 vp, s. 324.

tarkkailussa henkilöstä tehdään rikoksesta estämistä ja keskeyttämistä edistäviä havaintoja.[549] Pakkokeinolain mukaisessa tarkkailussa henkilöstä taas tehdään rikoksen selvittämistä edistäviä havaintoja.[550] Tarkkailussa voidaan RL 24:6:n estämättä käyttää näköhavaintojen tekemiseen tai tallentamiseen kameraa tai muuta sellaista teknistä laitetta (PolL 5:13.1 ja PKL 10:12.1), mutta tällä ei ole tietoverkoissa merkitystä.[551] Tarkkailua voidaan toteuttaa tietoverkossa tietokoneen välityksellä esimerkiksi katselemalla henkilön keskustelupalstalla käymää keskustelua. Kyseessä ei ole tekninen tarkkailu tai RL 24:6:n sääntelyyn liittyvä tilanne, koska tämä on toimintaympäristöön liittyvä erityispiirre, jossa tietokonetta käytetään muiden käyttäjien tavoin.[552] Tarkkailua on mahdollista suorittaa sekä poliisi- että peiteprofiililla.

Yleisvalvonnasta tarkkailun erottaa tiettyyn henkilöön kohdennettu tiedonhankintatarkoitus. Tiedonhankintatarkoitusta ei ole tarkemmin määritelty lainsäädännössä tai esitöissä, mutta näyttäisi siltä, että pelkkä salainen tiettyyn henkilöön kohdistuva toiminta riittää, koska tarkkailussa ei välttämättä kerry mitään poliisin tietojärjestelmiin tallennettavaa tietoa.[553] Reaalimaailmassa tarkkailussa on yleensä kyse poliisimiehen tiettyyn henkilöön tosiasiallisesti kohdistamista reaaliaikaisista aistihavainnoista. Laissa tai esitöissä ei ole kuitenkaan määritelty aikarajaa sille, kuinka kauan poliisimiehen pitää kohdistaa havainnointiaan tiettyyn henkilöön, ennen kuin yleisvalvonta muuttuu tarkkailuksi. Vuoden 1995 poliisilain esitöiden mukaan valvonnan ja tarkkailun välille ei voitu määrittää yksiselitteistä rajaa, koska valvonnan avulla voitiin saada tietoja, joiden johdosta yleisvalvonnan sijasta ryhdyttiin tarkkailemaan tiettyä henkilöä.[554] Esimerkkinä problematiikasta reaalimaailmassa voidaan käyttää tilannetta, jossa kauppakeskuksen edessä oleva poliisipartio seuraa alueella oleskelevia henkilöitä ja yksi heistä alkaa elehtiä levottomasti. Kuinka kauan poliisipartion tulee kohdistaa huomiotaan kyseiseen henkilöön, jotta kyseessä voitaisiin katsoa olevan tarkkailun määritelmän mukainen toimenpide? Etenkin jos henkilön perässä ei erikseen kävellä muualle, hänestä ei tallenneta mitään tietoa,

[549] HE 224/2010 vp, s. 101–102.
[550] HE 222/2010 vp, s. 325.
[551] Teknisellä laitteella tarkoitetaan esimerkiksi kiikaria, kameraa, videokameraa, valonvahvistinta tai muuta vastaavaa teknistä laitetta. Tekniseen katseluun verrattuna tarkkailussa käytettävä laitteisto tulisi koko tiedonhankinnan ajan olla poliisimiehen valvonnassa ja käytössä.
[552] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.
[553] Tarkkailusta ei myöskään PolL 5:59:n ja PKL 10:61:n mukaan tarvitse laatia pöytäkirjaa. Tarkkailusta olisi kuitenkin tarvittaessa tehtävä merkintä muuhun asiakirjaan, esimerkiksi tehtävänsuorituslomakkeeseen. Ks. HE 224/2010 vp, s. 139; HE 222/2010 vp, s. 363. Tämä ei kuitenkaan tarkoita tarkkailussa kertyneiden havaintotietojen kirjaamista, vaan yleisesti tarkkailua ja sen kulkua. Epäselväksi jää, miten muutoin PolL 5 ja 10 luvun yhteisiä säännöksiä tulisi soveltaa tarkkailussa.
[554] HE 57/1994 vp, s. 57

eikä lopulta ryhdytä mihinkään toimenpiteisiin.[555] Käytännössä tarkkailun voidaan katsoa alkavan nykylainsäädännön mukaan suhteellisen nopeasti, jos tietyn henkilön toimintaa seurataan, koska lainsäätäjä ei ole asettanut mitään ajallista alarajaa tarkkailun alkamisajankohdalle. Tietoverkossa kyseinen problematiikka voisi rinnastua keskustelupalstalla tai ryhmässä tilanteeseen, jossa jokin henkilön viestinnässä kiinnittää poliisimiehen huomion. Jos poliisimies alkaa tarkastelemaan pelkästään kyseisen henkilön profiilia ja hänen suorittamaa viestintää, siirtyy toiminta melko nopeasti tarkkailun puolelle, koska tiedonhankinnan voidaan katsoa kohdistuvan tiettyyn henkilöön.

Vaikka myös poliisilain mukaisessa tarkkailussa kohdehenkilö voi olla jo valmiiksi tiedossa, on tämä yleisempää pakkokeinolain mukaisessa tarkkailussa, koska silloin poliisilla on tiedossa rikoksesta epäilty, johon tarkkailu yleensä kohdistuu.[556] Rajanveto on tällöin helpompi, koska tarkkailtava kohde on jo valmiiksi poliisin yksilöimänä ja tiedossa. Heti kun hänestä saadaan ensimmäinen havainto, voidaan tämä tulkita tarkkailun alkamisajankohdaksi.[557] Jos kohdehenkilöä ei reaalimaailmassa löydetä, ei tämä ole tarkkailua, koska se ei kohdistu tiettyyn henkilöön. Sama pätee myös tietoverkkoihin, jossa poliisilla voi olla vinkkitietona tietty profiili tai linkki tietylle blogille. Jos poliisi yrittää mennä katsomaan kyseistä kohdetta ja se on jo poistettu, ei tätä ole pidettävä tarkkailuna koska tosiasiallista havaintoa kohteesta ei ole saatu. Jos kyseinen profiili tai blogi on tallella, alkaa tarkkailu siitä ajankohdasta kun poliisimies klikkaa itsensä kohteeseen. Oli kyse poliisi- tai pakkokeinolain mukaisesta tarkkailusta, voidaan tarkkailun aikajana jakaa siten, että tarkkailu alkaa siinä vaiheessa kun kohteeksi valikoidusta tietystä profiilista tehdään havaintoja ja päättyy siinä tilanteessa kun profiilia ei enää syystä tai toisesta havaita. Jossain harvoissa tapauksissa tilanne voi olla monimutkaisempi. Esimerkiksi ratkaisussa Itä-Uudenmaan KO 11.2.2019 R 18/3115/766 takavarikoitiin huumausaineiden kauppapaikkana

[555] Jos otetaan huomioon yleisvalvonnan yhteydessä mainittu salaisia tiedonhankinta- ja pakkokeinoja koskevan määräyksen raportointivelvoite, ei kyseisenlaisesta tilanteesta tehdä ymmärrykseni mukaan merkintöjä tarkkailuna, vaikka henkilön toimintaa seurattaisiin kauppakeskuksen edessä useita minuutteja ja toiminta voitaisiin tulkita tarkkailuksi. Ks. Poliisihallitus 2018a, s. 5.

[556] Tarkkailu voi kohdistua muuhunkin kuin rikoksesta epäiltyyn, mutta käytännössä tämä on selvästi harvinaisempaa. Ks. Poliisihallitus 2018a, s. 5.

[557] Vrt. AOA 2.7.2015 Dnro 87/4/15, missä oli kyse tilanteesta, jossa siviilipukuinen poliisipartio meni vihjetiedon perusteella tarkastamaan rappukäytävää kannabiksen hajun vuoksi. Vihjeen saanut konstaapeli oli tunnistanut rapusta aikaisemmin yhden asukkaan, jolla oli huumausainerikostaustaa. Pari viikkoa myöhemmin kyseinen konstaapeli oli siviilipukuisena kenttävalvontaryhmäläisenä mennyt samaan rappuun ja haistanut kannabiksen, joka oli voimakkainta hänelle entuudestaan tutun henkilön ovella. Kyseisellä perusteella POV oli antanut kotietsintäluvan. AOA katsoi ettei rappukäytävään meno vaatinut erityistä toimivaltanormia, vaikka kyseessä olikin kotirauhan suojaama alue. AOA tulkitsi poliisin toiminnan rappukäytävässä olevan ”lähinnä tarkkailua”. Kyseessä on kuitenkin tulkintani mukaan vielä enemmän yleisvalvontaa viittaava toimenpide, vaikka kohdehenkilö oli jo tiedossa. Kyseisestä kohdehenkilöstä ei ollut vielä rappukäytävässä mitään aistihavaintoja vaan havainnointi kohdistui rappukäytävään ja kannabiksen hajuun siellä.

toimineen Sipulikanavan palvelimet, joissa oli tallentuneena suuri määrä eri käyttäjien viestejä. Jos näitä viestejä tarkastellaan jälkeenpäin poliisin toimesta, voisi myös tässä tilanteessa tulla kyseeseen tarkkailu jokaisen tarkastelun kohteena olevan profiilin kohdalla. Tilanne on osittain verrattavissa teknisen tarkkailun menetelmiin, jossa esimerkiksi teknisen katselun jälkeen poliisille muodostuu tallenne, jota tarkastellaan yleensä vasta myöhemmin. Toisaalta yksittäisen henkilön profiilista laajamittaisesti tietoja tallettaessa myöhempää tarkastelua varten, kyseeseen voisi tulla jo suunnitelmallinen tarkkailu. Tähän palataan tarkemmin seuraavassa alaluvussa.

Käytännössä reaalimaailmassa tai tietoverkoissa yksittäisellä tarkkailutoimenpiteellä ei ole juurikaan merkitystä henkilön yksityiselämän suojan kannalta, niin kuin on tuotu jo aikaisemmin esille. Merkitystä tarkkailun alkamisajankohdalla on tietoverkoissa kuitenkin erityisesti dokumentoinnin osalta. Vaikka tarkkailusta ei tarvitse tehdä pöytäkirjaa, todetaan hallituksen esityksissä, että tarkkailusta on tarvittaessa tehtävä merkintä muuhun asiakirjaan, esimerkiksi tehtävänsuorituslomakkeeseen. [558] Reaalimaailmassa tämä onnistuu vielä suhteellisen hyvin, mutta jos jokaisen profiilin erillisestä tarkastelusta kirjattaisiin tarkkailutiedot ylös, joutuisi yleisvalvontaa suorittava poliisi- tai peiteprofiili kirjaamaan jopa satoja tarkkailukertoja päivän aikana, koska hän voi vierailla useissa profiileissa. Dokumentointi ei ole mielestäni tällöin tarpeellista, vaikka yksittäisten profiilien tarkastelun takia toiminnan voitaisiinkin katsoa menevän tarkkailun puolelle.[559] Jos taas kyse on tietystä jo entuudestaan tiedossa olevasta kohteesta jonka tarkkailu tulee mahdollisesti toistumaan, on dokumentointi tärkeää sen takia, että rajaa suunnitelmalliseen tarkkailuun voidaan arvioida asianmukaisesti.

Tutkimuksen alussa on käsitelty laajasti yksityiselämän suojan eroja reaalimaailman ja tietoverkkojen välillä. Kohdehenkilöä käsittelevässä kohdassa on tuotu esille, että kohdehenkilöstä voi löytyä tietoverkoista paljon tietoa myös jonkun toisen tahon lisäämänä.[560] Tarkkailun kannalta ei ole ei ole määritelty missä asemassa olevaa henkilöä voidaan tarkkailla, mutta reaalimaailmassa ei yleensä kohdisteta tarkkailua muihin kuin rikokseen oletettavasti syyllistyvään tai rikoksesta epäiltyyn. Suunnitelmallisessa tarkkailussa on kuitenkin mainittu tilanteesta, jossa kyse on muihin kuin rikoksesta epäiltyyn

[558] HE 224/2010 vp, s. 139; HE 222/2010 vp, s. 363.
[559] Merkitystä tulee antaa myös sille, kirjataanko kohteeseen liittyen jotain tietoa ylös poliisin tietojärjestelmiin. Tosin tällöin myös merkintä tarkkailusta tulee suoritetuksi havaintotiedon kirjaamisen yhteydessä.
[560] Tällaisia voivat olla esimerkiksi kohdehenkilöstä kertovat blogikirjoitukset tai keskustelupalstalle lähetetty viesti kohdehenkilöön liittyen.

kohdistuvasta tarkkailusta. Kyseinen tarkkailu on mahdollista vain lyhytkestoisena yksittäisenä toimenpiteenä ja lähinnä siitä syystä, että varsinainen suunnitelmallisen tarkkailun kohde pystytään varmistamaan tai tavoittamaan. Esimerkkinä tavoittamisesta mainitaan tilanne, jossa tiedetään tietyn henkilön toimittavan pakoilua varten varoja esitutkintaa karttavalle rikoksesta epäillylle, jolloin kyseistä henkilöä voitaisiin seurata tarkkailun puitteissa piilopaikkaan varsinaisen epäillyn tavoittamiseksi.[561] Käytännössä tämä tarkoittaa sitä, ettei tietoverkoissa tapahtuvassa tarkkailussa ole juurikaan merkitystä yksittäisen tapahtuman kannalta, saadaanko tieto itse kohdehenkilön vai jonkun muun viestinnän perusteella. Muuhun kuin kohdehenkilöön kohdistuva tarkkailu ei kuitenkaan ole mahdollista kuin lyhytaikaisesti ja yleensä vain muutaman kerran tapahtuvana. Siten esimerkiksi kohdehenkilön aviopuolison tunnettujen ystävien sosiaalisen median profiilin pidempiaikainen seuraaminen ei ole mahdollista, jos hän ei ole epäiltynä rikoksesta.[562]

Salaa tehtävistä havainnoista esitöissä viitataan tarkkailijan ja tarkkailtavan henkilön välisen vuorovaikutuksen passiivisuuteen, eikä keskusteluun tiedonhankinnan kohteen kanssa saa hakeutua aktiivisesti.[563] Tarkkailu tapahtuu salaa, mutta tarkkailua voidaan sinänsä suorittaa myös reaalimaailmassa esimerkiksi tunnuksellisesta poliisiautosta, jolloin kohdehenkilö ei itse tiedä olevansa tiedonhankinnan kohteena. Käytännössä tämä tarkoittaa sitä, että tarkkailua tietoverkoissa voidaan suorittaa peiteprofiilien lisäksi myös poliisiprofiileilla.[564] Vuorovaikutus ei kuitenkaan ole täysin poissuljettua, koska vuorovaikutus on mahdollista tilanteissa joissa tarkkailun toteuttaja paljastuu tahattomasti tai tarkkailija poistuu tilanteesta vuorovaikutuksen keinoin.[565] Esimerkkinä esitöissä mainitaan kahvilan viereisen pöydän äärestä tarkkailu, jossa poliisimies joutuu poistumaan tilanteesta keskustelemalla tiedonhankinnan kohteen kanssa. Aloitteen vuorovaikutukseen tulisi kuitenkin näissä tapauksissa tulla tiedonhankinnan kohteelta.[566]

Tietoverkoissa esitöiden esimerkki poliisiautosta tarkkailussa ja sen liittymisestä vuorovaikutukseen on vaikeampi hahmottaa. Tietoverkoissa kyse voi olla esimerkiksi

[561] HE 222/2010 vp, s. 325–326.
[562] Vierailut profiilissa ovat siis kuitenkin perusmuotoisen tarkkailun puitteissa mahdollisia, vaikka varsinainen tiedonhankinta ei kohdistukaan kyseiseen puolisoon.
[563] Jos kohdehenkilön kanssa hakeudutaan vuorovaikutukseen, kyseeseen voi tulla peitelty tiedonhankinta tai peitetoiminta. Ks. HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.
[564] Toisaalta asialla ei ole niin suurta merkitystä kuin reaalimaailmassa, koska tarkkailutyyppinen toiminta tietoverkoissa ei välttämättä näy muille käyttäjille millään tavalla.
[565] Kyseiselle ”pelastautumiselle” ei ole asetettu aikarajaa, mutta käytännössä kyse voisi olla korkeintaan muutaman minuutin kestävästä keskustelusta ja tietoverkon puolella muutamista viesteistä.
[566] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.

tilanteesta, jossa sosiaalisen median palvelu ilmoittaa kaikista profiilissa vierailleista käyttäjistä.[567] On myös esiintynyt arveluja, että esimerkiksi Facebook ehdottaisi kaveriksi profiileja, jotka ovat vierailleet toisen henkilön profiilissa. Tällöin poliisimiehen vierailu kohdehenkilön profiilissa laukaisisi kaveriehdotuksen algoritmin perusteella kohdehenkilölle.[568] Kysymys kuuluukin rinnastuvatko kyseiset tilanteet siihen, että kohdehenkilö vain näkee poliisiauton ilman tietoa häneen kohdistuvasta tarkkailusta, vai siihen, että poliisimies ryhtyy vuorovaikutukseen kohteen kanssa?

Vuorovaikutuksen merkitystä kyseisessä tilanteessa voidaan tarkastella arvioimalla tarkkailua suhteessa peitellyn tiedonhankinnan (PolL 5:15 ja PKL 10:14) tunnusmerkistöön.[569] Tarkkailuun verrattuna peitelty tiedonhankinta eroaa siten, että peitellyssä tiedonhankinnassa on luonteenomaista pyrkimys henkilökohtaiseen tapaamiseen tai vastaavaan vuorovaikutustilanteeseen tiedonhankinnan kohteen kanssa. Kyse on yleensä yksittäisestä tiedonhankintatapahtumasta.[570] Kohdehenkilön profiilissa vieraillessa kyse on sinänsä yksittäisestä tiedonhankintatilanteesta, mutta poliisimiehellä ei ole tarkkailutilanteessa tarkoitusta ryhtyä vuorovaikutukseen tiedonhankinnan kohteen kanssa, vaan mahdollinen tieto poliisimiehen poliisi- tai peiteprofiilista vierailusta johtuu pikemminkin palvelun teknisistä ominaisuuksista. Jos kohdehenkilön profiilin tarkasteluun käytetään poliisiprofiilia, voi kohdehenkilö huomata vierailun aiheuttaman jäljen takia reaalimaailmaa helpommin, että hän on tarkkailun kohteena.[571] Poliisin vierailu kohdehenkilön profiilissa rinnastuukin reaalimaailman verrattuna tilanteeseen, jossa kohdehenkilö huomaa virkapukuisen poliisin seuraavan nimenomaan häntä syystä tai toisesta.[572] Kyse on siten enemmän poliisimiehen huonosta suojautumisesta ja tarkkailun paljastumisesta kuin vuorovaikutuksesta kohteen kanssa, koska pelkkää poliisin tarkkailutoiminnan paljastumista ei voida pitää sellaisena seikkana, että se tekisi toiminnasta

[567] Tällainen on esimerkiksi LinkedIn.
[568] Facebook ilmoittaa itse ohje- ja tukikeskuksessaan, että kaveriehdotukset syntyvät seuraavilla perusteilla: 1) yhteiset kaverit, 2) kuuluminen samaan ryhmään tai profiilit on merkitty samaan ryhmään, 3) verkostot (esimerkiksi koulu, yliopisto, tai työ) ja 4) ladatut yhteystiedot. Ks. tarkemmin Facebook 2019b.
[569] Peitetoiminnan (PolL 5:28 ja PKL 10:27) määritelmä ei tilanteessa täyty, koska kyse tulee olla jo soluttautumisesta, jossa pyritään muodostamaan erityinen luottamussuhde kohteeseen.
[570] HE 224/2010 vp, s. 104; HE 222/2010 vp, s. 327.
[571] Ks. profiilissa vierailuun ja siitä jäävään jälkeen liittyvästä problematiikasta OSINT-toimintaan liittyen tarkemmin McKeown – Maxwell – Azzopardi 2014, s. 7
[572] Kyseistä toimintamallia käytettiin joskus nettipoliisityön alkuvaiheessa IRC-Galleriassa, jossa sai itse asetuksista määritellä näkyykö vierailu toisen profiilissa vai ei. Poliisiprofiililla vierailu satunnaisissa profiileissa sai monesti kohteet kyselemään ovatko he tehneet jotain ja miksi poliisi vieraili heidän profiilissaan. Kyseisellä toiminnalla kiinnitettiin tarkoituksella kohteiden huomiota, eikä tarkoituksena ollut tarkkailla heitä. Pääajatuksena oli lähinnä levittää tietoa siitä, että poliisin palveluita oli saatavilla myös sosiaalisesta mediasta käsin sekä lisäksi ennalta estää rikoksia näkyvällä toiminnalla.

vuorovaikutukseen pyrkivän. Peiteprofiilitoiminnassa kohdehenkilö ei voi tietää kuka profiilia todellisuudessa käyttää, joten vaikka poliisimiehen vierailusta jäisi jälki, ei poliisin toiminta lähtökohtaisesti paljastu kohdehenkilölle. Etenkin kun toisten profiileissa vierailu on luonteenomaista sosiaalisen median palveluille siinä missä ihmisten ohi kävely kaupungilla, eikä erilaisia profiileja selaillessa olla välttämättä vuorovaikutuksessa muutoin millään tavalla kohteen kanssa.[573] Vuorovaikutusta ovat pikemminkin kommentointi sekä erilaiset reagoinnit tykkäyksin tai viestein toisen henkilön päivityksiin. Jos peiteprofiililla vieraillaan kohdehenkilön profiilissa on se tulkittava pelkäksi tarkkailuksi, vaikka kohdehenkilö saisi vierailusta palvelun teknisen ominaisuuden takia jonkinlaisen tiedon käyttäjätililleen.

Tarkkailuun liittyen ryhmiin liittymistä voidaan arvioida yleisvalvonnan yhteydessä esitetyn mukaisesti. Tällöin ryhmään pääsemisen tarkoituksena ei ole yleisvalvonta, vaan johonkin tiettyyn ryhmässä olevaan henkilöön tai henkilöihin kohdistuva tiedonhankinta. Tulkinnan lähtökohtana tulee ottaa huomioon se, että reaalimaailmassa tarkkailua on mahdollista kohdistaa myös kotirauhan piirissä oleskelevaan henkilöön. Kunhan ei käytä tässä tarkkailussa teknistä laitetta, eikä kohde oleskele vakituiseen asumiseen käytettävässä tilassa (PolL 5:13.4 ja PKL 10:12.4). Tämä tukee sitä, ettei sosiaalisen median ryhmää tule pitää siinä mielessä erityisesti suojattuna tilana, joka nauttisi ”tietoverkkojen kotirauhan” osalta laajempaa suojaa kuin kotirauhan suojaama alue reaalimaailmassa. Ryhmään liittymisessä yleisvalvonnan tapaan vuorovaikutusta ryhmän ylläpitäjän tai moderaattorin kanssa voidaan pitää tiedonhankintaan liittyvinä ”normaaleina keskusteluina”, jolloin ei puhuta tietyn toimivaltuuden käyttämisestä.[574] Poislukien tilanteet, joissa ryhmään pääseminen edellyttää laajempaa vuorovaikutus ylläpitäjän kanssa.[575]

Tulkinta koskee myös tilannetta, jossa kohdehenkilö sattuisi jäsenenä hyväksymään ryhmään liittymispyynnön. Tällainen toiminta rinnastuu tilanteeseen, jossa poliisimies ei ole nimenomaisesti pyrkinyt vuorovaikutukseen kohteen kanssa, vaan aloite vuorovaikutukseen tullut ennemminkin kohdehenkilöltä. Tämä sen takia, että pääsääntöisesti ylläpitäjä ja moderoija hyväksyvät jäsenet ryhmään, eikä poliisimies välttämättä tiedä ryhmän

[573] Selkeimpänä esimerkkinä voidaan mainita seuranhaku palvelu Tinder, joka perustuu juurikin aktiivisen toisten profiilien selailuun.
[574] HE 57/1994 vp, s. 15 ja 56.
[575] Ks. Poliisihallitus 2017c, s. 5, jonka mukaan laaja vuorovaikutus ylläpitäjän tai ”portinvartijan” kanssa vaatii peitellyn tiedonhankinnan edellytysten täyttymistä.

asetuksia.[576] Tilanne voisi rinnastua reaalimaailmassa tilanteeseen, jossa kohdehenkilö menee sisälle kahvilaan ennen tarkkailua suorittavaa poliisimiestä, mutta jääkin pitämään ovea auki perässä sisään tulevalle poliisimiehelle. Jos poliisimies vain kiittää oven auki pitämisestä ja sisään päästämisestä, on kyseessä vuorovaikutuksen keinoin tilanteesta vetäytymisestä, vaikka molemmat päätyvät sisälle kahvilaan.[577]

Tilannetta voidaan arvioida toisin silloin, jos kohdehenkilö toimii ryhmän ylläpitäjänä tai moderaattorina. Tällöin poliisimiehen voidaan katsoa pyrkivän tietoisesti vuorovaikutukseen kohdehenkilön kanssa, jotta hän pääsisi mukaan ryhmään. Tämän seurauksena toimintaa voidaan pitää jo vähintään peiteltynä tiedonhankintana (PolL 5:15 ja PKL 10:14). Niin kuin tutkimuksessa on tuotu esille, huomioon tulee kuitenkin ottaa ryhmän koko. Voidaan katsoa, että lainsäädäntö jättää etenkin laajojen useita satoja jäseniä sisältävän ryhmien kohdalla tilaa toisenlaisellekin tulkinnalle. Siinä pelkkä ryhmään pääsyn yrittäminen tilanteessa jossa kohdehenkilö on moderaattorina tai ylläpitäjänä, olisi kuitenkin vain tarkkailua. Mitä pienemmästä ryhmästä on kyse, sitä todennäköisemmin kyseeseen voi tulla peitetoiminta (PolL 5:28 ja PKL 10:27). Tällainen voi olla esimerkiksi kymmenen toisilleen tutun henkilön ryhmä, johon poliisimies pyrkii tavalla tai toisella peiteprofiilillaan. Tällöin ryhmän koon takia voidaan katsoa kyseessä olevan jo soluttautumistyylisen toiminnan.[578] Myös yksittäisen profiilin kaverilistalle pyrkiminen tulee nähdä mieluummin peitetoimintana kuin tarkkailuna, vaikka poliisimies ei sinänsä pyrkisikään muutoin vuorovaikutukseen kohteen kanssa. Tähän voidaan kuitenkin nähdä poikkeuksena tilanteet, joissa kyseinen yksittäinenkin profiili omaa julkisen luonteen.[579]

### 7.3 Suunnitelmallinen tarkkailu

[576] Jos ryhmän asetukset ovat sellaiset, että ylläpitäjien ja moderaattorien lisäksi myös jäsenet pystyvät hyväksymään jäseniä, ei kyseisillä jäsenillä ole yleensä kovinkaan suuria intressejä seurata ketä ryhmään liittyy. Etenkin kun ylläpitäjä on ulkoistanut hyväksymisen kaikille jäsenille. Jos kohdehenkilö alkaa kuitenkin kyselemään ryhmään liittymisen tarkoitusta syystä tai toisesta, tulee tilanteesta vetäytyä mahdollisimman nopeasti, ettei kyseinen tilanne muutu peitellyn tiedonhankinnan toimivaltuutta vaativaksi. Toisaalta vuorovaikutus vetäytymisessä saa tapahtua myös siten, että pyrkii sisälle ryhmään joka tapauksessa ja passivoituu tämän jälkeen.

[577] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325.

[578] Vrt. Poliisihallitus 2017c, s. 5, jossa katsotaan että suppeassa muutaman hengen ryhmässä tapahtuva toiminta voitaisiin katsoa vielä tarkkailuksi tai suunnitelmalliseksi tarkkailuksi.

[579] Tällaisia voivat olla esimerkiksi erilaiset julkkisten, yrittäjien ja poliitikkojen profiilit, jotka hyväksyvät kaverilistalleen kaikki halukkaat sekä pitävät yleensä päivitykset muutoinkin avoimesti kaikkien luettavana.

Suunnitelmallisella tarkkailulla tarkoitetaan rikokseen perustellusti syyllistyväksi oletettavaan tai rikoksesta epäiltyyn kohdistuvaa muuta kuin lyhytaikaista tarkkailua (PolL 5:13.2 ja PKL 10:12.2).[580] Edellytyksenä suunnitelmallisen tarkkailun suorittamiseen on rikos, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Lisäksi varkaus tai kätkemisrikos mahdollistaa suunnitelmallisen tarkkailun kohdistamiseen rikoksesta epäiltyyn (PolL 5:13.3 ja PKL 10:12.3). Kyseistä rajaa on perusteltu sillä, että suunnitelmallisella tarkkailulla puututaan henkilön yksityiselämän suojaan. Yleisten edellytysten mukaan suunnitelmallisella tarkkailulla tulee olla poliisilain mukaan erittäin tärkeä merkitys rikoksen estämiselle tai paljastamiselle ja pakkokeinolain osalta rikoksen selvittämiselle.[581]

Suunnitelmallisen tarkkailun määritelmän täyttymistä voidaan arvioida tilanteessa, jossa poliisiprofiililla haetaan kaverilistalle kavereita tai seurataan muutoin tiettyjä sivustoja joiden voidaan katsoa kuuluvan tietylle henkilölle.[582] Jos kaverilistalle hakeutuminen tapahtuu poliisiprofiililla, ei kyseessä ole kohteelta salassa pidettävä toiminta ja henkilö voi esimerkiksi poistaa vapaasti nettipoliisin kaverilistaltaan. Jos taas kyseessä on peiteprofiili, tilanne muuttuu. Jos tietyn henkilön toimintaan seurataan tietoverkossa häneltä salaa tiedonhankintatarkoituksessa muuten kuin lyhytaikaisesti, tulee suunnitelmallisen tarkkailun edellytysten täyttyä. Lisäksi voidaan mainita erilaisia teknisiä mahdollisuuksia seurata kohdehenkilön viestintään, joista esimerkkinä voidaan mainita RSS-syötteen (Really Simple Syndication) avulla tapahtuva seuraaminen tai esimerkiksi www.blogit.fi palvelun kautta, jossa voi valita seurattavia blogeja listalleen.[583] Jos kyseinen seuraaminen tapahtuu poliisitausta kohteelta salaten voi kyseeseen tulla suunnitelmallinen tarkkailu.

Niin kuin edellisessä tarkkailua koskevassa kohdassa on käyty läpi, muun kuin suunnitelmallisen tarkkailun kohteena olevan henkilön tarkkailu on mahdollista niissä tapauksissa, joissa oikea suunnitelmallisen tarkkailun kohde pyritään varmistamaan muiden ihmisten joukosta. Toisaalta kyseeseen voi tulla myös tilanne, jossa tietyn henkilön tiedetään toimittavan pakoilua varten varoja esitutkintaa karttavalle rikoksesta epäillylle, jolloin tätä henkilöä voidaan seurata piilopaikkaan epäillyn tavoittamiseksi. Toimenpiteen tulee

[580] Suunnitelmallista tarkkailua on käytetty erityisesti törkeiden huumausainerikosten selvittämiseen ja paljastamiseen. Vuosittaiset määrät ovat vuoden 2014 uudistuksen jälkeen olleet kahden sadan paikkeilla. Ks. Poliisihallitus 2018c, s. 19 ja 21.
[581] HE 224/2010 vp, s. 102–103; HE 222/2010 vp, s. 326.
[582] Tällaisia voi olla esimerkiksi tietyt fanisivut Facebookissa tai tietyn henkilön blogi.
[583] RSS-syöte mahdollistaa seurata sitä, kun tietylle internetsivustolle julkaistaan uutta sisältöä.

kuitenkin olla yksittäinen ja lyhytkestoinen.[584] Suunnitelmallista tarkkailua suoritetaan tarkkailun tapaan kohteelta salassa ja tyypillistä suunnitelmalliselle tarkkailulle on sen seuraaminen, mitä kohdehenkilö tekee ja keitä hän tapaa. Hänen elämäänsä siis seurataan jonkin aikaa. Suunnitelmallisella tarkkailulla ei ole esitöiden mukaan olemassa mitään vähimmäiskestoa, koska tarkkailuun vaadittava vähimmäisaika riippuu tapauskohtaisista olosuhteista. Tarkkailu voi muuttua suunnitelmalliseksi tarkkailuksi myös lyhytkestoisena, jos se toistuu jonkin ajan kuluttua. Lyhytkestoisuuden arvioinnin kannalta merkityksellistä on siten ensimmäisen ja viimeisen tarkkailutoimenpiteen välinen aika.[585] Suunnitelmalliseen tarkkailuun liittyen esitöissä todettiin, että tarkoitus oli täsmentää tarkkailun määritelmän tavoin tuolloin epäselvää lainsäädäntötilannetta. Käytännössä tilanne ei kuitenkaan selkeytynyt, jonka takia pakkokeinolain uudistusta koskien perustuslakivaliokunta kiinnitti asiaan huomiota. Perustuslakivaliokunta katsoi, että tarkkailun eroaminen suunnitelmallisesta tarkkailusta sen perusteella, että se on ”muuta kuin lyhytaikaista tarkkailua” vaatisi täsmentämistä.[586] Kyseinen täsmentäminen ei kuitenkaan syystä tai toisesta realisoitunut.

Jo aikaisemman vuoden 1995 poliisilain aikana voimassa olleen ja nykyistä suunnitelmallista tarkkailua pääosin vastaavan tarkkailun määritelmä ”jatkuvuudesta ja toistuvuudesta” aiheutti tulkintaongelmia, jonka takia poliisi- ja pakkokeinolain uudistuksessa tämä puute piti korjata.[587] Vuoden 2009 komiteamietinnössä ei ollut vielä puhetta suunnitelmallisesta tarkkailusta, vaan käytettiin pelkkää tarkkailun määritelmää. Jatkuvuuden tuli jatkossa katsoa tarkoittavan enintään muutaman kymmenen minuutin kestoa ja toistuvuuden muutaman tiedonhankintakerran.[588] Komiteamietintövaiheessa toiminnan jatkuvuuden ja toistuvuuden korvaavana määritelmänä aiottiin käyttää muotoa ”muuta kuin satunnaista”, jolla olisi suljettu sääntelyn piiristä pois satunnaiset tiedonhankintatilanteet.[589] Tarkoituksena oli saattaa sääntelyn piiriin suunnitellut tarkkailutilanteet, joissa tarkkailutapahtuma ei välttämättä kestänyt kuin kymmenen minuutin ajan, mutta jotka olivat etukäteen suunniteltuja. Jatkuvuudella olisi ollut jatkossa

[584] HE 224/2010 vp, s. 102; HE 222/2010 vp, s. 325–326.
[585] HE 224/2010 vp, s. 34 ja 102; HE 222/2010 vp, s. 117 ja 325–326.
[586] PeVL 66/2010 vp, s. 8.
[587] Ks. tarkkailua koskevan sääntelyn alkuperäisestä tarkoituksesta ja sisällöstä tarkemmin HE 57/1994 vp, s. 21.
[588] Komiteamietinnön mukaan aikaisemmin jatkuvuuden ja toistuvuuden käsitteiden oli katsottu tarkoittavan muutamien tuntien kestoa ja jälkimmäisen tätä aikaa lyhyempää ajanjaksoa, jotka yhteenlaskettuna muodostaisivat muutamien tuntien keston.
[589] Esimerkkinä satunnaisesta tapahtumasta mainittiin poliisimies, joka torilla kävellessään kiinnittää huomiota henkilön käyttäytymiseen ja päättää tarkkailla tätä rikoksen selvittämiseksi.

huomattavasti lyhyempi kesto. Kysymyksessä olisi voinut olla jatkossa enintään muutaman kymmenen minuutin mittainen ajanjakso. Toistuvuuden osalta taas katsottiin, että jos tarkkailu toistettaisiin muutaman kerran ja vaikka niiden yhteenlaskettu kesto ei ylittäisikään mainittua muutaman kymmenen minuutin ajanjaksoa, olisi kyseessä kuitenkin tarkkailu.[590] Kyseisiä rajoja ei kuitenkaan mainittu nykyisten poliisi- ja pakkokeinolakien esitöissä.

Poliisihallitus on päätynyt omassa tulkinnassaan ratkaisuun, jossa tarkkailusta siirrytään suunnitelmalliseen tarkkailuun, jos tarkkailukertoja on noin viisi erillistä kertaa tai yksittäinen tarkkailutapahtuma jatkuu enemmän kuin vuorokauden.[591] Sama koskee myös tietoverkoissa tapahtuvaa tarkkailua, vaikka linjausta onkin osittain haastavampi soveltaa kyseiseen toimintaympäristöön.[592] Poliisihallituksen linjaus näyttää ainakin komiteamietintöön verrattuna lievemmältä tulkinnalta, jossa raja suunnitelmalliseen tarkkailuun on pidempi. Oli Poliisihallituksen tulkinnasta samaa tai eri mieltä voidaan kuitenkin perustellusti kysyä, miksi lainsäätäjä ei ole kyennyt luomaan kyseisenlaisia selviä tarkkarajaisempia ja täsmällisempiä rajoja säännökseen? Etenkin kun rajan määrittely oli haasteellinen jo vanhan poliisilain aikana ”jatkuvuuden” ja ”toistuvuuden” käsitteiden takia.[593] Jos kyseistä 24h/5krt -linjausta pyritään tarkastelemaan tietoverkoissa, on näistä selvempi tilanne jossa yksittäistä profiilia tarkkaillaan yli 24h yhtäjaksoisesti. Tällainen tarkkailu voi tapahtua esimerkiksi poliisimiehen toimesta reaaliaikaisesti päivityksiä tai suoraa videolähetystä seuraamalla.[594] Toisaalta on myös mahdollista seurata päivitysvirtaa algoritmien antamien ilmoitusten perusteella, joka voi jatkua pitkäänkin.[595]

---

[590] Sisäministeriö 2009a, s. 197 ja 462. Tarkkailun sääntelyn tiukentamiseen kiinnitettiin huomiota lausuntovaiheessa suojelupoliisin toimesta. Ks. lausuntotiivistelmään liittyen Sisäministeriö 2009b, s. 161.

[591] Poliisihallitus 2016b, s. 24.

[592] Poliisihallitus 2017c, s. 4.

[593] Hallituksen esityksissä suunnitelmallista tarkkailun katsottiin kuitenkin täsmentäneen silloista epäselvää oikeustilaa, jonka takia sääntelyn katsottiin olevan täsmällistä ja kattavaa. Ks. HE 224/2010 vp, s. 177; HE 222/2010 vp, s. 386. Vrt. tähän liittyen jo aikaisemmin mainittu perustuslakivaliokunnan kritiikki PeVL 66/2010 vp, s. 8, joka ei kuitenkaan näyttänyt aiheuttavan toimenpiteitä. Todettakoon vielä, että muutoin poliisi- ja pakkokeinolaista löytyy useita erilaisia tarkkoja rajoja, jotka määrittävät poliisin toimintaa. Näin on esimerkiksi pidättämisen ja vangiksi vaatimisen sääntely (PKL 2:7 ja 3:4).

[594] Käytännössä tällainen toiminta on tuskin operatiivisesti järkevää kuin erittäin harvoissa akuuteissa tilanteissa. Tällainen voisi olla esimerkiksi piiritystilanne, jossa henkilö olisi linnoittautuneena asuntoon tai kouluun ja linnoittautuneen henkilön eri profiilien liikennettä seurataan koko piiritystilanteen ajan. Ks. esimerkiksi The Press 2019, jossa mies oli linnoittautunut kotiinsa yhdeksän tunnin ajaksi ja striimasi suorana lähetyksenä videota tapahtumista sosiaaliseen mediaan. Poliisin pystyi kyseisen videolähetyksen avulla ajoittamaan rynnäkön sisälle asuntoon.

[595] Ks. esimerkiksi Campus Safety 2018, jossa kerrotaan Virginian Yliopiston poliisin ottaneen käyttöön ohjelman nimeltä Social Sentinel, jolla he valvovat oppilaiden sosiaalisen median käyttöä. Kyseisen ohjelman avulla voi säätää erilaisiin algoritmeihin perustuvia ”hälytyksiä” päivityksiin liittyen. Toimita ei tosin liity suoraan poliisi- ja peiteprofiileihin.

> Aiheeseen liittyen mielenkiintoinen oli tapaus, jossa yhdenvertaisuusvaltuutettu seurasi vuoden 2017 kuntavaalien alla tiettyjen ehdokkaiden julkisia Twitter- ja Facebook-viestejä tietokoneistetun algoritmin perusteella ja niistä seulottiin mahdollisia vihapuheita sisältäviä viestejä. Vaikka asiasta oli tiedotettu yleisesti, käytännössä ehdokkailla itsellään ei välttämättä ollut mitään tietoa seurannasta, joten toiminta tapahtui ainakin osittain salaa.[596] Seurannan perusteella yhdestä ehdokkaasta tehtiin rikosilmoitus.[597] Poliisin toimintana kyseessä olisi ollut tiettyihin ehdokkaisiin kohdistunut suunnitelmallinen tarkkailu. Yhdenvertaisuuslaista (1325/2014) tai yhdenvertaisuusvaltuutetusta annetusta laista (1326/2014) ei tällaista toimivaltuussäännöstä löydy.[598] Koska yhdenvertaisuusvaltuutettu on viranomainen näyttää siltä, että kyseisessä asiassa olisi toimittu ilman nimenomaista toimivaltuutta. Tämä sen takia, että jos yleisluonteisten tehtävien ja toimivaltuuksien katsottaisiin soveltuvan suunnitelmalliseen tarkkailuun toimivaltuutena, niin teoriassa yhdenvertaisuusvaltuutettu voisi käyttää myös kaikkia muita salaisia tiedonhankinta- ja pakkokeinoja yhdenvertaisuuden edistämiseen ja syrjinnän ehkäisyyn.[599]

Arvioitaessa reaalimaailmaan paremmin soveltuvaa viiden tarkkailukerran vaatimusta on tilanne epäselvempi. Onko esimerkiksi profiilin klikkaaminen yli viisi kertaa, viiden eri blogauksen tarkastelu yksittäisen henkilön blogilta, kohdehenkilön viidessä eri palvelussa sijaitsevan profiilin tarkastelu, tai yli viisi kertaa päivän aikana profiilissa vierailu jo suunnitelmallista tarkkailua? Selvemmin tarkkailun puolelle jäävät tilanteet, joissa yksittäisen profiilin eri tietoja klikkaillaan auki useita kertoja yksittäisen tarkastelukerran aikana. Yksittäistä profiilissa vierailua, jossa käydään läpi profiilin tietoja, päivityksiä ja alasivuja ei siten pidä laskea eri tarkkailukerroiksi klikkauksien määrän mukaisesti. Tarkkailun puolelle jäävät mielestäni myös tilanteet, joissa poliisi käy hankkimassa tietoa saman tarkastelukerran aikana useista eri palveluista samasta kohdehenkilöstä. Eli vaikka henkilöllä olisi kuusi eri profiilia eri palveluissa, näissä vierailu on vielä katsottava yksittäiseksi tarkkailukerraksi. Lisäksi voidaan tulkita 24 tunnin rajausta siten, että yksittäiseksi tarkastelukerraksi tulee laskea myös vuorokauden sisällä tapahtuneet useat

[596] Kyseinen julkinen tieto siitä, että ehdokkaisiin kohdistuu valvontaa ei vielä poista salassapitoelementtiä. Poliisi voi esimerkiksi todeta, että se seuraa rikollisia moottoripyöräjengien jäseniä, mutta tämä ei poista suunnitelmallisesta tarkkailusta salassapitoelementtiä yksittäisen jengiläisen kohdalla. Voidaan myös ottaa huomioon, että valvonta ei kohdistunut kaikkiin yli 30 000:een kuntavaaliehdokkaaseen.
[597] Ks. asiasta tehty kirjallinen kysymys 468/2017 vp ja vastaus siihen KKV 468/2017 vp.
[598] Yhdenvertaisuuslain 19 §:n mukaan yhdenvertaisuusvaltuutettu tehtävänä ja toimivaltuuksina on lähinnä avustaa, antaa yleisiä suosituksia, sovitella ja antaa tarvittaessa kannanottoja yksittäistapauksissa.
[599] Asiaa ei voi perustella yhdenvertaisuusvaltuutetusta annetun lain 3 §:n mukaisilla tehtävillä, koska ne rinnastuvat PolL 1:1:n mukaisiin poliisin tehtäviin, jotka eivät ole toimivaltuussäännöksiä. Tilanteeseen ei myöskään vaikuta se, että toimintaa suoritettiin yhteistyössä kolmannen sektorin tahojen kanssa, koska viranomainen ei voi kiertää toimivaltuussäännöksiä muita ohjaamalla.

tarkastelukerrat. Käytännössä tämä vastaa korkeintaan yksittäisen poliisimiehen yksittäisen työvuoron aikana tapahtuvaa tarkastelua.[600] Jos tiedonhankintaa suoritetaan enemmän kuin viitenä eri tarkastelukerralla, jotka on suoritettu eri päivinä, tulisi toiminta tulkita suunnitelmalliseksi tarkkailuksi.

Reaalimaailmassa tarkkailun suhdetta suunnitelmalliseen tarkkailuun on arvioitu edellä vain 1) *tarkkailukertojen* ja 2) *tarkkailun keston* perusteella. Niin kuin tutkimuksen alussa käsiteltäessä yksityiselämän suojaa on tuotu esille, eroaa reaalimaailman ja tietoverkkojen suojan tarve toisistaan. Tämän takia tietoverkoissa tarkastelua tulisi tehdä myös 3) *tiedon keräämistavan ja laajuuden* perusteella. Tämä koskee tapauksia, joissa kohdehenkilöstä voidaan tallentaa laajasti tietoa erilaisin teknisin sovelluksin. Kyseisen tiedonhankinnan perusteella poliisille voi syntyä laaja staattinen tietomassa. Tietomassaa jälkikäteen useita kertoja tarkastelemalla ja analysoimalla voidaan tehdä erilaisia havaintoja kohdehenkilöstä siten, että Poliisihallituksen määrittelemät rajat suunnitelmallisesta tarkkailusta täyttyisivät, jos kyseessä olisi henkilön varsinaisen profiilin tarkastelu. Tältä osin voidaan tosin ottaa huomioon yksityiselämän suojaa tietoverkoissa suhteessa reaalimaailmaan heikentävät elementit. Voidaan tuoda esille myös se, että poliisilla voi olla hyvinkin laajasti jo valmiina tietoja omissa rekistereissä, tai muissa rekistereissä, joihin sillä on pääsy PolL 4:3:n perusteella. Lisäksi erilainen koneellinen tietojen kerääminen ei välttämättä liity poliisi- ja peiteprofiileihin. Joka tapauksessa laajan tietomassan keräämismahdollisuus tulisi huomioida lainsäädännössä nykyistä paremmin.

### 7.4 Peitelty tiedonhankinta

Peitellyllä tiedonhankinnalla tarkoitetaan tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa poliisimiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja (PolL 5:15.1 ja PKL 10.14.1).[601] Peitelty tiedonhankinta lisättiin poliisi- ja pakkokeinolakiin vuoden 2014 kokonaisuudistuksessa. Aikaisemmassa lainsäädännössä oli epäselvää, miten tulisi arvioida lyhytkestoista ja toistumatonta soluttautumista. Tällaisen toiminnan katsottiin voivan olla hyvin

[600] Tällä tarkoitan sitä, että jos poliisimies esimerkiksi vierailee kohdehenkilön profiileissa työvuoron alussa ja palaa tarkastamaan profiilit vielä työvuoron lopussa, tulee tämä laskea yksittäiseksi tarkkailukerraksi.
[601] Lisäksi pakkokeinolain säännöksessä mainitaan mahdollisena peitellyn tiedonhankinnan suorittajana Tullin rikostorjunnan tullimies. Erityiset edellytykset perustuvat kuitenkin Tullin tehtäväkenttään kuuluviin rikoksiin (PKL 10:14.3).

suunnitelmallista ja pitkällistä taustatyötä vaativaa, vaikka kyseessä oli vain kymmenen minuutin tapaaminen. Tämän takia laissa haluttiin säätää lyhytkestoisesta peitetoimintatyyppisestä tiedonhankinnasta, jossa toimitaan vuorovaikutuksessa.[602]

Poliisilaissa peitelty tiedonhankinta on mahdollista rikoksen estämiseksi, jos henkilön lausumien tai muun käyttäytymisen perusteella voidaan perustellusti olettaa hänen syyllistyvän 1) rikokseen, josta ankarin rangaistus on vähintään neljä vuotta vankeutta, 2) seksikaupan kohteena olevan henkilön hyväksikäyttöön tai paritukseen, 3) huumausainerikokseen, 4) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun taikka kouluttautumiseen terrorismirikoksen tekemistä varten, terroristiryhmän rahoittamiseen tai matkustamiseen terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta, 5) törkeään tulliselvitysrikokseen tai 6) suunnitelmalliseen, järjestäytyneeseen, ammattimaiseen, jatkuvaan tai toistuvaan rikolliseen toimintaan liittyvään varkauteen tai kätkemisrikokseen (PolL 5:15.2). Pakkokeinolaissa peitellyn tiedonhankinnan edellytyksenä on poliisilaissa mainittujen rikosten lisäksi 7) panttivangin ottamisen valmistelu ja 8) törkeän ryöstön valmistelu. Pakkokeinolain mukaisesti tulee olla syytä olettaa, että toimenpiteellä saadaan selvitystä kyseisestä rikoksesta (PKL 10:14.2).[603] Peitellystä tiedonhankinnasta päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka STEKPOV (PolL 5:16.1 ja PKL 10:15.1).[604] STEKPOV-vaatimus perustuu siihen, että peitellyn tiedonhankinnan ja peitetoiminnan ero tunnistetaan eikä peiteltyä tiedonhankintaa käytetä tilanteissa, joissa tosiasiallisesti on kyse peitetoiminnasta. Lisäksi erityisen koulutuksen vaatimuksella pyritään vähentämään rikosprovokaation ja tiedonhankinnan paljastumisen riskiä sekä edistämään toiminnan tuloksellisuutta.[605]

---

[602] HE 224/2010 vp, s. 37; HE 222/2010 vp, s. 119.

[603] Peitelty tiedonhankinta ei ole sallittua asunnossa riippumatta siitä, myötävaikuttaako asunnonhaltija asiaan vai ei (PolL 5:15.3 ja PKL 10:14.4). Pois lukien tilanteet, joissa poliisi esimerkiksi esiintyy lähettinä ja lähetyksen vastaanottaja pyytää lähetystä kuitatessaan hänet eteiseen odottamaan. Ks. HE 224/2010 vp, s. 105; HE 222/2010 vp, s. 328. Vrt. kuitenkin Tullin rikostorjuntalakia (623/2015) koskeva PeVL 49/2014 vp, s. 3. Siinä perustuslakivaliokunta toteaa, että edes lyhytaikainen asunnossa käynti ei ole sallittua peitellyssä tiedonhankinnassa. Syynä lausumaan oli HE 174/2014 vp toteamus, että tiedonhankinnan paljastumisen estämiseksi toimintaan saattoi tapauskohtaisesti liittyä tarve käydä lyhytaikaisesti asunnossa. Vaikka asiassa viitattiin PolL 5:15.3 ja PKL 10:14.4 sääntelyyn, ei esitöissä otettu poliisi- ja pakkokeinolakia koskevaa esimerkkiä eteisessä odottamisesta huomioon.

[604] Ks. päätöksen sisältö- ja muuttamisvaatimuksista PolL 5:16.2–3 ja PKL 10:15.2–3. Ks. myös tarkemmin muutostarpeisiin liittyen HE 224/2010 vp, s. 105; HE 222/2010 vp, s. 328. Esitöissä päätöksentekijä velvoitetaan seuraamaan edellytysten olemassaoloa ja tiedonhankinnan tarpeellisuutta erityisesti silloin, kun päätöksentekohetki ja tiedonhankinnan toteuttaminen eroavat ajallisesti paljon toisistaan.

[605] HE 224/2010 vp, s. 104; HE 222/2010 vp, s. 327–328.

Peitellyn tiedonhankinnan esimerkkinä esitöissä mainitaan tilanne, jossa rikollisryhmä tilaa taksin, jota tosiasiallisesti kuljettaa poliisimies ja mainittu henkilö on ryhmän mukana. Peiteltynä tiedonhankintana voidaan pitää myös tilannetta, jossa tietylle henkilölle tarkoitettu lähetys toimitetaan perille lähettinä esiintyen, jolloin on mahdollista, että lähetyksen ottaa vastaan muu kuin kohteena oleva henkilö. Edelleen esimerkkinä mainitaan tilanne, jossa poliisimies on tekeytynyt tarjoilijaksi ja harjoittaa tiedonhankintaa ravintolassa kohdehenkilön läheisyydessä. Peitellyllä tiedonhankinnalla ei ole olemassa mitään tarkkaa aikarajaa, koska on mahdollista, että vuorovaikutuksen toinen osapuoli pitkittää tilannetta vaikka tiedonhankinnan tavoite olisi jo saavutettu. Tällöin epäluonteva irtautuminen tilanteesta voi paljastaa tiedonhankinnan. Tilanteiden uskottavuuden mahdollistamiseksi toiminnan luonteeseen kuuluu PolL 5:46:n ja PKL 10:47:n mukaisesti erilaisten väärien, harhauttavien ja peiteltyjen tietojen käyttäminen. Näitä ovat esimerkiksi eri yhtiöiden haalarien ja nimikylttien käyttäminen.[606]

Tarkkailuun ja suunnitelmalliseen tarkkailuun verrattuna peitelty tiedonhankinta eroaa siten, että peitellyssä tiedonhankinnassa on luonteenomaista pyrkimys henkilökohtaiseen tapaamiseen tai vastaavaan vuorovaikutustilanteeseen tiedonhankinnan kohteen kanssa. Vuorovaikutusta ei saa viedä niin pitkälle, että kyseessä olisi peitetoiminta, jossa pyritään muodostamaan erityinen luottamussuhde kohteeseen. Kyse ei siis ole soluttautumisesta, vaan pikemminkin yksittäisestä tiedonhankintatapahtumasta.[607] Vaikka toimenpiteenä oleva rikos tuleekin mainita, tulee huomioida että vuorovaikutuksen kohteena voi olla joku muukin kuin kohdehenkilö. Peitellyssä tiedonhankinnassa toteuttamisajankohtaa ei tarvitse mainita kellonajan tarkkuudella, koska kyse on ennemmin yksittäisen toimenpiteen suorittamisesta sopivana ajankohtana. Erilaiset rajoitukset ja ehdot voivat johtua esimerkiksi suhteellisuusperiaatteesta sekä tarkoituksenmukaisuus-, oikeusturva- ja työturvallisuusnäkökohdista.[608] Tietoverkoista lainvalmisteluaineistosta ei löydy kannanottoja lainkaan.

Tietoverkkojen, mutta myös reaalimaailman osalta, peitellyn tiedonhankinnan käyttö on jäänyt todella vähäiseksi. Vuosittaisen PolL 5:63.2:n ja PKL 10:65.2:n mukaisen salaisia

[606] HE 224/2010 vp, s. 103–104; HE 222/2010 vp, s. 327. Tulee huomioida, että säännös ei mahdollista asiakirjojen valmistamista tai rekisterimerkintöjen tekemistä. Jos näitä halutaan käyttää peitellyssä tiedonhankinnassa, tulee noudattaa PolL 5:46 ja PKL 10:47 mukaista suojaamissääntelyä koskevia edellytyksiä. Peitellyn tiedonhankinnan osalta ei kuitenkaan tarvitse tehdä erillistä suojaamissääntelyyn perustuvaa päätöstä väärien, harhauttavien ja peiteltyjen tietojen osalta.
[607] HE 224/2010 vp, s. 104; HE 222/2010 vp, s. 327.
[608] HE 224/2010 vp, s. 104–105; HE 222/2010 vp, s. 328.

tiedonhankinta- ja pakkokeinoja koskevan kertomuksen mukaan peitellystä tiedonhankinnasta tehdään vuosittain vain muutamia päätöksiä. Syyksi tähän mainitaan korkea perusterikoskynnys, jonka Poliisihallitus toivoo laskettavan neljästä vuodesta kahteen vuoteen.[609] Vuoden 2014 kokonaisuudistuksen myötä poliisi- ja pakkokeinolakiin säädettyä uutta toimivaltuutta ei voidakaan pitää kovin onnistuneena. Erityisesti tämä koskee tietoverkkojen osuutta, koska varsinaisessa peitetoiminnassa raja on tietoverkoissa laskettu kahteen vuoteen (PolL 5:28.3 ja PKL 10:27.3).[610] Tietoverkkojen kohdalla onkin epäloogista, että tilanteissa joissa on mahdollisuus peitetoimintaan, ei välttämättä ole mahdollisuutta vähemmän perus- ja ihmisoikeuksiin puuttuvaan peiteltyyn tiedonhankintaan. Peiteltyyn tiedonhankintaan liittyy kuitenkin aivan samat jo erityisiä edellytyksiä käsiteltäessä esille tuodut sääntelyyn vaikuttavat seikat. Näitä ovat tietoverkkojen anonyymi luonne, dokumentoinnin helppous ja tarkkuus sekä vähäisemmät turvallisuusriskit.[611]

Voidaan myös kritisoida sitä, että peitelty tiedonhankinta on sijoitettu tarkkailutyyppisiin keinoihin, vaikka kyse on vuorovaikutukseen perustuvasta tiedonhankinnasta. Tämän takia se onkin tässä tutkimuksessa luettu erityisiin toimivaltuuksiin. Ottaen huomioon tutkimuksessa esille tuodut erot yksityiselämän suojan tarpeessa reaalimaailman ja tietoverkkojen välillä tulisi *de lege ferenda* arvioida, olisiko suunnitelmalliseen tarkkailun säännökseen mahdollisuus sisällyttää peitellyn tiedonhankinnan kaltaiset yksittäiset vuorovaikutuksen sisältävät tilanteet erityisesti tietoverkoissa. Joka tapauksessa peitellyn tiedonhankinnan erityisten edellytysten rajaa tulisi laskea nykyisestä neljästä vuodesta erityisesti tietoverkkojen osalta Poliisihallituksen toiveiden mukaisesti.[612] Tietoverkoissa kyseinen muutos tarkoittaisi sitä, ettei olisi tarvetta käyttää raskaahkoa peitetoimintalupaa esimerkiksi hetkellisessä kohdehenkilön kaverilistalle hakeutumisessa, jossa käydään taltioimassa hänen viestintää ja muita tietoja.[613] Jos kyseisenkaltaisessa tilanteessa pyrittäisiin vain saamaan paremmat tarkkailumahdollisuudet kaverilistan kautta, eikä tarkoituksena olisi pidempiaikainen soluttautumiseen liittyvä vuorovaikutus kohteen kanssa, voisi tämä sisältyä vielä suunnitelmallisen tarkkailun sääntelyyn. Tällä hetkellä kyseinen

[609] Poliisihallitus 2018c, s. 19. Ks. myös Poliisihallitus 2017a, s. 26, jossa on identtinen teksti vuoden 2018 kertomuksen kanssa.
[610] Etenkin kun otetaan huomioon, että myös varsinainen peitetoiminta voi olla lyhytkestoista. Ks. HE 224/2010 vp, s. 114; HE 222/2010 vp, s. 337.
[611] HE 224/2010 vp, s.116; HE 222/2010 vp, s. 339.
[612] Ks. Poliisihallitus 2018c, s. 19, jonka mukaan peiteltyä tiedonhankintaa käytetään vain muutaman kerran vuosittain erityisten edellytysten takia.
[613] Reaalimaailmassa muutoksella olisi laajemmat vaikutukset ja se mahdollistaisi tarkkailutoiminnassa yksittäisten vuorovaikutustilanteiden tehokkaamman käytön. Näitä voisi olla suunnitelmallisen tarkkailun yhteydessäkin useita, koska vuorovaikutustilanteissa olisi mahdollisuus käyttää useita eri poliisimiehiä.

toiminta voidaan katsoa peitellyksi tiedonhankinnaksi lyhytkestoisena toimenpiteenä ja peitetoiminnaksi, jos kaverilistalle jäädään seuraamaan toimintaa pidemmäksi aikaa.

### 7.5 Peitetoiminta

Peitetoiminnalla tarkoitetaan tiettyyn henkilöön tai hänen toimintaansa kohdistuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistetaan tai käytetään vääriä asiakirjoja (PolL 5:28.1 ja PKL 10:27.1).[614] Poliisilain mukaan poliisi saa kohdistaa rikoksen estämiseksi peitetoimintaa henkilöön, jos henkilön lausumien tai muun käyttäytymisen perusteella voidaan perustellusti olettaa hänen syyllistyvän tai myötävaikuttavan PKL 10:3:ssä tarkoitettuun muuhun rikokseen kuin törkeän laittoman maahantulon järjestämiseen tai törkeään tulliselvitysrikokseen taikka jos tämän voidaan perustellusti olettaa syyllistyvän tai myötävaikuttavan RL 17:18.1,1:n mukaiseen sukupuolisiveellisyyttä loukkaavaan lasta esittävän kuvan levittämiseen (PolL 5:28.2). Pakkokeinolaissa perusteet ovat samat, mutta kyse on rikoksen selvittämisestä ja rikoksesta epäiltyyn kohdistettavasta peitetoiminnasta (PKL 10:27.2).

Tietoverkoissa peitetoiminnan erityisten edellytysten raja on alhaisempi, koska edellytyksenä on vain kahden vuoden rangaistusmaksimi tai vaihtoehtoisesti RL 17:19:ssä tarkoitettu sukupuolisiveellisyyttä loukkaavan lasta esittävän kuvan hallussapito. Poliisilain mukaan tulee henkilön lausumien tai muun käyttäytymisen perusteella voida perustellusti olettaa hänen syyllistyvän kyseiseen rikokseen ja pakkokeinolain kohdalla tulee olla syytä epäillä kyseistä rikosta (PolL 5:28.3 ja PKL 10.27.3).[615] Tietoverkkoja ei koske PolL 5.28.2:n ja PKL 10:27.2:n mukainen lisäedellytys, että tiedonhankintaa on rikollisen toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena.[616] Tietoverkkoihin liittyen lainsäädännössä ei ole lievennyksiä yleisissä edellytyksissä, joten myös

[614] Peitetoimintaa on käytetty lähinnä törkeiden huumausainerikosten paljastamiseen, mutta vuotta 2017 koskevassa Poliisihallituksen kertomuksessa mainittiin ensimmäisen kerran myös rahanpesurikokset. Ks. Poliisihallitus 2018c, s. 29.
[615] Lisäksi säännöksessä todetaan, että asunnossa peitetoimintaa ei saa suorittaa kuin asuntoa käyttävän aktiivisella myötävaikutuksella (PolL 5:28.4 ja PKL 10:27.4).
[616] Ks. HE 224/2010 vp, s. 120; HE 222/2010 vp, s. 155.

tietoverkoissa tapahtuvassa toiminnassa tulee PolL 5:2.1:n ja PKL 10:2.1:n mukaisen välttämättömyysvaatimuksen täyttyä.[617]

Peitetoiminnasta on laadittava esitys ja suunnitelma (PolL 5:31.1 ja PKL 10:30.1).[618] Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava (PolL 5:31.2 ja PKL 10:30.2). Pelkästään tietoverkoissa toteutettavasta peitetoiminnasta päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka STEKPOV (PolL 5:32.1 ja PKL 10:31:1).[619] Peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan (PolL 5:32.2 ja PKL 10:31.2).[620] Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava ja peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös (PolL 5:32.2 ja PKL 10:31.3).[621] Pakkokeinolain mukaisesta peitetoiminnasta päättäneen poliisimiehen on saatettava tuomioistuimen ratkaistavaksi, ovatko PKL 10:27.1:ssä tarkoitetut peitetoiminnan edellytykset olemassa (PKL 10:32). Poliisilain kohdalla tämä tulee tarpeelliseksi vain silloin, jos peitetoiminnalla saatua tietoa on tarkoitus käyttää oikeudenkäynnissä syyllisyyttä tukevana selvityksenä, jolloin poliisimiehen on saatettava tuomioistuimen ratkaistavaksi olivatko PolL 5:28.2:ssä tarkoitetut peitetoiminnan edellytykset olemassa, tai oliko kysymys peitetoiminnasta 5:3:ssä tarkoitetuissa tapauksissa (PolL 5:33). Peitetoimintaa koskevaa asiaa varten tuomioistuimelle on toimitettava ainoastaan asian käsittelemiseksi välttämättömät tiedot. Asian käsittelyssä on kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin (PolL 5:45.6 ja PKL 10:43.6).[622]

---

[617] Syynä lievennyksille oli jo aikaisemmin käsitellyt tietoverkon anonymiteetti, dokumentointimahdollisuudet ja peitepoliisin turvallisuus. Ks. HE 224/2010 vp, s. 116; HE 222/2010 vp, s. 149.

[618] Esityksessä on mainittava 1) toimenpiteen esittäjä, 2) tiedonhankinnan kohteena oleva henkilö riittävästi yksilöitynä, 3) toimenpiteen perusteena oleva rikos riittävästi yksilöitynä, 4) peitetoiminnan tavoite, 5) peitetoiminnan tarpeellisuus ja 6) muun peitetoiminnan edellytysten arviointia varten tarvittavat tiedot. Suunnitelma tulee tehdä kirjallisesti ja sen tulee sisältää peitetoimintaa koskevan päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot.

[619] Muutoin päätöksen tekee keskusrikospoliisin tai suojelupoliisin päällikkö.

[620] Päätös on tehtävä kirjallisesti ja siinä on mainittava 1) toimenpiteen esittäjä, 2) peitetoiminnan toteuttava poliisiyksikkö ja peitetoiminnan toteuttamisesta vastaava poliisimies, 3) tunnistetiedot peitetoiminnan suorittavista poliisimiehistä, 4) tiedonhankinnan perusteena oleva rikos, 5) peitetoiminnan kohteena oleva henkilö, jonka voidaan perustellusti olettaa syyllistyvän 4 kohdassa tarkoitettuun rikokseen, 6) tosiseikat, joihin epäily ja peitetoiminnan edellytykset perustuvat, 7) peitetoiminnan tavoite ja toteuttamissuunnitelma, 8) päätöksen voimassaoloaika ja 9) voidaanko peitetoiminnassa tehdä PolL 5:30:ssä tai PKL 10:29:ssä tarkoitettuja toimenpiteitä, ja toimenpiteiden perusteena olevat tosiseikat sekä peitetoiminnan mahdolliset rajoitukset ja ehdot (PolL 5:32.2 ja PKL 10:31.2).

[621] Peitetoiminnasta vastanneen poliisimiehen tulee laatia peitetoiminnan toteuttamisesta EPSA 3:10:n mukainen pöytäkirja ilman aiheetonta viivytystä peitetoiminnan lopettamisen jälkeen.

[622] Käytännössä tämä tarkoittaa sitä, että tuomioistuimelle ei tarvitse toimittaa tietoa siitä kuka on poliisilain mukaisen tiedonhankinnan kohteena tai keitä epäillään rikoksesta pakkokeinolain mukaisessa peitetoiminnassa. Myöskään paikkakunnan ilmoittaminen ei ole tarpeellista. Olennaista ja riittävää on epäillyn rikoksen tai

Peitetoimintaa voi suorittaa yksinomaan tietoverkoissa tapahtuvassa toiminnassa poliisilaitos, mutta muutoin toteuttamisesta vastaa keskusrikospoliisi tai suojelupoliisi (EPSA 3:9.1). Peitetoimintaa suorittavan poliisimiehen toiminta salataan kohteen lisäksi myös ulkopuolisilta.[623] Peitetoiminnan tulee kohdistua joko tiettyyn henkilöön tai henkilöryhmään, mutta ryhmän henkilöt tulee olla yksilöitävissä riittävällä tarkkuudella heidän rooliensa tai tehtäviensä kautta, vaikka henkilöllisyys olisi epäselvä. Selvää on myös se, että jokaisen henkilön kohdalla tulee peitetoiminnan edellytysten täyttyä.[624] Tietoverkoissa henkilön yksilöiminen ja tunnistaminen muodostaa erityisen haasteen niin kuin yksityiselämän suojaa käsiteltäessä on jo tässä tutkimuksessa tuotu aikaisemmin esille. Lähtökohtana voidaan kuitenkin pitää sitä, että jos peitetoiminta kohdistuu tiettyyn profiiliin tai muuhun teleosoitteeseen, on kyseinen kohde riittävällä tavalla yksilöity.[625] Peitetoimintaa voidaan jatkaa niin kauan kuin poliisimies voi olettaa kyseessä olevan sama henkilö tai henkilöt joihin peitetoimintaa koskeva päätös on tehty.[626]

Jos kyseeseen tulee joku muu kuin peitetoiminnan perusterikoksena oleva rikos tai kohteena on joku muu kuin kohdehenkilö, voidaan peitetoimintaa laajentaa PolL 5:34 tai PKL 10:33:n perusteella. Jos peitetoiminnan aikana ilmenee, että voidaan perustellusti olettaa peitetoiminnan kohteena olevan henkilön syyllistyvän sen käyttämisen perusteena olevan rikoksen lisäksi siihen välittömästi liittyvään muuhun kuin PolL 5:28.2:ssä tarkoitettuun rikokseen, jonka estämiseksi on välittömästi tehtävä peitetoimintaa, peitetoimintaa suorittava poliisimies saa laajentaa peitetoiminnan koskemaan myös tämän rikoksen estämistä (PolL 5:34.1). Pakkokeinolaissa sääntely on muutoin sama, mutta siinä viitataan PKL 10:27.2:n perusteisiin ja puhutaan rikoksen selvittämisestä (PKL 10:33.1).[627] Muihin kuin

rikollisen toiminnan kuvaaminen yleisellä tasolla. Asian käsittely on myös mahdollista pitää esimerkiksi poliisin tiloissa. Ks. HE 224/2010 vp, s. 130 ja HE 222/2010 vp, s. 352.

[623] HE 224/2010 vp, s.115; HE 222/2010 vp, s. 338. Ks. myös HE 34/1999 vp, s. 26.

[624] Peitetoiminnalla katsotaan olevan niin merkittäviä vaikutuksia henkilön asemaan ja myös peitepoliisin turvallisuuteen, ettei kohteen rajaamista voida jättää epätarkaksi. Ks. HE 224/2010 vp, s. 115; HE 222/2010 vp, s. 338.

[625] Tätä tulkintaa tukee jo aikaisemmin mainitut telekuunteluun liittyvät esityöt, jossa epäilty voi olla esitutkintaviranomaiselle toistaiseksi nimeltään tuntematon, mutta hänet voidaan yksilöidä hallussa olevan tai hänen muuten oletettavasti käyttämän teleosoitteen tai telepäätelaitteen avulla. Ks. HE 224/2010 vp, s. 94; HE 222/2010 vp, s. 318.

[626] Jos peitetoiminnan aikana tulee selvästi ilmi, että profiilin käyttäjä vaihtuu, ei peitetoimintaa voida jatkaa samalla päätöksellä. Ks. myös HE 224/2010 vp, s. 94; HE 222/2010 vp, s. 318 ja vertaa tiedonvälittäjäpuheluihin. Näiden osalta tietoverkoissa on mahdotonta sanoa, onko kyse tiedonvälittäjäpuheluun rinnastettavasta toiminnasta, koska poliisimies ei voi tietää kuka profiilia tosiasiallisesti käyttää, jos kyse ei ole esimerkiksi webkameran kautta tai äänen perusteella tapahtuvasta viestinnästä.

[627] Vaikka poliisimies voi itse päättää laajentamisesta, tulee peitetoiminnan laajentaminen saattaa ilman aiheetonta viivytystä ja viimeistään kolmen vuorokauden kuluttua tiedonhankinnan aloittamisesta

peitetoiminnan kohteen laajentamisen osalta poliisilaissa todetaan, että jos peitetoiminnan aikana ilmenee, että voidaan perustellusti olettaa muun kuin peitetoiminnan kohteena olevan henkilön syyllistyvän PolL 5:28.2:ssä tarkoitettuun rikokseen, jonka estämiseksi häneen on välittömästi kohdennettava peitetoimintaa, peitetoimintaa suorittava poliisimies saa laajentaa peitetoiminnan koskemaan myös mainittua henkilöä (PolL 5:34.2).[628] Pakkokeinolaissa sääntely on samansuuntainen, mutta sen osalta puhutaan rikoksen selvittämisestä (PKL 10:33.2). Yksinomaan tietoverkossa tehtävän peitetoiminnan laajentamista ei kuitenkaan tarvitse pakkokeinolain osalta poliisilain tapaan saattaa ilman aiheetonta viivytystä tai kolmen vuorokauden määräajassa tuomioistuimen ratkaistavaksi, vaan peitetoiminnasta päättänyt poliisimies voi ratkaista asian (PKL 10:33.2).

Pitkäaikaisen peitetoiminnan tietoverkoissa voidaan katsoa monesti vaativan vahvan peitteen profiilia, jossa aikaisemmin käsiteltyihin suojaamiskäytäntöihin tulee kiinnittää erityistä huomiota. Tämä johtuu siitä, että soluttautumisena ymmärretään yleensä toiminta, jossa henkilö liittyy organisaatioon tai muuhun ryhmään tarkoituksena hankkia tietoja sisältä päin tai vaikuttaa ryhmän toimintaan.[629] Aina näin ei kuitenkaan ole ja voidaan toimia esimerkiksi pelkän nimimerkin tai sähköpostiosoitteen perusteella. Lisäksi on huomioitava poliisimiehen ammattitaito ja ymmärrys tietoverkoista, jotta peite ei paljastu.[630] Peitetoimintaan osallistuvalla poliisimielellä tulee olla EPSA:n 9.3:n mukaan koulutus ja hänen tulee olla tehtävään vapaaehtoinen, henkilökohtaisilta ominaisuuksiltaan sopiva ja jolla on tehtävän edellyttämä poliisitoiminnan tuntemus.

Tietoverkoissa kohteen ja soluttautumisen määritelmät liittyvät kiinteästi jo aikaisemmin muiden toimivaltuuksien kohdalla käsiteltyjen kaveriksi pyytämisen ja ryhmiin liittymisen problematiikkaan. Peitetoiminnassa tällaiseen arviointiin ei ole juurikaan tarvetta, koska kaverilistoille ja erilaisiin suppeisiin ja laajempiin yhteisöihin hakeutuminen on koko soluttautumisen idea.[631] Siten esimerkiksi kohdehenkilön läheisten pyytäminen kaverilistalle

peitetoiminnasta päättäneen poliisimiehen ratkaistavaksi (PolL 5:33.1 ja PKL 10:33.1).

[628] Peitetoiminnan laajentaminen on kuitenkin saatettava ilman aiheetonta viivytystä ja viimeistään kolmen vuorokauden kuluttua tiedonhankinnan aloittamisesta peitetoiminnasta päättäneen poliisimiehen ratkaistavaksi (PolL 5:34.2).

[629] Erityisesti tämä koskee tilanteita, joissa tietoverkoissa tapahtuva peitetoiminnan lisäksi poliisimies harjoittaisi peitetoimintaa myös reaalimaailman puolella.

[630] Ks. esimerkiksi ratkaisu Helsingin KO 22.3.2019 R 19/1572, jossa poliisimies oli käyttänyt peitetoiminnassa kohdehenkilön kanssa käytyyn keskusteluun Wickr-sovellusta ja Protonmail-sähköpostia. Samaisessa ratkaisussa tuli esille myös se, että uskottavan peitetoiminnan suorittaminen on erittäin haastavaa. Tuomittu kyseenalaisti useissa keskusteluissa peitepoliisina toiminutta.

[631] Toisaalta tulee ottaa huomioon PolL 5:31 ja PKL 10:30 peitetoiminnan esitystä ja suunnitelmaa koskeva sääntely, jonka perusteella erilaisten yhteyksien luominen tulee perustua ennalta suunniteltuun toimintaan.

tai muu peitetoimintaan liittyvä normaali vuorovaikutus muun kuin kohdehenkilön kanssa on lähtökohtaisesti sallittua. Muilta kuin kohdehenkilöltä voi myös ottaa vastaan poliisia hyödyntävää tietoa, jos he sen oma-aloitteisesti kertovat.[632] Tästä pitää kuitenkin erottaa aktiivinen tiedonhankinta, jossa peitetoimintaa suorittava poliisimies kyselee aktiivisesti merkityksellisiä seikkoja peitetoiminnan kohteena olevalta tai muulla tavoin vaikuttaa häneen, jotta tämä paljastaisi kyseisiä tietoja.[633] Tämä aktiivinen tiedonkerääminen koske vain kohdehenkilöä.

Peitetoiminnan poliisilakiin tuoneissa esitöissä 34/1999 vp toimintamahdollisuudet jaettiin kolmeen eri tasoon: 1) yleinen peitetoiminta (under cover agent), 2) soluttautuva peitetoiminta (agent infiltré) ja äärimmäisenä toimintamuotona 3) osallistuva peitetoiminta.[634] Ensimmäisessä kohdassa on kyse tilanteesta, jossa soluttautuja salaa rikostorjunnallisen tavoitteensa ja yhteytensä poliisiin. Tällaista toimintaa on peiteammatissa työskentely, kuten autonkuljettajana, putkimiehenä, isännöitsijänä tai tarjoilijana toimiminen. Lisäksi esimerkkinä mainittiin liittyminen sosiaaliseen tai taloudelliseen ryhmään, jonka jäsenillä on mahdollisuus saada tietoja rikollisesta toiminnasta.[635] Soluttautuvassa peitetoiminnassa toiminta menee jo asetetta pidemmälle, jossa peitepoliisi osallistuu rikollisen ryhmän toimintaan, vaikka ei suoranaisesti syyllisty laittomiin tekoihin. Peitepoliisi on ryhmän jäsen, mutta suhtautuu passiivisesti ryhmän tekemiin rikoksiin.[636] Osallistuvaa peitetoimintaa kuvailtiin siten, että peitepoliisi hankkiutuu rikollisryhmän jäseneksi sekä osallistuu ryhmän laittomaan toimintaan, jolloin poliisimies syyllistyy vähintäänkin rikolliseen avunantoon.[637] Nykylainsäädännön mukaan peitetoimintaa suorittava poliisimies ei saa tehdä rikoksia eikä aloitetta rikoksen tekemiseen (PolL 5:29.1 ja PKL 10:28.1). Myös sellainen aloitteellisuus, joka ei vielä ole rikoslain tarkoittamaa rikokseen yllyttämistä, olisi peiteprofiililta kielletty.[638] Käytännössä jää kuitenkin epäselväksi mitä yllytysrikoksen ulkopuolelle jäävä toiminta tarkoittaa ja millaiset toteamukset menevät jo kielletyn puolelle. Esimerkkinä voidaan mainita tilanne, jossa poliisimies on soluttautunut radikalisoituneen ääriryhmän keskustelupalstalle ja viestii keskusteluryhmässä muiden ryhmäläisten kanssa. Keskustelua voidaan käydä esimerkiksi

[632] HE 224/2010 vp, s.115; HE 222/2010 vp, s. 338.
[633] HE 224/2010 vp, s.115; HE 222/2010 vp, s. 338.
[634] Kyseiset suomenkieliset määritelmät eivät löydy esitöistä, vaan on muodostettu niiden sisällön perusteella tätä tutkimusta varten.
[635] Tällainen toiminta katsottiin jo säätämishetkellä sallituksi ilman nimenomaista säännöstäkin. Tarkoituksena oli kuitenkin säätää juuri tämäntyylisestä toiminnasta.
[636] Säätämishetkellä tämänasteinen soluttautuminen katsottiin mahdolliseksi vain harvoissa tapauksissa.
[637] HE 34/1999 vp, s. 26.
[638] HE 224/2010 vp, s.116; HE 222/2010 vp, s. 339.

tarkoituksesta kohdistaa väkivaltaa tiettyihin henkilöihin, ryhmiin tai paikkoihin. Vaikka peiteprofiili ei itse voi yllyttää väkivaltaan esimerkiksi kiihottaminen kansanryhmää vastaan (RL 11:10) rikoksen mukaisesti tai kirjoittaa kunnianloukkauksen (RL 24:9) tunnusmerkistön mukaisia viestejä, tulisi muiden ryhmäläisten tällaisten rikosten täyttävään toimintaan saada suhtautua sellaisella tavalla, että sitä voisi tulkita lähelle rangaistavaa yllytystä olevaksi ja tietynlaisena kannatuksena näille ajatuksille. Etenkin kun tulee muistaa, että peitetoimintaa suorittavan poliisimiehen tulisi olla uskottava ja hänellä tulisi olla mahdollisuus suhtautua rikolliseen toimintaan välinpitämättömästi ja jopa hyväksyvästi.[639] Peiteprofiililla tulisi olla mahdollisuus tykätä tai muuten kommentoida rikoksen tunnusmerkistön täyttäviä viestejä kannustavasti ja hyväksyvästi.[640]

Joissakin tilanteissa rikokseen syyllistyminen on mahdollista. PolL 5:29.2:n ja PKL 10:28.2:n mukaan peitetoimintaa suorittava poliisimies on rangaistusvastuusta vapaa tehdessään liikennerikkomuksen, järjestysrikkomuksen tai muun niihin rinnastettavan rikoksen, josta on säädetty rangaistukseksi rikesakko. Teon tulee kuitenkin olla välttämätön peitetoiminnan tavoitteen saavuttamiseksi tai tiedonhankinnan paljastumisen estämiseksi. Tässäkään tapauksessa lainsäätäjä ei ole huomioinut tietoverkkojen osuutta, koska liikennerikkomukset eivät liity tietoverkkoihin ja rikesakkorikokset ovat hyvin pitkälti reaalimaailmaan liittyviä rikkomuksia.[641] Tietoverkkoihin liittyen lainsäätäjän tulisi arvioida *de lege ferenda* esimerkiksi erilaisten sananvapausrikosten tekomahdollisuutta, jotka voivat olla oleellisia tietoverkoissa tapahtuvan peitetoiminnan uskottavuudelle.[642] Sama koskee myös tekijänoikeuksiin liittyviä asioita, joista esimerkkinä voidaan mainita tekijänoikeuslain

[639] HE 224/2010 vp, s. 180; HE 222/2010 vp, s. 133. Ks. myös ratkaisu Helsingin KO 22.3.2019 R 19/1572, jossa peitepoliisi esiintyi ihmisten laajamittaista surmaamista toivovana ja suunnittelevana henkilönä.

[640] Vrt. kuitenkin Länsi-Uudenmaan KO 26.09.2013 R 13/1208, jossa henkilö tuomittiin kiusaamiseen liittyvässä tapauksessa kunnianloukkauksesta, koska oli toisen kiusaamiseen osallistuneet olivat ottaneet kuvia kiusatusta, ladanneet ne Facebookiin tehdylle fanisivulle kiusatusta, jolloin tuomittu oli painanut Facebookissa tykkää-nappia kyseisen kuvan kohdalla. Käräjäoikeus katsoi, että koska tykkäämisen seurauksena kyseinen tykkäys tuli mahdollisesti nähtäville tykkääjän 150:lle kaverille, oli kyseessä kunnianloukkaus. Käytännössä jonkin sananvapausrikoksen tunnusmerkistön mukaisten viestien tykkäysten tai kommentointien ei voida katsoa olevan suoraan rangaistavaa toimintaa, vaikka tämä toisi ne kaverilistan nähtäville. Tekoa tulee arvioida kokonaisuutena ja tykkääminen voi olla osa kokonaisuutta, jossa loukkaamistarkoitus tulee selvästi ilmi, niin kuin esimerkkitapauksessa.

[641] Rikesakkoja määrätään yleensä tie- ja vesiliikenteeseen liittyvistä rikoksista, jonka lisäksi mahdollisia ovat erilaiset järjestysrikkomukset sekä esimerkiksi alkoholin nauttimiseen liittyvät rikesakot. Kaikki nämä ovat reaalimaailman rikoksia.

[642] Näitä ovat esimerkiksi jo mainittu kiihottamisrikos ja kunnianloukkaus. Toisaalta myöskään reaalimaailmassa peitetoimintaa suorittava poliisimies ei saa loukata ketään kunnianloukkauksen tunnusmerkistön mukaisella tavalla, joka tuo hyvin esille äärimmäisen tiukan linjan peitetoiminnan rikoksentekokiellolle. Voidaan kuvitella tilanne, jossa joku ”soittaa suuta” peitepoliisille, mutta hän ei voi sanoa loukkaavasti takaisin toiselle osapuolelle ilman rikosoikeudellista vastuuta.

(404/1961) 56 a §:n mukainen tekijänoikeusrikkomus, josta voi seurata sakkoa.[643] Mielenkiintoinen olisi myös mahdollisuus, jossa poliisi voisi esiintyä identiteettivarkauden (RL 38:9a) tunnusmerkistön toisena henkilönä. Tämä voisi mahdollistaa soluttautumisen ainakin joksikin aikaa tilanteissa, joissa esimerkiksi rikollisjärjestöön kuuluva henkilö ei omaisi sosiaalisen median profiilia. Jos hänen tiedoillaan perustettaisiin profiili ja pyydettäisiin muutaman päivän aikana kavereiksi samaan rikollisjärjestöön kuuluvia henkilöitä, olisi melko todennäköistä että ainakin jotkut heistä hyväksyisivät peiteprofiilin kaverilistalleen, jonka seurauksena poliisin olisi mahdollisuus kerätä erilaista tietoa.[644]

Erikseen esimerkkinä voidaan nostaa esille RL 17:18.1,1:n mukainen sukupuolisiveellisyyttä loukkaava lasta esittävän kuvan levittäminen. On yleistä, että kyseiseen rikollisuuteen liittyen tekijät vaihtelevat laittomia tallenteita keskenään.[645] Tällaiseen toimintaan soluttautumisen kannalta voisi olla paikallaan, että peiteprofiililla olisi mahdollista vaihtaa todenmukaisia digitaalisesti valmistettuja kuvia ja kuvatallenteita epäiltyjen kanssa.[646] Vaikka kyse olisi moraalisesti kyseenalaisesta mahdollisuudesta ja kyseinen materiaali voisi lähteä leviämään tietoverkoissa, olisi se kuitenkin vailla todellisuuspohjaa, eikä kyseisen materiaalin voida katsoa vahingoittavan ketään tiettyä henkilöä. Samalla kyseisellä toiminnalla voitaisiin auttaa oikeita uhreja sekä saada torjuttua tehokkaammin lapsiin kohdistuvaa seksuaalirikollisuutta.[647]

Lapsiin kohdistuvaan seksuaalirikollisuuden torjuntaan ja peitetoimintaan liittyy myös jo aikaisemmin esille tuotu Sweetie, jossa oli kyse digitaalisesta luodusta lasta esittävästä henkilöstä, jonka seurauksena saatiin tietoa useista lapsiin tietoverkkojen kautta seksuaalirikoksia kohdistavista henkilöistä.[648] Kyseisenlainen toiminta ei ole tällä hetkellä

[643] Käytännössä kyse voisi olla teoista, jossa tekijänoikeuksien alaista materiaalia, kuten valokuvia, julkaistaan peiteprofiililla.

[644] Kyseisessä tilanteessa ei välttämättä olisi edes merkitystä sillä, että poliisin toiminta paljastuisi jälkeenpäin. Etenkin jos muutamia päiviä kestävän operaation aikana poliisi saisi useammilta henkilöiltä erilaisia valokuvia, paikkatietoja ja verkostotietoja.

[645] Ks. esimerkiksi Martellozzo 2015, s. 43–45. Ks. myös Europol 2011, jossa kerrottiin operaatiosta nimeltä ”Operation Rescue”, jossa paljastettiin pedofiilirinki sivustolta www.boylover.net, jolla oli 70 000 jäsentä useista eri maista. Toiminnan paljastamisessa käytettiin avuksi muun muassa peitetoimintaa.

[646] Todenmukaisella tarkoitetaan kuvaa tai kuvatallennetta, joka muistuttaa erehdyttävästi valokuvaamalla tai muulla vastaavalla menetelmällä valmistettua tilanteesta otettua kuvaa tai kuvatallennetta, jossa lapsi on sukupuolisiveellisyyttä loukkaavan toiminnan kohteena (RL 17:18.4). Kyseessä ei siten ole todellinen tilanne tai todelliset ihmiset.

[647] Huomioon voidaan ottaa sääntelyn mahdollisuudet vastata toimintaympäristön tekniseen kehittymisen asettamiin haasteisiin ja laajemminkin rikostorjunnan tehokkuusvaatimukset suhteessa perus- ja ihmisoikeuksiin, jossa todenmukainen materiaali ei loukkaa kenenkään perus- ja ihmisoikeuksia. Ks. tarkemmin HE 224/2010 vp, s. 31; HE 222/2010 vp, s. 113–114.

[648] Terre des Hommes 2013, s. 54. Ks. myös Forss 2014, s. 100–101, jossa kerrotaan niin sanotusta ”pedofiilinmetsästyksestä”, jossa yksittäiset kansalaiset ovat tehneet lasta esittäviä profiileja sosiaalisen median

mahdollista poliisin toimesta Suomessa, eikä kuvitteellisen hahmon lähestyminen seksuaalissävytteisesti täytä RL 20:6:n tunnusmerkistöä lapsen seksuaalisesta hyväksikäytöstä. Tämän takia henkilöön ei voida kohdistaa pakkokeinoja.[649] Lapsiin kohdistuvaa seksuaalirikollisuutta olisi mahdollista torjua tehokkaasti siten, että poliisilla olisi mahdollisuus luoda lasta esittävä peiteprofiili, jota käytettäisiin palveluissa ja odotettaisiin aikuisten lähestymisyrityksiä. Tämän jälkeen kyseisiin kohdehenkilöihin tulisi olla mahdollisuus kohdistaa pakkokeinoja, joiden perusteella voisi löytyä oikeita uhreja, koska monesti näillä tietoverkkojen kautta hyväksikäyttöihin syyllistyvillä on useita uhreja samanaikaisesti.[650]

Rikoksentekokiellon lisäksi peitetoimintaa suorittavan rangaistusvastuuseen vaikuttaa PolL 5:30:n ja PKL 10:29:n sääntely. Jos peitetoimintaa suorittava poliisimies osallistuessaan järjestäytyneen rikollisryhmän toimintaan hankkii toimitiloja tai kulku- tai muita sellaisia välineitä, kuljettaa henkilöitä, esineitä tai aineita, hoitaa taloudellisia asioita taikka avustaa rikollisryhmää muilla näihin rinnastettavilla tavoilla, on hän rangaistusvastuusta vapaa, jos erittäin pätevin perustein voidaan olettaa, että 1) toimenpide tehdään ilman hänen myötävaikutustankin, 2) poliisimiehen toiminta ei aiheuta vaaraa tai vahinkoa kenenkään hengelle, terveydelle tai vapaudelle taikka merkittävää vaaraa tai vahinkoa omaisuudelle ja 3) avustaminen edistää merkittävästi peitetoiminnan tavoitteen saavuttamista.[651] Esimerkiksi *Sequeira* -tapauksessa EIT arvioi sitä, olivatko peitepoliisit puuttuneet jo käynnissä olevaan huumekauppaan vai olivatko he provosoineet rikoksen tekemiseen. EIT:n mukaan tapauksessa ei ollut viitteitä siitä, että rikos olisi tapahtunut ilman poliisin myötävaikuttamista, joten kyse oli EIS:n 6 artiklan rikkomisesta.[652] Rikoksen tulisi siis tapahtua poliisista riippumatta. Tietoverkkojen osuutta ei mainita lainvalmisteluaineistossa lainkaan. Toisaalta kyseisenlaisiin esimerkkeihin rinnastuvien tilanteiden syntyminen tietoverkoissa ei voida katsoa olevan yleistä. Tällainen tilanne liittyisi lähtökohtaisesti

palveluihin ja sopineet tapaamisen aikuisen kanssa. Tapaaminen on videoitu ja julkaistu nolaamistarkoituksessa sosiaalisessa mediassa. Kyseistä toimintaa ovat harrastaneet myös toimittajat, mutta tarkoituksena on ollut kartoittaa ilmiön laajuutta.

649 Ks. tietoverkoissa tapahtuvan peitetoiminnan eri muodoista laajasti sekä taktisesta näkökulmasta eri peiteroolien kohdalla Shipley – Bowker 2014, s. 233–250. Esille nostetaan myös lapsen seksuaaliseen hyväksikäyttöön tietoverkoissa puuttuva toiminta.

650 Ks. Forss 2011, s. 251, jossa kerrotaan Ranskassa toimivasta poliisin yksiköstä, joka suorittaa nimenomaan tämänkaltaista toimintaa ja on saanut paljastettua esimerkiksi tapauksen, jossa yksittäisellä tekijällä oli 300 uhria.

651 Lisäksi voidaan mainita, että peitetoimintaa suorittava poliisimies saa osallistua PolL 5:43:ssä tai PKL 10:41:ssä tarkoitetun valvotun läpilaskun kohteen olevaan toimitukseen, jos osallistuminen edistää merkittävästi läpilaskun tavoitteen saavuttamista.

652 *Sequeira v. Portugali* (2009).

reaalimaailman toimintaan, jossa peitetoimintaa suoritettaisiin myös tietoverkoissa. Pelkästään tietoverkoissa voitaisiin avustaa esimerkiksi huumausaineiden myymisessä tai viharikoksiin liittyvien rangaistavien kuvamanipulaatioiden tekemisessä.

### 7.6 Valeosto

Poliisi- ja pakkokeinolaissa valeostolla tarkoitetaan poliisin tekemää esineen, aineen, omaisuuden tai palvelun ostotarjousta tai ostoa. Poliisilain kohdalla tavoitteena on rikoksen estämiseksi saada poliisin haltuun tai löytää estettävään rikokseen liittyvä esine, aine tai omaisuus (PolL 5:35.1). Pakkokeinolain kohdalla tavoite muodostuu PKL 7:1ssä mainituista takavarikon edellytyksistä.[653] Tavoitteena on saada poliisin haltuun tai löytää todiste rikosasiassa, rikoksella saatu hyöty taikka esine, aine tai omaisuus, joka on rikoksella viety tai jonka tuomioistuin voi julistaa menetetyksi taikka jonka avulla voidaan muuten saada selvitystä rikosasiassa (PKL 10:34.1).[654] Sekä poliisi- että pakkokeinolain mukaisen valeoston saa tehdä jos kyseessä on rikos, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta. Kyseisten rikosten lisäksi valeosto voi olla mahdollista myös varkauden tai kätkemisrikoksen osalta.[655] Lisäedellytyksenä on, että on todennäköistä että valeostolla saavutetaan PolL 5:35.1:ssä tai PKL 10:34.1:ssä mainittu tavoite (PolL 5:35.2 ja PKL 10:34.2). Todennäköisyysedellytys on jostain syystä lisätty säännökseen, vaikka valeostoa koskee jo muutoinkin tiukin yleisten edellytysten välttämättömyysvaatimus.[656] Sinänsä välttämättömyys- ja todennäköisyysvaatimus eivät käytännössä aiheuta ongelmia, jos kyseessä on esimerkiksi darknetissä tapahtuva kaupankäynti. Reaalimaailmassa tehtävä ”katuvalvonta” kun ei toimi tietoverkossa eikä kohdehenkilöiden IP-osoitteita voida selvittää, niin ainoaksi mahdollisuudeksi selvittää huumausaineiden myyjä, jää valeosto tai peitetoiminta.

Valeostosta päättää keskusrikospoliisin tai suojelupoliisin päällikkö, mutta yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös

[653] Ks. HE 222/2010 vp, s. 344.
[654] PKL 7:1.1:n mukaan esine, omaisuus tai asiakirja voidaan takavarikoida, jos on syytä olettaa, että 1) sitä voidaan käyttää todisteena rikosasiassa, 2) se on rikoksella joltakulta viety tai 3) se tuomitaan menetetyksi. Pakkokeinolain osalta tulee myös huomioida, että valeosto voidaan suorittaa rikoshyödyn ja anastetun omaisuuden osalta myös silloin, kun mahdollinen oikeudenkäynti on jo asian tiimoilta käyty. Ks. HE 222/2010 vp, s. 344.
[655] Asunnossa valeosto on sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella (PolL 5:35.4 ja PKL 10:34.4).
[656] Kyseessä voidaankin katsoa olevan tietynlainen ylisääntely. Ks. aiheesta tarkemmin Helminen ym. 2014, s. 1201–1202.

STEKPOV (PolL 5:36.1 ja PKL 10:35.1). Yleisön saataville toimitettuun myyntitarjoukseen tehtävän valeoston eroa selittää se, että rikosprovokaatioriski on lähtökohtaisesti vähäinen, jolloin myös päätöksentekotasoa on voitu laskea.[657] Yleisön saataville -käsitettä ei ole avattu esitöissä tarkemmin, mutta sillä voidaan katsoa tarkoitettavan tietoverkoissa SVL 2.1,2:n mukaista verkkoviestiä. Jos kyse on suljetusta ryhmästä, jossa kyse on korkeintaan vain muutamien kymmenien ihmisten ryhmästä, ei STEKPOV voi välttämättä tehdä PolL 5:36.1:n tai PKL 10:35.1:n mukaista päätöstä valeoston tekemisestä. Tällöin päätöksentekijänä tulee olla keskusrikospoliisin tai suojelupoliisin päällikkö.[658]

Valeostopäätös voidaan antaa enintään kahdeksi kuukaudeksi kerrallaan (PolL 5:36.2 ja PKL 10:35.2). Päätös valeostosta on tehtävä kirjallisesti ja siinä on mainittava PolL 5:36.3:ssä ja PKL 10:35.3:ssä mainitut seikat.[659] Valeoston toteuttamisesta on laadittava kirjallinen suunnitelma, jos se on tarpeen toiminnan laajuuden tai muun vastaavan syyn vuoksi (PolL 5:37.1 ja PKL 10:36.1). Erillinen suunnitelma voi olla tarpeellinen esimerkiksi sen takia, että valeostosta päättää eri poliisiyksikkö kuin sen toteuttava yksikkö tai suunnitelma on tarpeen erityisesti toimintaa sisältyvien riskien torjumiseksi.[660] Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava (PolL 5:37.2 ja PKL 10:36.2). Valeoston toteuttamista koskeva päätös tehdään kirjallisesti ja päätöksen tekee valeoston toteuttamisesta vastaava STEKPOV. Päätöksessä on mainittava valeostosta päättänyt poliisimies, päätöksen antopäivä ja sisältö sekä mahdolliset rajoitukset ja ehdot. Toteuttavan poliisiyksikön lisäksi tulee mainita tunnistetiedot valeoston suorittavista poliisimiehistä.[661] Päätöksessä on myös perusteltava se, miten on varmistettu että valeosto ei saa sen kohteena olevaa tai muuta henkilöä tekemään rikosta jota hän ei muuten tekisi (PolL 5:38.1–2 ja PKL 10:37.1–2).[662] Valeoston toteuttamista koskevaa päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava (PolL 5:38.4 ja PKL 10.37.4). Valeoston käytöstä on laadittava pöytäkirja (PolL

[657] HE 224/2010 vp, s. 123; HE 222/2010 vp, s. 346.
[658] Tulee myös ottaa huomioon, että kyseisenlaisessa tilanteessa saattaa tulla kysymykseen jo peitetoiminta, jotta kyseisenlaiseen ryhmään voidaan edes hakeutua.
[659] Näitä ovat 1) rikos, 2) kohdehenkilö, 3) tosiseikat, joihin epäily ja valeoston edellytykset perustuvat, 4) valeoston kohteena oleva esine, aine, omaisuus tai palvelu, 5) valeoston tarkoitus, 6) päätöksen voimassaoloaika, 7) valeoston suorittamista johtava ja valvova POV ja 8) mahdolliset valeoston rajoitukset ja ehdot.
[660] HE 224/2010 vp, s. 123; HE 222/2010 vp, s. 346. Poliisilaitos ei voi päättää kuin yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta (EPSA 3:11.1).
[661] Valeostossa käytettäviä suojaamissääntelyyn perustuvia rekisterimerkintöjä tai asiakirjoja ei ole tarkoitettu käytettäväksi peitetoiminnan tapaan, vaan ainoastaan sellaisissa yksittäisissä tilanteissa, joissa valeostajan turvallisuus ja valeoston paljastumisen estäminen välttämättömästi edellyttävät suojaamisen käyttämistä. Ks. HE 224/2010 vp, s. 55; HE 222/2010 vp, s. 139.
[662] Päätöstä ei tarvitse laatia kirjallisesti ennen valeostoa, jos toimenpide ei siedä viivytystä. Päätös on kuitenkin laadittava viipymättä myös tällaisissa tapauksissa (PolL 5:38.3 ja PKL 10:37.3).

5:59 ja PKL 10:61).[663] Valeostoja voidaan määrätä suorittamaan vain Poliisihallituksen hyväksymä koulutuksen suorittanut poliisimies, joka on tehtävään vapaaehtoinen, henkilökohtaisilta ominaisuuksiltaan sopiva ja jolla on tehtävän edellyttämä poliisitoiminnan tuntemus (EPSA 3:11.3). Koulutuksesta voidaan todeta, että tietoverkoissa tapahtuva valeosto vaatii selkeästi erilaisia valmiuksia kuin reaalimaailmassa.[664]

Valeoston ei tarvitse kohdistua varsinaisen esirikoksen tekijään. Esimerkkinä voidaan mainita anastetun omaisuuden hallussapitäjän lisäksi huumausainerikollisuus, jossa pyritään saamaan tietoa huumausaineen jakelukanavista, maksuyhteyksistä sekä taustalla toimivasta organisaatiosta ja sen johdosta. Esimerkkeinä voidaan mainita myös paritus (RL 20:9) ja ihmiskauppa (RL 25:3), joissa valeosto voidaan kohdistaa seksipalveluja myyvään, vaikka hän ei välttämättä syyllisty mihinkään rikokseen. Poliisi voi näissä tapauksissa tehdä valeostoja esimerkiksi sen selvittämiseksi, onko seksipalveluja myyvä kyseisten rikosten kohteena.[665] Valeoston yhteydessä on mahdollista tehdä valmistelevia toimenpiteitä, kuten valeoston kohteena olevan tavaran varastoiminen tai siirtäminen ennen varsinaista ostotarjousta tai ostoa, jolloin tällainen toimenpide voisi muodostaa myös osan vastikkeesta. Palvelun ostaminen ei saa olla hyvän tavan vastaista. Ostotarjous, mutta myös osto, voidaan kuitenkin suorittaa esimerkiksi paritukseen liittyvissä tapauksissa, joissa ostetaan seksuaalipalveluja. Palvelua ei voida kuitenkaan käyttää.[666] Ongelmaksi voi muodostua se, että myös annettu vastike voi olla hyvän tavan vastainen. Esimerkkinä voidaan mainita tilanne, jossa valeosto suoritettaisiin siten, että aseita yritettäisiin ostaa huumausaineilla. Käytännössä ei pitäisi olla kuitenkaan ongelmaa suorittaa kyseisenlaista valeostoa, jos oikeita huumausaineita ei tosiasiallisesti annettaisi toisen osapuolen haltuun tai kyse olisi huumausaineita muistuttavista aineista.[667] Toisena ongelmallisena esimerkkinä voidaan mainita jo peitetoiminnan yhteydessä esille tuotu problematiikka lapsen seksuaalista hyväksikäyttöä koskevien kuvien ja kuvatallenteiden kohdalla, joissa valeosto voisi tapahtua kuvilla kuvia vastaan.

[663] Pöytäkirja tulee laatia ilman aiheetonta viivytystä ja siitä tulee ilmetä EPSA 3:12:ssä mainitut seikat.
[664] Ks. tähän liittyen Poliisihallitus 2019, s. 43, jossa kerrotaan keskusrikospoliisin ja Poliisihallituksen yhteistyössä järjestämästä seminaarista ”Huumerikostorjunta tietoverkossa”, johon oli kutsuttu poliisiyksiköiden vale- ja peitetoiminnasta vastaavat.
[665] Ks. esimerkiksi HS 2019a, jossa kerrotaan suomalaisen Sihteeriopisto-sivuston sulkemisesta, jota luonnehditaan suomen tunnetuimpana seksipalveluita välittävänä sivustona.
[666] HE 224/2010 vp, s. 122; HE 222/2010 vp, s. 344–345.
[667] Kyseisenlaiseen tilanteeseen voisi tietyissä tapauksissa soveltua valvottua läpilaskua (PolL 5:43 ja PKL 10:41) koskeva sääntely.

Käytännössä suurin osa valeostoista kohdistuu huumausainerikollisuuteen ja yleisin paikka kaupantekoon on darknet.[668] Se tarjoaa alustan huumeiden, mutta myös esimerkiksi aseiden kauppapaikkana, koska se on lähtökohtaisesti anonyymi, antaa hyvän vasteen riskinotolle ja mahdollistaa helpon tavan tavata toinen osapuoli. Toisaalta sen heikkouksina voidaan mainita poliisin mahdollisuus helpompaan soluttautumiseen sekä puuttua laajempaan yhteisöön saamalla, jos yksi yhteisön jäsen kiinni, jolloin hänen laitteillaan olevat tiedot voivat paljastaa laajan yhteisön.[669] Tällainen oli tilanne laajamittaista TOR-verkossa toiminutta huumausaineiden kauppapaikkaa Sipulikanavaa koskevassa ratkaisussa Itä-Uudenmaan KO 11.2.2019 R 18/3115/766, jossa henkilö tuomittiin kyseisen markkinapaikan ylläpitäjänä törkeästä huumausainerikoksesta. Sivustolle oli luotu omat kaupunkikohtaiset osiot ja myynti-ilmoituksiin kirjattiin myytävät huumausaineet, myynnissä olevien huumausaine-erien suuruus, huumausaineiden hinta, Wickr-pikaviestisovellukseen liittyvä käyttäjätunnus sekä mahdollinen kuva huumausaineesta tai -aineista.[670] Tutkinnassa selvisi useita sivustolla toimivia henkilöitä, jotka olivat myös syytettynä samassa oikeudenkäynnissä. Tutkinnan yhteydessä oli huomattu Sipulikanavalla myös laitonta ase-, doping-, henkilötieto-, lääke- ja nuuskakauppaa koskevia viestejä, mutta tutkinnassa oli keskitytty vain törkeään huumausainerikokseen. Tuomiosta käy myös ilmi se, että yleensä kaupantekoon käytetään käteisen ohella erilaisia virtuaalivaluuttoja.[671]

Sekä poliisi- että pakkokeinolain mukaan muun kuin näyte-erän ostaminen edellyttää, että ostaminen on välttämätöntä valeoston toteuttamiseksi (PolL 5:35.1 ja PKL 10:34.1). Näyte-erän ostaminen on ensisijainen toimintatapa.[672] Jos kuitenkin on kyse esineestä tai omaisuudesta, joka ei ole sen luonteista että sitä voitaisiin myydä erissä, voidaan ostotarjous kohdistaa esineeseen tai omaisuuteen kokonaisuudessaan. Tämän lisäksi on mahdollisuus

[668] Tietoverkkoihin liittyen valeosto voi kohdistua myös anastettuun omaisuuteen, joista voidaan mainita esimerkkeinä polkupyörät. Näiden osalta valeostot vaikuttavat jäävän enemmän kansalaisten itsensä tehtäväksi. Ks. esimerkiksi ESS 2016, jossa tyttö oli sopinut treffit henkilön kanssa, joka oli laittanut hänen anastetun polkupyörän myyntiin. Tytön huomattua pyörän olevan varmuudella hänen, oli lähellä ollut poliisipartio puuttunut tilanteen selvittelyyn. Näissä tapauksissa tulee muistaa erityisesti se, että poliisi ei voi kiertää toimivaltuussäännöksiä ohjaamalla asianomistajaa tekemään valeosto. Lisäksi tulee huomioida, että jos kyse on esimerkiksi tilanteesta jossa huoltaja havaitsee lapsensa ostavan huumausaineita tietyltä henkilöltä tietoverkoista, ei huoltaja voi sopia kaupanteosta henkilön kiinni saadakseen, koska hän voi itse syyllistyä tapauksessa huumausainerikokseen.

[669] Bright 2015, s. 40–42

[670] Tämän perusteella myyjät olivat sopineet tarkemmin kaupan sisällöstä Wickr-pikaviestisovellusta käyttäen. Myytävänä oli ollut useita erilaisia huumausaineita, kuten amfetamiinia, ekstaasia, kokaiinia ja marihuanaa.

[671] Ks. edellä mainitun tuomion lisäksi virtuaalivaluuttojen yleisestä hyödyntämisestä huumausainerikoksissa myös Turun HO 25.10.2018 R 17/1974, jossa vastaaja väitti saaneensa noin 5000 euron käteisvarat laillisesta bitcoin-kaupasta huumausainekaupan sijaan.

[672] Hallituksen esityksessä viitataan lakivaliokunnan lausuntoon 6/2005 vp, jonka mukaan ei olisi perusteltua, että poliisimies voisi hankkia esimerkiksi huomattavia huumausaine-eriä, tai että ostotoiminta jatkuisi pitkään. Ks. HE 224/2010 vp, s. 122; HE 222/2010 vp, s. 344.

suorittaa näyte-erää suurempaankin kokonaisuuteen kohdistuva ostotarjous, jos se on välttämätöntä valeoston toteuttamiselle. Tällöin on varmistuttava erityisen huolellisesti siitä, ettei muun kuin näyte-erän hankkiminen johda rikosprovokaatioon.[673] Rikosprovokaatio voisi tulla kyseeseen esimerkiksi tapauksissa, joissa henkilöltä tiedustellaan suurempaa määrää huumausaineita kuin hänellä on tietoverkoista löytyvän ilmoituksen mukaan myynnissä. Muun kuin näyte-erän ostaminen voi monissa tapauksissa kuitenkin olla enemmän poliisitaktinen ja uskottavuuteen liittyvä haaste, kuin lainsäädännön välttämättömyyteen perustuva rajoitus.[674] Toisaalta lainsäätäjän tulisi ottaa huomioon se seikka, että jossain tilanteissa poliisilla tulisi olla ensisijaisena tarkoituksena hankkia poliisin haltuun koko omaisuus. Näitä tilanteita voisivat olla erilaisiin räjähteisiin, ydinaineisiin tai terveydelle erittäin vaarallisiin yhdisteisiin liittyvät valeostot, joissa olisi tarkoituksenmukaista saada aineet kokonaisuudessaan pois.[675]

Valeoston yhteydessä poliisimies ei saa tehdä kuin sellaista tiedonhankintaa, joka on välttämätöntä valeoston toteuttamiseksi. Valeosto on toteutettava siten, ettei se saa kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi (PolL 5:35.3 ja PKL 10:34.3).

> Valeostoksi ei katsota esitöiden mukaan tiedustelujen tekemistä esimerkiksi lehti-ilmoituksesta.[676] Tätä voidaan pitää mielenkiintoisena linjauksena. Jos poliisi lähtee tekemään tiedusteluja kohteelta, on poliisilla tällöin olemassa jonkinlainen intressi kohdehenkilöä kohtaan ja vuorovaikutuksessa tapahtuva tiedonhankinta kohdistuu nimenomaan kyseiseen ilmoituksessa mainittuun tahoon. Poliisin hakeutuessa vuorovaikutukseen kohteen kanssa salaten poliisitaustansa, voidaan katsoa kyseessä olevan ennemminkin peitelty tiedonhankinta (PolL 5:15 ja PKL 10:14).[677]

Valeostoa edeltävää tiedonhankintaa voidaan tehdä esimerkiksi sen takia, että pyritään varmistamaan se, että valeoston kohteena olevan esine, aine tai omaisuus on kohteena olevan henkilön hallussa. Tällöin suljetaan pois vaaraa rikosprovokaatiosta. Jos henkilö esimerkiksi myy TOR-verkossa huumeita, voi esillä olla vain grammahinta. Myyjällä ei ole

---

[673] HE 224/2010 vp, s. 122; HE 222/2010 vp, s. 344.
[674] Ei ole välttämättä uskottavaa, jos poliisimies kertoo huumausaineita tai aseita TOR-verkossa kauppaavalle henkilölle, että hän haluaa ostaa heti hänen kaikki huumausaineet tai aseet.
[675] Etenkin niiden esineiden tai aineiden osalta, joita voidaan käyttää terroristisiin tarkoituksiin.
[676] HE 224/2010 vp, s. 122; HE 222/2010 vp, s. 345.
[677] Kyseistä tiedustelua ei voida myöskään pitää normaalia tiedonhankintaan liittyvänä keskusteluna, koska kohteena on nimenomaan kyseisen ilmoituksen jättäjä.

tällöin välttämättä tuotetta hallussa peitepoliisin pyytämää määrää, joten tilanne voi vasta ostotarjouksen jälkeen johtaa siihen, että myyjä hankkii kyseistä huumausainetta itselleen. Näissä tapauksissa pitäisi tiedonhankinnan kautta selvittää asiaa siinä määrin, ettei kohdehenkilö hanki lisää huumausaineita poliisimiehen ostotarjouksen takia.[678]

Rikosprovokaation osalta problematiikka on EIT:n ratkaisukäytännössä arvioitu yleensä käsitteiden agent infiltré ja agent provocateur alla. Ensimmäisen kohdalla kyse on poliisin puuttumisesta jo käynnissä olevaan operaatioon ja jälkimmäisessä siitä, että poliisi on omalla toiminnallaan provosoinut kohteen rikoksen tekemiseen.[679] Esimerkiksi *Bannikova* -tapauksessa EIT arvioi rikosprovokaatiota punniten puolesta ja vastaan puhuvia seikkoja. Olisiko rikos tehty ilman poliisin puuttumista, onko voitu objektiivisesti arvioituna epäillä, että kohdehenkilö on ollut mukana rikollisessa toiminnassa, vai altistettiinko hänet sellaiseen.[680] Rikosprovokaatiota puoltavia seikkoja olivat esimerkiksi poliisin painostus, hylätyn ostotarjouksen jälkeen tehdyt uudet tarjoukset, kauppahinnan normaalista poikkeava korottaminen tai vetoaminen vieroitusoireisiin.[681] Tietoverkkoja koskevaa ratkaisukäytäntöä ei EIT:n osalta ole saatavilla ja niin kuin esitöissä todetaan on tietoverkoissa rikosprovokaatioriski pienempi kuin reaalimaailmassa.[682] Toisaalta Poliisihallitus on katsonut, että tietoverkoissa tehtävien huumausaineita koskevien niin sanottujen rajoitettujen valeostojen osalta olisi syytä linjata, millaisia tarjouksia voidaan esittää ja millä perusteilla, jotta rikosprovokaation riskiltä vältyttäisiin.[683] Ei ole kuitenkaan tiedossa, että epäselvyydet olisivat johtaneet laillisuusvalvojan arviointeihin.

Oman kysymyksensä muodostaa kuinka pitkälle reaalimaailman toimintaan tietoverkkoja koskeva valeostopäätös ylettyy. Lähtökohtaisesti huumausainekauppaa tietoverkoissa tehdään kahdella eri tavalla. Ostaja ja myyjä sopivat myynti-ilmoituksen perusteella tapaamispaikan tietoverkoissa ja tekevät kaupat kasvotusten. Toisessa tilanteessa kaupat tehdään esimerkiksi virtuaalivaluutalla ja huumausaineet lähetetään postin kautta tiettyyn

[678] Ks. tarkemmin rikosprovokaatiosta poliisimiehen osalta ja siihen liittyvästä rangaistusvastuusta Frände 2004, s. 408.
[679] Ks. käsitteistä tarkemmin Reinikainen 2003, s. 91–93.
[680] Lisäksi todettiin, että kohdehenkilön rikollinen entisyys ei itsessään ole indikaatio meneillään olevasta rikollisesta toiminnasta ja rikollinen aikomus on oltava todennettavissa olemassa olevien tietojen perusteella. Merkitystä oli myös toiminnan aloitushetkellä, jossa poliisi saa tiedon rikollisesta toiminnasta vasta sen alettua.
[681] *Bannikova v. Venäjä* (2010), kohdat 37–47. Ks. laajemmin EIT:n ratkaisukäytännöstä rikosprovokaatioon liittyen Helminen 2014, s. 1186–1190.
[682] HE 224/2010 vp, s. 123; HE 222/2010 vp, s. 345.
[683] Poliisihallitus 2018c, s. 29.

paikkaan tai vaihtoehtoisesti suurempien määrien kohdalla esimerkiksi maastokätköön.[684] Jos poliisi menee tapaamaan valeostajaa reaalimaailmassa, niin tulisiko tällä olla vaikutusta valeoston päätöksentekijätasoon? Jos itse valeostopäätös on tehty jo tietoverkkojen puolella, katson tietoverkkoja koskevan valeoston mahdollistavan vastikkeiden vaihdon reaalimaailman puolella lyhytaikaisessa vuorovaikutuksessa.[685] Sama tulkinta koskee myös reaalimaailmassa lehti-ilmoituksen perusteella tapahtuvaa valeostoa, joten oleellista toimivaltuuden käytössä on itse ilmoituksen jättämistapa, eikä konkreettinen valeostotilanne. Reaalimaailman puolella poliisimiehellä on lisäksi käytössä PolL 5:39:ssä ja PKL 10:38:ssä mainitut turvaamistoimenpiteet.[686] Tietoverkossa toteutettu valeosto ei kuitenkaan mahdollista pidempiaikaista vuorovaikutusta reaalimaailmassa kohdehenkilön kanssa, mutta esimerkiksi lyhytaikainen tarkkailu myyjän seuraamiseksi kaupanteon jälkeen on mahdollista.[687] Lisäksi voidaan huomioida, että jos valeostossa joudutaan käyttämään sivullisia henkilöitä yhteyden muodostamiseksi kohteena olevaan henkilöön, tulee varmistua siitä ettei valeosto saa sivullisen tekemään rikoksen.[688] Toisaalta poliisilta ei odoteta kovin ankaraa selonottovelvollisuutta, koska poliisin vaikutusmahdollisuudet tällaisiin henkilöihin ovat heikot. Pääpaino on siten valeoston kohteena olevassa henkilössä.[689]

Huumeidenkäytön tutkimukset ovat ottaneet huomioon internetin 1990-luvun lopulta asti, mutta vasta viime vuosina internetistä on tullut tiedon hakemisen ja käyttökokemusten arvioinnin sijaan kauppapaikka huumeille.[690] Poliisi on ollut tämän kehityksen seuraamisessa selvästi jäljessä. Tietoverkkojen roolia ei ole otettu riittävällä vakavuudella huomioon, vaikka kyseessä on rajat ylittävän rikollisuuden muoto, jossa vähittäiskaupan lisäksi liikkuu

[684] Ks. Iltalehti 2018, jossa poliisi kertoo tietoverkkojen huumausainekaupasta. Huumausaineita myyvät voivat käyttää hyväksi esimerkiksi syyttömien naapurien postilaatikoita. Näissä tilanteissa huumeidenkäyttäjä tilaa huumausaineita naapurin postilaatikkoon ja odottaa postinkantajan tuloa, jonka jälkeen tekijä ottaa huumausaineet postilaatikosta ennen kuin postilaatikon oikea haltija käy katsomassa postinsa.
[685] Jos tilanne johtaa alun perin tietoverkoissa tapahtuneen seksuaalipalveluja koskevan valeoston yhteydessä asuttuun asuntoon sisälle, tulee huomioida PolL 5:35.4:n ja PKL 10:34.4:n sääntely.
[686] Erityisen tärkeäksi tämä seikka on noussut sen takia, että tietoverkkoihin liittyvään huumausaine- ja nuuskakauppaan liittyen erilaisten ryöstöjen määrä on noussut viime vuosina ilmiötasolle. Ks. tähän liittyen esimerkiksi Helsingin poliisilaitos 2019, jossa kerrotaan ryöstöjen yleisyydestä tietoverkkojen avulla tapahtuvaan huumausainekauppaan liittyen.
[687] Myöskään tietoverkkojen puolella valeostotoiminta ei saa edetä soluttautumiseen rinnastettavaan toimintaan, jossa samalta henkilöltä tehdään useita valeostoja ja pyritään pidempiaikaisella kaupankäynnillä mahdollisesti paljastamaan kuuluminen isompaan järjestäytyneeseen ryhmään. Lainsäädännöllisesti tämä ei kuitenkaan aiheuta juurikaan ongelmia, koska peitetoiminnan raja tietoverkoissa on erityisten edellytysten osalta sama kuin valeostossa. Tulee vain huomioida kyseisten säännösten erilaiset muotomääräykset. Tarkkailussa tarkoituksena voi olla poliisille tuntemattoman henkilön henkilöllisyyden paljastaminen ja asuinpaikan selvittäminen, johon voidaan esimerkiksi kohdistaa valeoston jälkeinen kotietsintä.
[688] Tämä liittyy vahvasti seuraavaksi käsiteltävään tietolähdetoimintaan.
[689] HE 224/2010 vp, s. 123; HE 222/2010 vp, s. 345.
[690] Ks. huumeisiin liittyvän keskustelukulttuurin kehityksestä internetissä Seppälä – Mikkola 2004, s. 39–44.

myös tukkukauppatasoisia määriä huumausaineita.[691] Valeostot tietoverkoissa ovat olleet viime vuosiin asti poliisin suorittamina harvinaisia, vaikka suunta on ollut parempaa päin.[692] Poliisihallituksen vuosittaisissa kertomuksissa mainitaan vasta vuotta 2016 koskevassa raportissa ensimmäisen kerran tietoverkoissa suoritetut valeostot.[693] Vuotta 2017 koskevassa kertomuksessa todetaan, että valeostopäätösten kirjaaminen tietoverkoissa lisääntyi merkittävästi. Syynä tähän oli valtakunnallinen tehostettu valvontaoperaatio, jossa suoritettiin tehostettua huumausaineiden valvontaa verkossa anonyymeillä myyntikanavilla.[694] Edellisen vuoden 2016 kertomuksessa valeostopäätöksiä kerrottiin tehdyn hieman toistakymmentä pääosin tietoverkkoihin liittyen. Poliisihallitus katsoi ettei keinon käytön hyötyjä oltu edelleenkään sisäistetty poliisiyksiköissä.[695] Viimeisimmässä vuotta 2018 koskevassa kertomuksessa todetaan, että valeostopäätösten perusterikosten kirjo on laajentunut huomattavasti ja valtakunnallisesti toteutettujen operaatioiden määrät nousseet. Tämän takia Poliisihallitus toteaa, että keino on havaittu toimivaksi jokapäiväiseksi työkaluksi ja poliisiyksiköissä on lopullisesti sisäistetty keinon käytön hyödyt.[696] Eri asia on, että panostetaanko siihen edelleenkään riittävästi.

### 7.7 Tietolähdetoiminta

Tietolähdetoiminnasta ja sen ohjatusta käytöstä on säännelty samansuuntaisesti poliisi- ja pakkokeinolaissa ja toiminta tulee kyseeseen sekä poliisi- että peiteprofiileilla.[697] Poliisilaissa tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, poliisilain 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen

[691] Ks. esimerkiksi Keskusrikospoliisi 2018, s. 4–5. Ks. myös Varsinais-Suomen KO 10.2.2017 R 16/5348, jossa vastaajat olivat ostaneet TOR-verkon kautta suuren määrän huumausaineita ja yksi heistä oli käynyt hakemassa ne Hollanista Suomeen, jossa niitä oli levitetty edelleen tietoverkkojen kautta eteenpäin. Osan huumausaineista vastaaja oli lähettänyt myös postin kautta Suomeen.

[692] Ensimmäinen tietoverkkoja koskeva valeostokoulutus järjestettiin vasta vuonna 2015. Ks. Poliisihallitus 2016a, s. 45.

[693] Poliisihallitus 2017a, s. 33. Ks. tähän liittyen Poliisihallitus 2016b, s. 34, jossa todettiin valeostopäätöksiä tehdyn vain muutaman, ja pääasiassa vain törkeisiin huumausainerikoksiin liittyen.

[694] Poliisihallitus 2018c, s. 29. Valvontaan osallistuivat kaikki poliisilaitokset ja keskusrikospoliisi. Valvonnan aikana kirjattiin 116 rikosilmoitusta huumausainerikoksista. Tarkoituksena oli kehittää poliisin valmiuksia kyseisenlaiseen toimintaan sekä jalkauttaa hyviä käytäntöjä laitoksilta toisille. Kokemusten perusteella verkkovalvontaa oli tarkoitus lisätä vaikka sen katsottiin olevan pääsääntöisesti erittäin henkilöresursseja vaativaa.

[695] Poliisihallitus 2017a, s. 33.

[696] Poliisihallitus 2019, s. 35–36.

[697] Tässä yhteydessä voidaan todeta, että poliisin omat tarkemmat ohjeet tietolähdetoiminnasta ovat salassa pidettäviä, joten niitä ei voida käyttää tässä tutkimuksessa. Ks. Poliisihallitus 2018a, s. 2, jossa todetaan, että tietolähdetoiminnasta on annettu erillinen salassa pidettävä määräys (POL-2018-11897) ja lisäksi salaista tiedonhankintaa koskevaan käsikirjaan on kirjattu yksityiskohtaisempia toimintamalleja poliisin salaisten tiedonhankinta- ja pakkokeinojen taktisesta ja teknisestä käytöstä.

vastaanottamista poliisin ja muun esitutkintaviranomaisen ulkopuoliselta henkilöltä.[698] Pakkokeinolain kohdalla kyse on rikoksen selvittämiselle merkityksellisten tietojen vastaanottamisesta.[699] Tätä ulkopuolista henkilöä kutsutaan tietolähteeksi (PolL 5:40.1 ja PKL 10:39.1). Tietolähdetoiminta on muuta kuin satunnaista tietojen vastaanottamista, joten yksittäisten vihjeiden antajat rajautuvat pois tietolähteen määritelmästä.[700] Mitään tarkkaa rajaa ei laissa tai esitöissä kuitenkaan anneta, milloin tietojen ja erilaisten vihjeiden antaja voidaan katsoa tietolähteeksi. Joka tapauksessa yhteydenottoja tulee olla useita. Tietolähdetoiminnan luottamuksellisuus viittaakin enemmän tilanteisiin, joissa poliisimiehen ja tietolähteen välille on muodostunut jonkinlainen pidempiaikaisempi luottamussuhde.[701]

Tietolähteenä ei käsitellä poliisin tai muun esitutkintaviranomaisen antamia tietoja. Esitutkintaviranomaisia ovat poliisin lisäksi ETL 2:1.2:n mukaan rajavartio-, tulli- ja sotilasviranomaiset, jotka rajautuvat selvästi pois tietolähteen määritelmästä.[702] Yleisesti viranomaisten osalta taas voidaan viitata RL 40:11.1:n määritelmään virkamiehestä, mutta kyseinen rajaus ei ylety heihin.[703] Kirjoitushetkellä lainsäädäntö on muuttumassa siten, että myös virkamiehet suljetaan säännöksestä pois. Rajaus on kuitenkin edelleen ongelmallinen, koska se ei sulje pois poliisin erilaisia sidosryhmiä tai muita yhteistyötahoja, jotka voivat toimittaa tietoa poliisille muutenkin kuin satunnaisesti.[704] Tietolähteeksi pitäisi laskea tämän tulkinnan perusteella tahot, jotka toimittavat toistuvasti tietylle yksittäiselle poliisiprofiilille

[698] Tietolähdetoimintaa ei ole sidottu pelkkään rikostorjuntaan, josta esimerkkinä voidaan mainita tilanne, jossa tietolähteeltä saadaan aseharrastajan terveydentilaa koskeva tieto, joka voi johtaa esimerkiksi ampuma-aseluvan peruuttamiseen. Ks. HE 224/2010 vp, s. 124. Ks. myös HE 266/2004, s. 24 ja 35, jonka mukaan tietolähdetoimintaa voidaan käyttää myös järjestyshäiriöiden torjunnassa.

[699] Myöskään pakkokeinolaissa ei ole mitään tiettyä rikoksen rangaistukseen sidottua rajaa tilanteista, joissa tietolähdettä voi käyttää. Siten se sopii järjestäytyneen rikollisuuden lisäksi niin sanottujen massarikostenkin selvittämiseen. Ks. HE 266/2004 vp, s. 24.

[700] HE 224/2010 vp, s. 125; HE 222/2010 vp, s. 347.

[701] Satunnaisuuteen sisältyväksi on laskettava myös samaan aiheeseen käyty keskustelu, joka voi mahdollisesti jatkua poliisi- tai peiteprofiililla tiettyyn aiheeseen liittyen useita päiviä. Kyse voi olla esimerkiksi viharikoksista epäillystä henkilöstä, johon liittyen kansalainen on lähettänyt vihjeen poliisille ja poliisi kyselee tilanteesta tarkentavia tietoja. Tämä vihjeen perusteella vuoropuhelu sisältyy siten satunnaisuuden käsitteen alle.

[702] Lisäksi esitutkintaan osallistuu ETL 2.1.3:n mukaan syyttäjä, mutta syyttäjä ei ole esitutkintalain mukainen esitutkintaviranomainen. Tietoliikennetiedusteluun liittyen tietolähteen määritelmää on tarkoitus tarkentaa siten, että esitutkintaviranomaisen sijaan mainitaan vain viranomainen, jolloin rajataan selkeästi muut kuin esitutkintaviranomaiset pois. Ks. tästä tarkemmin HE 202/2017 vp, s. 167.

[703] Säännöksen mukaan virkamiehellä tarkoitetaan henkilöä, joka on virka- tai siihen rinnastettavassa palvelussuhteessa valtioon, kuntaan taikka kuntayhtymään tai muuhun kuntien julkisoikeudelliseen yhteistoimintaelimeen, eduskuntaan, valtion liikelaitokseen taikka evankelisluterilaiseen kirkkoon tai ortodoksiseen kirkkokuntaan tai sen seurakuntaan tai seurakuntien yhteistoimintaelimeen, Ahvenanmaan maakuntaan, Suomen Pankkiin, Kansaneläkelaitokseen, Työterveyslaitokseen, kunnalliseen eläkelaitokseen, Kuntien takauskeskukseen tai kunnalliseen työmarkkinalaitokseen. Yleensä tiedonhankinta näihin tahoihin perustuu PolL 4:2:n sääntelyyn, eikä näissä tapauksissa ole kyse tietolähdetoiminnasta.

[704] Esimerkkinä voidaan mainita nuorten kanssa työtä tekevät sidosryhmät, jotka voivat välittää tietoa alueen nuorista poliisille. Pois lukien kuitenkin ne tapaukset, joissa tiedonsaanti perustuu PolL 4:3:ään. Ks. tähän liittyen HE 266/2004 vp, s.35.

vihjetietoa ja osapuolten välille on syntynyt luottamussuhde.[705] Toisaalta vaikka kyseessä olisi säännöllisesti poliisille tietoa toimittava henkilö ei sitä ole katsottava tietolähdetoiminnaksi, jos tieto lähetetään yleisesti poliisille vinkkikanavaan.[706]

Tietolähdettä koskevien tietojen käsittelystä ja palkkion maksusta säännellään vain poliisilain puolella, mutta sääntelyyn viitataan myös pakkokeinolain puolella (PolL 5:41 ja PKL 10:39.4).[707] Rekisteröidylle tietolähteelle voidaan maksaa palkkio, mutta perustellusta syystä palkkio voidaan maksaa myös rekisteröimättömälle tietolähteelle. Palkkion veronalaisuudesta säädetään erikseen (PolL 5:41.2).[708] Esitöissä ei ole avattu tarkemmin millaisista palkkiosummista on kyse ja millä eri keinoin palkkio voidaan maksaa.[709] Poliisilain 5 luvun 41 §:n 1 momentin mukaan tietolähdettä koskevat tiedot voidaan tallettaa henkilörekisteriin ja tietojen käsittelyyn sovelletaan henkilötietojen käsittelystä poliisitoimessa annettua lakia (761/2003).[710] Rekisteröinnin pakollisuus on lainsäädännöllisesti osittain epäselvää, mutta pääsääntönä on se, että tietolähde rekisteröidään.[711]

Tietolähdetoiminnalla on saatu tietoa etsintäkuulutettujen henkilöiden olinpaikasta, terrorismintorjuntaan liittyvää tietoa, tuotettu tietoa rikoshyödyn poisottamiseksi sekä kyetty

[705] Tällainen voi olla esimerkiksi yksittäinen henkilö, joka käyttää tiettyä keskustelupalstaa ja havaitessaan rikokseen viittaavaa toimintaa, toimittaa tämän tiedon aina tietylle nettipoliisille, johon hänelle on syntynyt luottamuksellinen suhde. Kyse voi myös olla palvelun ylläpitoon liittyvästä toiminnasta, jossa yksittäinen ylläpitäjä, moderaattori tai muu sivustolla toimiva on kiinteässä yhteistyössä yksittäisen nettipoliisin kanssa.

[706] Tällainen on esimerkiksi www.poliisi.fi/nettivinkki. Tulkintaa puoltaa esimerkiksi EPSA 3:14.1,1:n kirjaamisvelvoite osapuolista, jonka perusteella toisena osapuolena on tietty poliisimies.

[707] Pakkokeinolain puolelta viitataan myös Tullia ja Rajavartiolaitosta koskevaan lainsäädäntöön.

[708] Tietolähteelle maksettavasta palkkiosta päättää tietolähdetoiminnan toteuttamisesta vastaavan poliisimiehen esimies (EPSA 3:16).

[709] Tietolähdetoimintaan liittyvään palkkionmaksuun liittyy myös erilaisia moraalisia ongelmia. Onko esimerkiksi ongelmallista jos tietolähde on narkomaani, joka rahoittaa huumausaineiden käyttöä tietolähdepalkkioilla?

[710] Poliisin henkilötietojen käsittelyä koskeva lainsäädäntö on muuttumassa kirjoitushetkellä. Rekisteröimisestä ja tietolähteen hyväksymisestä päättää tietolähdetoiminnan toteuttamisesta vastaava poliisimies. Tietolähteeksi hyväksytty henkilö on rekisteröitävä poliisin henkilörekisteriin siten, ettei se vaaranna tietolähteen henkilöllisyyden salassa pysymistä. (EPSA 3:13). Tietolähdetoiminnasta on kirjattava 1) osapuolten tunnistetiedot, 2) kertomuksen pääasiallinen sisältö, 3) yhteydenpidon ajankohta, 4) yhteydenottotapa ja 5) palkkion maksu tietolähteelle (EPSA 3:14). Mainittakoon, että poliisin henkilötietojen käsittelystä annettu laki on muuttumassa tutkimuksentekohetkellä.

[711] Ks. HaVM 10/2005 vp, s. 16, jonka mukaan rekisteröimättä jättäminen voisi tulla kyseeseen vain aivan poikkeuksellisissa tapauksissa, jottei tietolähteet pääsisi käyttämään asemaansa hyväksi epäasiallisella tavalla. Kirjoitushetkellä odotellaan tuomiota Helsingin poliisilaitoksen tietolähdetoiminnan rekisteröintiin liittyen, jossa on ollut syytettynä laajasti nykyistä ja entistä poliisijohtoa. Syytteessä on vedottu esimerkiksi silloisen Sisäasiainministeriön asetukseen poliisin tiedonhankinnan järjestämisestä ja valvonnasta (174/2008) 12.2 §:ään, jonka mukaan hyväksytty tietolähde on rekisteröitävä. Ks. rekisteröinnin pakollisuuteen liittyen myös Rainiala 2009, s. 125–126. Tällä hetkellä rekisteröityjä tietolähteitä poliisilla on valtakunnallisesti pitkälti toistasataa, mutta määrät vaihtelevat vuosittain. Ks. Poliisihallitus 2017a, s. 33

onnistuneesti estämään vakavia rikoksia.[712] Tietolähdetoiminta on tärkeää erityisesti sellaisilla poliisitoiminnan alueilla, joissa ei ole suoraa uhria tai kyseessä on ryhmittymä, joista on vaikea saada tietoa muutoin. Molempien osalta esimerkkeinä toimivat huumausainerikollisuuteen liittyvä toiminta ja terrorismissa kyse on monesti yhteisöistä, joista on muutoin vaikea saada tietoa.[713] Esimerkiksi englantilainen tiedustelupalvelu MI6 käyttää terrorisminvastaisessa taistelussa taktiikkaa, jossa se yrittää rekrytoida tiedottajiksi tietyn etnisen taustan omaavia henkilöitä, jotka voisivat tunnistaa äidinkielellisten syiden takia terrorismiin liittyvää viestintää paremmin.[714] Verrattuna reaalimaailmaan poliisi voi saada sosiaalisen median kautta helpommin tietoja ja todistusaineistoa, koska tiedonhankinnan kohteen sosiaalinen piiri on saatavilla kaverilistan muodossa ja poliisi voi olla heihin yhteydessä saadakseen tietoa kohteesta. Myös tietolähteenhankintatarkoituksessa.[715]

Poliisi arvioi tiedon luotettavuutta poliisin tiedustelujärjestelmään (POTI) tietoja kirjatessa, jossa lähteen luotettavuus ja tiedon oikeellisuus arvioidaan molemmat neliportaisella asteikolla.[716] Poliisi luokittelee lähteen luotettavuuden seuraavasti: A) viranomainen tai vastaava lähde, B) vakiintunut lähde, jonka aikaisemmin antamat rikosperusteiset tiedot ovat pääosin osoittautuneet paikkansa pitäväksi, C) vakiintunut lähde, jonka aikaisemmin antamat tiedot ovat pääosin osoittautuneet paikkansa pitämättömäksi ja X) tuntematon lähde, tunnistettu uusi lähde tai vakiintunut lähde, jonka ei vielä voida arvioida kuuluvan luokkiin B tai C taikka luokittelematon lähde. Lisäksi poliisi luokittelee tiedon oikeudellisuuden seuraavasti: 1) tosiasia, 2) oman käden tieto, 3) toisen käden tieto ja 4) huhu. Ensimmäisessä todenperäisyys on kiistaton (usein rekisteritieto). Toisen kohdan osalta kyse on tiedosta, jonka syntyyn tietolähteellä on välitön yhteys. Tietolähde on esimerkiksi itse nähnyt anastetun omaisuuden tai huumausaineen. Toisen käden tiedolla tarkoitettaan tietoa, jonka

[712] Poliisihallitus 2017a, s. 33.
[713] Miller – Gordon 2014, s. 232–233. Miller ja Gordon nostavat esille myös tietolähdetoiminnan negatiivisen puolen, jolla voi olla oikeasti heikko vaikutus rikollisuuden laskuun ja korruptoiva vaikutus poliisiin. Tästä meillä on Suomessakin tuore esimerkki, mutta useita myös maailmalta. Tämän takia Miller ja Gordon toteaakin, että tiedottajat tulisi aina rekisteröidä, yhteyshenkilön lisäksi tapaamisiin tulisi osallistua valvoja ja tiedottajien luotettavuutta tulisi arvioida sopivin väliajoin. Ks. myös Rainiala 2009, s. 19–20 ja 24–25, jossa esimerkkejä kansainvälisistä, mutta myös kansallisista poliiseja koskevista rikostapauksista.
[714] Awan 2012, s. 28.
[715] Trottier 2012, s. 151–152. Vaikka kyse ei ole yksittäisen yhteydenoton osalta tietolähdetoiminnasta, on nettipoliisi käyttänyt esimerkiksi kaverilistalta löytyviä henkilöitä apuna epäillyn henkilöllisyyden selvittämiseksi siten, että näihin kaverilistalla oleviin henkilöihin on oltu yhteydessä sosiaalisen median kautta. Esimerkkinä voidaan mainita tapaus, jossa uhrin raiskaukseen epäillyksi nimeämän Facebook-profiilin kaverilistalla olleilta tiedusteltiin epäillyn henkilöllisyyttä.
[716] Tiedon luokittelu tapahtuu asteikolla A1–X4, jossa X4-luokan tieto voi olla esimerkiksi anonyyminä nettivinkkiin lähetty tieto koulu-uhkauksesta.

syntyyn tietolähteellä on välillinen yhteys. Tietolähde on esimerkiksi kuullut tiedon henkilöltä, jolla on välitön yhteys tiedon syntyyn. Viimeisen kohdan, eli huhun kohdalla, kyseessä on tieto, joka on kulkenut useamman välikäden kautta. Huhuksi luokitellaan myös muihin luokkiin sopimattomat tiedot.[717]

Tietoverkkojen kohdalla herää myös kysymys siitä, voidaanko anonyymiä henkilöä käyttää tietolähteenä? Lainsäädäntö ei ota suoraan kantaa siihen, etteikö esimerkiksi poliisiprofiilin tietoverkoissa tapaamaan anonyymiä profiilia voisi rekisteröidä tietolähteeksi pelkillä profiilin tunnistetiedoilla. Toisaalta EPSA 3:13.1:ssä todetaan, että rekisteröiminen on tehtävä siten, ettei se vaaranna tietolähteen henkilöllisyyden salassa pysymistä, joka viittaa siihen, että henkilöllisyys tulisi olla tiedossa. PolL 5:40.2: ja PKL 10:39.2:n perusteella ongelmaksi nousee myös henkilökohtaisten ominaisuuksien arvioiminen, jos kyseessä on anonyymi henkilö.[718] On kuitenkin ongelmallista, jos poliisin tulisi kieltää anonyymiä profiilia lähettämästä toistuvasti tietoa tietystä aiheesta jos tieto voisi olla poliisin työn kannalta erittäin tärkeää. Sen takia tietoa tulisikin pystyä ottamaan vastaan, vaikka pyrkimyksenä tulisi olla koko tietolähdetoiminnan ajan luotua niin luottamuksellinen suhde, että tietolähteen henkilöllisyys saataisiin selville ja hänet voitaisiin rekisteröidä varsinaisilla henkilötiedoillaan tietolähteeksi.

Tietolähteen ohjatussa käytössä poliisi saa pyytää tietolähteeksi hyväksyttyä, henkilökohtaisilta ominaisuuksilta sopivaa, rekisteröityä ja tiedonhankintaan suostunutta henkilöä hankkimaan PolL 5:40:1:n tai PKL 10:39.1:n mukaisia tietoja.[719] Tietolähteen henkilökohtaisilla ominaisuuksilla tarkoitetaan sitä, että tietolähteellä ei saa olla epäasiallisia syitä tietolähteenä toimimiseen. Näitä ovat esitöiden mukaan esimerkiksi taloudellisen hyödyn tai muun edun tavoittelu sekä kosto.[720] *Rainiala* jakaa motiivit neljään eri ryhmään: 1) hyödyntavoittelu, 2) vastenmielisyys ja viha rikollisuutta kohtaan, 3) viranomaisten avustaminen ja 4) kilpailijoiden toiminnan haittaaminen tai poistaminen. Pääasiallisena motiivina Rainiala pitää hyödyntavoittelua.[721] Tietolähdetoimintaa käynnistettäessä tulisikin selvittää mikä motiivi tietolähteellä on lähteä tämän kaltaiseen toimintaan. Henkilön

[717] Poliisihallitus 2016c, s. 10.
[718] Toisaalta kyseistä säännöstä voidaan tulkita siten, että henkilökohtaisten ominaisuuksien vaatimus koskee vain ohjattu tietolähdetoimintaa. Omana erityiskysymyksenä tietolähteen hyväksyttävyyteen voidaan mainita myös alle 18-vuotiaat, joita ei lähtökohtaisesti käytetä poliisin tietolähteinä.
[719] Tietolähteen ohjatun käytön ulkopuolelle rajautuvat tilanteet, joissa tietolähde kertoo oma-aloitteisesti poliisille tätä oletettavasti kiinnostavista seikoista, joita poliisiviranomainen harkintansa mukaan hyödyntää. Ks. HE 224/2010 vp, s. 125; HE 222/2010 vp, s. 347.
[720] HE 224/2010 vp, s. 125; HE 222/2010 vp, s. 347–348.
[721] Rainiala 2009, s. 25.

suostumuksen tulee myös olla aina aidosti vapaaehtoinen, eikä poliisi saa painostaa tietolähdettä tiedonhankintaan lupaamalla etuja, joita ei voida voimassa olevan lainsäädännön perustella antaa. Lisäksi epäasiallinen riippuvuussuhde saattaa syntyä silloin, kun tietolähteestä muodostuu poliisille liian tärkeä muut tiedonhankintakeinot ohittava keino.[722] Tietolähdetoimintaa hoitavilla käsittelijöiden ei tulisi olla mukana asian esitutkinnassa, koska luottamus tehtävän asianmukaiseen hoitoon voisi vaarantua.[723]

Tietolähteen ohjatusta käytöstä päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka STEKPOV (PolL 5:41.1 ja PKL 10:40.1).[724] Päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan (PolL 5:41.2 ja PKL 10.40.2).[725] Päätös on tehtävä kirjallisesti ja päätöksessä on mainittava: 1) toimenpiteen esittäjä, 2) tiedonhankinnan toteuttava poliisiyksikkö ja sen toteuttamisesta vastaava poliisimies, 3) tunnistetiedot tietolähteestä, 4) toimenpiteen peruste[726], 5) tiedonhankinnan tavoite ja toteuttamissuunnitelma, 6) päätöksen voimassaoloaika ja 7) mahdolliset tietolähteen ohjatun käytön rajoitukset ja ehdot (PolL 5:42.3 ja PKL 10:40.3). Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava ja jos tietolähteen ohjattu käyttö lopetetaan, tulee siitä tehdä kirjallinen päätös (PolL 5:42.4 ja PKL 10:40.4). Tietolähteen ohjatussa käytössä on myös tiettyjä rajoituksia. Tietoja ei saa pyytää hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaisille kuuluvien toimivaltuuksien käyttöä tai vaarantaisi tietolähteen tai muun henkilön hengen tai terveyden.[727] Sallittua on kuitenkin se, että tietolähde liikkuu jo ennen ohjattua tietolähdetoimintaa tuntemansa rikollisryhmän parissa tai tapaa henkilöitä sekä keskustelee heidän kanssaan.[728] Tämän takia ennen tietolähteen ohjattua käyttöä tietolähteelle on tehtävä selkoa hänen oikeuksistaan ja velvollisuuksistaan sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta. Lisäksi tietolähteen turvallisuudesta on tarpeen mukaan huolehdittava tiedonhankinnan aikana ja sen jälkeen (PolL 5:40.3 ja PKL 10:39.3).

---

[722] HE 224/2010 vp, s. 125; HE 222/2010 vp, s. 347–348.
[723] Ks. Poliisihallitus 2018c, s. 36.
[724] Tietolähdetoiminnan kansallisena keskuksena toimii ja kehittämisestä vastaa keskusrikospoliisi muulla muin suojelupoliisin tehtäväalueella (EPSA 3:17).
[725] Poliisi- ja pakkokeinolain alkuperäisissä esitöissä puhuttiin kahden kuukauden määräajasta, mutta aikaa pidettiin liian lyhyenä, jonka takia poliisi- ja pakkokeinolakia muutettiin vielä ennen niiden voimaantuloa. Muutoksen yhteydessä todettiin tietolähteen ohjatun käytön rinnastuvan peitetoimintaan, jossa käytetään kuuden kuukauden määräaikaa. Lisäksi kiinnitettiin huomiota siihen, että salainen tiedonhankinta- tai pakkokeino tulee PolL 5:2.3:n tai PKL 10:2.3:n mukaisesti lopettaa ennen päätöksessä mainittua määräaikaa, jos käytön tarkoitus on saavutettu tai sen edellytyksiä enää ole. Ks. HE 16/2013 vp, s. 24; HE 14/2013 vp, s. 44–45.
[726] Pakkokeinolaissa 4 kohdassa puhutaan epäillystä rikoksesta.
[727] Ks. esimerkiksi *Allan v. Yhdistynyt kuningaskunta* (2002), jossa oli kyse kotietsintäsäännösten kiertämisestä.
[728] HE 224/2010 vp, s. 125; HE 222/2010 vp, s. 348.

Käytännössä rajan tulkitseminen voi olla tietoverkoissa haastavaa, koska lainsäätäjä ei ole avannut asiaa millään tavalla. Herääkin myös kysymys miten poliisimies voi täyttää PolL 5:40.3:n tai PKL 10:39.3:n velvollisuuden tehdä selkoa tietolähteen oikeuksista ja velvollisuuksista sekä erityisesti hänelle lain mukaan sallitusta ja kielletystä toiminnasta, kun tilanne on tietoverkkojen osalta esitöiden perusteella vähintäänkin epäselvä? Lisäksi lainsäädännössä ei ole rajattu ohjatun tietolähdetoiminnan tarkoitusta tiettyyn henkilöön kohdistuvaan tiedonhankintaan, vaan puhutaan yleisesti joko PolL 1:1:n tehtävien hoitamiseen tai pakkokeinolain osalta rikoksen selvittämistä koskevista merkittävistä tiedoista. Siten tietoverkoissa tiedonhankinta voi kohdistua esimerkiksi tiettyyn sivustoon, sosiaalisen median ryhmään tai yksittäiseen profiiliin, mutta myös näin kaikkiin yhtä aikaa.

Pyytämällä tietolähdettä seuraamaan yleisvalvontaan rinnastettavin tavoin tiettyyn ääriryhmään liittyvää avointa keskusteluryhmää, ei kyseinen toiminta tuota tulkintaongelmia ohjatun tietolähdetoiminnan toimivaltuuksien kiertämiskysymyksessä, koska kyseessä ei ole toimivaltuus.[729] Sama koskee myös tarkkailun piiriin kuuluvaa toimintaa, jossa tietolähde kerää tietoa lyhytaikaisesti tietystä henkilöstä (PolL 5:13.2 ja PKL 10:12.2). Jos poliisimies pyytää seuraamaan jonkun tietyn henkilön profiilia muutoin kuin lyhytaikaisesti on tällainen toiminta poliisin suorittamana suunnitelmallista tarkkailua (PolL 5:13.2 ja PKL 10:12.2). Tällöin toiminnan laillisuutta tulee arvioida sen perusteella mikä on ollut lähtötilanne. Jos tietolähde oli jo seurannut kyseistä henkilöä esimerkiksi tietyssä sosiaalisen median palvelussa voi tietolähde jatkaa seuraamista ja toimittaa tietoja henkilöstä poliisille. Tulkintaan ei vaikuta se onko kyseessä avoin vai muilta kuin kavereilta suljettu profiili. Tämä sen takia, että kyseessä on entuudestaan olemassa oleva kaverisuhde, eikä tiedonhankinnan takia tapahtunut soluttautuminen.[730] Rajanvetokysymyksiä ovat tilanteet, jossa tietolähde hakeutuisi poliisin pyynnöstä tietyn profiilin kaverilistalle. Jos kyseessä on poliisin nimenomainen pyyntö tietyn profiilin kaverilistalle pyrkimiseksi on tätä tulkittava toimivaltuuksien kiertämiseksi. Jos taas kyseessä on tietolähteen oma-aloitteinen kaveripyyntö johon poliisi ei ole omalla toiminnallaan vaikuttanut, on toiminta

[729] Tällainen voi olla esimerkiksi terrorismiin liittyvien tahojen sivustojen ja erilaisten videokanavien tarkkailu. Ks. tähän liittyen esimerkiksi Ammar – Xu 2018, s. 94–97, jossa kerrotaan ISIS-ryhmän laajamittaisesta sosiaalisen median käytöstä Facebookin, Twitterin ja yleisesti internetin avulla. Ks. Suomeen liittyvästä jihadistisestä viestinnästä tietoverkoissa kokonaisuudessaan Malkki – Pohjonen 2019.

[730] Ks. henkilösuhteiden entisyyden merkityksestä ohjattuun tietolähdetoimintaan HE 224/2010 vp, s. 125–126; HE 222/2010 vp, s. 348. Sama tulkinta koskee myös peiteltyä tiedonhankintaa ja peitetoimintaa.

lähtökohtaisesti sallittua vaikka kyseinen henkilö olisi muutoin ohjatun tietolähdetoiminnan piirissä.[731]

Oma erityiskysymyksensä muodostaa kuvakaappausten ottaminen. Eli voiko tietolähde toimittaa poliisille kuvakaappauksia ohjattuun tietolähdetoimintaan liittyen.[732] Kuvakaappausten ottamisessa oleellista on ensinnäkin se, onko kyse poliisin ohjaamasta tietolähdetoiminnasta, jossa poliisi on nimenomaisesti pyytänyt kuvakaappauksia. Vai onko kyse pelkästään passiivisesta tietolähdetoiminnasta, jossa tietolähde on toimittanut omasta aloitteestaan tietoa. EIT:n *van Vondel* -tapauksessa oli kyse tilanteesta, jossa tietolähteenä toiminut keskustelukumppani nauhoitti keskustelut viranomaisilta saamillaan laitteilla. EIT totesi, että jos kyseessä olisi ollut nauhoitus omaan käyttöön ei kyseessä olisi ollut EIS:n 8 artiklan vastainen toiminta.[733] Koska keskustelut nauhoitettiin rikos- tai muun tutkinnan yhteydessä yhteistyössä viranomaisten kanssa ja heidän antamalla tuella, katsoi EIT kyseessä olevan EIS:n 8 artiklan rikkomisen.[734] Merkitystä oli nimenomaan poliisiin ohjauksella ja heidän antamalla tuella välineistön ja neuvojen suhteen.

EIT päätyikin toisenlaiseen ratkaisuun *Shannon* -tapauksessa, jossa toimittaja oli nauhoittanut ja videoinut salaa hotellihuoneessa huumausainekauppaan liittyvät tapahtumat. Toimittaja oli myöhemmin antanut aineiston poliisille, joka oli aloittanut esitutkinnan ja asia oli johtanut tuomioon. Koska toimittaja ei ollut toiminut poliisin toimeksiannosta tai

---

[731] Esimerkkinä voidaan mainita tilanne, jossa tietolähde on mukana tietyssä ääri-ideologiaan suuntautuneessa suljetussa keskusteluryhmässä. Ryhmässä tietolähde tutustuu ja pyytää kaverilistalle joko ryhmään uutena liittyneen tai ryhmässä tapahtuneen keskustelun perusteella vanhan jäsenen. Jos kyseinen kaverilistalle lisääminen tapahtuu ilman poliisin nimenomaista ohjausta ja luonnollisena osana ryhmän toimintaa, voidaan tätä pitää vielä sallittuna toimintana. Ks. poliisin ohjaukseen liittyen esimerkiksi myöhemmin käsiteltävä *van Vondel* -tapaus.

[732] Kuvakaappaukset voisivat tulla kyseeseen erityisesti erilaisin yksityisyysasetuksin suljetusta sisällöstä, mutta toisaalta myös avoimista lähteistä, koska voi olla että tieto ei ole esillä kuin hetken aikaa.

[733] Ks. myös KKO 1981-II-182, jossa henkilö oli äänittänyt omassa asunnossa salaa keskustelun, jossa hän oli itse mukana. Korkein oikeus katsoi, että koska henkilö oli ollut itse mukana keskustelussa, ei kyseessä ollut rangaistava menettely.

[734] *van Vondel v. Alankomaat* (2007), kohta 49. Ks. myös *M.M. v. Alankomaat* (2003), jossa poliisi oli pyytänyt seksuaalirikoksen uhria nauhoittamaan puhelinkeskustelut ja myös tässä tapauksessa EIS:n 8 artiklaa katsottiin rikotun. Vrt. kuitenkin *Rajcoomar v. Yhdistynyt kuningaskunta* (2004), jossa EIT totesi, ettei valittajan toimet kuuluneet EIS 8 artiklan yksityiselämän suojan piiriin, koska hän oli itse aktiivisesti hakeutunut rikolliseen toimintaan ottamalla yhteyttä peitehenkilöllisyyden avulla soluttautuneisiin poliiseihin, jotta saisi rahaa vankilasta vapautumisensa jälkeen. Peitepoliiseihin yhteys oli luotu vankilassa tavatun toisen vangin avulla, joka oli poliisin tietolähde. Tilanteeseen ei vaikuttanut edes se, että idea huumausainerikokseen oli tullut poliisilta. Ks. myös EOA 14.11.1989 Dnro 1255/4/87, jossa Tulli oli pyytänyt salakuljetuksesta epäillyn nauhoittamaan keskustelun toisen henkilön kanssa. Vaikka oman keskustelun tallentaminen on lähtökohtaisesti laillista, ei poliisi EOA:n mukaan voi kiertää toimivaltuuksia pyytämällä nauhoittamaan keskusteluja.

muutoinkaan poliisin ohjaamana, eikä poliisilla ollut ennen tietojen luovuttamista edes tietoa asiasta, ei EIS:n oikeudenmukaisen oikeudenkäynnin 6 artiklaa oltu rikottu.[735]

Vaikka kuvakaappauksien ottamiseen ei poliisin tarvitse toimittaa tietolähteelle välineistöä niin näyttää siltä, että jo pelkkä poliisin ohjauksessa toimiminen estää kuvakaappauksien toimittamisen poliisille todisteeksi. Eli jos poliisi ohjeistaa ottamaan kuvakaappauksia esimerkiksi yksityisyysasetuksin suljetusta profiilista, on tätä pidettävä toimivaltuuksien kiertämisenä. Sama koskee lähtökohtaisesti myös tilannetta, jossa tietolähde antaisi esimerkiksi profiilinsa käyttäjätunnuksen ja salasanan poliisille sen takia, että se saisi näkyvyyden tietyn henkilön kaverilistalle tai suljettuun ryhmään. Jotta tällainen toiminta olisi sallittua tulisi siitä säätää erikseen poliisi- ja pakkokeinolaissa. Passiivisessa tietolähdetoiminnassa tällaisten kuvakaappausten toimittaminen poliisille on kuitenkin lähtökohtaisesti mahdollista, koska siihen ei liity poliisin aktiivista ohjaamista.[736]

Esitöiden mukaan sallittua tiedonhankintaa on yhteyden muodostaminen valeostajan ja valeoston kohteen välille, tai heidän tutustuttaminen toisiinsa.[737] Esitöissä todetaan, että tällaisen yhteyden luominen voi olla tietolähteen kannalta arveluttavaa, koska huumausainerikoksen tunnusmerkistö kattaa laajalti erilaisia tekomuotoja, jolloin tietolähteen toimintaa voitaisiin arvioida huumausainerikoksena tai avunantona siihen. Poliisin tulisi näissä tapauksissa toimia passiivisesti, jotta vältettäisiin rikosprovokaatio. Tällä pyritään välttämään se, ettei tietolähde syyllisty itse rikokseen tai että tietolähde ei saa toista henkilöä ryhtymään rikokseen. Toiminta ei saa johtaa siihen, että tietolähde syyllistyisi toiminnallaan rikokseen.[738] Esimerkiksi EIS:n 6 artiklan rikkomuksen toteamiseen päättyneessä *Vanyan* -tapauksessa, poliisi oli ohjeistanut huumausaineiden myyjää ja toiminut tämän kanssa yhteistyössä, jotta valittaja saataisiin paljastetuksi huumausainerikokseen. Vaikutusta oli lisäksi sillä, ettei poliisilla ollut tiedossa, että valittaja

[735] *Shannon v. Yhdistynyt kuningaskunta* (2005). Kyseisessä tapauksessa EIT näytti lähtevän siitä, ettei EIS 8 artikla sovellu tapaukseen, koska kyseessä ei ollut poliisin ohjauksessa tapahtuva toiminta. Ks. tästä tarkemmin Rainiala 2009, s. 60–61.

[736] Tältäkin osin voidaan joutua rajanvetotilanteisiin, jos poliisimies on esimerkiksi tietolähdettä tavatessaan yksilöinyt tiettyjä profiileja tai ryhmiä, joista poliisi on erityisen kiinnostunut. Jos tietolähde hakeutuu tällaisten profiilien ja ryhmien pariin poliisimiehen kanssa käytyyn keskusteluun liittyen, ollaan lähellä kiellettyä ohjattua tietolähdetoimintaa ja todistusaineisto voidaan asettaa hyödyntämiskieltoon. Ks. myös hyödyntämiskiellon etäisvaikutuksesta Pölönen – Tapanila 2015, s. 250 ja 326.

[737] Lisäksi tietolähde voi välittää myös tietoja ja toimia rajoitetusti esimerkiksi tulkkina. Vuoden 1995 poliisilaissa ei vielä säännelty tietolähdetoiminnasta, mutta otettiin kantaa niin sanottuihin välimiehiin, jotka välittivät viestejä poliisin ja kohteen välillä valeostoihin liittyen. Jo tällöin välimiehen asema katsottiin oikeudelliselta kannalta haastavaksi ja näihin tuli lähtökohtaisesti suhtautua pidättyvästi. Ks. HE 34/1999 vp, s. 22.

[738] HE 224/2010 vp, s. 126; HE 222/2010 vp, s. 348.

olisi aikaisemmin ollut tekemisissä huumausainerikollisuuden kanssa.[739] Tällaista tietolähteen osallistuvaa toimintaa harkittiin hallituksen esitykseen 266/2004 vp liittyen, mutta koska se poikkesi niin paljon silloisesta tietolähdetoimintamuodoista joita tuolloin sovellettiin, ei sääntelyä katsottu tarpeelliseksi.[740]

Tällä hetkellä tietolähde ei saa osallistua minkäänlaiseen rikolliseen toimintaan, millä on suora vaikutus tietolähteen kykyyn tuottaa tietoa vakavasta ja järjestäytyneestä rikollisuudesta.[741] Tietoverkkojen osalta poliisin tulisi esimerkiksi kirjata rikosilmoitus tilanteissa, joissa tietolähde toimittaa darknetissä myydyt huumausaineet noutopaikkaan, lähettää näitä postitse eteenpäin tai toimii pyynnöstä profiilien käyttäjänä.[742] Oman vaikeutensa nykytilanteeseen tuottaa myös vaatimus tietolähteen ja hänen läheistensä turvallisuudesta huolehtimisesta ohjatun käytön aikana ja sen jälkeen. Jos tietolähteen ohjattu käyttö jouduttaisiin PolL 5:58:n tai PKL 10:60:n mukaisesti paljastamaan, tarkoittaisi se käytännössä sitä, että poliisi olisi velvollinen suorittamaan henkilöturvallisuustoimenpiteitä tietolähteen suojaamiseksi.[743] Käytännössä tietolähteen ohjatun käytön käyttömahdollisuudet jäävätkin erittäin kapeiksi, vaikka tietolähteellä on olevinaan lain mukaan nimenomainen mahdollisuus hankkia tietoa.[744] Nykytilanne ei olekaan ohjatun tietolähteen tai poliisimiehen oikeusturvan kannalta tyydyttävä.[745]

---

[739] *Vanyan v. Venäjä* (2005), kohdat 49–50. EIT katsoi, ettei ollut tarvetta tulkita EIS:n 8 artiklan rikkomista, koska jo 6 artiklan rikkominen oli selvä. Ks. kohdat 69–70. Ks. myös samantyylisestä tapauksesta syyttäjää koskevan lahjonnan osalta *Ramanauskas.v. Liettua* (2008), jossa käytettiin tietolähdettä välimiehenä.

[740] Ks. HE 266/2004 vp, s. 6. Toisaalta tämä poikkeavuus asettuu mielenkiintoiseen valoon, koska jo aikaisemmin oli käyty oikeutta tilanteista, joissa poliisin epäiltiin käyttäneen tietolähteitä rikolliseen toimintaan. Ks. ratkaisut Helsingin HO 14.11.1996 R 96/1503 ja 8.2.2000 R 98/1662 sekä Helsingin KO 1.8.1995 R 95/2808.

[741] Ks. tietolähteen suhteesta rikoksentekijöihin ja rikollisuuteen Rainiala 2009, s. 106–110. Rainiala jakaa rikollisen alakulttuurin osa-alueet seuraavasti: 1) kantarikollisten ydin, 2) alakulttuurin välialueen puoliammattilaiset, 3) alakulttuurin perifeerinen osa ja 4) rikolliseen alakulttuuriin kuulumattomat henkilöt. Mitä lähempänä tietolähde on kantarikollisten ydintä, sitä tärkeämpää sen voidaan katsoa olevan vakavan ja järjestäytyneen rikollisuuden torjunnassa. Ks. myös Mäkipää 2008, s. 593–594.

[742] Teoriassa poliisi voisi siirtää rikokseen puuttumista PolL 5:46.1:n tai PKL 10:47.1:n perusteella tietolähteen osalta ja suorittaa operaation loppuun. Tämä olisi ongelmallista erityisesti PolL 5:40.3:n ja PKL 10:39.3:n takia, koska poliisimiehen olisi tullut tehdä selvää tietolähteelle hänen oikeuksista ja velvollisuuksista sekä siitä mikä on hänelle lain mukaan sallittua tai kiellettyä.

[743] HE 224/2010 vp, s. 126; HE 222/2010 vp, s. 348. Ks. tähän liittyen myös *Teixeira de Castro v. Portugali* (1998).

[744] Hankkiminen viittaa tietolähteen aktiiviseen toimintaan, joka liittyy vahvasti vuorovaikutukseen muiden ihmisten kanssa. Oman ongelmansa tuottaa tosin myös se, että tietolähdettä ei ole erikseen koulutettu peitetoimintamaiseen työhön eikä hän toimi virkavastuulla. Puhumattakaan siitä, miten poliisimies voisi tehokkaasti valvoa tietolähteen toiminnan laillisuutta.

[745] Ks. Mäkipää LM 2008, s. 589–590. Tilanne oli sama jo ennen vuoden 2014 uudistusta, vaikka vasta tuolloin lainsäädäntöön tuli uutena tietolähteen ohjattu käyttö. Huomioon voidaan ottaa tässä yhteydessä lainsäädäntökehitys esimerkiksi RL 6:8a:n osalta, jossa rikoksesta tuomittu voi saada kolmanneksen alennuksen tuomioonsa tunnustuksen perusteella tai muuttaa vankeustuomion sakoksi.

# 8 JOHTOPÄÄTÖKSET

Teoriassa perus- ja ihmisoikeudet vallitsevat identtisinä reaalimaailmassa ja tietoverkoissa, mutta tutkimuksessa on tuotu esille selvät erot salaisten tiedonhankinta- ja pakkokeinojen välillä näissä ympäristöissä. Tähän liittyen ensimmäinen tutkimuskysymys kuului,

> 1) miten salaisiin tiedonhankinta- ja pakkokeinoihin liittyvät perus- ja ihmisoikeussuojatarpeet eroavat reaalimaailmassa ja tietoverkoissa sekä millainen vaikutus eroilla tulisi olla toimivaltuussäännöksiin?

**Kotirauhan suoja ja luottamuksellinen viestintä**

Tietoverkoissa kotirauhan suojan merkitys on minimaalinen, koska kotirauhan suojan tarkoituksena ei ole suojata toimintaa avoimissa tietoverkoissa. Luottamuksellisen viestin suojan osaltakin haasteet kohdistuvat lähinnä luottamuksellisten viestien ja verkkoviestien väliin jääviin rajanvetotilanteisiin. Viestinnän luottamuksellisuuden problematiikka tietoverkoissa poliisi- ja peiteprofiileilla voidaan karkeasti jakaa 1) *luottamuksellisen viestinnän*, 2) *suljetussa ryhmässä tai profiilissa tapahtuvan viestinnän* ja 3) *verkkoviestin* välille. Mitä lähempänä luottamuksellista viestintää poliisin toiminta on, sitä vahvemmin se puuttuu henkilön yksityiselämän suojaan. Voidaan myös todeta, että yksittäisen henkilön profiilissa tapahtuva viestintä on jo lähtökohtaisestikin lähempänä yksityiselämän suojan ydinaluetta, kuin ryhmässä tapahtuva viestintä.

Suljetussa ryhmässä tai profiilissa tapahtuvan viestinnän suojan eroja tulee arvioida tapauskohtaisesti. Ensinnäkin kyse tulee olla tilanteesta, jossa 1) viestintä ei ole enää nähtävissä ryhmään tai profiilin kaverilistalle uutena hyväksytyille, koska muutoin kyse on miltei aina verkkoviestistä.[746] Jos viestit eivät ole enää jälkikäteen liittyvien nähtävissä, merkitystä viestinnän luottamuksellisuuteen on sillä 2) kuinka laajasta ryhmästä tai kaverilistasta on kyse ja 3) mitä tarkoitusta varten ryhmä tai profiili on luotu. Mitä

[746] Muunlainen tulkinta voisi tulla kyseeseen tilanteissa, jossa alkuperäiset viestitkin olisi lähetetty hyvin suppealle muutaman henkilön ryhmälle. Näissä vallitsee yleensä keskinäinen yhteisymmärrys siitä, että viestintä on tarkoitettu vain kyseiselle ryhmälle ja mahdollisesti siihen myöhemmin liitettävien tietoon.

suppeammasta ryhmästä on kyse, sitä lähempänä se on luottamuksellista viestintää ja yksityiselämän suojan ydinaluetta. Sama koskee myös henkilön lähipiiriä, jossa jaetaan yleensä arkaluontoisia yksityiselämän piiriin kuuluvia asioita. Lisäksi ryhmän tai kaverilistan 4) hyväksymisprosessilla voidaan katsoa olevan merkitystä viestinnän luottamuksellisuudelle. Mitä tiukemmalla seulalla henkilöitä hyväksytään kaverilistalle tai ryhmään, sitä korostuneempi rooli perusoikeussuojalla on. Lainsäätäjän tulisikin arvioida *de lege ferenda* ”tietoverkkojen kotirauhan” suojan vaikutusta salaisiin tiedonhankinta- ja pakkokeinoihin luottamuksellisen viestinnän ja verkkoviestin välisessä maastossa.

**Yksityiselämän suoja**

Laajempia tulkintaongelmia salaisten tiedonhankinta- ja pakkokeinojen näkökulmasta tietoverkoissa tuottaa yksityiselämän suojan tasot tietoverkoissa verrattuna reaalimaailmaan, vaikka ne ovatkin osittain päällekkäisiä luottamuksellisen viestinnän problematiikkaan liittyen. Tässä tutkimuksessa suojan eroja on arvioitu 1*) tiedon syntymistavan*, 2) *henkilön yksilöimisen ja tunnistamisen*, 3) *tiedonhankinnan kohteen*, 4) *tiedon keräämistavan, reaaliaikaisuuden ja laajuuden* sekä 5) *tiedon laadun ja luotettavuuden* alaotsikoiden alla. Reaalimaailman ja tietoverkkojen erojen vaikutus tulisi *de lege ferenda* arvioida kokonaisvaltaisesti salaisiin tiedonhankinta- ja pakkokeinoihin liittyen.

*Tiedon syntymistapa*

Tiedon syntymistapa itsessään muodostaa jo perustavanlaatuisen eron reaalimaailman henkilön *oleskeluun* ja tietoverkkojen *julkaisuun* perustuvan tiedon syntymistavan takia. Reaalimaailmassa tiedonhankinta perustuu oleskeluun, kun tietoverkoissa tiedonhankinta kohdistuu julkaisemiseen.[747] Tietoverkkojen globaalin ja koko ajan saatavilla olevan luonteen takia tietoverkkojen yksityiselämän suojan tarve ei ole yhtä vahva kuin reaalimaailmassa. Tämä koskee tarkkailutyyppisiä keinoja siinä missä erityisiä toimivaltuuksiakin.

*Henkilön yksilöiminen ja tunnistaminen*

Henkilön yksilöimiseen ja tunnistamiseen liittyvä problematiikka on tunnistettu osittain salaisia tiedonhankinta- ja pakkokeinoja koskevissa esitöissä. Poliisi- ja pakkokeinolain esitöiden mukaan tietoverkoissa tapahtuvalle ihmisten väliselle vuorovaikutukselle on

[747] Tietoverkkojen syntymistapa liittyy myös luottamuksellisen viestinnän ja verkkoviestin väliseen maastoon, jota on käsitelty edellä.

luonteenomaista tietynlainen toimivien henkilöiden identiteettien epäselvyys. Tämä johtuu siitä, että tietoverkoissa käytetään esimerkiksi nimimerkkejä tai muita vastaavia henkilöiden yksilöintitapoja. Kyseisen huomion vaikutus on kuitenkin jäänyt vähäiseksi arvioitaessa eroja yksityiselämän suojan osalta reaalimaailman ja tietoverkkojen välillä, eikä niillä ole ollut juurikaan vaikutusta sääntelyyn.[748] Lisäksi esityöt tunnistavat vain henkilön tunnistamiseen liittyvän problematiikan, vaikka jo yksittäisen henkilön yksilöiminen tietoverkoista on ongelmallista.

Reaalimaailmassa henkilö on aina yksilöitävissä ja yleensä tunnistettavissa, mutta tietoverkoissa tähän vaikuttavat useat epävarmuustekijät. Tietoverkoissa tunnistamiseen liittyvä problematiikka voidaan jakaa esiintymiseen 1) *todellisilla tiedoilla*, 2) *pseudonyyminä*, 3) *anonyyminä*, 4) *toisena henkilönä*, 5) *yhteiskäyttöroolissa* tai kyse voi olla 6) *keinoälyyn* perustuvasta viestinnästä. Tietoverkoissa henkilö ei ole yleensä yksilöitävissä tai tunnistettavissa, koska täyden varmuuden saaminen on erityisesti tarkkailutyylisten keinojen osalta miltei mahdotonta. Voidaankin todeta, että tietoverkkojen yksilöimistä ja tunnistettavuutta koskevan epävarmuuden tulisi vaikuttaa selvemmin yksityiselämän suojan tasoon. Etenkin kun avoimessa tietoverkoissa henkilö voi itse reaalimaailmaa helpommin määritellä yksityisyytensä tason. Tämä koskee erityisesti tarkkailutyyppisiä keinoja, mutta myös erityisiä toimivaltuuksia, ellei kyse ole reaalimaailmaan toimintaan rinnastettavasta webkamerayhteydestä.[749] Voidaankin todeta, että tietoverkkojen yksilöimistä ja tunnistettavuutta koskevan epäluotettavuuden tulisi vaikuttaa selvemmin eri toimivaltuussäännöksiin, koska perusoikeussuojan tarve ei ole niin kattava kuin reaalimaailmassa.

*Tiedonhankinnan kohde*

Tunnistamiseen ja yksilöimiseen liittyvä problematiikka on yhteydessä tiedonhankinnan kohteen hahmottamisongelmiin tietoverkoissa. Tiedonhankinnan kohteeseen liittyvä problematiikka voidaan jakaa tietoverkoissa 1) *kohdehenkilön omaan toimintaan*, 2) *muiden tuottamaan tietoon* ja 3) *muuhun tietotoverkoista saatavaan tietoon*. Kohdehenkilön itse tuottaman tiedon osalta tilanne on selvä, mutta muiden tuottaman ja kohdehenkilöstä riippumattoman tiedon kerääminen rinnastuu mieluumminkin vinkkitietoon sekä erilaisiin

[748] Käytännössä ero on otettu huomioon poliisi- ja peiteprofiileilla mahdollisten keinojen osalta vain peitetoimintaa koskevan sääntelyn erityisissä edellytyksissä.
[749] Tutkimuksessa on tosin tuotu esille se, että nykytekniikalla edes webkamerayhteys ei riitä varmistamaan sitä, että kyseessä on todella tietty yksittäinen henkilö, koska kyseessä voi olla digitaalisesti luotu hahmo.

poliisin suorittamiin rekisterikyselyihin. Tietoverkoissa kohteena on reaalimaailman kohdehenkilön fyysisen toiminnan sijaan eri henkilöiden tietoverkkoihin lisäämä data. Yksityiselämän suojan näkökulmasta voidaan todeta, että mitä kauempana ja mitä vähemmän vuorovaikutuksessa viestintä tapahtuu kohdehenkilöön nähden, sitä kauempana se on kohdehenkilön yksityiselämän suojan ydinalueelta. Tämä koskee erityisesti tarkkailutyyppisiä toimivaltuuksia, koska erityisissä toimivaltuuksissa ollaan yleensä tekemisissä nimenomaan kohdehenkilön kanssa.

*Tiedon keräämistapa, reaaliaikaisuus ja laajuus*

Reaalimaailmassa tietoa kerätään fyysisiin ja tosiasiallisiin aistihavaintoihin perustuen, mutta teknisen tarkkailun kohdalla myös teknisillä laitteilla. Reaalimaailmassa kyse on tiettyyn paikkaan ja aikaan sidotuista reaaliaikaisista ja pistemäisistä tiedonkeruutilanteista, kun taas tietoverkoissa tiedon kerääminen on mahdollista globaalisti ja jatkuvasti saatavilla olevasta datasta. Tiedon kerääminen voi tapahtua fyysisten aistihavaintojen lisäksi erilaisin hakutoiminnoin tai koneellisesti, joka mahdollistaa laajojen datamassojen keräämisen yksittäisen käyttäjän profiileista vuosienkin ajalta. Ero koskee erityisesti tarkkailutyyppisiä toimenpiteitä, mutta myös erityisiä toimivaltuuksia. Tämä sen takia, että peitetoiminnan turvin voidaan hakeutua kohdehenkilön kaverilistalle, jossa voi aueta suuri määrä tietoa. Tietoverkkoja koskevan laajan tiedonkeruumahdollisuuksien takia voidaan katsoa, että tietoverkoissa tapahtuvaa tiedonhankintaa tulisi suojata yksityiselämän suojan näkökulmasta vahvemmin kuin reaalimaailmassa.

*Tiedon laatu ja luotettavuus*

Tiedon laajuudella ei ole välttämättä suoraa vaikutusta tiedon laatuun, joten tiedon arkaluontoisuus ja siten puuttumisen voimakkuus yksityiselämän suojan piiriin riippuu satunnaisista syistä. Reaalimaailman tiedonhankinnassa on tehty eroja äänen, kuvan ja sijaintitiedon välille, mutta tämä ei sovellu tietoverkkojen datan arviointiin. Tietoverkoissa korostuvat kuitenkin tiedon laadun näkökulmasta laajojen tietomassojen analysointimahdollisuudet, joiden takia vähäpätöiseltäkin vaikuttavalla tiedolla voi olla käytännössä vaikutusta. Ero koskee tarkkailutyyppisiä, mutta myös erityisiä toimivaltuuksia.

Merkittävä vaikutus tiedon laatuun – mutta myös yleisesti tiedonhankintaan tietoverkoissa – on tiedon luotettavuudella. Jo esitutkinta- ja pakkokeinolakia koskevassa komiteamietintövaiheessa vuonna 2009 ihmisten vuorovaikutukseen tietoverkoissa kuvattiin

olevan luonteenomaista tietynlainen epäluottamus. Tätä vaikutusta ei kuitenkaan otettu ainakaan lainvalmisteluaineiston perusteella huomioon yksittäisten toimivaltuuksien kohdalla. Tietoverkoista kerätyn tiedon laatua voidaan arvioida luotettavuuden näkökulmasta joko 1) poliisin toiminnan tai 2) kohdehenkilön toiminnan perusteella. Tietoverkoissa tapahtuvassa toiminnassa dokumentoinnin toteuttamisen helppous ja tarkkuus ovat esimerkiksi vaikuttaneet siihen, että peitetoiminnan erityisten edellytysten raja on tietoverkoissa alempi kuin reaalimaailmassa. Muihin säännöksiin tämä ei ole jostain syystä vaikuttanut. Kohdehenkilön toimintaan liittyen tiedon voidaan katsoa olevan lähtökohtaisesti epäluotettavaa, koska tiedon luotettavuus perustuu kohdehenkilön tai muiden julkaisupäätökseen. Vaikka tietoverkoista kerätyt laajat tietomassat voivat mahdollistaa tarkan ja tehokkaan analyysin kohdehenkilöstä ja hänen ominaisuuksistaan, muodostaa tiedon luotettavuuteen liittyvät ongelmat perustavanlaatuisen eron yksityiselämän suojan tarpeen näkökulmasta. Erityisesti tämä koskee tarkkailutyyppisiä keinoja. Erityisten toimivaltuuksienkin osalta tiedon heikko luotettavuusarvo on omiaan heikentämään tiedonkeruumahdollisuuksien ja laajuuden suojan tarvetta tietoverkkojen osalta suhteessa reaalimaailmaan.

**Yleiset ja erityiset edellytykset sekä muut oikeusturvatakeet**

Yleiset edellytykset jaetaan 1) tuloksellisuusodotukseen, 2) erittäin tärkeä merkitys -edellytykseen ja 3) välttämättömyysvaatimukseen. Perus- ja ihmisoikeusnäkökulma on ollut oleellisessa roolissa yleisten edellytysten säätämisessä ja koska reaalimaailman ja tietoverkkojen osalta on havaittavissa selkeitä eroja, olisi edellytyksiä tullut arvioida tästä näkökulmasta tarkemmin. Yleisiin edellytyksiin liittyy kiinteästi yhteys erityisiin edellytyksiin. Erityisiä edellytyksiä ei ole lainsäädännössä tai oikeuskirjallisuudessa systematisoitu kokonaisuutena, vaan yleensä tarkastelu on jäänyt rikosnimikkeen ja rangaistusmaksimin tasolle. Erityiset edellytykset voidaan jakaa salaisten tiedonhankinta- ja pakkokeinojen osalta seuraavasti:

1) *rikosnimike*,
2) *rangaistusmaksimi,*
3) *kohdehenkilön asema*,
4) *kohteen laatu ja sijainti*,
5) *suostumus*

6) *henkeä ja terveyttä välittömästi uhkaava vaara* ja
7) *erityisten edellytysten säännöskohtaiset rajoitukset*.[750]

Tietoverkkojen vaikutus on jäänyt vain yksittäisten säännösten varaan, eikä arviointia ole tehty suhteessa yleisiin edellytyksiin. Esimerkkinä tästä voidaan mainita peitetoiminta tietoverkossa, jossa erityiset edellytykset ovat lievemmät kuin reaalimaailman peitetoiminnassa, mutta yleiset edellytykset ovat samat. Peitelty tiedonhankinta taas toimii esimerkkinä tilanteesta, jossa peitetoiminnasta poiketen ei tietoverkkoja ole huomioitu edes erityisissä edellytyksissä mitenkään, vaikka samat kevennykseen johtaneet perusteet pätevät myös peiteltyyn tiedonhankintaan.[751] *De lege ferenda* tulisi ottaa huomioon tutkimuksessa esitetyt erot yksityiselämän suojan reaalimaailman ja tietoverkkojen välillä arvioitaessa yleisten ja erityisten edellytysten sääntelyä. Tämä arviointi tulisi tehdä lainsäätäjän toimesta selvemmin loogisena kokonaisuutena ottaen mukaan yleisten ja erityisten edellytysten lisäksi myös erilaiset oikeusturvatakeet.

**Poliisiprofiili**

Jotta salaisia tiedonhankinta- ja pakkokeinoja poliisi- ja peiteprofiileilla mahdollisia toimivaltuuksia voidaan kuvata tarkemmin, tulee määritellä mitä poliisi- ja peiteprofiilit ovat. Tämän takia on tutkimuksessa on vastattu kysymykseen,

| |
|---|
| 2) mikä on poliisiprofiili ja miten se liittyy salaisiin tiedonhankinta- ja pakkokeinoihin? |

Nettipoliisitoiminnaksi kutsutaan lähtökohtaisesti toimintaa, jossa poliisimies tekee työtä sosiaalisessa mediassa poliisiprofiililla joko täysipäiväisesti tai käyttäen sosiaalista mediaa työkaluna omassa työssään. Profiili luodaan omalla nimellä ja kuvalla, joten kyseessä ei ole salassa tapahtuva toiminta, vaan päinvastoin tarkoituksena on saada mahdollisimman suuri näkyvyys ennalta estävässä mielessä. Reaalimaailman ja tietoverkkojen luonteesta johtuen poliisin näkyväkin toiminta eroaa siten, että tietynlainen salainen tiedonhankinta on mahdollista myös näkyvällä poliisiprofiililla. Salaisista tiedonhankinta- ja pakkokeinoista

[750] Kyseiset edellytykset eroavat sen mukaan, onko kyse rikosten estämisestä, paljastamisesta tai selvittämisestä.
[751] Esitöissä mainitut perusteet olivat tietoverkkojen anonyymi luonne, dokumentoinnin helppous ja tarkkuus sekä vähäisemmät turvallisuusriskit.

tulee kyseeseen tarkkailu (PolL 5:13.1 ja PKL 10:12.1), suunnitelmallinen tarkkailu (PolL 5:13.2 ja PKL 10:12.2) ja tietolähteen ohjattu käyttö (PolL 5:40.2 ja PKL 10:39.2). Näiden lisäksi mahdollista on myös yleisvalvonta.

**Siviiliprofiili**

Poliisi- ja peiteprofiileihin liittyy myös poliisimiehen siviiliprofiilin käyttöön liittyvä problematiikka. Siinä missä poliisimiehen vapaa-ajalla tapahtuvaa asiakkaiden seuraamista voidaan pitää äärimmäisenä poikkeuksena, ei ole mitenkään tavatonta etteikö poliisimies kohtaisi asiakkaita erilaisissa sosiaalisen median palveluissa siviiliprofiilillaan. Tutkimuksessa aiheeseen liittyen kysyttiin,

> 3) onko poliisimiehellä mahdollisuus käyttää omaa siviiliprofiiliaan salaisessa tiedonhankinnassa?

Eroja työtehtävän ja vapaa-ajan toiminnan välillä voidaan arvioitiin seuraavin kriteerein: 1) *mitä tarkoitusta varten ja millä tiedoilla siviiliprofiili on luotu?* 2) *onko kyseessä salainen tiedonhankinta- tai pakkokeino?* 3*) onko poliisilla vireillä toimintaa tiedonhankinnan kohteena olevaan henkilöön liittyen?* 4) *missä, milloin ja millä laitteella tiedonhankinta tapahtuu?* 5) *tapahtuuko tiedonhankinta esimiehen ohjauksessa?*. Käytännössä poliisimiehen mahdollisuudet omatoimiseen tiedonhankintaan siviiliprofiililla ovat kuitenkin minimaaliset, koska myös salainen tiedonhankinta on esimiesohjattua toimintaa. Lisäksi eri toimivaltuuksien muotomääräyksiä on noudatettava myös siviiliprofiililla toimiessa, joka rajoittaa erityisesti päätöksentekijätason takia toimintaa. Toimivaltuuksien käytön tulisikin aina perustua työn puolesta luotujen profiilien käyttöön.

**Peiteprofiilit ja suojaamissääntely**

Salaiset tiedonhankinta- ja pakkokeinot perustuvat näkyviä poliisiprofiileja laajemmin peiteprofiilien käyttöön. Peiteprofiilin luomiseen liittyvään problematiikkaan liittyen on tutkimuksessa esitetty kysymys,

4) mikä on peiteprofiili ja miten suojaamissääntely liittyy sen luomiseen sekä käyttöön?

*Peiteprofiilin luominen*

Peiteprofiilin osalta päätös sen luomisesta perustuu yleisesti PolL 5:46.2:n ja PKL 10:47.2:n suojaamissääntelyyn. Suojaamissäännöksessä ei ole kyse poliisin toimivaltuudesta, vaan sillä pyritään turvaamaan jo olemassa olevien keinojen tehokas käyttäminen niiden erityisluonne huomioon ottaen.[752] Tutkimuksessa on tuotu esille problematiikka rekisterin käsitteen kanssa, jonka osalta rekisterin määritelmää ja siten myös päätöksentekijätasoa tulisi tarkentaa *de lege ferenda* siten, että vain viranomaisen ylläpitämistä rekistereistä katsottaisiin sääntelyn mukaiseksi rekisteriksi. Myös asiakirjan sääntelyä tulisi tarkistaa samoin.

Käytännössä on mahdollista luoda peiteprofiileja myös pelkkää tarkkailua ja yleisvalvontaa varten, vaikka niitä ei olekaan mainittu PolL 5:2:n tai PKL 10:2:n salaisia tiedonhankinta- tai pakkokeinoja koskevassa luettelossa. Tämä perustuu siihen, että niin sanotun kevyen valeprofiilin luomiseen ei tarvita mitään sellaisia tietoja, jotka poikkeaisivat reaalimaailman poliisimiehen siviilivaatetuksesta, leasing-ajoneuvon tai prepaid-liittymän käytöstä. Näissä ei käytetä suojaamissääntelyä. Toiminnalla ei myöskään puututa kenenkään oikeuksiin siinä määrin, että asiasta tulisi säätää tarkemmin. Etenkin kun lainsäätäjä on nimenomaisesti sanonut, että kyseessä ei ole toimivaltuus. *De lege ferenda* olisi kuitenkin selvempää, jos lainsäätäjä toisi myös perusmuotoisen tarkkailun ja yleisvalvonnan tietoverkoissa suojaamissääntelyn piiriin.

*Rikoksiin puuttumisen siirtäminen*

Suojaamissääntelyyn liittyy myös PolL 5:46.1:ä ja PKL 10:47.1:ä, joissa on kyse poliisin mahdollisuudesta siirtää puuttumista rikokseen. Problematiikka sen suhteen voidaan tietoverkoissa jakaa 1) *välittömään puuttumiseen* ja 2) *rikosepäilyjen suureen määrään*. Välitön puuttuminen on tietoverkoissa voi olla mahdotonta, vaikka kyse olisi akuutista ja vakavaa vaaraa aiheuttavasta tilanteesta. Tämä johtuu lähinnä tietoverkkojen anonyymistä luonteesta. Sääntely ei siten ole tietoverkoissa kovinkaan realistinen. Sama koskee myös

[752] Toisaalta mahdollisuudet tehdä rekisterimerkintöjä ja valmistaa asiakirjoja puoltavat toimivaltuusluonteista sääntelyä.

rikosepäilyjen suurta määrää, jossa esimerkiksi huumausaineiden myymiseen liittyvällä palstalla jokaisesta havaitusta myynti-ilmoituksesta tulisi tehdä rikosilmoitus, vaikka käytännössä ainoaksi vaihtoehdoksi jäisi esitutkinnan keskeyttäminen. Sääntelyssä ei olekaan otettu huomioon tietoverkkojen erityisluonnetta.

**Toimivaltuudet poliisi- ja peiteprofiileilla**

Salaisten tiedonhankinta- ja pakkokeinojen toimivaltuussääntely on rakennettu hyvin pitkälti reaalimaailman tilanteita varten ja tämä näkyy selvästi sekä toimivaltuussäännöksissä että esitöissä. Toimivaltuuksien soveltaminen tietoverkoissa voidaankin katsoa vähintään haasteelliseksi nykytilanteessa. Viimeiseen tutkimuskysymykseen liittyen on käyty läpi kattavasti jokaista yksittäistä poliisi- ja peiteprofiilia koskevaa toimivaltuutta. Tutkimuskysymyksenä oli,

> 5) miten tulisi tulkita poliisi- ja peiteprofiileilla mahdollisten salaisten tiedonhankinta- ja pakkokeinojen ulottuvuuksia sekä eroja tietoverkoissa?

*Yleisvalvonta*

Yleisvalvontana tulisi pitää kaikkea yleisesti tietoverkkoon tai sen eri ryhmiin kohdistuvaa valvontaa. Valvontaa on mahdollista suorittaa myös siten, että hakeudutaan suljettuihin ryhmiin. Tähän vaikuttaa kuitenkin 1) ryhmän tai kaverilistan laajuus, 2) mitä tarkoitusta varten ryhmä tai profiili on luotu ja 3) millainen hyväksymisprosessi ryhmällä on. Joskin ryhmän tarkoituksella on näistä itsenäisesti vähäisin vaikutus. Jos kyseessä on laajempi ryhmä voidaan yleisvalvonnan yhteydessä olla lyhyessä vuorovaikutuksessa ryhmän ylläpitäjän tai moderaattorin kanssa sen takia, että saadaan pääsy ryhmään. Jos kyse on vain muutaman hengen suppeasta ryhmästä tai yksittäisen profiilin kaverilistalle hakeutumisesta, tulisi toimintaa pitää yleisvalvonnan sijaan mieluummin peitetoimintana. Näkyvällä poliisiprofiililla tätä problematiikkaa ei kuitenkaan ole, koska toiminta ei tapahdu salassa. Siten erilaisiin ryhmiin liittyminen tai kaverilistalle hakeutumisen voi tehdä suhteellisen vapaasti, koska kyseessä ole salainen tiedonhankinta.

*Tarkkailu*

Tarkkailu (PolL 5:13.1 ja PKL 10:12.1) kohdistuu tiettyyn henkilöön salaisessa tiedonhankintatarkoituksessa, joka erottaa sen yleisvalvonnasta. Tarkkailun tietoverkoissa voidaan katsoa alkavan silloin, kun poliisimies kohdistaa havaintoja tiettyyn profiiliin ja loppuvan siihen, kun kyseistä profiilia ei enää tarkastella. Tarkastelu voi tapahtua peiteprofiilin lisäksi poliisiprofiililla. Tilanteeseen ei vaikuta poliisiprofiilin kohdalla edes se, että kohdehenkilö saisi tiedon tarkkailusta esimerkiksi sillä perusteella, että vierailusta jää palvelun ominaisuuksien takia jälki kohdehenkilölle. Peiteprofiilin jättämä jälki taas ei yleensä herätä epäilyksiä tarkkailusta, koska toisten profiilien selailu on ominaista tietoverkoissa. Tämä sen takia, että jälki on rinnastettavissa tiedonhankinnan paljastumiseen reaalimaailmassa. Tarkkailuna voidaan pitää myös toimintaa, jossa laajaa tietoverkoista tallennettua datamassaa tarkastellaan yksittäisten profiilin osalta myöhemmin tallenteelta.[753] Tarkkailun yhteydessä ryhmiin liittyminen on mahdollista siinä missä yleisvalvonnankin kohdalla, mutta jos tarkkailun kohdehenkilö on ryhmän ylläpitäjä tai moderaattori, menee toiminta jo enemmän peitellyn tiedonhankinnan (PolL 5:15 ja PKL 10:14) puolelle.

*Suunnitelmallinen tarkkailu*

Jos tarkkailu jatkuu pidempään tai toistuu useamman kerran, voi kyseeseen tulla suunnitelmallinen tarkkailu (PolL 5:13.2 ja PKL 10:12.2). Tarkkailun ja suunnitelmallisen tarkkailun eroa voidaan arvioida 1) *tarkkailukertojen* ja 2) *tarkkailun keston* perusteella. Kertoja voi olla noin viisi erillistä kertaa ennen kuin siirrytään suunnitelmallisen tarkkailun puolelle. Yksittäiseksi tarkkailukerraksi tulee käsittää poliisimiehen yksittäisen työvuoron aikana suorittamat tiedonhankintakerrat, vaikka yksittäistä profiilia olisi klikattu useita kertoja tai vierailtu useissa kohdehenkilön eri profiileissa. Tarkkailun keston rajana voidaan pitää 24 tunnin yhtäjaksoista tarkkailua. Tämä voi täyttyä tietoverkoissa siten, että tarkkailu kestää tosiasiallisesti yli 24h. Tämä pätee fyysisten aistihavaintojen lisäksi erilaisiin apuohjelmiin, jotka voidaan asettaa seuraamaan tiettyä profiilia pitkäänkin. Lisäksi lainsäätäjän tulisi arvioida *de lege ferenda* tarvetta erottaa tietoverkoissa suunnitelmalliseksi tarkkailuksi myös 3) *tiedon keräämistavan ja laajuuden* perusteella tapahtuva toiminta, jossa kerätään yksittäisellä tarkastelukerralla laaja määrä tietoa kohdehenkilöstä myöhempää analysointia ja tarkastelua varten joko koneellisesti tai muilla keinoin.

*Peitelty tiedonhankinta*

[753] Jos taas kyseinen tieto tallennetaan laajamittaisesti yksittäisestä profiilista, voi kyseeseen tulla jo suunnitelmallinen tarkkailu (PolL 5:13.2 ja PKL 10:12.2).

Peitellyn tiedonhankinnan (Pol 5:15.1 ja PKL 10.14.1) osuus tietoverkoissa, mutta myös reaalimaailmassa on jäänyt erittäin vähäiseksi säännöksen erityisiä edellytyksiä koskevan pääsääntöisen neljän vuoden rangaistusmaksimin vuoksi. Etenkin kun raja tietoverkkoja koskevassa peitetoiminnassa on vain kaksi vuotta. Peitellyksi tiedonhankinnaksi tulisi katsoa esimerkiksi tilanteet, joissa hakeudutaan hetkeksi kohdehenkilön kaverilistalle ja kerätään tietoa hänestä lyhytaikaisessa vuorovaikutustilanteessa. *De lege ferenda* voisi arvioida, voisiko suunnitelmalliseen tarkkailun säännökseen sisällyttää peitellyn tiedonhankinnan kaltaiset yksittäiset vuorovaikutuksen sisältävät tilanteet. Erityisesti tämä koskee avoimia tietoverkkoja heikomman yksityiselämän suojan tarpeen takia.

*Peitetoiminta*

Peitetoiminnan (PolL 5:28 ja PKL 10:27) sääntelyssä lainsäätäjä on huomioinut tietoverkkojen osuuden, jonka takia sen käyttömahdollisuudet ovat tietoverkoissa laajahkot. Peitetoiminta mahdollistaa kohdehenkilön profiilin kaverilistalle ja ryhmiin hakeutumisen sekä muun soluttautumisen tietoverkoissa. Tähän tosin vaikuttaa mahdollisuudet rakentaa suojaa jo hyvissä ajoin ennen operatiivisen toiminnan aloittamista, koska sillä on suora vaikutus toiminnan uskottavuuteen. Uskottavuusongelmat koskevat osittain myös rikoksentekomahdollisuutta, jossa nykyisellä PolL 5:29.2:n ja PKL 10:28.2:n sääntelyllä ei ole merkitystä tietoverkoissa. Tulkinta perustuu siihen, että lainsäätäjä on sallinut vain reaalimaailmaa koskevat rikkeet.[754] *De lege ferenda* lainsäätäjän tulisikin arvioida ainakin tiettyjen sananvapausrikosten tekomahdollisuutta tietoverkoissa peitetoimintaa suorittavalle poliisimiehelle. Sama koskee myös tekijänoikeuksiin liittyviä asioita, identiteettivarkauksia ja lapsen seksuaaliseen hyväksikäytön torjuntaan liittyvää toimintaa.

*Valeosto*

Valeoston erityiset edellytykset ovat suhteellisen kevyet, vaikka sen yleiset edellytykset ovat tiukimmat. Peitetoiminnan tapaan myös valeostossa (PolL 5:35 ja PKL 10:34) on huomioitu tietoverkkojen osuus, joskin ehkä osittain tahattomasti. Poikkeuksellinen sääntely koskee vain päätöksentekijätasoa, koska rikosprovokaatiovaaran on katsottu olevan vähäisempi.[755] Rikosprovokaatioon on muutoinkin lainsäädännössä kiinnitetty huomiota, joka liittyy näyte-erän ostamisen problematiikka. Poliisi ei voi omalla toiminnallaan provosoida kohdetta

[754] Tämä tuskin on ollut tietoinen valinta, vaan rikesakkojen alaan perustuva toiminta koskee pääosin vain reaalimaailman toimintaa.

[755] Voidaan myös mainita, että poikkeus koskee myös reaalimaailmassa yleisön saataville toimitettuja myyntitarjouksia, joten sinänsä kyse ei ole edes poikkeuksesta reaalimaailman ja tietoverkkojen välillä.

rikokseen esimerkiksi pyrkimällä ostamaan enemmän huumausaineita kuin kohdehenkilöllä on tosiasiallisesti hallussa. Käytännössä näyte-erään liittyvässä problematiikassa kyseessä on enemmän poliisitaktinen ja peiteprofiilin uskottavuuteen liittyvä seikka, koska suurien määrien ostotarjoukset entuudestaan tuntemattomien toimesta vaikuttavat jo lähtökohtaisesti epäluotettavilta. Tietyissä tapauksissa tulisi kuitenkin olla selvemmin oikeus muunkin kuin näyte-erän ostoon. Tällainen voi olla esimerkiksi suurehkon räjähde- tai asemäärän ostaminen.[756] Valeoston kohdalla mielenkiintoinen poikkeavuus on se, että vaikka itse valeoston sopiminen tapahtuu tietoverkoissa, voidaan varsinainen vaihto suorittaa reaalimaailmassa. Tältä osin tulee tosin huomioida muiden toimivaltuuksien vaikutus toimintaan, koska vain valeoston toteuttamiseksi välttämätön toiminta on sallittua.

*Tietolähdetoiminta*

Tietolähdetoiminnassa (PolL 5:40 ja PKL 10:39) poliisimies ottaa vastaan muuten kuin satunnaisesti luottamuksellista tietoa tietolähteeltä. Tietolähteen määritelmä on ongelmallinen, koska sen osalta ei ole rajattu pois kuin esitutkintaviranomaiset.[757] Käytännössä tilanne onkin epäselvä erilaiset sidosryhmien kanssa, jotka eivät ole viranomaisia. Tietoverkoissa tietolähdetoiminta voi perustua siihen, että joko poliisi- tai peiteprofiili saa toistuvasti tietoa tietyltä toiselta profiililta. Ongelmallisia ovat erityisesti ne tilanteet, joissa tietoa toimittavan profiilin henkilöllisyyttä ei tiedetä ja hänen motiivejaan toimia tietolähteenä ei voida arvioida. Näissä tapauksissa tietoa tulisi kuitenkin pystyä ottamaan vastaan, vaikka samaan aikaan pyrkimyksenä tulisi olla tietolähteen rekisteröinti todellisilla tiedoilla.

Ohjattu tietolähdetoiminta on erittäin vähän käytetty toimivaltuus, eikä sääntely olekaan sen kohdalla tällä hetkellä toimiva. Tietoverkoissa ongelmalliseksi voivat muodostua tilanteet, joissa poliisimies ohjaa tietolähdettä siten, että kyse on *de facto* poliisin toimivaltuuteen rinnastettavasta toiminnasta. Tähän vaikuttaa oleellisesti se onko tietolähde jo seurannut tiettyä henkilöä suunnitelmallisen tarkkailun kaltaisella tavalla tai ollut hänen kaverilistallaan peitetoimintaan rinnastettavin tavoin. Tällöin kyse on sallitusta toiminnasta, jos suunnitemallisesti tapahtuvaa tarkkailua, kaverilistalle tai erilaisiin ryhmiin hakeutumista ei suoriteta poliisin neuvoin ja ohjauksessa. Sama koskee myös kuvakaappausten ottamista.

---

[756] Etenkin jos toiminta liittyy terrorismiin tai että on oletettavaa, että räjähteillä tai aseilla tultaisiin suorittamaan laajaa vahinkoa ihmisille tai omaisuudelle aiheuttava teko.
[757] Ja tutkimuksen jälkeen lakimuutoksen jälkeen myös viranomaiset.

**Loppusanat ja jatkotyöskentelyn tarve**

Tässä tutkimuksessa esille tuotuja salaisia tiedonhankinta- ja pakkokeinoja koskevia perus- ja ihmisoikeussuojaeroja reaalimaailman ja tietoverkkojen välillä ei ole otettu riittävällä tavalla huomioon sääntelyssä. Tällä hetkellä epäselvä tilanne vaikuttaa sekä poliisimiesten että kansalaisten oikeusturvaan heikentävästi, koska sääntely ei ole riittävän tarkkarajaista ja täsmällistä. Nykytilanteen kohdalla voidaankin lainata johdannossa mainittua AOA:n jo vuonna 2010 valeostoon liittyvää lausumaa. Se kiteyttää hyvin nykytilanteen, vaikka itse yhteenvedossa olikin kyse pelkästään valeostoa koskevasta sääntelystä.

> ”Totean lopuksi, että puheena oleva toimintakenttä on monin tavoin erittäin vaativaa. Sallitun ja kielletyn toiminnan rajanvetoa operationaalisella tasolla ei ole tehty yksityiskohtaisesti lainsäädännössä tai muissa normeissa. En voi pitää hyväksyttävänä sitä, että kaikkein vaikeimmat toiminnan laillisuutta koskevat rajanvedot on jätetty pitkälti suorittavan tason vastuulle. Asiantila on kestämätön paitsi yleisistä oikeusturvasyistä, myös esitutkintaviranomaisten oman oikeusturvan johdosta”.

Laajapohjaisella työryhmätyöskentelyllä saataisiin luultavasti selvennystä tietoverkkoja koskevan sääntelyn nykytilaan, jolloin tulkinnat olisivat ainakin valtakunnallisesti yhdenmukaiset. Tutkimuksessa esille tuodut seikat kuitenkin puoltavat sitä, että aiheen tiimoilta tulisi aloittaa lainvalmisteluhanke, jossa tietoverkkojen roolia tarkasteltaisiin kokonaisvaltaisesti salaisten tiedonhankinta- ja pakkokeinojen sääntelyyn liittyen.