Yksityisetsivätoiminta 2020 luvulla ja henkilötietojen käsittelyyn liittyvät lainsäädännölliset velvoitteet Suomessa

Jari Ala-Varvi

2022 Laurea

Laurea-ammattikorkeakoulu

Yksityisetsivätoiminta 2020 luvulla ja henkilötietojen käsittelyyn liittyvät lainsäädännölliset velvoitteet Suomessa

Jari Ala-Varvi

Turvallisuusjohtamisen koulutus

Opinnäytetyö

Huhtikuu 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusjohtamisen koulutus

Liiketalouden ylempi ammattikorkeakoulututkinto (YAMK)

Jari Ala-Varvi

Yksityisetsivätoiminta 2020 luvulla ja henkilötietojen käsittelyyn liittyvät lainsäädännölliset velvoitteet Suomessa

Vuosi 2022 Sivumäärä 205

Työn tarkoituksena on tuottaa tietoa siitä, miten viime vuosina muuttunut henkilötietojen käsittelyyn liittyvät lainsäädäntömuutokset ovat vaikuttaneet yksityisetsivien toimintaan. Päätavoitteena on tunnistaa toimijoihin kohdistuvat velvoitteet ja tuottaa ohjeita velvoitteisiin varautumiseksi. Velvoitteiden tunnistamiseksi tulee arvioida myös yksityisetsivätoimintaa tänä päivänä. Henkilötietojen käsittelyyn liittyvien velvoitteiden tunnistaminen edellyttää tutustumista siihen, miten henkilötietietoja yksityisetsivätoiminnassa tänä päivänä käsitellään.

Työn tilaajana on Suomen Yksityisetsivä- ja Lakitoimistoliitto ry, joka hakee ensisijaisesti hyötyä työn tuloksista omalle jäsenistölleen heidän toimintansa kehittämisessä. Työn tuloksia voivat hyödyntää kaikki toimintaa harjoittavat. Samoin niitä voi hyödyntää myös tahot, jotka käyttävät yksityisetsivien palveluita tai ovat aikeissa käyttää sellaisia.

Työtapana on tapaustutkimus. Taustana oli sekä kansallinen, että EU-lainsäädäntö, mutta myös tuomioistuinten ja valvontaviranomaisten ratkaisukäytäntö. Ensin kuvattiin kehittämisen kohteena olevaa toimintaa kirjallisuuden ja käytännön toiminnasta hankitun tiedon perusteella. Sen pohjalta muodostettiin toiminnalle tyypilliset tapaukset. Tyypillisten tapausten pohjalta määriteltiin niihin sovellettava lainsäädäntökehikko. Teoreettisen ja käytännöllisen lainopin menetelmin tunnistettiin lainsäädäntökehikosta tapauksiin sovellettavat velvoitteet. Lopuksi laadittiin prosessiohjeet, joita noudattamalla velvoitteisiin voi varautua.

Tuloksena on kuvaus, mitä ja millaista yksityisetsivätoiminta on tänä päivänä. Keskeinen havainto on, että kaikessa yksityisetsivätoiminnassa käsitellään henkilötietoja ja käsittelyllä on lähes aina oikeusvaikutuksia niihin ihmisiin, joiden tietoja käsitellään. Oikeusvaikutukset eivät ole aina positiivisia, vaan työssä nostetaan esiin myös eettisiä ongelmia. Työn päätavoitteena olleet kehittämismallit jaettiin yleisesti yksityisetsiviin kohdistuviin velvoitteisiin ja täsmällisemmin valittuihin tapauksiin sovellettaviin prosessimalleihin. Ottamalla nämä mallit esimerkiksi toimintakäsikirjaan prosessiohjeiksi, voivat sekä yksityisetsivät, että mahdolliset palveluiden ostajat varautua henkilötietojen käsittelyyn liittyviin lainsäädäntövaatimuksiin.

Asiasanat: vartioimisliiketoiminta, yksityisetsivät, henkilötietojen käsittely, tietosuoja

Laurea University of Applied Sciences **Abstract**

Degree Programme in Security Management

Master of Business Administration

Jari Ala-Varvi

Private Investigation in the 2020s and Legal Obligations Related to Processing of Personal Data in Finland

Year 2022 Pages 205

The purpose of the work is to provide information on how the changes related to the processing of personal data have affected the activities of private investigators. The main objective is to identify the obligations imposed on private nvestigators and to provide guidance on how to prepare for them. To identify the obligations, private investigator activities must also be assessed. The identification of obligations requires describing how the personal data are processed in private investigator activities today.

The work was commissioned by the Finnish Association of Private Investigators and Law Offices, which primarily seeks to benefit its members with the results of this work and thus help them to develop their activities. The results of this work can also be used by other private investigators, not just the members. Similarly, the results can also be used by those who use or intend to use the services of private investigators.

The working method is a case study. The legal framework consists of both national and EU legislation and the decisions of courts and supervisory authorities. First, this work describes the activities of private investigators based on literature and information obtained from practical activities. On this basis, the typical cases were established. Based on the typical cases, the legal framework applicable to them was defined. With theoretical and practical legal doctrine, the obligations applicable to cases were identified. Based on this analysis, the process guidelines were drawn up to help to prepare for the obligations.

The result is a description of the private investigator activities today. A key finding is that all private investigator activities include the processing of personal data and that the processing almost always has legal effects on the people whose data are processed. The legal effects are not always positive, and therefore ethical problems are also discussed in this work. The process guidelines, which were the main objective of the work, were generally divided into obligations on private investigators and process models applicable to the selected cases idnetified in this work. By including these models, for example, in an operations manual as process instructions, both private investigators and potential clients can prepare for legal requirements related to the processing of personal data.

Keywords: security services, private investigator, processing of personal data, data protection

Sisällys

1 Johdanto

Suomessa yksityisetsivätoimintaa ei enää nimenomaisesti säädellä. Rikoksen paljastamista alihankintana tai palveluna määrittelee laki yksityisistä turvallisuuspalveluista (1085/2015) ja se on luvanvaraista toimintaa. Yksityisetsivätoiminta on paljon laajempi käsite, kuin lain tarkoittama rikoksen paljastaminen. Siksi suuri osa toiminnasta on sääntelemätöntä. Yksityisetsivätoiminta on myös tänä päivänä yhä enemmän sähköisessä maailmassa tapahtuvaa näytönhankintaa johtuen viime vuosina tapahtuneen yritysten ja julkisten organisaatioiden toiminnan voimakkaasta digitalisoitumisesta.

Digitalisoituminen mahdollistaa paljon tehokkaamman tutkinnan, koska sähköisiin ympäristöihin jää jälkiä hyvin paljon. Käytännössä ihmisten toimista kyberavaruudessa voidaan jäljittää järjestelmien ja laitteiden käyttöön liittyviä jälkiä, tiedostojen käsittelystä ja viestinnästä jääviä jälkiä ja usein jopa paikkatietoja siitä, mistä käsin ja milloin on toimittu. Melkein jokaisella on jonkinlainen älylaite ja jopa useita tilejä sosiaalisen median ympäristöissä. Tallennumme monissa paikoissa kameroihin ja sovellusten käytöstä jää jatkuvasti jälkiä verkkoon, eri laitteille ja sovelluksiin. Verkkoon jää myös henkilötietojamme ja viestintäsovellusten lisääntymisen myötä myös viestintään liittyvää tietoa.

Digitalisoitumisen lisäksi myös lainsäädäntö on kehittynyt paljon. Suurin muutos on 2018 alkanut tietosuoja-asetuksen 679/2016 soveltaminen. Sitä sovelletaan kaikkeen henkilötietojen käsittelyyn. Henkilötietolain kumoaminen ja vuoden 2019 alussa voimaan tullut uusi tietosuojalaki (1050/2018) ovat tuoneet myös muutoksia. Tällä hetkellä EU:ssa on valmistelussa sähköisen viestinnän tietosuoja-asetus, joka tuo muutospaineita myös lakiin sähköisen viestinnän palveluista (917/2014), jolla sähköisen viestinnän tietosuojadirektiivi (2002/58/EY) on Suomessa lokalisoitu ja joka tullee muuttamaan sähköisen viestinnän käsittelyä (Euroopan neuvosto 2021, Council mandate).

Yksityisetsivät ovat havainneet myös kasvavan kiinnostuksen väärinkäytösten tutkintaan liittyviin toimeksiantoihin yrityksissä. 2019 tuli voimaan direktiivi unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta. Direktiivin tavoitteena on varmistaa korkea suojelu ja yhtenäiset säännöt Euroopassa niille, jotka ilmoittavat oikeuden rikkomisesta (Ilmiantajien suojeludirektiivi 1937/2019, 1. artikla). Direktiivin perusteella Suomessa valmisteilla oleva laki velvoittaisi kaikkia yli 50 henkilöä työllistäviä organisaatioita perustamaan ilmiantokanavan (HE luonnos 2021a, 140). Se tarkoittaa sitä, että Suomessa todella monet yritykset joutuvat lähiaikoina sen ongelman eteen, että lain rikkomista koskevat ilmoitukset on myös tutkittava ja siinä käytetään usein yksityisiä toimijoita apuna (Gottschalk 2017, 229).

Muuttunut lainsäädäntö asettaa lukuisia velvoitteita niin yksityisetsivätoimintaa harjoittaville kuin heidän toimeksiantajilleen. Toimeksiantajat ovat tilaajina usein työnantajia ja siten yhteisötilaajia viestintäpalveluiden osalta. Sitä kautta velvoitteita asettaa myös viestintäpalvelulaki (917/2014), työelämän tietosuojalaki (759/2004), laki yhteistoiminnasta yrityksissä (334/2007) ja tietenkin työsopimuslaki (55/2001). Sen lisäksi toimeksiantosopimukset kuuluvat suurelta osin sopimusvapauden piiriin. Sopimuksilla on kuitenkin merkittäviä vaikutuksia osapuolten vastuisiin ja velvoitteisiin muun muassa juuri muuttuneen henkilötietojen käsittelyyn liittyvän lainsäädännön vuoksi.

Laki yksityisistä turvallisuuspalveluista ei suoraan määrittele mitään henkilötietojen käsittelystä rikoksen paljastamiseen johtavassa tutkinnassa. Tämä tarkoittaa sitä, että henkilötietojen käsittelyyn liittyen toimeksiantajan ja yksityisetsivätoimintaa harjoittavan on haettava oikeudet ja velvoitteet lukuisista eri laeista. Tietosuojavaltuutettu, Traficom, turvallisuusalan valvontayksikkö tai yksityisen turvallisuusalan lainsäädännöstä vastaava ministeriö eivät ole julkaisseet tarkentavia soveltamisohjeita toimialalle. Tämä on johtanut nyt tilanteeseen, jossa yksityisetsivät joutuvat keräämään toimintaa ohjaavan sääntelyn lukuisista eri laeista oman kykynsä mukaan. Etsiviltä saadun palautteen ja kyselyiden perusteella yksityisyydensuojaan liittyvät velvoitteet ovat tällä hetkellä hyvin sekavia. Tämä vaarantaa sekä tutkinnan kohteiden yksityisyydensuojan, mutta voi olla vahingollinen lain rikkomisesta aiheutuvien seurausten kautta toimijoille tai heidän toimeksiantajilleen.

Nykyinen lainsäädännön kehitys on tehnyt yksityisetsivän ammatista yhä vaikeampaa, ellei jopa mahdotonta (SYL ry jäsenen asiantuntijahaastattelu 2021). Elinkeino on ollut suomalaisessa lainsäädännössä vuodesta 1919 vuoteen 2002, mutta turvallisuusalan lainsäädännön uudistamisen yhteydessä lainsäätäjä on keskittynyt vain vartiointiin. Yksityisetsiviä koskeva sääntely on käytännössä hävinnyt laista kokonaan. (Savolainen 2021, Yksityisetsivät ovat korvaamaton apu monelle, 58-59). Nyt tietosuojalainsäädännön muututtua, on epäselvää, miten esimerkiksi henkilötietoja saa käsitellä. Yksityisetsivän ammatissa on pitänyt käsitellä myös rikoksiin ja rikosepäilyihin liittyviä tietoja, mutta 2016 julkaistu yleinen tietosuoja-asetus näyttää käytännössä kieltävän näiden tietojen käsittelyn. Yksityisetsivätoimintaan viitataan vain joiltain osin enää lainsäädännössä. Siksi on hyvin epäselvää, millainen toiminta on laillista missäkin olosuhteissa. Tietosuojalainsäädännön muutosten vuoksi on myös epäselvää, missä kulkee tilaajan ja toimeksisaajan vastuiden rajat tutkintaa suoritettaessa ja luonnollisten henkilöiden oikeuksien ja vapauksien suojelussa.

Tässä tutkimuksessa haetaan vastauksia juuri noihin kysymyksiin: millainen on yksityisetsivä tänään, mitä he tekevät ja mitä henkilötietojen käsittelyssä on huomioitava. Ja onko meillä ehkä tarvetta tarkemmalle sääntelylle vai pärjätäänkö nykyisellä?

2 Työn toteutustapa

Tässä luvussa esitellään työn tavoite ja rajaukset. Erityisesti rajaukset ovat hyvin tärkeässä asemassa, koska työ keskittyy hyvin kapea-alaiseen ammattitoimintaan, josta Suomessa ei ole saatavilla selvästi tilastoitua tietoa. Työ ei käsittele kaikkea ammattiin liittyvää toimintaa, oikeuksia tai lainsäädännöllisiä ulottuvuuksia. Vain niitä jotka liittyvät tietosuojalainsäädännön asettamiin velvoitteisiin yksityisetsivätoimintaa suorittaville tahoille henkilötietojen käsittelyssä. Alaluvuissa asiasta tarkemmin.

2.1 Tavoite

Tämä työ lähti liikkeelle keskusteluista Suomen Yksityisetsivä- ja Lakitoimistoliitto ry:n yksityisetsivien kanssa. Liitto on Suomen vanhin yksityisetsivien yhteenliittymä ja toimii työn tilaajana. Alan toimijoilla ja jäsenillä on suuri halu saada ohjeita ja varmuutta omaan toimintaansa, koska kaikissa toimeksiannoissa käsitellään henkilötietoja ja lainsäädäntö on sen osalta merkittävästi muuttunut. Suomen Yksityisetsivä ja Lakitoimistoliitto ry viettää myös 50-vuotisen toimintansa juhlavuotta vuonna 2022. Sen vuoksi tilaajan toiveena oli tuottaa yleisesti saataville tietoa suomen kielellä yksityisetsivien työstä ja suomalaisista toimijoista. Toiveena oli myös vertailla suomalaista toimintaa kansainväliseen toimintaan sen selvittämiseksi, onko meillä jotain selvää poikkeavuutta tai erityispiirrettä.

Työn ensisijaisena tavoitteena on arvioida mitä toimintaa harjoittavien tulee vähintään huomioida lainsäädännön näkökulmasta henkilötietojen käsittelyssä. Tavoitteen saavuttamiseksi on tarkoitus tuottaa malli tai malleja, joilla yksityisetsivätoimintaa harjoittava voi tarkistaa omaan toimintaan kohdistuvat velvoitteet ja suunnitella omaa toimintaa. Arviointi tulee siksi keskittymään toimijoihin kohdistuviin velvoitteisiin, joiden tunnistaminen on toiminnan lainmukaisuuden varmistamiseksi tärkeää. Toissijaisena tavoitteena on tuottaa tietoa siitä, mitä yksityisetsivien toiminta on tänä päivänä. Paitsi, että se on työn tilaajan toive, tietoa tarvitaan myös siihen, että voidaan arvioida sitä, miten henkilötietojen käsittelyyn liittyvät lainsäädäntömuutokset vaikuttavat toimintaan. Tämän tueksi työssä tulee kyetä tuomaan esiin reunaehdot siitä, mitä henkilötietojen käsittelyssä on huomioitava, että ammatinharjoittaminen on mahdollista ja henkilötietojen käsittely laillista. Työssä siis keskitytään ensisijaisesti henkilötietojen käsittelyn lainmukaisuuteen yksityisetsivätoiminnassa ja sen perusteluihin ja reunaehtoihin.

Tavoitteiden saavuttamista varten on kuvattava toimintaa harjoittavia toimijoita ja heidän oikeuksiaan ja velvollisuuksiaan. Sen lisäksi työssä on kyettävä rakentamaan kuva siitä, mitä on tämän päivän yksityisetsivätoiminta. Vasta sen perusteella tiedetään, mitä yksityisetsivät tekevät tänä päivänä. Ilman sitä ei voida arvioida, miten he käsittelevät henkilötietoja. Tätä varten kerätään ammatinharjoittajien toiminnasta aineistoa, josta määrällisin perustein pyritään tunnistamaan pari yleisintä tapaustyyppiä, joissa arvioidaan henkilötietojen

käsittelyyn liittyviä reunaehtoja. Esiintymislukumääriin nojaavan valinnan jälkeen voidaan valintakriteerejä tarkentaa laadullisilla elementeillä vaihtelevuuden tai monipuolisuuden lisäämiseksi. Koska työllä pyritään tuottamaan tietoa alan toimijoille sen osalta, mitä omassa toiminnassa on huomioitava, ei esimerkiksi kahden identtisen tilanteen käsittely tuottaisi haluttua lisäarvoa.

Luonnollisesti on kuvattava myös henkilötietojen käsittelyn taustalla vaikuttavaa lainsäädäntökehikkoa ja sen asettamia velvoitteita tai suomia oikeuksia. Samoin tutkinnan kohteena olevia tahoja ja heihin liittyvät oikeudet ja vapaudet ovat olennaisia. Näin voidaan huomioida luonnollisten henkilöiden yksityisyydensuojaa, uhat oikeuksille ja vapauksille sekä eri osapuolten oikeudet ja velvollisuudet ja niiden välillä mahdollisesti olevia intressiristiriidat. Työssä ei tarkastella vain tietosuoja-asetusta, vaan pyritään ottamaan huomioon hajanainen lainsäädäntökenttä ja koota yhteen perusteluja eri velvoitteille tai oikeuksille siten, että se lisää toimijoiden itsensä ymmärrystä toiminnan taustoista.

Työn valmistelun yhteydessä kävi ilmi, että Suomesta on heikosti saatavilla sellaista aineistoa, jonka perusteella voitaisiin muodostaa yleistyksiä toiminnasta. Toimialaa valvonut viranomainen on salannut toimeksiantoihin liittyvän toimialan valvonnan osalta kerätyn aineiston siinä olleiden virheiden suuren määrän vuoksi. Tutkimustietoa tai tilastoja ei ole löytynyt ja toimijoiden itsensä ylivarovainen asenne tietojen luovuttamiseen omasta toiminnasta selvisi jo alussa. Siksi jo alusta alkaen oli tiedossa, että aineistoa joudutaan keräämän itse.

Työn lisäarvona tuotetaan tietoa siitä, miten tutkintaan osallistuvien ja sen kohteena olevien henkilöiden perusoikeudet ja -vapaudet toteutuvat. Työn edistyessä voi tulla eteen myös lainsäädännöllisiä kehitystarpeita tai selkiyttämiseen liittyviä tarpeita. Näkökulma ei ole pelkästään sähköisessä ympäristössä, vaikka siellä suurin osa tietojen käsittelystä tapahtuukin tänä päivänä. Tietosuojaa koskevia yleislakeja sovelletaan kuitenkin muussakin muodossa olevan tiedon käsittelyyn, joten monet selvityksen velvoitteista soveltuvat sellaisenaan kaikkeen tiedon käsittelyyn riippumatta sen olomuodosta.

2.2 Rajaukset

Tietosuoja-asetuksen vaikutuksista vartioimisliiketoimintaan ja sitä harjoittaviin turvallisuusalan yrityksiin on jo tehty opinnäytetöitä ja tutkimuksia. Niissä ei kuitenkaan käsitellä rikoksen paljastamista tai yksityisetsivätoimintaa, jos niitä edes huomioidaan. Siksi omaisuuden vartiointi, turvasuojaustoiminta ja järjestyksenvalvontatoiminta ovat tämän tutkimuksen ulkopuolella. Tässä keskitytään vain yksityisetsivätoimintaan ja lain yksityisistä turvallisuuspalveluista tarkoittamaan rikoksen paljastamiseen, jonka lasken kuuluvan myöhempien perustelujen kautta yksityisetsivätoiminnan käsitteen alle. Ulkopuolelle jätetään kokonaan myös itsenäisesti suoritettu omaan toimintaan kohdistuva tutkinta,

tilintarkastustoiminta ja asianajotoiminta. Työssä käsitellään vain toimeksiantoja, joissa tutkintaa suorittaa turvallisuusalan elinkeinoluvan haltija tai ilman turvallisuusalan elinkeinolupaa toimiva yksityisetsivä.

Turvallisuusalan elinkeinoluvan haltijan rooli työnantajana on myös tutkimuksen ulkopuolella, sillä työnantajien vastuita ja velvoitteita on jo tutkittu ja niihin on myös viranomaisohjeistusta saatavilla, esimerkiksi 2020 uudistettu Tietosuojavaltuutetun päivittämä Työelämän tietosuojan käsikirja (Tietosuojavaltuutetun toimisto, 2020). Turvallisuusalan elinkeinoluvan haltija on työnantaja siinä, missä mikä tahansa muukin työnantaja Suomessa ja sitä koskee samalla tavalla työalainsäädännön velvoitteet.

Työn ulkopuolelle jää myös itse tutkinta ja sen menetelmät. Jokaisella turvallisuusalan yrityksellä on omat tutkintamenetelmänsä, eikä tarkoituksena ole kehittää niitä. Siksi esimerkiksi yksityisetsivien tiedonsaantioikeudet vaikkapa julkisuuslain (621/1999) perusteella on jätetty ulkopuolelle. Työn tavoitteena oli tunnistaa ensisijaisesti toimijoiden velvollisuuksia, eikä oikeuksia toimeksiantojen menetelmiä valitessa. Toimintakäsikirjaan tästä työstä voi saada apua myös menetelmiä ajatellen, mutta työn ei ole tarkoitus muodostaa suoraan toimintaan siirrettävää osaa sellaisesta.

Taustalla olevia toimeksiantoja ja tutkintatapauksia käsitellään kuvaamaan toimintaa, mutta tavoitteena ei ole luoda kattavaa tilastointia tai kehittää toimialan tilastointi- tai analyysimenetelmiä. Työssä ei myöskään oteta kantaa siihen, mikä yksityisen tai viranomaisen välinen rajanveto tulisi olla, vaan perehdytään nykytilanteen kautta tämänhetkiseen tilanteeseen. Viranomaisvalvontaan ja sen laajuuteen ja mahdolliseen sääntelytarpeeseen otetaan kantaa, jos sellaisia asioita nousee esiin. Monet yksityisetsivät ja turvallisuusalan elinkeinoluvan haltijat voivat suorittaa myös muita turvallisuusalaan linkittyviä tehtäviä, mutta myös ne ovat tämän työn ulkopuolella.

Työssä käsitellään paljon lainsäädäntöä, mutta sitä käsitellään vain siinä laajuudessa kuin se yksityisetsivätoiminnassa henkilötietojen käsittelyn näkökulmasta on olennaista. Tässä työssä ei käsitellä itse tutkinnan kohteena olevia tapauksia tai oteta kantaa syyteharkintaan saattamiseen tai tuomioprosessiin vaan käsitellään pelkästään muodostettujen tapaustyyppien kautta henkilötietojen käsittelyä niissä. Henkilötietojen käsittelyn analysoinnissa huomioidaan eri vaiheet sopimuksenteosta käsittelyn aloittamiseen ja toimeksiannon suorittamisen aikaiseen toimintaan. Keskittyminen on kuitenkin toimeksiannon vastaanotossa ja käsittelyn aloittamisessa ja velvoitteissa siihen vaiheeseen liittyen. Siten esimerkiksi tekojen rangaistavuuden tapauskohtaiseen kynnyksen ylittymiseen ei oteta kantaa. Ei myöskään siihen, millainen rangaistus yksittäisestä laiminlyönnistä voisi seurata.

Myös poliisi suorittaa rikosten paljastamista ja tutkintaa. Poliisilla tarkoitetaan tässä työssä virkamiestä, joka on virkasuhteessa valtioon ja harjoittaa poliisin ammattia (Tikkanen et al.

2017, s53). Poliisin suorittama rikostutkinta ei kuitenkaan kuulu tähän työhän, koska tarkoitus on tutkia nimenomaan yksityissektorilla tapahtuvaa rikostutkintaa. Esitutkintavaihe on muutenkin tämän työn ulkopuolella jo edellä kuvatun perusteella.

Kattavaa poissulkumenetelmää sen arvioimiseksi, mitä velvoitteita toimijoihin sovelletaan tai ei sovelleta, on työn resurssien puitteissa mahdotonta suorittaa. Yleisesti tietosuoja-asetuksen viisi ensimmäistä lukua soveltuvat toimijoihin ja sen jälkeen tulevat luvut, joita sovelletaan valvontaviranomaisiin, rekisteröityjen oikeussuojakeinoihin, seuraamusmenettelyihin ja niin edelleen. Viisi ensimmäistä lukua pitää sisällään 50 ensimmäistä artiklaa, joissa on useita velvoitteita yhdessä artiklassa. Sen lisäksi näitä artikloja tarkentaa yli sata resitaalia, asetuksen perusteluihin liittyvää lausumaa. (Tietosuoja-asetus 679/2016). Kun tähän lisätään muiden lakien pykälät ja niiden sisältämien velvoitteiden määrä, olisi työssä käsiteltävä satoja yksittäisiä velvoitteita pelkästään sen tunnistamiseksi, mitä valittuihin tapauksiin sovelletaan ja mitä ei. Sen vuoksi työ pyrkii antamaan yleiskuvan useimmista velvoitteista ja niiden vaikutuksista.

Työssä joudutaan käsittelemään sekä yksityisoikeutta, että julkisoikeutta, mutta työn tarkoitus ei ole kuitenkaan analysoida näiden välistä suhdetta muutoin kuin sellaisten mahdollisesti esiin tulevien tilanteiden osalta, joissa ne voivat olla ristiriidassa. Tässä työssä ei myöskään tarkastella tarkemmin yksityisen ja julkisen välistä kehitystä tai historiaa. Koska jokaisella maalla on oma lainsäädäntönsä, työ ei tuota sellaisenaan kansainvälisesti yleistettävää informaatiota. Poikkeuksen muodostaa sellainen lainsäädäntö, joka on EU-tasolla sovellettavaa ja josta ei ole annettu oikeuksia poiketa kansallisella lainsäädännöllä. Toimintaan, lupaprosesseihin, oikeuksiin ja valtuuksiin sovellettava lainsäädäntö voi olla niin erilaista, etteivät työn tulokset ja havainnot ole sellaisenaan soveltuvia automaattisesti toisen valtion lainsäädäntökontekstissa.

Monessa maassa Euroopan Union sisällä yksityisen turvallisuusalan lainsäädäntö poikkeaa oikeuksineen ja valvontaperiaatteineen eri maiden välillä. Toimialan ohjaus ja valvonta voi olla jopa eri ministeriöiden alla, kuten työssä myöhemmin selviää. Siksi on mahdotonta työn resurssit huomioiden tuottaa kansainvälisesti yleistettävää tietoa. Joissakin tapauksissa joudutaan käsittelemään kansainvälistä lainsäädäntöä, Euroopan tuomioistuimen tai muiden maiden oikeustapauksia, mutta niitä käsitellään vain silloin, jos vastaava esimerkki puuttuu Suomesta tai kyse on päätöksestä, joka muodostaa Suomea kansainvälisten sopimusten kautta sitovan ennakkotapauksen.

Työ ei ota huomioon myöskään eri toimialojen erityispiirteitä. Suomen sisällä on toimialakohtaista sääntelyä paljon, eikä työssä käytettävissä olevin resurssein ole mahdollisuus pureutua kaikkiin niihin. Esimerkiksi finanssialaa sitoo oma sääntelynsä terrorismirikoksista ja rahanpesusta (Laki rahanpesun ja terrorismin rahoittamisen

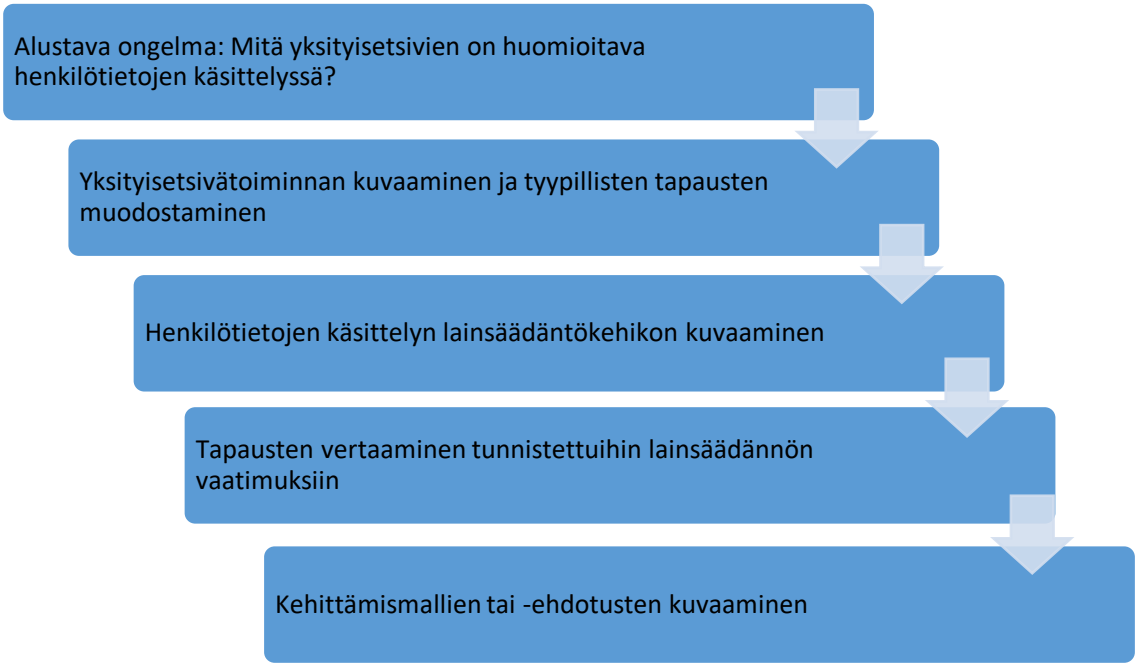
estämisestä, 444/2017) ja terveydenhuollon sähköistä tietojen käsittelyä omat lakinsa (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, 159/2017). Kuitenkin se yleinen lanisäädäntökehikko, joka tässä työssä esitellään, sitoo myös näitä toimijoita. Toimialakohtainen sääntely voi kuitenkin asettaa poikkeuksia siihen. Koska työ ei ole oikeustieteellinen, ei tässä ole tarkoitus myöskään arvioida tehtyjä tulkintoja tai tuottaa niitä lisää.

2.3 Työntapa ja työmenetelmät

Tämä työn strategiaa ja työtapaa kuvaa parhaiten tapaustutkimus. Tapaustutkimuksen kohteena voi olla yritys, tuote, palvelu tai prosessi tai mikä tahansa nykyajan ilmiö ja sen pyrkimys on tuottaa syvällistä ja yksityiskohtaista tietoa tutkimuksen kohteesta (Ojasalo et al. 2018, 52). Vaikka tapaustutkimuksessa on usein kysymys suuren tietomäärän tuottamisesta suppeasta kohteesta, voi tapaus olla muodostettu myös useammasta tapauksesta, kunhan ne ovat ymmärrettävissä kokonaisuutena eli yksittäisenä tapauksena (Ojasalo et al. 2018, 52-53). Tapaustutkimuksen periaatteiden mukaan tavoitteena on tuottaa kehittämisehdotuksia tutkittavasta tapauksesta (Ojasalo et al. 2018, 52). Tässä tutkimuksessa tutkittavina tapauksina ovat yksityisetsivätoiminnan kuvauksesta muodostetut esimerkkitapaukset. Tuotettavat kehittämisehdotukset ovat työn tavoitteissa mainittujen lainsäädäntövelvoitteiden tunnistaminen ja nimeäminen, joiden avulla henkilötietojen käsittelyn lainmukaisuus yksityisetsivätoiminnassa varmistetaan. Monimuotoisen lainsäädäntökehikon ja yksityisetsivätoiminnasta olemassa olevan suppean tutkimustiedon vuoksi tässä työssä on tärkeää perehtyä ensin huolellisesti tutkittavaan kohteeseen, kuten tapaustutkimuksen luonteeseen kuuluu (Ojasalo et al. 2018, 54).

Tapaustutkimuksen luonteeseen kuuluu myös, että kehittämiskohde tarkentuu tutkimuksen edetessä (Ojasalo et al. 2018, 54). Myös tässä työssä on tunnistettu jo tavoitteen asettamisvaiheessa, että työn tuloksena voi olla myös tilanne, jossa joudutaan toteamaan, ettei henkilötietojen käsittelylle ole kaikissa tapauksissa riittäviä perusteluja. Tai käsittelyn osalta voidaan tarvita lainsäätäjän puolesta tarkennuksia lakiin tai lakien soveltamiseen. Ilman perehtymistä kohteeseen on kuitenkaan vaikea tunnistaa, voidaanko tutkimuksen tavoitteeseen edes päästä tai mikä lopullinen tunnistettu kehittämismalli tai ongelma tulee olemaan (Ojasalo et al. 2018, 54).

Työn vaiheet tapaustutkimuksessa ovat yleensä kehittämistehtävän tai ongelman nimeäminen, ilmiöön perehtyminen, aineiston keruu ja kehittämisehdotusten tai -mallin tuottaminen (Ojasalo et al. 2018, 54). Tämän työn osalta nämä vaiheet asettuvat kuvion 1 mukaan seuraavasti:



Kuvio 1: Työn eteneminen tapaustutkimuksen etenemiskaavaa mukaillen

Metodien ja menetelmien valinnassa on otettava huomioon se, että suomalaisesta yksityisetsivätoiminnasta on hankalasti saatavilla tutkimustietoa tai kattavia tilastoja tai analyysejä. Siten työn kohteena olevasta toiminnasta saatava tieto on uutta ja siten epävarmaa ja mahdollisesti kapea-alaista. Myös lainsäädännön tulkinta on epävarmaa – vasta tiettyjen arviointien ja analyysien jälkeen voidaan esittää jonkin asian olevan lainsäädännön näkökulmasta vaatimus, mutta siltikin se on vain esitys, joka on mahdollisesti kumottavissa (Kiikeri & Ylikoski 2004, 103). Toiminnan kuvaaminen on tärkeää kahdesta syystä. Ensinnäkin siksi, että voidaan kuvata se viitekehys ja lainsäädännöllinen kehikko, joka kohdistuu alan toimijoihin. Toiseksi on vaikea tutkia henkilötietojen käsittelyyn liittyviä reunaehtoja, ellei tiedetä, mitä henkilötietoja ja millä tavalla henkilötietoja käsitellään yksityisetsivätoiminnassa. Vasta sen jälkeen voidaan systemaattisesti kuvata eri lait, niiden soveltaminen ja niiden suhde henkilötietojen käsittelyyn. Kun puretaan toimintaan liittyviä velvoitteita, on lähtökohta lainopillinen ja keskittyy kuvaamaan eri säännösten ja lakien suhdetta suoraan rikoksen paljastamiseen liittyviin esimerkkeihin.

Oikeudellisia ja lainopillisia asioita lähestytään sekä teoreettisen lainopin ja käytännöllisen lainopin kautta. Teoreettinen lainoppi on oikeudellisten käsitteiden käsiteanalyysiä ja systematisointia, joilla pyritään kuvaamaan lainsäädännölliset käsitteet (Aarnio 1997, 43, 53). Tässä työssä systematisointi ja käsitteiden avaaminen kohdistuu lainsäädäntökehyksen kuvaamiseen ja toimijoihin kohdistuvan lainsäädännön avaamiseen keskittyen etenkin tietosuojalainsäädännön muutosten mukanaan tuomiin uusiin käsitteisiin ja niiden sisältöihin: esimerkiksi termien ”rekisterinpitäjä” ja ”käsittelijä” sisällöt ja merkitys sekä soveltaminen

käytännön toiminnassa. Mitä selkeämpi käsitteistö on käytössä, sen monipuolisemmin voimme käsitellä kysymyksiä toimijoihin kohdistuvista käytännön velvoitteista (Aarnio 1997, 53).

Teoreettisen lainopin soveltaminen on taas edellytys käytännöllisen lainopin soveltamiselle. Käytännöllisessä lainopissa on yksinkertaistaen kyse tulkinta- ja lainsoveltamiskysymyksistä: mistä oikeustosiseikoista johtuu mitäkin oikeusseuraamuksia (Aarnio 1997, 53). Tässä työssä käytännölliseen lainoppiin päästään työn lopussa, jossa on tarkoitus aiemmissa luvuissa tehtyjen yksityisetsivätoiminnan tapaustyyppien ja toimijoihin kohdistuvan lainsäädäntökehyksen kautta kuvata niitä oikeusseuraamuksia, joita toimijoihin omassa toiminnassaan kohdistuu. Oikeusseuraamuksilla tarkoitetaan sitä, millaisia konkreettisia velvoitteita tai rajoituksia toimijoihin kohdistuu esimerkiksi sen vuoksi, että ovat käsittelyssä ”rekisterinpitäjän” tai ”käsittelijän” roolissa.

Aarnio kuvaa käytännöllisen lainopin menetelmän olevan argumentatiivinen (1997, 53). Se tarkoittaa sitä, että kannanotot on perusteltava siten, että ”mahdollisimman moni rationaalisesti asiaa harkitseva oikeusyhteisön jäsen voi kaikki asianhaarat huomioon ottaen hyväksyä kannanottosi” (Aarnio 1997, 51). Argumentaation osapuolina on tässä keskustelussa minä työn kirjoittajana ja tulkintojen tekijänä ja ammatillinen yhteisö ja muu yhteiskunta, joka on kiinnostunut tehdyistä tulkinnoista tai toimijat joihin tulkinnat vaikuttavat. Argumentaatio tässä työssä perustuu sekä formalistiseen kirjoitetun lain tulkintaan, viranomaisten antamiin tulkintaohjeisiin ja tuomioistuinratkaisuihin lain tulkinnassa. Kirjoitetun lain tulkinnassa lähtökohta on se, että lakia tulkitaan kirjaimellisesti, kuten se on kirjoitettu (Aarnio 1997, 50). Tuomioistuinratkaisut ja viranomaisen tulkintaohjeet tuovat mukaan myös muita oikeuslähteitä, jolloin kirjoitettua lakia täydentävät myös siitä tehdyt tulkinnat.

Työ itsessään pyrkii argumentin tuottamiseen sen osalta, mitä yksityisetsivien on ammattia harjoittaessaan huomioitava henkilötietojen käsittelyssä. Tämä argumentti ovat ne kehitysehdotukset, jotka työn tuloksena syntyvät. Tämän argumentin voi taas kumota tai vahvistaa kuka tahansa aiemmin mainituista osapuolista esittäessään uusia perusteluja asiasta. Tavoitteena ei kuitenkaan ole väittely, vaan rationaalinen hyväksyttävyys (Aarnio 1997, 51). Laintulkinnallinen lähtökohta tässä työssä on yleinen intentiotulkinta, joka Frändenmukaan (2005, 56) tarkoittaa periaatetta, että lainsäätäjä tarkoittaa aina täyttä totta ja lakia on tulkittava sen sanamuodon perusteella. Tietyt esiin tuodut asiat sisältävät myös teleologista tulkintaa, jolla tarkoitetaan huomioin kohdistamista siihen, mitä lainsäädännöllä on tarkoitus suojella (Frände 2005, 56–57, Kerttula 2010, 23). Tässä työssä teleologista tulkintaa edustaa asioiden arvioinnissa hallituksen esitysten, tuomioistuinten tai henkilötietojen käsittelyä valvovien valvontaviranomaisten esiin nostamat päätökset ja ohjaus.

Tapaustutkimukselle ominaista on, että tuloksiin päästään monenlaisia menetelmiä yhdistämällä. Tämän työn tekijällä on 15 vuoden työkokemus rikoksen paljastamiseen johtavan tutkinnan suorittamisesta yksityissektorilla sekä viranomaisille, että yksityisille toimeksiantajille. Siten oma kokemus on lähtökohtana menetelmien ja lähteiden valinnassa. Työssä käytetään aineistona julkisista lähteistä saatavilla olevia tietoja yksityisetsivätoiminnasta. Näitä tietoja on täydennetty työn tekijän ammatillisten järjestöjen ja jäsenyyksien kautta saatavilla tiedoilla. Yhdistelmänä on sekä määrällisten analyysien, että laadullisten arvioiden kautta kohteena olevien tapausten muodostaminen. Johtuen käytettävissä olevan aineiston laadusta, jouduttiin käytännössä tukeutumaan myös kvalitatiiviseen tulkintaan aineiston luokittelemiseksi. Esimerkiksi kansainvälisestä yksityisetsivätoiminnasta oli käytettävissä määrällisiä aineistoja, mutta kotimaisesta vain laadullisia kuvauksia, joiden pohjalta ei voinut tehdä määrällisten analyysien kautta yhteenvetoja.

Lainsäädäntökehikon tunnistamisessa keskitytään pelkästään siitä saatavilla olevan kirjallisen ja julkisen aineiston analyysiin. Tämä tarkoittaa lakien ja hallitusten esitysten sisältöihin, tuomioistuinten päätöksiin ja viranomaisen ohjaukseen liittyvien aineistojen ja sisältöjen analysointia sekä vertailua. Tapaustutkimukselle tyypillisesti tässäkään ei lähdetä liikkeelle lainsäädännön yleisistä teorioista ja kuvaamisesta vaan jo saatavilla olevan tiedon ohjaamana keskittymällä tapausten kannalta olennaisiin asioihin (Ojasalo et al. 2018, 54).

Yhteenvetona voidaan sanoa, että työssä esitetään esiin nostettujen tapausten kautta käsitteiden kuvaamisen, kirjoitetun lain ja oikeustapausten tulkinnan avulla toimijoihin kohdistuvia oikeudellisia velvoitteita. Näiden velvoitteiden pohjalta esitetään kahitämismallit tai -ehdotukset, joiden on tarkoitus parantaa alalla toimivien mahdollisuuksia vastata muuttuneen henkilötietojen käsittelyyn vaikuttavan lainsäädännön vaatimuksiin omalla toimialallaan.

2.4 Käsitteet ja lyhenteet

C-XXX. Unionin tuomioistuimen päätökset on yksilöity tapausnumerolla, jonka se on Unionin tuomioistuimen käsittelyssä saanut. Nämä numerot ovat yksilöllisiä.

EDPB. European Data Protection Board, Euroopan tietosuojaneuvosto, joka jatkoi tietosuojatyöryhmän (Working Party 29, lyhyemmin WP 29) työtä ja vastaa yleisen tietosuoja-asetuksen ja poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin yhdenmukaisesta soveltamisesta kaikkialla Euroopassa (EDPB 2021, Organisaatio). Tietosuojaneuvoston ohjeet eivät ole suoraan lakitekstiin verrattavia ohjeita. Koska neuvostolla on mahdollisuus antaa valvontaviranomaisia sitovia päätöksiä, ohjeet käytännössä muodostavat usein tulkinnan lainsäädännöstä. Tätä tarkastellaan työssä myöhemmin.

Tietosuojaneuvosto on suoraan hyväksynyt useita tietosuojatyöryhmän ohjeita omina ohjeinaan (EDPB 2018a) ja muita se on päivittänyt tarvittavilta osin adoptoidessaan ne itselleen (esimerkiksi Guidelines 07/2020 on the concepts of controller and processor in the GDPR, mikä korvasi vuonna 2010 WP 29:n julkaiseman vastaavan ohjeiston).

EDPS. European Data Protection Supervisor, Euroopan tietosuojavaltuutettu. Valvoo henkilötietojen käsittelyä ja tietosuojalainsäädännön noudattamista Euroopan unionin toimielinten suorittamassa henkilötietojen käsittelyssä ja muun muassa toimii Euroopan tuomioistuimen asiantuntijana tietosuojalainsäädännön tulkinnassa. (EDPS 2022).

HE. Hallituksen esitys.

Henkilötietodirektiivi. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (Henkilötietodirektiivi 95/46/EY).

Ilmiantajien suojeludirektiivi. Euroopan parlamentin ja neuvoston direktiivi (EU) 2019/1937, unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta, 23.10.2019 (Ilmiantajien suojeludirektiivi 1937/2016).

Oikeustoimilaki. Laki varallisuusoikeudellisista oikeustoimista 228/1929.

Sähköisen viestinnän tietosuoja-asetus. Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus 2017).

Sähköisen viestinnän tietosuojadirektiivi. Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi 2002/58/EY).

Tietosuoja-asetus. Euroopan parlamentin ja neuvoston asetus 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (tietosuoja-asetus 679/2016).

Työelämän tietosuojalaki. Laki yksityisyyden suojasta työelämässä 759/2004.

Viestintäpalvelulaki. Laki sähköisen viestinnän palveluista 917/2014.

WP 29. Working Party 29, Euroopan tietosuojaneuvoston edeltäjä tietosuojadirektiivin ajalta, joka käsittely henkilötietojen käsittelyyn liittyviä kysymyksiä tietosuoja-asetuksen soveltamisen alkuun asti (Tietosuojatyöryhmä WP 29 2021)

Yhteistoimintalaki. Laki yhteistoiminnasta yrityksissä 334/2007.

3 Yksityisetsivätoiminnan tausta ja viitekehys

Yksityisetsivätoimintaan on aiemmin muiden tehtävien lisäksi kuulunut myös rikoksen paljastaminen. Rikoksen paljastaminen on lainsäädännössä määritelty nyt vartioimisliiketoiminnaksi (laki yksityisistä turvallisuuspalveluista 1085/2015, 2 §, kohta 2). Yksityisetsivätoimintaan liittyy kuitenkin muutamia erityiskysymyksiä ja näkökulmia, joita on tarkasteltava, että voimme määritellä, milloin on kysymys luvanvaraisesta lain yksityisistä turvallisuuspalveluista tarkoittamasta rikosten paljastamisesta ja milloin muusta yksityisetsivätoiminnasta.

Julkinen ja julkisrahoitteinen poliisi ainoana rikosten tutkijana ei ole ollut kansainvälisestikään ainoa tapa rikosten selvittämisessä (esimerkiksi Prenzler 2006, 424). Syitä tukeutua yksityissektoriin voi olla monia ja niissä heijastuu aina eri aikakausille tyypilliset tarpeet, mutta monesti kyse on siitä, että julkinen prosessi ei tarjoa riittäviä oikeussuojakeinoja (Prenzler 2006, 424 ja 434). Myös Suomessa hiljattain julkaistu väitös toteaa poliisin rikostutkinnan tehon merkittävästi heikenneen ja tämä voi olla yksi syy hakea oikeutta muuta kautta kuin julkisesta prosessista (Savolainen 2021). Julkisen prosessin tavoite yhteiskunnassa rikokseksi säädeltävän teon sovittamisesta yhteiskunnalle ei aina ole välttämättä rikoksen uhrin tavoite. Rikoksen sovittamisessa voi painaa enemmän esimerkiksi tehokkaampi menetetyn omaisuuden tai korvauksen saanti tai pelkästään tilanteen uudelleen tapahtumisen estäminen. (Sennewald & Tsukayama 2015, 22; Gottschalk 2017, 231).

Tässä luvussa on tarkoitus määritellä tarkemmin yksityisetsivätoimintaa ja rikoksen paljastamista sekä niiden suhdetta. Luku myös tarkentaa tämän työn rajauksia sen osalta, mitä työssä tullaan käsittelemään. Luvun tarkoitus on kuitenkin käsitellä vain sitä, mitä yksityisetsivätoiminta on tänä päivänä sääntelyn näkökulmasta. Vasta seuraavassa luvussa arvioidaan sitä, mitä toiminta on käytännössä.

3.1 Yksityisetsivätoiminta ja rikoksen paljastamiseen johtava tutkinta

Yksityisen turvallisuusalan voidaan nähdä koostuvan vartioimisliiketoiminnasta, yksityisetsivätoiminnasta, turvasuojaustoiminnasta, turvallisuusalan asiantuntijapalveluista ja turvallisuusalan koulutuksesta, joiden tarkoituksena on tukea organisaatioita ja kuluttajia turvallisuuden ylläpitämisessä (Tikkanen et al. 2017, 9). Rikoksen paljastamiseen johtava tutkinta liitetään usein käsitteeseen yksityisetsivätoiminta. Näissä ei kuitenkaan ole kysymys täysin samasta asiasta. Termi ”yksityisetsivä” juontaa juurensa 11.2.1944 voimaan tulleesta asetuksesta yksityisetsivän ammatista (112/1944). Siinä määritellään yksityisetsivätoiminta seuraavasti:

”Yksityisetsivän ammatilla tarkoitetaan tässä asetuksessa sellaista jatkuvaa toimintaa ansion tai elatuksen hankkimiseksi, jossa ammatin harjoittaja asiakkaittensa toimeksiannosta poliisimiehen oikeuksitta suorittaa rikosten tutkimista ja selvittämistä.” (Asetus yksityisetsivän ammatista 112/1944, luku 1, 1 §).

Yksityisetsivätoiminnassa on siis ollut alun perinkin kyse rikosten paljastamisesta, mutta ilman viranomaisen toimivaltuuksia. Tarpeen loi etenkin vähäisemmät rikokset tai rikokset, joihin poliisi ei tutkintaresursseja ohjannut. Esimerkiksi -70 luvulla alkanut suurten hypermarkettien rakentaminen vaikutti myymälätarkkailun kasvavaan tarpeeseen. Myös ennen vuotta 1986 avioliittolaissa ollut pykälä erotilanteessa tasinko-oikeuden menetyksestä puolison pettäessä olivat tyypillisiä tutkintatapauksia. (Iltalehti 2021a). Uskottomuustapauksia on edelleen yksityisetsivätoiminnassa, mutta sinällään nykylainsäädännössä ne harvoin täyttävät enää rikoksen tunnusmerkistöä tai aiheuttaisivat oikeudellisia seurauksia tasinko-oikeuden kautta ja niiden merkitys toimeksiantoina on siten vähentynyt, kuten myöhemmin tässä työssä tarkennetaan. Muita syitä ovat viranomaisen tai julkisprosessin tehottomuus, mutta monille tärkeää on myös yksityisetsivän käytön tarjoama yksityisyys ja asian pitäminen poissa julkisesta käsittelystä (Prenzler & King 2002, 4).

Yksityisetsivätoiminta rikosten paljastamisen ja selvittämisen kontekstissa tuli vuonna 2002 lakiin yksityisistä turvallisuuspalveluista, jonka toinen pykälä liitti rikosten paljastamisen luvanvaraiseksi vartioimisliiketoiminnaksi. Vartioimisliikkeiden harjoittamaa toimintaa on Suomessa taas rajoitettu laissa elinkeinon harjoittamisen oikeudesta (122/1999), jonka kolmannen pykälän kohta 20 määrittelee vartioimisliiketoiminnasta säädeltävän erikseen. Sellaista yksityisetsivätoimintaa, jonka tarkoituksena ei ole rikoksen paljastaminen tai selvittäminen, ei ole kuitenkaan rajoitettu mitenkään kyseisessä laissa, koska sitä pidettiin silloin vähämerkityksisenä lainsäädäntönä. Siten erityissääntelylle ei nähty tarvetta. (HE 69/2001 vp, 28).

Yksityisetsivätoiminnan osalta taustalla oli tavoitteena täsmentää tämän elinkeinotoiminnan määritelmää ja taata tehokkaampi viranomaisvalvonta (HE 69/2001 vp, 29 ja 30). Rikoksen paljastaminen määriteltiin hallituksen esityksessä ”…muiden kuin viranomaisten suorittamasta rikosten ilmisaattamisesta ja sellaisista siihen liittyvistä rikosten alustavista selvittämistoimenpiteistä, joiden avulla hankitaan riittävät tiedot viranomaisille tehtävää rikosilmoitusta varten. Rikosten paljastamiseen liittyvään toimintaan katsottaisiin myös sisältyvän jo paljastuneen rikoksen vuoksi mahdollisesti suoritettavat lisäselvitystoimenpiteet.” (HE 69/2001 vp, 30).

Vuonna 2008 sisäasianministeriö käynnisti yksityisen turvallisuusalan lainsäädännön uudistamishankkeen. Sen oli tarkoitus yhtenäistää lainsäädäntöä, tehostaa alan valvontaa ja kehittää koulutusta. Yksityisetsivätoiminnasta tai sen paremmin rikoksen paljastamiseen

johtavasta tutkinnasta ei puhuttu hankkeen alkuvaiheessa mitään. (Edilex uutinen 2008 ja 2009). Myöhempi hallituksen esitys 239/2009 ei sekään ottanut kantaa rikosten paljastamiseen johtavaan tutkintaan muutoksen valmistelussa. Rikosten paljastaminen mainittiin vain yhtenä asiana luettelossa, jossa lueteltiin ne tehtävät, joista toimeksiantosopimus tulisi tehdä (HE 239/2009 vp, 7). Sisäministeri itsekään ei maininnut lakiuudistuksen yhteydessä missään vaiheessa rikosten paljastamiseen johtavaa tutkintaa (esimerkiksi Räsänen 2012 ja 2013).

Myöhemmin hallituksen esitys 22/2014 tarkensi rikoksen paljastamista siten, että esimerkiksi tilintarkastusyhteisöjen suorittamia tilintarkastuksia tai erikoistarkastuksia ei pidettäisi lain yksityisistä turvallisuuspalveluista tarkoittamana vartioimisliiketoimintana. Samoin asianajotoimintaan liittyvä rikoksen paljastaminen on rajattu lain tarkoittaman luvanvaraisen vartioimisliiketoiminnan ulkopuolelle. Perusteluna nähtiin tällaisen toiminnan määritteleminen vartioimistehtäväksi epätarkoituksenmukaiseksi. Mutta myös siksi, että kyseistä toimintaa harjoittavat ovat jo omaa toimialaansa koskevan valvonnan piirissä. (HE 22/2014, 26). Viranomaisvalvonnan tarkoituksena on taata kansalaisten suojelu julkista valtaa käytettäessä (esimerkiksi Hautamäki 2016, 23; HE 69/2001 vp, 29 ja 30) mukaan lukien yksityisetsivätoiminta (Kerttula 2010, 127)

Seuravan kerran lakia yksityisistä turvallisuuspalveluista käsiteltiin hallituksen esityksessä 42/2016, mutta vartioimisliiketoimintaa koskien kyseessä oli tekninen sanamuodon muutos, jossa pykälää 4 muutettiin vartijan toimialueen osalta (Vartijan tehtävät ja toimialue):

”Erillisen omaisuuden vartiointia, henkilön koskemattomuuden suojaamista, rikoksen paljastamista koskevaa sekä vartioimisalueella suoritettavaa tehtävää tukevaa tai siihen muutoin liittyvää vartioimistehtävää vartija voi suorittaa myös muualla kuin vartioimisalueella.” (HE 42/2016 vp, 27)

Muutos toki selkiytti etenkin rikoksen paljastamista. Kuten myöhemmin tässä työssä tullaan toteamaan, rikoksen paljastamisessa on usein kysymys tehtävistä muualla kuin suoraan toimeksiantajan määrittelemässä vartioimiskohteessa. Myös hallituksen täysistunnossa käsiteltiin tätä muutosta. Mutta hallituksen esitystä 42/2016 käsiteltäessä ei rikosten paljastamiseen puututtu, vaan keskustelussa päähuomion tuntui saavan poliisin resurssit tai poliisin määrän väheneminen, joita käsiteltiin 27 puheenvuorossa 51:stä (PTK 36/2016/4 2016).

Myös omavartiointi on luettu luvanvaraisen vartioimisliiketoiminnan ulkopuolelle jo vuodesta 2001. Omavartioinnissa on kyse siitä, että toimija tuottaa itse lain yksityisistä turvallisuuspalveluista tarvittavat palvelut (HE 69/2001 vp, 41). Omavartiointi tapahtuu jokamiehenoikeuksin (HE 69/2001 vp, 8) ja se perustuu perustuslain omaisuuden suojaan (perustuslaki 731/1999, 2 luku, 15 § ja Paasonen & Ellonen 2018, 20). Niin ikään säädökset

eivät koske naapuriapua, kuntaa, valtiota, julkisia laitoksia tai muuta tilapäisluontoista ja vähäistä vartioimistehtävää (HE 69/2001 vp, 12 ja Paasonen & Ellonen 2018, 20–21).

Vartioimisliiketoiminnan ulkopuolelle rajattujen tilintarkastustoimintaa ja asianajotoimintaa harjoittavien toimijoiden lisäksi on myös muita tänä päivänä rikosten tutkintaan liitettäviä toimijoita. Hämmennystä voivat herättää muun muassa IT-yhtiöt, jotka tuottavat esimerkiksi laissa rangaistavaksi säädettyjen tietomurtojen paljastamista, eivät ole minkään viranomaisen erityisessä valvonnassa, eikä niitä koske tavanomaisesta yritystoiminnasta tiukempi tai järjestelmällisempi valvonta. Tätä käsitellään myöhemmin tarkemmin. Turvallisuusalan valvontayksikön näkemys oli kuitenkin vuonna 2010 esimerkiksi Opsec Oy:tä koskien se, että rikosten paljastaminen vaatii turvallisuusalan elinkeinoluvan riippumatta siitä, tehdäänkö sitä IT-ympäristöissä vai tavanomaisin menetelmin. Opsec Oy:llä onkin ollut turvallisuusalaan valvontayksikön myöntämä turvallisuusalan elinkeinolupa jo vuodesta 2010 ja toimintakäsikirja on turvallisuusalan valvontayksikön hyväksymä ja toiminnan tarkastaa vuosittain poliisi. (Vastaavan hoitajan haastattelu 2021).

Tällä hetkellä rikosten paljastaminen ansiotarkoituksessa on vartioimistehtävänä nyt voimassa olevassa laissa yksityisistä turvallisuuspalveluista (1085/2015, 2 §, 1 kohta). Toiminta on edelleen luvanvaraista saman lain kolmannen pykälän perusteella. Saman lain toinen luku, joka käsittelee vartioimisliiketoimintaa, ei kuitenkaan ohjeista juuri mitään rikosten paljastamiseen liittyvästä tutkinnasta. Kyseisen lain toisen pykälän perusteella voidaan sanoa, että rikoksen paljastamisesta on kyse silloin kun:

1. Siitä saadaan korvaus (laki yksityisistä turvallisuuspalveluista 1 luku, 2 §, kohta 1)
2. Se perustuu toimeksiantosopimukseen (laki yksityisistä turvallisuuspalveluista 1 luku, 2 §, kohta 1)
3. Toiminnan tarkoituksena on paljastaa rikos tai paljastuneen rikoksen lisäselvitystoimet (laki yksityisistä turvallisuuspalveluista 1 luku, 2 §, kohta 2; HE 69/2001, 30)

Ansaintatarkoitus täyttyy, vaikka vain osa ostetuista tehtävistä olisi turvallisuustoimenpiteitä. Vähäinenkin työajan käyttö omaisuuden vartiointiin, henkilön koskemattomuuden suojaamiseen tai rikosten paljastamiseen tai näiden tehtävien valvomiseen, vaikuttaa siihen, että tehtäväkokonaisuutta on pidettävä vartioimistehtävänä. (Helsingin käräjäoikeus 2005, 5). Toimeksiantosopimus ei myöskään viittaa tehtyyn sopimukseen tai sen muotoiluun vaan analyysiin siitä, mitä tehtäviä teollisuudessa alihankintana tai toimittajana tuotetaan (Helsingin käräjäoikeus 2005, 3).

Rikoksen paljastamisen ja selvittämisen osalta itse rikoksen käsite on myös merkityksellinen. Rikos terminä liittyy myös moraalifilosofiaan ja etiikkaan siten, että teot voivat olla moraalisesti oikein tai väärin (Melander 2010, 10). Esimerkiksi valkokaulusrikollisuuden

yhteydessä voidaan puhua moraalisista periaatteista ja yhteisöjen vastuun kantamisesta näitä moraalisia periaatteita rikottaessa tai muutoin kansalaismielipiteessä tuomittavina pidettyjä tekoja (Laitinen & Aromaa 2005, 21). Rikosten paljastamiseen tai niiden poliisitutkintaan saattamiseen ei kuitenkaan kuulu kriminaalipoliittinen tai yhteiskunnallinen keskustelu siitä, mikä on rikos ja mikä ei. Siksi tässä yhteydessä rikosta lähestytään sen legaalin tulkinnan mukaan – rikos on teko, josta on laissa säädetty rangaistus (Laitinen & Aromaa 2005, 14).

Yhtiöiden vastuullisuussäännökset ovat kehittyneet viime vuosien aikana voimakkaasti. Jo vuosia sitten alkanut ympäristövastuullisuus on johtanut siihen, että yhtiöissä voi olla tiukempia vaatimuksia energiankulutukselle tai raaka-aineille kuin mitä laki edellyttää. Yhtiön sisäisen politiikan vastainen toiminta ei välttämättä täytä silti rikoslain ympäristörikoksen tunnusmerkistöä. Myös erilaiset metoo- ja punkstoo -ilmiöt ovat nostaneet esiin eettiset kysymykset eri aloilla ja niihin liittyvät toimintapolitiikat voivat olla tiukkojakin. Raja loukkaavan käytöksen tai kohtelun ja rikoksen välillä menee siinä, että toiminta täyttäisi esimerkiksi rikoslaissa olevan syrjinnän tai seksuaalisen hyväksikäytön tunnusmerkistön.

Voi siis olla, että tutkinnan lähtökohta on esimerkiksi yhtiön sisäisen tarkastuksen havaitsema yhtiön toimintaohjeiden tai eettisten ohjeiden vastainen toiminta. Tutkinta voi toki alkaa ulkoisen toimijan kanssa silloin ilman, että käytetään turvallisuusalan elinkeinoluvan haltijaa. Työn suorittajaksi kelpaa tällöin kuka tahansa esimerkiksi sisäiseen tarkastukseen, kirjanpitoon, tilintarkastukseen tai tietotekniikkaan erikoistunut yhtiö tai henkilö. Erityistä huomiota tulee kuitenkin kiinnittää siihen, jos selvityksen yhteydessä paljastuu, että toimeksianto muuttuukin rikoksen paljastamiseksi. Sama tilanne voi tapahtua myös aiemmin mainittujen tietoteknisten valvontajärjestelmien kanssa. Hallituksen esitys 22/2014 vp mainitsee, että pelkästään teknisillä välineillä suoritettua valvontaa ei pidetä vartioimistehtävänä (25). Mutta siinä vaiheessa, kun järjestelmän automaattisesti generoimaa hälytystä aletaan tutkimaan tarkemmin tapahtuman ja mahdollisesti tekijän selvittämiseksi, voi kyseeseen tulla luvanvarainen rikoksen paljastaminen (Paasonen & Ellonen 2010, 68-69).

Rikoksen rakenne voidaan määritellä siten, että se on tunnusmerkistön mukainen, oikeudenvastainen teko, joka osoittaa syyllisyyttä tekijässään (Paasonen 2008, 58; Frände 2005, 10; Melander 2010, 87). Tunnusmerkistön mukaisuus liittyy itse tekoon, sen seurauksiin ja tahallisuuteen ja siihen, täyttääkö teon tunnusmerkistö lainsäädännössä minkään rikoksen tunnusmerkistöä (Frände 2005, 11; Melander 2010, 88).

Jos teko täyttää rikoksen tunnusmerkistön, tutkitaan seuraavaksi voisiko teko oikeuttamisperusteiden (esimerkiksi hätävarjelu tai pakkotila) mukaan olla kuitenkin oikeudenmukainen (Frände 2005, 11; Melander 2010, 89). Syyllisyyden ratkaisuun taas kuuluu sen tahallisuuden ja tuottamuksellisuuden arviointi, syyksiluettavuuden arviointi ja näitä käsitellään oikeudessa vähintään tuomarin toimesta (Frände 2005, 11; Melander 2010, 90).

Nämä asiat kuuluvat kuitenkin usein oikeusprosessiin, joten ne harvoin ovat tiedossa tutkinnan alkaessa. Siksi tulkinta rikoksen paljastamisesta tai selvittämisestä tulisi tehdä ensisijaisesti edellisessä kappaleessa käsitellyn rikoksen tunnusmerkistön täyttymisellä.

Periaatteessa mukaan voitaisiin laskea neljäntenä osana myös teko, kuten Ruotsissa tehdään (Melander 2010, 90). Suomessa teon on kuitenkin katsottu kuuluvan syyllisyysperiaatteen edellytyksiin (Melander 2010, 90). Rikoksen rakenteen toisen tai kolmannen tekijän arviointi ei kuulu enää rikosten paljastamiseen, vaan nämä asiat ratkeavat yleensä myöhemmin oikeuskäsittelyssä. Rikosprosessiin kuuluu esitutkinta, syyteharkinta, oikeudenkäynti ja rangaistuksen täytäntöönpano (Melander 2010, 4). Rikoksen paljastaminen ei kuulu Suomessa siten rikosprosessiin. Suomessa poliisi suorittaa rikosprosessin esitutkinnalla, kun sille tehdyn ilmoituksen tai muun syyn perusteella on syytä epäillä rikoksen tapahtuneen (esitutkintalaki 805/2011, 3 luku 1§).

Rikosoikeudellinen laillisuusperiaate edellyttää, että rikokseksi voidaan luokitella vain teko, josta on sen tekohetkellä laissa säädetty rangaistus. Laillisuusperiaate liittyy myös kansainvälisiin säädöksiin, kuten Euroopan ihmisoikeussopimukseen, eikä kyseessä ole vain kansallinen periaate. Yksi laillisuusperiaatteen ydintekijöistä on kirjoitetun lain vaatimus. Tämä tarkoittaa sitä, että tuomion tulee perustua aina eduskunnan hyväksymään lakiin siten kuin siitä on laissa kirjotettu. Epätäsmällisyyskiellon mukaan taas laki on kirjoitettava siten, että sen perusteella voi kuka tahansa ilman lainopillista apua epäillä rikoksen tapahtuneen. (Melander 2010, 40–46).

Rikokseen liittyy myös rangaistus, mutta tämän työn tavoitteena ei ole pohtia rikosten luonnetta syvemmin, niiden seurauksia tai esimerkiksi erilaisen rikollisuuden selvittämisen tehokkuutta tai sopivuutta yksityistämisen tai viranomaisprosessin välillä. Samasta syystä työn näkökulmasta yksityissektorille kuulumaton kriminalisointiteoria rangaistuksen säätämisen oikeudellisista reunaehdoista jätetään käsittelemättä (Melander 2010, 20). Tässä työssä rikoksena pidetään loppujen lopuksi vaan laissa rikoksen tunnusmerkistön täyttävää tekoa riippumatta syyllisyyden arvioinnista.

Yksityisetsivätoimintaa liitettäessä lakiin yksityisistä turvallisuuspalveluista, hallituksen esityksen perusteluissa todettiin rikosten paljastamisen olevan ”… selvittämistoimenpiteistä, joiden avulla hankitaan riittävät tiedot viranomaisille tehtävää rikosilmoitusta varten.” (HE 69/2001, 30). Voisi ajatella, että sellaiset selvitykset, joiden perusteella rikosilmoituksen tekeminen ei olisi mahdollista, eivät kuuluneet alun perin lainsäätäjän ajatukseen rikosten paljastamisesta. Toimeksianto, joka alkaa rikoksen paljastamisena, voi loppujen lopuksi paljastaa jonkin muunlaisen tapahtuman kuin rikoksen. Toisaalta esimerkiksi työnantajan ohjeiden vastaisen toiminnan selvittäminen voi johtaa hyvin tilanteeseen, jossa päädytään selvittämään myös rikoksen tunnusmerkistön täyttävää tekoa.

Rikos- ja oikeusprosessi edustavat merkittävää julkisen vallan käyttöä, eikä sellaisia tehtäviä voi perustuslain mukaan antaa muuta kuin viranomaiselle (perustuslaki 731/1999, 11 luku, 124 §). Rikoksen paljastaminen ja selvittäminen yksityissektorilla sijoittuu siis ennen virallista rikosprosessia ja siinä korostuu siis eniten tunnusmerkistö. Viranomaisprosessi taas ei kuulu tämän työn sisältöön. Joka tapauksessa puututtaessa yksilön perusoikeuksiin, myös henkilötietoja käsitellessä, tulee siitä aina säännellä riittävän tarkkarajaisella lainsäädännöllä ja soveltamisalaltaan täsmällisellä lailla (HE 7/2021 vp, 4 ja 26; PeVL 30/2010 vp, 6/II; HE 22/2014 vp, 4; PeVL 23/2020 vp, luku Henkilötietojen käsittely; Halford v. The United Kingdom, kohdat 49–50). Siten ilman turvallisuusalan elinkeinolupaa suoritettavaan yksityisetsivätoimintaan ei voi liittyä yksilön perusoikeuksiin puuttumista.

3.2 Erityiskysymykset ja rajanvedot

Rikoksen paljastamista ja yleisesti turvallisuuspalveluita voi olla vaikea erottaa toisistaan. Jos ostetaan omaan asuntoon tai yritykseen kamera tai liiketunnistin, niin melko varmasti siitä on apua myös rikoksen paljastamisessa. Kameran asentamisessa tai sen tallenteiden käytössä ei ole välttämättä kuitenkaan kyse rikoksen paljastamisesta, vaan siinä voi olla kysymys myös lemmikkien seuraamisesta isäntäväen poissa ollessa tai työntekijöiden turvallisuuden varmistamisesta ennaltaehkäisevänä ratkaisuna. Tänä päivänä monet väärinkäytösten ehkäisyyn käytetyt työvälineet tietoverkoissakin toimivat hyvin samalla tavalla kuin rikosten paljastamisessa käytetyt työvälineet. Verkkoliikenteen seulonta, tietojärjestelmien käytön ja käyttötapojen valvonta ja erilaiset automaattiset tietojen esille haun, tallentamisen ja välittämisen seurantajärjestelmät ovat laajasti käytössä niin ennaltaehkäisevässä tarkoituksessa kuin selvitystyössäkin. Monia turvallisuustuotteita ja -palveluita voidaan myydä tai tarjota vapaasti ilman erityistä toimilupaa palveluiden tarjoamisesta annetun lain tarkoituksen mukaan (laki palvelujen tarjoamisesta 22.12.2009/1166, 1 §).

Erityistä toimilupaa edellytetään vasta, kun palvelu kuuluu edellä mainitun lain soveltamisalan poikkeuksiin, esimerkiksi silloin, kun kyse on laissa yksityisistä turvallisuuspalveluista säädellyistä yksityisistä turvallisuuspalveluista (laki palvelujen tarjoamisesta 22.12.2009/1166, 2 §, kohta 10). Rajanveto ei ole aina selvä esimerkiksi aiemmin mainittujen tietoteknisten ja tietohallinnon menetelmien näkökulmasta. Esimerkiksi hyväksymistä edellyttävällä turvasuojaustehtävällä tarkoitetaan ”…sähköisten ja mekaanisten lukitusjärjestelmien, murtohälytysjärjestelmien ja kulunvalvontajärjestelmien asentamista, korjaamista tai muuttamista niihin kuuluvaa kaapelointityötä lukuun ottamatta” (laki yksityisistä turvallisuuspalveluista 2 §, kohta 15). Monessa yrityksessä esimerkiksi kulunvalvontaan hallinnoivien tietojärjestelmien alustat ja ohjelmistot voidaan asentaa oman tai ulkoistetun IT-yrityksen toimesta, vaikka IT-yrityksellä ei olisi edellä mainittua hyväksyntää. Ratkaisun fyysiset elementit, lukijat, päätteet ja ohjelmistot, voi tosin toimittaa yhtiö, jolla lupa on. Usein heillä ei ole kuitenkaan riittävää osaamista tai

pääsyoikeuksia suorittaa lopullista sovittamista asiakkaan muuhun IT-infrastruktuuriin. Eikä siten mahdollisuus varmistua esimerkiksi järjestelmän pääsynhallinnasta ja myöhemmin suoritettavista ylläpitotoimista. Tilanne on ongelmallinen, koska loppujen lopuksi toimitettua järjestelmää ovat asentamassa ja hallinnoimassa pääkäyttäjäoikeuksilla henkilöt, joilla ei olisi lain sanatarkan tulkinnan mukaan oikeutta asentaa niitä. Turvasuojaustoiminta ei kuitenkaan kuulu tämän työn piiriin, mutta tämä kertoo siitä, että tulkinnallisia asioita on yksityisen turvallisuusalan lainsäädännön osalta muuallakin.

Tietojärjestelmät taas suorittavat monesti erilaisia automaattisia operaatioita, joiden voisi tulkita olevan rikoksen paljastamista. Esimerkiksi tunkeutumisen havaitsemiseen tarkoitetut tietojärjestelmät ja palomuurit tekevät sensoriensa kautta jatkuvaa IT-ympäristön seurantaa etsien poikkeavuuksia, jotka viittaisivat tunkeutumiseen. Myös Helsingin käräjäoikeus (2001, 5) tulkitsi vartioimistehtäväksi toiminnan, johon kuuluu ”rikosten paljastamiseen liittyvien hälyttimien tai monitorien tarkkailu”. Poikkeama voi olla ennalta kuvatun tai haittaohjelmalle tyypillisen ”sormenjäljen” etsintää. Poikkeama tai hälytys voi perustua myös laitteiden toiminnan seurantaan ja toiminnan vertaamiseen normaalitilaan. Etenkin jälkimmäinen voi aiheuttaa usein myös vääriä hälytyksiä. (What is an Intrusion Detection System? 2022). Siten tätä voisi pitää rikoslain tarkoittamana tietomurron tai sen yrityksen paljastamisena, koska jo tietoverkon skannaaminen siellä olevien haavoittuvuuksien paljastamiseksi täyttää tietomurron yrityksen tunnusmerkistön, vaikkei varsinaista tunkeutumista olisi tapahtunut (Rikoslaki 39/1889, luku 38, 8 §).

Tosin suuri osa näiden järjestelmien käsittelemästä datasta on täysin normaalia tietoliikennettä. Esimerkiksi lähiverkkojen toiminnan kannalta elintärkeä DHCP (Dynamic Host Configuration Protocol) toimii siten, että verkkoon kytkeytyvä laite lähettää aina koko verkkoon tiedustelun, jossa se etsii DHCP-palvelinta, jolta saisi osoitteen ja muut liikennöimiseen tarvittavat tiedot (IETF 1997, luku 3.1). Protokolla käyttää IP-osoitteita, jotka ovat henkilötietoa, mutta eivät välttämättä suoraan paljasta niiden haltijaa, koska ne ovat pelkkiä numerosarjoja (IETF 1983). Tietyillä suojausasetuksilla tai liiallisesti toistuvana tavanomainen verkkoliikenne voi muodostaa tunkeutumien havaitsemiseen tarkoitetutussa järjestelmässä hälytyksen, kuten edellisessä luvussa todettiin. Kyse ei kuitenkaan ole oikeasta poikkeamasta, vaan sinällään tavallista laitteen toimintaa, mutta väärässä paikassa tai väärillä asetuksilla. Hälytys ei myöskään suoraan yksilöi tekijää, vaan vaatii aina lisäselvityksiä toisin kuin esimerkiksi kameravalvonta. Tietoverkkojen hallinnassa kyse ei myöskään ole aina rikollisen teon selvittämisestä ja syyteharkintaan saattamisesta. Kyseessä voi olla vain teknisen vian havaitseminen. Usein tavoitteena on vahinkojen rajoittaminen ja normaalitoimintaan palaaminen. Tapahtuma voi toki paljastua tietomurroksi, mutta sitä ei ole tarkoituskaan selvittää sen rikostutkinnallisessa mielessä (esimerkiksi Mikkola 2021).

Tietoverkoissa ja järjestelmäympäristöissä yksittäisen havainnon käsittely tai edes useamman automaattisen analysoinnin tuloksena muodostuva hälytys ei siten ole aina rikos, vaan voi olla myös täysin normaalia verkon toimintaa tai vaan rikkinäisen laitteen aiheuttama hälytys. Sähköisen viestinnän palveluista annetun lain luvun 18 pykälä 149 antaa luvattoman käytön selvittämiseksi oikeuden kenelle tahansa yhteisötilaajan määritelmän täyttävälle – esimerkiksi työnantajalle. Vasta käsittelyn muuttuessa manuaaliseksi, voidaan alkaa puhua siitä, onko kyse rikoksen paljastamisesta. Siihenkin viestintäpalvelulain 18 luku antaa kuitenkin oikeuden myös muille kuin pelkästään lain yksityisistä turvallisuuspalveluista tarkoittamille turvallisuusalan elinkeinoluvan haltijoille. Kyseiseen lakiin on kirjattu myös siihen liittyvät huolehtimis- ja ilmoitusvelvollisuudet niitä valvovalle viranomaiselle ja siten käsittely on viranomaisvalvonnan piirissä. Tätä käsitellään myöhemmin tarkemmin luvussa Viestintäpalvelulaki.

Julkisuudessa on puhuttu viime aikoina myös niin sanotuista ”valkohattuhakkereista”. Nämä ovat pääsääntöisesti tietoturva-aukkoja ja heikkouksia etsiviä henkilöitä, eivätkä varsinaisesti rikosten selvittäjiä. Myös viranomaiset voivat käyttää heitä apuna. (YLE 2019; Aamulehti 2020). Kuten aiemmin todettiin, toiminta täyttää helposti tietomurron yrityksen tunnusmerkistön kohdistuessaan muihin kuin omiin laitteisiin tai ohjelmistoihin. Tätä varten on myös laillisia niin sanottuja ”bug bounty” -ohjelmia, joiden avulla yritykset etsivät haavoittuvuuksia omista tuotteistaan (esimerkiksi F-Secure 2020). Näissä ei siis ole kyse tapahtuneen rikoksen selvittämisestä, vaan tuotteiden kartoittamisesta sellaisten ominaisuuksien osalta, joita voitaisiin käyttää rikoksen tekemisessä hyödyksi. Haavoittuvuuksia etsivä toimija voisi osallistua rikoksen selvittämiseen myös viranomaisen ohjauksessa. Silloin se toimisi viranomaisen luovuttamilla valtuuksilla sen ohjauksessa ja yksityisyyden suojasta vastaisi silloin toimintaa johtava viranominen. Jos tällaisessa toiminnassa käsiteltäisiin henkilötietoa (esimerkiksi verkoissa välitetyt IP-osoitteet), soveltuisi toimijaan myös henkilötietojen käsittelyyn sovellettava lainsäädäntö, koska IP-osoitteet voivat olla myös henkilötietoa (2/936/2005 2005).

Hallituksen esitys 69/2001 nosti esiin, että yksityisetsivätoiminnassa on monesti kyse muustakin kuin luvanvaraisesta toiminnasta. Tällaisiksi eriteltiin muun muassa aiemmin mainitut tasinko-oikeuden selvitystilanteet, mutta myös muut tiedonhankintatehtävät, kuten tietojen ja selvitysten hankkiminen vireillä oleviin oikeustapauksiin sekä henkilöiden oleskelun seuranta julkisilla paikoilla (HE 69/2001, 28). Hallituksen esityksen (69/2001, 30) sanamuodosta selviää kuitenkin, että rikoksen paljastamista ovat selvitystoimenpiteet, joiden perusteella voitaisiin vasta jättää rikosilmoitus. Siten laissakin on tarkoitettu selvittämistoimia rikoksen tunnusmerkistön täyttäviin tekoihin. Lain tarkoittamat rikoksen paljastaminen ja selvittämistoimet eivät voisi riippua siten syyllisyysarviosta tai myöhempään rikosprosessiin kuuluvien oikeuttamisperusteiden arvioinnista. Rikoksen paljastamista on siis

minkä tahansa rikoksen tunnusmerkistön täyttävän teon tai toiminnan tutkinta riippumatta siihen myöhemmin liittyvän viranomaistutkinnan tai oikeusprosessin tuloksista.

Perusteluista saa siis vaikutelman, että rikoksen paljastamiseksi tai selvittämiseksi luetaan vain toiminta, jonka on tarkoitus paljastaa lainsäädännössä rangaistavaksi määritelty teko. Rajanveto oikeustapauksiin liittyvien tietojen ja selvitysten hankkimisen ja rikoksen selvittämisen välillä ei välttämättä ole aina yksiselitteinen. Syyllisyys ratkeaa kuteinkin vasta oikeusprosessissa.

3.3 Edellytykset, toimivaltuudet ja velvollisuudet rikoksen paljastamisessa

Turvallisuusalan elinkeinolupa voidaan myöntää luonnolliselle henkilölle tai oikeushenkilölle (laki yksityisistä turvallisuuspalveluista, 3 §). Lupa on voimassa Suomen alueella ja suomalaisilla aluksilla ja sen myöntää poliisihallitus (laki yksityisistä turvallisuuspalveluista, 68 §). Toimintaa valvoo poliisilaitokset toimialueillaan (laki yksityisistä turvallisuuspalveluista, 84 §). Koska lupa rajoittuu Suomeen ja suomalaisiin aluksiin, käsitellään tässä työssä toimintaan liittyvää henkilötietojen käsittelyä myös suhteessa suomalaiseen lainsäädäntöön, vaikka joidenkin kysymysten osalta ja esimerkkien puuttuessa oikeustapauksia voidaan joutua käsittelemään muualtakin kuin Suomesta.

Rikoksen paljastaminen luetaan vartioimistehtäväksi (laki yksityisistä turvallisuuspalveluista, 2 §, 2 kohta). Henkilö, joka työskentelee turvallisuusalan elinkeinoluvan palveluksessa suorittaessaan vartioimistehtäviä, on lain tarkoittama vartija (laki yksityisistä turvallisuuspalveluista, 2 §, 6 kohta). Siten rikoksen paljastamista suorittavalla henkilöllä tulee olla voimassa myös vartijaksi hyväksyminen (laki yksityisistä turvallisuuspalveluista, 10 §). Vartioimisliiketoiminnassa ei saa ottaa vastaan tehtävää, joka sisältäisi sitoumuksen ylläpitää yleistä järjestystä tai turvallisuutta (laki yksityisistä turvallisuuspalveluista, 5 §). Rikoksen paljastamisen näkökulmasta tämä tarkoittaa sitä, että vartioimisliike tai sen palveluksessa olevan vartijan rikoksen paljastamiseen liittyvät oikeudet rajoittuvat lain yksityisistä turvallisuuspalveluista neljännen pykälän mukaan vartioimisalueelle ja toimeksiantosopimuksen osapuolena olevaan tahoon.

Hallituksen esityksellä 42/2016 vp vartijan toimialuetta kuitenkin laajennettiin käsittämään muutkin alueet, kunhan sillä on jokin liityntä vartioimisalueeseen (2016, 10). Tämä lisäys on rikoksen paljastamisen näkökulmasta tarpeellinen. Esimerkiksi näyttöaineiston analysointi tai tietolähteet eivät välttämättä sijaitse kohteessa tai toimeksiantajalla, johon liittyvää rikosta selvitetään. Muuhun kuin turvallisuusalan elinkeinoluvalla tehtävään yksityisetsivätoimintaan ei myöskään käy lainmukaisuusperusteeksi yleisen järjestyksen tai turvallisuuden ylläpitäminen, sillä sellainen vastuu kuuluu yksinomaan valtion viranomaisten tehtäväksi (HE 69/2001 vp, 15). Julkisilla paikoilla tapahtuva yksittäisen henkilön tarkkailuun liittyvä oikeus ja oikeus tietojen ja selvitysten hankkimiseen jo vireillä oleviin oikeustapauksiin muussa kuin

turvallisuusalan elinkeinolupaan liittyvässä toiminnassa on kuitenkin huomioitu hallituksen esityksen perusteluissa (HE 69/2001 vp, 28, 43).

Rikoksen paljastamista suorittavan yhtiön toimivaltuudet perustuvat erityissäännöksiin ja oikeuttamisperusteisiin ja joistakin on säädetty viittaussäännöksin (Paasonen 2008, 127). Käytännössä toimivaltuudet vastaavat edellä perustellun mukaan siis vartijan toimivaltuuksia. (Laki yksityisistä turvallisuuspalveluista, luku 1, 2 § ja Paasonen 2008, 100). Vartijan toimivaltuuksia ovat (esimerkiksi Paasonen 2008 ja laki yksityisistä turvallisuuspalveluista 1085/2015):

1. Pääsyn estäminen ja henkilön poistaminen vartioimisalueelta (15 §)
2. Kiinniotto-oikeus ja oikeus turvallisuustarkastukseen kiinnioton yhteydessä (16 §)
3. Voimakeinojen käyttö edellisten yhteydessä (17 §)

Sen lisäksi lain yksityisistä turvallisuuspalveluista (1085/2015) 18-21 pykälien perusteella vartijalla on oikeuksia voimankäyttövälineiden ja ampuma-aseen kantamiseen ja koiran käyttöön tietyissä tilanteissa. Rikoksen paljastamisen osalta ei tässä laissa ole erityisiä, esimerkiksi tiedonhankintaan, liittyviä erityissäännöksiä tai erityistä toimivaltaa.

Oikeuttamisperusteina Paasonen mainitsee muiden muassa hätävarjelun, pakkotilan, jokamiehen kiinniotto-oikeuden, itseavun, loukatun suostumuksen ja poliisin avustamisen (Paasonen 2008, 101-113). Hätävarjelusta säädetään rikoslain (39/1889) neljännen luvun neljännessä pykälässä, pakkotilasta saman lain ja saman luvun viidennessä pykälässä, yleisestä kiinniotto-oikeudesta pakkokeinolain (806/2011) toisen luvun toisessa pykälässä ja itseavusta saman lain ensimmäisen luvun viidennessä pykälässä. Suostumus on rikoslaissa usein oikeuttamisperusteena (Paasonen 2008, 113). Poliisilla taas on poliisilain perusteella oikeus pyytää apua muiltakin kuin turvallisuusalan toimijoilta (esimerkiksi virka-apuna muilta viranomaisilta, poliisilaki 872/2011, luku 9, 2 §). Jos rikosta selvittäessä henkilö joutuisi hätävarjelutilanteeseen tai joutuisi selvitystehtävissä todistamaan pakkokeinolain toisen luvun toisen pykälän tunnusmerkistön täyttävää rikosta, nämä oikeuttamisperusteet täyttyisivät. Mutta ne kuuluvat kaikille kansalaisille. Oikeuttamisperusteissa ei siis ole mitään erityisesti rikoksen paljastamiseen tai sitä suorittavan henkilön asemaan liittyvää oikeutta.

Vartioimistehtävissä noudatettavista yleisistä periaatteista on todettu, että tehtäviä suoritettaessa on toimittava oikein, olla aiheuttamatta suurempaa haittaa tai puuttumatta kenenkään perusoikeuksiin enempää kuin on tarpeen tehtävien suorittamiseksi (laki yksityisistä turvallisuuspalveluista 1085/2015, 6 §). Hallituksen esityksessä (HE 22/2014 vp) viitataan poliisilain tarpeellisuus- ja suhteellisuusvaatimuksiin, joiden perusteella kaikki toimenpiteet tulee olla puolustettavia suhteessa tehtävän tärkeyteen, eikä kenenkään oikeuksiin saa puuttua enempää kuin on tehtävien suorittamiseksi välttämätöntä (33). Aiemman lain perusteluissa teksti oli melkein saman muotoinen, mutta uudemmasta on jäänyt

pois periaatteiden suuntaviivojen määrittyminen perustettavaksi ehdotetun turvallisuusalan neuvottelukunnan ja yksittäistapauksiin liittyvän lupa- ja valvontakäytännön mukaan (HE 69/2001 vp, 58). Koska uudempi ei kuitenkaan sisällä mitään korvaavaa käytäntöä tai erityisesti lakkauta aiempaa, vanhemman käytännön voi ajatella olevan edelleen voimassa. Siten turvallisuusalan elinkeinoluvan haltijoiden on syytä seurata myös näitä päätöksiä ja julkaisuja toiminnan lainmukaisuuden varmistamiseksi.

Perustuslakivaliokunta lausui 2014 vuonna 2015 voimaan tulleen ja voimassa olevan yksityisiä turvallisuuspalveluita koskevan lain (1085/2015) osalta, että vartijoiden tehtävät ovat julkisia hallintotehtäviä. Vartijoiden asema tunnustetaan viranomaisia avustavana ja merkittävänä julkisen vallan käyttönä pidetään esimerkiksi itsenäiseen harkintaan perustuvaa puuttumista yksilön perusoikeuksiin. Valiokunta mainitsee myös Suomen perustuslain estävän poliisitoiminnan yksityistämisen. Lausunnossaan perustuslakivaliokunta kertoi myös antaneensa paljon painoarvoa sille, että vartijoiden valtuudet ovat pääosin samoja kuin kenellä tahansa yksityishenkilöllä, eikä toimivaltuuksien saakaan muodostua olennaisiksi vallankäyttötavoiksi. (PeVL 22/2014 vp, 2).

Julkisen hallintotehtävän perusteluissa korostuvat usein nimenomaan voimankäyttöoikeudet (esimerkiksi Keravuori-Rusanen 2008, 176). Rikoksen paljastamisessa on myös muita tekijöitä. Rikoksen paljastaminen ja selvittelyssä poliisin avustaminen on myös viranomaistoimintaa täydentävä tehtävä, mikä luetaan julkiseksi hallintotehtäväksi (Keravuori-Rusanen 2008, 171). Ja vaikka rikoksen paljastamista suorittavalla ei ole suoraan päätös- tai tuomiovaltaa asioissa, lasketaan myös päätöksen kannalta merkitykselliset valmistelutoimet ja siten esimerkiksi rikosoikeudessa esitutkinta ja poliisitutkinta julkisen vallan käyttämiseksi (Keravuori-Rusanen 2008, 124). Siten esimerkiksi rikosoikeudellista virkavastuuta voidaan soveltaa valmisteluun samoin kuin asian ratkaisuun (Keravuori-Rusanen 2008, 124). Valmistelun ja vaikutuksia aiheuttavien päätösten rajan hämärtyessä, tulee asiaa tulkita siten, että myös valmistelu on julkisen vallan käyttöä, joka kuuluu viranomaiselle (Apulaisoikeuskansleri 2021, 12). Toiminnassa, jossa on julkisen hallintotehtävän piirteitä, on toimijan noudatettava erityistä huolellisuutta, kuten selviää muun muassa tietosuojavaltuutetun seuraamuskollegion sakotusperusteista liittyen pysäköintivirhemaksuihin liittyvään tietojen käsittelyyn (2477/161/21, 25).

Perustuslaki on Suomen lainsäädännön perusta ja määrittää muiden muassa yksilön ja julkisen vallan välisestä suhteesta ja julkisen vallan käytön periaatteet (Oikeusministeriö 2021). Julkiseen hallintotehtävään ja sen hoitamiseen on otettu kantaa perustuslakien yhtenäistämisen ja ajantasaistamisen yhteydessä vuonna 1998. Sen yhteydessä puhuttiin perustuslakiin kirjatusta niin sanotusta valtiosääntöoikeudellisesta virkamieshallintoperiaatteesta, joka tarkoittaa sitä, että Suomessa julkista valtaa voivat käyttää vain viranomaiset ja virkoihin nimetyt virkamiehet. Myös tässä yhteydessä

tunnustettiin se mahdollisuus, että julkista valtaa voisivat käyttää myös liikelaitokset ja julkisoikeudelliset yhteisöt. Edellytykseksi asetettiin kuitenkin, että tällaisesta julkisen vallan käyttämisestä olisi säädettävä lailla. Perusteluna mainittiin muun muassa kansalaisten perusoikeuksien ja oikeusturvan säilyminen. Merkittävää julkista valtaa voisi kuitenkin jatkossakin käyttää vain viranomainen. Merkittävän julkisen vallan tunnusmerkistöön luettiin tässäkin kuuluvaksi itsenäiseen harkintaan perustuva voimakeinojen käyttö tai merkittävä yksilön perusoikeuksiin puuttuminen. (HE 1/1998 vp, 179/II).

Lisäksi tulee ottaa huomioon, että yksityisen turvallisuuspalvelulain valmistelun osalta mainittiin, yhteiskunnan kannalta tärkeäksi se, että viranomaisten ja yksityisten turvallisuuspalvelujen tehtäväjaosta säädetään täsmällisesti (HE 22/2014vp, 4). Lisäksi perustuslakivaliokunta on ottanut kantaa yksityisen turvallisuusalan lainsäädäntövalmistelussa, että kaikki toimivaltuudet tulisi aina olla tapauskohtaisia ja ajallisesti rajallisia (PeVL 10/2006 vp, 2–3/I & PeVL 13/2010 vp, 2). Edelliset asiat huomioiden, ei voida vetää johtopäätöstä, että vartijalla olisi oikeus muihin kuin laissa yksityisistä turvallisuuspalveluista määriteltyihin toimivaltuuksiin. Siten ei olisi myöskään itsenäiseen harkintaan perustuvaa oikeutta puuttua kenenkään oikeuksiin tai vapauksiin merkittävästi, vaikka rikoksen paljastamiseksi se olisikin välttämätöntä.

Toimivaltuuksia voi saada myös muualta lainsäädännöstä. Esimerkiksi tarkkailu havaintojen tekemiseksi salaa henkilöstä kameran tai katseluun tarkoitetun teknisen välineen avulla on sallittua, kunhan ei syyllisty salakatseluun tai salakuunteluun. Suunnitelmallisella tarkkailulla taas tarkoitetaan rikoksesta epäiltyyn kohdistuvaa muuta kuin lyhytaikaista tarkkailua. Suunnitelmallisen tarkkailun edellytyksenä, että epäillystä rikoksesta ankarin rangaistus olisi vähintään kaksi vuotta vankeutta ja toimivaltuus on määritelty vain esitutkintaviranomaiselle. (Pakkokeinolaki 806/2011, luku 10, 12§). Tästä päätellen yksityisetsivätoiminnassa voisi käyttää vain lyhytaikaista tarkkailua työvälineenä. Tarkkailun ollessa rikoksen paljastamista, se edellyttäisi kuitenkin turvallisuusalan elinkeinolupaa ja tulisi huomioida milloin se ei ole enää lyhytaikaista ja olisi siten siirrettävä esitutkintaviranomaiselle.

Myöhemmin luvussa Työelämän tietosuojalainsäädäntö tullaan käsittelemään työnantajan oikeuksia tekniseen tarkkailuun ja valvontaan. Yksityishenkilöihin kohdennettuna ilman työsuhdekontekstia ei laissa ole tästä säännöksiä lukuun ottamatta viranomaisen toimivaltuuksia pakkokeinolain (806/2011) kymmenennessä luvussa (1 §). Samoin peitetoiminnasta ja valeostoista on annettu toimivaltuuksia vain viranomaiselle (pakkokeinolaki 806/2011, luku 10, 27 §). Siten voisi ajatella, että teknisen tarkkailun, peitetoiminnan tai valeostojen kohdistaminen ei ole mahdollista muissa tapauksissa yksityishenkilöihin. Toisaalta valeostojen osalta on aika vaikea pohtia, missä menee raja valeoston ja tavanomaisen oston välillä, etenkin jos tapaus perustellaan todisteiden kokoamiseksi jälkimmäisestä. Näissä on kuitenkin huomioitava rikokseen yllyttämisen

mahdollisuus. Jos tarkkailu, peitetoiminta tai valeostot suoritetaan siten, että voidaan katsoa yksityisetsivän syyllistyneen rikokseen yllyttämiseen, hänet voidaan myös tuomita rikoksesta (rikoslaki 39/1889, luku 5, 5 §). Keinovalikoiman osalta tulee olla ehdottoman varma, että kohdetta ei tahallisesti tai tahattomasti ohjata rikoksen tekemiseen.

4 Yksityisetsivätoiminta käytännössä

Yksityisetsivätoimintaan kuuluu myös muita toimeksiantoja kuin rikosten paljastamista. Tämä toiminta ei Suomessa vaadi erityistä lupaa eikä sitä säännellä missään lainsäädännössä, vaan toimijat toimivat jokamiehenoikeuksin. Yksityisetsivätoiminnan ensisijainen tarkoitus on palvella toimeksiantajaa, eikä olla yhteiskunnallisesti yleistä järjestystä tai turvallisuutta edistävää toimintaa (Sennewald & Tsukayama 2015, 22). Tällainen tilanne voi olla esimerkiksi tapauksissa, jotka eivät ole rikoksia, mutta muodostavat sopimusrikkomuksen tai ovat eettisesti arveluttavia. Esimerkiksi työantajan ohjeita vastaan toimiminen tai uskottomuus parisuhteessa.

Edellisessä luvussa kuvattiin yksityisetsivätoimintaa lainsäädännön näkökulmasta. Sen mukaan yksityisetsivätoiminnasta on lainsäädännössä enää se ulottuvuus, joka edellyttää turvallisuusalan elinkeinolupaa. Muun yksityisetsivätoiminnan nähtiin olevan vähämerkityksistä, joten sääntelylle ei nähty tarvetta. Työn tulosten saavuttamiseksi on huomioitava koko yksityisetsivätoiminnan kenttä, koska henkilötietoja käsitellään todennäköisesti muussakin toiminnassa. Tämän luvun tarkoitus on pyrkiä kuvaamaan yksityisetsivätoimintaa käytännön näkökulmasta ilman rajausta johonkin tietyn tyyppiseen toimintaan. Työn tilaajan toiveena oli myös kuvata yksityisetsivätoimintaa ja sen suhdetta kansainväliseen toimintaan tänä päivänä.

4.1 Yksityisetsivätoiminta Suomessa

Turvallisuusalalla toimi palvelualojen toimialakatsauksen mukaan vuonna 2007 etsivä-, vartiointi- ja turvallisuuspalvelujen toimialaluokituksen (TOL 746) alla 400 yritystä. 80 % yrityksistä työllisti alle viisi henkilöä. Finnsecurity ry:n arvion mukaan tämä on noin 60 koko turvallisuusalasta koko turvallisuusalan työllistäessä noin 12000-13000 henkilöä. Toimialaraportin mukaan yritystoiminta on keskittynyt muutamalle suurelle yritykselle. (Tilastokeskus 2008).

Finnsecurity ry:n teettämän suhdanne- ja toimialaraportin mukaan vuonna 2020 turvallisuusalalla toimi noin 1000 yritystä, joista vajaat 800 sen toimialaluokituksen alla. Yritysten määrä etsivä- vartiointi ja turvallisuuspalvelujen toimialalla on noin kaksinkertaistunut, mutta tilanne toimijoiden suhteen on edelleen saman kaltainen. Kahdeksan suurinta yhtiötä vastaa 60 %:a toimialan työllisyydestä ja yli 50 %:a liikevaihdosta,

konsernikokonaisuudet huomioiden lähes 80 % molemmista. (Finnsecurity ry 2020). Näiden tulosten perusteella ei voida kuitenkaan vielä sanoa, millaista ja miten laajaa on yksityisetsivätoiminta.

Poliisihallitukseen kuuluva turvallisuusalan valvontayksikkö pitää kirjaa voimassa olevista turvallisuusalan elinkeinoluvista ja niiden tyypittely on järjestetty seuraavasti (Poliisi 2021):

- järjestyksenvalvojatoiminta
- vartioimisliiketoiminta
- turvasuojaustoiminta

Siirryttäessä uuden lainsäädännön piiriin 2002, saivat yksityisetsivät jatkaa toimintaansa, kun vain hakivat uutta lupaa määräajassa. Lupa myönnettiin rajoitettuna vartioimisliikelupana siten, että se oikeutti vain rikoksen paljastamiseen, mutta ei vartioimistehtäviin. Näitä rajoitettuja lupia saattoi hakea 1.1.2017 asti, jonka jälkeen niitä ei enää myönnetty lakimuutoksen vuoksi rajoitettuna. Lupa tuli hakea sen jälkeen vartioimisliiketoimintaan sisältäen myös vartioimistehtävät. Lupia myönnettiin 2003 rajoitettuna 36 kappaletta. Turvallisuusalan valvontayksikkö siirtyi uuteen lupajärjestelmään toukokuussa 2015, jolloin lupia oli jäljellä enää 15. Nämä olivat voimassa 31.12.2016 asti, ellei lupaa haettu uudelleen. Näistä luvista jäljelle jäi kahdeksan. Peruuttamisista suurin osa on tehty luvanhaltijan itsensä pyynnöstä, muutama viranomaisaloitteisesti. (Turvallisuusalan valvontayksikön asiantuntija 2021).

Rajoitetun vartioimisliikeluvan hakijoiden joukossa ei ollut vain yksityisetsiviä. Mukana on ollut myös yrityksiä, jotka esimerkiksi asentavat ja hallinnoivat kulunvalvontajärjestelmiä turvasuojaukseen liittyvällä luvalla, mutta joutuvat työssään käsittelemään rikoksen paljastamiseen liittyviä tilanteita. Esimerkiksi kameravalvonnan tallenteiden käsittely rikoksen paljastamistarkoituksessa on edellyttänyt turvasuojausluvan laajentamista myös rikosten paljastamiseen. Mukana voi myös olla yrityksiä, jotka ovat siirtymäsäännöksen nojalla hakeneet lupaa, mutta joiden toiminta nykyään kuitenkin rajoittuu vain muuhun toimintaan kuin rikosten paljastamiseen. Näitä ovat esimerkiksi aiemmin mainitut puolisojen pettäjien paljastajat tai muita selvityksiä tuottavat yhtiöt. (Turvallisuusalan valvontayksikön asiantuntija 2021).

Rikoksen paljastamiseen liittyvä tilastointi oli jo 2001 yksityisen turvallisuusalan lainsäädäntömuutoksen aikaan aika ohuella pohjalla. Hallituksen esityksessä 69/2001 tukeuduttiin arvioon, että yrityksiä olisi noin 20–30, jossa taustana oli Suomen yksityisetsivä- ja lakitoimistoliiton jäsenmäärä, joka oli silloin noin 20 yritystä (HE 69/2001 vp, 28). Tällä hetkellä jäsenmäärä on 19 varsinaista jäsentä (Suomen yksityisetsivä- ja lakitoimistoliitto ry 2021c). Jäsenet ovat tosin henkilöjäseniä ja voivat siten edustaa myös samaa yritystä.

Turvallisuusalan toimijoita on selvitetty myös 2007–2009 turvallisuusalan lainsäädännön kokonaisuudistusta koskevassa hankkeessa. Silloin syntyi Poliisiammattikorkeakoulun tutkimus- ja kehittämisyksikössä selvitys, jonka keskiössä muun muassa oli turvallisuusalan elinkeinoluvan alainen liiketoiminta ja toimijat (Heinämäki 2009, 5). Sen aikaisen selvityksen perusteella vartioimisliikelupia oli vuonna 2008 220 kappaletta, vastaavia hoitajia 290 kappaletta ja toimessa olevia vartijoita 11014 kappaletta (Heinämäki 2009, 23–25). Toimeksiantoja oli vuonna 2008 91359 kappaletta ja toimeksiantoihin sisältyivät omaisuuden vartiointitehtävät, henkilön koskemattomuuden suojaaminen, rikoksen paljastaminen ja näiden tehtävien valvonta. Vartioimisliike saa ottaa vastaan myös järjestyksenvalvontatehtävien suorittamiseen liittyvän toimeksiannon, joten toimeksiantojen lukumäärissä ovat mukana kaikki edellä mainitut tehtävät. Rikoksen paljastamiseen liittyviä tehtäviä ei tässäkään selvityksessä ole yksilöity. (Heinämäki 2009, 27–28).

Ennen vuotta 2017 turvallisuusalan valvonnassa eriteltiin myös rikoksen paljastaminen. Paremmin rikoksen paljastamisen laajuudesta kertoisi juuri näiden toimeksiantojen määrä. Niitä yritettiin kerätä vuosina 2010–2011 käsin tehdyistä vuosi-ilmoituksista käsityönä. Tilastoissa havaittiin kuitenkin olevan niin paljon poikkeamia ja virheitä, että niitä ei sellaisenaan koskaan julkaistu, enkä saanut niitä tietopyynnöstä huolimatta käyttööni. Nykyään toimeksiantojen lukumääriä käsitellään vain vartioimisliiketoiminnan toimeksiantoina sisältäen kaikki siihen liittyvät toimeksiannot. (Turvallisuusalan valvontayksikön asiantuntija 2021). Siten pelkkää yksityisetsivätoimintaa ei voi eritellä niistäkään.

Tutkittaessa tarkemmin Finnsecurity ry:n turvallisuusalan suhdanne- ja toimialaraportissa mainittuja suuria yrityksiä, ei yksityisetsiväpalveluista löydy heidän sivuiltaan tietoja. Securitaksen sivustolla ei mainita sanaa yksityisetsivä missään ja sanaan etsivä viitataan vain parissa kohtaa, blogikirjoituksessa vuodelta 2016 ja sekin koskee myymäläetsivän toimenkuvaa (Securitas 2016). Toinen maininta on tapahtumaturvallisuuspalveluiden alla olevalla sivulla, jossa puhutaan tiedonhankintapalveluista (Securitas 2021a). Turvallisuuspalvelut -sivuilla ei yksityisetsivätoimintaa ole mainittu ollenkaan (Securitas 2021b). Avarnin sivuilta ei löydy etsivä tai yksityisetsivä sanoja ollenkaan. Palmialla etsivä -sana tuottaa vain työn etsintään liittyviä artikkeleita, eikä palveluista löydy etsivätoimintaa. Sama havainto koskee myös Stanley Securityä. (Sanojen hakemiseksi sivustoilta käytettiin menetelmää, jossa Google haku kohdistettiin site -attribuutilla pelkkään yrityksen verkkotunnukseen ja haettiin edellä mainittuja avainvasanoja). Ainakaan alan suurimmat yritykset eivät aktiivisesti kerro näistä palveluista, joten saadakseen paremman kuvan näistä toimijoista, tulee tarkastelua tarkentaa.

Toimijoiden kuvaaminen on toinen tapa lähestyä yksityisetsivätoimintaa toiminnan laadun selvittämiseksi. Yksityissektorilla usein toimijoiden koko ja liikevaihto vaikuttavat merkittävästi siihen, millaisia resursseja heillä on käytössään. Myös lainsäädäntö suhtautuu

toimijoihin eri tavalla. Esimerkiksi yleisessä tietosuoja-asetuksessa on pienten ja mikroyritysten osalta kiinnitetty huomiota velvoitteisiin liittyen muun muassa käsittelytoimien selosteeseen, tietosuoja-asetuksen soveltamiseen, käytännesääntöihin ja täytäntöönpanoon (tietosuoja-asetus 679/2016, resitaalit 39, 98, 167).

Turvallisuusalan valvontayksikön mukaan luotettavin arvio pelkästään rikoksen paljastamisesta saadaan edelleen vertaamalla Suomen Yksityisetsivä- ja Lakitoimistoliitto ry:n jäseniä ja yrityksiä, jotka löytyvät turvallisuusalan valvontayksikön julkaisemasta luettelosta turvallisuusalan elinkeinoluvan haltijoista. Poliisin oma tuntuma on, että pelkästään rikoksen paljastamiseen erikoistuneita yhtiöitä on enää noin kaksi tai kolme toimijaa johtuen muiden syiden lisäksi siitä, että siirtymäsäännöksellä yksityisetsivätoiminnasta turvallisuusalan elinkeinoluvalle siirtyneitä toimijoita on lopettanut ajan myötä. Toiminta on voinut lakata joko kokonaan tai tarve rikosten paljastamiseen tarvittavalle luvalle on lakannut yhtiön siirryttyä tekemään muita selvityksiä. (Turvallisuusalan valvontayksikön asiantuntija 2021).

Suomen yksityisetsivä- ja lakitoimistoliiton jäsenet ovat julkisesti esillä liiton internet-sivuilla (Suomen yksityisetsivä- ja lakitoimistoliitto 2021a). Ristiintaulukoimalla tieto turvallisuusalan valvontayksikön ylläpitämiin turvallisuusalan elinkeinoluvan haltijoihin, saadaan taulukossa 1 esitetty tieto luvanhaltijoista ja luvan laajuudesta:

Yritys	Järjestyksenvalvonta	Vartioimisliiketoiminta	Turvasuojaus
Kerberos turvallisuuspalvelut	X	X	X
AERTS		X	
AMCASE	X	X	X
Nordic Security Service Ltd Oy	X	X	X
Opsec Oy		X	X
AKM Consulting (Finsec aputoiminimi)	X	X	X
Patrikainen M. J.		X	X
Rösund Lillgård		X	X

Taulukko 1: Suomen yksityisetsivä- ja lakitoimistoliiton jäsenet ja turvallisuusalan elinkeinoluvat 2021 (tiedot: Poliisi 2021).

Suomen Yksityisetsivä- ja Lakitoimistoliiton jäsenluettelon perusteella osalla jäsenistä on aiemmin ollut turvallisuusalan elinkeinolupa. Esimerkiksi Etelä-Savon turvamiehet on kertonut kotisivuillaan 2016 saaneensa poliisihallitukselta vartioimisliikeluvan, mutta yritystä ei löydy enää turvallisuusalan valvontayksikön luettelosta (Etelä-Savon turvamiehet 2021; Poliisi 2021). Suomen Yksityisetsivä- ja Lakitoimistoliitto ry:n jäsenluettelossa on myös toimijoita, jotka mainostavat yksityisetsiväpalveluita, mutta joilla ei ole rikoksen paljastamiseen oikeuttavaa turvallisuusalan elinkeinolupaa. Tällöin toimeksiantosopimuksen kohteena on henkilön etsintä, taustaselvitykset tai muu selvitys, eikä rikoksen paljastaminen (esimerkiksi SYL ry jäsenen asiantuntijahaastattelu 2020; Yksityisetsivä Partes 2021). Näitä toimijoita jäsenistössä on 11.

Verkosta löytyy myös toimijoita, joilla on turvallisuusalan elinkeinolupa rikoksen paljastamiseen, mutta jotka eivät ole Suomen yksityisetsivä- ja lakitoimistoliiton jäseniä, esimerkiksi Safetion (Safetion 2021). On myös toimijoita, joiden palvelukuvaukset viittaavat rikoksen paljastamiseen, mutta turvallisuusalan elinkeinolupaa ei toimijalla ole. Esimerkiksi Etsiväpalvelu Paananen puhuu kotisivuilla myymälävarkauksien paljastamisesta ja tekijöiden kiinniottamisesta (Etsiväpalvelu Paananen 2021). Kyseinen verkko-osoite on rekisteröity Kuljettajapalvelu ja Markkinointi Paananen -nimiselle yritykselle, jonka Y-tunnus ei ole turvallisuusalan valvontayksikön luettelossa luvanvaraisista toimijoista (Traficom 2021; Poliisi 2021). On myös aktiivisesti Google Ads:ssa mainostavia toimijoita, kuten esimerkiksi etsivatoimisto.fi, mutta verkkotunnus on rekisteröity media-alan yhtiölle (Traficom 2021). Ilmeisesti rekisteröijä on verkkosivun ylläpitäjälle päätellen yrityksen nimenä löytyvän verkkotunnuksen sisällöstä, eikä itse etsivätoimiston yritystietoja löydy sivuilta. Toki toiminta edellisillä voi olla jonkin toisen Y-tunnuksen alla, mutta luvanvaraisen toiminnan yhteydessä tämä tieto tulisi olla asiakkaan saatavilla. Google Ads mainos haettiin Google -haulla avainsanalla ”yksityisetsivä” Google hakukoneella.

Kauppalehden sivuilta toimialaa 80300 (etsivätoiminta) löytyi lisäksi 23 toimijaa, joiden joukosta löytyi vain yksi turvallisuusalan elinkeinoluvan haltija, joka ei ole Suomen Yksityisetsivä- ja Lakitoimistoliiton jäsen (Kauppalehti 2021). Yritysten nimistä kymmenen viittaa henkilön nimeen, joten todennäköisesti kysymys on yksittäisestä toimijasta (Kauppalehti 2021). Yritystelen sivuilta löytyi yhdeksän toimijaa samalta toimialalta ja Vainu.io sivuilta 21 toimijaa, mutta turvallisuusalan elinkeinoluvan haltijoita ei sen enempää kuin Kauppalehdenkään sivuilta (Yritystele 2021; Vainu.io 2021a). Jos hakua laajentaa Vainu.io sivuilla pääluokkaan turvallisuus- vartiointi- ja etsiväpalvelut, nousee tulosten määrä 1 640 yritykseen. Yritysten joukossa on perinteiseen vartiointiin liittyvät palvelut ja sähköiset hälytysjärjestelmät ja asennus- ja korjauspalvelut, jotka voidaan luokitella myös vähittäiskauppaan tai rakentamiseen (vainu.io 2021b). Niiden läpikäynti ei ole tämän tutkimuksen näkökulmasta olennaista.

Suomen Yksityisetsivä ja Lakitoimistoliitolla on pitkä historia ja se on tunnustettu toimija pitkältä ajalta niin lainsäätäjän kuin lakia valvovan viranomaisenkin toimesta. Liitto on myös kansainvälisesti järjestäytynyt ja se on sitoutunut noudattamaan toiminnassaan kansainvälisen etsiväjärjestön IKD:n (Internationale Kommission der Detektiv-Verbänd) eettisiä ohjeita (Suomen yksityisetsivä- ja lakitoimistoliitto ry 2021b). Yhdistys osallistuu myös yhteiskunnalliseen vaikuttamistyöhön, viimeisin esimerkki lausunto lausuntopalvelussa olevasta työelämän tietosuojalain 4§ muuttamisesta. Olin mukana laatimassa lausuntoa jäsenistön puolesta ja sen tarkoituksena oli tuoda esiin rikoksia tutkivien toimijoiden näkökulmaa. (Suomen yksityisetsivä- ja lakitoimistoliitto ry 2021d; TEM097:00/2020, 2020). Koska kyseessä on ainoa yksityisetsivätoimintaa tavoitteellisesti edistävä organisaatio, jolla on alaan liittyvää merkityksellistä historiaa ja toimintaa alan edustajana Suomessa, keskitytään tässä tutkimuksessa näihin tunnistettuihin luvanvaraisiin toimijoihin. Luvanvaraisiin siksi, että heidän voidaan olettaa suorittavan myös rikoksiin liittyvää tutkintaa.

Liikevaihdon ja henkilöstömäärän kuvaamiseksi on käytetty viiden viimeisen vuoden keskiarvoa. Tutkimuksessa haetaan tyypillistä toimijaa, jolloin talouslukuihin tai niiden kehitykseen pureutuminen tarkemmin ei ole olennaista. Mukana on myös toimialalle 80300 (etsivätoiminta) rekisteröity Vercari Oy, joka ei ole Suomen yksityisetsivä- ja lakitoimistoliiton jäsen. Yritykset näyttävät liikevaihdolta ja henkilöstömäärältään seuraavilta:

Yritys	Liikevaihto (keskiarvo 5 vuodelta	Henkilöstö (keskiarvo 5 vuodelta)	Rekisteröinnit
Kerberos turvallisuuspalvelut	Ei tiedossa	Ei tiedossa	Kaupparekisteri Ennakkoperintärekisteri Työnantajarekisteri
AERTS	Ei tiedossa	Ei tiedossa	Kaupparekisteri
AMCASE			Kaupparekisteri Ennakkoperintärekisteri
Nordic Security Service Ltd Oy	46 800	1	Kaupparekisteri Ennakkoperintärekisteri Työnantajarekisteri
Opsec Oy	766 500 €	10	Kaupparekisteri Ennakkoperintärekisteri Työnantajarekisteri
AKM Consulting (Finsec aputoiminimi)	773 000 €	5	Kaupparekisteri Ennakkoperintärekisteri Työnantajarekisteri
Patrikainen M. J.	Ei tiedossa	Ei tiedossa	Kaupparekisteri Ennakkoperintärekisteri

Rösund Lillgård	Ei tiedossa	Ei tiedossa	Kaupparekisteri Ennakkoperintärekisteri
Vercari Oy	48 400 €	Ei tiedossa	Kaupparekisteri Ennakkoperintärekisteri Työnantajarekisteri

Taulukko 2: Yksityisetsivätoimintaa turvallisuusalan elinkeinoluvalla tekevät Suomen yksityisetsivä- ja lakitoimistoliiton jäsenet (Tiedot: Suomen Asiakastieto 2021)

Suomessa tilinpäätös on rekisteröitävä julkisesti vain, jos kaksi seuraavista ehdoista täyttyy (Taloushallintoliitto 2021):

- liikevaihto 12 000 000 €
- taseen loppusumma 6 000 000 €
- palveluksessa keskimäärin 50 henkilöä.

Edellisen vuoksi monet pienyritykset jättävät tilinpäätöksen julkaisematta, eikä tietoja kaikkien toimijoiden osalta ole tässäkään tapauksessa käytettävissä. Yrityksistä vain viisi on rekisteröitynyt työantajarekisteriin, jolloin muiden kohdalla kyse on todennäköisesti yksityisestä elinkeinonharjoittajasta. Neljä yrityksistä, jotka ovat työnantajarekisterissä taas menevät mikroyritys -luokkaan vuosiliikevaihdon jäädessä alle 2 miljoonaan euroon ja henkilöstömäärän jäädessä alle 10:een (Tilastokeskus 2021). Voidaan siis todeta, että etsivätoimintaa harjoittavat yritykset Suomessa ovat pääsääntöisesti pieniä toimijoita yksittäisistä elinkeinonharjoittajista noin 10 henkilöä työllistäviin yrityksiin alle miljoonan liikevaihtoluokassa.

4.2 Yksityisetsivät kansainvälisesti

Edellisen luvun tulokset suomalaisista toimijoista vastaavat kansainvälistä vertailua, jonka mukaan yksittäisen yrityksen koko on keskimäärin 2,5 tutkijaa per yritys. Pieni yrityskoko mahdollistaa erikoistumisen, joustavan työskentelyn asiakkaiden kanssa ja työvoimaan liittyvien hallinnollisten kustannusten välttämisen. Toimialalle tyypillistä on alihankinta ja alihankintaverkostojen käyttö taas mahdollistaa maantieteellisen kattavuuden. (Prenzler 2006, 425).

Suomessa tehdyssä kansainvälisessä vertailussa Heinämäki tukeutui CoESS:in (Confederation of European Security Services) raportteihin, joissa rikoksen paljastamista ei ole eritelty säännönmukaisesti (2009, 77-93). Samoin Hautamäki nojaa turvallisuusalan valvontaa koskevassa väitöskirjassaan alan kansainvälisessä vertailussa CoESS:in raportteihin (2016, 9-10). Niiden ongelmana on tosin, että CoESS on suurimmaksi osaksi ammattiliittojen tai turvallisuusalan järjestöjen muodostama liitto (CoESS 2021, Members). Esimerkiksi Suomea

CoESS:issa edustava Palvelualojen työnantajat ei ole valvontaviranomainen, eikä erityisesti yksityisetsivätoimintaan keskittynyt asiantuntijaorganisaatio. Siksi sen julkaisutkin ovat hyvin yleistasoisia turvallisuusalan suhdannekuvauksia, eivätkä ole siten mitenkään hyödynnettävissä esimerkiksi tämän tutkimuksen tarpeisiin yksityisetsivätoiminnasta (Palta 2021, Tutkimukset ja julkaisut).

CoESS:in viimeisin Facts & Figures -raportti, jossa on käyty laajemmin läpi Euroopan maat, on vuodelta 2013. Tämän raportin perusteella Euroopan alueella on 11 maata, joissa yksityissektorilla on sellaisia oikeuksia, jotka yleensä kuuluvat poliisille (CoESS 2013, 246). Vain Suomen kohdalla on mainittu yksityisetsivätoiminta (termit ”investigation” tai ”detective”), tosin esimerkiksi Norjan ja Espanjan kohdalla jää yhteenvedosta epäselväksi, mitä ovat ”erityiset palvelut” tai ”poliisitoiminnan avustaminen” (CoESS 2013, 247). Raporttia tarkemmin luettuna maakohtaisesti, löytyy mainintoja yksityisten suorittamasta tutkinnasta enemmänkin. Koko koonti on esitelty tarkemmin liitteessä 1 olevassa taulukossa. Alla taulukossa 3 kuitenkin muutama pääkohta havainnoista koskien kaikkia raportissa mukana ollutta 34 maata. (CoESS 2013).

Yksityisetsivätoiminta mainittu turvallisuusalan yritysten palveluina	Itävalta, Serbia, Slovenia, Sveitsi (4 kpl)
Yksityisetsivätoiminnan luvanvaraisuus (poiketen yleisestä turvallisuusalan luvanvaraisuudesta)	Itävalta, Serbia, Slovenia (3 kpl)
Yksityisetsivätoiminta sisältyy turvallisuusalan koulutukseen	Belgia, Kroatia, Serbia, Espanja, Alankomaat (5 kpl)
Erityinen laki yksityisetsivätoiminnasta	Latvia, Slovenia (2 kpl)

Taulukko 3: Yksityisetsivätoiminta Euroopassa (CoESS 2013)

Suomessa yksityisetsivätoiminta ei ole erikseen luvanvaraista, eikä sitä ole raportissa erikseen Suomen kohdalla eritelty (CoESS 2013, 69-76). On todennäköistä, että monissa muissakin maissa on vastaava tilanne, eikä tämän raportin perusteella voi tehdä luotettavia arvioita nimenomaan yksityisetsivätoiminnasta tai rikoksen paljastamiseen johtavasta tutkinnasta ja sitä harjoittavista yrityksistä Euroopassa. Raportin pääasiallinen tarkoitus on tarjota tietoa yksityisten turvallisuuspalveluiden tarjonnasta ja markkinan koosta sekä ylipäätään turvallisuusalan liiketoimintaa harjoittavien yritysten määristä ja sopimusten lukumääristä (CoESS 2013, 4). Voi siis olla, että yksityisetsivätoiminta ei ole tästä näkökulmasta kiinnostavan kokoinen markkina ja huomio on siksikin jäänyt vähemmälle. Joka tapauksessa

raportista voi vetää sen johtopäätöksen, että yksityisetsivätoimintaa turvallisuusalalla kuitenkin harjoitetaan.

Muita virallisia tilastoja on saatavilla aika huonosti. Yksi tapa saada jonkinlainen kuva siitä, millaista toiminta on kansainvälisesti ja missä maissa sitä harjoitetaan, on seurata esimerkiksi yhdistysten muodostamia järjestöjä. Suomen Yksityisetsivä- ja Lakitoimistoliitto on jäsen kansainvälisessä yksityisetsivien yhdistysten liitossa, IKD:ssa (Internationale Kommission der Detektiv-Verbände). Sillä on tällä hetkellä 14 yhdistystä jäsenenä ja yhdistykset raportoivat toiminnastaan liitolle vuosittain. Nämä raportit ovat julkisia ja niiden perusteella voidaan tehdä jotain johtopäätöksiä eurooppalaisesta yksityisetsivätoiminnasta (IKD 2021, Delegate's reports). Alla olevaan taulukkoon 4 on koottu jäsenyhdistysten vuonna 2019 toimittamat tiedot liitolle.

Järjestö	Jäsenmäärä	Toimintalupa	Valvontaviranomainen	Luvan valvoja
European Academy for Private Investigators	19	Kyllä	Federal Ministry of Economics and Labour	Austrian Federal Economic Chamber
Österreichischer Detektiv-Verband	95	Kyllä	Federal Ministry of Economics and Labour	Austrian Federal Economic Chamber
Federazzione Italiana Instituti Investigazioni Informazioni Sicurezza	950	Kyllä	Ministry of Interior through the Provincial Prefect	Department of Public Security
Suomen Yksityisetsivä- ja Lakitoimistoliitto ry	20	Kyllä ja ei	The Police Board of Finland	The Police Board of Finland
Syndicat National des Agents de Recherches Privées	195	Kyllä	Government control body under jurisdiction of the Ministry of Homeland security	CNAPS (Conseil National des Activités de Sécurité Privées)
Bund internationaler Detektive	150 kansallista 60 ulkomaista	Ei	N/A	N/A
Der Bundesverband deutscher Detektive	90 (vuoden 2018 ilmoitus)	Ei	N/A	N/A
Magyar Detektív Szövetség	35	Kyllä	Hung Law CXXXIII of 2005	Police
NorskForening for EtterforskningogSikkerhet	47	Ei	N/A	N/A
Patronatul Detectivilor din România	36 (vain yrityksiä)	Kyllä	Ministry of Internal Affairs / General Inspectorate of Romanian Police	Ministry of Internal Affairs / General Inspectorate of Romanian Police
Detektivske zbornice Republike Slovenije	87 hlö 23 yritystä	Kyllä	Ministry of Interior	The Detective Chamber of the Republic of Slovenia
Asociación Profesional de Detectives Privados de España	350	Kyllä	Ministry of Interior	Unidad Central de seguridad Privada (a specific Police unit)
Özel Dedektifler Derneği	43	Ei	N/A	N/A

Association of British Investigators	450+	Ei	N/A	N/A
International Association of Investigators and Anti-Crisis Experts	50+	N/A	N/A	N/A

Taulukko 4: IKD jäsenyhdistysten raportoimat tiedot vuonna 2019 (IKD 2021, Delegate's reports)

Eri valvontaviranomaisten ja ministeriöiden nimiä ei ole suomennettu, koska vastaavat suomenkieliset termit eivät ole sellaisenaan täysin yhteneviä ja vertailukelpoisia. Osalla suomenkilisistä vastineista voi olla jopa erilainen merkitys Suomessa. Nimet ovat kyseisen maan delegaattien itsensä raporteilla ilmoittamia.

Toimiluvat eivät vaikuta olevan mitenkään yhdenmukaisia Euroopassa. Toimilupia sääntelevät kansalliset viranomaiset ja siksi niiden osalta on vaihtelua yhtä paljon kuin on lainsäätäjiä. Esimerkiksi Sloveniassa ei vaadita toimilupaa, mutta laki oikeuttaa silti yksityisetsivän suorittamaan tiettyjä laissa nimettyjä tehtäviä. Näitä ovat esimerkiksi tietojen keruu velallisten omaisuuden jäljittämisessä, todisteiden keräämisessä oikeustapauksissa asiakkaille, liiketoiminnasta ja yrityksistä, rikoksiin ja epäiltyihin yksityiskanteissa ja työsuhteeseen liittyviin petoksiin kuten perättömät sairaslomat tai matkalaskut tai huumausainerikkeet työpaikoilla. (Private detective services act 2011, artikla 26).

Eri maiden lainsäädäntöjen kehitys on myös ollut erilaista: esimerkiksi Itävallassa aiemmin sääntelemätön yksityisetsivätoiminta ja sen harjoittamisen yhteydessä tapahtuneet laittomuudet alkoivat olla rasite alan toimijoille. Sen sijaan, että aloite olisi tullut lainsäätäjältä, alkoivat toimijat itse järjestäytyä ja määritellä alan standardeja ja koulutusvaatimuksia. Sen jälkeen yhdistyksenä avattiin neuvotteluyhteys lainsäätäjään ja pyydettiin yhdistyksen suunnittelemien standardien vahvistamista elinkeinon harjoittamisesta yleisesti. Asia eteni laiksi asti ja elinkeinoelämän aloitteen vuoksi Itävallassa valvovana viranomaisena on yhä edelleen talous- ja työministeriö toisin kuin monessa muussa maassa. (ÖDV-luottamushenkilön haastattelu 2021).

Euroopassa palveludirektiivin tarkoitus on edistää palvelujen vapaata liikkuvuutta. Yksityiset turvallisuuspalvelut eivät kuulu kuitenkaan sen piiriin. (Palveludirektiivi 2006/123/EY, artiklat 1 ja 2). Tämä yhdessä aiempien syiden kanssa on todennäköisesi vaikuttanut siihen, miksi kansainvälisiä yhtiötä on työlästä perustaa ja ovat ehkä siksikin harvassa. Hallinnollinen taakka on melko suuri, kun joka maassa on omat lupaprosessinsa, vaatimuksensa toimiluville ja koulutukselle ja usein vieläpä työtä suorittavalle henkilötasolle asti. Lisäksi lainsäädäntö ja siihen liittyvä toimintakulttuuri olisi hallittava. On ehkä helpompaa ottaa yhteys kohdemaan luvanhaltijaan ja ostaa työ alihankintana.

IKD ei kuitenkaan kerää tarkempaa tietoa itse jäsenistään tai julkaise sitä. Osallistuin 2021 syyskuussa Suomen edustajana IKD:n vuosikokoukseen ja pääsin tapaamaan yhdistysten virallisia kansainvälisiä virallisia delegaatteja ja muita edustajia. Useimmat heistä olivat joko pienistä yrityksistä tai jopa yksityisyrittäjiä. Monissa keskusteluissa vahvistui toimialan verkostomainen työtapa ja erikoistumisen merkitys ja etenkin rajat ylittävissä tapauksissa yhteistyö ja alihankinta pienten toimijoiden välillä. Huomattavaa on myös se, että monissa yhdistyksissä on vain henkilöjäseniä. Paremman kuvan saamiseksi toimijoiden kokoluokasta, pitäisi perehtyä edellä olevien yhdistysten jäsenrekistereihin ja yritysten tietoihin tarkemmin. Mikään ei kuitenkaan viittaa siihen, että kansainvälisten toimijoiden osalta kokoluokassa olisi merkittävää poikkeamaa Suomeen nähden. Ja koska toimijoiden tilastointi ei ole tutkimuksen tarkoitus, ei tähän käytetä tässä työssä enempää resursseja.

4.3 Toimeksiannot kirjallisuuden perusteella

Henkilötietojen käsittelyn osalta toimijoiden kuvaamisen lisäksi tärkeää on itse toiminnan ymmärtäminen. Toiminnan kautta nousevat esiin varsinaiset konkreettiset henkilötietojen käsittelytoimet. Esimerkiksi mitä henkilötietoja käsitellään, mihin tarkoituksiin ja millaisilla tavoilla. Jo toistakymmentä vuotta julkaistu ja monien lähteenä käyttämä Pricewaterhouse Coopersin raportti (PwC’s Global Economic Crime and Fraud Survey) listasi viime vuonna kyberrikollisuuden toiseksi suurimmaksi uhaksi yrityksille (PwC 2020, 4). Kuitenkin vuoden 2018 raportista selviää, että kyberrikollisuudessa vain neljänneksessä on kyse tietoverkkokatkoista tai toiminnan lamauttamisesta, kun kyseinen luokka sisältää yhtä lailla kiristyksiä, varojen väärinkäyttöä tai aineettomiin oikeuksiin kohdistuvia loukkauksia (PwC 2018, 12). Koska kaikessa tänä päivänä käytetään apuna tietotekniikkaa, niin myös rikollisuudessa. Myös Poliisin selvityshankkeessa todettiin, että tietotekniikkaa hyödyntävässä rikollisuudessa voi olla kyse melkein mistä tahansa rikollisuuden lajista (Kurenmaa 2018, 28). Tietoverkkorikollisuuskaan ei näytä siten muodostavan mitään kovin erikoista ryhmää, vaan sähköinen tiedonkäsittely on myös otettava huomioon.

Yksityisetsivätoimintaa maailmalla tutkinut Prenzler kategorisoi yksityisetsivätoiminnan neljään eri tyyppiin sen mukaan, millaisia palveluita he tarjoavat (2006, 427–428):

1. Petosrikollisuuden vastainen toiminta (”Anti-fraud work”)
2. Lainopillinen työ (”Legal work”)
3. Yritystoimeksiannot (”Commercial enquiry”)
4. Yksityiset ja kotitalouksien toimeksiannot (”Domestic investigations or personal work”)

Termeillä ei ole Suomessa vakiintuneita vastineita, kahdessa ensimmäisessä olen käyttänyt Kerttulan (2010, 128) käyttämiä termejä ja kaksi viimeistä luokkaa olen muotoiltu osin niiden sisältöjen ja omien kokemusten kautta. Vaikka kaikki kyseiset luokat eivät välttämättä sisällä

rikosten paljastamista tai tutkimista, käytän toimeksianto -sanaa yhdenmukaisesti kuvaamaan tehtäviä. Samalla termillä siis kuin miten laki yksityisistä turvallisuuspalveluista sopimussuhteeseen liittyvästä työstä puhuu.

Petosrikollisuuden vastaisessa toiminnassa on kyse yleensä vakuutustoimintaan liittyvän rikollisuuden paljastamisesta, mutta kyse voi olla hyvin myös sosiaalietuuksien tai -tukien väärinkäytön paljastamista. Lähtökohtaisesti taustalla on tilanne, jossa haetaan yleensä vakuutusyhtiöltä tai sosiaalietuuksien myöntäjältä korvauksia terveydentilaan liittyvän heikkenemisen johdosta valheellisin perustein (muiden muassa tilapäinen tai pysyvä työkyvyttömyys). (Prenzler 2006, 427).

Menetelmät: Etuuden hakijan seurantaa ja tarkkailua, jonka avulla pyritään hankkimaan todisteita valheellisin perustein saadusta etuudesta, haastattelut, videovalvonta, terveystietojen käsittely. (Prenzler 2006, 427; Prenzler & King 2002, 3).

Lainopillinen työ on usein taustatyötä, joka liittyy yksityisoikeudellisiin vaateisiin tai kanteisiin. Se voi sisältää todisteiden hankkimista asianajajille, kuten dokumenttien tai tapahtumakuvausten hankintaa. Usein työmuotona on haastattelut ja todistajien kuuleminen, mutta voi sisältää myös henkilöiden paikantamista, tarkkailua tai valvontaa, kun haetaan esimerkiksi henkilön sijaintia tai todisteita maksukyvystä tai toimitetaan haasteita tai oikeudellisia vaateita. (Prenzler 2006, 427).

Menetelmät: Haastattelut, todisteiden ja näytön hankinta dokumentaatiota ja lausuntoja keräämällä, tarkkailu, valvonta, henkilöiden jäljitys (Prenzler 2006, 427).

Yritystoimeksiantoja kuvaa ensisijaisesti se, että kyseessä on jonkin yrityksen tekemä toimeksianto, joka voi olla mitä tahansa kyseisen oikeushenkilön intresseihin liittyvää selvitystyötä tai tiedonhankintaa. Kyseessä voi olla vastuuselvitykset liiketoimintaan liittyen, työntekijöiden ja sopimuskumppanien taustatarkistukset, työpaikalla tapahtuvan häirinnän selvittäminen, tekijänoikeuksiin liittyvät selvitykset ja jopa saatavien perintä. Tähän luokkaan kuuluvat myös yrityksille tehtävä tilintarkastustoiminta tai tietotekninen forensiikka, mutta yhtä lailla erilaiset riskiarviot ja turvallisuustason arviointi. Etenkin yrityskauppojen yhteydessä käytetyt Due diligence -tarkistukset, joissa selvitetään toisen osapuolten tietyn vaatimustenmukaisuuskehyksen (esimerkiksi toiminnan lainmukaisuuden tai turvallisuustason) vaatimusten täyttymistä, kuuluvat tähän luokkaan. (Prenzler 2006, 427).

Menetelmät: tietojen ja dokumentaation hankinta ja/tai sellaisten oikeellisuuden tarkistus kohdehenkilöstä tai yrityksestä. Elektroninen ja tietotekninen tiedonhankinta, haastattelut, rikostekninen kirjanpito, omaisuus- ja tulotietojen hankinta, motiivien selvitys, rikostaustojen selvitys, peitetyöskentely tai soluttautuminen. (Prenzler 2006, 427–428).

Yksityiset ja kotitalouksien toimeksiannot koostuvat nimensä mukaisesti yksityishenkilöiden tai kotitalouksen teettämistä toimeksiannoista. Näissä on usein uskottomuusepäilyjä, mutta taustalla voi olla myös huoli lapsen tai teini-ikäisen huumeidenkäytöstä, karkaamisesta tai kadonneiden sukulaisten etsimisestä tai vainorikollisuuden selvittämisestä. Edellisissä kyse on lähes aina henkilöiden etsinnästä tai seurannasta, mutta esimerkiksi elatusvelvollisuuteen liittyvien riitojen selvittämisessä kyse voi olla tulotasoon liittyvien todisteiden hankinnasta. (Prenzler 2006, 427–428; Prenzler & King 2002, 4).

Menetelmät: Henkilöiden jäljitys, tulotietojen hankinta, valokuvaus (Prenzler 2006, 427-428; Prenzler & King 2002, 3).

Edellä oleviin kategorioihin sopii heikosti viranomaisen tekemät pyynnöt. Prenzlerin ja Kingin haastattelututkimuksen mukaan Australiassa poliisi on ohjannut Asiakkaita suoraan yksityisetsiville olematta itse osapuolena mitenkään toiminnassa (2002, 4). Silloin toimeksianto luokiteltaisiin yksityisten toimeksiantoihin poliisin ollessa vain ohjaavana toimijana palveluiden äärelle. Suomessa tällaisia pyyntöjä ja yhteistyötä on ollut sekä viranomaisen ohjaamana, että suoraan viranomaisen hankkimana palveluna (esimerkiksi vastaavan hoitajan haastattelu 2021). Kategoriat vaikuttavat kuitenkin toimijoiden kuvaamiseen riittävältä, henkilötietojen käsittelyn näkökulmasta tärkeämpää on menetelmien kuvaaminen.

Käytännön menetelmien ja taitojen perusteella tekijät jakautuvat Prenzlerin ja Kingin mukaan (2002, 3) henkilöiden tarkkailua ja valvontaa tekeviin ja muuhun tiedusteluun, jossa tietoja ei hankita välttämättä suoraan henkilöitä seuraamalla. Itse tutkinta prosessina voidaan jakaa myös muilla tavoilla, esimerkiksi konstruktiiviseen ja rekonstruktiiviseen tapaan riippuen siitä, onko kyse meneillään olevan tapauksen selvityksestä tai aiemman tapahtuman selvityksestä, jota toisinnetaan (Sennewald & Tsukayama 2015, 17). Tämän työn tarkoituksena ei ole kuitenkaan keskittyä erilaisiin tutkintaprosesseihin, vaan pyrkiä tunnistamaan henkilötietojen käsittelyyn liittyviä tilanteita. Oli kyse meneillään olevan tapauksen selvityksestä tai sellaisen toisintamisesta, voidaan molemmissa tavoissa käyttää henkilöihin liittyviä tietoja.

Todisteiden ja näytön hankinta, muu tietojen hankinta sekä henkilöiden jäljitys ovat menetelminä sellaisia, että ne voivat sisältää useita eri tietolähteitä. Pääasiallisesti lähteet ovat julkisia; puhelinluettelot, kiinteistötietokannat, vaaliluettelot, luottotietojen tarjoajat, kaupparekisteritiedot tai mitkä tahansa pääasiassa julkiset tietolähteet (Prenzler 2006, 428; Prenzler & King 2012, 5). Sinällään menetelmä ei määrittele sitä, mistä tietoja milloinkin haetaan, vaikka toiset voivat olla henkilöiden jäljitykseen sopivampia kuin esimerkiksi varallisuuteen tai luotettavuuteen liittyvät selvitykset. Käytetyt menetelmät eivät vaikuta

suoraan liittyvän myöskään toimeksiannon luonteeseen tai toimeksisaajaan, sillä samoja menetelmiä voidaan käyttää erilaisissa toimeksiannoissa.

Sennewald ja Tsukayma yksinkertaistavat tutkinnassa olevan aina menetelmien tasolla kysymys viestinnästä ja tarkkailusta ja näiden yhdistelmästä. Viestinnän avulla hankitaan tietoja ihmisiltä haastatteluin ja kuulusteluin ja muussa vuorovaikutuksessa. Tarkkailulla hankitaan näyttöä tapahtumista joko seuraamalla tilanteita ja tapahtumia, tallentamalla niitä, analysoimalla valokuvia ja videoita, mutta yhtä lailla internetistä, DNA-analyysein ja tietoteknisen forensiikan avulla. Kaikki tiedonhankinta, joka ei tapahdu vuorovaikutuksessa ihmisten kesken menee siis tarkkailun alle. (Sennewald & Tsukayama 2015, 17-18)

Työvälineinä mainitaan tallentimet, kamerat, tarkoitusta varten valmistetut ajoneuvot, ja radiot sekä menetelminä soluttautuminen ja liikkuva tai paikallaan oleva tarkkailu tai niiden yhdistelmä (Sennewald & Tsukayama 2015, 49, 54 ja 66). Tietolähteinä mainitaan aiemmat työnantajat, koulut, luottotietorekisterit, lääkärit, vuokranantajat ja jopa naapurien antamat lausunnot (Sennewald & Tsukayama 2015, 85-86). Myös oikeudenkäyntihistoria, konkurssirekisterit, huumausainetestit, yritysten ylläpitämät rekisterit ja paikallisten viranomaisten rekisterit tunnistetaan tietolähteinä (Sennewald & Tsukayama 2015, 91, 239, 242, 245 ja 246). He eivät kuitenkaan liitä mitään tietolähdettä erityisesti tietyn tyyppisiin menetelmiin tai toimeksiantoihin, vaan niissä korostuu enemmän tarkoituksenmukaisuus tavoitteen näkökulmasta. Toimeksiantajastakaan ei voi aina päätellä käytettäviä menetelmiä, esimerkiksi yksityishenkilön toimiessa esimerkiksi yrityksen edun nimissä.

4.4 Toimeksiannot käytännössä

Prenzlerin luokittelu antaa hyvän kuvan erityyppisistä toimeksiannoista, mutta miten hyvin nämä sitten vastaavat todellisuutta, miten toimeksiantojen lukumäärät painottuvat käytännössä, ja mitä itse toimeksiannot ovat onkin oma kysymyksensä. Ja tähän liittyviä tutkimuksia tai tilastoja ei tältä vuosikymmeneltä löytynyt. Paras käytettävissä oleva tietolähde tähän oli kansainvälisen World Association of Detectives -järjestön toimeksiantojen välityslista, johon minulla on pääsy jäsenyyteni kautta. Toimeksiantojen selvittämiseksi analysoitiin W.A.D.:in jäsenten toimeksiantojen välityslistalla välitetyt yksityisetsivien toimeksiannot (470 kpl) puolen vuoden ajalta (1.1.2021 – 30.6.2021). Luvan materiaalin käyttöön sain yhdistyksen toiminnanjohtajalta sillä edellytyksellä, että tulokset anonymisoidaan huolellisesti ja arvioisin sen sisältöä tarkemmin myös järjestölle itselleen. Tästä syystä aineisto ja sen terminologia on englannin kielellä.

Kyseisen listan tarkoitus on palvella jäsenistöä siten, että maiden rajat ylittävissä tapauksissa jäsenillä olisi mahdollisuus verkoston avulla saada asiakastoimeksiantoja suoritettua. Lista palvelee myös erityisasiantuntemuksen etsimisessä tai vaikka vaan lisätyövoiman saamisessa, vaikka tapaus ei sinällään vaatisi rajat ylittävää toimintaa. Listalle pääsee vain erityisen

valiokunnan hyväksymät jäsenet, jotka joutuvat toimittamaan jäsenyyshakemuksen yhteydessä henkilötietonsa ja kussakin maassa kansalliseen luvanvaraisuuteen liittyvät lupa-asiakirjat sekä toimintaan liittyvän vakuutustodistuksen. Hakija joutuu myös allekirjoittamaan lupa-asiakirjan taustojensa selvittämiseksi kohdemaassa. Jokaisella hakijalla tulee olla myös suosittelija yhdistyksen sisältä, jos haluaa suoraan jäseneksi ilman kolmen vuoden koeaikaa. Jäsenhakemukset myös julkaistaan listalla, jolloin kenellä tahansa jäsenellä on mahdollisuus vaikuttaa jäsenyyshakemukseen (W.A.D. 2021a).

Jäsenyysprosessin osalta voidaan olla melko varmoja, että kyse on ammattimaisesti toimivista henkilöistä tai yrityksistä. Jäseniä yhdistyksessä oli 8.10.2021 924 henkilöä, joista suomalaisia kuusi (W.A.D. 2021b). Kaikki välitetyt toimeksiannot ovat näiden ammattilaisten välittämiä. Siten taustalla on tilanne, jossa asiakas on jo kontaktoinut etsivää ja ensimmäinen arvio siitä, voidaanko toimeksiantoa edes suorittaa, on jo tehty. Toimeksiantoja välitetään myös listan ohi suoraan omille verkostoille tai W.A.D.:in verkkosivuilla olevan ”Find an Investigator” -työkalun avulla, jossa myös asiakkailla on mahdollisuus kontaktoida etsiviä suoraan (W.A.D. 2021b). Nämä toimeksiannot eivät luonnollisesti ole käytettävissä ja suoraan yhtiölleni tulleet pyynnöt on jätetty vertailukelpoisuuden vuoksi pois analyysistä. Pois on jätetty myös listalla välitetyt:

- Mainokset
- Ohjeet palvelun käytölle
- Varoitukset roskapostista, huijauksista, valelaskuista, ym.
- Ohjeiden tai opastukseen pyytäminen tai koulutukseen liittyvät pyynnöt tai tarjoukset
- Uusien jäsenten tiedottaminen ja taustatarkistukset
- Työpaikkatarjoukset

Viestin on täytynyt muodostaa todellinen mahdollisuus sopimuksen tekemiseen ja sitä kautta toimeksiantoon, että se on otettu huomioon.

Toimeksiantojen analyysistä on luonnollisesti jätetty pois kaikki henkilöihin ja yrityksiin liittyvät tiedot. Jos pyyntö on koskenut useita henkilöitä, mutta liittyy samaan tapaukseen, niin ne on käsitelty yhtenä toimeksiantona (esimerkiksi "kolmen sijoittajan taustan selvitys" n muodostanut yhden toimeksiannon). Jos pyynnössä on ollut jonkin asian suorittaminen useassa maassa, on siitä generoitu maakohtaisesti omat toimeksiannot. Syynä on se, että lähes aina joka maasta tarvitaan oma toimeksiantaja suorittamaan tehtävän kansallisten lakien ollessa erilaisia. Maakohtaisuus näkyi usein myös siten, että toimeksiannon viestissä saattoi olla kysymys ”Onko tämän selvittäminen laillista [maassa]?”. Usein toimeksiantaja halusi myös tarjoukset jokaisen maan osalta erikseen, mikä viittaa siihen, että niiden oli tarkoitus ollakin erillisiä toimeksiantoja. Eri maihin kohdistuvassa toiminnassa yhden pyynnön perusteella voi siis generoitua kolme erillistä toimeksiantoa tilastoon.

Jos pyynnössä oli erillisiä toisistaan eroteltuja toimeksiantoja, joille halutaan esimerkiksi eri hinnoittelu, myös nämä on laskettu erillisiksi toimeksiannoiksi. Pääsääntöisesti yksi välitetty viesti kuitenkin sisälsi yhden toimeksiannon ja jos toimeksiannon saatteessa olikin mainittu, että henkilön onnistunut jäljitys voi laukaista tarpeen valvontatehtävälle, vain ensimmäinen laskettiin toimeksiannoksi. Johtuen siitä, että toisen toimeksiannon käynnistymiselle oli ehtona ensimmäisen onnistuminen, eikä siitä ollut vielä takeita.

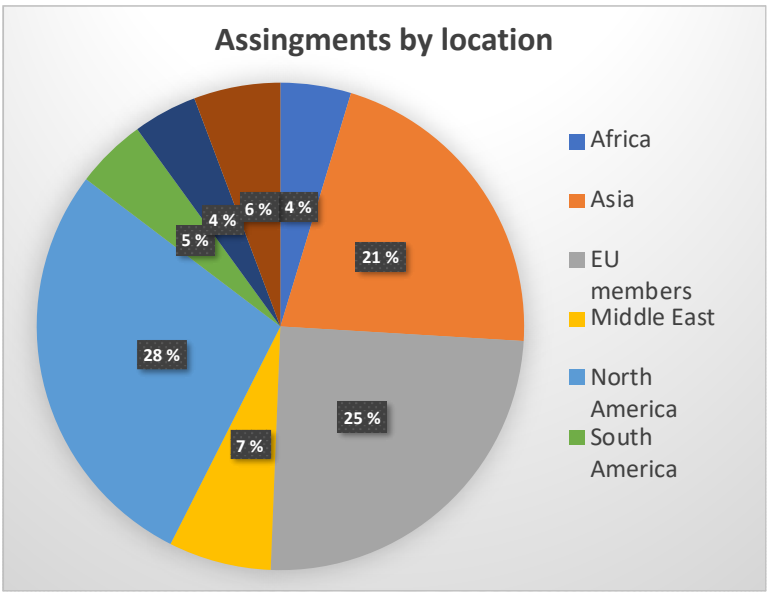
Toimeksiannoista kirjattiin ylös seuraavat asiat:

1. ID – tietojen yhdistämisen vuoksi generoitu satunnaisluku
2. Date – Toimeksiannon julkaisun päivämäärä
3. Assignment – toimeksiannon tyyppi siten, kuin se on kuvattu toimeksiannolla
4. Category – Prenzlerin kategoria
5. Client – Toimeksiantaja (yksityinen / yritys / ei tiedossa)
6. Country – Maa, jossa toimeksianto tulee suorittaa.
7. Target – kohde, johon toimeksianto kohdistuu (yksityinen / yritys / ei tiedossa)
8. Details – Toimeksiantoon liittyvä tarkempi kuvaus

Aineisto on liitteessä 2. Toimeksiantajan maata ei ole kirjattu, koska se puuttui lähes aina välitysilmoituksesta. Lisäksi tämän työn yhteydessä julkaistusta aineistosta on jouduttu jättämään pois tietoja sen vuoksi, ettei mahdollisten kohteiden, toimeksiantajien tai toimeksisaajien yksityisyys tai turvallisuus vaarantuisi. Siitä on jätetty pois kokonaan kohdat kaksi (päivämäärä) ja kahdeksan (yksityiskohdat), koska niiden avulla ulkopuolisen on mahdollisuus yhdistää toimeksianto tosielämässä tapahtuneeseen tutkintaan ja henkilöihin. Sen lisäksi maat, joihin on kohdistunut alle viisi (1-4) toimeksiantoa, on korvattu julkisessa aineistossa pelkällä maata vastaavalla numerolla. Kaikki yllä olevat tiedot ovat kuitenkin olleet saatavilla tilastoja luodessa, joten ne ovat oikeissa paikoissa tilastoinneissa ja analyyseissä. Jos jokin asia ei ole tiedossa (kuten client tai target), tai se ei ole ollut merkityksellinen toimeksiannon kannalta (maa), se on aineistossa merkinnällä na (not available/not applicable). Satunnaisluku, joka yksittäiselle toimeksiannolle on luotu, on tehty siksi, että mahdolliset virheet ovat tarkastettavissa sen avulla myöhemmin niiden avulla alkuperäisestä julkaisemattomasta aineistosta. Aineisto on järjestetty satunnaislukujen luonnin jälkeen tällä perusteella, joten ne eivät noudata mitään logiikkaa päivämäärien tai maiden tai minkään muunkaan tekijän osalta. Satunnaisluku on luotu Mersenne Twister -algoritmilla, joka on vahva satunnaislukualgoritmi (ScienceDirect 2021, Mersenne Twister).

Maailmanlaajuisesti toimeksiannot sijoittuvat ympäri maailman. Tässä yhteydessä maaksi on laskettu myös emämaiden merien takana sijaitsevat itsehallintoalueet, mutta yhtenäisten alueiden itsehallintoalueita ei ole eroteltu toisistaan (esimerkiksi Ahvenanmaa on laskettu Suomen alle alueen läheisyyden vuoksi, mutta Ranskan Guayana on laskettu omaksi maaksi).

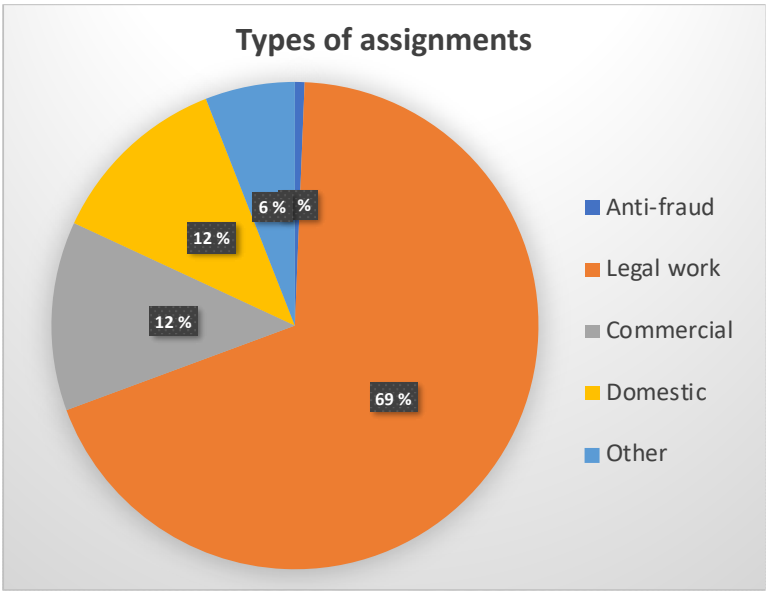
Toimeksiantoja oli tarjolla kaikkiaan 136 maahan. Kuitenkin maita, joihin kohdistui 10 tai useampia toimeksiantoja on vain 20 kappaletta, 14,7 % kaikista maista. Yli 50 maassa on taas välitetty vain yksi toimeksianto alkuvuoden aikana, suuressa osassa lukumäärän jäädessä alle viiteen. Alla kuviossa 2 on kuvattu toimeksiantojen sijoittuminen maanosien suhteen:



Kuvio 2: Toimeksiantojen jakautuminen alueittain

Kuvion 2 International -kategoria muodostuu niistä toimeksiannoista, joiden osalta toimeksiannon suorittamisen sijainnilla ei ollut väliä (country -kentässä na). Näitä olivat internetissä tapahtuvat selvitykset tai erilaiset asiantuntija- ja tiedonhankintatehtävät, joissa aineistoa voitiin käsitellä sähköisesti välimatkoista riippumatta. Other -kategoria taas sisältää esimerkiksi Euroopassa sijaitsevat maat, jotka eivät ole EU-jäseniä ja Australian. EU jäsenmaat eroteltu muusta Euroopasta siksi, että EU-jäsenmaat ovat todennäköisesti lähimpänä toisiaan lainsäädännöllisesti Euroopan unionin perustamisesta ja toiminnasta tehtyjen sopimusten vuoksi. Siksi EU-jäsenissä ovat mukana myös ETA-maat. Toimeksiantoja vaikuttaa olevan kaikkiin maanosiin melko tasaisesti, vaikka Yhdysvaltojen ja EU-jäsenmaiden merkitys näkyy – yhdessä ne muodostavat 41,5 % kaikista toimeksiannoista. Eurooppalainen lainsäädäntö ei siis vaikuta erityisen haitallisesti toimintaan Euroopassa, koska sen osuus on kuitenkin erottuva aineistossa.

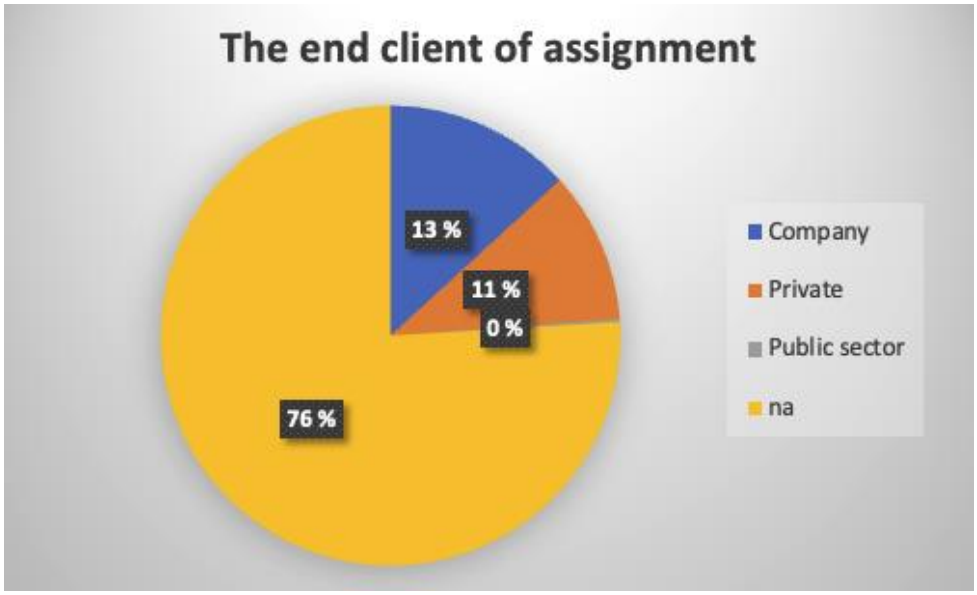
Prenzlerin aiemmin kuvatun tyypityksen mukaan jaoteltuna toimeksiannot jakautuvat kuviossa 3 esitetyn mukaan seuraavasti:



Kuvio 3: Yksityisetsivätoiminnan tyypittely Prenzlerin (2006) mukaan

Petosrikollisuuteen (anti-fraud) liittyvien toimeksiantojen vähyys kuviossa 3 selittynee sillä, että toimeksiannossa ei useinkaan yksilöity, minkä vuoksi palvelua tarvitaan. Osa tehtävistä oli vain valvonta- ja seurantatehtäviä, mutta niiden luokittelu nimenomaan vakuutus- tai hyvinvointipalveluiden petoksiin olisi edellyttänyt toimeksiantajalta selkeämpää kuvausta. Työn suorittamistapa henkilöseurannassa tai -valvonnassa ei välttämättä muutu miksikään, vaikka tekemisen syy muuttuisi, joten ehkä syytä ei nähty siksi tarpeelliseksi ilmoittaa.

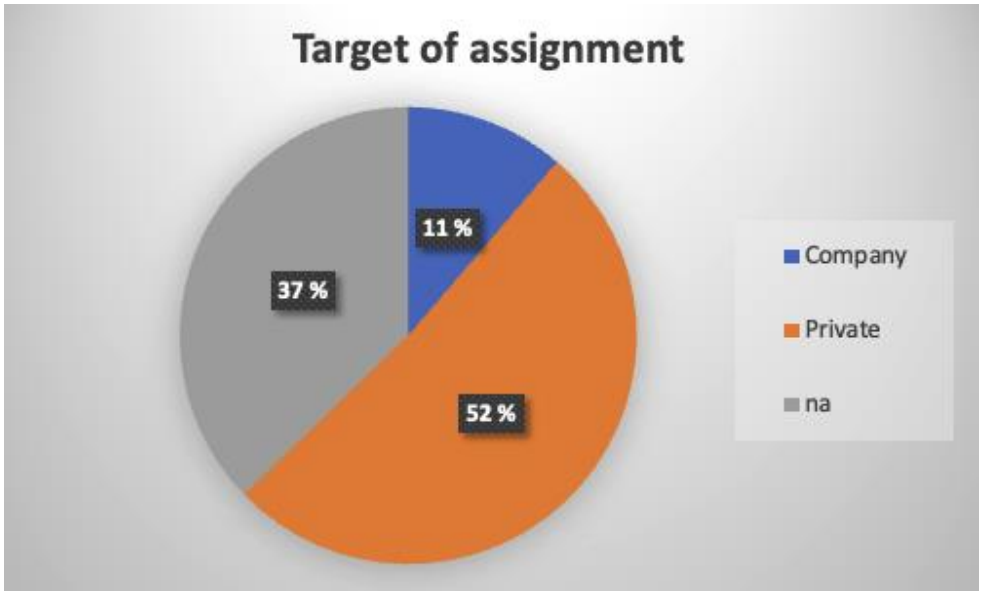
Yritystoimeksiannoksi (commercial) tai yksityiseksi (domestic) tapaus luokiteltiin pelkästään sillä, että toimeksiantaja oli joko yritys tai yksityinen. Jos toimeksiantaja ei ollut tiedossa, yksityisiin on luokiteltu myös sellaiset toimeksiannot, joissa oli kyse esimerkiksi testamentin laatimisesta tai perintöasioista, koska yritykset eivät jätä perintöjä. Legal work muodostaa suurimman osan toimeksiannoista siksi, että toimeksiantajaa ei ollut ilmoitettu suurimmassa osassa tapauksia. Silloin toimeksianto sijoittui usein tuohon tyyppiin, koska sitä ei voinut sijoittaa muualle. Toimeksiantajan puuttuminen tiedoista vaikutti hyvin paljon myös toimeksiannon taustalla vaikuttavien motiivien päättelemisen vaikeuteen. On vaikea sanoa esimerkiksi, miksi joku taustatarkistus halutaan, koska syitä voi olla lukuisia. Joissain taustarkistuksissa mainittiin suoraan syynä olevan työsuhteeseen liittyvä tarkistus, mutta saattoi olla myös maahanmuuttoon liittyvien asiakirjojen pätevyyden varmistamista tai ennen avioliittoa toisen perheen varallisuuden kartoittaminen. Suuressa osassa toimeksiannoista ei annettu mitään syytä. Lopullinen toimeksiantaja, eli asiakas toimeksiannon taustalla, ilmoitettiin kuvion 4 mukaan seuraavasti:



Kuvio 4: Toimeksiannon taustalla ilmoitettu asiakas

Kuten kuviosta 4 ilmenee, karkeasti vain 15 %:ssa kaikista toimeksiannoista ilmoitettiin taustalla oleva asiakas. Muut sijoittuivat kategoriaan na (”not available”). Julkiselle sektorille voitiin luokitella vain yksi toimeksianto, jossa lainsäädäntönsä puolesta länsimaiseksi miellettävän valtion yliopisto halusi teettää eurooppalaisesta valtiosta selvityksen kaikista sen maan valtio-omisteisista yhtiöistä. Julkista sektoria ei muuten mainittu, mutta seitsemän kappaletta toimeksiannoista ilmoitettiin suoraan liittyvän maahanmuutto- tai viisumiselvityksiin. Sen lisäksi toimeksiannoissa oli paljon tiettyjen asiakirjojen aitoustarkistuksia maissa, joista maahanmuutto Suomessakin on tavallista sekä perheenyhdistämisissä tavanomaisesti käsiteltäviä avioliitto- ja perhesuhdeselvityksiä. Mutta että nämä voitaisiin aukottomasti yhdistää viranomaisiin tai julkiseen sektoriin, vaatisi se lisätutkimuksia.

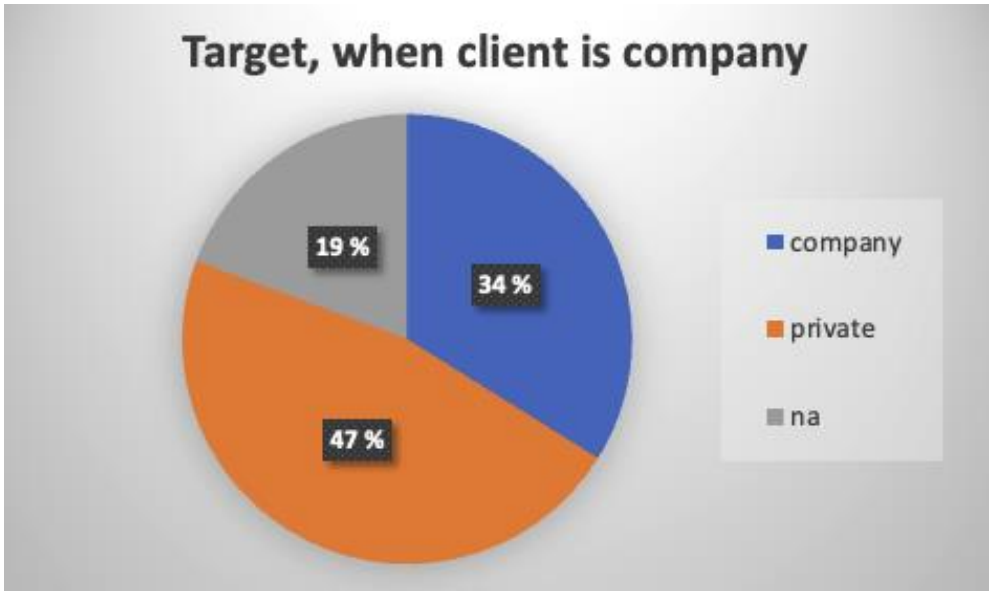
Toinen tapa hahmottaa taustalta yritystoimeksiantojen ja yksityistoimeksiantojen suhdetta, voisi olla tarkastella toimeksiannon kohdetta. Tämä ilmoitettiin melko usein johtuen siitä, että kohteella on paljonkin vaikutusta työn suorittamistapaan. Yksityishenkilöön kohdistuva valvontatehtävä on luonteeltaan erilainen kuin yritykseen tai yksittäiseen tehtaaseen kohdistuva toimeksianto. Kohteet toimeksiannoista ilmoitettiin kuviossa 5 esitetyn mukaan seuraavasti:



Kuvio 5: Toimeksiannon kohde

Yli puolet toimeksiannoista kohdistuu siis yksityishenkilöihin. Jos toimeksiantaja oli yksityishenkilö (70 kpl), 96 %:ia toimeksiannoista (67 kpl) kohdistui yksityishenkilöön. Lopuissa kohdetta ei ollut ilmoitettu. Kaksi tapauksista liittyi kuitenkin internetissä tehtävään tutkintaan identiteettivarkaudesta tai haitallisen tiedon levittämisestä ja yhdessä oli ilmoitettu vaan toimeksiannon olevan ”kotitalouteen liittyvä”. On siis melko todennäköistä, että näidenkin takaa löytyy yksityishenkilö, eikä yritys.

Kun toimeksiantaja oli yritys (yhteensä 62 kpl), oli tapausten kohde ilmoitettu seuraavasti:



Kuvio 6: Toimeksiannon kohde, kun asiakas on yritys

Tapauksista, joissa toimeksiannon kohdetta ei ollut ilmoitettu (12 kpl), oli kaksi sellaista, jotka liittyivät IPR-oikeudenloukkausten tutkimiseen, jolloin kohteena on todennäköisesti toinen yritys ja kahdessa ei ollut ilmoitettu tarkempia tietoja ollenkaan. Loput olivat sellaisia, joissa kohteena voisi olla yhtä hyvin niin yritys kuin yksityishenkilökin. Valvontatehtäviä oli kaksi, kaksi vakuutuspetostutkintaa, yksi asiakirjojen toimittaminen, yksi vuokrasopimuksen rikkomiseen liittyvä tapaus, yksi testamenttiin liittyvä toimeksianto ja yksi toimeksianto lahjoittajien etsimiseen terrorisminvastaisen propagandan levittämiseksi. Yritystenkin toimeksiannoista karkeasti puolet kohdistuu yksityishenkilöihin. Voisi siis yleistää, että on kyse mistä tahansa Prenzlerin (2006) luokituksesta, toimeksiantoihin liittyy aina henkilötietojen käsittelyä ja vähemmistöön jää puhtaasti yritysten väliset asiat.

Yhteenvetona voisi sanoa, että tämän työn havaintojen perusteella yksityishenkilöiden toimeksiannot kohdistuvat pääsääntöisesti yksityishenkilöihin, mutta yritysten toimeksiannot voivat kohdistua yhtä hyvin joko yritykseen tai yksityishenkilöön. Tosin toimeksiantaja oli ilmoitettu hyvin harvoin ja saatetekstit saattoivat olla ristiriidassa edellisen yleistyksen kanssa, joten varmoja päätelmiä ei tästä aineistosta voi tehdä.

4.5 Toimeksiantojen tyypittely

Tyypittelyä tarvitaan työn tavoitteissa mainittujen tyypillisten tapausten tunnistamiseksi. Prenzlerin tyypittely itsessään oli hankala päätelmien muodostamisen näkökulmasta siksi, että jakauma ei juuri kerro toimeksiannoista konkreettisesti tai niissä tapahuvasta henkilötietojen käsittelystä (kuvio 3). Sen vuoksi toimeksiannot tyypiteltiin vielä niiden saatetekstien ja ilmoituksessa annettujen tietojen mukaan. Saatetekstit olivat usein lyhyitä, vain muutamia lauseita ja aina niitä ei ollut ollenkaan. Toimeksiantoja, joissa ei ollut määritelty asiakasta, kohdetta eikä annettu mitään lisätietoja oli 16 % (75 kpl). Siitä huolimatta toimeksiannon tyyppi oli kuvattu vähintäänkin muutamalla sanalla. Lisätiedot luvattiin toimittaa usein vain potentiaalisille suorittajille, eikä jokaisen toimeksiannon osalta olisi niiden suuren määrän vuoksi ollut tämän työn puitteissa mahdollisuutta perehtyä niihin tarkemmin. Näistä toimeksiantojen kuvauksista nousi aineistossa esiin taulukossa 5 esitetyt tyypit:

Assignment category	amount	%
person trace	122	25,96 %
background check	96	20,43 %
information acquisition	59	12,55 %
asset trace	42	8,94 %
investigator trace	36	7,66 %
surveillance	35	7,45 %
lawyer search	14	2,98 %
due diligence	12	2,55 %
bank account	10	2,13 %
company trace	10	2,13 %
credit check	6	1,28 %

insurance investigation	5	1,06 %
IPR protection	5	1,06 %
crime forensics	3	0,64 %
infidelity	3	0,64 %
physical protection	3	0,64 %
trace	3	0,64 %
technical surveillance countermeasures (TSCM)	2	0,43 %
child abduction	1	0,21 %
debt collection	1	0,21 %
repossession of property	1	0,21 %
reputation protection	1	0,21 %

Taulukko 5: Toimeksiantojen tyypit

Kategoriat eivät muodostuneet ihan itsestään yllä olevan kaltaiseksi listaksi, vaan jonkin verran niiden osalta piti tehdä kategorisointeja ja päätelmiä. Seuraavaksi avataan yhdistämisen tapaa.

Taustatarkistuksista (background check) on kyse silloin, jos tarvitaan tietoja laajemmin kohdehenkilöstä tai yrityksestä, esimerkiksi omistajatietoja, tietoja operatiivisesta toiminnasta, maineeseen ja rikoshistoriaan liittyviä selvityksiä tai vaikka syntymätodistuksen validointi tietystä henkilöstä. Taustatarkistuksia oli niin yritysten työllistämistarkoituksissa, mutta myös yksityisillä esimerkiksi romanssihuijausepäilyissä, minkä vuoksi ne olivat Prenzlerin tyypityksessä lainopillisen työn alla, ellei toimeksiantaja ollut tiedossa. Toimeksiantajina ja kohteina oli niin yrityksiä kuin yksityishenkilöitäkin.

Taustatarkistuksiin liittyen Prenzler luokitteli due diligence -vaatimustenmukaisuustarkistukset yritystoimeksiantoihin (Prenzler 2006, 427). Due diligence on vakiintunut termiksi selvityksissä ja tarkistuksissa, joita tehdään yleensä yrityskauppojen yhteydessä, kun halutaan saada selvyys toisen osapuolen liiketoiminnan tilasta (Åstrand 2020). Tämän työn tausta-aineistossa mukana oli myös due diligence -termillä olevia toimeksiantoja, joita haluttiin teettää esimerkiksi suunnitellun sopimussuhteen taustaselvityksenä. Taustatarkistuksista osa ei taas viitannut mitenkään aikomukseen sopimussuhteesta, joten niitä ei voinut sellaisenaan luokitella due diligence -tarkistukseksi, vaikka termi olisi ollut mainittukin toimeksiannossa. Due diligence termiä tunnuttiin käytettävän monessa toimeksiannossa hyvin väljästi viittaamaan ylipäätään erilaisiin taustojen tarkistamisiin. Due diligence -luokkaan on laitettu myös sellaiset toimeksiannot, joissa oli mainittu kyseinen termi, mutta ei tarkennettu asiaa muuten. Yritystoimeksiantoihin ne on sijoitettu aiempana edellisessä luvussa, jos sekä toimeksiantaja, että kohde on yritys, muutoin lainopilliseen työhön, koska kaupallinen intressi ei käynyt ilmi toimeksiannosta muuten.

Eräänlainen taustojen tarkistus on myös luottotarkistus (credit check). Se kuitenkin poikkeaa omaisuuden jäljittämisestä (asset trace) siten, että siinä ei tarvinnut jäljittää omaisuutta tai

omistajuuksia, vaan lausunto luottokelpoisuudesta riitti. Asiakas ei siis halunnut yksilöidysti tietää kohteen omaisuudesta yksityiskohtia. Pankkitilitiedustelut on taas luokiteltu omikseen (bank account), koska niissä oli kyse nimenomaan pankkitilistä ja sen käyttöön tai saldoihin liittyvistä tiedusteluista. Suomalaisena pankkisalaisuuteen tottuneena tuntuu oudolta, että tällaisia tiedusteluja ylipäätään välitetään, mutta niitä oli kuitenkin puolen vuoden aikana 10 kappaletta, joista 4 kohdistui EU-jäsenvaltioon. Luottotietotarkistukset olivat kaikki yritysten toimeksiantoja yksityishenkilöistä, mutta pankkitileihin liittyvissä tiedusteluissa oli kohteena myös yrityksiä. Niissä ei usein ollut mainittu asiakasta, vain yhdessä asiakkaaksi oli mainittu yksityishenkilö.

Jäljityksiä oli neljänlaisia. Omaisuuden jäljittämisen lisäksi on henkilöiden jäljittämistä (person trace), yritysten jäljittämistä (company trace) ja pelkkä jäljitys (trace), jos toimeksianto oli niin ylimalkainen, ettei sitä selvinnyt kumman ensimmäisen vaihtoehdon jäljittämisestä on kyse. Jos kyse oli vain jäljityksestä – osoitteen hankinnasta tai paikantamisesta – tuli toimeksianto tähän kategoriaan. Tässä kategoriassa olivat myös Prenzlerin (2006, 427) lainopilliseen työhön tyypitellyt virallisten tai oikeudellisten asiakirjojen dokumentoitu toimitus (process service, 35 kpl) ja yritystoimeksiantoihin luokiteltu osoitteen selvitys velkojaa varten (12 kpl). Ikävä kyllä omassa aineistossani yhdessäkään velkomistapauksessa ei ollut mainittu loppuasiakasta, niin tällä aineistolla ei voi valottaa, mikä on yritysten ja yksityisten jakauma toimeksiantajana niissä. Jos kohteesta tarvittiin muuta kuin kohteen osoite- tai sijaintitietoa, niin kategoriaksi tuli taustatarkistus.

Omaisuuden jäljittämisessä (asset trace) ei useinkaan ollut kysymys siitä, että jokin omaisuus pitäisi löytää, vaikka niitäkin oli. Useimmiten jäljitettiin olemassa olevalle omaisuudelle omistajaa tai haluttiin selvittää jonkun henkilön tai yhtiön omaisuutta. Useimmiten nämä olivat kiinteistöjä ja ne oli mainittu omaisuuden jäljitystehtävistä 43 %:ssa (18 kpl). Ainoa omaisuuden takaisinotto (repossession of property) oli sellainen, jossa omaisuus oli myynnissä internetissä ja palkattiin vain ostajia hankkimaan se takaisin – omaisuus ei itsessään ollut hukassa. Asset trace saattoi olla kuitenkin myös osa taustatarkistusta, jossa haluttiin kartoittaa esimerkiksi henkilön omaisuutta muiden taustatietojen lisäksi. Nämä ovat tosin tässä yhteydessä kategorisoitu taustatarkistuksiin, ellei kyse ollut esimerkiksi pelkästään tietyn yhden nimetyn ajoneuvo- tai kiinteistöomistuksen selvityksestä.

Osassa toimeksiannoista etsittiin vain työvoimaa, kuten tutkijoita tai asianajajia (investigator search ja lawyer search) tietystä maasta erittelemättä toimeksiantoa sen tarkemmin. Esimerkiksi fyysiseen suojaukseen liittyvissä toimeksiannoissa haettiin suoraan henkivartijaa tai tiimiä suojaamaan joko itseä tai vierailijaa jossain maassa vierailun ajan. Myös velkomistoimeksianto vaikutti hyvin epätyypilliseltä, vaikka velallisten jäljitystehtäviä olikin useita – vain yhdessä oli mainittu yritys velkojen perimisen kohteena asiakkaan puolesta. Edellä mainitun omaisuuden takaisinostajien haun lisäksi myös maineen suojaamiseen

(reputation protection) liittyvä toimeksianto vaikutti epätyypilliseltä etsivän tehtävältä. Toimeksiannosta sai sellaisen kuvan, kuin taustalla olisi ollut tietoteknisen tai viestintäosaajan haku internetissä olevan aineiston poisto- ja oikaisutarkoituksissa. Lakimiesten tarpeen osalta painottuivat yksityishenkilöt toimeksiantajina: 14 tapauksesta 9 oli perintöasioihin tai avioeroon liittyviä toimeksiantoja.

Osassa taas haettiin suoraan tutkinnan suorittamista johonkin tiettyyn tehtävään tai mahdollisesti toimeksiannon siirtoa kokonaan toiselle yksityisetsivälle. Näitä olivat yleiset tiedonhankintaan liittyvät tehtävät, jotka Prenzlerin tyypittelyssä sijoittuivat lainopilliseen työhön. Mukana oli todisteiden hankintaa, asiakirjojen oikeellisuuden tarkistuksia, kuulusteluja tai haastatteluja, rikos- tai onnettomuustutkintaa, audio- tai käsiala-analyyseja, uskottomuusepäilyjen tutkintaa, vakuutuspetostutkintaa, asiakirjojen hankintaa oikeuden päätöksistä, valheenpaljastuksen suorittamista, sosiaalisen median profiilien selvitystä ja sähköistä tiedonhakua, mutta ylipäätään kaikenlaisia sekalaisia tarkistuksia. Eräässä toimeksiannossa pyydettiin esimerkiksi pelkästään lentoaikataulujen selvittämistä tietyssä kohdemaassa tiettynä aikana. Taulukossa 5 moni yksittäisistä listan loppupään havainnoista sopisi myös tähän kategoriaan, kuten teknisen seurannan paljastaminen (TSCM), lapsikidnappauksen selvitys, sekä esimerkiksi uskottomuusepäilyjen ja rikosten tutkinta.

Valvontatehtävät (surveillance) olivat ehkä hankalimpia sijoittaa muihin kategorioihin, vaikka toimeksiannossa saatettiin ilmoittaa syy sellaiseen. Oli kyse sitten uskottumuusasioista (infidelity) tai vakuutuspetostutkinnasta (insurance investigation), valvonta on tyypillisesti menetelmä, jota kysyttiin. Mutta valvontatehtäville on tyypillistä, että tavoitetta tai lisätietoja ei toimeksiannossa kerrottu. Melkein 70 %:ssa toimeksiantoja oli tehtävän kuvauksena vain surveillance, mutta mitään muita lisätietoja ei kerrottu. Joissain oli tarkenteena esimerkiksi ”useampia henkilöitä suorittamaan tehtävää”, ”valokuvaus”, ”verkossa ja reaalimaailmassa” tai ”sopimusrikkomisen selvittämisen tueksi”. Viimeisin menisi kategoriaan tutkinnan suorittaminen, mikäli koko sopimusrikkomisen selvittäminen olisi ollut toimeksianto, mutta tässä haettiin vain valvonnan suorittajaa, ei tutkijaa koko tapaukseen. Siten jäljelle jäi joukko valvontaan liittyviä toimeksiantoja, joita ei lisätietojenkaan avulla voinut sijoittaa mihinkään edellisistä.

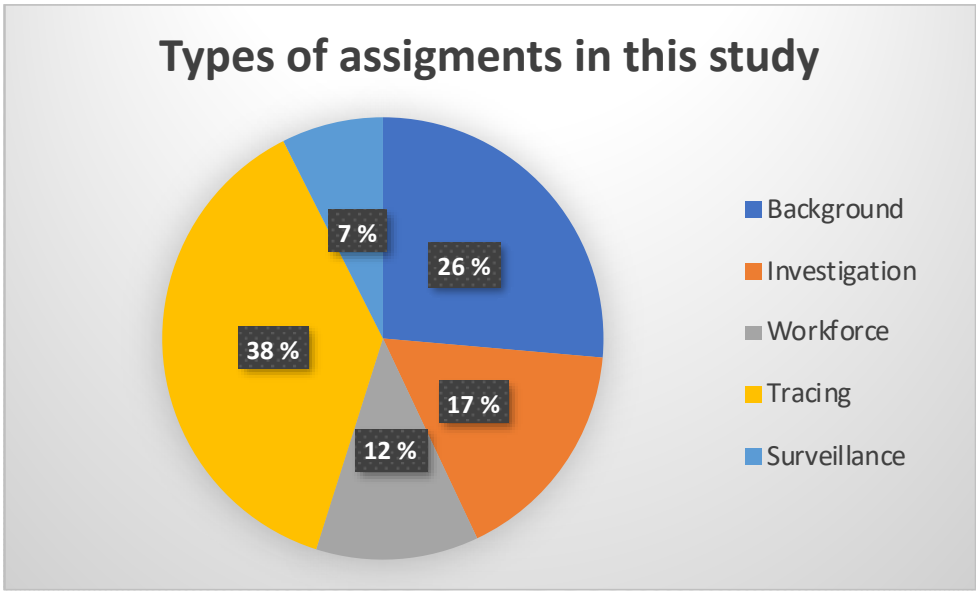
Edellä lueteltuja kategorioita olisi voinut hajottaa vielä tarkempiin osiin, mutta se ei ole tämän työn eikä välttämättä edes toiminnan kuvaamisen kannalta olennaista. Sen sijaan kategoriat voisi yhdistää ylätason tyyppeihin selvemmän kuvan muodostamiseksi ja toiminnan kuvaamisen helpottamiseksi edellä hahmotellun jaottelun mukaan. Kategoriat yhdistettiin taulukossa 6 esitetyllä tavalla:

Main category	Assignment category	amount	%
Tracing	person trace	122	25,96 %
	asset trace	42	8,94 %

	company trace	10	2,13 %
	trace	3	0,64 %
Background	background check	96	20,43 %
	due diligence	12	2,55 %
	bank account	10	2,13 %
	credit check	6	1,28 %
Investigation	information acquisition	59	12,55 %
	insurance investigation	5	1,06 %
	IPR protection	5	1,06 %
	crime forensics	3	0,64 %
	infidelity	3	0,64 %
	Technical surveillance countermeasures (TSCM)	2	0,43 %
	child abduction	1	0,21 %
Workforce	investigator trace	36	7,66 %
	lawyer search	14	2,98 %
	physical protection	3	0,64 %
	debt collection	1	0,21 %
	repossession of property	1	0,21 %
	reputation protection	1	0,21 %
Surveillance	surveillance	35	7,45 %

Taulukko 6: Kategorioiden yhdistäminen

Edellisen perusteella toimeksiannoista muodostuu kuviossa 7 esitetty yleiskuva:



Kuvio 7: Toimeksiantojen tyypit tämän tutkimuksen aineiston valossa

Tarkoitus ei ole kuitenkaan tutkia tai kehittää itse toimialan analyysimenetelmiä, joten jätetään se jatkotutkimukselle. Aineistosta muodostuu kuitenkin selvästi kuva, että henkilötietojen käsittelyä joudutaan kaikissa toimeksiannoissa tekemään. Jonkin työn luokittelu yritystoimeksiannoksi ei aineiston perusteella tarkoita sitä, että käsiteltäisiin vain

yrityksiin liittyviä tietoja. Pelkästään työvoimaa etsiessäkin taustalla on jokin ihmisiin tai perhesuhteisiin liittyvä asia. Ainoat tapaukset, joissa henkilötietojen käsittelyä ei välttämättä tarvitse huomioida olisivat tämän aineiston perusteella yhtiöiden väliset IPR-oikeuksien loukkaukset. Niissä kaikissa oli toimeksiantajana yritys, mutta yhdessäkään ei ollut viitteitä, että tutkinnan kohteena voisi olla yksityishenkilö, vaikka kahdessa tutkinnan kohdetta ei mainittu. Todennäköisesti selvityksen yhteydessä epäiltyyn IPR-oikeudenrikkomiseen voisi liittyä kuitenkin myyntipisteiden tai jakelijoiden selvittämistä, joka edellyttää myös henkilöiden tietojen käsittelyä.

4.6 Tyypittelyn vertailu suomalaiseen aineistoon

Aiemmin taulukossa 2 mainituista yhdeksästä suomalaisesta luvanvaraisesta toimijasta löytyy kolme myös W.A.D.:in jäsenlistoilta. Kaiken kaikkiaan W.A.D. -jäseniä, joilla on toiminta-alueena Suomi, on kuusi kappaletta. On siis syytä olettaa, että toimeksiannot voivat olla saman kaltaisia. Suomalaisesta toiminnasta tuntuu tosin olevan aiemmin vain lehtileikkeitä ja yksittäisiä tarinoita. Yritin tätä tutkimusta varten lähestyä toimijoita suoraan ja kartoittaa eri vaihtoehtoja tilastojen luomiseksi ja millaiset tiedonhankintatavat koettaisiin helpoimmiksi ja mihin voitaisiin sitoutua luotettavan aineiston keräämiseksi. Siinä mielessä suomalaiset toimijat menevät kansainväliseen kategoriaan, että posteihin on turha odottaa vastauksia (esimerkiksi Prenzler & King, 2002, 1). Osasta palautteista kävi ilmi myös se, että omien tapausten avaaminen tilastointimielessäkin ulkopuolisille koettiin negatiiviseksi. Oman yritykseni tilastot eivät taas antaisi kokonaiskuvaa, koska yksityisetsivätoiminta ja rikoksen paljastaminen yrityksessäni keskittyy pelkästään tietoverkkoihin ja -järjestelmiin ja toimimme usein vain tukena toiselle toimeksiantajalle tai lakitoimistolle. Muutaman haastattelun sain parilta innokkaammalta yksityisetsivältä, mutta yleistettävää tai vertailukelpoista tietoa ei näiden kahden perusteella vielä voinut tuottaa.

Tämän työn tekemisen aikana julkaistiin kuitenkin poikkeuksellinen tietoteos suomalaisesta yksityisetsivätoiminnasta. Kyseessä on tietokirjailija Pauliina Susi ja hänen kirjansa Yksityisetsivä, varjo kannoillasi. Teoksessa on koottu neljäntoista yksityisetsiväammatinharjoittajan kertomuksia omalta uraltaan ja etsivistä useimmat ovat myös Suomen Yksityisetsivä- ja Lakitoimistoliiton jäseniä (Susi 2021, 15). Tähän ryhmään nojasin aiemmin muun muassa toimijoiden kuvauksissa ja siten ainakin kaksi asiaa tutkivaa on Suomessa päätynyt saman lähteen äärelle toisistaan tietämättä. Vaikka minunkin antama haastattelu on kirjassa, emme tehneet aineistojen tai lähteiden kartoittamisen osalta yhteistyötä tai olleet tietoisia toistemme kokonaistavoitteista haastattelun aikaan. Kirjan perusteella ei ole mahdollista tehdä luotettavaa tilastoa tai jakaumia siitä, miten tapaukset jakautuvat. Siten tulevien kappaleiden suluissa olevat viittaukset ovat kirjan sivunumeroita, eivätkä kappalemääriä. Kirjan mukaan siinä on pyritty kertomaan yleisimmistä toimeksiannoista (Susi 2021, 15). On kuitenkin aina pidettävä mielessä, että monesti

kiinnostavammat ja raflaavammat jutut saavat palstatilaa. Monet kirjan tarinoista olivat itselle jo oman historian kautta hyvinkin tuttuja ja useasti kuultuja.

Joka tapauksessa toimeksiantojen kuvaukset ovat hyvin samankaltaisia kuin W.A.D.:in listoilta aiemmin analysoidut tapaukset. Taustatarkistuksia kirjassa (Susi 2021) oli esitelty niin yksityisten teettämiä selvityksiä puolisoehdokkaista tai lasten aviopuolisoista (23, 218-219) kuin yritysten tekemiä työnhakijoiden taustatarkistuksia (46-47) toimeksiantajan ollessa joskus ulkomailtakin (38). Vakuutuspetoksia tutkittiin Suomessa myös useassa esimerkissä (18-20, 21-22, 31-32) toimeksiantajan näissäkin ollessa joskus ulkomailta (esimerkiksi 39). Valvontaa suoritettiin vakuutuspetosten tutkinnan yhteydessä (33-35, 36-37), työntekijän epärehellisyyttä arvioitaessa (46, 49-50) tai avainhenkilön epärehellisyyttä tutkittaessa (28-29) ja todisteiden hankinnassa oikeuteen toimeksiantajankin ollessa ulkomailta (32-33), mutta myös yksityistoimeksiantoina (24). (Susi 2021).

Henkilöitä jäljitettiin kirjassa (Susi 2021) myös, milloin sukulaisen tai lapsen löytämiseksi (25-26, 51-52, 56), milloin velallisen löytämiseksi (55) ja milloin vanhojen tuttavuuksien tavoittamiseksi (26, 31). Mutta myös asiakirjojen, kuten testamenttien ja haasteiden toimitukset (89, 149-151) näkyivät myös suomalaisissa toimeksiannoissa. Myös omaisuuden jäljitystehtäviä oli velallisten osalta (48-49), mutta myös yritystoimeksiantoina (55, 68) jopa ulkomailta (100). Omaisuuden takaisinottamiseen liittyviä tapauksia kuvattiin (44-45, 58) ja velkojen perintätapauksia löytyi joukosta myös (68, 126-129). Uskottomuustapauksiin liittyviä toimeksiantoja kuvattiin useita (24-25, 121-122, 196, 206-210) ja näissäkin toimeksiantaja saattoi olla ulkomailtakin (40). (Susi 2021).

Kirjassa (Susi 2021) omassa kansainvälisessä tilastossa vähemmälle jäänyt fyysiseen suojaamiseen liittyvä konsultointi (43) ja itse turvamies- tai suojaamistehtävät löytyivät myös suomalaisesta aineistosta (116-117, 167-168, 201). Toimeksiannoissa oli useita todisteiden hankintaan ja siten tutkintaan sopivaa tapausta, esimerkiksi työnantajan omaisuuden varastaminen työntekijöiden toimesta (72-73, joista kirjattiin yli 6000 rikosta), kassan ohi lyöminen ja rahojen ottaminen itselle (69-70) sekä yrityksen laitteilla kilpailevien tuotteiden valmistaminen (84). Edellisissä toimeksiannoissa usein käytettiin apuna valvontaa, mutta tarvittiin myös muita todisteita. Kun taas hävikin taustalla epäillään olevan asiakas, on myymäläetsivien työstä suurin osa valvontaa (58). (Susi 2021). Myymäläetsivien työ on aina hyvin paikallista ja varmasti sen vuoksi tällaisia toimeksiantoja ei välitetä kansainvälisesti, eikä niitä ollut minun aineistossani. Jos taas yksittäinen kauppa tai kauppaketju etsisi myymäläetsivää, se saattaisi näkyä tämän työn aineistossa vain työvoiman etsimisenä valvontatehtäviin.

Yhteenvetona voidaan sanoa, että tehtäviä ja toimijoita Suomesta löytyy jokaiseen taulukossa 6 esitettyyn kansainvälisen aineiston perusteella muodostettuun pääkategoriaan. Toiminta

Suomessakin on verkottunutta päätellen jo siitä, että monessa tapauksessa taustalla oli ulkomainen toimeksiantaja ja yhdessä käytettiin ulkomaista alihankkijaa (Susi 2021, 182). Edellisen perusteella ei ole syytä epäillä, että yksityisetsiväammatin harjoittaminen olisi Suomessa merkittävästi erilaista kansainvälisestä. Tämän tarkempaan toimiala-analyysiin ei tämän työn puitteissa ole tarve, mutta Pauliina Suden kirjan paljon tarkemmat ja yksityiskohtaisemmat kuvaukset nostivat esiin näkökohtia, jotka ovat olennaisia henkilötietojen käsittelyn lainmukaisuusvaatimuksen ja käsittelystä aiheutuvien riskien näkökulmasta. Kotimaisen aineiston tarkempien kertomusten perusteella vahvistuu myös, että osa toimeksiantajista on työnantajia ja henkilötietoja käsitellään myös työsuhteen kontekstissa.

4.7 Tulosten perusteella valitut tapaukset

Edellisten lukujen perusteella määrällisesti tyypillisimmät toimeksiannot ovat jäljitys-, taustatarkistus- ja tutkintatoimeksiannot niin suomalaisessa kuin kansainvälisessäkin aineistossa. Henkilötietojen käsittelyn näkökulmasta ei ole kiinnostavaa yritysten väliset tai yrityksiin kohdistuvat toimeksiannot, koska silloin käsitellään oikeushenkilöitä, ei välttämättä luonnollisia henkilöitä. Myöskään yritysten omaisuuden jäljittäminen tai yrityksiin kohdistuvat oikeudelliset selvitykset eivät ole kiinnostavia. Etenkin siksi, että vaikka tällaisissa selvityksissä voidaan käsitellä myös henkilötietoja, ne saattavat olla julkisten kauppa-, yritys-, kiinteistö- tai maaomistusrekisterien kautta julkisia tietoja. Henkilöt, joiden tietoja näissä on, ovat usein pelkästään yritysten edustajia tai luottamustehtävissä ja heidän tietojaan saatetaan käsitellä esimerkiksi lakisääteisten rekisterien ylläpidon vuoksi. Niinpä esimerkiksi yrityskauppoihin liittyvät due-diligence-tarkistukset tai yritysten taustojen tarkistaminen ei usein tuota tilanteita, joissa kohteen yksityisyyden suoja tai perusoikeudet edustaisivat merkittävää osaa. Siten esimerkkitapausten valinnassa esimerkiksi pelkästään lukumääriin perustuva valintatapa ei ole tutkimuksen kannalta kiinnostava.

Jäljitystehtäviä oli aineistossa suurin osa. Niiden osalta henkilötietojen käsittely näkökulmasta kiinnostavin tilanne on sellainen, jossa sekä toimeksiantaja, että kohde ovat yksityishenkilöitä. Kummallakin osapuolella on siten lain takaamat perusoikeudet, jotka saattavat olla jopa ristiriidassa keskenään. Tällainen tilanne voi syntyä esimerkiksi silloin, kun vanhempi etsii täysi-ikäistä lastaan, tai aviopuoliso kumppaniaan, mutta toinen osapuoli ei halua tulla löydetyksi.

Taustatarkistukset olivat toisiksi suurin osa aineoston pääkategorioista. Taustatarkistuksista tilanne, jossa toinen yksityishenkilö etsisi tietoja toisen yksityishenkilön taustoista, muistuttaa tietyllä tavalla edellistä jäljitystehtävää. Siinäkin haetaan esimerkiksi osoitetietoja, mahdollisesti pyritään pääsemään jäljille omaisuuden kautta ja siten edellisessä tapauksessa tulee kuvattua jo pitkälle tällainen tilanne. Taustatarkistuksista yksi selkeä esiin

noussut peruste on rekrytointitilanteeseen liittyvä taustojen tarkistaminen. Tässä tilanteessa joudutaan tulkitsemaan oikeushenkilön tiedonsaantioikeutta ja valtaa henkilötietojen käsittelyssä suhteessa yksityishenkilöön. Tilanteessa joudutaan huomioimaan myös työoikeudellisia näkökulmia ja siten tällaisen tilanteen käsittely voi tuottaa enemmän kiinnostavaa informaatiota kuin toistaa edellisen tyyppiesimerkin tilanne.

Tutkintatoimeksiannot olivat kolmanneksi suurin kategoria. Tutkintatoimeksiannoissa tyypillisin suomalaisessa aineistossa on yleensä joko uskottomuusepäily tai työantajaan kohdistuvan väärinkäytöksen selvittäminen. Koska käytössä ei ollut määrällistä tilastovertailua, valitaan tapausesimerkiksi kiinnostavampi työantajan työntekijään kohdistuva väärinkäytös- tai rikostutkinta. Asia on myös ilmiantajien suojelua koskevan lainvalmistelun vuoksi ajankohtainen, sillä yhä useampi yritys joutuu alkaa myös selvittämään ilmiantokanavien kautta tulleita ilmoituksia mahdollisista lain rikkomisista tai muista väärinkäytöksistä (esimerkiksi Gottschalk 2017, 229). Sen lisäksi tässä päästään arvioimaan myös työntekijöiden viestintään ja viestinnän suojaan liittyvää problematiikkaa työsuhteen kontekstissa.

Tutkintatapaukset etenevät yleensä hyvin samalla tavalla riippumatta siitä, millaisesta tapauksesta on kyse. Väärinkäytöstutkinnassa yksi tapa jäsentää tutkinnan etenemistä on Niina Ratsulan tapaa mukaileva tutkinnan jäsentäminen seuraaviin ajallisessa järjestyksessä eteneviin päävaiheisiin (2016, luku 8):

1. Tutkintapäätös
2. Suunnittelu
3. Tiedonkeruu
4. Faktojen arviointi
5. Raportointi
6. Seuraamukset ja korjaavat toimenpiteet

Henkilötietojen käsittelyn näkökulmasta edellisissä vaiheissa osallisiksi saattavat tulla niin epäilty itse kuin muutkin organisaation tutkintaa suorittavat tai sen kohteena tai kuultavana olevat työntekijät, alihankkijat, toimittajat ja asiakkaat ja heidän henkilöstönsä (Ratsula 2006, luku 8.1). Etenkin suunnitteluvaihe on olennainen valitessa tietolähteitä, koska tutkintaan liittyvät henkilöt eivät ole vain epäiltyjä, vaan voivat olla myös todistajan roolissa olevia sivullisia (Ratsula 2006, luku 8.3). Suunnitteluvaiheen osalta Ratsula nostaa esiin problematiikan esimerkiksi sähköpostien avaamiseen tai henkilökohtaisen omaisuuden tutkimiseen liittyen, mitkä eivät ole välttämättä suoraviivaisia tai automaattisesti sallittuja toimia (2016, luku 8.2). Näitä käsitellään myöhemmin tarkemmin lainsäädäntökehikon käsittelyn yhteydessä.

Myös yksityishenkilöiden toimeksiannoissa edellä oleva malli soveltuu käytettäväksi. Tutkintapäätöksen osalta olennaisessa osassa ovat neuvottelut asiakkaan kanssa ja suunnitteluvaiheessa korostuvat tapaukseen liittyvien tietolähteiden määrittely suhteessa toimeksiannon tavoitteisiin. Esimerkiksi henkilöitä jäljitettäessä mukaan voivat tulla sukututkimukset, seurakuntien väestöön liittyvät arkistot, väestörekisteri, ajoneuvorekisterit, viranomaiset, kiinteistörekisterit ja julkiset maksulliset tietokannat tai ketkä tahansa kolmannet osapuolet, jos tarvitaan esimerkiksi jonkun kertomuksen vahvistamista tilanteesta, johon liittyy muita osapuolia. Ennakkovalmistautumista asiakkaalta ei yleensä edellytetä, mutta toimeksiannon vastaanottajan on silti valmistauduttava riittävillä sopimuksilla ja esimerkiksi tietolähteiden valinnalla ennakkosuunnittelussa. Raportointi tapahtuu luonnollisesti aina vain toimeksiantajalle, mutta seuraamuksiin tai korjaaviin toimenpiteisiin tutkintaa suorittava puuttuu vain, mikäli sellaisesta työstä erikseen sovitaan. (SYL ry jäsenen asiantuntijahaastattelu 24.10.2020).

Monesti tietojen keruun ympäristöllä on myös vaikutusta. Eräs slovenialainen etsivä kertoi kerran lainanneensa ystävänsä koiraa ja mennyt juoksuttamaan sitä pellolle. Samalla pellolla oli peltotöissä hänen kohdehenkilönsä, joka oli samaan aikaan päätyöstään sairaslomalla. Näin hän pystyi kuvaamaan päätoimen työnantajalle kohdehenkilön työskentelyä pellolla, kun oli kuvaavinaan koiran leikkiä. (Slovenialaisen etsivän haastattelu, 2021). Tämä oikeus perustuu Sloveniassa lakiin yksityisetsivistä, kuten myös oikeus jäljitä kadonneita ja piiloutuneita ihmisiä (private detective services act 2011, artikla 26).

Esimerkiksi kotirauhan piiriin kuuluvalla alueella kohdehenkilön kuvaaminen Suomessa ei onnistuisi ilman hänen lupaansa syyllistymättä salakatseluun (rikoslaki 39/1889, luku 24, 6 §). Jäljitystehtävien osalta on tietysti muistettava, että oikeus yksityisyyteen kuuluu kaikille ja siten myös henkilöille, joita jäljitetään. Jos jäljityksen taustalla ei ole laina kautta tulevaa oikeutusta tai kohteen hengen tai terveyden suojelu, joutuu viranomainenkin joskus oleman luovuttamatta jäljitettävien henkilöiden tietoja kadonneita ihmisiä etsiville henkilöille (YLE 2015; Iltalehti 2021b; Digi- ja väestötietovirasto 2022, Jos läheinen katoaa).

Tietoja voidaan joskus joutua hankkimaan myös sähköisen viestinnän välitystietojen ja viestiliikenteen avulla. Opsec Oy on erikoistunut sähköisiin ympäristöihin rikosten paljastamisessa. Toimintaa mainostaa tekevänsä moni tavallinen IT-yhtiökin ilman tuntemusta lainsäädännöstä tai sen rajoitteista, esimerkiksi luvanvaraisuudesta ja siihen liittyvien viestintäpalvelulain rajoitteista. Yhtiön vastaava hoitaja kertoo viestiliikenteen välitystietojen liittyneen 81 %:iin yrityksen tilastoimista rikoksen paljastamiseen liittyvistä toimeksiannoista. Sähköistä viestiliikennettä ja joissain tapauksissa liikenteen sisältödataa on jouduttu käsittelemään 42 %:ssa tapauksista. Nämä liittyvät usein yritysten toimeksiantoihin, sillä yksityisenä toimijana yhtiöllä on erittäin rajoitetusti pääsy julkisen verkon viestiliikenteeseen tai välitystietoihin ja näitä on voitu käsitellä vain, jos toimeksiantoon

liittyvät asianosaiset ovat itse sellaista dataa luovuttaneet. (Vastaavan hoitajan haastattelu 2021).

Työantajat kuitenkin tuntevat hyvin harvoin sähköisen viestiliikenteen tai viestinnän tietojen suojaan liittyvää lainsäädäntöä tai huolehtimisvelvoitteita. Toisaalta niitä eivät tunne tutkintaa tekevätkään, koska luvanvaraisen toimijan koulutusedellytys on vartijakortin suorittaminen, eikä sen yhteydessä käsitellä rikosten paljastamista, viestiliikenteen tai henkilötietojen käsittelyä. Sen lisäksi pelkkä välitystietojen käsittely ei usein ratkaise yhtään rikosta, koska tämän päivän verkottuneessa työelämässä on vaikea sanoa, onko jokin viesti välitetty kilpailijalle yhteistyöprojektin edistämiseksi vai liikesalaisuuksien luovuttamiseksi. (Vastaavan hoitajan haastattelu 2021). Siten myös sähköinen viestintä etenkin työsuhteissa voi olla kohteena tietoja käsitellessä.

Olennaista on siis se, että tutkinnassa voi joutua käsittelemään missä vaiheessa tahansa melkein kenen tahansa henkilötietoja ja keräämään niitä joko kolmansilta osapuolilta tai suoraan kohdehenkilöä tarkkailemalla. Pääsääntö on kuitenkin edellisten pohjalta se, että kyse on joko toimeksiantajan henkilötiedoista, toimeksiannon kohteesta tai jostain ulkopuolisesta tapahtumaan liittyvästä henkilöstä. Siten työn tuloksena esiteltävissä kehitysehdotuksissa arvioidaan lainmukaisuusperusteita ja huolehtimisvelvoitteita näistä kolmesta näkökulmasta.

Yhteenvetona valittujen tapausten ja niissä esiintyvän henkilötiedon käsittelyn osalta tulee lainsäädäntöä käsitellä vähintään seuraavasti:

- Yleislait, joita sovelletaan kaikkeen henkilötietojen käsittelyyn
- Turvallisuusalan elinkeinoluvanhaltijaan sovellettava lainsäädäntö
- Sähköiseen viestintään liittyvä lainsäädäntö
- Työelämään ja työsuhteisiin sovellettava lainsäädäntö

4.8 Lainmukaisuusriskit ja etiikka toimeksiannoissa

Ennen kuin seuraavassa luvussa siirrytään käsittelemään lainsäädäntökehikkoa, tulee huomioida aineistoanalyysin perusteella esiin noussut toiminnan lainmukaisuus ja etiikka. Epäeettiset tai suoraan laittomat tiedonhankintamenetelmät yksityisetsivätoiminnan yhteydessä ovat nousseet esiin kansainvälisesti (Prenzler 2006, 429-430; Prenzler & King 2002, 4, Prenzler & Milroy 2012, 343). Lain rikkominen on vahingossakin helppoa, ellei tunne lainsäädäntöä. Yksityisetsiviä on käytetty jopa valtiollisessa vakoilussa ja viimeksi tästä varoitti esimerkiksi FBI:n johtaja Christopher Wray haastattelussaan Kiinan Yhdysvaltoihin kohdistamasta vakoilusta helmikuun alussa (Williams 2022, kohta 8min 29s).

Myös Pauliina Suden kirjan (2021) tarkat kuvaukset nostivat esiin myös kotimaassa moraalisesti ja eettisesti – mahdollisesti jopa lainsäädännöllisesti – ongelmallisia tilanteita. Henkilötietojen käsittelyn näkökulmasta kaikki käsittely tarvitsee aina laissa määritellyn perusteen ja käsittely on oltava lainmukaista (tietosuoja-asetus 679/2016, artikla 5. kohta 1 a). Lainsäädännön tarkoituksena on suojata myös luonnollisten henkilöiden perusoikeuksia ja vapauksia (tietosuoja-asetus, artikla 1, kohta 2). Kirjan (Susi 2021) esimerkeissä oli kuvattuna myös tilanteita, joissa käsittely ei ole mahdollisesti lainmukaista, eikä välttämättä luonnollisten henkilöiden perusoikeuksien ja -vapauksien mukaista.

Sivuilla 63-64 (Susi 2021) oli kuvattuna esimerkki, jossa huoltajuuskiistan yhteydessä palkattiin etsivät paikantamaan kiistan keskiössä oleva lapsi ja palauttamaan tämä äidilleen. Taustalla oli oikeuden päätös ja tilanteessa oli mukana lapsen äiti ja tehtävässä oli käytetty apuna lakimiestä (Susi 2021, 63-64). Tapauksessa jää silti auki itse toimijan vastuu. Entä jos oikeuden päätös ei ole lainvoimainen? Ja ovatko etsivät varmistuneet päätöksen lainvoimaisuudesta tai edes sen olemassaolosta? Ja onko teko, jolla on näin suoria ja merkittäviä oikeusvaikutuksia, silti puolustettavissa? Lakimieshän ei viime kädessä ratkaise teon lainmukaisuutta, vaan lopullisesti se ratkaistaan oikeuskäsittelyssä. Lastensuojelulain näkökulmasta tulee pohtia myös itse lapselle aiheutuvia vahinkoja ja ottaa huomioon myös lapsen etu (lastensuojelulaki 417/2007, 4 §). Teolla voi hyvinkin olla negatiivisia vaikutuksia asianosaisille eikä tapauksen osalta käynyt missään kohtaa selväksi, oliko lapsen etu otettu huomioon päätöstä tehdessä. Tietenkin myös etsivien oikeusturva on toiselta näkökulmalta ongelmallinen – jos teko tuomittaisiin laittomaksi, niin johtaako se korvausvastuuseen tai rangaistusvaatimuksiin ja kuka viime kädessä vastaisi valitusta menettelytavasta?

Toinen esimerkki on sivulla 65 (Susi 2021) mainittu syötin käyttäminen tulevan tai nykyisen puolison uskollisuuden selvittämisessä. Vaikka uskottomuus ei täytä minkään rikoksen tunnusmerkistöä, voidaan teko silti nähdä epäeettisenä. Pelkkä uskottomuuden toteaminen seurannan perusteella on eri asia, koska etsivä ei itse pyri aktiivisesti vaikuttamaan tapahtumien kulkuun. Lisäksi herää kysymys, miten pitkälle näissä tapauksissa oltiin valmiita menemään? Jos palkkion saanti edellyttää tuloksia ja toinen osapuoli odotti pettämisen tapahtuvan, niin johtaako se houkutukseen käyttää tilanteessa päihdyttäviä tai huumavia aineita tai painostusta, jolloin kyse ei ole enää toimeksiannon kohteena olevan henkilön omaan määräysvaltaan täysin kuuluvasta valinnasta. Jos tutkittaisiin vaikka epärehellisyyttä osto- tai myyntitilanteissa tai työntekijän lojaliteettia, syöttiä tai lavastettua tilannetta käytettäessä kysymykseen voisi tulla myös rikokseen houkuttelu.

Etsiviä ainakin yritettiin houkutella rikokseen asiakkaiden toimesta. Sivulla 125-129 (Susi 2021) kuvattiin tilanne, jossa asiakas oli tilaamassa tuhopolttoa vakuutusrahojen saamiseksi. Sivulla 105-108 (Susi 2021) kuvattiin tilanne, jossa asiakas pyrki palkkaamaan etsivän saadakseen epämieluisan henkilön katoamaan. Myös sivulla 239 (Susi 2021) kuvataan, miten

asiakkaat ovat pyrkineet teettämään tietomurtoja. Selvityksen yhteydessä rikoksiin on myös syyllistytty, vaikka ei välttämättä etsivän toimesta, kuten sivun 139-140 (Susi 2021) esimerkissä, jossa yksityisasuntoon murtautumalla jäljitettiin omaisuutta. Jälkimmäisessä esimerkissä esiin nousee myös henkeen ja terveyteen kohdistuva vaara etsivän joutuessa aseella uhatuksi. Puhumattakaan oikeusturvakysymyksistä, joita liittyy hyvin paljon esimerkiksi sivuilla 136-137 (Susi 2021) kuvattuun tapaukseen, jossa todistusaineistoa väärentämällä pyrittiin auttamaan asiakasta.

Hankalia oikeudellisia kysymyksiä liittyy myös henkilöiden jäljitystilanteisiin (Susi 2021, 153-155, 205-206, 227-228), joissa tulee punnittavaksi myös kohdehenkilön perusoikeudet ja vapaudet. Joissain tilanteissa kävi selvästi ilmi, että henkilön oikeutta kadota kunnioitettiin yksityisetsivän toimiessa lähinnä neuvottelijana osapuolten välillä. Kuitenkin etsivän palkkiot on joissain esimerkeissä mainittu kiistetyn, koska haluttuja tuloksia ei ole tullut. Avoimeksi jää, etenkin yritystoiminnan ollessa aika pienimuotoista, voiko toimeksisaajan taloudellinen riippuvuus toimeksiantojen onnistumisesta vaikuttaa menetelmiin ja keinoihin?

Asiakkaiden ja toimeksiantojen kohteiden perusoikeuksien ja -vapauksien toteutuminen voi olla myös ongelmallisia. Paitsi, että toimeksiannot saattoivat epämieluisissa havainnoissa aiheuttaa surua, saattoi se aiheuttaa vakavampiakin ongelmia. Esimerkiksi sivuilla 74-75 (Susi 2021) kuvataan, miten kiinnijäämisen aiheuttama häpeä saattoi johtaa jopa itsemurhayrityksiin. On hyvin todennäköistä, että joissain tapauksissa myös avustaville tai muille asiaan yhdistetyille henkilöille saattaa aiheutua negatiivisia seurauksia. Suomessa on vielä tutkittu hyvin vähän esimerkiksi lakia tai yritysten toimintaohjeita rikkovien ilmiantajille aiheutuvia seurauksia, mutta terveydenhuollosta saatujen esimerkkien perusteella lähes puolet kokee negatiivisia seurauksia raportoidessaan epäeettisestä tai lainvastaisesta toiminnasta (Pohjanoksa et al. 2019a, 535). Ihmiset jättävät jopa suoranaisia rikoksia ilmoittamatta johtuen siitä, että pelätään itselle aiheutuvia seurauksia (Pohjanoksa, et al. 2019b, 15 - 16). Norjasta löytyy esimerkkejä siitä, miten jopa väärinkäytösten tutkijat itse voivat kääntyä ilmiantajia vastaan perusteetta (Gottschalk 2017, 235-236).

Henkilötietojen käsittelyn osalta on todettava, että luonnollisille henkilöille – niin ammatinharjoittajille, asianosaisille ja asiakkaille – on yksityisetsivätoimintaan liittyen olemassa konkreettisia riskejä. Henkilötietojen käsittely taas on erottamaton osa toimintaa, koska aina puhutaan viime kädessä ihmisistä. Etenkin epärehellisen toiminnan kautta oikeusvaikutukset voivat olla merkittäviä, jolloin toimintaan liittyy riskejä vartioimisliiketoiminnan yleisten periaatteiden rikkomisesta, mutta myös henkilötietojen käsittelyn lainmukaisuuden kautta, jota tässä työssä käsitellään seuraavaksi. Yhteenvetona voidaan sanoa, että henkilötietojen käsittely yksityisetsivätoiminnassa on aina tietynlaisen tavanomaisesta poikkeavan keinovalikoiman käyttöä, joka kohdistuu ihmisten yksityisyyteen ja jolla voi olla seurauksia ja oikeusvaikutuksia ihmisten oikeuksiin ja vapauksiin. Rikoksen

paljastamisen ja selvittämisen intention yhteydessä voidaan ehkä yksinkertaistaa, että yksityisetsivien suorittama tutkinta on tietyllä tavalla voimakeinojen käyttöä, joka kohdistuu ihmisten yksityisyyteen.

5 Henkilötietojen käsittelyyn sovellettava lainsäädäntö yksityisetsivien toimeksiannoissa

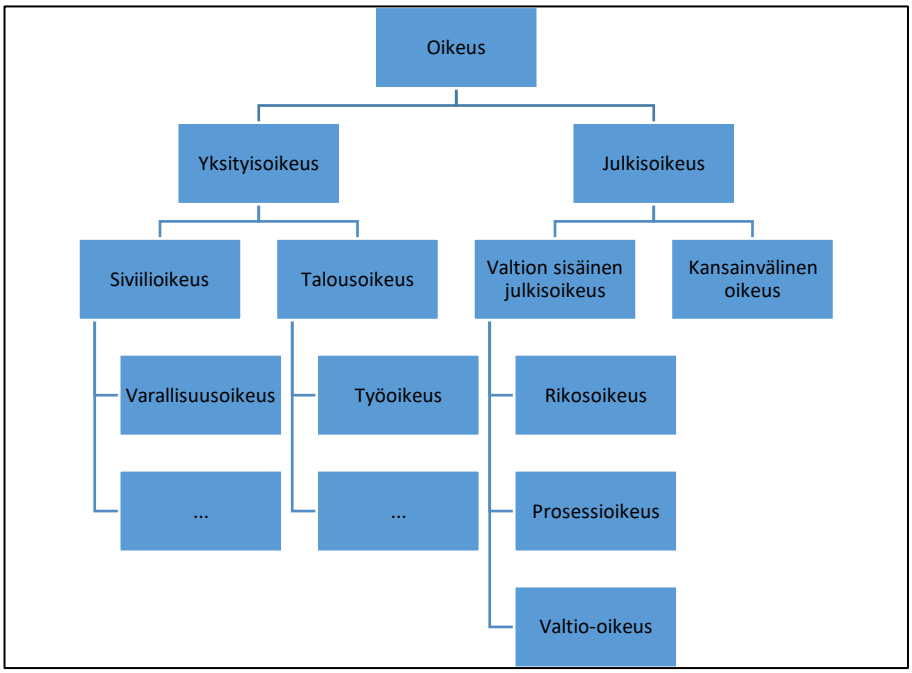
Tässä luvussa käsitellään henkilötietojen käsittelyyn sovellettavaa lainsäädäntökehikkoa. Kehikon pääelementit nimettiin luvussa neljä sen luvun havaintojen perusteella siitä, millaisia ovat tyypilliset toimeksiannot. Luvun tarkoitus on tunnistaa yksityisetsivätoimintaan kustakin lainsäädännön osa-alueesta sovellettavat velvoitteet. Mutta myös arvioida sellaisia toimivaltuuksia tai lainmukaisuusperusteita, jotka eivät aiempien lukujen kolme ja neljä perusteella soveltuisi yksityisetsivätoimintaan. Esimerkiksi tieteellisestä ja historiallisesta tutkimuksesta on tietosuoja-asetuksessa määritelty kansallista liikkumavaraa ja sitä onkin säännelty tarkemmin omassa lainsäädännössämme (tietosuoja-asetus 679/2016, 89 artikla, kohta 2; tietosuojalaki 1050/2018, 31 §). Vaikka yksityisetsivätoimintaa harjoittava voisi omasta toiminnastaan tehdä historiallista tutkimusta tai luovuttaa oman toimintansa tilastoja tutkimuksellisiin tarkoituksiin, ei sellaista nähdä lukujen kolme ja neljä perusteella tavanomaisena yksityisetsivätoimintana. Siksi esimerkiksi tieteellinen ja historiallinen tutkimus on jätetty pois tästä työstä. Samoin kaikki muutkin tilanteet, joihin ei toimeksiantoja suoritettaessa todennäköisesti törmätä.

Luvussa kuvataan ensin yleiskehys, lainsäädännön tausta ja soveltamisjärjestys ja sen jälkeen edetään velvoittavimmasta EU-lainsäädännöstä suomalaiseen erityislainsäädäntöön. Koska työ käsittelee vain yleisiä luvuissa kolme ja neljä kuvattua toimintaa, eikä pohjaudu konkreettisen toimeksiannon analyysiin, ei tässä kuvattu kehikko ole tyhjentävä tai täydellinen. Henkilötietojen käsittelystä voidaan säätää myös erityislainsäädännössä, joka voi vaihdella täysin palveluiden tarjoajan tai asiakkaan erityispiirteiden tai toimialan mukaan.

5.1 Henkilötietojen käsittelyn lainsäädäntötausta

Suomen oikeusjärjestelmä jakautuu julkisoikeuteen ja yksityisoikeuteen, jotka ovat osittain päällekkäisiäkin. Subjektiteorian mukaan julkisoikeudellisena asiana pidetään sellaista, jossa osapuolena on julkinen valta, esimerkiksi valtio. Muuten asia on yksityisoikeudellinen. Valtio tai julkisen vallan edustaja voi olla myös yksityisoikeudellisessa suhteessa esimerkiksi yksityisoikeuteen luettavan sopimuksen osapuolena. Suhteen luonne ja rajanveto ovat siis kiinni siitä, ketkä ovat oikeussuhteen osapuolia, mutta myös siitä, missä suhteessa he ovat toisiinsa. (Björne 1986, 15). Subjektiteorian mukaan yksityisetsivätoiminnassa on kysymys yksityisoikeuden alaan kuuluvista asioista.

Julkisoikeus ja yksityisoikeus jakautuvat Björnen (1986, 16) mukaan kuviossa 8 esitetyn mukaan seuraavasti:



Kuvio 8: Suomen oikeusjärjestelmän rakenne (Björne 1986 mukaillen)

Julkisoikeuteen kuuluu valtion järjestykseen, valtioelinten toimivaltaan ja kansalaisten suhteeseen valtioon liittyvä sääntely ja kansainväliseen oikeuteen valtioiden ja kansainvälisten järjestöjen väliset suhteet (Björne 1986, 18). Siten esimerkiksi EU:n kautta tuleva sääntely kuuluu julkisoikeuden alaan. Yksityisoikeuteen lukeutuvan varallisuusoikeuden alle kuuluu taas velvoite- ja esineoikeus, jotka säätelevät sopijapuolten välisiä suhteita sekä sivullissuhteita (Björne 1986, 17). Työn kohteena olevaan rikoksen paljastamista suorittaviin toimijoihin kohdistuu velvoitteita yksityisoikeuden puolelta esimerkiksi asiakassopimusten ja työsopimusten kautta, mutta julkisoikeuden puolelta taas EU-oikeuden velvoitteita ja rikosoikeuden puolelta rikosoikeudelliset vastuukysymykset. Täten yksityisetsivätoiminnassakaan ei riitä pelkän yksityisoikeudellisen lainsäädännön huomiointi.

Koska tietosuoja-asetuksesta tuli suoraan jäsenvaltioissa sovellettavaa lainsäädäntöä, on tietosuoja-asetus eurooppalaisena yleislakina keskeisin laki henkilötietojen käsittelyssä (tietosuoja-asetus 679/2016, resitaali 12). Vaikka puhutaan rikoksen paljastamisesta, tulee muistaa, että tietosuoja-asetusta ei sovelleta tiettyihin viranomaisen suorittamiin henkilötietojen käsittelytoimiin. Poliisiviranomaisen suorittamaa henkilötietojen käsittelyä ohjaa niin sanottu poliisidirektiivi (2016/680/EU) ja uusi poliisin henkilötietolaki (Ustaran 2018, 18; Pyykkö 2020, 34-35). Koska tämä työ käsittelee vain yksityissektoria, eivät kyseiset säädökset kuulu tämän työn sisältöön.

Tietosuoja-asetus (679/2016) jättää kuitenkin liikkumavaraa jäsenvaltioille erikseen määritellyissä tilanteissa. Näitä ovat esimerkiksi:

- Erityisten henkilötietoryhmien käsittely (artikla 9, kohta 4)
- Lakisääteiseen velvoitteeseen ja yleiseen etuun ja julkisen vallan käyttöön perustuva käsittely (Artikla 6, kohta 2)
- Sektorispesifinen lainsäädäntö, esimerkiksi työoikeus (artikla 88)
- Arkistointi sekä tieteellinen ja historiallinen tutkimus (artikla 89)

Muun muassa näistä liikkumavaratekijöistä johtuen Suomessa on tullut voimaan 1.1.2019 tietosuojalaki, jossa on tarkoitus määritellä tarkemmin edellä mainituista asioista. Suomessa on myös työlainsäädännön alaan kuuluvaa lainsäädäntöä, jonka soveltaminen tulee myös kyseeseen silloin, kun yksityisetsivätoiminta liittyy työsuhteessa tapahtuvaan henkilötietojen käsittelyyn. Näihin liittyviä asioita käsitellään omissa alaluvuissaan.

Kuten luvussa neljä todettiin, yksityisetsivien toimeksiannoissa puhutaan aina henkilötiedoista. Syyllisyyden ja rangaistuksen osoittamien ei ole mahdollista, ellei taustalta löydy luonnollista henkilöä, johon syyllisyys tai rangaistus kohdistuisi. Tutkintaprosessissa on aina olennaisesti kyse vastausten hankkimisesta kuuteen peruskysymykseen; Mitä, kuka, missä, milloin, miten ja miksi (Sennewald & Tsukayama 2015, 17). Tietosuoja-asetuksen mukaan henkilötiedon käsite taas kattaa kaiken tiedon, joka on jollain tavalla suoraan tai epäsuorasti liitettävissä tunnistettavissa olevaan luonnolliseen henkilöön (tietosuoja-asetus 679/2016, artikla 4, kohta 1). Siten myös vastaukset muihin tutkimuskysymyksiin, kuten mitä on tapahtunut, milloin ja kysymykset motiiveista ovat aina yksityisetsivätoiminnassa tekijään jollain tavalla liitettäviä tietoja.

Henkilötietojen käsittelyssä puhutaan usein myös tietosuojasta. Tietosuoja ei ole uusi termi, vaan se on määritelty jo 1992 Yleissopimuksessa yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (36/1992). Tietosuojalla tarkoitettiin silloin yksilön oikeuksien ja perusvapauksien turvaamista automaattisessa tietojenkäsittelyssä ja oikeutta yksityisyyteen (Yleissopimus 16/1992, luku 1, artikla 1). Tietosuoja-asetus myöhemmin laajentaa nämä oikeudet myös muussa kuin automaattisessa tietojenkäsittelyssä tapahtuvaan tietojen käsittelyyn silloin, kun tiedot muodostavat tai niiden on tarkoitus muodostaa rekisteri tai rekisterin osa (tietosuoja-asetus 679/2016, luku 1, artikla 2). Kannattaa huomioida, että tietoja ei tarvitse varsinaisesti tallentaa rekisteriin, vaan riittää, että niiden käsittelyn taustalla on tarkoitus muodostaa osa jotain rekisteriä.

Tietosuojan ja henkilötietojen käsittelyn osalta on syytä tunnistaa kaksi asiaa. Ensinnäkin kyse ei ole mistään uudesta asiasta, vaan sillä on pitkä historia. Se luo pohjan sille, miten henkilötietojen käsittelyn konteksti tulee ymmärtää, miten sitä tulee tulkita ja millaisia

taustoja siihen liittyvällä sääntelyllä on. Toinen tekijä on näiden asioiden välitön liitos kansainväliseen lainsäädäntöön ja kansainvälisiin sopimuksiin, joista kaikki eivät ole vain EU:n sisäisiä. Näitä käsitellään tarkemmin seuraavassa luvussa. Tämän työn tavoitteena ei ole kuitenkaan käsitellä lainsäädännön historiaa tai kehitystä. Lainsäädännön historiaa ja taustoja käsitellään kuitenkin sen verran, että voidaan ymmärtää mitä sen muodostumisen taustalla on ja miten sen velvoittavuus muodostuu.

5.2 Henkilötietojen käsittelyn ja tietosuojan kansainvälinen tausta

Henkilötietojen käsittelyyn liittyvät asiat alkoivat nousta teknologisen kehityksen ja erityisesti tietokoneiden käytön lisääntymisen vuoksi esiin jo -70 luvulla (Carey 2015, 1; Ustaran 2018, 3). Yksityisyyden suojan kannalta lähtökohtana mainitaan kuitenkin jo YK:n yleismaailmallinen ihmisoikeuksien julistus vuodelta 1948, jonka taustalla vaikutti myös toinen maailmansota (Ustaran 2018, 3). Julistuksessa on mainittu yhdenvertaiset ja luovuttamattomat oikeudet, sekä yksityisyyden, kotirauhan ja viestinnän luottamuksellisuus ja lain suoma oikeus suojautua oikeudettomilta hyökkäyksiltä, jotka kohdistuvat maineeseen ja kunniaan (Ihmisoikeuksien julistus 1948, johdanto ja artikla 12). Suomessa tämä ratifioitiin 1976 kansalaisoikeuksia ja poliittisia oikeuksia koskevalla kansainvälinen yleissopimus 23.6.1975/107 (SopS 7/1976), jossa yksityisyyteen liittyvät oikeudet ovat artiklassa 17 (SopS 8/1976). Samalla sopimuksella vahvistettiin myös rikosoikeuteen liittyvään aiemmin mainittu laillisuusperiaatteeseen kuuluvia perustekijöitä artiklassa 15 (SopS 8/1976).

Nämä oikeudet vahvistettiin myös Euroopan ihmisoikeussopimuksessa vuodelta 1950. Sopimus astui voimaan 3.7.1953. Tämä sopimus oli kuitenkin velvoittava vain silloisen Euroopan neuvoston jäsenmaille. Sitovaksi sen teki se, että jäsenmaita sitoi velvoite oman lainsäädännön ja käytäntöjen sovittamiseen varta vasten perustetun Euroopan ihmisoikeustuomioistuimen ratkaisujen mukaan. (Ustaran 2018, 5). Suomi ratifioi sopimuksen 1990, mikä oli edellytys Euroopan neuvoston jäsenyydelle (Ihmisoikeuskeskus 2021, Euroopan neuvoston ihmisoikeussopimukset, jotka Suomi on allekirjoittanut ja ratifioinut; HE 22/1990 vp, 1).

Sen jälkeen henkilötietojen käsittelyyn ja etenkin haasteisiin kansainvälisissä valtioiden välisissä siirroissa ottivat kantaa myös OECD:n linjaukset, jotka eivät kuitenkaan olleet laillisesti sitovia (Ustaran 2018, 7-20). Euroopan neuvosto avasi allekirjoitusprosessin 1981 Yleissopimuksesta yksilöiden suojelemisesta henkilötietojen automaattisessa käsittelyssä (myös yleissopimus 108, Convention 108). Sen tavoitteena oli taata kansalaisille yhtäläiset oikeudet ja vapaudet yksityisyydensuojaan liittyen. Siihen ei haluttu viitata Euroopan yleissopimuksena, koska sillä haluttiin korostaa sitä, että sen voisi allekirjoittaa myös maat Euroopan ulkopuolelta. (Ustaran 2018, 10–11; Käsikirja Euroopan tietosuojaoikeudesta 2014, 15-16). Kaikki EU valtiot ovat ratifioineet sen ja vuonna 2001 hyväksyttiin myös lisäpöytäkirja,

jolla määrättiin myös maiden rajat ylittävästä käsittelystä (Käsikirja Euroopan tietosuojaoikeudesta 2014, 16).

Yleissopimus 108 sisälsi monia nykypäivän tietosuojalainsäädännölle tyypillisiä elementtejä. Sitä sovelletaan ensinnäkin sekä julkiselle, että yksityissektorille. Henkilötietoja ei saa kerätä kuin tiettyä nimenomaista ja lainmukaista tarkoitusta varten, se rajaa arkaluontoisten tietojen käsittelyä (kuten rotu, terveystiedot, poliittinen suuntaus, ja niin edelleen). Siinä vahvistetaan myös yksilön oikeuksia saada tietää häneen liittyvien tietojen käsittelystä. (Käsikirja Euroopan tietosuojaoikeudesta 2014, 16). Euroopan unionin perusoikeuskirja ei sisältänyt aiemmin mitään kansalaisten perusoikeuksien ja vapauksien suojaamisesta, mutta myöhemmin muun muassa nämä yleissopimuksen 108 mainitsemat oikeudet vahvistettiin EU-kansalaisten oikeuksiksi ja vapauksiksi Lissabonin sopimuksella 2009 (Ustaran 2018, 15-16; Carey 2015, 14). Lissabonin sopimuksella muutettiin suoraan sopimusta Euroopan unionista ja Sopimusta Euroopan unionin perustamisesta (Ustaran 2018, 15). Näin näistä periaatteista tuli Euroopan unionin kaikkien jäsenvaltioiden hyväksymää primaarioikeutta (Käsikirja Euroopan tietosuojaoikeudesta 2014, 17). Tämä antoi EU:lle myös lainsäädäntövallan tietosuoja-asioissa (Käsikirja Euroopan tietosuojaoikeudesta 2014, 20).

Euroopan unionin kehittyessä tunnistettiin tarve tarkemmalle ja harmonisoidummalle lainsäädännölle. Euroopan parlamentti pyysi komissiota jo 1976 laatimaan ehdotuksen tätä varten. Sen perusteella syntyi henkilötietodirektiivi (95/46/EU), joka tuli voimaan lokakuussa 1995 (Carey 2015, 6). Direktiivi on lainsäädäntöä, joka sitoo jäsenvaltioita, mutta jättää liikkumavaraa jäsenvaltioille päättää lainsäädännön implementoinnissa sen keinovalikoimasta tarkemmin. (Ustaran 2018, 13–14). Suomessa direktiivi lokalisoitiin kansalliseen lainsäädäntöön nyttemmin kumotulla henkilötietolailla (HE 96/1998 vp, 1). Direktiivi ei kyennyt kuitenkaan vastaamaan haasteeseen harmonisointityökaluna johtuen jokaisen valtion oikeudesta päättää lopullisesta lain keinovalikoimasta. Samoin teknologian kehitys toi lukuisia uusia tilanteita, miten henkilötietoja käsitellään. Komissio aloitti työn tietosuojalainsäädännön vahvistamiseksi 2010 ja päätyi 2012 ehdottamaan direktiivin tilalle tietosuoja-asetusta. Trilogineuvottelujen (kolmenväliset neuvottelut parlamentin, komission ja neuvoston välillä) jälkeen tietosuoja-asetus astui voimaan 2016 ja se soveltaminen alkoi 25.5.2018. Asetuksen ja direktiivin välinen olennaisin ero oli se, että asetus on suoraan jäsenvaltioissa sovellettavaa lainsäädäntöä. (Ustaran 2018, 16-17).

Tietosuoja-asetuksen lisäksi henkilötietojen käsittelyssä on huomioitava sähköinen käsittely tarkemmin, mitä säätelee sähköisen viestinnän tietosuojadirektiivi (2002/58/EY). Direktiivi on luonteeltaan teknologianeutraali ja sen tavoite on säädellä internetissä tapahtuvaa tiedonvälitystä, kuten tavanomaista puhelinliikennettä säädellään (Carey 2015, 14). Direktiivin tavoitteena on yhdenmukaistaa jäsenvaltioiden säännöksiä ja turvata yksityisyyteen liittyvät oikeudet ja tietojen suoja henkilötietojen käsittelyssä sähköisen

viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi 2002/58/EY, 1 artikla). Johtuen teknologisesta kehityksestä ja uusien sähköisisten palveluiden kehittymisestä, katsottiin tarpeelliseksi säätää tarkemmin viestintäverkoissa ja viestintälaitteilla tapahtuvasta henkilötietojen käsittelystä. Se asettaa vaatimuksia palveluntarjoajille tietoturvallisuuden varmistamisesta, luottamuksellisuuden varmistamisesta viestintäverkoissa ja sähköiseen markkinointiin liittyviä reunaehtoja. Se esittelee myös niin sanotun ”välitystiedon” määritelmän ja säätelee erikseen esimerkiksi tämän viestinnän välittämiseksi tarpeellisen tiedon käsittelystä samoin kuin käsittelyä esimerkiksi laskutusta varten. (Ustaran 2018, 54–56).

Sähköisen viestinnän tietosuojadirektiivin (2002/58/EY) 15 artikla jättää varaa kansallisvaltioille säätää erikseen liikennetietojen käsittelystä esimerkiksi rikosten torjunnan, tutkinnan ja syyteharkintaan saattamisen osalta. Edellytys tällaiselle on kuitenkin se, että käsittelyn tulisi olla rajattu välttämättömään ja että se tapahtuisi esimerkiksi kansallisen tuomioistuimen tai riippumattoman hallinnollisen elimen valvonnassa ja etukäteisluvalla (yhdistetyt tapaukset C-203/15 ja C-698/15, kappaleet 119-120). Tällaisessa käsittelyssä tulee myös huomioida, miten vakavasti yksityisyyteen puututaan sekä selvitettävien rikosten vakavuus (C-207/16, kappaleet 60–62). Edelliset päätökset koskevat viranomaisten tiedonsaantioikeuksia, mutta päätöksessä Mircom vs. Telenet BVBA viime vuodelta, unionin tuomioistuin on todennut, etteikö tällaisia liikennetietoja ja siten myös liittymän omistajan tietoja voitaisi luovuttaa myös tekijänoikeusrikkomuksissa tekijänoikeuksien haltijalle siviilikanteen nostamista varten. Edellytys tälle kuitenkin on se, että asiasta on säädetty kansallisessa laissa ja toimenpiteet ovat oikeasuhtaisia. (C597/19, kappale 133, kohta 3). Kaikki tällaiset rajoitukset ja poikkeamat tulisi siten olla säädettynä kansallisessa laissa sähköisen viestinnän tietosuojadirektiivin (2002/58/EY) viidennentoista artiklan 1 kohdan mukaan.

Sähköisen viestinnän tietosuojadirektiivistä on valmisteilla myös asetus, jonka tarkoitus on yhdistää tietosuoja-asetuksen ja sähköisen viestinnän vaatimukset keskenään ja laajentaa sen soveltamisalaa sekä vahvistaa EU-kansalaisten perusoikeuksia yksityisyyden osalta (Euroopan komissio 2021a, Key points of the Commission's proposal). Sähköisen viestinnän tietosuoja-asetuksen piti tulla alun perin voimaan samaan aikaan kuin yleisen tietosuoja-asetuksen (Ustaran 2018, 59). Luonnostekstistä päästiin yksimielisyyteen kuitenkin vasta 10.2.2021 ja nyt vasta Portugalin puheenjohtajuuskauden vuoksi heidän johdollaan päästään lopullisesta tekstistä neuvottelemaan Euroopan parlamentin kanssa. Jos yksimielisyyteen päästään, astuu asetus voimaan 20 päivää sen jälkeen, kun se on julkaistu Euroopan unionin virallisessa lehdessä ja sen soveltaminen alkaa siitä kahden vuoden kuluttua. (Euroopan neuvosto 2021, Council mandate).

Koska kyseessä on direktiivi, on se sen vuoksi implementoitava kansalliseen lainsäädäntöön. Suomessa se on implementoitu lailla sähköisen viestinnän palveluista (917/2014) ja sitä käsitellään tarkemmin myöhemmin. EU-oikeuden ja kansallisen oikeuden välillä on huomioitava myös EU-oikeuden ensisijaisuusperiaate. Se tarkoittaa sitä, että EU-oikeutta tulkitaan aina ensisijaisesti jäsenvaltioiden oikeuteen nähden (Euroopan unionin virallinen lehti 2016, 344). Ensisijaisuuden taustalla on itse asiassa juuri perusoikeuskysymykset ja erityisesti tapaus Costa v. ENEL, jonka yhteydessä todettiin, että jäsenvaltiot eivät voi asettaa omaa säännöstöään perustamissopimukseen nähden etusijalle (Costa v. ENEL 1964, kohta tuomion perustelut). Tuomiossa käytettiin myös sanaa etusijaisuus kuvaamaan ensisijaisuutta, joten niillä on tässäkin työssä sama merkitys.

Käytännössä tämä tarkoittaa sitä, että ylintä tuomiovaltaa Euroopan unionin jäsenmaissa käyttää Euroopan unionin tuomioistuin. Tuomioistuin voi antaa ratkaisuja sellaisissa kansallisen oikeuden tapauksissa, joissa kansallinen tuomioistuin ei pääse ratkaisuun. Mutta sinne voivat tietyissä tapauksissa viedä asioita myös yksityishenkilöt, yritykset ja muut organisaatiot. (Ustaran 2018, 34-36; Euroopan unioni 2021). Tuomioistuin voi käsitellä rikkomusten ja vahingonkorvauskanteiden lisäksi myös ennakkoratkaisupyyntöjä esimerkiksi tilanteissa, joissa perusoikeudet ovat ristiriidassa, kuten esimerkiksi yksityisyyden suojan ja tekijänoikeuksien välistä tasapainoa tulkitessa (Europan unioni 2021 ja esimerkiksi C-597/19). Tästä johtuen myös tietosuoja-asetus (679/2016) on Suomessa soveltamisestaan alkaen olut ensisijaisesti sovellettavaa lainsäädäntöä.

Tietosuoja-asetuksen ensisijaisuutta korostetaan myös tuomioistuinten toimivaltaa koskevan lainsäädännön osalta, tuomioistuimen toimivallasta sekä tuomioiden tunnustamisesta ja täytäntöönpanosta siviili- ja kauppaoikeuden osalta. Käytännössä se tarkoittaa, että toisessa EU-maassa annettu tuomio on tunnustettava toisessa EU-maassa ilman eri menettelyä. (Euroopan parlamentin ja neuvoston asetus 1215/2012, luku Tärkeimmät kohdat). Myös esimerkiksi kanteen nostamiseen liittyvä rekisteröidyn oikeus ohittaa sen, mitä muuten on säädetty yleisestä tuomioistuinten toimivallasta. Sama koskee myös tuotteiden kaupan akkreditointia ja markkinavalvontaa, esimerkiksi tietosuojamerkkejä tai -sertifiointeja. (Kuner et al. 2020, 1138, 1180, 751)

Tietosuoja-asetuksen ja sähköisen viestinnän tietosuojadirektiivin yhteydessä puhutaan usein ”lex specialis derogat legi generali” -periaatteesta. Yleisesti sillä viitataan periaatteeseen, jonka mukaan laissa oleva tarkempi säännös ohittaa yleisemmän säännöksen (esimerkiksi Italia v. komissio 2016, kohta 81). Sähköisen viestinnän tietosuojadirektiivin tarkoitus on ensisijaisesti suojata viestinnän luottamuksellisuutta ja tarkentamalla nimenomaan sähköiseen viestintään liittyvää lainsäädäntöä yleisestä henkilötietojen käsittelystä, tulee tätä direktiiviä tulkita erityislainsäädäntönä tietosuoja-asetukseen nähden (Kuner et al. 2020, 1297). Tietosuoja-asetus ja sähköisen viestinnän tietosuojadirektiivi sisältävät myös erityisiä

ohjeita niiden välisestä suhteesta. Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY) sisältää jonkin verran viittauksia tietosuoja-asetuksella kumotuksi tulleeseen henkilötietodirektiiviin (95/46/EY). Tietosuoja-asetuksen (679/2016) artikla 94 toteaakin, että näitä viittauksia tulee jatkossa tulkita viittauksina tietosuoja-asetukseen (kohta 2). Myös tietosuoja-asetuksen (679/2016) resitaali 173 toteaa, että asetusta on sovellettava kaikkeen sellaiseen henkilötietojen käsittelyyn, josta ei säädetä sähköisen viestinnän tietosuojadirektiivissä.

Sähköisen viestinnän tietosuojadirektiivin (2002/58/EY) resitaali 10 taas sanoo, että kumottua tietosuojadirektiiviä, eli nykyistä tietosuoja-asetusta, tulee soveltaa kaikkiin ihmisten perusturvaan ja -oikeuksiin liittyviin kysymyksiin tai rekisterinpitäjän velvoitteisiin, joista sähköisen viestinnän tietosuojadirektiivi ei nimenomaisesti säädä. Tästä siis seuraa se, että molempia voidaan joutua tulkitsemaan yhtä aikaa ja jotkut asiat osuvat yhtä aikaa molempien soveltamisalaan (EDPB 2019, 11). Tällainen tilanne voi syntyä esimerkiksi silloin, kun välitystiedot sisältävät henkilötietoja (esimerkiksi IP-osoite tai sähköpostiosoite) ja käsittelyyn liittyvät vaatimukset tulevat sähköisen viestinnän tietosuojadirektiivistä, joista se erityisesti säätää. Kyseinen direktiivi (2002/58/EY) ei kuitenkaan säädä mitään rekisteröityjen oikeuksista tai esimerkiksi yleisistä henkilötietojen käsittelyperiaatteista. Lex specialis -periaatteen vuoksi yleissäännöstä poiketaan vain erityissäännön ollessa olemassa. Näin ollen edellä mainittuun käsittelyyn sovelletaan sekä sähköisen viestinnän tietosuojadirektiiviä, mutta niiltä osin mistä se ei sääntele, noudatetaan tietosuoja-asetusta. Jos siis rekisteröity haluaa käyttää oikeuksiaan esimerkiksi pyytämällä pääsyä tietoihinsa, sovelletaan henkilötietoja sisältäviin välitystietoihin tietosuoja-asetusta, koska sähköisen viestinnän tietosuojadirektiivi ei säädä tästä mitään. (EDPB 2019, 13-15).

Tietosuoja-asetuksen (679/2016) artiklan 95 mukaan se ei kuitenkaan aseta sellaisia lisävelvoitteita, jotka on jo huomioitu sähköisen viestinnän tietosuojadirektiivissä ja joilla on sama tavoite. Tällainen tilanne voi seurata esimerkiksi siitä, kun viestintäpalvelun tarjoaja on jo tehnyt tietosuojaloukkauksesta ilmoituksen sähköisen viestinnän tietosuojadirektiivin velvoitteen perusteella, joten ilmoitusvelvollisuutta ei enää ole tietosuoja-asetuksen artiklan 33 perusteella (EDPB 2019, 15).

Rikoksen paljastamisen näkökulmasta on huomioitava myös sähköisen viestinnän tietosuojadirektiivin (2002/58/EY) täydentävä vaikutus. Koska se suojaa ”käyttäjiä” ja ”tilaajia”, se laajentaa viestinnän luottamuksellisuuden suojan koskemaan myös oikeushenkilöitä, kun taas tietosuoja-asetus suojaa vain luonnollisia henkilöitä. (EDPB 2019, 14). Tilaajana olevalla työnantajallakin on siis oikeus viestinnän suojaan siten kuin sähköisen viestinnän tietosuojadirektiivi tästä säätää. Samalla tavalla on huomioitava alihankintaketjut ja henkilötietojen jatkokäsittely, josta sähköisen viestinnän tietosuojadirektiivi (2002/58/EY) toteaa resitaalissa 32, että näiden osalta noudatetaan sitä, mitä tietosuoja-asetus asettaa

velvoitteita rekisterinpitäjille ja käsittelijöille. Siten yksityisetsivätoiminnassa tulee huomioida myös sähköisen viestinnän tietosuojadirektiivi käsiteltäessä sen alaisia tietoja.

5.3 Tietosuoja-asetus

Tietosuoja-asetus (679/2016) korostaa ihmisillä käytössä olevia tehokkaita oikeussuojakeinoja heidän tietojaan käsitteleviä vastaan ja toi mukanaan varsin korkeat hallinnolliset seuraamusmaksut, jos asetusta ei noudateta (artiklat 79 ja 83). Monella on vieläkin käsitys, että viranomainen ensin ohjaa ja vasta sitten sakottaa, jos toiminta ei ole lainmukaista. Mutta kuten selviää sakkotuomioista, viranomainen ei itse näe asiaa siten, vaan toiminnan lainvastaisuus voi johtaa suoraan sakkotuomioon (esimerkiksi 2477/161/21, 25). Ihmisille aiheutuvien vahinkojen ei tarvitse myöskään olla konkreettisia vahinkoja, vaan myös aineettomat vahingot huomioidaan. Esimerkiksi pelkästään se, että henkilö menettää mahdollisuuden valvoa omien tietojensa käsittelyä, on määritelty vahingoksi, joka oikeuttaa korvauksiin (tietosuoja-asetus 679/2016, resitaali 85 ja artikla 82). Henkilötietojen käsittely muodostaa siten jo merkittävän liiketoimintariskin, ellei käsittelyä tehdä lain mukaan. Kyse ei siis ole vain toiminnan kohteiden suojaamisesta vaan myös toimijan itsensä oikeusturvasta.

Työn tarkoitus ei ole käsitellä tietosuoja-asetusta kokonaisuudessaan tai esitellä kaikkia sen velvoitteita tyhjentävästi. Työn kannalta tässä esitellään merkittävimmät asiat ja syvennetään sellaisia alueita, jotka ovat yksityisetsivän ammatinharjoittamiseen liittyvän lainmukaisen käsittelyn näkökulmasta olennaisia aiemmin esitettyjen tavoitteiden mukaan. Tietosuoja-asetuksen soveltamisala määrittyy sekä aineellisen, että alueellisen soveltamisalan kautta. Aineellisesti sitä sovelletaan kaikkeen käsittelyyn, joka on

1. joko kokonaan tai osittain automaattista
2. käsittelyyn muussa kuin automaattisessa muodossa, jos henkilötiedot muodostavat, tai niiden on tarkoitus muodostaa rekisterin osa
   (tietosuoja-asetus 679/2016, artikla 2, kohta 1)

Henkilötietojen käsittelyä on mikä tahansa henkilötietoihin kohdistettu toimenpide aina keruusta, välittämisestä ja säilytyksestä tuhoamiseen asti ja johtuen tietojärjestelmien luonteesta, lähes kaikki yritystoiminnassa tapahtuva sähköinen tai manuaalinen käsittely menee tämän soveltamisalan piiriin (Euroopan komissio 2021c). Ainoastaan asiakirjat tai asiakirjakokoelmat kansilehtineen, jotka eivät ole järjestettävissä henkilötietojen perusteella, ovat soveltamisalan ulkopuolella (tietosuoja-asetus 679/2016, resitaali 15). Tosin tämän päivän tietojärjestelmät vaikuttavat siihen, että skannaaminen lukukelpoiseen sähköiseen muotoon indeksoi asiakirjat automaattisesti rekisteriksi, joka on järjestettävissä myös asiakirjojen sisältämän henkilötiedon perusteella.

Rekisterin määritelmä ei kuitenkaan tarkoita sitä, että kyseessä pitäisi olla jokin henkilötietokortisto tai että tiedot tulisi olla henkilötiedon perusteella jäsenneltynä. Tietosuoja-asetus tai sen edeltäjä tietosuojadirektiivi, eivät määrittele mitään täsmentäviä kriteerejä, millä tavalla henkilötiedot olisi oltava järjestetty, että ne muodostaisivat rekisterin. Rekisteri voi muodostua jo sillä perusteella, että rekisterinpitäjä tai käsittelijä voi helposti hakea henkilöä koskevia tietoja aineistosta, eikä itse rekisterin tarvitse sisältää mitään luetteloita tai hakua palvelevia järjestelyitä. (C25/17, kappale 62). Siten esimerkiksi yksityisetsivän muistikirjat tai paperiarkistot voivat kuulua tietosuoja-asetuksen soveltamisalan piiriin, vaikka olisi kyse paperilla olevasta jäsentämättömästä aineistosta, jos edellä mainittu haun helppous toteutuu. Ottaen huomioon sen, että toimeksiantojen suorittaminen edellyttää tietojen saatavilla oloa ja edes kohtuullista käytettävyyttä, olisi aika vaikea perustella tapauksista kerätyn aineiston olevan tietosuoja-asetuksen soveltamisalan ulkopuolella.

Alueellinen soveltamisala taas on määritelty siten, että tietosuoja-asetusta sovelletaan Euroopan unionin alueelle sijoittuneeseen toimintaan liittyvään käsittelyyn. Käsittelyn itsensä ei tarvitse tapahtua EU-alueella. Eikä toimijankaan tarvitse olla EU-alueella, jos se on sijoittunut alueelle, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla. Alueellinen soveltamisala lähestyy asiaa myös niiden henkilöiden näkökulmasta, joiden tietoja käsitellään. Vaikka rekisterinpitäjä tai käsittelijä ei olisi sijoittunut unionin alueelle, mutta se käsittelee unionin alueella olevien henkilöiden tietoja tavaroiden tai palvelujen tarjoamiseksi näille tai näiden henkilöiden käyttäytymisen seurantaan, sovelletaan silloinkin tietosuoja-asetusta. (tietosuoja-asetus 679/2016, artikla 3). Euroopan unionin alue tulee lukea tässä yhteydessä Euroopan talousalueena (ETA), johon kuuluvat unionin jäsenten lisäksi Islanti, Liechtenstein ja Norja (Euroopan komissio2021c, International transfers of personal data).

Soveltamisesta on myös poikkeamia. Tietosuoja-asetusta (670/2016) ei sovelleta esimerkiksi toimintaan, joka ei kuulu Euroopan unionin lainsäädännön soveltamisalaan, unionin ulkoiseen toimintaan, yhteiseen ulko- ja turvallisuuspolitiikkaan tai viranomaisten suorittamaan käsittelyyn (artikla 2, kohta 2). Edellä mainitut poikkeamat ovat sellaisia, jotka eivät liity yksityisetsivätoiminnan harjoittamiseen. Tietosuoja-asetuksen (679/2016) artiklan 2 kohdassa 2 määritellään myös niin sanotusta kotitalouspoikkeamasta, mikä tarkoittaa, että asetusta ei sovelleta käsittelyyn, mikä tapahtuu yksinomaan henkilökohtaista tai kotitaloutta koskevassa toiminnassa. Kyseistä poikkeamaa tulkitaan kuitenkin suppeasti ja jos käsittelyyn liittyy esimerkiksi julkista aluetta tai sillä oleskelevia ihmisiä, ei kyse ole enää yksinomaan kotitalouden piirissä tapahtuvasta käsittelystä (C-212/13, kohdat 29 ja 35). Merkitystä on myös sillä, kenen tietoja käsitellään. Elleivät käsittelyn kohteena olevat henkilöt kuulu henkilötietoja käsittelevän henkilön yksityiseen piiriin, ei kyse ole henkilökohtaisesta tai

kotitaloutta koskevasta toiminnasta (C-25/17, kappaleet 44 ja 51). Siten yksityisetsivä ei voisi perustella toimeksiannoissa käsittelyn kuuluvan kotitalouspoikkeaman piiriin.

Tietosuoja-asetusta (679/2016) ei sovelleta myöskään oikeushenkilöiden tai oikeushenkilöiden muodossa perustettujen yritysten henkilötietojen käsittelyyn: esimerkiksi oikeushenkilön nimeen, oikeudelliseen muotoon tai yhteystietoihin (resitaali 14). Tämä ei kuitenkaan tarkoita sitä, että tietosuoja-asetusta ei sovellettaisi käsittelyyn, joka tapahtuu yritysten välisessä toiminnassa. Tietosuojavaltuutettu on ottanut asiaan kantaa viimeksi 21.10.2021 todetessaan, että niiltä osin kuin käsitellyt tiedot ovat yhdistettävissä luonnolliseen henkilöön, on kyse tietosuoja-asetuksen soveltamistalaan kuuluvasta henkilötietojen käsittelystä, vaikka osapuolina ovatkin yhtiöt (3592/152/2019, luku Sovellettavasta lainsäädännöstä).

Henkilötietojen käsittelyn osalta on tärkeää tunnistaa myös, missä roolissa käsittelyä tekevä taho sitä suorittaa. Tietosuoja-asetus erittelee neljännessä artiklassa kaksi erilaista roolia henkilötietojen käsittelyssä. Rekisterinpitäjällä viitataan luonnolliseen henkilöön tai oikeushenkilöön, viranomaiseen, virastoon, tai muuhun elimeen, joka henkilötietojen käsittelyä suorittaa. Käsittelijällä taas viitataan luonnolliseen henkilöön tai oikeushenkilöön, viranomaiseen, virastoon, tai muuhun elimeen, joka suorittaa käsittelyä rekisterinpitäjän puolesta. (tietosuoja-asetus 679/2016, artikla 4, kohdat 7 ja 8). Koska näillä rooleilla on merkittävä ero vastuissa ja velvollisuuksissa, esitellään nämä vielä myöhemmin tarkemmin.

Henkilötiedon määritelmä on varsin laaja. Henkilötietona pidetään mitä tahansa luonnolliseen henkilöön (”rekisteröity”) liittyvää tietoa, minkä perusteella henkilö voi olla tunnistettavissa suoraan tai epäsuorasti (tietosuoja-asetus 679/2016, artikla 4, kohta). Määritelmä on huomioitava myös teknisessä valvonnassa, jossa esimerkiksi kameravalvonnan tallennin sisältää tunnistettavien henkilöiden kuvaa ja siten kameravalvontaa harjoittava käsittelee myös henkilötietoja (esimerkiksi Frände & Wahlberg 2018b, 418). Jo tietosuojadirektiivin voimassaoloaikana henkilötietolain perusteella esimerkiksi ajoneuvon rekisteritunnus on henkilötieto, koska se on rekisterien kautta yhdistettävissä haltijaan tai omistajaan (344/45/2000). Samalla perusteella myös esimerkiksi kiinteistön rekisteritunnus on henkilötieto – kiinteistörekistereissä on aina myös omistajatieto (Isotalo 2018, Rekisteritunnus on henkilötieto).

Tietosuojan yhteydessä puhutaan myös pseudonymisoinnista, mikä tarkoittaa esimerkiksi tutkimuksissa aineistoissa tunnistettavien tietojen korvaamista koodeilla tunnistamisen vaikeuttamiseksi (Jyväskylän yliopisto 2020, Anonymisointi ja pseudonymisointi). Pseudonymisoituja tietoja on kuitenkin kohdeltava samoin kuin mitä tahansa henkilötietoa, jos on mahdollista, että ne voitaisiin liittää luonnollisiin henkilöihin. Arvioitaessa pseudonymisoinnin tasoa ei tule arvioida vain sitä, ovatko tiedot juuri sillä hetkellä kyseisen

toimijan osalta yhdistettävissä, vaan siinä tulee huomioida myös muiden henkilöiden mahdollisuudet, teknologinen kehitys, kulut ja tarvittava aika. (tietosuoja-asetus 679/2016, resitaali 26).

Henkilötietojen osalta esitellään myös niin sanotut erityiset tietoryhmät, jotka tunnettiin pääosiltaan henkilötietolain aikaan arkaluoteisina tietoina (henkilötietolaki 523/1999, luku 3). Erityisiin tietoryhmiin kuuluvat esimerkiksi tiedot, joista ilmenee etnisyys, poliittinen tai seksuaalinen suuntautuminen, uskonnollinen vakaumus ja terveyteen liittyviä tietoja ja niiden käsittely on lähtökohtaisesti kielletty (tietosuoja-asetus 679/2016, artikla 9, kohta 1). Edellä mainittu kiinteistön rekisteritunnus voi siten olla myös erityisiin tietoryhmiin lukeutuva tieto, jos kiinteistöön liittyy remontti- tai muutostyötietoja, jotka paljastaisivat asukkaan olevan liikuntavammainen (Korpisaari 2018, 50). Tämä on tärkeä muistaa etenkin työelämän kontekstissa – pelkkä sairasloman pituus voi jo indikoida tietynlaista terveysongelmaa, vaikka itse sairautta ei mainittaisi.

Erityisten tietoryhmien käsittely on sallittua vain tietyillä poikkeuksilla, joista yksityisetsivätoimintaan voi soveltua muutama tilanne. Jos henkilö itse antaa nimenomaisen suostumuksen nimettyjen erityisten tietoryhmien käsittelylle nimettyihin käyttötarkoituksiin, voidaan tietoja käsitellä (tietosuoja-asetus 679/2016, 9 artikla, kohta 2 a ja resitaalit 39 ja 51). Käsittely edellyttää nimenomaista suostumusta, joka on tiukempi kuin yleinen suostumuksen määritelmä ja sitä käsitellään tarkemmin myöhemmin käsittelyn lainmukaisuuden yhteydessä. Toinen perustelu voisi olla käsittely oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi (tietosuoja-asetus 679/2016, 9 artikla, kohta 2 f). Kolmas ja erittäin harvinainen perustelu voisi olla sellainen, jossa näitä tietoja käsitellään henkilön itsensä tai toisen henkilön elintärkeiden etujen suojaamisessa. Lisäedellytys on lisäksi se, että henkilö olisi fyysisesti tai juridisesti estynyt antamaan suostumuksensa. (tietosuoja-asetus 679/2016, artikla 9, kohta 2 c). Tässä on huomioitava myös elintärkeille eduille määritelty korkea kynnys liittyen hengen ja terveyden suojaamiseen, mitä käsitellään tarkemmin myöhemmin.

Erityisten tietoryhmien lisäksi tietosuoja-asetuksessa on toinenkin henkilötietojen ryhmä, jonka käsittelystä on poikkeuksia. Näitä ovat tietosuoja-asetuksen (679/2016) kymmenennen artiklan tarkoittamat rikostuomioihin ja rikoksiin ja näiden turvaamistoimiin liittyvät henkilötiedot, joita ei saa kyseisen artiklan mukaan käsitellä kuin viranomaisen valvonnassa tai kun siitä erikseen säädetään laissa. Aiemmassa suomenkielisessä käännöksessä puhuttiin rikostuomioista ja rikkomuksista, mutta rikkomus -sana on korvattu suomennoksen oikaisussa sanalla ”rikos” (Oikaisu tietosuoja-asetukseen 679/2016 2021, kohta 87). Rikkomuksella viitataan Suomen rikoslaissa yleensä rikoksiin, jotka ovat kokonaisuutena arvostellen vähäisiä, kuten esimerkiksi velallisrikkomuksessa tai ympäristörikkomuksessa (Rikoslaki 39/1889, luku 5, 39 § ja luku 48, 3 §).

On otettava huomioon, että tietosuoja-asetuksen alkuperäinen englanninkielinen teksti ei muuttunut ja maailmalta löytyy kyllä tulkintoja siitä, mitä näillä tiedoilla tarkoitetaan. Esimerkiksi Ison-Britannian valvontaviranomainen (Information Commissioner's Office, ICO) on ilmaissut näiden tietojen osalta tulkinnan olevan laaja ja käsittävän mitä tahansa rikoksiin ja rikostuomioihin liittyviä tietoja, joiden perusteella voi oppia jotain yksityisen ihmisen rikostaustasta tai käyttäytymisestä (ICO, What is criminal offence data?). Vaikka Iso-Britannia ei ole enää EU:n jäsenmaa, on lainsäädäntö kuitenkin vielä muuttumaton näiltä osin ajalta, jolloin maa oli vielä unionin jäsen. Pohjoismaista Ruotsin yksityisyydensuojaviranomainen (Integritetsskydds myndigheten, IMY) on maininnut kyseisten tietojen käsittävän tiedot myös rikosepäilyistä (IMY 2021, Brottsuppgifter).

Puolassa käynnistettiin 19.10.2021 julkinen konsultaatio ilmiantajien suojelua koskevan kansallisesta laista. Ilmiantajien suojelua koskeva laki velvoittaa yhtiöt tutkimaan ilmoitettuja väärinkäytöksiä ja suojelemaan ilmiantajia. Tämän lakiehdotuksen (Ustawa z dnia o ochronie osób zgłaszających naruszenia prawa 2021) viidennessä artiklassa lain soveltamisalan ulkopuolelle jää ”rikosoikeudelliset menettelyt” (”postępowania karnego”), mikä viittaisi siihen, että sellaisten asioiden käsittely nähdään Puolassakin arkaluonteisena. Espanjassa eräs yritys yritti kiertää rikoksiin liittyvien tietojen käsittelyä keräämällä niin sanottuja negatiivisia todistuksia, eli asiakirjoja rikosrekisterin puuttumisesta. Espanjan valvontaviranomainen (Agencia Española de Protección de Datos, AEPD) katsoi kuitenkin päätöksellä PS/00267/2020, että todistus rikosrekisterin puuttumisesta on yhtä lailla rikostuomioihin ja rikoksiin liittyvien tietojen käsittelyä. Viranomainen määräsi yrityksen lopettamaan todistusten keräämisen, tuhoamaan kerätyt todistukset ja kahden miljoonan euron hallinnollisen seuraamusmaksun lainvastaisesta henkilötietojen käsittelystä. (Dataguidance 2022; AEPD 2022).

Myös ilmiantajien suojelua koskevan direktiivin (1937/2019) johdanto-osassa on maininta, että jäsenvaltioilla tulee olla menettelyt ilmoituskanaviin jätettyjen henkilötietojen suojaamiseksi (resitaali 76). Pelkästään siis rikosepäilyjen käsittelyn voisi johtaa näin kuuluvan tietosuoja-asetuksen artiklan 10 rajoitusten piiriin ja käsittely olisi suoritettava vain viranomaisen valvonnassa tai kun siitä on laissa erikseen säädetty. Koska rikoksiin liittyvien tietojen käsittelystä tulee säännellä kansallisessa lainsäädännössä tarkemmin, käsitellään näitä tarkemmin vielä kansallisen lainsäädännön yhteydessä luvussa Tietosuojalaki.

Tietosuoja-asetuksen (679/2016) 23. artikla antaa oikeuden poiketa edellä käsitellyistä informointiin ja rekisteröityjen oikeuksiin liittyvistä velvoitteista. Tässä tulee kuitenkin muistaa, että tämä poikkeus annetaan kansallisvaltioille ja poikkeukset tulee olla määriteltynä kansallisessa tai unionin lainsäädännössä (tietosuoja-asetus 679/2016, 23 artikla, kohta 1; EDPB 2021b, 7). Lainsäädännöksi ei kelpaa mikä tahansa laki tai laissa mainittu perustelu, vaan sen tulee olla tarpeeksi selkeä siten, että luonnolliset henkilöt voisivat

riittävällä tavalla päätellä olosuhteet ja edellytykset, milloin näistä oikeuksista voidaan poiketa (EDPB 2021b, 16). Myös Euroopan ihmisoikeustuomioistuin on ottanut kantaa siihen, että puututtaessa yksilön perusoikeuksiin, tulee lainsäädännön olla niin täsmällistä, että yksilö voi päättää käyttäytymisestään, eikä edes toimeenpanovaltaa käyttävä viranomainen voi venyttää näitä rajoja mielivaltaisesti (EIT 14.9.2010). Rikosten ennalta estämisessä, tutkinnassa ja paljastamisessa käsitellyistä tiedoista mainitaan vielä erikseen, että sellaisetkin tiedot on luovutettava asianosaisille kuitenkin heti, kun se voidaan tehdä tutkintaa vaarantamatta (EDPB 2021b, 9). Kaikki poikkeukset informointiin on siis löydyttävä kansallisesta laista tai muualta unionin lainsäädännöstä, eikä tähän artiklan 23 tarjoamaan poikkeamaan voi suoraan vedota yksittäinen yritys tai luonnollinen henkilö. Informoinnista poikkeaminen ei anna myöskään oikeutta poiketa osoitusvelvollisuudesta tietosuoja-asetuksen noudattamisen osalta (EDPBb 2021, 6).

5.3.1 Henkilötietojen käsittelyn periaatteet

Käsittelyn periaatteet on kuvattu tietosuoja-asetuksen (679/2016) artiklassa viisi (kohdat 1 ja 2) ja ne ovat kiteytetysti:

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus
- osoitusvelvollisuus

Periaatteet eivät itsessään sisällä selkeitä ohjeita tai neuvoja itse käsittelyyn. Loput tietosuoja-asetuksen artikloista tarkentavat näitä periaatteita käytännönläheisemmillä ohjeilla; Esimerkiksi läpinäkyvyyttä ohjeistetaan artiklasta 12 eteenpäin, eheyden ja luottamuksellisuuden toteuttamista artiklassa 32 ja esimerkiksi osoitusvelvollisuutta tarkennetaan artikloissa 24 ja 25 (Kuner et al. 2020, 312).

Tuomioita yksistään periaatteiden noudattamisen laiminlyönneistä on annettu Euroopassa useita. Näitä oli 18.1.2022 200 oikeustapausta 993:sta (CMS 2020, oikeustapaukset, joiden tyyppinä on pelkästään Non-compliance with general data processing principles). Siitä huolimatta, että periaatteet eivät sisällä yksityiskohtaisia ohjeita, periaatteiden toteutumista arvioidaan usein oikeustapauksissa viranomaisen päätöksissä Suomessakin (esimerkiksi 2477/161/21, 15; 2890/161/2021, luku Rikkomuksen tahallisuus tai tuottamuksellisuus; 531/161/20, 3). Kohtuullisuuden periaatetta arvioidaan usein, koska artiklaan 5 liittyvä resitaali toteaa muun muassa, että ”Henkilötietoja olisi käsiteltävä vain, jos käsittelyn

tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin" (tietosuoja-asetus 679/2016, resitaali 39). Esimerkiksi Euroopan tuomioistuin pohti samaa ratkaistessaan, voidaanko kansallisella lainsäädännöllä säätää videovalvonnasta ilman suostumusta ja voitaisiinko rikoksia torjua vähemmän yksityisyyteen puuttuvilla keinoilla (C-708/18 2018, kohta 47). Myös käyttötarkoitussidonnaisuus on yksi avainperiaatteista – käytännössä se tarkoittaa, että henkilötietoja saa kerätä vain tiettyä, nimenomaista ja laillista tarkoitusta varten (WP 29 2013, 4). WP 29 tarkentaa vielä, että nimenomaisen tarkoituksen ymmärtämistä helpottaa sen vertaaminen esimerkiksi piilotarkoitukseen, jolloin käsitteen soveltamista on helpompi ymmärtää (WP 29 2013, 11).

5.3.2 Käsittelyn lainmukaisuus

Tietosuoja-asetuksen (679/2016) artiklassa viisi kuvattujen perusperiaatteiden ensimmäiseen periaatteeseen liittyy käsittelyn lainmukaisuus, kohtuullisuus ja läpinäkyvyys (kohta 1 a). Tätä periaatetta avataan tarkemmin tietosuoja-asetuksen (679/2016) johdantotekstin resitaalissa 30, jossa todetaan, että käsittelyn tulee olla laillista, asianmukaista ja luonnollisille henkilöille läpinäkyvää myös siten. Läpinäkyvyys kattaa tiedottamisen myös käsittelyn riskeistä. (tietosuoja-asetus 679/2016, resitaali 30).

Tietosuoja-asetuksessa luetellut lainmukaisuusperusteet ovat käytännössä ainoat perusteet, joilla henkilötietoa voi käsitellä, eivätkä jäsenvaltiot voi lisätä omiaan. Jo tietosuojadirektiivin voimassaollessa Euroopan tuomioistuin totesi direktiivissä olevan luettelon lainmukaisuusperusteista olevan tyhjentävä, eivätkä jäsenvaltiot voi lisätä uusia periaatteita tai asettaa lisävaatimuksia. (C-582/14, kappale 57). Vaikka jokin jäljempänä luetelluista lainmukaisuusperusteista olisikin olemassa, voidaan käsitellä kuitenkin vain sellaisia tietoja, jotka ovat tarpeen ilmoitetun käyttötarkoituksen ja lainmukaisuusperusteen osalta (C-524/06, kappaleet 59 ja 82). Tarpeellisuudella on oma käsitteensä unionin lainsäädännössä, eivätkä toimijat voi itse venyttää sen rajoja tarpeettomasti (C-524/06, kappale 52). Lainmukaisuusperusteet tietosuoja-asetus määrittelee seuraavasti:

- Suostumus
    - "rekisteröity on antanut suostumuksensa henkilötietojensa käsittelyyn yhtä tai useampaa erityistä tarkoitusta varten"
- Sopimus
    - "käsittely on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena, tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä"
- Lakisääteinen velvoite
    - "käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi"

- Elintärkeät edut
    - ”käsittely on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi”
- Yleinen etu ja julkinen valta
    - ”käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi”
- Oikeutetut edut
    - ”käsittely on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi, paitsi milloin henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut, erityisesti jos rekisteröity on lapsi”

(Lainaukset: Tietosuoja-asetus 679/2016, artikla 6, kohta 1)

Suostumuksen osalta sanamuodossa on pari tärkeää elementtiä. Ensinnäkin rekisteröidyn tulee itse antaa suostumus ja suostumus tulee antaa aina tiettyihin tarkoituksiin. Jo asetuksen määritelmissä on tulkittu suostumuksen olevan vapaaehtoinen, yksilöity, tietoinen ja sisältävän yksiselitteisen tahdonilmaisun (tietosuoja-asetus 679/2016, artikla 4). Vapaaehtoisuus tarkoittaa sitä, että suostumus ei voi olla pakotettu, eikä suostumuksen pyytäjän ja sen antajan välillä voi olla vallan epätasapainoa, joka voisi vaikuttaa suostumuksen vapaaehtoisuuteen (WP 29 2017, 6). Tällainen vallan tasapaino voi olla esimerkiksi työnantajan direktio-oikeuden vuoksi, mutta tätä käsitellään tarkemmin kansallisen työlainsäädännön käsittelyn yhteydessä. Suostumuksen edellytyksiin liitetään myös, että suostumuksen tulee olla informoitu. Se johtuu tietosuoja-asetuksen (679/2016) artiklan seitsemän vaatimuksesta, jossa edellytetään suostumukselta sitä, että se kysytään helposti ymmärrettävässä muodossa ja selkeästi erillään muista asioista sekä ymmärrettävällä kielellä.

Yksilöidyllä suostumuksella viitataan siihen, että suostumuksen pyytäjän on yksilöitävä jokainen henkilötiedon käyttötarkoitus erikseen, siihen liittyvät käsittelytoimet sekä mahdolliset jatkokäyttötarkoitukset ja tarjottava mahdollisuus yksilöidä, mihin suostumus annetaan (tietosuoja-asetus 679/2016, resitaali 32; WP 29 2017, 12-13). Suostumusta ei siis voi antaa yleisesti mihin tahansa tarkoituksiin. Tietoisella tarkoitetaan sitä, että ollakseen pätevä, on suostumusta kerättäessä informoitava vähintään esimerkiksi rekisterinpitäjä, käsittelytoimien tarkoitukset, mitä tietoja käytetään, miten suostumuksen voi peruuttaa ja miten pitkään se on voimassa (WP 29 2017, 14). Yksiselitteisellä tahdonilmaisulla viitataan johonkin konkreettiseen tekoon, jolla suostumus annetaan, eikä suostumus voi perustua valmiiksi rastitettuihin ruutuihin, vaikenemiseen tai jonkin asian tekemättä jättämiseen (tietosuoja-asetus 679/2016, resitaali 32; C-673/17, kappale 65).

Tietosuoja-asetus (679/2016) puhuu myös nimenomaisen suostumuksen käsitteestä, jota käsiteltiin aiemmin erityisten tietoryhmien käsittelyn yhteydessä. Koska tavanomainenkin suostumus on jo aika tiukka muun muassa yksilöintiin liittyvine vaatimuksineen, voidaan päätellä, että nimenomainen suostumus on vieläkin tiukempi. Sitä käytetäänkin usein sellaisissa tilanteissa, joissa on vakava tietoturvariskin mahdollisuus, kun tehdään henkilötietojen siirtoja kolmansiin maihin ilman riittäviä takeita ja automatisoitujen yksittäispäätösten ja profiloinnin yhteydessä. Termillä nimenomainen viitataan suostumuksen antamisen tapaan, josta on selvittävä yksiselitteisesti suostumuksen antaminen. Usein siksi tässä yhteydessä on syytä käyttää esimerkiksi kirjallista allekirjoitettua lausumaa. (EDPB 2020b, 22).

Sopimusperusteiseen käsittelyyn sisältyy sekä sopimuksen valmistelu, että sopimuksen täytäntöönpano. Sopimusperusteisen käsittelyn tärkeimmät elementit ovat, että oikeus käsittelyyn koskee vain sopimuksen osapuolia, sopimus tulee olla olemassa ja sen tulee olla kansallisen sopimuslainsäädännön mukainen (EDPB 2019, 9; WP 29 2014, 16). Sopimusta ei voi tehdä kenenkään toisen puolesta eikä sopimusosapuoleksi voi tulla ilman omaa vaikutustaan, kuten myöhemmin sopimusoikeutta käsitellessä todetaan. Tähänkin lainmukaisuusperusteeseen sovelletaan tietenkin edellä mainittua tarpeellisuusperiaatetta, jonka perusteella tietojen käsittelyn tulee olla objektiivisesti arvioituna tarpeellista sopimuksen täytäntöönpanoa tai valmistelua varten (EDPB 2019, 9). Ei siis ole riittävää, että käsiteltävät tiedot jotenkin liittyvät sopimukseen tai sen valmisteluun (The Data Protection Commission 2019, 11). Johtuen etenkin sopimuksen valmistelun käsitteeseen liittyvästä epämääräisyydestä, tulkitaan tarpeellisuusperiaatetta tiukasti ja arvioinnissa on huomioitava myös sopimusosapuolten odotukset (Kuner et al. 2020, 331-332). Siten tämän käsittelyoikeuden piiriin ei mene käsittely, jota suoritetaan pelkästään toisen tai kolmannen osapuolen aloitteesta tai pyynnöstä ilman ensimmäisen osapuolen osallistamista (EDPB 2019, s14).

Lakisääteisen velvoitteen lainmukaisuusperuste on ehkä helpoin ymmärtää. Aina kun toimijaan – oli kyseessä julkinen tai yksityinen - kohdistuu jokin lakisääteinen velvoite, on henkilötietojen käsittelylle oikeus, siinä määrin kuin velvoitteen täyttäminen edellyttää henkilötietojen käsittelyä. Esimerkiksi palkkatietojen ilmoittaminen sosiaali- tai veroviranomaisille voi olla tällainen. (WP 29 2014, 19). Kyseessä on kuitenkin oltava velvoite, eikä tämä lainmukaisuusperuste kata tilanteita, joissa toimijalla on vain lakiin perustuva lupa tai oikeus käsittelyyn (Kuner et al. 2020, 333). Vain sellaisia tietoja saa käsitellä, mitä kyseinen laki edellyttää käsiteltävän – esimerkiksi kirjanpitolainsäädännön perusteella voidaan käsitellä vain sellaisia tietoja, jotka ovat osa kirjanpitoa ja muut tiedot on poistettava (2477/161/21, 14).

Elintärkeiden etujen suojaamiseen liittyvä oikeusperuste on mahdollinen silloin, kun on kyse ihmisen hengen kannalta olennaisista eduista, esimerkiksi epidemioiden ja katastrofien yhteydessä tai muista vastaavista humanitaarisista syistä (tietosuoja-asetus 679/2016, resitaali 46). Oikeus elämään ohittaa muut perusoikeudet ja tämä lainmukaisuusperuste voi tulla kysymykseen elämään ja kuolemaan liittyvissä tilanteissa, jossa henkilöön kohdistuu konkreettinen ja välittömästi uhkaava vaara (Kuner et al. 2020, 333; WP 29 2014, 20). Tätä lainmukaisuusperustetta ei tulisi kuitenkaan ensisijaisesti soveltaa kolmansien osapuolten elintärkeiden etujen suojaamiseen, vaan nimenomaisesti rekisteröityyn itseensä, jota ollaan suojaamassa (tietosuoja-asetus 679/2016, resitaali 46; EDPB-EDPS joint response 2019, 4).

Henkilötietojen käsittely yleisen edun ja julkisen vallan käyttämiselle on sanamuodoista päätelleen varattu pääsääntöisesti viranomaisille, jotka ovat useimmiten julkisen vallan käyttäjiä. Yksityinen yritys voi kuitenkin toimia yleisen edun mukaan esimerkiksi järjestäessään julkisia palveluita, kuten liikennöintipalveluita tai terveydenhuoltoa (WP 29 2014, 22). Julkisen vallan osalta työssä on jo aiemminkin todettu, että vaikka merkittävän julkisen vallan käyttö voi kuulua vain viranomaiselle, voi yksityinen yritys käyttää toimintansa yhteydessä julkista valtaa. Vartioimisliiketoiminta muun muassa on määritelty Suomessa sellaiseksi, kuten aiemmin todettiin luvussa Edellytykset, toimivaltuudet ja velvollisuudet rikoksen paljastamisessa. Lisäksi tämä lainmukaisuusperuste voi kattaa myös sellaisia tilanteita, joissa esimerkiksi viranomainen rikosta tutkiessaan voisi pyytää yhteistyötä yritykseltä tai yrityksen toimiessa oma-aloitteisesti toimittaessaan tällaisia tietoja viranomaiselle rikoksen havaittuaan (WP 29 2014, 21).

Henkilötietojen käsittelyn on rajoituttava vain sellaisten tietojen käsittelyyn, jotka ovat tarpeen yleisen edun mukaisen tehtävän tai julkisen vallan käyttämiseksi ja jos vähemmän yksityisyyden suojaan puuttuva lainmukaisuusperuste on käytettävissä, on sellaista käytettävä (WP 29 2014, 21-22; Kuner et al. 2020, 336). Maailmalla on kuitenkin erilaisia tulkintoja siitä, onko kaupalliselle toimijalle tultava erityisesti lainsäädännöstä valtuutus vai voiko toimija käyttää tätä lainmukaisuusperustetta muulloinkin. Artiklassa ”tai” sanan käyttö vaikuttaisi viittaavan kuitenkin siihen, että lainsäätäjille on jätetty valta päättää siitä, annetaanko jompaakumpaa oikeutta toimijoille vai ei. (Kuner et al 2020, 336).

Vaikka artiklan tekstissä mainitaan kolmannen osapuolen edut, ei tällä tarkoiteta esimerkiksi muita rekisterinpitäjiä, sillä jokaisen rekisterinpitäjän tulee itsenäisesti perustella henkilötietojen käsittelyssä oikeutensa ja arvioida käsittelyn asianmukaisuus ja oikeasuhtaisuus, että käsittely olisi oikeutettua niiden osalta (C-40/17, kappale 96). Joskus tämä kuitenkin saattaa venyttää vastuuta jopa sopimuskumppanien henkilötietojen käsittelyyn, vaikka käsittelyn perusteet olisi määritelty osapuolten välisellä sopimuksella. Tämä näkyy esimerkiksi Alankomaiden henkilötietojen käsittelyn valvontaviranomaisen (Autoriteit Persoongegevens) päätöksestä Z2015-00062, joka koski Adecco:n tekemää

työntekijöiden taustatarkistamista ja minkä yhteydessä käsitellään rikostuomioihin ja rikoksiin liittyviä tietoja. Adeccolla katsottiin olevan laadukas menetelmä sen varmistamiseen, että sen asiakkaalla taustatarkistuksen teettäjänä on riittävä oikeutettu etu. Päätöksen mukaan Adecco ei voi yksin vedota omaan oikeutettuun etuunsa, vaan sen asiakkaalla tulee täyttyä riittävät perusteet edun käyttämiselle. Sen lisäksi valvontaviranomainen arvioi Adeccon suorittaman käsittelyn riittävän yksityiskohtaisesti suunnitelluksi ja huolelliseksi, että sen avulla voidaan tarjota riittävä käsittelyn kohteena olevien henkilöiden suoja. Myönteistä näkökulmaa käsittelylle puolsi myös se, että erityisen riskialttiita käsittelytoimia varten oli suunniteltu erityiset suojatoimet. (Autoriteit Persoongegevens 2015, 3 ja 5). Tärkeä huomio on kuitenkin se, että Alankomaiden laki on määritellyt tällaisten tietojen käsittelystä erikseen, joten tästä ei voida vetää suoraa tulkintaa suomalaisesta oikeustilasta (Autoriteit Persoongegevens 2015, 1).

Oikeutetun edun käyttäminen lainmukaisuusperusteena ja siitä seuraavat velvoitteet ovat melko hankala ja tulkintaa edellyttävä kokonaisuus, minkä vuoksi pelkästään tämä yksi käsittelyperuste on poikinut viime vuosina muun muassa useita Pro Gradu -tutkielmia (Esimerkiksi Korpisaari 2017, Räsänen 2018, Lukkarinen 2019). Oikeutettu etu on ensinnäkin nimettävä. Etu voi olla esimerkiksi suoramarkkinointi, yrityksen turvallisuuden varmistaminen, petosten ehkäisy tai oikeudellisten vaateiden ajaminen. Edun tulee kuitenkin olla lainmukainen, joten tällä käsittelyperusteella ei voi perustella lainvastaista toimintaa tai pelkkää kaupallista etua. (tietosuoja-asetus 679/2016, resitaali 47; Kuner et al. 2020, 337). Edun tulee myös olla todellinen, eikä henkilötietojen käsittelyä voi oikeuttaa tällä siten, että käsittelyn tuloksena on pelkästään mahdollista tai todennäköistä saavuttaa jokin etu. (WP 29 2014, 25-26). Edellisten lisäksi on muistettava, että henkilötietojen käsittelijän ja käsittelyn kohteena olevien henkilöiden välillä on vallittava jokin asianmukainen suhde, esimerkiksi asiakkuus tai työsuhde (tietosuoja-asetus 679/2016, resitaali 47).

Edellisten lisäksi henkilötietoja käsittelevän on kyettävä osoittamaan, että se on arvioinut oman edun ja käsittelyn kohteena olevien luonnollisten henkilöiden oikeuksien ja vapauksien suhdetta toisiinsa (WP 29 2014, 25). Osoitusvelvollisuudesta johtuen tällä tarkoitetaan kirjallista arviota, koska suullisen arvion toteennäyttäminen jälkikäteen on erittäin ongelmallista. Esimerkiksi seuraamuskollegion päätöksessä 531/161/20 on todettu, että vaikka yhtiö on kertonut arvioineensa käsittelyn riskejä, ei se ole kyennyt osoittamaan sitä kirjallisen arvion puuttuessa, mikä osoittaa myös yhtiön perehtymättömyyttä lainsäädännön sisältöön (14). Kirjallisen muodon vaatimuksen lisäksi oikeuksien tasapaino ei ole pelkästään kahden tekijän keskenään vertailua, vaan se voi olla hyvin monimutkainen ja siinä on otettava huomioon kaikki käsittelyyn liittyvät tekijät (WP 29 2014, 23). Vastaavanlainen tasapainotesti vaaditaan muissakin tilanteissa, esimerkiksi arvioitaessa käsittelyn tarpeellisuutta, suhteellisuutta ja tarkoitussidonnaisuutta (WP 29 2014, 11). Rekisterinpitäjä vastaa itse tarpeellisista arvioista ja niistä seuraavien päätelmien tekemisestä (2477/161/21, 23).

5.3.3 Informointi käsittelystä henkilöille, joiden tietoja käsitellään ja heidän oikeutensa

Henkilötietojen käsittelystä on aina kerrottava käsittelyn kohteena oleville luonnollisille henkilöille läpinäkyvässä ja helposti ymmärrettävässä muodossa jo silloin, kun henkilötietoja kerätään henkilöltä itseltään (tietosuoja-asetus 679/2016, artikla 12, kohta 1 ja artikla 13, kohta 1). Kun henkilötietoja kerätään tai saadaan muualta kuin henkilöltä itseltään, on käsittelystä kerrottava heti, kun henkilöön ollaan ensimmäistä kertaa yhteydessä tai viimeistään 30 päivää tietojen saamisesta (tietosuoja-asetus 679/2016, artikla 14, kohta 3). Tästä on vain joitain poikkeamia, jotka perustuvat tietosuoja-asetuksen (679/2016) artiklan 14 kohtaan 5. Näitä erityistilanteita käsitellään myöhemmin esimerkiksi yhteistoimintalain, tietosuojalain ja viestintäpalvelulain käsittelyn yhteydessä. Kukaan ei siis voi kenenkään tietämättä kerätä henkilötietoja tai viivyttää henkilötietojen käsittelystä tiedottamista siten, että henkilö ei itse olisi käsittelystä tietoinen.

Taustalla on ajatus henkilötietojen käsittelyyn ja yksityisyyteen liittyvästä itsemääräämisoikeudesta: Jokaisen tulee olla tietoinen itseensä liittyvästä henkilötietojen käsittelystä voidakseen käyttää hänelle kuuluvia oikeuksiaan (Kuner et al. 2020, 403–404). Myös sellaisessa tilanteessa, jossa henkilöön liittyviä tietoja kertyy kerättäessä tietoja muualta, on tietojen kerääjä rekisterinpitäjä, joka vastaa luonnollisten henkilöiden suuntaan heidän oikeuksiensa toteuttamisesta. Tällainen tilanne voi olla esimerkiksi, kun tietoja kerätään verkkosivuilta tai teknisillä valvontamenetelmillä. (C-131/12, kappale 34; WP 29 2018, 15). Erityisen tärkeää on tiedottaa myös siitä, mikäli rekisterinpitäjä siirtää tietoja muualle, että henkilöt voisivat käyttää heille kuuluvia oikeuksiaan myös niiden tahojen kohdalla, joille tietoja on siirretty (esimerkiksi C-201/14, kohdat 33, 34, 46).

Käsittelystä tiedottaminen, eli rekisteröidyn informointi, edellyttää rekisterinpitäjältä aktiivisuutta ja aktiivisia toimia (WP 29 2018, 18). Tämä näkyy myös monissa Suomessa annetuissa valvontaviranomaisen päätöksissä, joiden perusteluissa on viitattu asiaan siten, että ”…rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet toimittaakseen rekisteröidylle 15 artiklan mukaiset kaikki käsittelyä koskevat tiedot…” (esimerkiksi päätökset: 3021/452/2017, 3592/152/2019, 3343/163/20). Myös päätöksessä 3813/161/2020 todetaan erikseen, että pelkästään tietojen passiivinen saatavilla pito ja mahdollisuus selvittää henkilötietojen käsittelyn perusteita, ei täytä vaatimusta tiedottamisen aktiivisesta toimittamisvaatimuksesta (9).

Informoinnin yhteydessä annettavista tiedoista on selvä määrittely. Kun tietoja kerätään henkilöistä, on heille kyettävä kertomaan tietosuoja-asetuksen (679/2016) mukaan vähintään (artiklat 13-14):

- Rekisterinpitäjän identiteetti ja yhteystiedot
- Tietosuojavastaavan yhteystiedot

- Käsittelyn tarkoitukset ja oikeusperusteet
- Tahot, joille henkilötietoja siirretään
- EU-alueen ulkopuolelle kohdistuvat siirrot
- Oikeudet, joita henkilöillä on tietoihinsa nähden
- Oikeudesta peruuttaa suostumus
- Oikeus valittaa valvontaviranomaiselle
- Tieto automaattisesta päätöksenteosta ja profiloinnista
- Tietojen mahdolliset jatkokäyttötarkoitukset

Edellisten lisäksi, kun tietoja kerätään suoraan henkilöltä itseltään, tulee lisäksi kertoa, onko tietojen antaminen esimerkiksi lakisääteinen vaatimus tai sopimusedellytys ja mitä seuraa, ellei tietoja luovuta (tietosuoja-asetus 679/2016 13 artikla). Jos tietoja ei ole kerätty henkilöltä itseltään, edellistä ei sovelleta, mutta toinen lisävelvoite tulee sovellettavaksi. Sen mukaan tulee lisäksi tiedottaa siitä, mitä henkilötietoryhmiä on saatu ja mistä lähteistä ne on saatu (tietosuoja-asetus 679/2016, 14 artikla).

Lista on aika pitkä ja Euroopan tietosuojaneuvosto itsekin ymmärtää ristiriidan ymmärrettävyyden ja riittävän informoinnin välillä (WP 29 2018, 18). Jos kaikki tieto toimitettaisiin yhtenä isona pakettina, voisi seurauksena olla se, että henkilö ei kykene sisäistämään koko tietomäärää. Jos taas kaikkea ei kerrottaisi, ei noudatettaisi lakia. Yhtenä ratkaisuna tietosuojaneuvosto ehdottaakin informoinnin vaiheistamista ja tiedon jakamista kerroksiin sellaisella tavalla, että henkilö saa aina vain tarpeellisia tietoja kunkin käsittelyn vaiheen osalta. Esimerkiksi tietojen jatkokäyttö voi selvitä rekisterinpitäjälle itselleenkin vasta tulevaisuudessa. (WP 29 2018, 18-19). Mutta aina kaikissa tapauksissa tulisi tietosuojatyöryhmän mukaan (WP 29 2018, 19) heti tietojen keruun yhteydessä, tai heti kun se on mahdollista, informoida vähintään:

- Käsittelyn tarkoitukset
- Rekisterinpitäjän identiteetti
- Kuvaus henkilöillä olevista oikeuksista

Lisäksi näiden tietojen tulisi sisältää erityisesti tiedot käsittelystä, jolla on eniten vaikutuksia henkilöille, joiden tietoja käsitellään ja tiedot, jotka voivat olla yllättäviä heille (WP 29 2018, 19).

Kun tietoja kerätään henkilöiltä itseltään, ei informointiin ole mitään poikkeusta – muutoin kuin tilanteessa, jossa henkilö jo tietää käsittelystä (tietosuoja-asetus 679/2016, artikla 13, kohta 4). Tällainen tilanne voi tulle kyseeseen esimerkiksi silloin, kun työnantaja on jo tiedottanut esimerkiksi käynnissä olevasta väärinkäytöstutkinnasta tai kertonut työnhakijoille taustaselvityksistä, joita alihankkija heille suorittaa. Tässäkin on kuitenkin huomioitava, että

rekisterinpitäjä on todistusvelvollinen informoinnin suorittamisesta ja voi joka tapauksessa joutua täydentämään informointia tilanteiden muuttuessa (WP 29 2018, 27). Kun tietoja saadaan muilta kuin henkilöiltä itseltään, poikkeuksia hiukan enemmän. Ne ovat:

1. Rekisteröity on jo saanut tiedot
2. Tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa
3. Tietojen hankinnasta tai luovuttamisesta säädetään laissa muuta
4. Tietoihin kohdistuu unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuva vaitiolovelvollisuus, kuten lakisääteinen salassapitovelvollisuus
   (Lähde: tietosuoja-asetus 679/2016, artikla 14, kohta 5)

Ensimmäinen on selvä tilanne. Toinen taas jo tulkinnanvaraisempi. Asetus kuitenkin viittaa tässä tieteelliseen, historialliseen tai tilastolliseen tutkimukseen, jossa henkilötietojen massat voivat olla suuria tai pitkältä ajalta ja yhteystietojen keruu siten mahdotonta (tietosuoja-asetus 679/2016, artikla 14, kohta 5; Kuner et al 2020, 446–447; WP 29 2018, 28-29). Tämä poikkeus ei sovellu kuitenkaan yksityisetsivätoimintaan, koska väärinkäytöksiä ja rikoksia ei paljasteta historiallisista aineistoista tai tilastoista. Kolmas kohta voi soveltua yksityisetsivätoimintaan, mutta sen osalta tulee huomioida, että käsittelystä on nimenomaan säädettävä laissa ja rekisterinpitäjään soveltuu kuitenkin lisävelvoitteita, joita käsitellään myöhemmin tietosuojalakia koskevassa luvussa (C-201/14, kappaleet 40–41 ja 45). Pelkästään luvanvarainen rikoksen paljastaminen ei riittäne poikkeusperusteena informoinnin suorittamatta jättämiselle. Tämä johtuu siitä, että laissa yksityisistä turvallisuuspalveluista ei määritellä rikoksen paljastamisessa tapahtuvaan henkilötietojen käsittelyyn liittyviä suojatoimia, mikä olisi edellytys informoinnista poikkeamiselle (C-201/14, kappale 45). Neljäs tilanne voisi liittyä esimerkiksi siihen, että tutkinnan osalta jouduttaisiin käsittelemään esimerkiksi terveystietoja, jotka ovat työelämän tietosuojalain mukaan salassa pidettäviä. Tätä ja siihenkin liittyviä huolehtimisvelvoitteita käsitellään myöhemmin työelämän tietosuojaa koskevassa luvussa.

Aiemmin todettiin, että informoinnin tärkeys korostuu siksi, että henkilöt voisivat käyttää tehokkaasti heille kuuluvia oikeuksiaan. Tietosuoja-asetuksen (679/2016) 12 artikla velvoittaa rekisterinpitäjiä kertomaan henkilöille edellisten tietojen lisäksi myös heidän oikeuksistaan. Tällä varmistetaan se, että henkilöt tietävät oikeutensa. Sen lisäksi rekisterinpitäjän on helpotettava näiden oikeuksien käyttämistä toimillaan, sekä vastattava kaikkiin oikeuksien käyttöön liittyviin pyyntöihin viimeistään kuukauden kuluessa. Vain perustelluista syistä pyyntöihin vastaamista voi jatkaa enintään kahdella kuukaudella. (tietosuoja-asetus 679/2016, artikla 12, kohdat 1–3; WP 29 2018, 26). Sen lisäksi rekisterinpitäjällä on velvollisuus tiedottaa myös henkilötietoihin kohdistuvista tietoturvaloukkauksista ja nämä sekä edellä mainitut oikeuksien käyttöpyynnöt on pääsääntöisesti ainakin ensimmäisellä kerralla suoritettava maksuttomasti (tietosuoja-asetus 679/2016, artikla 12, kohdat 1 ja 5).

Rekisteröidyille kuuluvat oikeudet on määritelty tietosuoja-asetuksen (679/2016) artikloissa 15-22 ja ne ovat seuraavat:

1. Rekisteröidyn oikeus saada pääsy tietoihin
2. Oikeus tietojen oikaisemiseen
3. Oikeus tietojen poistamiseen
4. Oikeus käsittelyn rajoittamiseen
5. Rekisterinpitäjää koskeva ilmoitusvelvollisuus kaikille tietojen vastaanottajille, kun tietoja on käsitelty edellä olevien kohtien 2 – 4 tarkoituksissa
6. Oikeus siirtää tiedot järjestelmästä toiseen
7. Vastustamisoikeus, kun käsittely perustuu yleiseen etuun tai rekisterinpitäjän tai kolmannen osapuolen oikeutettuihin etuihin
8. Oikeus välttää automatisoituja yksittäispäätöksiä, profilointi mukaan luettuna

Ensimmäinen oikeuksista generoi suhteessa eniten valituksia valvontaviranomaisille (Kuner et al. 2020, 454). Todennäköisesti siksi, että sen laajuutta ei aina ymmärretä, sillä se laajentaa merkittävästi rekisteröidyn oikeuksia saada tietoja itseään koskevien tietojen käsittelystä aiemmin käsiteltyihin artikloihin 13 ja 14 verrattuna. Kyseinen oikeus tarkoittaa sitä, että henkilöillä on tosiasiallinen oikeus saada kopioita ja päivitettyä tietoa itseensä liittyvien tietojen käsittelystä ilmaiseksi (tietosuoja-asetus 679/2016, artikla 15; Kuner et al. 2020, 452). Käytännössä tämä tarkoittaa sitä, että rekisteröidylle tulee toimittaa myös sellaiset tiedot, joita rekisterinpitäjä on itse liittänyt henkilöön myöhemmin kerättyään tästä mahdollisesti muita tietoja (esimerkiksi C-434/16, tuomiotiivistelmän kohta 2). Edellinen on usein edellytys sille, että kukaan voisi esimerkiksi osata pyytää korjata häntä koskevia virheellisiä tietoja, mihin kenellä tahansa on oikeus tietosuoja-asetuksen (679/2016) artiklan 16 mukaan (Kuner et al. 2020, 452).

”Oikeus tulla unohdetuksi” oli tietosuoja-asetuksen voimaan tullessa ehkä tietosuoja-asetuksen eniten keskustelua herättänyt oikeus. Todennäköisesti siksi, että se korosti juuri tämän päivän yhteiskunnan massiivista tiedon tuottamisen ja jakamisen vastapainoksi asetettua oikeutta säilyttää jonkinlainen kontrolli omiin tietoihinsa (Kuner et al. 2020, 477). Kyseinen oikeus ei ole kuitenkaan mitenkään absoluuttinen, vaan sen edellytyksiä on muun muassa, että henkilötiedot eivät ole enää tarpeen tarkoituksiin, joihin ne kerättiin. Tai että rekisteröity peruuttaa suostumuksensa ja käsittely on perustunut suostumukseen. Tai tilanteessa, jossa rekisteröity vastustaa käsittelyä, eikä rekisterinpitäjällä ole esittää painavampaa intressiä tai rekisteröity peruuttaa suostumuksen suoramarkkinointiin tai henkilötietoja on käsitelty lainvastaisesti. (tietosuoja-asetus 679/2016, artikla 17, kohta 1). Toisin sanoen käsittelylle, jolle on osoitettavissa lainmukaisuusperuste, on sellaista henkilötietoa, jota voidaan käsitellä niihin tarkoituksiin, joihin lainmukaisuusperuste voidaan osoittaa.

Rekisteröity voi pyytää henkilötietojensa käsittelyn rajoittamista, jos käsittely on lainvastaista, mutta rekisteröity haluaa tiedot säilytettävän. Tai silloin, kun rekisterinpitäjä ei enää tarvitse tietoja, mutta rekisteröity haluaa ne säilytettävän oikeudellisen vaateen vuoksi. Edellisten lisäksi rajoittamista voidaan pyytää, kun rekisteröity on kiistänyt henkilötietojensa paikkansapitävyyden siksi aikaa, kun rekisterinpitäjä selvittää niiden paikkansapitävyyttä. Tai kun rekisteröity on vastustanut henkilötietojen käsittelyä ja odottaa rekisterinpitäjältä selvitystä vastustamisoikeutensa käytöstä. (tietosuoja-asetus 679/2016, artikla 18, kohta 1; Kuner et al. 2020, 487). Käytännössä kyse on oikeudesta, jolla rekisteröity voi rajata tietojensa käsittelyä väliaikaisesti, kun on kyse sen selvittämisestä, voidaanko käsittelyä jatkaa lainmukaisesti tai kun rekisteröity haluaa tietojaan säilytettävän tilanteessa, jossa sellainen palvelee paremmin hänen etujaan kuin niiden poistaminen (Kuner et al. 2020, 286-487). Kun käsittelyä on pyydetty rajoitettavan, henkilötietoja saa käsitellä vain rekisteröidyn suostumuksella tai oikeudelliseen vaateeseen liittyen tai jos kyse on toisen luonnollisen henkilön tai oikeushenkilön oikeuksien suojaamisesta tai tärkeästä unionin tai jäsenvaltion yleisestä edusta (tietosuoja-asetus 679/2016, artikla 18, kohta 2).

Edellisen luettelon kohdan viisi velvollisuus laajentaa rekisterinpitäjän vastuun ilmoittaa oikaisuista, poistoista ja rajoituksista myös muille tahoille, joille se on tietoja luovuttanut ja ilmoittaa rekisteröidyille näistä tahoista (tietosuoja-asetus 679/2016, artikla 19; Kuner et al. 2020, 493). Kohdan kuusi tietojen siirtoon liittyvä oikeus tulee sovellettavaksi vain, jos tietoja käsitellään suostumukseen tai sopimukseen perustuen ja käsittelyä suoritetaan automaattisesti (tietosuoja-asetus 679/2016, artikla 20, kohta 1). Käytännössä yksityisetsivätoiminnassa tuskin on kovin paljon tilanteita, joissa eri rekisterinpitäjät käsittelisivät tietoja teknisesti yhteensopivilla järjestelmillä, jolloin kyse olisi melko varmasti tilanteesta, jossa tiedot luovutettaisiin sähköisesti luettavassa muodossa rekisteröidylle itselleen (tietosuoja-asetus 679/2016, artikla 20, kohdat 1 ja 2).

Tietojen siirto-oikeus on muutenkin tarkoitettu pääsääntöisesti sovellettavan sähköisiin ympäristöihin ja sähköisten palveluiden tehokkaampaan valintaan (Kuner et al 2020, 499-500). Silloinkin tiedot koskisivat vain sellaisia tietoja, joissa on kyse sopimusosapuolena olevan rekisteröidyn luovuttamista tiedoista tai häntä itseään koskevista tiedoista, joihin suostumus on annettu (Kuner et al 2020, 502). Oikeutta ei myöskään sovelleta tilanteissa, joissa kyse on yleistä etua koskevan tehtävän suorittamisesta tai julkisen vallan käytöstä, eikä oikeuden käyttämien saa haitata muiden oikeuksia tai vapauksia (tietosuoja-asetus 679/2016, artikla 20, kohdat 3 ja 4). Koska luvanvarainen rikoksen paljastaminen on määritelty yleisen edun mukaiseksi tehtäväksi, jossa käytetään julkista valtaa, ei tätä oikeutta sovellettaisi sellaisiin tilanteisiin.

Kohdan seitsemän vastustamisoikeus olisi olemassa luvanvaraisessa rikoksen paljastamisessa, sillä oikeutta voi käyttää aina, kun tietoja käsitellään yleisen edun tai julkisen vallankäytön

mukaisissa tarkoituksissa (tietosuoja-asetus 679/2016, artikla 21, kohta 1). Oikeus koskisi myös esimerkiksi työantajalle suoritettavaa väärinkäytöstutkintaa muissakin kuin luvanvaraisissa rikoksen paljastamiseen liittyvissä tehtävissä, koska niitä suoritetaan usein rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi (tietosuoja-asetus 679/2016, artikla 21, kohta 1). Käsittely on lopetettava, ellei rekisterinpitäjä voi osoittaa, että sillä on huomattavan tärkeä ja perusteltu syy, joka ohittaa rekisteröidyn oikeudet ja vapaudet (tietosuoja-asetus 679/2016, artikla 21, kohta 1). Kohdan 8 oikeus vastustaa automatisoituja yksittäispäätöksiä ja profilointia koskee tilanteita, joissa rekisteröityä koskevat päätökset tai profilointi perustuisivat ainoastaan sähköiseen käsittelyyn (tietosuoja-asetus 679/2016, artikla 22, kohta 1). Tämä voisi tulla kyseeseen esimerkiksi tekoälyn käyttämisessä rikos- tai väärinkäytöstutkinnassa vaikkapa epäiltyjen seulonnassa, mutta luvun neljä taustatiedoista ei mistään ilmene, että yksityissektorilla olisi käytössä tällaisia työvälineitä tai -menetelmiä.

5.3.4 Riskienarvioinnin merkitys henkilötietojen käsittelyssä

Henkilötietoja käsittelevien tahojen on aiempaa paremmin arvioitava itse käsittelyyn liittyvät riskit ja yhdessä aiemmin käsitellyn osoitusvelvollisuuden vuoksi, kirjallisessa muodossa. Näin voidaan täyttää tietosuoja-asetuksen (679/2016) artiklan viisi, kohdan kaksi osoitusvelvollisuus siitä, että riskit on todella arvioitu. Riskin seurauksena aiheutuvan vahingon erityislaatuisuutta ei ole mitenkään rajoitettu esimerkiksi taloudellisiin tai materiaalisiin vahinkoihin. Riskejä arvioitaessa tulee huomioida potentiaaliset henkilötietoihin kohdistuvat loukkaukset hyvin laajasti. Ne voivat olla esimerkiksi yksilön kontrollin menettämistä henkilötietojensa käsittelyyn, yksilön oikeuksien rajoittamista, epätasa-arvoista kohtelua, identiteettivarkaus tai petos. (tietosuoja-asetus 679/2016, resitaali 75; EDPB 2021c, 5).

Riskienarviointi on ensisijaisesti määritelty rekisterinpitäjän vastuulle ja sitä korostaa se, että asiaa käsittelevä artikla on vieläpä otsikoitu nimellä rekisterinpitäjän vastuu. Tämä artikla korostaa, että riskienarvioinnin taustalla tulee olla asetuksen noudattamisesta huolehtiminen ja osoitusvelvollisuus siitä niin teknisin kuin organisatorisin keinoin. (tietosuoja-asetus 679/2016, 24 artikla; Kuner et al. 2020, 557). Myös seuraavassa artiklassa muistutetaan riskienarvioinnin tärkeydestä, mutta se lisää vaatimukseksi myös sen, että rekisterinpitäjällä on vastuu käsittelytoimien määrittämisen yhteydessä ja riskejä arvioitaessa varmistaa myös rekisteröityjen oikeuksien suojaaminen niin käytetyissä järjestelmissä kuin laajemmin käsittelytoimissa (tietosuoja-asetus 679/2016, artikla 25, kohta 1; Kuner et al. 2020, 577). Tietosuoja-asetus edellyttää riskejä arvioitaessa ottamaan huomioon käsittelyn luonteen, laajuuden, asiayhteyden, tarkoitukset, uusimman tekniikan mahdollisuudet ja toteuttamiskustannukset (tietosuoja-asetu 679/2016, artikla 24, kohta 1 ja artikla 25, kohta 1).

Riskeistä riippumatta rekisterinpitäjä vastaa myös siitä, että aina käsitellään vain kunkin tarkoituksen kannalta tarpeellisia henkilötietoja. Tässä on huomioitava käsiteltyjen henkilötietojen lisäksi myös niiden määrä, laajuus, säilytysaika ja saatavilla olo. Erityisesti olisi varmistettava se, että käsiteltävät henkilötiedot eivät olisi rajoittamattoman henkilömäärän saatavilla ilman luonnollisen henkilön myötävaikutusta. (tietosuoja-asetus 679/2016, artikla 25, kohta 2). Parhaiten näiden asioiden osoittaminen onnistuu rekisterinpitäjän ja käsittelijän osalta käsittelytoimien selosteella, johon kuvataan edellisen lisäksi muun muassa käsittelyn tarkoitukset, rekisteröityjen ryhmät, henkilötietoryhmät ja kenelle tietoja luovutetaan. Velvollisuus tehdä seloste käsittelytoimista on käsittelijällä hiukan suppeampi. Molempien on se tehtävä aina tilanteissa, joissa organisaation koko on yli 250 henkilöä tai jos henkilötietojen käsittely ei ole satunnaista, käsittelyssä on todennäköisiä riskejä henkilöiden oikeuksille ja vapauksille tai käsitellään erityisiä tietoryhmiä tai rikoksiin liittyviä tietoja. (tietosuoja-asetus 679/2016, artikla 30; Tietosuojavaltuutetun toimisto 2021a).

Organisaatioiden sisällä voi olla hyvin erilaisia käsittelytoimia ja kaikessa käsittelytoiminnassa riskiarvioista esitetyt huomioonotettavat muuttujat ovat usein hyvin erilaisia. Tästä voidaan päätellä, että jokainen käsittelytoimi edellyttää omanlaisensa riskiarvion, joka kohdistuu aina käsittelytoimien selosteella esitettyyn käsittelyn ryhmään. Joissain organisaatioissa väärinkäytöstutkinta voi olla satunnaista, paitsi jos organisaatiolla on esimerkiksi väärinkäytösten ilmoituskanavat tai muut menettelyt sitä varten olemassa. Sen lisäksi on vaikea argumentoida, ettei väärinkäytöstutkinta aiheuttaisi riskejä kenenkään oikeuksille tai vapauksille tai ettei niiden perusteella voitaisi joutua käsittelemään rikoksiin liittyviä tietoja. Vaikka väärinkäytös ei muodostaisi rikosoikeudellista vastuuta, se voi aiheuttaa työoikeudellisia seuraamuksia, joilla voi olla negatiivinen vaikutus rekisteröidyn oikeuksille ja vapauksille. Väärinkäytös- tai rikostutkintaa suorittavalla käsittelijällä tällainen käsittely ei varmasti ole satunnaista. Riskienarviointivelvoite ei ole kuitenkaan rajattu vain satunnaiseen käsittelyyn.

Käsittelijään kohdistuvia riskienarviointivelvoitteita ei ole yhtä monessa kohdassa tietosuoja-asetuksessa. Tämä johtunee siitä, että rekisterinpitäjä vastaa itse siitä, että se käyttää käsittelijöitä, jotka antavat riittävät takeet tietosuoja-asetuksen noudattamisesta (tietosuoja-asetus 679/2016, artikla 28, kohta 1). Sen lisäksi rekisterinpitäjä vastaa siitä, että se ohjeistaa käsittelijänsä aina henkilötietojen käsittelyssä (tietosuoja-asetus 679/2016, artikla 29). Käsittelijällä kuitenkin on velvollisuus huolehtia myös omaan toimintaansa liittyvistä riskiarvioista. Tämä tulee sitä kautta, että henkilötietojen käsittelijän on toteutettava kaikki tietosuoja-asetuksen (679/2016) artiklan 32 käsittelyn turvallisuuteen liittyvät toimenpiteet (artikla 28). Riskienarviointi on tietosuoja-asetuksen (679/2016) artiklan 32 ensimmäisen kohdan velvoite niin rekisterinpitäjille kuin käsittelijöille. Riskit huomioiden tulee varmistua tietojen salaamisesta, pseudonymisoinnista,

luottamuksellisuudesta, eheydestä ja käytettävyydestä sekä menettelyistä, joilla tietoturvakontrolleja testataan säännöllisesti. (tietosuoja-asetus 679/2016, artikla 32, kohta 1). Lisäksi käsittelijällä tulee olla menettely, jolla varmistetaan, että rekisterinpitäjän ohjeistus on käsittelyä suorittavien saatavilla (tietosuoja-asetus 679/2016, artikla 32, kohta 4).

Tietosuojaviranomaiset eivät lähtökohtaisesti suorita riskien arvioimiseksi itse ennakkotarkastuksia, sillä jälkikäteen tapahtuvan valvonnan on katsottu oleva riittävä menettely (esimerkiksi yhdistetyt tapaukset C-92/09 ja C-93/09, kappale 104). Rekisterinpitäjän onkin itse suoritettava ennakkoon riskiarviot sellaisten käsittelytoimien osalta, joissa etenkin uutta teknologiaa käytettäessä on mahdollisuus korkeaan riskiin rekisteröityjen oikeuksien ja vapauksien kannalta (tietosuoja-asetus 679/2016, artikla 35). Tällaisia käsittelytoimia voidaan paikallisten valvontaviranomaisten suosituksesta listata ennakolta, vaikkakin sellaisten listojen tulisi olla rajallisia (tietosuoja-asetus 679/2016, artikla 35, kohta 4; yhdistetyt tapaukset C-92/09 ja C-93/09, kappale 105). Tietosuojaa koskeva vaikutustenarviointi on myös tärkeä työväline tietosuoja-asetuksen noudattamiseen liittyvän osoitusvelvollisuuden osalta (WP 29 2017c, 4).

Kuten aiemmin todettiin, kaikki riskit on arvioitava yleisesti käsittelytoimien osalta, mutta tietosuojaa koskeva vaikutustenarviointi vain sellaisten tilanteiden kohdalla, joissa on korkean riskin mahdollisuus. Tällaisiksi tilanteiksi tietosuoja-asetus (679/2016, artikla 35, kohta 3) nimeää erityisesti:

1. luonnollisten henkilöiden henkilökohtaisten ominaisuuksien järjestelmällinen ja kattava arviointi, joka perustuu automaattiseen käsittelyyn, kuten profilointiin, ja johtaa päätöksiin, joilla on luonnollista henkilöä koskevia oikeusvaikutuksia tai jotka vaikuttavat luonnolliseen henkilöön vastaavalla tavalla merkittävästi;
2. laajamittainen käsittely, joka kohdistuu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin tietoihin; tai
3. yleisölle avoimen alueen järjestelmällinen valvonta laajamittaisesti.

Lista on siis esimerkinomainen, eikä tyhjentävä ja korkea riski voi sisältyä myös muunlaisiin käsittelytoimiin (WP 29 2017c, 7). Esimerkiksi työpaikalla tapahtuva työntekijöiden työasemien ja internetissä tapahtuvien toimien seuranta voi jo aiheuttaa tarpeen suorittaa tietosuojaa koskeva vaikutustenarviointi (WP 29 2017c, 10). Ja kuten aiemmin todettiin, voi väärinkäytöstutkinnalla olla myös työoikeudellisia seuraamuksia. Näin ollen tietosuojaa koskeva vaikutustenarviointi tulee melko varmasti kyseeseen väärinkäytöstutkinnan yhteydessä tavanomaisten käsittelytoimien riskiarvioiden lisäksi. Tietosuojaa koskevan vaikutustenarvioinnin on sisällettävä systemaattinen kuvaus käsittelytoimista ja tarkoituksista

sekä rekisterinpitäjän oikeutetuista eduista sen taustalla, tarpeellisuuteen ja oikeasuhtaisuuteen liittyvät arviot, henkilöiden oikeuksia ja vapauksia koskevat riskiarviot sekä suunnitellut toimenpiteet, joilla varmistetaan henkilötietojen suoja ja oikeuksien toteutuminen (tietosuoja-asetus 679/2016, artikla 35, kohta 7). Vaikka tietosuoja-asetus (679/2016) ei sisällä määrämuotoa vaikutustenarvioinnin tekemiselle, ovat monien maiden valvontaviranomaiset julkaisseet työkaluja tätä varten (esimerkiksi Tietosuojavaltuutetun toimisto 2021c; CNIL 2021).

Jos tietosuojaa koskeva vaikutustenarviointi osoittaa, ettei rekisterinpitäjä kykene hallitsemaan riskejä riittävällä tavalla, on sen kuultava valvontaviranomaista ennen käsittelytoimien aloittamista (tietosuoja-asetus 679/2016, artikla 36, kohta 1). Viranomaisen kuulemiseksi on rekisterinpitäjän toimitettava sille esimerkiksi tiedot käsittelyyn osallistuvista tahoista, henkilötietojen käsittelyn keinoista ja tarkoituksista, suojatoimenpiteistä riskeihin varautumiseksi sekä itse vaikutustenarviointi (tietosuoja-asetus 679/2016, artikla 36, kohta 3). Tietosuojaa koskevia vaikutustenarviointeja on myös tarkasteltava säännöllisesti, viimeistään kolmen vuoden kuluttua sen tekemisestä (tietosuoja-asetus 679/2016, artikla 35, kohta 11; WP 29 2017c, 12). Suomen valvontaviranomaisen mukaan esimerkiksi jo kahden vuoden välein (Tietosuojavaltuutetun toimisto 2021c).

5.3.5 Käsittelyn roolit tietosuojalainsäädännön näkökulmasta

Tietosuoja-asetuksen roolit ”rekisterinpitäjä” ja ”käsittelijä” ovat Suomen lainsäädännössä 2018 voimaan tulleen asetuksen vuoksi tarkentuneet. Henkilötietolaki viittasi kolmannen pykälän määritelmissä henkilötietojen käsittelijään sivullisen määritelmässä, mutta sen kummemmin käsittelijän roolia tai siihen liittyviä vastuita tai velvollisuuksia ei määritelty (henkilötietolaki 523/1999, 3 §). Kyse on siis Suomessa uusista termeistä. Määritelmien tulkinnasta on annettu monia erilaisia ohjeita. Tahojen määrittely sopimussuhteissa on tärkeää siksi, että niiden perusteella määräytyvät osapuolten lakisääteiset vastuut (EDPB 2021a, 3 ja 7).

Euroopan komissio on tarkentanut termien tulkintaa omilla sivuillaan. Henkilötietojen käsittelyyn liittyviä rooleja on käytännössä kolme – rekisterinpitäjä, käsittelijä tai yhteisrekisterinpitäjä (Euroopan komissio 2021d). Tarkennuksen mukaan rekisterinpitäjä on taho, joka päättää mihin tarkoituksiin ja miten henkilötietoja käsitellään. Ja kun tahoja on useampi, jotka päättävät yhdessä henkilötietojen käsittelyn tarkoituksista ja keinoista, on kyse yhteisrekisterinpitäjyydestä. (EDPB 2021a, 3). Organisaation työntekijät käsittelevät myös henkilötietoja suorittaakseen työnantajansa tehtäviä rekisterinpitäjänä. Käsittelijä -termi ei tässä yhteydessä viittaa tietosuoja-asetuksen artiklan 28 mukaiseen käsittelijärooliin, jossa toinen yhtiö toimisi. Rekisterinpitäjällä työskentelevien työntekijöiden katsotaan

edustavan rekisterinpitäjää, koska he kuuluvat yritykseen ja toimivat sen suorassa määräysvallassa. (EDPB 2021a, 26).

Esimerkiksi osakeyhtiön osalta vastuuta kantaa osakeyhtiölain mukaan omistajien yhtiökokous, jossa voidaan määrätä hallituksen ja toimitusjohtajan toimivallasta (osakeyhtiölaki 624/2006, luku 5, 2 §). Hallitus huolehtii yhtiön hallinnosta ja kantaa siten päävastuun yhtiön toiminnasta (osakeyhtiölaki 624/2006, luku 6, 2 §). Yksittäinen henkilö rekisterinpitäjän palveluksessa ei siis ole rekisterinpitäjä, koska ei voi tehdä päätöksiä rekisterinpitäjän toimivaltaan kuuluvista henkilötietojen käsittelyn keinoista ja tarkoituksista. Omistajavaihdoksessakaan vastuut tietosuojasta eivät jää edellisille henkilöomistajille, vaan uuden omistajan velvollisuus on vastata yhtiön aiemmasta ja senhetkisestä toiminnasta. (2890/161/2021, luku Perustelut). Edes yhtiön asettaminen konkurssiin ei siirrä vastuita konkurssipesälle (2890/161/2021, luku Rekisterinpitäjyydestä).

Rekisterinpitäjyyden määritelmä on yksilöiden suojelemisen vuoksi määritelty tulkittavan laajasti (WP29 2010, 3; C-210/16, kappaleet 26–27; C-131/12, kappale 34; EDPB 2021a, 9). Yhteisrekisterinpitäjyys syntyy silloin, kun kaksi rekisterinpitäjää yhdessä päättää henkilötietojen käsittelyn keinoista tai tarkoituksista (Euroopan komissio 2021d, Mikä on rekisterinpitäjä tai tietojen käsittelijä). Näiden rekisterinpitäjien vastuu ei kuitenkaan ole välttämättä samanlainen eivätkä ne välttämättä suorita käsittelytoimia samalla tavalla tai samassa kohdassa käsittelyketjua, jolloin heidän roolissaan on arvioitava tapauskohtaisesti merkitykselliset asiat. Itse asiassa näillä tahoilla ei tarvitse välttämättä olla edes pääsyä käsiteltäviin henkilötietoihin ollakseen rekisterinpitäjä. (C-40/17, kappaleet 69-70; C-25/17, kappale 75; EDPB 2021a, 3).

Tietosuojadirektiivin aikaan komission asettama tietosuojatyöryhmä (WP 29), nykyinen Euroopan tietosuojaneuvosto (EDPB), on myös julkaissut ensimmäisen kerran vuonna 2010 tarkennukset, miten kyseisiä käsitteitä tulisi tulkita (Opinion 1/2010 on the concepts of "controller" and "processor"). Komissio viittaa edelleen tähän direktiivin aikaiseen ohjeeseen omilla sivuillaan virallisena tulkintaohjeena, vaikka uudemmatkin ohjeet kyseisestä käsittelystä on jo julkaistu. (Euroopan komissio, 2021d). Uusimmat ohjeet kävivät läpi myös julkisen konsultoinnin ennen niiden vahvistamista (EDPB 2021a, 2). Näiden pohjalta syntynyt versio on kuitenkin käsitesisällöltään edelleen hyvin samanlainen kuin vuoden 2010 ensimmäinen tietosuojadirektiivin voimassaoloaikana julkaistu, vaikka käytännön esimerkkejä ja selkeyttäviä vuokaavioita on tullut lisää (esimerkiksi EDPB 2021a, 7-9, 49-51).

Edellä mainittu lausunto jakaa rekisterinpitäjän määritelmän kolmeen eri osatekijään, joiden kautta asiaa on katsottava (WP 29 2010, 7-8):

1. Subjektiivinen näkökulma (“…luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä…”)

2. Mahdollisuus monitahoiseen käsittelyyn (”…joka yksin tai yhdessä toisten kanssa…”)
3. Olennaiset tekijät, jotka erottavat rekisterinpitäjän muista toimijoista (“…määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot…”) (Lainaukset: tietosuoja-asetus 679/2016, artikla 4, kohta 7)

2021 päivitetyt ohjeet jakavat käsitteisiin liittyvät elementit viiteen osaan, mutta sinällään niiden sisältö on samanlainen. Subjektiivisen näkökulman osalta kuitenkin korostetaan sitä, että vaikka määritelmä kuulostaa muodolliselta, niin mikään ei rajoita sitä, kuka voi joutua rekisterinpitäjäksi. Periaatteessa yksi ihminen tai vaikka ryhmä ihmisiä voivat ihan yhtä hyvin täyttää rekisterinpitäjän määritelmän muodostamatta virallista oikeushenkilöä. (EDPB 2021a, 10).

Rekisterinpitäjä on se taho, joka on ensisijaisesti vastuussa tietosuojalainsäädännön noudattamisesta ja jonka vastuulla on myös lainsäädännön noudattamisen osoittaminen (WP 29 2010a, 4; EDPB 2021a, 7-8; tietosuoja-asetus 679/2016, artikla 5, kohta 2). Rekisterinpitäjän status voi kuulua kenelle tahansa ilman, että sitä määrittelisi käsittelyä suorittavan kompetenssi, mikään laki tai sopimus (WP 29 2010, 8-11). Statuksen muodostumisen taustalla korostetaan tosiasiallisten (“factual”) tekijöiden tilaa (WP 29 2010, 8; C-25/17, kappale 66; C-40/17, kappale 70; EDPB 2021a, 9). Kuka tahansa voi siis tosiasiallisten käsittelytoimien perusteella joutua ottamaan tai päättää ottaa rekisterinpitäjän roolin. Jopa yksityishenkilö voi olla esimerkiksi verkkopalvelun ylläpitäjänä sellainen, jos käsittely ei enää mene kotitalouden piiriin suoritettavaan käsittelyyn. (WP 29 2010, 29). Henkilötietojen käsittelyssä keinoista päättäminen ei tarkoita vain teknisiä keinoja tai automaattista tietojenkäsittelyä, vaan ne voivat liittyä myös prosesseihin ja työtapoihin (WP 29 2010, 14).

Rekisterinpitäjän määritelmän täyttyminen ei edellytä henkilötietojen laillista käsittelyä. Asetuksen määritelmä on “...joka […] määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot…”. Se ei sano: “...joka laillisesti […] määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot.” Vaikka henkilötietojen käsittely tai rekisterinpitäjyyden määrittely olisivat lakien tai sopimusten vastaisia, rekisterinpitäjän statuksen ja vastuut voi silti saada. Mikäli tosiasiallisten tekijöiden perusteella taho määrittelee - laillisesti tai laittomasti - henkilötietojen käsittelyn keinot ja tarkoitukset, on häntä pidettävä rekisterinpitäjänä. (WP 29 2010, 9). Näin voi käydä myös yksittäisen työntekijän ylittäessä valtuutensa. Tällöin kuitenkin ensisijaisesti vastuu toiminnasta on työnantajalla, jos kyse on vain erehdyksestä tai ohjeiden puutteesta. (EDPB 2021a, 10). Vaikkei tarkoitus olisi edes käsitellä henkilötietoa, mutta sitä vahingossa päädytään käsittelemään, voidaan käsittelyä suorittava taho lukea rekisterinpitäjäksi (EDPB 2021a, 17).

Rekisterinpitäjyys voi johtua myös lainsäädännöllisestä velvoitteesta. Joko unionin lainsäädäntö tai kansallinen lainsäädäntö voi määritellä suoraan rekisterinpitäjyyden statuksen kuuluvaksi jollekin organisaatiolle – esimerkiksi julkista hallintotehtävää suorittavalle elimelle. Tavallisempaa on kuitenkin se, että laki määrittelee tehtävät ja siten käsittelyn tarkoituksen ja keinot ja nimeää tehtävän jonkun vastuulle. Periaatteessa näitä tehtäviä voisi kuitenkin hoitaa myös yksityinen yritys esimerkiksi terveyspalvelujen tuottajana. (EDPB 2021a, 11). Rekisterinpitäjyyttä ei voi kuitenkaan johtaa muusta kuin tietosuojalainsäädännöstä. Esimerkiksi immateriaalioikeuksien haltijuus tai omistusoikeudet eivät vaikuta mitenkään siihen, miten rekisterinpitäjyys määrittyy (WP 29 2010, 9). Termit ovat sinällään autonomisia ja vaikka muustakin lainsäädännöstä voitaisiin saada apua näiden käsitteiden tulkintaan, tulisi taustalla käyttää vain eurooppalaista tietosuojalainsäädäntöä. Tietosuojalainsäädännön termejä ei erityisesti tulisi sekoittaa esimerkiksi kilpailulainsäädäntöön tai aineettomia oikeuksia koskevaan lainsäädäntöön, vaikka niissä esiintyy samoja termejä. (EDPB 2021a, 9).

Samoin tahojen keskinäiset sopimukset ovat irrelevantteja rekisterinpitäjyyden määräytymisen osalta, eivätkä keskinäiset sopimukset määrää sitä, missä roolissa henkilötietoja käsittelevä taho lainsäädännön näkökulmasta on (WP 29 2010, 9; WP 29 2006, 11). Henkilötietojen käsittelijänkään status ei määräydy esimerkiksi sopimuksiin, käsittelevään tahoon tai sen ominaisuuksiin liittyen, vaan konkreettisten käsittelytoimien perusteella (WP 29 2010, 24). Sopimukset voivat sisältää sellaisia elementtejä, joiden avulla voitaisiin tulkita osapuolten osallisuutta henkilötietojen käsittelyssä. Myös silloin, kun sopimus ei määrittelisi näitä rooleja esimerkiksi tilanteessa, jossa sopimuslausekkein annettaisiin tai rajattaisiin oikeuksia päättää käsittelyn keinoista ja tarkoituksista. (EDPB 2021a, 13). Mutta vaikka sopimus määrittelisikin toisen osapuolen tiettyyn rooliin, voi osapuolen rooli olla tosiasiassa toinen. Esimerkiksi työn suorittaminen alihankkijana ei automattisesti tarkoita, että toimittaja on käsittelijä (EDPB 2021a, 13). Mikään annettu julkinen ilmoituskaan ei määritä rekisterinpitäjän statusta (WP 29 2010, 15).

Käsittelijän määritelmän olennaiset tekijät ovat kaksi elementtiä (WP 29 2010, 24; EDPB 2021a, 25):

1. Käsittelijä on erillinen oikeudellinen taho
2. Käsittely suoritetaan rekisterinpitäjän puolesta

Käsittelijä voi myös olla luonnollinen henkilö tai oikeushenkilö, julkishallinnon elin tai vastaava. Käytännössä määritelmä on hyvin laaja. Toinen edellytys on se, että kyseessä on käsittely, jota suoritetaan rekisterinpitäjän puolesta - ei käsittelijän omiin tarkoituksiin. (Euroopan komissio, 2021d; EDPB 2021a, 3 ja 25). Toisen lukuun ja toisen puolesta henkilötietoja käsitellessä, on kyse kokonaan toisen intressin palvelemisesta ja se on lähellä

oikeudellista termiä “valtuuttaminen” (“delegation”) (WP29 2010, 25; EDPB 2021a, 26). Käsittelyn lainmukaisuus tällaisissa tilanteissa johdetaan rekisterinpitäjän toiminnasta (EDPB 2021a, 26).

Valtuuttamisessa ja sopimuksin voidaan tietenkin luovuttaa myös harkintavaltaa, mutta se ei voi kohdistua olennaisiin keinoihin henkilötietojen käsittelystä päätettäessä, jos halutaan osapuolten pysyvän ennalta sovituissa rooleissa. Vain sopimuksen muotoilulla ei voi tähän vaikuttaa, jos todellisuus on muuta (EDPB 2012a, 13). Olennaisiin keinoihin kuuluu Euroopan tietosuojaneuvoston mukaan (WP29 2010, 16; EDPB 2021a, 15) esimerkiksi päättäminen siitä:

- kenen henkilötietoja käsitellään
- mitä henkilötietoja käsitellään
- miten pitkään niitä käsitellään
- kenellä on pääsy tietoihin

Käsittelijän valtaan voi silti kuulua esimerkiksi päättäminen siitä, millaista laitteistoa tai ohjelmistoa käsittelyssä käytetään, jos käsittely edelleen palvelee vain rekisterinpitäjän etua. (WP29 2010, 16; EDPB 2021a, 15). Yllä olevan listan olennaisten keinojen katsotan olevan tiukasti liitoksissa tarkoituksen määrittämiseen, koska niiden osalta itsenäinen päättäminen voi muuttaa käsittelyn tarkoitusta ja siten esimerkiksi lainmukaisuutta (EDPB 2021a, 15). Esimerkiksi palkkahallintopalveluita tarjoava tilitoimisto ei voi asiakkaansa puolesta päättää, kenelle se maksaa palkkoja asiakkaan tililtä ja miten paljon, vaikka voi päättää siinä käytettävistä tietojärjestelmistä, jolloin tilitoimisto olisi edelleen käsittelijä. Toisaalta tilintarkastuspalveluja tilatessa tarkastuspalvelun suorittaja voi itse päättää miten se auditoinnin suorittaa, mitä tietoja käsittelee ja miten pitkään. Jos tämä tapahtuu täysin ilman asiakkaan ohjeita, on tilintarkastaja todennäköisesti rekisterinpitäjä. Mutta status voi riippua täysin siitä, miten tarkan ohjauksen tilaaja antaa ja mahdollisesti jopa paikallisesta lainsäädännöstä. (EDPB 2021a, 15-16).

Jos käsittelijä käsittelee henkilötietoja yli rekisterinpitäjän valtuutuksen ja ohjeistuksen, on seurauksena se, että tahosta tulee vähintäänkin yhteisrekisterinpitäjä. Tietosuojalainsäädännön näkökulmasta tämä tietenkin tarkoittaa sitä, että rekisterinpitäjille asetettavat vaatimukset on täytettävä. Muita seurauksia voi tulla myös sopimusvapauden piirissä tehtyjen sopimusten perusteella. Mikäli käsittelijä ylittää rekisterinpitäjän ohjeistuksen henkilötietojen käsittelyssä, hänen voi kohdistua myös sanktioita tietosuojalainsäädännön rikkomisesta (EDPB 2021a, 26). Käsittelijän velvollisuus on kuitenkin aina noudattaa rekisterinpitäjän ohjeita (tietosuoja-asetus 679/2016, artikla 28, kohta 10).

Edellä mainittu tilitoimisto voisi esittää ennakolta aiemmin mainittujen olennaisten keinojen osalta tiettyjä palveluun kiinteästi kuuluvia piirteitä. Esimerkiksi säilytysaika voisi olla sidottu

tietojärjestelmään tai pääsy tietoihin tulisi sallia sen kaikille alihankkijoille palvelun tuottamiseksi. Se ei kuitenkaan tekisi vielä siitä yhteisrekisterinpitäjää, koska tilaajalla on kuitenkin mahdollisuus hyväksyä tai olla hyväksymättä tällaisia ehtoja ja ostaa palvelu muualta (EDPB 2021a, 13). Jos tarkoitus olisi silti ainoastaan palkkahallinnon toteuttaminen, olisi asiakas edelleen tarkoituksen osalta ainoa määrittelijä ja tilitoimisto käsittelijä, vaikka se olisi joitain olennaisia elementtejä päässytkin määrittelemään. Ollakseen yhteisrekisterinpitäjiä, tulee kaikkien osapuolten kyetä vaikuttamaan sekä tarkoituksen, että keinojen määrittelyyn. (EDPB 2021a, 19). Myöskään se, että käsittelystä olisi yhteistä, esimerkiksi kaupallista, hyötyä ei tee osapuolista yhteisrekisterinpitäjiä. Jos toimittajalla ei ole käsittelylle mitään omia tarkoituksia, vaan toimittaa pelkästään palveluita maksua vastaan, on toimittaja käsittelijä. (EDPB 2021a, 21).

Käsittelijän rooli on tärkeää määritellä oikein siksi, että tietosuoja-asetus tuo kokonaan uutena asiana suoraan käsittelijään kohdistuvat velvoitteet (EDPB 2021a, 30). Salassapitovelvoitteen olemassaolosta varmistuminen käsittelyä suorittavien osalta ja käsittelyn tietoturvasta varmistuminen sekä rekisterinpitäjän avustaminen lainmukaisuuden toteuttamisessa ovat käsittelijän vastuulla (tietosuoja-asetus 679/2016, artiklat 28 ja 32). Mutta tiukempiakin velvoitteita on: Käsittelijän on esimerkiksi pidettävä käsittelytoimien selostetta vastuullaan olevista käsittelytoimista, nimitettävä tietosuojavastaava tietyissä tilanteissa ja kansainvälisiä henkilötietojen siirtoja koskevat velvoitteet koskevat myös käsittelijää (tietosuoja-asetus 679/2016, artiklat 30, 37 ja luku 5).

Euroopan tietosuojaneuvosto (EDPB) nostaa esiin tapauksen, jossa asiakas valtuuttaa lakitoimiston edustamaan itseään oikeudessa. Tämä mandaatti ei ole erityisesti kohdistettu henkilötietojen käsittelyyn, ja jättää lakitoimistolle merkittävää päätäntävaltaa siinä, mihin tarkoituksiin ja miten se käsittelee henkilötietoja. Asiakasyritys ei ole myöskään ohjeistanut henkilötietojen käsittelyä. Tässä tapauksessa asianajotoimistoa olisi pidettävä käsittelyn rekisterinpitäjänä. (EDPB 2021a, 12). Lakitoimistojen edustustehtävät voivat tosin liittyä hyvin monenlaisiin tapauksiin yritysfuusioista kilpailulainsäädäntöön, joten esimerkistä ei voi tehdä yleistystä kaikkiin toimeksiantoihin. Yksityisetsivä ei todennäköisesti toimisi näin laajalla valtuutuksella luvussa 4 käsiteltyjen esimerkkien pohjalta pääteltynä.

Yhteisrekisterinpitäjien on siis vaikutettava sekä käsittelyn tarkoitukseen, että keinoihin (EDPB 2021a, 19). Tämä voidaan tehdä yhdellä yhteisellä päätöksellä määrittelemällä yhteinen tarkoitus ja keinot. Tai sitten toisiaan täydentävillä päätöksillä pidemmässä käsittelyketjussa. Olennaista on kuitenkin se, että täydentäviä päätöksiä tulee käsitellä suhteessa käsittelyn keinoihin ja tarkoituksiin, ei esimerkiksi kaupallisiin näkökohtiin. Käsittelyn ei tulisi siis olla mahdollista ilman molempien osapuolten osallistumista tarkoitusten ja keinojen määrittelyyn. (EDPB 2021a, 19).

Vaikuttaminen ei edellytä suoraa määräysvaltaa. Pelkästään auktoriteetti, joka ohjaa rekisterinpitäjien toimintaa, voidaan tulkita yhteisrekisterinpitäjäksi. Näin Euroopan unionin tuomioistuin tulkitsi muun muassa tapauksessa Jehovan todistajat vastaan Suomen tietosuojavaltuutettu, jossa uskonnollinen yhteisö katsottiin yhteisrekisterinpitäjäksi, vaikkei jäsenistö luovuttanut sille käsittelemiään henkilötietoja, eikä yhteisö ollut antanut kirjallisia ohjeita tai käskyjä käsittelystä. (C-25/17, kappale 75). Yksityisetsivätoiminnassa palveluja tuottava taho voi olla yhteisrekisterinpitäjä siten esimerkiksi liiton, kattojärjestön tai taloudellisen yhteenliittymän kautta, mikäli se luovuttaisi liian paljon valtaa henkilötietojen käsittelyn tarkoituksista tai keinoista päättämisessä muille. Mikäli kyseessä olisi rikoksen paljastaminen, tulisi tästä olla sovittuna myös toimeksiantosopimuksella, koska sitä voitaisiin keinoista riippuen tulkita alihankintasuhteeksi (laki yksityisistä turvallisuuspalveluista 1085/2015, luku 6, 80 §).

Yhteisrekisterinpitäjien on sovittava yhteisesti avoimella järjestelyllä lainsäädännön noudattamisen vastuista ja keskinäisistä vastuista ja velvoitteista rekisteröityjä kohtaan ja kerrottava käsittelystä avoimesti (Tietosuoja-asetus 679/2016, artikla 26; Kuner et al. 2020, 587; EDPB 2021a, 18). Tämä tarkoittaa sitä, että osapuolet sopivat selvästi rekisterinpitäjille kuuluvien velvoitteiden täyttämisestä ja työnjaosta niiden osalta. Niihin kuuluu esimerkiksi tietosuojaperiaatteiden toteuttaminen ja sen osoittaminen, lainmukaisuusperusteista huolehtiminen, turvallisuusjärjestelyistä sopiminen ja aiemmin mainitut riskiarviot ja tietosuojaa koskevat vaikutustenarvioinnit. (EDPB 2021a, 44–45). Käytännössä informoinnin rekisteröityjen suuntaan tulee sisältää konkreettisia ohjeita – esimerkiksi selkeä määrittely siitä, kuka on vastuussa järjestelystä ja käsittelystä informoinnista ja mikä on rekisteröidyn kontaktipiste, kun hän haluaa käyttää hänelle kuuluvia oikeuksiaan (EDPB 2021a, 47). Yksityisetsivien toimeksiannoissa, joissa kyse on pelkästään toisen intressin palvelemisesta, ei yhteisrekisterinpitäjyys olisi todennäköinen tilanne, joten asiaa ei käsitellä sen enempää, vaikka se onkin melko varmasti rooleista monimutkaisin ja monitulkinnallisin.

Eri organisaatiot voivat olla eri roolissa eri käsittelyn vaiheissa. Tietosuoja-asetuksen (679/2016) mukaan henkilötietojen käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin (artikla 4, kohta 2). Koska henkilötietojen käsittelyketjussa voi olla useita toimintoja, voi eri toiminnoissa olla eri roolit eri käsittelijöillä. Koko ketjun osalta tulee huolellisesti varmistua siitä, ettei kyse ole vain toimintojen sarjasta, jotka kuitenkin kaikki tähtäävät samaan tarkoitukseen yhdessä sovituilla keinoilla. (EDPB 2021a, 17). Jos yritys ostaisi toiselta alihankintana esimerkiksi tutkimuksen, jonka tarkoitukset ja keinot se määrittelisi tiukasti, jättäen vain vähän harkintavaltaa toimittajalle, olisi tutkimuksen tilaaja rekisterinpitäjä ja toimittaja käsittelijä. Jos taas yritys tilaisi alihankintana tutkimuksen, jossa toimittaja päättäisi vapaasti tutkimuksen menetelmistä, tulosten jatkohyödyntämisestä ja käytettävistä henkilötiedoista

saaden vain anonyymin tilaston, olisivat molemmat itsenäisiä rekisterinpitäjiä. (EDPB 2021a, 17-18).

Ainoa tapa tunnistaa rekisterinpitäjä on pohtia sitä tahon vaikutuskeinojen ja -mahdollisuuksien kautta, joihin liittyy muun muassa oikeustoimikelpoisuus, toimivalta tai tosiasialliset vaikuttamismahdollisuudet (WP29 20110, 10-12; EDPB 2021a, 9). Mitä enemmän keinoja vaikuttaa käsittelytoimien tarkoitukseen ja keinoihin, sen todennäköisemmin on rekisterinpitäjä. Rekisterinpitäjä - käsittelijäsuhteissa on tietenkin voitava olla jonkinlainen liikkumavara keinojen määrittelyssä, mutta jos ei yhtäkään keinoa tunnisteta mahdollisuuksissa vaikuttaa henkilötietojen käsittelyn keinoihin ja tarkoituksiin, ei voi olla kyse rekisterinpitäjästä (WP29 2010, 12).

Kuten luvun alussa todettiin, on rekisterinpitäjä aina ensisijaisesti vastuussa käsittelytoiminnasta ja velvoitteista. Yhteisrekisterinpitäjät niiltä osin kuin käsittelytoimet kuuluvat heidän vastuulleen ja miten järjestelyistä on sovittu. Käsittelijät siltä osin kuin heitä on ohjeistettu tai heidän kanssaan on sovittu. Osapuolet voidaan vapauttaa vastuista ainoastaan, jos ne voivat itse osoittaa, etteivät ole millään tavalla vastuussa vahingoista. Jos henkilötietojen käsittelyketjussa olevat osapuolet ovat vähäisessäkään määrin vastuussa vahingoista tai eivät voi osoittaa vastuuvapauttaan, ne ovat vastuussa koko vahingosta riippumatta osallisuudestaan. Tällä pyritään varmistamaan se, että rekisteröidyt saavat kaikissa tilanteissa korvauksen. (tietosuoja-asetus 679/2016, 82 artikla).

Esimerkiksi sakkopäätöksessä tietoturvallisuuden laiminlyöntien osalta hallinnollinen seuraamusmaksu kohdennettiin useampaan yritykseen siitä huolimatta, että kyse oli vain yhtä osakeyhtiötä koskevasta laiminlyönnistä. Seuraamuskollegio katsoi tässä tapauksessa yritysten muodostavan sekä keskittyneen päätöksentekovallan, että toisiaan taloudellisessa mielessä täydentävän palvelukokonaisuuden vuoksi taloudellisen yksikön ja kohdensi seuraamusmaksun kaikille kolmelle konserniyhtiölle. (4282/161/21 2021, kappale Hallinnollisen seuraamusmaksun kohdentaminen).

5.3.6 Henkilötietojen käsittely sopimussuhteessa

Tässä käsitellään ainoastaan henkilötietojen käsittelyyn liittyvää sopimusvelvoitetta. Myöhemmin luvussa Sopimusoikeus käsitellään muuta sopimussuhteessa sopimusosapuoliin sovellettavia ja huomioon otettavia seikkoja. Tietosuoja-asetuksen edeltäjä tietosuojadirektiivi ei määritellyt vielä mitään henkilötietojen käsittelyyn osallistuvien eri osapuolten välisen sopimuksen sisällöstä. Sopimuksen sisällön määrittely katsottiin kuitenkin tarpeelliseksi, koska tietosuoja-asetus asettaa enemmän vastuita käsittelijöillekin muun muassa vahinkovastuun muodossa. Tietosuoja-asetuksen (679/2016) artikla 28 määrittelee vastuita myös kansainvälisistä siirroista, minkä vuoksi niitä käsitellään myös tässä luvussa. (Kuner et al. 2020, 602). Kyseessä on siis tietosuoja-asetuksen tuomia uusia muutoksia.

Kaikkea käsittelijän rekisterinpitäjän puolesta suorittamaa henkilötietojen käsittelyä on aina ohjattava sopimuksella ja sopimuksen tulee olla kirjallinen ja sitova (tietosuoja-asetus 679/2017, artikla 28; EDPB 2021a, 4 ja 31). Sanamuodossa on huomioitava ”rekisterinpitäjän puolesta” suoritettava käsittely. Pelkästään osapuolten välinen sopimus ei siis tarkoita, että tietosuoja-asetuksen vaatima henkilötietojen käsittelysopimus olisi tehtävä, ellei kyse ole tilanteesta, jossa joku osapuolista käsittelisi toisen puolesta henkilötietoja. Tavanomaisessa palveluiden tai tavaran toimituksissa ei aina käsitellä toisen puolesta henkilötietoja, vaan pelkästään rekisterinpitäjän omiin tarkoituksiin tavaroiden tai palveluiden toimittamiseksi tai laskuttamiseksi.

Yhteisrekisterinpitäjyys vähän poikkeaa sopimusvelvoitteen osalta tietosuoja-asetuksen sanamuodossa. Asetus ei suoraan edellytä sopimusta, mutta se edellyttää sitä, että osapuolet ”määrittelevät keskinäisellä järjestelyllä läpinäkyvällä tavalla kunkin vastuualueen tässä asetuksessa vahvistettujen velvoitteiden noudattamiseksi” (tietosuoja-asetus 679/2017, artikla 26). Tämä keskinäinen järjestely tulkitaan kuitenkin usein vähintään osapuolten väliseksi sopimukseksi (Euroopan komissio 2021d, Mikä on rekisterinpitäjä tai tietojen käsittelijä?). Myös tietosuojaneuvosto edellyttää järjestelyltä jonkinlaista lain tai sopimussuhteiden kautta muodostuvaa sitovuutta (EDPB 2021a, 46).

Sopimus on erittäin tärkeä elementti, koska toisinaan siihen perustuu kokonaan henkilötietojen käsittelyn lainmukaisuus. Jos sopimus puuttuu, on kyseessä vain tietosuoja-asetuksen (679/2016) artiklan 28 rikkominen, koska osapuolten välisen suhteen analyysi tehdään tosiallisten käsittelytoiminen pohjalta, kuten edellisessä luvussa todettiin. Mutta esimerkiksi palveluita tarjotessa käsittelijän lainmukaisuusperuste johdetaan kokonaan rekisterinpitäjän määrittelemästä tarkoituksesta ja siihen liittyvästä lainmukaisuusperusteesta. Palveluntarjoajalla ei olisi oikeutta käsitellä henkilötietoja ilman rekisterinpitäjää ja osapuolten välistä sopimusta palveluiden tuottamisesta. (EDPB 2021a, 32).

Sopimuksilla on tietosuoja-asetuksen (679/2016) 28 artiklan ja Euroopan tietosuojaneuvoston (EDPB 2021a, 34 – 35) mukaan oltava seuraavat elementit:

1. Käsittelijän takeet tietosuoja-asetuksen noudattamiseksi
2. Sopimuksella määritellään:
    a. käsittelyn kohde ja kesto
    b. käsittelyn luonne ja tarkoitus
    c. henkilötietojen tyyppi ja rekisteröityjen ryhmät
    d. rekisterinpitäjän velvollisuudet ja oikeudet
3. Sopimuksen tulee sitoa käsittelijä rekisterinpitäjään juridisesti riittävällä tavalla

4. Velvoittaa käsittelijän käsittelemään henkilötietoja ainoastaan rekisterinpitäjän antamien dokumentoitujen ohjeiden mukaisesti
5. Sopimaan alikäsittelijöiden (alihankkijat) käytöstä ja määritellä niihin menettelyt ja käytön edellytykset
6. Sopimaan kansainvälisten siirtojen toteuttamisesta ja siirtomekanismien toteuttamisvastuista
7. Salassapitovelvollisuuden varmistaminen
8. Sitouttaa käsittelijä riittäviin tietoturvamenettelyihin
9. Rekisteröidyn oikeuksien käyttöön liittyvät reunaehdot
10. Määritellä tietoturvaloukkausten ilmoittamiseen ja tietosuojaa koskeviin vaikutustenarviointeihin liittyvät velvoitteet
11. Tietojen käsittelyn määrittely sopimuksen päätyttyä, mitä henkilötiedoille tapahtuu
12. Auditoinnit, tarkastukset, niihin osallistuminen ja kustannusvastuiden ja velvoitteiden jakautuminen

Ensimmäisen kohdan osalta joissain vanhoissa tietosuoja-asetuksen käännöksissä sanotaan vielä, että ”…rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka toteuttavat riittävät suojatoimet […] niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu.” (tietosuoja-asetus 679/2016, artikla 28, kohta 1). Tällä muotoilulla korostui edellisen luettelon kohdan 12 auditoinnit ja tarkastukset, joihin rekisterinpitäjällä on oikeus. Siksi että se voisi arvioida toteuttavatko käsittelijät todella käytännössä riittävät suojatoimet. Muotoilu kuitenkin korjattiin 3.4.2021 vastaamaan englanninkielistä käännöstä ja kuuluu nyt: ”…rekisterinpitäjä saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka antavat riittävät takeet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu.” (oikaisu tietosuoja-asetukseen 679/2016 2021, kohta 110).

Uudessa muotoilussa korostuu sopimuksen velvoittavat elementit ja erilaisten tietoturvaan liittyvien ohjeiden ja määrittelyjen olemassaolo. Toisin sanoen niiden takeiden, joiden avulla käsittelijä voi todistaa noudattavansa asetusta. Käsittelytoimia voi olla hyvin monenlaisia ja takeiden osalta on aina tehtävä tapauskohtainen arvio. Olennaisia elementtejä käsittelijää arvioitaessa ovat käsittelijän asiantuntemus esimerkiksi turvallisuusmenettelyistä, käsittelijän luotettavuus ja sen resurssit. Maineellakin saattaa olla merkitystä ja arvioinnissa voidaan ottaa huomion esimerkiksi käsittelijän tietoturvallisuuteen tai tietojen käsittelyyn liittyvät auditointiraportit ja sertifioinnit. Takeiden tulisi kuitenkin olla sellaisia, jotka voidaan osoittaa toteen rekisterinpitäjää tyydyttävällä tavalla, että ne voitaisiin huomioida. (EDPB 2021a, 31). Käsittelijä vastaa itseen kohdistuvien velvoitteiden kohdistamisesta omiin alihankkijoihinsa vähintään saman tasoisina (tietosuoja-asetus 679/2016, artikla 28, kohta 4).

Aiemmin esitetyn sopimusvaatimusluettelon kohdat ovat ikään kuin yläotsikoita asioista, jotka tulee huomioida, mutta niiden toistaminen sellaisenaan sopimuksella ei muodosta riittävää sopimusta. Sen sijaan sopimuksesta tulisi käydä ilmi, mitä luettelon kohtien osalta on sovittu osapuolten välillä ja miten asiat on sovittu hoidettavaksi. (EDPB 2021a, 34). Toimeksiantoja ajatellen olisi edellä oleva lista nähtävä siis muistilistana siitä, mistä osapuolten tulee sopia. Listan kohta kolme, juridinen sitovuus, on siis ajateltava siten, että miten osapuolet näyttävät toteen sopimuksen sitovuuden: Jos osapuolilla ei ole korvausvelvollisuuksia toisiaan kohtaan tai kaikki vahingonkorvausvastuut on rajattu pois, onko sopimus sitova? Kohta neljä edellyttää sitä, että ohjeet ovat todella olemassa ja ne on kommunikoitu osapuolten kesken (EDPB 2021a, 35-26). Samoin kohta 11 edellyttää sitä, että on todella sovittu käytännön prosessista, miten henkilötietojen kohtalosta päätetään sopimuksen päättyessä (EDPB 2021a, 40).

Vakiomuotoisen kaikkiin tilanteisiin sopivan sopimuksen laatiminen ei ole mahdollista, koska sopimus tulisi luoda aina tiettyä käsittelytoimintaa ajatellen (EDPB 2021a, 34). Usein tämä ei ole mahdollista siksikään, että sopimuksella on määriteltävä muun muassa ”…käsittelyn kohde ja kesto, käsittelyn luonne ja tarkoitus, henkilötietojen tyyppi ja rekisteröityjen ryhmät…” sekä rekisterinpitäjän velvollisuudet ja oikeudet (tietosuoja-asetus 679/2017, artikla 26). Nämä eivät ole kaikissa yksityisetsivien toimeksiannoissa samoja, kuten toimeksiantojen analyysissä havaittiin. Vakiomuotoisuutta on mahdollisuus noudattaa johonkin asti, mutta esimerkiksi edellä mainitut seikat voivat olla muuttuvia. Tämän vuoksi monissa vakiomuotoisissa sopimusehdoissa yksityissektorilla ja julkishallinnossa on aina erikseen ohjeistettu myös näiden muuttujien kuvaamisesta joko liitteillä tai erillisillä asiakirjoilla sopimuksessa (esimerkiksi IT 2018 käyttöohje, 18; JUHTA 2018, sivu 1).

Kaikkia kohtia ei ole tarkoituksenmukaista analysoida erikseen. Mutta pari kohtaa edellisten lisäksi kaipaa tarkennusta. Molemmat johtuvat yksityisetsivätoimeksiantojen luonteesta. Edellä olevan luettelon kohdan 12 osalta on mainittu kustannuksista sopiminen auditointien ja tarkastusten osalta. Koska yksityisetsivien toimeksiannoissa on kyse aina ostettavasta palvelusta, on palvelusta aiheutuvista kustannuksista hyvä sopia. Tietosuoja-asetus on muiltakin osiltaan sellainen, että se luettelee eri osapuolten vastuut ja velvollisuudet, mutta se ei ota kantaa siihen, miten kustannukset jaetaan. Tässä kohtaa Euroopan tietosuojaneuvosto on katsonut kuitenkin tarpeen ohjeistaa niistä tarkemmin. Kustannukset voivat määräytyä kaupallisten näkökohtien perusteella. Niiden ei kuitenkaan tulisi olla sen luontoisia, että ne olisivat suhteettoman suuria siten, että ne rajoittaisivat jommankumman osapuolen mahdollisuutta turvautua artiklan 28 suomiin oikeuksiin tai että ne tekisivät oikeuksien käyttämisestä puhtaasti teoreettista (EDPB 2021a, 41). Tätä rikkova sopimus voitaisiin tulkita pätemättömäksi, jonka jälkeen oltaisiin tilanteessa, jossa vaadittavaa sopimusta ei ole tai sopimusta ei voitaisi tulkita tarpeeksi sitovana.

Toinen huomioitava asia ja edellisen luettelon kohta 11 liittyy henkilötietojen säilyttämiseen. Tietosuoja-asetuksen mukaan käsittelijällä ei ole muuta mahdollisuutta kuin palauttaa tai poistaa käsittelemänsä henkilötiedot sopimuksen määrittelemän käsittelyn päätyttyä (tietosuoja-asetus 679/2016, artikla 28, kohta 3 g). Henkilötiedon piiriinhän kuuluu kaikki luonnollisiin tunnistettaviin henkilöihin liittyvä tieto (tietosuoja-asetus 679/2016, artikla 4, kohta 1). Siten yksityisetsivälle ei voi käsittelijänä jäädä kehenkään rekisterinpitäjän puolesta käsiteltyyn luonnolliseen henkilöön liitettäviä tietoja kuin siksi ajaksi, mitä rekisterinpitäjä sopimuksella on määrittänyt.

Kolmas huomioitava asia on kansainvälisten siirtojen toteuttaminen, joka saattaa usein tapahtua jopa vahingossa. Tämä on syytä käsitellä tarkemmin siksi, että yksityisetsivien toiminta todettiin jo aiemmin olevan kansainvälistä. Henkilötietojen käsittelyn määritelmässä on mainittu käsittelynä muun muassa henkilötietojen asettaminen saataville (tietosuoja-asetus 679/2016, artikla 4 ja 44). Siirrettäessä tietoja esimerkiksi yhdysvaltalaiseen pilvipalveluun, ne usein asetetaan siellä ylläpitäjän saataville. Siten kyseessä on siirto kolmanteen maahan, jossa ei olla enää eurooppalaisen lainsäädännön piirissä. Henkilötietojen siirto ja saataville asettaminen on määritelmällisesti yhtenevä myös laissa henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018, 32 §, kohta 6). Tietoja voidaan vapaasti siirtää Euroopan talousalueella, mutta kun henkilötietoja siirretään suoraan tai myöhemmän käsittelyn kautta edelleen kolmanteen maahan tai kansainväliselle järjestölle, tulee siirrossa noudattaa tietosuoja-asetuksen viidettä lukua (tietosuoja-asetus 679/2016, artikla 44; EDPB 2021d, 3). Kansainvälisellä järjestöllä tarkoitetaan järjestöä tai sen osaa, johon sovelletaan kansainvälistä julkisoikeutta, tai joka on perustettu kahden tai useamman maan välisellä sopimuksella ilman, että tietojen tarvitsee fyysisesti sijaita EU-alueen ulkopuolella (tietosuoja-asetus 679/2016, artikla 4, kohta 26).

Luvun viisi tarkoituksena on taata saman tasoinen henkilötietojen suoja kolmansissa maissa kuin mitä niillä on ETA-alueella (tietosuoja-asetus 679/2016, resitaali 108 ja artikla 44; EDPB 2021d, 3-4). Henkilötietojen siirto on kyseessä, kun rekisterinpitäjään tai käsittelijään sovelletaan tietosuoja-asetusta ja kun se siirtää henkilötietoja toiselle rekisterinpitäjälle, yhteisrekisterinpitäjälle tai käsittelijälle ja tietojen vastaanottaja on kolmannessa maassa tai kansainvälinen järjestö (EDPB 2021d, 4). Tietojen siirrosta on informoitava rekisteröidyille vähintään kolmansien maiden nimet (WP 29 2018, 38). Käytännössä tällainen siirto edellyttää Euroopan tietosuojaneuvoston mukaan (EDPB 2021e, 3–4) kuusiportaista arviota:

1. Tietojen siirtojen kartoitus
2. Siirron perusteena olevien asianmukaisten suojatoimien varmistaminen
3. Kohdemaan lainsäädäntötason ja henkilötietojen käsittelyn käytäntöjen arviointi
4. Lisäsuojakeinojen tunnistaminen ja valinta
5. Lisäsuojakeinojen käyttöönottoon liittyviin menettelyihin ryhtyminen

6. Henkilötietojen suojan tason uudelleenarviointi säännöllisesti

Koko arviointi tulee olla tehty huolellisesti ja kirjallisessa muodossa. Tämä johtuu tavanomaisen osoitusvelvollisuuden lisäksi siitä, että valvontaviranomainen voi pyytää sitä nähtäväksi ja arviolla voi olla vaikutuksia vastuiden osalta. (EDPB 2021e, 4).

Siirtojen kartoituksen perustana voi käyttää esimerkiksi tietosuoja-asetuksen 30 artiklan tarkoittamaa käsittelytoimien selostetta. Kartoituksessa tulee huomioida esimerkiksi alihankintaketjussa myös tietojen vastaanottajien suorittamat mahdolliset siirrot edelleen muille käsittelijöille, vaikka suora alihankkija toimisikin EU-alueella. Samoin niissä on huomioitava myös tilanteet, joissa tiedot fyysisesti eivät siirry, mutta ovat saatavilla kolmansissa maissa toimiville alihankkijoille; esimerkiksi tukipyyntöjen toteuttamiseksi ylläpitotoimissa. (EDPB 2021e, 10 – 11).

Siirtoihin käytettävissä olevat suojatoimet ovat tietosuoja-asetuksen (679/2016) artiklan 45 (kohta 3), artiklan 46 (kohta 2) ja artiklan 49 mukaan:

1. komission tekemä päätös kohdemaan tietosuojan riittävästä tasosta
2. viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline
3. 47 artiklan mukaiset yritystä koskevat sitovat säännöt
4. komission 93 artiklan 2 kohdassa tarkoitettua tarkastelumenettelyä noudattaen antamat tietosuojaa koskevat vakiolausekkeet tai tietosuojaa koskevat vakiolausekkeet, jotka tietosuojaviranomainen vahvistaa ja jotka komissio hyväksyy
5. 40 artiklassa tarkoitetut hyväksytyt käytännesäännöt yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa
6. 42 artiklassa tarkoitettu hyväksytty sertifiointimekanismi yhdessä kolmannen maan rekisterinpitäjän tai henkilötietojen käsittelijän sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa
7. Erityistilanteita koskevat poikkeamat

Voimassa olevia käytännesääntöjä ja hyväksyttyjä sertifiointimekanismeja ei ole tällä hetkellä ja niistä on vasta kaksi pilvipalveluja koskevaa käsitelty Euroopan tietosuojaneuvoston toimesta (EDPB 2022, Code of conduct). Aiemmin siirrot Yhdysvaltoihin perustuivat niin sanottuun Privacy Shield -järjestelyyn, joka takasi riittävät suojakeinot. Tämä järjestely kuitenkin kumottiin heinäkuussa 2020 Euroopan tuomioistuimen toimesta, koska se ei taannut riittävää suojaa viranomaisten suorittamalta käsittelyltä. (EDPB 2020c, 5). Samassa yhteydessä lisäsuojakeinojen määrittely tuli tarpeelliseksi, koska kohdemaan viranomaiset eivät ole vakiomuotoisten sopimuslausekkeiden osapuolia, eivätkä ne siten sido niitä (EDPB 2021e, 7).

Koska yksityisetsivät ovat pääsääntöisesti pieniä yrityksiä, eivätkä monikansallisia yhtiöitä, niillä ei todennäköisesti ole yrityksiä koskevia sitovia sääntöjä (EDPB 2018b, 15). Sen lisäksi yksityisetsivä on usein palkattu toimeksisaaja, joihin ei tällaista säännöstöä sovellettaisi, vaikka toimeksiantajalla sellaiset olisivat. Sen vuoksi edellisiä ei käsitellä tässä työssä pidemmälle. Jäljelle jääviä asianmukaisia suojatoimia ovat käytännössä luettelon kohdat yksi, neljä ja seitsemän. Ensimmäinen niistä on helpoin. Kun Euroopan komissio on tehnyt kohdemaasta riittävyyspäätöksen, voidaan henkilötietoja siirtää nimettyjen maiden välillä niihin liittyvät rajoitukset huomioiden. Rajoitukset ja päätökset ovat luettavissa Euroopan komission sivuilta. (Euroopan komissio 2021e).

Neljäs kohtaa viittaa komission laatimiin vakiomuotoisiin sopimuslausekkeisiin. Ne uusiutuivat kesäkuussa 2001 ja siirtymäaika niiden käyttöönotolle on jo ohi. Uusissa sekä vanhoissa sopimuksissa tulisi olla pohjalla uudet julkaistut lausekkeet. (Komission hyväksymät vakiolausekkeet 2022). Sopimuslausekkeita voi käyttää hyvin monenlaisissa erilaisissa tilanteissa ja eri rooleissa. Käytännössä kaikkiin tilanteisiin sopivat löytyvät, oli kyse sitten kolmanteen maahan sijoittuneen toimeksiantajan palvelemisesta, kolmanteen maahan sijoittuneen käsittelijänä toimivan alihankkijan alihankkijana toimimisesta tai kolmanteen maahan sijoittuneen käsittelijän käyttämisestä esimerkiksi omien pilvipalveluiden toimittajana (Komission hyväksymät vakiolausekkeet 2022).

Seitsemäs kohta, erityistilanteita koskevat poikkeukset, ovat juuri sitä, miltä ne kuulostavat. Ne liittyvät erityistilanteisiin, joissa ei ole käytettävissä muita asianmukaisia suojatoimia (tietosuoja-asetus 679/2016, artikla 49, kohta 1; EDPB 2018b, 4). Sen poikkeuksenomaisuuden vuoksi sitä tulkitaan lisäksi suppeasti, ettei poikkeuksen käytöstä tulisi säännönmukaista (EDPB 2018b, 4). Jokaisen poikkeuksen osalta on aina suoritettava tarpeellisuustesti sen osalta, onko kyseisten tietojen siirto todella tarpeen niihin tarkoituksiin ja niillä lainmukaisuusperusteilla, joilla siirto tehdään (EDPB 2018b, 5). Sen lisäksi siirtäjä vastaa myös siitä, että kaikkia muita tietosuoja-asetuksen velvoitteita noudatetaan ja rekisteröidyille taataan samanlainen suojan taso kuin muissakin tilanteissa (EDPB 2018b, 3). Tämä siirtoperuste ei siis vapauta mistään muusta vastuusta ja poikkeusluontoisuuden vaatimuksen lisäksi lisää myös hallinnollista taakkaa. Poikkeusluontoisuuden vaatimuksen vuoksi se ei myöskään sovellu käytettäväksi liiketoiminnassa.

Ensimmäisenä poikkeuksena on mainittu siirto rekisteröidyn nimenomaisella suostumuksella, kun hänelle on ensin informoitu siirron riskeistä (tietosuoja-asetus 679/2016, artikla 49, kohta 1 a). Nimenomaisen suostumuksen käsite purettiin jo aiemmin, mutta tässä lisätään sen lisäksi vielä vaatimukseksi suostumuksen kohdentaminen erityisesti nimettyihin siirtoihin ja velvoite informoida myös riskeistä. Näin esimerkiksi aiemmin annettu suostumus tietojen keruun yhteydessä ei ole riittävä, vaan suostumus on saatava itse siirron yhteydessä nimettyihin tarkoituksiin ja henkilötietoihin. Riskien lisäksi myös vastaanottajat on nimettävä. (EDPB

2018b, 7). Siirtoperusteena voi olla myös rekisteröidyn ja rekisterinpitäjän välinen tai rekisterinpitäjän ja toisen luonnollisen henkilön tai oikeushenkilön edun mukainen sopimus (tietosuoja-asetus 679/2016, artikla 49, kohta 1 b ja c). Näille lisävaatimuksena on se, että siirto on satunnainen ja se tulee kyetä todentamaan kirjallisesti tapauskohtaisesti satunnaisuustestillä (tietosuoja-asetus 679/2016, resitaali 111; EDPB 2018b, 8-9). Jos siirtoja tapahtuu säännöllisesti esimerkiksi liiketoiminnan yhteydessä, ei ole enää kyse satunnaisuudesta (EDPB 2018b, 9).

Yksityisetsivätoiminnan näkökulmasta kyseeseen voisi tulla myös siirron tarpeellisuus yleistä etua koskevien syiden vuoksi, koska aiemmin todetun mukaan rikosten paljastaminen ja selvittäminen katsotaan Suomen lainsäädännössä yleistä etua palvelevaksi (tietosuoja-asetus 679/2016, artikla 49, kohta 1 d). Tätä siirtoperustetta ei ole myöskään varattu julkishallinnon organisaatioille, vaan sitä voivat käyttää myös yksityisyritykset. Siirrolle ei ole myöskään yhtä tiukkaa vaatimusta sen satunnaisuudesta. Joka tapauksessa liiketoiminnan harjoittamisen yhteydessä tapahtuvista siirroista Euroopan tietosuojaneuvosto kehottaa käyttämään muita siirtomekanismeja. (EDPB 2018b, 11). Myös oikeusvaateiden laatimiseksi, esittämiseksi ja puolustamiseksi voidaan käyttää tietosuoja-asetuksen (679/2916) artiklan 49 poikkeuksia (kohta 1 e). Tässä tulee kuitenkin huomioida, että pelkkä oikeusvaateen mahdollisuus ei vielä riitä ja siirrettävien tietojen tulee olla rajoitettuja olennaiseen ja siirtojen olla luonteeltaan satunnaisia. Tietosuojaneuvosto kehottaa arvioimaan myös sitä, päästäisiinkö asiassa samaan lopputulokseen käyttämällä anonymisoitua tai pseudonymisoitua tietoa. (EDPB 2018b, 11-12). Anonymisoidulla tiedolla tuskin ratkaistaan oikeusvaateita ja satunnaisuuden vaatimuksen vuoksi tämä ei tulisi sovellettavaksi liiketoiminnassa, joten tässä kappaleessa esiin nostetut seikat ovat luonteeltaan teoreettisia yksityisetsivätoiminnassa.

Yksityisetsivätoimintaan voi soveltua myös kansainvälinen siirto julkisista rekistereistä esimerkiksi taustatarkistusten osalta (tietosuoja-asetus 679/2016, artikla 49, kohta1 g). Tällä tarkoitetaan yleisölle avoimia rekisterejä tai rekisterejä, joihin pääsyn voi oikeuttaa oikeutetulla edulla. Näitä ovat esimerkiksi yritysrekisterit, ajoneuvorekisterit, maanmittauslaitoksen rekisterit ja vaikkapa oikeuden päätöksiin liittyvät julkiset rekisterit. Ei kuitenkaan yksityisten ylläpitämät rekisterit, kuten esimerkiksi luottotietorekisterit. (EDPB 2018b, 14). Siirto saa koskea kuitenkin vain yksittäisiä henkilötietoja ja siirtoja tahoille, joilla on niitä koskeva oikeutettu etu (tietosuoja-asetus 679/2016, artikla 49, kohta 2). Kuten yleisissä lainmukaisuusperusteissa, on siirtoperusteissakin huomioitu siirron tarpeellisuus rekisteröidyn tai muiden henkilöiden elintärkeiden etujen varmistamiseksi (tietosuoja-asetus 679/2016, artikla 49, kohta 1 f). Mutta tässäkin tarkoitetaan välitöntä hengenvaaraa ja kiireellistä hoitotarvetta, eikä esimerkiksi tutkimusta, jonka tuloksia joudutaan odottelemaan tulevaisuuteen (EDPB 2018b, 12-13). Siten tällainen toimeksianto tai siirto kohdistettaisiin todennäköisesti pelastusalan tai terveydenhuollon viranomaisiin, eikä yksityisetsivälle.

Mikäli mikään muu poikkeusperusteista ei sovellu, on olemassa myös mahdollisuus siirtää tietoja pakottavista oikeutetuista eduista johtuen. Tähän pätee kuitenkin vaatimus satunnaisuudesta, rajallisesta henkilöiden määrästä, asianmukaisista suojakeinoista ja kaikista arvioista, joita edellisiinkin siirtoihin sovelletaan (tarpeellisuus ja satunnaisuus). Sen lisäksi tietojen siirrosta tulee ilmoittaa valvontaviranomaiselle ja rekisteröidyille itselleen, joita siirto koskee. (tietosuoja-asetus 679/2016, artikla 49, kohta 1, mom. 2). Satunnaisuusvaatimuksen vuoksi tämä ei sovellu liiketoimintaan ja velvoitteiden lukumäärän vuoksi se edellyttäisi myös melkoista byrokratiaa ja valmistelua, mikä aiheuttaisi pienyritykselle merkittävän taakan.

Kun asianmukainen suojatoimi on valittu, jatketaan siirron arviointiin liittyvää prosessia seuraavaksi kohdemaan lainsäädäntötason ja henkilötietojen käsittelyn käytäntöjen arvioinnilla. Käytännössä tämän arvioinnin tarkoituksena on tuottaa tietoa siitä, onko kohdemaan lainsäädännössä tai käytännöissä jotain sellaista, mikä voisi vaarantaa valitun suojamekanismin tuoman henkilötietojen suojan suhteessa siirtoon (EDPB 2021e, 14). Tämä osa arvioinnista on usein työläs ja raskain, koska siinä on arvioitava luonnollisesti jokainen siirtoon osallistuva tekijä. Sen lisäksi siinä on tutustuttava kohdemaahan tai maihin niin syvällisesti, että opitaan ymmärtämään, onko kohdemaan viranomaisilla mahdollisuuksia päästä käsiksi muualta tuotuihin henkilötietoihin. Samoin tulee arvioida, onko näin käynyt sekä arvioida, mitä lainsäädännöllisiä, rahoitukseen liittyviä, teknisiä tai muita resursseja kohdemaan viranomaisilla olisi tähän käytettävissä. (EDPB 2021e, 14-15). Tässä on huomioitava, ettei kyse ole tavanomaisilta tietoturvauhilta välttyminen, vaan myös viranomaisten taholta tapahtuvien väärinkäytösten estäminen riittävän korkeatasoisen suojan takaamisella rekisteröidyille (EDPB 2020e, 7). Siten pelkästään se, että tiedot on salattu, ei ole riittävä suojakeino, jos viranomainen kohdemaassa voi pakottaa tietojen vastaanottajan avaamaan salauksen.

Selvityksessä voi käydä ilmi, että kohdemaassa on muodollisesti lainsäädäntö, joka täyttää vaatimukset, mutta sitä ei noudateta. Voi selvitä myös, että kohdemaan lainsäädännössä on sellaisia puutteita, että siirtovälineen tuomat takeet eivät ole riittävät. Voi käydä ilmi myös se, että tietojen tuojaan sovelletaan kohdemaassa jotain erityisen ongelmallista lainsäädäntöä, joka johtaa perusoikeuksien suojan vaarantumiseen. (EDPB 2021e, 17). Näin oli esimerkiksi Euroopan unionin tuomioistuimen päätöksessä C-311/18, joka kaatoi Privacy Shield siirtomekanismin Yhdysvaltain tiedustelulainsäädännön vuoksi (EDPB 2020d, 2). Näissä tapauksissa on Eurooppaan sijoittuneen siirtojen tekijän joko keskeytettävä siirrot tai otettava käyttöön lisäsuojakeinoja, joilla voidaan varmistaa riittävä suoja edellä mainituista olosuhteista huolimatta. Siirtoa voidaan jatkaa ilman lisäsuojakeinoja vain, mikäli siirtäjä voi osoittaa, ettei kyseisiä käytäntöjä tai lainsäädäntöä sovellettaisi siirtoon ja arvion tulee olla huolellisesti laadittu ja kirjallinen. (EDPB 2021e, 18).

Jos lisäsuojakeinoja tulee ottaa käyttöön, siirrytään niiden tunnistamiseen ja valintaan. Lisäsuojakeinoina voi olla esimerkiksi tietojen salaaminen siten, että niihin ei päästä käsiksi siirrossa tai niiden loppusijainnissa selväkielisenä. Käsittelytoimintaa voi myös hajauttaa siten, että se jakautuu useammalle toimijalle, jolloin yhdelläkään ei ole koko tietomassaa kerrallaan sellaisenaan. Myös arkaluontoisempien tietojen siirtämättä jättämistä tulisi harkita. Tietenkin lisäsuojakeinoissa on otettava huomioon se, että ne ovat käyttökelpoisia kohdemaassa, esimerkiksi salaus voi olla kielletty kohdemaassa. Lisäsuojakeinoja ei ole erityisesti rajattu ja ne voivat olla luonteeltaan organisatorisia, teknisiä tai sopimuksellisia. (EDPB 2021e, 22-23). Jos tehdään muutoksia esimerkiksi komission hyväksymiin vakiomuotoisiin sopimuslausekkeisiin, on lisäksi automaattisesti kuultava valvontaviranomaista (EDPB 2021e, 24). Valvontaviranomaisen konsultointi voi tulla tarpeeseen suojakeinoista riippuen muutenkin (EDPB 2021e, 4). Siirtoja on arvioitava yhdessä tietojen vastaanottajien kanssa säännöllisesti ottaen huomioon mahdolliset muutokset suojan tasossa (EDPB 2021e, 25).

5.3.7 Tietosuojavastavan nimittäminen

Tietosuojavastaavat ovat organisaatioissa tilivelvollisuuden kulmakivi ja heidän tehtävänsä on helpottaa tietosuoja-asetuksen säännösten noudattamista. Sen lisäksi he toimivat välittäjänä rekisteröityjen, rekisterinpitäjien ja käsittelijöiden sekä viranomaisten välillä. (WP 20 2017d, 5). Tietosuojavastaavan varsinaisia tehtäviä ovat edellisten lisäksi tietosuojalainsäädännön noudattamisen valvonta henkilötietojen käsittelyssä rekisterinpitäjillä ja käsittelijöillä. Tietosuojavastaavan tulee myös antaa neuvoja organisaatioiden suorittaessa tietosuojaa koskevia vaikutustenarviointeja. (Tietosuoja-asetus 679/2016, artikla 39, kohta 1). Valvontaroolinsa vuoksi tietosuojavastaavan aseman on oltava riippumaton, eikä hän saa ottaa vastaan ohjeita tehtäviensä suorittamiseksi tai olla organisaatiossa sellaisessa roolissa, jossa hänen olisi määriteltävä henkilötietojen käsittelyn keinoja tai tarkoituksia (WP 29 2017d, 16-17, 18; tietosuoja-astus 679/2016, artikla 38, kohdat 3 ja 6).

Tietosuojavastaavan tehtäviin ja asemaan liittyy paljon muutakin, mutta tämän työn kannalta olennaisinta on kysymys siitä, milloin tietosuojavastaava on organisaatioon nimitettävä. Tietosuoja-asetus (679/2016) yksilöi kolme tilannetta, joissa nimittäminen on lakisääteisesti pakollista (artikla 37, kohta 1):

1. tietojenkäsittelyä suorittaa viranomainen tai julkishallinnon elin
2. rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa

3. rekisterinpitäjän tai käsittelijän ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu 9 artiklan mukaisiin erityisiin henkilötietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikoksia koskeviin tietoihin.

Tietosuojavastaava voidaan nimittää myös vapaaehtoisesti, mutta vapaaehtoisessakin nimittämisessä tietosuojavastaavia koskee kaikki tietosuoja-asetuksen määrittämät tietosuojavastaavia koskevat velvoitteet (WP 29 2017d, 5 ja 7). Oli tietosuojavastaava nimitetty vapaaehtoisesti tai lakisääteisen pakon vuoksi, tietosuojavastaavan vastuulle kuuluvat rekisterinpitäjän ja käsittelijän kaikki käsittelytoimet – eivät vain ne käsittelytoimet, miksi nimittäminen on pitänyt tehdä (WP 29 2017d, 7 ja 11). Tietosuojavastaava voidaan nimittää usean organisaation yhteiseksi ja nimittäminen voi perustua myös palvelusopimukseen (WP 29 2017d, 24–25).

Lakisääteisistä tilanteista ensimmäinen ohitetaan yksityissektorilla melko usein, koska helposti voisi ajatella sen koskevan vain julkishallintoa. Tietosuojatyöryhmä muistuttaakin, että tämän piiriin kuuluvat myös yksityisoikeudelliset luonnolliset ja oikeushenkilöt, jotka hoitavat julkista hallintotehtävää tai käyttävät julkista valtaa (WP 20 2017d, 7). Perusteluna yksityisoikeudellisten organisaatioiden sisällyttämisen tähän WP 29 mainitsee, että rekisteröidyt saattavat olla niidenkin osalta samanlaisessa asemassa kuin tietoja käsittelisi viranomainen, eikä henkilöillä ole välttämättä vaikutusvaltaa siihen, miten heidän tietojaan käsitellään tai käsitelläänkö niitä ylipäätään. Siksi henkilöt voivat tarvita enemmän suojaa ja tietosuojavastaava on elementti, jolla suojan tasoa voidaan nostaa. (WP 29 2017, 7).

Tietosuojatyöryhmän WP 29 perusteluissa on nähty valvonnan olevan esimerkiksi kameravalvontaa toteutettaessa turvallisuusalan yrityksen ydintehtäviä, eikä vain toimintaa tukevia oheistoimintoja. Laajamittaisuuden esimerkkinä tietosuojatyöryhmä käyttää turvallisuusalan yritystä, joka vastaisi useista yksityisistä kauppakeskuksista ja siten julkisten tilojen valvonnasta. (WP 29 2017d, 8). Asiakkaana olevalla rekisterinpitäjällä kameravalvonta ei ole välttämättä sen organisaation ydintoiminto, jolloin tietosuojavastaavaa ei tarvitse välttämättä nimittää asiakasorganisaatioon (WP 29, 2017d, 8 ja 10–11). Jos molemmilla olisi tietosuojavastaava, olisi tietosuojavastaavien tehtävä yhteistyötä (WP 29 2017d, 11).

Taksi Helsinkiä koskevassa sakkopäätöksessä tietosuojavaltuutetun seuraamuskollegio katsoi takseissa olevan kameravalvonnan täyttävän laajamittaisen käsittelyn tunnusmerkit, myös siksi, että tietoja tallentuu sivullisista. Ei vain palvelun ostajasta. Sen lisäksi kuva- ja äänitallennus kerää runsaasti henkilötietoa, eikä käsittely koskenut vain näitä tietoja. Lisäksi tallenteet ovat aika- ja paikkasidonnaisia, mikä korostaa valvonnan vaikutuksia rekisteröityihin ja tuo lisää käsiteltäviä henkilötietoryhmiä. (8393/161/2019 2020, 24–25).

Kohdan kolme velvoite laajentaa nimittämisvelvollisuuden myös käsittelyyn, jossa käsitellään erityisiä tietoryhmiä tai rikoksiin liittyviä tietoja, riippumatta siitä, miten laaja

rekisteröityjen kohderyhmä on kyseessä. Tämä todennäköisesti väärinkäytöstutkinnassa ja ainakin luvanvaraisen rikoksen paljastamisen yhteydessä viimeistään pakottaa pohtimaan tietosuojavastaavaa. Kohdan kolme osalta on huomioitava, että tietosuoja-asetuksen (679/2016) artiklassa 37 sanamuoto on ”… erityisiin henkilötietoryhmiin ja 10 artiklassa tarkoitettuihin…” (kohta 1 c). Tietosuojatyöryhmä korostaa kuitenkin, että ei ole olemassa mitään poliittista perustetta sille, että molempia ehtoja olisi sovellettava yhtä aikaa ja teksti olisi luettava kuin siinä olisi tai -sana ja -sanan tilalla (WP 29 2017d, 10).

Laajamittaisen käsittelyn määritelmään ei ole yksiselitteistä lukua, vaan siihen voi vaikuttaa rekisteröityjen lukumäärän lisäksi myös heidän suhteellinen osuutensa kyseeseen tulevasta kokonaisotannasta tai käsiteltävien henkilötietojen ja tietotyyppien määrä. Myös käsittelyn kesto tai pysyvyys voi vaikuttaa laajamittaisuuteen. (WP 29 2017d, 23). Ainoa poikkeus laajamittaisuuden osalta sääntöön on niin sanottu ”yksinyrittäjäpoikkeus”, jossa yksittäisen lääkärin suorittama potilastietojen tai yksittäisen asianajajan suorittama rikostuomioihin ja rikoksiin liittyvien tietojen käsittely ei täytä laajamittaisuuden määritelmää (WP 29 2017d, 9). Siten tämän poikkeuksen voisi ajatella olevan käytettävissä myös yksityisetsivätoimintaa harjoittavalla yksinyrittäjällä.

Säännöllisen ja järjestelmällisen määritelmään ei myöskään ole yksiselitteisiä lukuja tai reunaehtoja. Säännöllisen ei tarvitse kuitenkaan tarkoittaa vain jatkuvaa, vaan pelkästään sen toistuminen määräajoin tai tietyillä aikaväleillä riittää tekemään käsittelystä säännöllistä. Järjestelmällisen määritelmä täyttyy sillä, että se on jonkin ennalta suunnitellun strategian osa, organisoitua ja menetelmällistä tai osana muuta tiedonkeruusuunnitelmaa. Konkreettisina esimerkkeinä mainitaan tietoliikenneverkon ylläpito, dataohjattu markkinointi tai pisteyttämine riskienarviointia varten esimerkiksi petosten torjunnassa ja sijainnin seuranta. (WP 29 2017d, 10). Väärinkäytöstutkintaa tekevän ei siis tarvitse käsitellä juuri saman asiakkaan tietoja jatkuvasti, vaan riittää, että liiketoimintastrategiaan kuuluu tällaisten palvelujen tarjoaminen useille asiakkaille, jolloin käsittely on säännöllistä ja järjestelmällistä.

Vaikka tietosuojavastaavaa ei nimitettäisi, on päätös perusteluineen dokumentoitava ja dokumentti säilytettävä osana normaalia osoitusvelvollisuutta ajatellen. Analyysi on kuvattava tarkasti, että valvontaviranomainen voi myöhemmin tarkastaa, että kaikki olennaiset tekijät on otettu päätöksessä huomioon. Arviota on luonnollisesti päivitettävä, jos organisaation toiminnassa tai olosuhteissa tapahtuu muutoksia. (WP 29 2017d, 67).

5.4 Henkilötietojen käsittelyn ohjaus laissa yksityisistä turvallisuuspalveluista

Henkilötietojen käsittelyyn liittyviä toimivaltuuksia laki yksityisistä turvallisuuspalveluista (1085/2015) ei erikseen nimeä, vaikka toimivaltuuksia on muuten määritelty. Henkilötietojen käsittelyyn ei laissa yksityisistä turvallisuuspalveluista tai kyseisen lain valmistelussa ole

otettu kantaa juuri muuten kuin yksityissektorin toimijaa rajoittavalla tavalla yksilöidyissä tilanteissa. Esimerkki tästä on poliisin säilöön ottamien henkilöiden vartioinnista. Hallituksen esityksessä erikseen mainittiin, että näissä tehtävissä yksityisen turvallisuusalan elinkeinoluvan haltijan alaisuudessa työskentelevällä vartijalla ei tule olla pääsyä poliisin tai viranomaisten tietojärjestelmiin, vaikka työskentely tapahtuukin poliisin valvonnan alla (HE 22/2014 vp, 4).

Laki yksityisistä turvallisuuspalveluista (1085/2015) säätää myös niin sanotusta tapahtumailmoituksesta, joka vartijan tulee laatia aina kiinniottamiseen tai voimakeinojen käyttöön liittyvistä tilanteista (luku 2, 8 §). Hallituksen esitys puhuu yleisemmin ”…sellaisista tapahtumista raportoimisesta, joilla on kiinteä yhteys ihmisten perusoikeuksiin” (HE 22/2014 vp, 34). Jatkossa sitä kuitenkin tarkennetaan siten, että se liittyisi vain voimakeinojen käyttöön, jolloin esimerkiksi vartioimisalueelle pääsyn estämisestä ei tarvitsisi tapahtumailmoitusta laatia, jos siihen ei ole liittynyt voimakeinojen käyttöä (HE 22/2014 vp, 34). Turvallisuusalan elinkeinoluvan haltijalla olisi kuitenkin oikeus sopia muustakin toimeksiantajalle suoritettavasta raportoinnista, mutta tästä ei ole laissa nimenomaisia sisältö- tai säilytysvaatimuksia (HE 22/2014 vp, 43). Tapahtumailmoitukset on säilytettävä kaksi vuotta niiden laatimisesta, minkä jälkeen henkilötietoja sisältävät tapahtumailmoitukset on hävitettävä (laki yksityisistä turvallisuuspalveluista 1085/2015, luku 2, 8 §).

Henkilötietojen käsittelyä muun raportoinnin yhteydessä ei määritellä edellistä tarkemmin. Paasonen & Ellonen ovat käsitelleet myös tapahtumailmoituksia henkilötietojen suojan näkökulmasta, mutta lähinnä asianosaisten tarkastusoikeuteen liittyen (2018, 100-102). Hekään eivät puhu muusta raportoinnista tai sen muodoista. Hallituksen esitys 22/2014 vp käsittelee henkilötietojen käsittelyä edellisten lisäksi vain poliisin suorittaman käsittelyn osalta (esimerkiksi 159, 174). Toiminnan kohteena olevien luonnollisten henkilöiden henkilötietojen käsittelystä laki yksityisistä turvallisuuspalveluista tai sen perustelutekstit eivät sano muuta. Edellä mainitun lain 81 § käsittelee turvallisuusalan elinkeinoluvan haltijan oman henkilöstön tietojen käsittelyä ja 86 § poliisin valvontatietoja, mutta nämä eivät olennaisesti liity tämän työn aiheena olevaan rikoksen paljastamiseen ja siinä tapahtuvaan henkilötietojen käsittelyyn. Henkilötietojen käsittelyyn liittyvät oikeudet ja toimivaltuudet on siis haettava muualta lainsäädännöstä.

5.5 Tietosuojalaki

Suomessa tietosuojan sääntelyn tausta on myös perusoikeuksien turvaamisessa, kuten aiemmin todettiin eurooppalaisesta lainsäädännöstä. Perustuslain (731/1999) 10 § takaa kaikille Suomen kansalaisille oikeuden yksityiselämään, kotirauhaan ja viestinnän luottamuksellisuuteen. Luottamuksellisen viestinnän ja henkilötietojen suoja sisältyy

yksityiselämän suojaan, joka tulee ymmärtää kenen tahansa yksityistä piiriä koskevaksi yleiskäsitteeksi, johon liittyy muun muassa vapaus solmia itsenäisiä suhteita toisiin ja ympäristöön (HE 309/1993 vp, 52-53). Perustuslain perusteluissa on velvoite lainsäätäjälle aktiivisista ja tehokkaista toimista kansalaisten yksityiselämän suojaamiseksi (HE 309/1993 vp, 53). Kyse on siis merkittävästä oikeudesta, jota lainsäätäjän tulee itsekin omilla toimilla suojata.

Henkilötietojen käsittelyä on Suomessa ohjannut aiemmin henkilörekisterilaki (471/1987) ja myöhemmin henkilötietolaki (523/1999). Suurin muutos kansallisessa lainsäädännössä tapahtui Euroopan yleisen tietosuoja-asetuksen (679/2016) voimaan tullessa. Ihan kaikki ei kuitenkaan muuttunut. Henkilörekisterilaissa oli jo yhteneväisyyksiä muun muassa henkilötiedon määritelmässä, rekisterinpitäjyyden määrittelyssä ja esimerkiksi arkaluonteisten tietojen ja erityistietoryhmien sisällöissä verrattuna nykyiseen asetukseen (henkilörekisterilaki 479/1987, 2 § ja 6 §). Henkilötietolaki oli yleisen tietosuoja-asetuksen edeltäjän tietosuojadirektiivin (95/46/EY) kansallinen toimeenpano suomalaisessa lainsäädännössä (HE 96/1998 vp, 4). Henkilötietolaki toi jo mukanaan useita yleisestä tietosuoja-asetuksestakin tuttuja termejä kuten henkilötiedon käsittelyn ja suostumuksen määritelmät, mutta tietyt asiat, kuten tarpeellisuusvaatimus, olivat tuttuja jo aiemman lainsäädännön ajalta (henkilötietolaki 523/1999, 3 §; henkilörekisterilaki 471/1987, 5 §).

Tietosuojalaki (1050/2018) säädettiin Suomessa täydentämään yleistä tietosuoja-asetusta. Yleinen tietosuoja-asetus ei sallinut enää kansallista liikkumavaraa muutoin kuin silloin, kun siitä oli erikseen yleisessä tietosuoja-asetuksessa määritelty (tietosuoja-asetus 679/2016, resitaali 10). Siten Suomessa katsottiin, että annettavaa tietosuojalakia tulisi lukea rinnakkain tietosuoja-asetuksen kanssa ja se koostuisi vain tietosuoja-asetusta täydentävistä pykälistä. (HE 9/2018 vp, 4-5). Tietosuojalain tarkoitus ja soveltamisalakin viittaa suoraan tietosuoja-asetukseen (1050/2018, 1 § ja 2 §). Koska tietosuojalainsäädäntö ei sinällään ole Suomessa enää itsenäinen lainsäädäntökokonaisuutensa, sen käsittely ei tässä yhteydessä ole laajemmin tarpeen muutoin kuin muutamien yksittäisten yksityisetsivätoimintaan liittyvien kohtien osalta.

Todettakoon ensin, että tietosuojalaki ei tuo lisää käsittelyperusteita tai lainmukaisuusperusteita henkilötietojen käsittelylle. Kansallinen liikkumavara, joka on jätetty yleisen edun tai julkisen vallan perusteella tapahtuvaan käsittelyyn, mainitsee vain muutaman tarkennuksen lainmukaisuusperusteisiin, joiden perusteella henkilötietoja voisi käsitellä (tietosuojalaki 1050/2018, luku 2). Niistä yksikään ei sovellu sellaisenaan henkilötietojen käsittelyyn rikos- tai väärinkäytöstutkinnassa, vaan edellyttää myös muiden olosuhteiden toteutumista. Osa ei sovellu ollenkaan, kuten esimerkiksi käsittely tieteelliseen tai historialliseen tutkimukseen tai kulttuuriperintöaineistojen kokoamiseen (tietosuojalaki 1050/2018, 4 §).

Tietosuojalain (1080/2018) neljännen pykälän ensimmäinen kohta antaa oikeuden käsitellä henkilön asemaa, tehtäviä ja niiden hoitoa julkishallinnossa, järjestötoiminnassa tai elinkeinoelämässä, jos tavoite on yleisen edun mukainen ja oikeasuhtaista päämäärään nähden. Tällainen tilanne voisi tulla kyseeseen jossain tutkintatoimeksiannossa. Oikeus on kuitenkin vain yhden henkilön toimien selvittämiseen ja jos tutkinta laajenisi tästä, tulisi pohtia muiden henkilöiden tietojen osalta käsittelyn lainmukaisuusperusteita, ellei kyse ole samaten heidän asemansa tai tehtäviensä hoitamisesta julkishallinnossa. On katsottu, että tällaisissa tilanteissa oikeus yksityisyyteen ei välttämättä syrjäytä rekisterinpitäjän tai sivullisen intressejä. Yleisen edun olemassaolo on kuitenkin edellytys näiden tietojen käsittelylle, eikä mitä tahansa käsittelyä voida perustella tällä. (HE 9/2018 vp, 79). Etujen välinen tasapaino olisi hyvä kirjata tällaisissa tilanteissa.

Neljännen pykälän toinen kohta antaa lainmukaisuusperusteen käsittelylle, jos käsittely on tarpeen ja oikeasuhtaista viranomaisen toiminnassa (tietosuojalaki 1050/2018, 4 §). Lain perusteluteksteissä on kuitenkin erikseen mainittu, että tällä tarkoitetaan vain viranomaisen suorittamaa käsittelyä, mutta ei yksityisoikeudellisia yhteisöjä niiden suorittaessa käsittelyä julkisen hallintotehtävän hoitamiseksi. Ne joutuvat turvautumaan joko muualla lainsäädännössä asetettuun velvoitteeseen taikka omiin tai kolmannen osapuolen oikeutettuihin etuihin. (HE 9/2018 vp, 80).

Tietosuojalaissa (1050/2018) säädetään myös tarkemmin tietosuoja-asetuksen (679/2016) artiklan 23 poikkeuksista tilanteissa, joissa rekisteröityä ei tarvitse informoida henkilötietojen käsittelystä sekä oikeudesta poiketa rekisteröidyille luovutettavien tietojen osalta. Näistä säädetään muussakin lainsäädännössä, kuten esimerkiksi työelämän tietosuojaa ja viestintäpalvelulakia käsittelevissä luvuissa todetaan. Tietosuojalaki (1050/2018) antaa mahdollisuuden poiketa informoinnista silloin kun tietoja kerätään henkilöltä itseltään tai muista lähteistä, jos tietojen keruu tapahtuu rikosten ehkäisemiseksi tai selvittämiseksi tai se vaarantaisi vakavasti rekisteröidyn terveyden, hoidon tai hänen itsensä tai jonkun muun oikeudet (33 §). Rekisterinpitäjän tulee kuitenkin varmistaa käsiteltäviin henkilötietoihin liittyvien henkilöiden oikeuksien suoja muun muassa pitämällä kaikkien saatavilla yleisiä käsittelyä koskevia tietosuoja-asetuksen tarkoittamia tietoja, joita käsiteltiin luvussa Informointi käsittelystä henkilöille, joiden tietoja käsitellään ja heidän oikeutensa (tietosuojalaki 1050/2018, 33 §, 3 mom.). Kuten Tietosuoja-asetus -luvussa todettiin, nämä ovat artikloiden 12-14 tarkoittamia yleisiä tietoja henkilötietojen käsittelystä.

Myös omien tietojen tarkastusoikeutta, esimerkiksi jäljennöksen saantia omista tiedoista, voidaan rajoittaa silloin, kun se vaarantaisi rikosten ehkäisemisen tai selvittämisen (tietosuojalaki 1050/2018, 34 §). Tietoja ei tarvitsisi luovuttaa myöskään silloin, jos se aiheuttaisi vaaraa jonkun muun oikeuksille (HE 9/2018 vp, 119). Kuitenkin rajoituksen syyt ja sellaiset tiedot, jotka eivät vaaranna rajoituksen tarkoitusta, on luovutettava (tietosuojalaki

1050/2018, 34 §, 2 ja 3 mom.) Joka tapauksessa rekisteröityä koskevat tiedot on rekisteröidyn pyynnöstä luovutettava tietosuojavaltuutetulle (tietosuojalaki 1050/2018, 34§, 4 mom.). Luonnollisesti tutkinnan päätyttyä rajoittamistarve luovutuksen osalta todennäköisesti lakkaa.

Henkilötietolain perusteluteksteissä mainittiin henkilötietojen käsittelyyn liittyvän rekisteriselosteen nähtävillä pidon velvoitteen ulkopuolelle rajatun suojelupoliisin toiminnallinen tietojärjestelmä (HE 96/1998 vp, 7). Lain perusteluteksteissä mainitaan nähtävillä pidosta poikkeamisesta säädettävän henkilörekisteriasetuksella tai erityislainsäädännöllä (HE 96/1998 vp, 43). Kumottu henkilörekisteriasetus (476/1987) taas sääti poikkeamisoikeuksista vain viranomaiselle tai valtioneuvoston päätöksellä (7 §). Tietosuojalain perusteluteksteissä taas mainitaan, että tietosuojalailla ei ole tarkoitus muuttaa informoinnista poikkeamisen osalta nykytilaa (HE 9/2018 vp, 117). Samaa mainintaa ei kuitenkaan löydy poikkeamisoikeudesta luovuttaa rekisteröidylle häntä koskevia tietoja ja perusteluina tietojen luovutuksesta poikkeamiselle mainitaan m. lastensuojelulliset syyt ja ilmiantokanaviin luovutetut tiedot (HE 9/2018 vp, 118–120). Vaikuttaisi siltä, että yksityisoikeudellisilla tahoilla ei ole oikeutta poiketa henkilötietojen käsittelystä kertomisesta yleisellä tasolla, siten kuin informoinnista säädetään tietosuoja-asetuksen 12–14 artikloissa. Jos henkilötietolain aikaista nykytilaa ei ole ollut tarkoitus muuttaa, tätä oikeutta ei olisi viranomaisellakaan, ellei sitä ole lainsäädännössä erikseen säädetty.

Hallituksen esityksessä oikeutta poiketa tietojen luovutusvelvollisuudesta siten kuin tietosuoja-asetuksen 15 artikla säätää, ei erityisesti rajata viranomaiselle. Sen voisi ajatella olevan käytettävissä myös yksityisoikeudellisille yhteisöille niiden käyttäessä henkilötietoja itseään koskevien rikosten ehkäisyyn tai selvittämiseen. (HE 9/2018 vp, 117–120). Jos tietojen käsittelyn kohteena ovat työntekijät, tulee kuitenkin lisäksi sovellettavaksi työelämää koskeva lainsäädäntö. Oikeutta poiketa velvollisuudesta tietojen luovuttamiselle rekisteröidystä itsestään tulee taas arvioida huolellisesti, perustellusti ja tapauskohtaisesti. Kynnys tietojen luovuttamisesta poikkeamiseen on siis varsin korkea, eikä se voi todennäköisesti olla rutiininomainen toimi. Tämä voidaan päätellä jo siitä, että rekisterinpitäjän on edellä esitetyn perusteella muun muassa arvioitava, mitkä tiedot voidaan luovuttaa ja mitä ei. Tämän voisi ajatella olevan tapauskohtainen arvio, ellei tutkintatapaus ole täysin identtinen jo jonkin aiemmin suoritetun tutkinnan kanssa, jolloin voitaisiin ehkä käyttää aiemmin tehtyä arviota.

Poikkeaminen luovutusvelvollisuudesta saattaa edellyttää jopa tietosuojavaltuutetun kuulemista. Tämä liittyy siihen, että rekisteröityä koskevien tietojen toimittamatta jättäminen hänelle voi aiheuttaa korkean riskin, ellei henkilö saa henkilötietojensa käsittelystä tietoja. Ja kuten aiemmin on todettu, tämä taas estää heitä käyttämästä oikeuksiaan. Rekisterinpitäjällä on tällaisessa tilanteessa velvollisuus tehdä tietosuojaa koskeva vaikutustenarviointi ja ellei riskiä voida osoittaa hallittavan rekisterinpitäjän

toimilla, tulee asiassa kuulla tietosuojavaltuutettua (tietosuoja-asetus 679/2016, artiklat 35 ja 36).

Rekisterinpitäjä voi poiketa informointivelvoitteesta tietosuoja-asetuksen perusteella myös silloin, kun tietoja hankitaan muualta kuin rekisteröidyltä tietyissä tilanteissa. Ne ovat tilanteita, joissa rekisteröity on jo aiemmin saanut tiedot, tietojen toimittaminen vaatisi kohtuutonta vaivaa tai olisi mahdotonta, tietojen hankinnasta tai luovuttamisesta säädetään lailla muuta tai tiedot ovat lakisääteisesti salassa pidettäviä. (tietosuoja-asetus 679/2016, artikla 14, kohta 5). Jos informointivelvoitteesta poiketaan ja tietoja käsitellään seuraaviin tarkoituksiin, tulee asiassa laatia 35 artiklan tarkoittama tietosuojaa koskeva vaikutustenarviointi (Tietosuojavaltuutetun toimisto 2018):

- henkilön arvioimiseksi tai pisteyttämiseksi
- automaattisessa päätöksenteossa, joilla on oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia
- järjestelmällisen valvonnan yhteydessä
- laajamittainen käsittely
- käsittely yhteensovittamiseksi tai yhdistämiseksi muihin tietokokonaisuuksiin
- heikommassa asemassa olevien rekisteröityjen tietojen käsittely
- uusien teknisten ja organisatoristen ratkaisujen innovatiivisten käytön tai soveltamisen yhteydessä
- siten, että henkilötietojen käsittely estää rekisteröityjä käyttämästä hänelle kuuluvaa oikeutta tai palvelua

Informoinnista poikkeamisesta ja henkilötietojen keruusta ilman lainmukaisuusperustetta on Suomessakin oikeuskäytäntöä. Esimerkiksi tietosuojavaltuutetun päätöksessä (5417/163/20) vuoden 2021 heinäkuulta arvioitiin, voidaanko asiakkaista kerätä henkilötietoja vain tarkkailemalla. Päätöksessä arvioitiin muun muassa läpinäkyvyyden periaatteen toteutumista ja sen osalta todettiin, että ellei tarkkailusta kerrota asiakkaille, läpinäkyvyyden periaate ei toteudu. (5417/163/20, luku Tietosuojavaltuutetun päätös). Myös hovioikeus on Suomessa antanut tuomion asiassa, jossa yksityishenkilö keräsi ja lajitteli omaan käyttöön henkilötietoja, voidakseen yhdistellä henkilöitä ja tapahtumia toisiinsa ja paljastaa henkilöiden tekemisiä myöhemmin. Vaikka tietoja ei julkaistu, oli rikostuomio 50 päiväsakkoa ja kärsimyskorvausvelvollisuus noin 500 euroa per henkilö, jonka tietoja oli käsitelty. Koska henkilöitä oli joitakin kymmeniä, nousi korvauksen suuruus aika merkittäväksi yksityishenkilöön kohdistuvana kärsimyskorvauksena. Huomioitavaa on vielä, että tietoja ei julkaistu, eikä kenellekään osoitettu aiheutuneen vahinkoa – jos näin olisi ollut, olisi päälle tullut vielä vahingonkorvausvelvollisuus. (Kiviniemi 2020). Edellä mainittu viranomaisen ja hovioikeuden päätös vahvistaa aiemmin tehtyä olettamusta, että kenellä tahansa ei ole

Suomessa oma-aloitteisesti oikeutta alkaa keräämään henkilöistä tietoja heidän seuraamiseksi ja olla kertomatta siitä.

Monimutkaisemmaksi tilanne muodostuu silloin, jos rikosten selvittämisen yhteydessä aletaan käsitellä aiemmin Tietosuoja-asetus-luvussa käsiteltyjä rikostuomioihin ja rikkomuksiin liittyviä tietoja. Rikoksiin liittyvät tiedot olivat aiempien lakien osalta arkaluonteisia henkilötietoja, joiden käsittely oli lähtökohtaisesti kielletty jo silloin (Henkilörekisterilaki 471/1987, 6 §; Henkilötietolaki 523/1999, 11 §). Henkilörekisterilaki oli siinä mielessä tiukempi laki, että se ei sallinut näiden tietojen käsittelyä henkilörekisterissä muutoin kuin laissa säädetyn tehtävän nojalla (Henkilörekisterilaki 471/1987, 7 §). Henkilötietolaki toi kuitenkin mukanaan mahdollisuuden käsitellä näitä tietoja myös ”oikeusvaateen laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi” (Henkilötietolaki 523/1999, 12 §). Nyt näiden tietojen käsittelystä on säädetty kansallisesti tietosuojalain (1050/2018) seitsemännessä pykälässä, jossa käsittelyn perusteena on edelleen oikeusvaateen selvittämiseksi, laatimiseksi, esittämiseksi, puolustamiseksi tai ratkaisemiseksi liittyvät tilanteet. Sen lisäksi näitä tietoja voisi käsitellä vakuutusyhtiön suorittamassa henkilötietojen käsittelyssä yhtiön vastuun selvittämiseksi, tieteellinen tai historiallinen tutkimus tai tilanteet, joissa siitä on erikseen laissa säädetty. (Tietosuojalaki 1050/2018, 6 § ja 7 §).

Suomesta ei löydy selkeää lainsäätäjän määritelmää tietosuoja-asetuksen (679/2016) 10 artiklan rikoksiin ja rikostuomioihin liittyvistä tiedoista suoraan lakitekstistä. Tietoja pidettiin henkilötietolain aikaan arkaluontoisina henkilötietoina ja kyseiset tiedot ovat edelleen tietoja, jotka ovat arkaluonteisia perusoikeuksien ja vapauksien kannalta (6689/186/20). Kumotun henkilötietolain perusteluteksteissä puhutaan arkaluonteisista henkilötiedoista ”rikolliseen tekoon” liittyvänä tietona (HE 96/1998 vp, 11). Myös tietosuojalain perustelut mainitsevat tällaisten tietojen olevan rikolliseen tekoon tai rangaistukseen liittyviä tai rikoksen seuraamusta kuvaavia tietoja (HE 9/2018 vp, 92). Rahanpesulain (Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017) neljäs luku velvoittaa ilmoittamaan pelkästään epäilyttävistä liiketoimista ja sitoo kyseiset tiedot salassapitovelvoitteen alle (1 § ja 4§). Myös ilmiantajien suojelua koskevan kansallisen lainvalmistelun luonnos edellyttää luottamuksellisuutta ilmoittajien ja ilmoitusten kohteen henkilöllisyydestä, vaikka tässä vaiheessa ei vielä käsitellä lainvoimaisia tuomioita (HE luonnos 2021a, 9). Siten voisi ajatella, että kyseessä ei tarvitse olla tieto nimenomaan rikostuomiosta, vaan jo pelkkä tekoon ja seuraamuksiin liittyvä tieto voi olla tällainen. Siten Suomessakin tulkinnan voidaan olettaa olevan eurooppalaisen linjan mukainen, mihin viitattiin aiemmin luvussa Tietosuoja-asetus.

Tietosuojalain (1050/2018) mukaan rikoksiin liittyviä henkilötietoja on mahdollista käsitellä myös silloin, kun siitä säädetään laissa tai jos velvoite johtuu rekisterinpitäjälle laissa säädetystä tehtävästä (7 §, 1 mom., kohta 2). Rikoksen paljastamisesta ja selvittämisestä on määritelty laissa, mutta LYTP ei määrittele erityisesti henkilötietojen käsittelystä tällaisessa

yhteydessä. Siten olisi aika uskaliasta venyttää lain rajoja ilman tarkkarajaista ja selkeää sääntelyä niin paljon, että perustelisi henkilötietojen käsittelyä vain sillä, että käsittelijällä on turvallisuusalan elinkeinolupa (esimerkiksi Halford v. The United Kingdom, kohdat 49-50). Tätä tukee sekin, että tietosuojalakia säädettäessä erityisten tietoryhmien käsittelyn kansalliset poikkeamat lainsäädännössä katsottiin oikeasuhtaisiksi, koska mahdollisuus käsitellä tietoja oli rajattu tietosuojalaissa mainittuihin toimijoihin ja tilanteisiin (HE 9/2018 vp, 89). Rikoksiin liittyvien tietojen osalta tällaista toimijoiden ja tilanteiden määrittelyä ei ole suoraan lakitekstissä.

Samalla perustelulla tietosuojalaki ei toisi mukanaan sellaisia käsittelytilanteita, joissa erityisiä henkilötietoryhmiä voitaisiin käsitellä yksityisetsivätoiminnassa. Kuten todettiin aiemmin luvussa Edellytykset, toimivaltuudet ja velvollisuudet rikoksen paljastamisessa, toimivaltuudet perustuvat erityissäännöksiin ja oikeuttamisperusteisiin. Edellä mainitut seikat huomioiden henkilötietojen käsittelystä tulisi olla erityissäännöksensä. Koska laissa yksityisistä turvallisuuspalveluista ei sellaisia ole, ei toimivaltuuksia pelkällä turvallisuusalan elinkeinoluvalla ole henkilötietojen käsittelyyn enempää kuin mitä muualta lainsäädännöstä voidaan johtaa.

Käytännössä yksityisetsivätoimintaan edellä esitetyistä perusteluista soveltuvat vain oikeusvaateisiin liittyvät asiat tai vakuutuspetoksia vakuutuslaitosten lukuun tutkivat etsivät. Yleisen tietosuoja-asetuksen osoitusvelvollisuusperiaatteen mukaan tällöinkin rekisterinpitäjän vastuulla on osoittaa, että käsittely on liittynyt nimenomaan siihen. Jos lähtökohtaisesti tiedetään, että oikeusvaadetta ei väärinkäytöksestä tulla esittämään, ei tällaisia tietojakaan saisi käsitellä. Edellä esitetyn perusteella myös rikoksiin liittyviä tietoja saa käsitellä vain tietyin perustein. Huolehtimisvelvoitteita tulee lisäksi paljon enemmän kuin informoinnista poikkeamisen yhteydessä.

Kun rikoksiin liittyviä tietoja käsitellään, tulee lisäksi huolehtia rekisteröityjen oikeuksien suojaamisesta (tietosuojalaki 1050/2018, 7 §, 2 mom.). Tietosuojalain (1050/2018) kuudennen pykälän toinen momentti määrittelee asianmukaiset ja erityiset toimenpiteet, joita sekä rekisterinpitäjän, että henkilötietojen käsittelijän on käytettävä rekisteröityjen oikeuksien suojaamiseksi ja näitä ovat:

1. toimenpiteet, joilla on jälkeenpäin mahdollista varmistaa ja todentaa kenen toimesta henkilötietoja on tallennettu, muutettu tai siirretty
2. toimenpiteet, joilla parannetaan henkilötietoja käsittelevän henkilöstön osaamista;
3. tietosuojavastaavan nimittäminen
4. rekisterinpitäjän ja käsittelijän sisäiset toimenpiteet, joilla estetään pääsy henkilötietoihin
5. henkilötietojen pseudonymisointi

6. henkilötietojen salaaminen
7. toimenpiteet, joilla käsittelyjärjestelmien ja henkilötietojen käsittelyyn liittyvien palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus taataan, mukaan lukien kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa
8. menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi
9. erityiset menettelysäännöt, joilla varmistetaan tietosuoja-asetuksen ja tämän lain noudattaminen siirrettäessä henkilötietoja tai käsiteltäessä henkilötietoja muuhun tarkoitukseen
10. tietosuoja-asetuksen 35 artiklan mukainen tietosuojaa koskevan vaikutustenarvioinnin laatiminen
11. muut tekniset, menettelylliset ja organisatoriset toimenpiteet

Lista ei ole täydellinen eikä se ole pakottava (HE 98/1998 vp, 91). Samoin tulee huomioida aiemmin esitetyt tietosuoja-asetuksen (679/2016) vaatimukset esimerkiksi osapuolten välisestä sopimuksesta, jos käsittelyä tehdään alihankintana. Nämä ovat siis lisävelvoitteita aiempiin, eivätkä korvaa muita tietosuojalainsäädännön vaatimuksia.

Tietosuoja-asetuksen (679/2016) viidennen artiklan toisesta kohdasta johtuu, että rekisterinpitäjän ja käsittelijän tulee osoittaa valittujen suojatoimien asianmukaisuus ja oikeasuhtaisuus (”osoitusvelvollisuus” (HE 9/2018 vp, 90). Edellä mainitut suojatoimet ovat tietosuoja-asetuksen rekisterinpitäjille määrittelemiä suojatoimia (HE 9/2018 vp, 91). Osa niistä, kuten esimerkiksi aiemmin käsitelty tietosuojaa koskeva vaikutustenarviointi henkilötietojen käsittelyssä tai tietosuojavastaavan nimittäminen voivat tulla joka tapauksessa eri käsittelytilanteista johtuen sovellettavaksi. Koska henkilötietojen käsittelyssä on tunnistettava organisaatioon lain kautta kohdistuvat vaatimukset, ei suojatoimien tekemättä jättämistä voi perustella tietämättömyydellä (esimerkiksi 531/161/20, 13). Tästä voisi päätellä, että suojatoimista poikkeaminen ilman päteviä, kirjallisia perusteluja ei olisi mahdollista. Tätä tukee myös tietosuojavaltuutetun ja seuraamuskollegion päätös (531/161/20), jossa tietosuojaa koskevan vaikutustenarvioinnin tekemättä jättämistä ei voitu pitää perusteltuna, koska rekisterinpitäjä ei voinut osoittaa, että tarpeellisuutta olisi asianmukaisesti arvioitu (14).

5.6 Viestintäpalvelulaki

Sähköistä käsittelyä ja erityisesti viestintään liittyvien tietojen käsittelyä säädellään laajemmin tässä erityislaissa kuin yleisessä tietosuoja-asetuksessa tai tietosuojalaissa. Yleinen tietosuojadirektiivi ja sähköisen viestinnän tietosuojadirektiivin edeltäjä, televiestinnän

tietosuojadirektiivi on huomioitu suomalaisessa sähköisen viestinnän lainsäädännössä jo ennen 2000-lukua (HE 85/1998, 6-7). Sähköisen viestinnän tietosuojalaissa huomioitiin nykyisin voimassa oleva sähköisen viestinnän tietosuojadirektiivi – lukuun ottamatta direktiiviin tietenkin myöhemmin 2011 tehtyjä lisäyksiä esimerkiksi tietosuojaloukkausten ilmoittamisesta ja suostumuksen hankkimisesta evästeiden ja vastaavien teknologioiden käytössä (HE 125/2003 vp, 6; Ustaran 2018, 56; Carey 2015, 14).

Silloinen sähköisen viestinnän tietosuojalaki tuli Suomessa kuuluisaksi siihen vuosina 2008–2009 tehtyjen lisäysten vuoksi. Lisäykset koskivat yhteisötilaajan oikeuksia käsitellä viestien välitystietoja (HE 48/2008 vp, 43-49). Koska yhteisötilaajalla tarkoitettiin viestintäpalvelun tai lisäarvopalvelun tilaajina toimivia yrityksiä, jotka käsittelivät verkoissaan käyttäjien luottamuksellisia tietoja, laajensi laki siis oikeutta työnantajille käsitellä työntekijöiden viestiliikennettä (HE 48/2008 vp, 3). Tämä toi sen aikaisen uutisoinnin vuoksi laille lisänimen ”Lex Nokia”, johtuen Nokiaan silloin liittyneistä urkintakohuista. Nimenomaan yhteisötilaajan oikeudet ovat se, miksi lakimuutos oli merkittävä myös rikosten paljastamisen näkökulmasta ja näihin palataankin jäljempänä.

Myöhemmin sähköisen viestinnän tietosuojalain korvasi tietoyhteiskuntakaari. Muutos liittyi sähköisen viestinnän kokonaisuudistukseen, jonka oli tarkoitus yhtenäistää sääntelyä ja poistaa päällekkäisyyksiä (HE 221/2013 vp, 3). Tietoyhteiskuntakaari taas muuttui lailla tietoyhteiskuntakaaren muuttamisesta (68/2018) laiksi sähköisen viestinnän palveluista. Sähköisen viestinnän palveluista annettu laki on tärkeä tässä yhteydessä siksi, että sen soveltamine ulottuu teleyritysten lisäksi myös yrityksiin, jotka tarjoavat esimerkiksi työntekijöilleen viestintäpalveluita (HE 221/2013, 95). Tässä yhteydessä elinkeinonharjoittajaan viittaava yhteisötilaaja sisältyy viestinnän välittäjien määritelmään ja siihen kuuluvat teleyritysten ja yhteisötilaajien lisäksi myös kaikki sellaiset tahot, joiden palvelu perustuu luottamuksellisen viestinnän välittämiseen. Siten esimerkiksi Facebook ja Suomi24 -palveluissa välitetty luottamuksellinen viestintä menee lain soveltamisalaan (HE 221/2013, 92).

5.6.1 Sähköisen viestin, välitystietojen ja rikoksia koskevien tietojen käsittely

Olennaista viestintäpalvelulaissa on se, että se ei missään tilanteissa anna kenellekään sivulliselle oikeutta toisen henkilön viestien sisältöihin. Kaikki oikeudet, joita yrityksille ja yhteisötilaajille lain myötä tulevat, koskevat niin sanottuja viestinnän tunnistetietoja (myös välitystiedot) yhtä poikkeusta lukuun ottamatta, johon palataan myöhemmin. (HE 48/2008 vp, 15). Mutta esimerkiksi yrityssalaisuuksien luvattoman luovuttamisen tutkinnassa annetut oikeudet eivät ulotu viestien sisältöihin, vaan viestien sisällöt on erityisesti rajattu ulkopuolelle (HE 48/2008 vp, 38).

Yksityisetsivätoiminnan yhteydessä tulee muistaa myös tietosuojadirektiivin (2002/58/EY) artikla viisi. Siinä erityisesti kielletään käyttäjien päätelaitteiden kuuntelu, viestien sieppaaminen tai laitteelle tallennettujen tietojen käyttö tai tietojen tallentaminen käyttäjän laitteelle ilman suostumusta (tietosuojadirektiivi 2002/58/EY, artikla 5). Artiklan perustelut ovat tietosuojadirektiivin (2002/58/EY) resitaalissa 24, joka määrittelee käyttäjän laitteet kuuluvan heidän yksityiselämänsä piiriin. Tätä voisi pitää eräänlaisena kotirauhan määritelmän laajennuksena: Samalla tavalla kuin ei ole oikeutta tunkeutua toisen kotirauhan suojaamalle alueelle, ei ole oikeutta tunkeutua toisen omistamalle laitteelle ilman lupaa.

Hallituksen esitys (HE 48/2008 vp) puhui tunnistamistiedoista, jotka ovat tilaajaan tai käyttäjään liittyviä tietoja, joita tarvitaan viestien siirtämiseksi tai jakelemiseksi. Näihin voi sisältyä viestien reititystietoja, tietoja viestinnän kestosta, määrästä, ajankohdasta ja käytetystä protokollasta ja viestin muodosta sekä viestinnän alku- ja loppupisteestä ja mahdollisesti päätelaitteen sijainnista (HE 48/2008 vp, 3). Nämä sisältyvät voimassa olevan viestintäpalvelulain (917/2014) määritelmään välitystiedoista (3 §). Tunnistamistiedoilla ja välitystiedoilla viitataan siis samaan asiaan (HE 221/2013 vp, 17). Viestintäpalvelulain (917/2014) viestinnän luottamuksellisuuden suoja ulottuu myös oikeushenkilöihin, joten suoja on laajempi kuin yleisessä tietosuoja-asetuksessa henkilötietojen käsittelyyn liittyvä suoja (3 §, kohta 30 ja 40; HE 48/2008 vp, 16; tietosuoja-asetus 679/2016, henkilötiedon määritelmä artikla 4 ja aineellinen soveltamisala artikla 2).

Viestintäpalvelulain (917/2014) 136 § määrittelee, että viestinnän osapuolella on aina oikeus käsitellä omia viestejään ja niihin liittyviä välitystietoja ja niitä saa käsitellä vain viestinnän osapuolen suostumuksella, jollei laissa toisin säädetä. Yleisissä käsittelyperiaatteissa määritellään periaatteet, joilla viestinnän välittäjä tai tilaaja tai näiden lukuun toimiva voi viestejä ja välitystietoja käsitellä. Niiden mukaan välitystietoja ei saa luovuttaa kuin tahoille, joilla on oikeus käsitellä niitä ja lähtökohtaisesti käsittelyä saa suorittaa vain välittäjän tai tilaajan lukuun toimiva. Käsittelyn jälkeen ne on myös hävitettävä tai anonymisoitava. Yksityisyyden tai viestinnän suojaa ei saa rajoittaa enempää kuin käsittelyn kannalta on tarpeen ja käsittelyä saa suorittaa vain tarkoituksen vaatimassa laajuudessa. (Viestintäpalvelulaki 917/2014, 137 §). Näitä tarkoituksia ovat viestintäpalvelulain (917/2014) mukaan seuraavat (luku 17):

1. Viestinnän välittäminen, palvelun toteuttaminen ja tietoturvasta huolehtiminen
2. Laskutus
3. Markkinointi
4. Tekninen kehittäminen
5. Tilastollinen analyysi
6. Väärinkäytökset
7. Teknisen vian tai virheen havaitseminen

Kaikesta välitystietojen käsittelystä tulee tallentua tieto siitä, miten välitystietoja on käsitelty ja näitä tietoja tulee säilyttää kahden vuoden ajan niiden tallentamisesta (Viestintäpalvelulaki 917/2014, 144 §). Rikoksiin liittyviä tietoja voivat käsitellä kyseisen lain (917/2014) mukaan vain teleyritykset tietyin edellytyksin (145 §). Tämä oikeus ei koskisi siis yhteisötilaajana toimivia yrityksiä.

Tilastollisella analyysillä voitaisiin tuottaa tietoa myös väärinkäytöksistä, mutta viestintäpalvelulain (917/2014) 142 § ei liity sellaiseen tarkoitukseen. Tilastollinen analyysi tarkoituksena on varattu sellaiseen, jossa viestinnän välittäjä pyrkii esimerkiksi ennakoimaan hinnoittelumuutosten vaikutuksia palveluun, eikä analyysistä saa olla tunnistettavissa luonnollista henkilöä (HE 48/2008 vp, 17). Väärinkäytösten tai rikosten tutkimiseen voisi ajatella soveltuvan myös edellä esitetyn listan kohta viisi, mutta sen osalta pykälä määrittelee väärinkäytökseksi esimerkiksi maksullisen viestintäpalvelun käytön maksutta (viestintäpalvelulaki 917/2014, 143 §). Siten se ei sovellu kuin sen kaltaisten väärinkäytösten tutkintaan, ei minkä tahansa väärinkäytöksen. Tässäkään yhteydessä ei ole tarkoitus, että yksittäistä käyttäjää voitaisiin tunnistaa tai seurata, vaan viestinnässä tapahtuvien poikkeamien analyysillä tuottaa tietoa mahdollisesta luvattomasta käytöstä (HE 48/2008 vp, 19). Siten syyllisen saattaminen rikosoikeudelliseen vastuuseen yksityissektorin toimijan toimesta tämän pykälän perusteella ei olisi todennäköisesti mahdollista.

Tietoturvasta huolehtimisen yhteydessä on tavoitteiksi erityisesti mainittu haittaa aiheuttavien häiriöiden havaitseminen, estäminen, selvittäminen ja esitutkintaan saattaminen. Lain perusteluteksteissä viitataan haittaohjelmien laajaan levittämiseen, palvelunestohyökkäyksiin, käyttäjätietojen urkintaan, ei toivottuun suoramarkkinointiin tai tietojärjestelmien tai tietoliikenteen lamauttamiseen liittyviin uhkiin. (HE 48/2008 vp, 29). Käytännössä tämä tulisi suorittaa ensisijaisesti automaattisella analyysilla ja liikenteen suodattamisella (HE 48/2009 vp, 30). Tietoturvasta huolehtimisen tavoitteet on uudessa viestintäpalvelulaissa (917/2014) määritelty seuraavasti (272 §):

1. Verkkoihin, niihin liittyviin palveluihin ja järjestelmiin haitta aiheuttavien häiriöiden havaitsemiseksi, estämiseksi ja selvittämiseksi sekä esitutkintaan saattamiseksi
2. Viestinnän osapuolten viestintämahdollisuuksien turvaamiseksi
3. Laajamittaisten maksuvälinepetosten valmistelun ehkäisemiseksi

Laki antaa tässä tilanteessa mahdollisuuden myös yksittäisen viestin manuaaliseen tutkimiseen, jos se tapahtuu edellä mainittujen tarkoitusten toteuttamista varten, viesti sisältää todennäköisesti haittaohjelman ja manuaalisesta käsittelystä ilmoitetaan viestinnän osapuolille (viestintäpalvelulaki 917/2014, 272 §). Oikeus ei olisi kuitenkaan mikään yleinen tarkastusoikeus, vaan erityinen poikkeustilanne, jossa toimenpiteet on toteutettava huolellisesti vaarantamatta sananvapautta, yksityisyyden suojaa tai viestin

luottamuksellisuutta siten, että viestien sisällöt paljastuisivat ulkopuolisille (HE 48/2008 vp, 31 ja 41).

Edellä mainittujen seikkojen perusteella viestintään, viestintäverkkoihin ja niihin liittyviin palveluihin kohdistuvia uhkia voidaan tutkia siis suoraan yhteisötilaajan tai tämän lukuun toimivan toimesta. Kyseessä voi olla myös rikos – esimerkiksi törkeä tietoliikenteen häirintä (rikoslaki 39/1889, luku 38, 3 §). Viestintäpalvelulain (917/2014) perusteella tällaisten rikosten tutkintaan ei kuitenkaan tarvittaisi rikoksen paljastamiseen liittyvää elinkeinolupaa. Toisaalta tutkintaoikeus on rajattu nimenomaan viestinnän jatkuvuuteen ja turvallisuuteen kohdistuviin uhkiin. Jos tavoitteena on nimenomaan edellä mainittuihin uhkiin varautuminen, voisivat edelliset oikeudet välitystietojen käsittelyssä soveltua myös yksityisetsivätoimintaan. Ei kuitenkaan esimerkiksi työntekijän epärehellisyyden tai petoksen selvittämiseksi, joihin palataan myöhemmin. Tutkinnan tavoitteena ei kuitenkaan voi olla epäillyn rikoksen lopullinen selvittäminen, koska yhtenä tavoitteena on mainittu esitutkintaan saattaminen. Oikeus esitutkinnan suorittamiselle taas on varattu esitutkintalaissa poliisille, rajavartiolaitokselle, tullille ja sotilasviranomaisille (esitutkintalaki 805/2011, 1 §). Siten voisi päätellä, että lain tarkoituksena olisi se, että tutkintaa voidaan jatkaa vain niin pitkälle, että se voidaan viedä viranomaiselle.

Yhden poikkeuksen tiedonsaantioikeuteen muodostavat tekijänoikeudet. Viestintäpalvelulaki (917/2014) edellyttää, että tietoyhteiskunnan palvelun tarjoajan on tekijänoikeuden haltijan kirjallisesta määrämuotoisesta pyynnöstä estettävä tekijänoikeutta loukkaavan materiaalin saanti ja ilmoitettava siitä edelleen sisällön tuottajalle (189 § - 192 §). Tuomioistuimen päätöksellä voi teleyritys myös luovuttaa oikeudenloukkaukseen käytetyn liittymän haltijan yhteistiedot (HE 235/2010, 6 ja 17). Tiedonsaantioikeus perustuu tekijänoikeuslain (404/1961) 60 a §:ään, jossa määritellään myös asian vireille saattamisesta käräjäoikeuteen toimitettavalla kirjallisella hakemuksella (myös oikeudenkäymiskaari 4/1734, luku 8, 1 §).

Suomessa näiden niin sanottujen ”tekijänoikeuskirjeiden” (esimerkiksi Komonen 2016) tai ”piratismikirjeiden” postittelu liittymien haltijoille loppui aika lailla vuonna 2017, jonka jälkeen markkinaoikeus ei ole tehnyt uusia luovutuspäätöksiä tekijänoikeuksia loukkaavien liittymäomistajien tiedoista (Linnake & Kärkkäinen, 2018). Taustalla on oletettavasti Euroopan unionin tuomioistuimen ns. Tele2 -päätös, jossa tuomioistuin edellytti, että tietojen tallentamiselle ja käsittelylle tulee edellytyksenä olla myös se, että rikos on vakava (yhdistetyt tapaukset C-203/15 ja C-698/15, kappaleet 114 ja 115). Ottaen huomioon myöhemmin annettu päätös tapauksessa Mircom vs. Telenet BVBA (C-597/19), kyse ei olisi kuitenkaan kategorisesta kiellosta käsitellä ja luovuttaa tietoja, vaan nimenomaan oikeasuhtaisuuden perusteluiden olemassaolosta.

5.6.2 Yhteisötilaajaa koskevat erityiset oikeudet

Viestintäpalvelulain (917/2014) 18. luku tuo kuitenkin yhteisötilaajille kaksi oikeutta, jotka lähenevät tällaisia oikeuksia. Ne ovat yhteisötilaajan oikeudet käsitellä välitystietoja:

1. Maksullisen tietoyhteiskunnan palvelun, viestintäverkon tai -palvelun luvattoman käytön selvittämiseksi
2. Liikesalaisuuksien paljastamisen selvittämiseksi

Molempiin oikeuksiin liittyy ennakkohuolehtimisvelvoitteita sekä jälkikäteiseen ilmoittamiseen liittyviä velvoitteita, eivätkä nämä oikeudet ole automaattisesti kenen tahansa käytettävissä. Koska molemmissa on omat huolehtimisvelvoitteensa, on periaatteessa mahdollista ottaa käyttöön vain jompikumpi oikeuksista ja siksi ne käsitellään alla erikseen. Kaikki välitystietojen käsittely on suoritettava yksityisyyden suojaa ja viestien luottamuksellisuutta vaarantamatta ja käsitellyt välitystiedot on tuhottava tai anonymisoitava käsittelyn jälkeen, kuten aiemmin todettiin. Väärinkäytökset tulee myös käsitellä ensisijaisesti muiden keinojen, kuin välitystietojen käsittelyn kautta (HE 48/2008, 37). Koska välitystietojen käsittelyn tulee olla välttämätöntä, tulee tämän välttämättömyysvaatimuksen vuoksi rajata käsittely yksittäisen käyttäjänkin osalta vain tarpeellisiin tietoihin; Esimerkiksi tutkittaessa haittaohjelmien levittämistä yritysverkosta, voisi käsittely kohdistua vain lähetettyyn viestiliikenteeseen, mutta ei saapuvaan (HE 48/2008, 19-20). Toisaalta saapuvaankin liikenteeseen voitaisiin tarpeen tullen toimenpiteitä kohdistaa (HE 48/2008 vp, 29).

Välttämättömyysvaatimuksesta johtuu myös se, että välitystietoja voi käsitellä vain nimenomaisiin tarkoituksiin, eikä esimerkiksi työajan seuraamiseksi tai sen paljastamiseksi, onko käyttäjä ollut yhteydessä työsuojeluviranomaisiin (HE 48/2008 vp, 19–20). Automaattista tai manuaalista käsittelyä ei saa myöskään kohdistaa sananvapauden käyttämisen yhteydessä viestin lähettäjän selvittämiseksi (viestintäpalvelulaki 917/2014, 151 §; oikeudenkäymiskaari 4/1734, luku 17, 20 §).

Ennen välitystietojen käsittelyn aloittamista, on yhteisötilaajan nimettävä käsittelyä tekevät henkilöt tai määriteltävä tehtävät, joissa välitystietoja käsitellään. Jos kyseessä on työnantaja, johon sovelletaan yhteistoimintalakia, tulee menettelyt ja perusteet käsitellä myös yhteistoimintamenettelyssä (myöhemmin YT-menettely) ja tiedotettava työntekijöitä ja heidän edustajiaan, kuten työelämän tietosuojalaissa määritellään. Jos työantajaan ei sovelleta yhteistoimintalakia, tulee työntekijöitä kuitenkin kuulla ja informoida käsittelystä. Jos kyseessä on yhteisötilaaja, joka ei ole työnantaja on välitystietojen menettelyt ja käytännöt kuitenkin informoitava käyttäjille. (Viestintäpalvelulaki 917/2014, 148 §).

Ennen kuin välitystietojen käsittelyä voidaan aloittaa edellä mainittujen oikeuksien käyttämiseksi, tulee asiasta tehdä viestintäpalvelulain (917/2014) mukaan ennakkoilmoitus tietosuojavaltuutetulle (154 §). Tämän ennakkoilmoituksen tarkoitus on parantaa käyttäjien oikeusturvaa ja antaa valvontaviranomaiselle mahdollisuudet toteuttaa välitystietojen käsittelyyn liittyvää valvontaa (HE 48/2008 vp, 28). Ennakkoilmoituksessa tulee viestintäpalvelulain (917/2014) pykälän 154 mukaan olla:

1. Luvattoman käytön selvittämiseksi ja liikesalaisuuksien luovuttamisen paljastamiseksi käytettävien menettelyjen perusteet ja käytännöt
2. Tehtävät tai henkilöstö, jolla on oikeus käsitellä välitystietoja
3. Miten yhteisötilaaja on toteuttanut tiedottamisvelvoitteensa henkilöstöedustajille tai henkilöstölle

Luvattoman käytön selvittäminen kohdistuu aiemmin läpikäytyjen käsittelytarkoitusten mukaan itse tietojärjestelmään ja viestintäpalveluihin ja järjestelmiin. Luvattoman käytön taustalla voi olla esimerkiksi epätavallisen suuret viestintäpalveluun liittyvät kustannukset. (HE 48/2008 vp, 20). Luvattomien laitteiden tai ohjelmien asennus tai pääsyn antaminen sivullisille yhteisötilaajan järjestelmiin ja verkkoihin olisi pääsääntöisesti luvatonta käyttöä (viestintäpalvelulaki 917/2014, 146 §). Välitystietoja saa käsitellä viestintäpalvelulain (917/2014) mukaan vain automaattisesti, mutta manuaalinen käsittely edellyttää perusteltua syytä epäillä luvatonta käyttöä (149 §):

1. Automattisella käsittelyllä on havaittu poikkeama
2. Tietoyhteiskunnan palvelun käyttökustannukset ovat nousseet epätavallisesti
3. Verkosta löydetään luvattomasti asennettu laite, ohjelmisto tai palvelu
4. Yksittäistapauksissa muista edelliseen rinnastettavasta, yleisesti havaittavasta seikasta, että viestintäverkkoa, -palvelua tai maksullista tietoyhteiskunnan palvelua käytetään luvatta

Edellytyksenä välitystietojen manuaaliselle käsittelylle on myös se, että tapahtuma aiheuttaa yhteisötilaajalle merkittävää vahinkoa ja luvattoman käytön, sen vastuullisten selvittäminen ja käytön lopettaminen edellyttää välitystietojen käsittelyä (viestintäpalvelulaki 917/2014 vp, 149 §).

Ennakkohuolehtimisvelvoitteisiin kuuluu yhteistoiminta- ja tiedottamismenettelyiden lisäksi myös muita toimenpiteitä. Yhteisötilaajan on ensinnäkin ryhdyttävä itse toimenpiteisiin verkon tai palvelunsa suojaamiseksi tavanomaisin tietoturvatoimenpitein. Lisäksi yhteisötilaajalta edellytetään, että se ohjeistaa käyttäjänsä siitä millaisia viestejä verkossa saa välittää, miten palvelua saa tai ei saa käyttää ja mihin viestintä ei ole sallittua. (Viestintäpalvelulaki 917/2014, 147 §).

Liikesalaisuuksien luovuttamisen paljastamiseksi voidaan välitystietoja käsitellä myös sekä automaattisesti, että manuaalisesti. Automaattinen käsittely voi kohdistua esimerkiksi viestien kokoon, liikenteen määrään, tyyppiin, yhteystapaan tai kohdeosoitteisiin. (Viestintäpalvelulaki 917/2014, 150 §). Manuaalinen käsittely edellyttää saman lain (917/2014) 150 §:n perusteella lisäksi:

1. Automaattisella käsittelyllä havaittua poikkeamaa
2. Liikesalaisuuden julkaisemista tai luvatonta käyttöä
3. Yksittäistapauksissa muista edelliseen rinnastettavasta, yleisesti havaittavasta seikasta johtuvaa epäilyä, että liikesalaisuuksia on luvattomasti luovutettu

Samoin kuin luvattoman käytön osalta, tulee tässäkin täytyä lisäksi muitakin edellytyksiä. Liikesalaisuuden tulee olla yhteisötilaajan tai sen kumppanien elinkeinotoiminnan kannalta keskeinen, tai luovuttamisen tulee kohdistua teknologisiin tai muihin kehittämistyön tuloksiin, jotka ovat todennäköisesti merkittäviä elinkeinotoiminnan käynnistämisen tai harjoittamisen kannalta. Samoin välitystietojen käsittelyn tulee olla välttämättömiä tapahtuman ja siitä vastuullisten selvittämiseksi. (Viestintäpalvelulaki 917/2014, 150 §). Liikesalaisuus ei ole mitä tahansa salassa pidettäväksi määriteltyä tietoa, vaan sen määritelmään sovelletaan sitä, mitä seuraavassa luvussa Työelämän tietosuojalainsäädäntö on esitetty (HE 48/2008 vp, 20).

Yhteistoiminta- ja tiedottamismenettelyiden lisäksi on tässäkin tapauksessa täytyttävä pari muutakin edellytystä. Liikesalaisuuksiin pääsyä on rajoitettava muilla asianmukaisilla tietoturvallisuusmenettelyillä, esimerkiksi salassapitosopimuksilla ja merkittäviä etuja suojatessa työntekijöiden luotettavuusselvityksillä (HE 48/2008 vp, 20). Myös käyttäjähallinto ja erityisesti käyttäjien määrittely, joilla on oikeus käsitellä kyseisiä tietoja, on merkittävää (HE 48/2008 vp, 21-22). Muun muassa siksi, että välitystietojen käsittelyoikeus koskee vain sellaisia henkilöitä, joilla on ollut pääsy liikesalaisuuksiin (HE 48/2008 vp, 26). Liikesalaisuuksien käsittelylle on laadittava hyväksytyn tai kielletyn käsittelyn periaatteet ja ohjeet heitä varten, joille on erityisesti määritelty oikeus käsitellä kyseisiä liikesalaisuuksia. (Viestintäpalvelulaki 917/2014, 147 §). Viestintäpalvelulailla ei ole kuitenkaan tarkoitus rajoittaa muiden tietohallinnollisten keinojen käyttöä, vaan varmistaa viestinnän luottamuksellisuus ja yksityisyydensuoja. Siten käyttäjälokien ja kirjautumislokien käsittely, tietojen tallentamisen ja siirron selvittäminen mukaan lukien ulkoiset tietovälineet ja esimerkiksi tulostamista koskevat tiedot olisivat työnantajan käytettävissä viestintäpalvelulaista huolimatta (HE 48/2008 vp, 20).

Oli kysymys luvattoman käytön selvittämisestä tai liikesalaisuuksien paljastamisesta, on molemmissa tapauksissa manuaalisesta käsittelystä laadittava viestintäpalvelulain (917/2014) 152 pykälän mukaan selvitys, josta ilmenee:

”1) käsittelyn peruste, ajankohta ja kesto;

2) syy, minkä vuoksi välitystietojen manuaaliseen käsittelyyn on ryhdytty;
3) käsittelijät;
4) käsittelystä päättänyt henkilö.”

Selvitys on allekirjoitettava osallistujien toimesta ja sitä on säilytettävä kaksi vuotta välitystietojen käsittelyn päättymisestä. Selvitys tulee luovuttaa myös heille, joiden välitystietoja on käsitelty heti, kun se voi tapahtua ilman käsittelyn syyn vaarantumista. Näillä käyttäjillä on oikeus käyttää ja luovuttaa selvitys omiin etuihin ja oikeuksiin liittyvän asian käsittelemiseksi. Selvitystä ei tarvitse luovuttaa kuitenkaan sellaisille käyttäjille, jotka ovat ehkä olleet tutkittavassa aineistossa, jota on käsitelty massamuotoisesti, mutta joiden välitystiedot eivät ole tulleet käsittelijän tietoon. (Viestintäpalvelulaki 917/2014, 152 §). Myös työntekijöiden edustajille on tehtävä vuosittain selvitys, mistä käy ilmi manuaalisen käsittelyn osalta käsittelykertojen määrä ja käsittelyn perusteet. Selvitys tulee antaa luottamusmiehelle, luottamusvaltuutetulle, yhteistoimintaedustajalle tai jos näitä ei ole valittu, kaikille henkilöstöryhmään kuuluville työntekijöille. (Viestintäpalvelulaki 917/2014, 153 §). Jälkikäteisselvitys manuaalisesta käsittelystä on annettava myös tietosuojavaltuutetulle vuosittain. Selvityksestä tulee ilmetä samat asiat kuin henkilöstöedustajille luovutettavasta selvityksestä. (Viestintäpalvelulaki 917/2014, 154 §).

Selainvälimuistien osalta on muistutettava siitä, että verkkoselailussa syntyvät tiedot ovat usein myös välitystietoja, jos selainta käytetään viestintään. Selain voi kysyä lupaa ja tallentaa myös sijaintietoja, joiden käsittely kuuluu lähtökohtaisesti työelämän tietosuojalainsäädännön tekniseen valvontaan, jota käsitellään seuraavassa luvussa. Mutta lähtökohtaisesti työnantajalla ei ole oikeutta käsitellä välitystietoja kuin viestintäpalvelulain mainitsemissa tilanteissa, jolloin selainten käytön seuranta ei kuulu automaattisesti työnantajan oikeuksiin (Tietosuojavaltuutetun toimisto 2021b).

Välttämättömyysperiaatteen ja etenkin manuaalisen käsittelyn tarkkarajaisuuden vuoksi voidaan siis sanoa, että kynnys puuttua yksittäisten käyttäjien liikenteeseen ei voi olla yleinen tai rutiininomainen menettelytapa, vaan edellyttää aina tapauskohtaista arviota. Koska viestivälitystiedot ovat lisäksi henkilötietoja sen vuoksi, että ne voivat olla liitettävissä luonnollisiin henkilöihin, tulisi osoitusvelvollisuuden täyttymiseksi perusteiden ja tarkoitusten olla mielellään kirjallisesti perusteltuja. Edellisistä voisi myös päätellä, että ellei yhteisötilaaja itse pyri suojaamaan verkkoaan luvattomalta käytöltä, ei luvatonta käyttöä voi osoittaa. Luvattomana käyttönä ei voisi siten tutkia sellaista käyttöä, jota ei ole määritelty ja ohjeistettu luvattomana. Samoin liikesalaisuuksien luovuttamista on mahdotonta tutkia, ellei luovutetuiksi epäiltyjä aineistoja ole muuten pyritty suojaamaan ja että ne on määritelty ja ohjeistettu liikesalaisuuksiksi.

Hallituksen esitys (HE 48/2008 vp) viestintäpalvelulainsäädännöksi mainitsee tavanomaisten tietohallinnollisten toimien, kuten tiedostojen tallentamisen tai tulostamisen käsittelyn kuuluvan viestintäpalvelulain rajoitusten ulkopuolelle, ja mainitsee, että näiden tietojen avulla pystytään vain harvoin selvittämään yrityssalaisuuden paljastuminen kokonaisuudessaan (20). Toisaalta ottaen huomioon aiemmin esitetyn, ei välitystietojenkaan perusteella sitä voida usein kokonaisuudessaan tehdä. Jos lainsäätäjän tarkoitus on ollut turvata välitystietojen käsittelyllä työnantajan oikeuksia, ei se tämän päivän yhteiskunnassa toteudu vain sallimalla välitystietojen käsittely. Jos taas tarkoituksena on ollut varsinaisen rikosten paljastamisen ja selvittämisen oikeuden siirto yksityissektorilta poliisille, on lain kehityssuunta siinä mielessä onnistunut. Joka tapauksessa ilman oikeutta viestisisältöihin ei voida mitenkään aukottomasti osoittaa liikesalaisuuden luovuttamisen paljastamista ja sitä oikeutta ei viestintäpalvelulakikaan anna.

Viestintäpalvelulaki ei kuitenkaan ota kantaa tilanteeseen, jossa viestivälitystietoja käsittelisi vaikkapa liikesalaisuuksien luovuttamiseen liittyen rikoksen paljastamiseksi ulkopuolinen taho toimeksiantosopimukseen perustuen. Tässä luvussa käsitellyt oikeudet on kuitenkin varattu vain yhteisötilaajalle itselleen. Kuten aiemmin tässä työssä todettiin, on poliisin näkemys se, että rikoksen paljastamiseen ansaintatarkoituksessa tulisi olla turvallisuusalan elinkeinolupa. Ja Lex specialis -periaatteen mukaan yleissäännöstä voidaan poiketa vain erityissäännöksen ollessa voimassa, joten yksityisetsivällä tulisi olla joka tapauksessa turvallisuusalan elinkeinolupa.

5.7 Työelämän tietosuojalainsäädäntö

Työelämää säätelee muutama yleislaki, joita täydentää tiettyjä toimialoja koskeva erityislainsäädäntö tai työehtosopimukset. Lähtökohtaisesti työelämässä toimitaan siten, että työntekijän on noudatettava työssään työnantajan määräyksiä työn suorittamisesta ja työnantajan vastuulla on huolehtia, että työntekijät suoriutuvat töistään (työsopimuslaki 55/2001, luku 3, 1 § ja luku 2, § 1). Työnantajalla on velvollisuus myös ohjata ja valvoa toimintaa: esimerkiksi osakeyhtiölaissa hallitus huolehtii yleistoimivallasta (624/2006, luku 6, 2 §). Julkisten yhtiöiden osalta velvoite on ulotettu erikseen mainiten sisäiseen valvontaan, tarkastuksiin ja riskienhallintaan asti (624/2006, luku 6, 16 §). Jos hallitus tässä epäonnistuu, voi vastuu muodostua jopa henkilökohtaiseksi (624/2006, luku 22, 1 §).

Myös työturvallisuuslaki edellyttää työnantajaa perehdyttämään työntekijät työhön, työvälineisiin ja niiden oikeaan käyttöön (työturvallisuuslaki 738/2002, luku 2, 14 §). Henkilötietojen käsittelyn osalta rekisterinpitäjänä toimiva työnantaja on nimenomaisesti velvollinen ohjeistamaan henkilötietojen käsittelyn sekä valvomaan ja päivittämään ohjeita (tietosuoja-asetus 679/2016, artiklat 24, 25 ja 29). Siten henkilötietojen käsittely

asiakasyrityksissä tai yksityisetsivillä ei voi olla koskaan kiinni työntekijöistä tai heidän osaamisestaan, vaan johdon on huolehdittava käsittelyn ohjeistamisesta ja valvonnasta.

Suomessa on aika yksityiskohtaista sääntelyä työelämään liittyen, kuten tässä luvussa myöhemmin tullaan osoittamaan. Se saattaa ainakin vaikuttaa olevan osin ristiriidassa yleisen tietosuoja-asetuksen kanssa. Tietosuoja-asetuksen (679/2016) artikla 88 määrittelee, että jäsenvaltiot voivat antaa lainsäädännössä yksityiskohtaisempaa sääntelyä työoikeuden alalla (kohta 1). Tämän on tulkittu tarkoittavan ensisijaisesti sitä, että tietosuoja-asetuksen minimivaatimuksista henkilötietojen suojaamisen osalta ei voida poiketa (Kuner et al. 2020, 1238). Tämä jättää kuitenkin auki sen kysymyksen, voivatko säännökset olla tiukempia. Esimerkiksi Nyyssölä (2020) tulkitsee asiaa sitä kautta, että sanamuoto muutettiin tietosuoja-asetusta valmistellessa myöhemmin ”tiukemmasta” ”yksityiskohtaisemmaksi” sen välttämiseksi, että jäsenvaltioille ei syntyisi taas erilaista lainsäädäntöä (68). Komissio lisäksi kokoaa nämä lainsäädäntöjen eroavaisuudet yhteen, joten tieto harmonisointitarpeista ainakin tulevaisuudessa voidaan todennäköisesti huomioida (Tietosuoja-asetus, artikla 88, kohta 3; Kuner et al. 2020, 1238). Tietosuojan kansainvälisen taustan analyysistä ja edellisestä voisi kuitenkin päätellä, että työelämään liittyvä työlainsäädäntö ei voisi olla tiukempaa kuin tietosuoja-asetus.

Suomessa on lisäksi kaksi merkittävää lakia rikoksen paljastamisen näkökulmasta, jotka määrittelevät työntekijöiden oikeuksia ja yksityisyyttä sekä työnantajan oikeuksia ja huolehtimisvelvoitteita; Laki yhteistoiminnasta yrityksissä (334/2007, myöhemmin yhteistoimintalaki) ja laki yksityisyyden suojasta työelämässä (759/2004, myöhemmin työelämän tietosuojalaki). Työsuhteeseen liittyvää lainsäädäntöä on myös vuosilomalaissa ja työterveyshuoltolaissa, mutta nämä lait harvoin liittyvät työpaikalla tehtävään rikosten selvittämiseen, joten ne on jätetty siksi tästä pois. On kuitenkin hyvä tunnistaa, että tässä oleva lista työsuhteeseen liittyvästä lainsäädännöstä ei ole tyhjentävä.

Yhteistoimintalaki on turvaamassa työntekijöiden suuntaan läpinäkyvyyttä ja mahdollisuuksia vaikuttaa omien tietojensa käsittelyyn (HE luonnos 2021b, 16; HE 254/2006 vp, 39). Työelämän tietosuojalain (759/2004) toisen luvun neljäs pykälä viittaa henkilötietojen keruun käytänteiden työhönotossa ja työsuhteen aikana kuuluvan yhteistoimintalakiin (yhteistoimintalaki 334/2007). Sama pykälä viittaa myös lakeihin yhteistoiminnasta valtion virastoissa ja laitoksissa (1233/2013) sekä työnantajan ja henkilöstön välisestä yhteistoiminnasta kunnissa (449/2007). Julkishallinnon organisaatio voi olla toimeksiantajana yksityisetsivätoimeksiannoissa, mutta ei toimeksisaajana, joten julkihallintoon soveltuvaa lainsäädäntöä ei käsitellä tarkemmin tässä.

Yhteistoimintalaki kattaa myös yhteisöt, säätiöt ja luonnolliset henkilöt, jotka harjoittavat taloudellista toimintaa riippumatta siitä, onko niiden tarkoitus tuottaa voittoa vai ei

(yhteistoimintalaki 334/2007, 3 §). Sen ulkopuolelle jäävät aiemmin mainitut kunnat ja valtion laitokset, sekä yritykset, joissa työskentelee säännöllisesti alle 20 henkilöä. Nykyisessä laissa yritysten sisäiseen tai ostettuun väärinkäytöstutkintaan olennaisesti liittyviä pykäliä 15 ja 19, sovelletaan vain yrityksessä, jonka työsuhteessa olevien työntekijöiden määrä säännöllisesti on vähintään 30 (HE 254/2006 vp). Vuonna 2022 voimaan astuvassa yhteistoimintalain muutoksessa raja laskisi kuitenkin näiltäkin osin 20 työntekijään, jolloin lain soveltamisalan piiriin kuuluisi siis aiempaa pienempiä yrityksiä (HE 159/2021 vp, 64).

Työelämän tietosuojalaki täydentää ja tarkentaa myös yhteistoimintalain velvoitteita. Toisin kuin yhteistoimintalakia sovellettiin vain tietyn kokoisiin yrityksiin, työelämän tietosuojalakia sovelletaan kaikkeen työntekijän henkilötietojen käsittelyyn kaikkialla työelämässä (työelämän tietosuojalaki 759/2004, 1 § ja 2 §). Työelämän tietosuojalaissa on eräs tärkeä piirre, joka on huomioitava kaikkialla työelämässä: Työelämän tietosuojalaki edellyttää, että työnantaja saa käsitellä ”vain välittömästi työntekijän työsuhteen kannalta tarpeellisia henkilötietoja”. Käsittelyssä tulee huomioida työsuhteen molempien osapuolten oikeudet ja työtehtävien erityisluonne. Tästä tarpeellisuusvaatimuksesta ei voida poiketa, vaikka työntekijä antaisi suostumuksen tietojensa käsittelyyn laajemmin. (työelämän tietosuojalaki 759/2004, 3 §). Vaikka myöhemmin puhutaan myös työntekijän suostumuksesta, tulee tämä erityinen poikkeamiskielto huomioida aina. Tarpeellisuuden osoittaminen ei aina ole helppoa moninaisista tilanteista johtuen (esimerkiksi Nyyssölä 2020, 93) ja kun samalla huomioi tietosuoja-asetuksen osoitusvelvollisuuden (tietosuoja-asetus 679/2016, artikla 5), on tarpeellisuusarvio etenkin poikkeavissa ja monimutkaisissa tilanteissa syytä tehdä kirjallisena.

Yhteistoimintalain (334/2007) pykälät 15 ja 19 ovat siinä mielessä merkittäviä väärinkäytöstutkinnan näkökulmasta, että 15 § säätelee työhönotossa noudatettavia periaatteita ja käytäntöjä ja 19 § työsuhteen aikana tapahtuvan teknisen valvonnan toteuttamista. Jos yrityksessä on tapana työhönoton yhteydessä suorittaa erityisiä menettelyjä, kuten taustatarkistuksia tai luotettavuusselvityksiä, tulisi nämä olla käsiteltynä henkilöstö- ja ammattiryhmittäin yhteistoimintamenettelyssä (HE 254/2006 vp, 48). Saman lain pykälän 15 kolmas kohta laajentaa velvollisuutta käsitellä periaatteet ja käytännöt yhteistoimintamenettelyssä myös työsuhteen aikana työntekijöistä kerättävistä tiedoista (HE 254/2006 vp, 49). Työnhakijoiden tai työntekijöiden tietojen kerääminen taustaselvitysten tai väärinkäytöstutkinnan yhteydessä kuuluisi myös yhteistoimintamenettelyjen piiriin, etenkin jos se on joidenkin henkilöstöryhmien kohdalla säännönmukaista. Pääsääntö on, että tietoja saa hankkia vain työnhakijalta tai työntekijältä itseltään tämän suostumuksella. Hankittaessa tietoja muualta, tästä on kerrottava etukäteen ja viimeistään siinä kohtaa, kun tietoja käytetään häntä koskevassa päätöksenteossa. (Työelämän tietosuojalaki 759/2004, luku 2, 4 §). työntekijän suostumukseen liittyen on meneillään lakimuutos, jota käsitellään jäljempänä.

Taustaselvityksiin ja väärinkäytöstutkintaan voivat liittyä muun muassa päihdetestit tai luottotietojen hankinta. Huumausainetestejä voi suorittaa vain terveydenhuollon viranomainen ja todistuksia saa käsitellä vain työantaja työntekijän toimittamana (työelämän tietosuojalaki 759/2004, luku 3, 6 §). Myös alkoholitestit kuuluvat terveydenhuollon ammattilaisille (työelämän tietosuojalaki 759/2004, luku 4, 14 §). Luottotietoja voidaan hankkia yksityisetsivien toimeksiannoissa, mutta yksityisetsivät harvoin pitävät itse tällaisia rekistereitä. Periaatteessa yksityisetsivä voisi olla myös luottotietotoiminnan harjoittaja, kunhan toiminta täyttää lain vaatimukset ja tarvittavat ilmoitukset on tehty (luottotietolaki 527/2007, luku 3 ja 38 §). Päihdetestien teettäminen ei ole automaattisesti ilman perusteluja sallittua, muta työnantajalla on kuitenkin oikeus valvoa työntekijöitä (työelämän tietosuojalaki 759/2004, 7 § ja 8 §; HE 75/2000, 27). Työnantaja voi saada perustellun epäilyn huumausaineiden vaikutusten alaisena työskentelystä myös havainnoilla käyttäytymisestä tai työsuorituksesta, asiakaspalautteesta tai muista luotettavista tietolähteistä (HE 75/2000, 45). Työnantajalla olisi periaatteessa mahdollista käyttää tällaisessa valvonnassa avukseen myös ulkopuolista toimeksisaajaa, mutta toimeksiannossa olisi huomioitava, onko kyse vain yleisestä valvonnasta vai tarkoituksesta paljastaa rikos. Edellisen vaikuttaessa lähinnä ulkopuolisen toimeksisaajan osalta vaatimukseen turvallisuusalan elinkeinoluvasta.

Taustaselvityksiin voi kuulua myös henkilö- ja soveltuvuusarvioinnit. Niiden osalta ei ole määritelty esimerkiksi testaajaan liittyvää luvanvaraisuusvaatimusta – esimerkiksi terveydenhuollon toimilupaa. Työnantaja kuitenkin vastaa siitä, että testausmenetelmä on luotettava ja se tuottaa virheetöntä tietoa. Testin tulokset on luovutettava työntekijälle. (työelämän tietosuojalaki 759/2004, 13 §). Testejä voi kuitenkin Suomessa suorittaa kuka tahansa (HE 75/2000, 19). Turvallisuusselvitysten suorittaminen on määritelty turvallisuusselvityslaissa (726/2014) ja siellä on lueteltu toimivaltaiset viranomaiset, jotka selvityksiä voivat tehdä ja millä perusteilla (luvut 3 ja 4). Turvallisuusselvityslain taustalla on ollut henkilötietojen ja yksityisyyden suoja ja sen vuoksi laissa on yksilöity tarkkaan suorittavat viranomaiset ja käytettävät rekisterit (HE 57/213 vp, 69-70).

Turvallisuusselvityslaissa tai työelämän tietosuojalaissa ei kuitenkaan yksiselitteisesti kielletä luottavuuteen liittyvän soveltuvuuslausunnon hankkimista yksityisetsivältä. Joka tapauksessa työnantajaa sitoo velvollisuus ilmoittaa etukäteen tällaisten tietojen hankkimisesta ja jos niitä on hankittu muualta kuin työntekijältä, viimeistään silloin, kun niitä käytetään työntekijää koskevassa päätöksenteossa (työelämän tietosuojalaki 759/2004, 4 §). Todennäköisesti luotettavuusselvitys voisi sisältää vain haastattelun tai testinomaisen vaiheen, jolloin siinä tulla sovellettavaksi myös mitä soveltuvuusarvioinneista säädetään. Työnhakijan tai työntekijän rikoksiin liittyviä tietoja tällainen selvitys ei voisi sisältää (3048/41/2015, Tietosuojavaltuutetun vastaus ja kannanotto).

Työntekijän soveltuvuutta arvioitaessa terveydentilaan liittyvät tiedot voivat myös olla tärkeä osa. Myös luotettavuuden selvittämiseen voi joskus liittyä myös terveydentilaan liittyvien tietojen käsittelyä. Esimerkkinä voisi olla tapaus, jossa työntekijän epäillään olevan aiheetta sairaslomalla. Työelämän tietosuojalain (759/2004) viides pykälä ja hallituksen esitys (75/2000 vp, 24) ovat kuitenkin ehdottoman tarkkoja muotoilussaan, että terveydentilaan, poissa-olo-oikeuden selvittämiseen, sairausajan palkkaan, terveydentilaan liittyviin vastaaviin etuisuuksiin ja työkykyisyyden selvittämiseen tietoja saa kerätä vain työntekijältä itseltään tai hänen kirjallisella suostumuksellaan. Sen lisäksi näitä tietoja on säilytettävä erillään muista työnantajan tiedoista ja niitä saa käsitellä vain erikseen nimetyt henkilöt (työelämän tietosuojalaki 759/2004, 5 §). Edellä mainitussa viidennessä pykälässä on lause, että ”Lisäksi työnantajalla on oikeus käsitellä näitä tietoja niissä tilanteissa ja siinä laajuudessa, kuin muualla laissa erikseen säädetään.” (työelämän tietosuojalaki 759/2004, 5 §).

Lain valmisteluteksteissä sen on kuitenkin ajateltu tarkoittavan sitä, mitä on säädetty työturvallisuudesta ja työterveyshuollosta (HE 75/2000 vp, 26). Aiemmin mainitun perusteella yksityisetsivää ei voisi käyttää poissaolo-oikeuden selvittämiseen muutoin kuin tilanteessa, jossa vakuutusyhtiö tekisi selvitystä sille kuuluvan korvausvastuun osalta (tietosuojalaki 1050/2018, 6 §). Lain valmisteluteksteissä kuitenkin todetaan, että työnantajalla tulisi olla mahdollista tutkia työstä poissaolon aiheellisuus perustellusta syystä, koska hoitava lääkäri ei aina tunne työolosuhteita, eikä lääkärin lausunto siksi vastaa välttämättä todellista tilannetta (HE 75/2000 vp, 25). Jos henkilö on aiheetta pois töistä, mutta nostaa sairasajan palkan, täyttyy myös petoksen tunnusmerkistö (rikoslaki 39/1889, luku 36, 1 §).

Siten esimerkiksi rekisterinpitäjän oikeutettu etu elinkeinotoimintaansa kohdistuvan petoksen paljastamiseksi voisi tulla kyseeseen, koska tietosuoja-asetus on kuitenkin ensisijaisesti sovellettavaa lainsäädäntöä, kuten luvussa 5.2 todettiin. Tällaiseen rikokseen liittyvien tietojen käsittelyn oikeutus taas saataisiin tietosuojalain (1050/2018) seitsemännestä pykälästä, jos kyse olisi oikeusvaateen laatimisesta.

Yhteistoimintalain (334/2007) 19 § määrittelee yhteistoiminnassa käsiteltäväksi kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin suoritettavan valvonnan. Tekniseen valvontaan lukeutuu myös työntekijöiden paikantaminen (Tietosuojavaltuutetun toimisto 2021b). Vaikka yritykseen ei sovellettaisi yhteistoimintalakia, se ei vapauta teknisen valvonnan käsittelyvastuusta. Tähän palataan myöhemmin työelämän tietosuojalain kohdalla tässä luvussa. Tekninen valvonta pitää sisällään myös sähköpostin ja tietoverkkojen käytön periaatteet sekä edellisten käytön ohjeistamista. Jos työpaikalla suoritetaan teknistä valvontaa, tulisi se olla käsiteltynä yhteistoimintamenettelyssä ennen kuin näillä menetelmillä hankittuja tietoja voitaisiin käyttää esimerkiksi väärinkäytöstutkintaan. (HE 254/2006 vp, 52). Teknisestä valvonnasta tulee olla yhteistoimintalain (334/2007, 19 §, kohta 3) mukaan käsiteltynä sen:

- tarkoitus
- käyttöönotto
- käytetyt menetelmät

Teknisten menetelmien osalta ei kuitenkaan tarvitse kertoa kaikkia yksityiskohtia tietojen keruusta (HE 75/2000 vp, 4). Mutta vaikka valvonta on lainmukaista, on siitä silti kerrottava, koska työntekijällä on oikeus yksityisyyteen myös työpaikalla (HE 75/2000 vp, 30; Halford v. The United Kingdom, kohdat 16 ja 44).

Laki ei kuitenkaan avaa sen täsmällisemmin, miten tarkasti menetelmistä on kerrottava. Yhtenä linjauksena voisi ehkä pitää yhteistoimintalain perusteluja, jossa yrityksen turvallisuusjärjestelyt ovat sellaisia, joista yhteistoimintamenettelyn osapuolet ovat salassapitovelvollisia ja yksityiskohtaisten menetelmätietojen osalta voisi ajatella voitavan poiketa informoinnista jokaiselle työntekijälle (HE 159/2021 vp, 114). Toisena linjauksena voisi ajatella olevan työelämän tietosuojalain perustelut vuodelta 2003, joissa kameravalvonnasta todetaan, että ellei valvonta kohdistu suoraan yksittäiseen työntekijän työpisteeseen, ei kameroiden sijainnista tarvitsisi kertoa (HE 162/2003 vp, 52). Perusteluissa huomioidaan myös se, että yleisimmissä tiloissa yksityiskohtainen kameroiden sijainnin tieto voisi haitata esimerkiksi rikossarjojen selvittämistä, jos yksityiskohtainen sijainti olisi työntekijän tai ulkopuolisten tiedossa (HE 162/2003 vp, 53).

Työelämän tietosuojalain perusteluissa todetaan myös, että ILO:n (International Labour Organization) ohjeissa salainen valvonta tulisi sallia vain lailla tai jos on syytä epäillä rikosta tai vakavaa väärinkäytöstä ja että jatkuvana se tulisi sallia vain, jos se on edellytys terveyden, turvallisuuden tai omaisuuden suojelulle (HE 75/2000 vp, 29). Kuten luvussa Tietosuojalaki todettiin, informoinnista voi poiketa rikosten ehkäisyn tai selvittämisen osalta. Koska työelämän lainsäädäntö on kuitenkin työelämää koskevaa erityistä lainsäädäntöä, ei voida välttämättä ajatella tietosuojalain antaman oikeuden automaattisesti ohittavan sitä, mitä työlainsäädännössä on säädetty nimenomaan työelämän erityispiirteisiin liittyen.

Edellä olevista esimerkeistä voi poimia sen keskeisen ajatuksen, että rikoksen tai vakavan väärinkäytöksen yhteydessä tiedottamisesta voisi jonkin verran poiketa, jos valvonta ei ole syrjivää, esimerkiksi yhteen tai tiettyihin työntekijöihin kohdistettua. Joka tapauksessa informoinnista poikkeaminen vaatisi huolellista työnantajan etujen ja työntekijän oikeuksien välistä intressien punnintaa, josta vastuu on työnantajalla. Toki työnantajalla on muitakin keinoja valvoa työtä kuin tekninen seuranta, joten rajoitukset tämän osalta eivät tee kokonaan mahdottomaksi työnantajan mahdollisuuksia puolustaa oikeuksiaan.

Yhteistoimintalaista on huomioitava, että vaikka lain tavoite on, että yhteistoiminnan osapuolina työnantaja ja työntekijät sopisivat asioista yhdessä, ei käytännössä aina voida

päästä sopimukseen, eikä laki sitä siksi edellytä (HE 254/2006 vp, 54). Siten esimerkiksi teknisten menetelmien käytöstä ei tarvitse saada työntekijöiden suostumusta. Kannattaa kuitenkin huomioida, että aiemmin todetun mukaan työnantajan työnjohto-oikeuden vuoksi vastuu menetelmien lainmukaisuudesta on silti työnantajalla. Yhteistoimintamenettelyssä ei voida sopia myöskään lainvastaisesta toiminnasta, vaikka siihen henkilöstö suostuisikin. Tämä näkyy muun muassa Tietosuojavaltuutetun toimiston päätöksessä (3843/163/20), jossa yhteistoimintamenettelyssä käsitelty sijaintitiedon käsittely oli huomioitu rekisterinpitäjän pyrkimyksenä noudattaa lainsäädäntöä, mutta mikä ei poistanut teon rangaistavuutta lainvastaisena (luku Rikkomisen tahallisuus tai tuottamuksellisuus).

Voimassa olevan lain ja tulevan yhteistoimintalain muutoksen mukaan työantajan on tehtävä selkoa henkilöstöedustajille alihankintana ostetun ja vuokratun työvoiman käytöstä (HE 254/2006 vp, 48; HE 159/2021 vp, 74). Voimassa olevan lain perusteluteksti rajaa lain soveltamisen tilanteisiin, jotka ovat tilaajan toiminnassa tavanomaisesti suoritettavia työtehtäviä (HE 254/2006 vp 48). Uudessa laissa ei ole yhtä selvää rajausta, vaan siitä voisi saada kuvan, että se kattaisi tällaiset tehtävät laajemminkin. Mutta perustelutekstit toki viittaavat ylipäätään yhtiön henkilöstörakenteisiin ja henkilöstön jakautumiseen yksiköiden välillä, mistä voisi saada kuvan, että väärinkäytös- tai taustaselvityksissä käytetty alihankinta ei kuuluisi jatkossakaan yhteistoimintamenettelyn piiriin (HE 159/2021 vp, 74). Tätä voi tukea se, että uudessa laissa esimerkiksi muutosneuvotteluihin liittyvää yhteistoimintamenettelyä ei tarvitsisi käydä ostopalveluina hankittavasta työstä, joka ei liity yhtiön varsinaiseen ydinliiketoimintaan (HE 159/2021 vp, 90). Ilmeisesti lainsäätäjän tarkoitus ei ole ollut laajentaa yhteistoimintamenettelyä kaikkeen alihankintaan ja ostopalveluun, ellei kyseessä ole yrityksessä merkittävä toiminnan osa. Siten esimerkiksi satunnainen yksityisetsivän käyttö yhtiön toiminnassa ei olisi tällainen käsiteltävä asia.

Yhteistoimintalaki laajentaa menettelyissä salassa pidettävän tiedon koskemaan myös henkilön taloudellista asemaa ja muutoin henkilökohtaista tietoa (yhteistoimintalaki 334/2007, luku 9, 57 §). Taloudellista asemaa kuvaavan tiedon käyttö on tunnistettu tietosuoja-asetuksessa (679/2016) arkaluonteiseksi profiloinnin osalta, mutta se ei kuulu esimerkiksi yhdeksännen artiklan tarkoittamiin erityisiin tietoryhmiin (resitaali 71). Yksityisetsivän tutkinnan valmistelussa ja edetessä tulisi huomioida, että työelämän kontekstissa ihmisillä katsotaan edellistenkin lukujen perusteella olevan oma työsuhteesta erillinen henkilökohtainen elämä ja yksityisyys.

Yhteistoimintamenettelyn osapuolet ovat salassapitovelvollisia sellaisista tiedoista, jotka liittyvät työnantajan liikesalaisuuksiin tai turvallisuusjärjestelyihin (yhteistoimintalaki 334/2007, 57 §). Edellytyksenä on se, että työnantaja on määritellyt erikseen, mikä on salassa pidettävää ja mitä tulee kohdella liikesalaisuutena (yhteistoimintalaki 334/2007, 57 §; HE 159/2021 vp, 113-114). Myös liikesalaisuuslaki edellyttää, että liikesalaisuuksia voivat olla

vain tiedot, jotka eivät ole yleisesti saatavilla tai jonka suojaamiseksi sen haltija on ryhtynyt toimenpiteisiin (liikesalaisuuslaki 595/2018, 2 §). Liikesalaisuuslaki on Euroopan unionin liikesalaisuuksien suojaamista koskevan direktiivin kansallinen täytäntöönpano ja edellä mainittu määritelmä on yhtenevä EU-oikeuden kanssa (HE 49/2018 vp, 1; liikesalaisuusdirektiivi 943/2016, artikla 2). Tästä voidaan johtaa, että työnantaja ei voi vedota liikesalaisuuteen tai salassa pidettävään tietoon, ellei taustalla ole sekä ohjeistusta, että todellisia toimia kyseisen tiedon suojaamiseksi.

Työelämän tietosuojalain (759/2004) 21 § toteaa, että kameravalvonnan, kulunvalvonnan ja muun teknisin menetelmin suoritetun valvonnan osalta tulee henkilöstöä kuulla myös muissa kuin yhteistoimintalain piiriin kuuluvissa yrityksissä ja julkisoikeudellisissa yhteisöissä. Tässä yhteydessä on käsiteltävä teknisen valvonnan käyttötarkoitus, menetelmät ja tiedotettava työntekijöitä edellisistä sekä niiden käyttöönoton aloituksesta ja muutoksista (työelämän tietosuojalaki 759/2004, 21 §; HE 75/200, 30). Siten myös pienemmät yritykset, jotka valvovat toimintaa kameravalvonnan tai muun teknisen valvonnan kautta, ovat velvollisia käsittelemään nämä asiat henkilöstön kanssa. Teknisellä valvonnalla tarkoitetaan muutakin kuin kameravalvontaa. Hallituksen esitys (75/2000 vp, 30) mainitsee muun muassa tietojen käsittelyyn liittyvän tiedostojen käsittelyn ja puhelinjärjestelmät ja niiden laskutuserittelyt.

Kameravalvontaa, niin kuin teknistä valvontaa yleensäkin, voidaan käyttää työturvallisuuden varmistamiseen, omaisuuden suojaamiseen tai suoraan työntekijän oikeuksien varmistamiseen hänen pyynnöstään (työelämän tietosuojalaki 759/2004, 16 §). Kameravalvonta on kuitenkin aina viimesijainen keino ja sen edellytys on välttämättömyys suhteessa muihin vähemmän yksityisyyttä loukkaaviin keinoihin (Frände & Wahlberg 2018b, 421). Kameravalvontaan liittyvät ennakkohuolehtimisvelvoitteet ovat yleisesti teknistä valvontaa laajemmat työelämän tietosuojalain (795/2004) 17 §:n mukaan ja liittyvät pääsääntöisesti siihen, että etukäteen on selvitetty:

- Miten on varmistuttu siitä, että kameravalvonta ei ole syrjivää tai sitä ei tehdä muuta kuin 16 §:ssä kuvattuihin tarkoituksiin?
- Mitä ovat ennen kameravalvonnan käyttöönottoa käytetyt työntekijöiden yksityisyyteen vähemmän puuttuvat keinot?
- Miten varmistetaan, että työntekijän yksityisyyteen ei puututa enempää kuin on välttämätöntä valvonnan tarkoitusten saavuttamiseksi?
- Miten varmistetaan, että tallenteita käytetään vain niihin tarkoituksiin, joita varten tarkkailua on suoritettu?
- Miten työntekijöille tiedotetaan kameravalvonnan alkamisesta, toteuttamisesta ja siitä, miten ja missä tilanteissa mahdollisia tallenteita käytetään sekä tieto kameroiden sijainnista?

Valvonnassa tulee huomioida, että salakuunteluun on helpompi syyllistyä kuin salakatseluun. Salakuunteluun voi syyllistyä julkisellakin paikalla, jos ääntä tallennetaan puhujan tietämättä, kun taas julkisella alueella kameravalvonta ei ole ongelma, kunhan siitä on tiedotettu. Rajoituksena on kuitenkin se, että kameravalvontaa ei voi ilman riittäviä perusteita kohdentaa tietyn tai tiettyjen henkilöiden pitkäaikaiseen tarkkailuun. (HE75/2000, 28-29). Salakuuntelulta pitää voida suojautua esimerkiksi tietoisesti hakeutumalla syrjään keskustelujensa yksityisyyden suojaamiseksi. Keskustelujen tallentajan tai laitteiden ei tarvitse olla samalla alueella, että salakuunteluun voi syyllistyä. Olennaista on se, että keskustelua ei ole tarkoitettu tallentajan tietoon, minkä vuoksi kotirauhankin piiriin kuuluvalla alueella keskusteluun osallistuja voi tallentaa keskustelun asianosaisten tietämättä. (Frände & Walhberg 2018c, 400-403).

Kotirauhan piiriin kuuluvalla alueella työnantajalla, tai kenelläkään muullakaan ilman alueen haltijan suostumusta, ei ole minkäänlaista toimivaltaa. Kotirauhan piiriin kuuluvat henkilökohtaiset alueet, kuten oma asunto, loma-asunto ja niiden pihat, rannat ja laiturit, kerrostalojen porraskäytävät ja yhteiset alueet, mutta ei kerrostalon piha-alue. Samoin hotellihuoneet, mutta myös asuntovaunut ja teltat, kun ne ovat luvallisella paikalla. Tällaiselle alueelle ei saa tunkeutua ilman haltijan lupaa, mutta ei myöskään mennä salaa tai piiloutua. (Frände & Wahlberg 2018c, 409; Frände & Wahlberg 2018d, 370-374). Sama koskee myös tiettyjä julkisrauhan suojaamia alueita. Julkisrauhalla on tarkoitus taata tiloissa työskentelevien rauhaa ja yksityisyyttä. Tällaisia ovat virastot ja toimistot ja niiden yhteydessä olevat kokoustilat, joissa tyypillisesti työskentelee ihmisiä, mutta julkisrauhaa voi rikkoa myös menemällä tilaan, vaikka siellä ei oleskelisi ketään. Tiloihin voivat lukeutua myös harrastustoimintaan käytettävät rakennukset, mutta edellä mainittujen ulkoalueet kuuluvat vain harvoin julkisrauhan piiriin. Julkisrauhan piiriin lukeutuvaksi tilaksi ulkoalueilta edellytetään usein sitä, että ne ovat aidattuja ja muuten selkeästi merkittyjä. (Frände & Wahlberg 2018a, 386-392).

Salakatselun suoja ei ulotu kaduille tai esimerkiksi virastojen ja kauppojen tiloihin, joihin on julkinen pääsy. Kuitenkin maisemakuvauksessakin on huolehdittava siitä, että tallenteesta tunnistettavilta henkilöiltä on lupa julkaisemiseen. Salakatselussakin olennaista on tallentaminen, jolloin pelkkä omin aistein tapahtuva havainnointi ja siitä muistiinpanojen tekeminen ei ole kiellettyä. (Frände & Wahlberg 2018c, 408-410). Teon oikeudettomuus voidaan salakuuntelun ja -katselun osalta usein poistaa asianosaisten suostumuksella (Frände & Walhberg 2018c, 406, 410). Salakatselu ei kuitenkaan aina loukkaa yksityisyyttä. Esimerkiksi sellaisessa tapauksessa, jossa henkilö tulee kuvatuksi oleskellessaan oikeudettomasti jollain alueella tai kuvaaminen alueella, jossa oleskelijat voivat olettaa tulevansa kuvatuksi (Frände & Wahlberg 2018c, 412). Pelkkä rikosten selvittäminen ei anna oikeutta työnantajalle poiketa kameravalvontaan liittyvistä huolehtimisvelvoitteista (Frände & Walhberg 2018b, 423-424). Jos tekninen katselu tai kuuntelu on salaista, puhutaan pakkokeinolain (806/211) salaisista

pakkokeinoista, joita voi käyttää vain laissa säädetty viranomainen tai kun siitä on lainsäädännössä erityisesti säädetty (luku 10, 1 §; Halford v. the United Kingdom, 8).

Toisaalta Euroopan ihmisoikeustuomioistuimelta on tullut päätös, jossa työnantajan suorittama yksittäiseen kassatyöntekijään kohdistama salainen kameravalvonta katsottiin oikeutetuksi. Tässä päätöksessä korostui se, että työnantajalla oli merkittävä syy epäillä petosta, työantajalla ei ollut juuri muita mahdollisuuksia petoksen paljastamiseen, tallenteet oli hyvin suojattu muulta käsittelyltä eikä kuvaan päätynyt muita ihmisiä ja käsittely oli muutenkin hyvin rajoitettu vain tarpeelliseen. Sen lisäksi salaista valvontaa puolsi myös se, että sen avulla voitiin vapauttaa muut epäillyt työntekijät syyllisyydestä (ECHR 1725, 3-11). Tosin oikeus totesi, että vaikka oikeuksien tasapaino toteutui tässä tapauksessa, näin ei välttämättä olisi tulevaisuudessa esimerkiksi tekniikan kehittyessä ja mahdollistaessa enemmän yksityisyyden suojan piiriin tunkeutuva valvonta (ECHR 1725, 11).

Tekninen katselu ja kuuntelu on mainittu myös pakkokeinolaissa viranomaisten tiedonhankinnan menetelminä. Teknisen tarkkailun lisäksi siellä on mainittu myös suunnitelmallinen tarkkailu, peitelty tiedonhankinta, peitetoiminta, valeostot ja tietolähdetoiminta. (Pakkokeinolaki 806/2011, luku 10, 1 §). Tässä luvussa todetun mukaan myös työnantajalla on oikeuksia hankkia tietoja hallinnoimistaan tietoverkoista ja tietyissä tilanteissa normaalin työnvalvonnan ja jopa salaisen tarkkailun kautta. Se mistä erityisesti ei säädetä, on peitetoiminnan käyttäminen. Tietolähteiden käytöstäkään ei ole mainintaa, mutta tuskin työnantajalta olisi kiellettyä käyttää työntekijöitään tietolähteenä työnjohdollisissa tai sen laadun valvontaan liittyvissä tapauksissa. Peitetoiminta on luvussa neljä todetun mukaan joskus käytetty menetelmä myös yksityisetsivätoiminnassa. Koska siitä ei ole erikseen säädetty tarkemmin, on olennainen huolehtimisvelvoite varmasti siinä, että peitetoiminta ei voi ulottua kuin passiiviseen lyhytkestoiseen tarkkailuun, ilman riskiä esimerkiksi rikokseen yllyttämisestä.

Työnantajalle kuuluvia, mutta työntekijälle osoitettuja sähköposteja saa käsitellä vain tiettyjen huolehtimisvelvoitteiden hoitamisen jälkeen. Näitä huolehtimisvelvoitteita on kolme ja ne ovat:

1. Automaattisen vastaustoiminnon tarjoaminen työntekijälle poissaolonsa ajaksi
2. Mahdollisuus työntekijälle ohjata viestinsä toiselle työnantajan hyväksymälle henkilölle tai työnantajan hyväksymään osoitteeseen
3. Työntekijän suostumuksella työantajan hyväksymä toinen henkilö voisi vastaanottaa viestit työnantajan puolesta työantajalle tarkoitettujen viestien käsittelemiseksi (Työelämän tietosuojalaki 759/2004, 18 §)

Pelkkä huolehtimisvelvoitteiden hoitaminen ei anna kuitenkaan oikeutta avata viestejä suoraan. Työnantajalle sallittu viestien jatkokäsittely on jaettu työelämän tietosuojalaissa

(759/2004) kahteen erilliseen vaiheeseen lain pykälissä 19 ja 20: esille hakemiseen ja avaamiseen. Oikeudet koskisivat vain sellaisia viestejä, jotka koskevat poissaolon aikaa (HE 162/2003 vp, 57). Esille hakemisella tarkoitetaan tilannetta, jossa työnantaja järjestelmän pääkäyttäjän avulla selvittää, onko työntekijä saanut työnantajalle kuuluvia viestejä (työelämän tietosuojalaki 759/2004, 19 §). Jos työntekijä ei noudata edellä mainittuja menettelytapoja, olisi työnantajalla silti oikeus hakea viestejä esille ja avatakin (HE 162/2003 vp, 55). Viestien esille hakemisen edellytyksenä työelämän tietosuojalain (759/2004, 19 §) mukaan on, että viesti on työantajalle välttämätön ja:

1. Työntekijä työskentelee itsenäisesti, eikä tietoja voida saada muualta
2. On ilmeistä, että viestejä on vastaanotettu
3. Työntekijä on tilapäisesti tai pysyvästi estynyt hoitamasta työtehtäviään
4. Työntekijän suostumusta ei voida saada asian selvittämisen näkökulmasta riittävän ajoissa

Vaikka työnantajalle kuuluvia viestejä ei löydettäisi, eikä tilanne johda viestien avaamiseen, on siitä silti kirjattava selvitys. Tästä selvityksestä on ilmettävä viestien hakemisen syy, ajankohta ja suorittajat. Se on toimitettava työntekijälle viivytyksettä, ellei työntekijä ole pysyväisluonteisesti tavoittamattomissa. Tietoja käsitelleitä koskee salassapitovelvoite, joka jatkuu myös työsuhteen päättymisen jälkeen. (Työelämän tietosuojalaki 759/2004, 19 §).

Jos esille hakemisen yhteydessä selviää lähettäjä- tai vastaanottajatietojen tai viestien otsikkotietojen perusteella, että työantajalle kuuluvia viestejä on vastaanotettu ja on perusteltavissa, että viesti on ehdottoman tärkeä, voidaan se avata. Avaamisen yhteydessä on kuitenkin oltava järjestelmän pääkäyttäjän lisäksi paikalla myös toinen henkilö, joka voisi edustaa työnantajaa. Pääkäyttäjä ei siten voisi suorittaa avaamista yksin. Avaamisesta on myös laadittava selvitys, josta selviää samat asiat kuin esille hakemiseen liittyvästä selvityksestä, mutta sen lisäksi avattu viesti tulee yksilöidä ja selvitykseen on kirjattava, kenelle sisällöstä on annettu tieto. Avaamisen välttämättömyys on myös uudelleenarvioitava, eikä tietoja saa käsitellä laajemmin kuin avaamisen perusteen vuoksi on välttämätöntä. (Työelämän tietosuojalaki 759/2004, 20 §; HE 162/2003 vp, 60).

Sähköpostien ja tietoverkon käytön periaatteet on käytävä läpi yhteistoimintamenettelyssä ja työelämän tietosuojalaki määrittelee tarkemmin, miten sähköposteja saa käsitellä (yhteistoimintalaki 334/2007, 19 §, kohta 4; Työelämän tietosuojalaki 759/2004, luku 6). Euroopan ihmisoikeustuomioistuimen mukaan kirjesalaisuuteen rinnastettavaa luottamuksellisuutta sovelletaan myös puhelinkeskusteluihin ja muihin sähköisiin viestintämuotoihin (HE 75/2000 vp, 27). Työntekijöiden sähköpostien käsittelystä säädetään erityislakina työelämän tietosuojalaissa. (HE 169/2003 vp, 36). Edellä mainitun viestien

käsittelyn osalta on huomioitava, että vaikka työntekijä olisi siirtynyt toiselle työnantajalle, on hänellä edelleen perustuslailliset oikeudet yksityisyyteen.

Hankalaksi tilanne saattaa muodostua kuitenkin silloin, jos viestien käsittelyn syy liittyy esimerkiksi työnantajan liikesalaisuuksiin, eikä entisellä työntekijällä ole enää salassapitovelvoitetta. Tämä voisi työskennellä myös kilpailijalla, jolloin työantajan toimintojen turvaamiseksi tehty toimenpide voisi jopa vaarantaa työnantajan etuja verrattuna kilpailijoihin samassa markkinassa. Joka tapauksessa työsuhteen päättämistilanteissakin työnantajan olisi tarjottava entiselle työntekijälle aiemmin mainittujen huolehtimisvelvoitteiden mahdollisuuksia, esimerkiksi viestin ohjaamista toiselle työnantajan hyväksymälle työntekijälle (HE 16/2003 vp, 59). Työantaja voisi hankkia suostumuksen myös työsuhteen päättyessä johonkin tiettyyn laista poikkeavaan menettelyyn, jolloin työelämän tietosuojalain velvoitteita menettelytavoista ei tarvitse noudattaa pois lukien selvitysten laatiminen ja toimittaminen asianosaisille (HE 162/2003 vp, 60; työelämän tietosuojalaki 20 §, 3 mom.).

Sähköpostin käsittelyn on perustuttava ensisijaisesti suostumukseen ja sähköposteista voidaan käsitellä vain toiminnan jatkumisen kannalta välttämättömiä viestejä (HE 162/2003 vp, 54). Suostumuksella ei ole muotovaatimusta, mutta lain perusteluissa suositaan kirjallista muotoa (HE 162/2003 vp, 56). Suostumuksen saamisesta voisi luopua vain erityistapauksissa, jolloin sen ei voi ajatella olla yleinen aina sovellettava oikeus (HE 162/2003 vp, 58). On huomioitava myös lain sanamuoto – toiminnan jatkumisen turvaaminen ei ole sama kuin esimerkiksi rikoksen selvittäminen. Eikä rikoksen selvittäminen ole välttämättä tarpeen jatkuvuuden turvaamiseksi. Toisaalta jatkuvuuden turvaamisen yhteydessä voi paljastua myös rikos, jos sähköpostien käsittelyn yhteydessä selviäisi jotain, missä olisi esimerkiksi tahallinen työnantajan vahingoittamisyritys tai työnantajan resurssien väärinkäytös oman hyödyn vuoksi. Lakiesitys puhuu muualla yleisesti työnantajan ”toimintojen turvaamisesta” (esimerkiksi HE 162/2003 vp, sivut 33, 57, 58, 59, 70, 76, 77). Toimintojen turvaamiseen voisi edellisten perusteella kuulua myös havaitun tai epäillyn rikoksen vahinkojen rajoittaminen tai korvausvelvollisuuden ratkaisu.

Sääntelyllä on kuitenkin muitakin tavoitteita kuin työntekijän yksityisyyden suojan varmistaminen. Esimerkiksi työnantajalle kuuluvien ja työntekijöiden yksityisyyteen liittyvien viestien erottaminen ja työnantajan turva, silloin, kun suostumus ei ole käyttökelpoinen käsittelyn peruste (HE 162/2003, 54). Laissa on asetettu edellytykseksi työntekijän poissaolo ja suostumuksen saaminen kohtuullisessa ajassa, mutta laki jättää hiukan auki sellaisen tilanteen, jossa työntekijä on ehkä tavoitettavissa, mutta ei anna suostumustaan. Suostumuksen epäämisen taustalla voi olla myös vahingoittamistarkoitus, eikä vain yksityisyyden turvaaminen. Tämän ja edellisen kappaleen perusteella voisi arvioida, että työantajalla olisi ehkä mahdollisuus hakea viestit esille silti toimintojen turvaamisen ja

häiriöttömän toiminnan jatkamiseksi. Joka tapauksessa silloin puututtaisiin hyvin suojattuun perusoikeuteen kirjesalaisuudesta, jolloin erityishuomio olisi oltava yksityisten ja työnantajalle kuuluvien viestien erottamisessa, työantajan intressin suuruuden ja työntekijän oikeuksien vertailussa sekä viestien esille haun ja avaamisen prosessin suorittamisessa tarkalleen laissa säädetyssä tavalla. Myös työelämän tietosuojalain perustelutekstit korostavat ehdotonta tarpeellisuutta ja viestin käsittelyn välttämättömyyttä, jolloin ne tulisi huolellisesti kirjata ylös myöhempää arviointia varten (HE 162/2003 vp, 57).

Viestintäpalvelulain muutokset vuonna 2009 muuttivat myös muita lakeja. Esimerkiksi yhteistoimintalaki sekä laki yhteistoiminnasta valtion virastoissa ja laitoksissa muuttui tuoden mukaan tunnistamistietojen käsittelyyn liittyvän informointivelvoitteet yhteistoiminamenettelyn kautta (HE 48/2008 vp, 12). Työelämän tietosuojalaki sisälsi jo muun muassa sähköpostien esille hausta ja avaamisesta ja teknisin menetelmin suoritettavasta valvonnasta säännöksiä, mutta toi uutena esimerkiksi ilmoitusvelvollisuuden sähköisen viestiliikenteen tunnistamistietojen käsittelystä (HE 48/2008 vp, 4, 22, 28). Työelämän tietosuojalakiin päivittyi myös viittaukset sähköisen viestinnän tietosuojalakiin, esimerkiksi yrityssalaisuuksien suojaamiseksi (HE 48/2008vp, 67). Edellisten vuoksi rikoksen paljastamisen näkökulmasta myös yhteistoimintalaki (334/2007) ja työelämän tietosuojalaki (759/2004) ovat tärkeitä lakeja huomioida juuri informointivelvoitteen näkökulmasta. Tietosuojalain (1050/2018) 30 § viittaa henkilötietojen käsittelystä työntekijöille informoinnin osalta työelämän tietosuojalakiin (759/2004), jonka toisen luvun neljäs pykälä taas viittaa henkilötietojen keruun osalta yleisen tietosuoja-asetuksen kolmanteen lukuun. Käytännössä tietosuoja-asetus siis määrittelee hyvin pitkälle sen, mitä henkilötietojen käsittelystä edellä mainituissa tapauksissa on kerrottava asianosaisille.

Lopuksi käsitellään vielä muutamaa erityiskysymystä liittyen alussa esitettyyn tietosuoja-asetuksen ja kansallisen lainsäädännön mahdolliseen ristiriitaan. Ensimmäinen tulkintaepäselvyys liittyy siihen, että työelämän tietosuojalaki antaa työnantajalle oikeuden käsitellä ”välittömästi tarpeellisia” tietoja, kun taas tietosuoja-asetus puhuu vain ”tarpeellisista” tiedoista (työelämän tietosuojalaki 759/2004, 3 §; tietosuoja-asetus 679/2016, 5 artikla, 1 c). Kuten luvussa 5.2 todettiin, on tietosuoja-asetus kuitenkin ensisijaista lainsäädäntöä. Käytännössä voisi myös olla vaikea todistaa sitä, onko jonkin tiedon käyttäminen tarpeellista, vai välittömästi tarpeellista. Joka tapauksessa asian ratkaisu edellyttäisi aina tapauskohtaista tulkintaa riippuen työsuhteen laadusta (Nyyssölä 2020, 75). Toki sana välittömästi voidaan liittää myös ajalliseen ulottuvuuteen, jolloin käsittelyn tulisi olla juuri siinä hetkessä tarpeellista, mutta tätä ei lainsäädännössä avata tarkemmin.

Toinen aiempaan liittyvä tulkintaepäselvyys koskee myös työelämän tietosuojalakia (759/2004) ja sitä, mitä tietoja työnantaja voi hankkia työnhakijasta. Nykylainsäädännössä työnantaja ei voisi hankkia mitään tietoja työntekijästä muualta kuin häneltä itseltään ilman

hänen suostumustaan (työelämän tietosuojalaki 759/2004, 4 §, 1 mom.). Aiemmin työnantajan luotettavuuden selvittämiseen liittyvää oikeutta on tulkittu laajasti. Esimerkiksi hallituksen esitys työelämän tietosuojalain osalta mainitsi, että työnhakijan tietoja voitaisiin hankkia muualta kuin henkilöltä itseltään ilman suostumusta luotettavuuden selvittämiseksi silloin, kun tiedot olisivat välittömästi työsuhteen kannalta tarpeellisia ja luotettavuuden selvittämiseen olisi perusteltu tarve (HE 75/2000, 17). Nämä tiedot voisivat olla edellisten työnantajien tai heidän edustajiensa muistikuvia tai vaikka tietoverkoista hankittuja tietoja (HE 75/2000, 17-18). Laki kuitenkin muuttui vuonna 2004 ja sen sanamuodosta tuli tiukempi siten, että tietoja ei voisi hankkia enää ulkopuolisilta ilman työnhakijan suostumusta, mutta itse käytäntö esimerkiksi tietosuojavaltuutetun ratkaisuissa ei muuttunut aiemmasta ja lakia ehdotettiinkin muutettavan sallivampaan suuntaan (Nyyssölä 2020, 67; TyVM 12/2018).

Muutos nähtiin tällä hetkellä vielä valmisteilla olevassa työ- ja elinkeinoministeriön lainsäädäntöhankkeessa (TEM097:00/2020), jossa hallituksen esitysluonnoksessa todetaan, että tarpeellisuusvaatimuksen täyttyessä tietoja voitaisiin kerätä muualta kuin työnhakijalta ilman suostumusta työantajan työnjohto- ja valvontaoikeuden perusteella, eikä tietolähteitä voitaisi välttämättä määritellä tyhjentävästi (HE luonnos 2021b, 22). Joka tapauksessa pykälässä säilyy työnantajan velvollisuus kuulla työntekijää ennen kuin kyseisiä tietoja käytetään häntä koskevassa päätöksenteossa. Seurauksena esimerkiksi tilanteessa, jossa tietoja ei ole mahdollista oikaista, voitaisiin soveltaa tietosuoja-asetuksen hallinnollista sakkoa, jonka maksimimäärä on 20 miljoonaa euroa tai 4 % edeltävän tilikauden maailmanlaajuisesta liikevaihdosta, kumpi näistä on suurempi (HE luonnos 2021b, 23).

Luottotietoja hankittaessa on nimettävä rekisteri, josta tiedot on hankittu (HE luonnos 2021b, 22-23; työelämän tietosuojalaki 759/2004, 4 §, 2 mom.). Tulkintakäytännön ollessa muuttumaton vuoden 2000 lainvalmistelusta tähän päivään, ei työnantajan ehkä voi olettaa syyllistyvän rikokseen, kunhan tietojen tarpeellisuudesta ja tietolähteiden oikeellisuudesta on huolehdittu ja työhakijaa on informoitu käsittelystä tai kuullaan viimeistään ennen häntä koskevassa päätöksenteossa (TyVM 12/2018 vp, luku Valiokunnan päätösehdotus; HE luonnos 2021b, 22). Huomattavaa on kuitenkin se, että rekrytointitilanteessa vaadittaisiin edelleen työnhakijaa koskien häneltä saatu suostumus tietojen keräämiseen muualta (HE luonnos 2021b, 21).

Myös jo työtehtäväänsä valitun työntekijän osalta tietojen käsittelyyn on tulossa muutos. Aiemmin Tietosuoja-asetus -luvussa jo käsiteltiin tietosuoja-asetuksen (679/2016) kohdalla suostumuksen vapaaehtoisuutta. Kuten aiemmin todettiin, suostumusta ei voida pitää työelämässä työntekijän osalta vapaaehtoisesti annettuna, koska työntekijä on työnantajan direktio-oikeuden vuoksi heikompi osapuoli valta-asemaa ajatellen (myös HE luonnos 2021b, 8 ja 11). Tämän vuoksi lainsäädäntöä päivitetään siihen suuntaan, jossa ei jouduttaisi

kansallisen lain nojalla käyttämään lainmukaisuusperustetta, joka ei ensisijaisesti sovellettavan lainsäädännön näkökulmasta ole hyväksyttävää.

Siksi meneillään oleva lakimuutosehdotus työelämän tietosuojalain 4 §:n muuttamisesta antaisi työnantajalle oikeuden käsitellä työnjohto- ja valvontaoikeuden toteuttamista varten sekä lakisääteisten oikeuksiensa ja velvollisuuksiensa toteuttamiseksi työntekijän tietoja myös ilman suostumusta (HE luonnos 2021b, 20). Tällaisia tietoja olisivat esimerkiksi työtehtävien suorittamiseen, työntekijävalintaan, työolosuhteisiin sekä työ- ja virkaehtosopimusten sekä lainsäädännön edellyttämät tiedot. Työnantaja olisi silti velvollinen tekemään aina tarpeellisuusarvioinnin yksittäistapauksissa erikseen. Tarpeellisia tietoja voisivat olla sellaiset, jotka osoittavat esimerkiksi työntekijän pätevyyttä tai sopivuutta tehtäviinsä. (HE luonnos 2021b, 4). Suostumus jäisi kuitenkin muiden henkilötietojen käsittelyn perustana työntekijöiden oikeuksien turvaajana (HE luonnos 2021b, 22).

Työlainsäädännöstä puhuttaessa on hyvä muistuttaa myös matalammasta kynnyksestä tietosuojaa koskevan vaikutustenarvioinnin tekemiseen. Työntekijän heikompi asema soveltuu myös tietosuojaa koskeviin vaikutustenarviointeihin, jolloin tämä asema on otettava huomioon käsittelyn riskejä arvioitaessa. Heikommasta asemasta voi johtua se, että henkilöillä ei ole tehokkaita keinoja käyttää oikeuksiaan. (WP 29 2017b, 12). Aiemmin mainitusta informoinnista poikkeamisen lisäksi työntekijän, tai kenen tahansa heikommassa asemassa olevan henkilön, biometristen, geneettisten tai sijaintitietojen käsittelyä ennen on suoritettava tietosuojaa koskeva vaikutustenarviointi (Tietosuojavaltuutetun toimisto 2018). Tekniseen valvontaan, kilometrikorvausten tai päivärahojen oikeellisuusselvitykseen tai työajan noudattamiseen liittyvään tapaukseen voisi helposti ajatella kytkeytyvän sijaintitiedon käsittely olennaisena osana yksityisetsivien toimeksiannoissa. Siten tällainen tutkinta edellyttäisi omaa vaikutustenarviointia. Mutta yhtä lailla työasemien valvonta ja internetin käytön valvonta edellyttää tietosuojaa koskevaa vaikutustenarviointia (WP 29 2017b, 13).

Työnhakijat voivat luovuttaa itsestään monia tietoja työnhakuvaiheessa, eikä työnantaja pysty tätä välttämättä rajaamaan. Olisi siten periaatteessa mahdollista, että joku voisi kertoa omasta rikollisesta taustastaan työhaastattelussa. Vaikka työnhakijoiden ja työntekijöiden tietoja voitaisiin periaatteessa käsitellä suostumuksella, mutta johtuen puuttuvasta tarkkarajaisesta lainsäädännöstä, tällaista käsittelyä ei tulisi harkita ainakaan ilman huolellista tietosuojaa koskevaa vaikutustenarviointia, luvallisia toimijoita ja valvontaviranomaisen ennakkokuulemista. Johtuen siitä, että tarkkarajaisten suojakeinojen puuttuessa käsittely todennäköisesti aiheuttaisi korkean riskin rekisteröidylle.

Tällaisten tietojen saamista ei tulisi myöskään tulkita siten, että niiden käsittelylle olisi annettu automaattisesti suostumus, vaikka luovuttaminen sinällään olisi vapaaehtoinen ja

aktiivinen teko hakijalta. Tietojen luovutus voi johtua esimerkiksi siitä, että hakija kuvittelee olevansa lakisääteisesti velvollinen kertomaan niistä tai jostain muusta syystä, jolloin suostumus ei ole vapaaehtoinen. Suostumukselta edellytettiin lisäksi informointia käsittelyn tarkoituksista, selkeyttä ja suostumuksen tulisi olla peruutettavissa. Voisi olla kohtuutonta osoittaa, että suostumuksen peruuttamisen yhteydessä työnantaja ei enää käyttäisi tällaisia tietoja päätöksenteossa tultuaan niistä kerran tietoiseksi. Jos tällaisen tiedon saanti vaikuttaisi valintaprosessiin, olisi päätös tehtävä pikimmiten ja lopetettava välittömästi tietojen käsittely, koska rikoksiin liittyvien tietojen käsittely ei ole pelkällä suostumuksella sallittu.

Kun työtehtävä edellyttää nuhteettomuutta, voidaan työnhakijalta kysyä, onko hänen tiedossaan sellaista rikoshistoriaa omalta kohdaltaan, minkä vuoksi hänen taustaansa ei voisi pitää nuhteettomana. Silloin ei tarvitsisi käsitellä rikoksiin liittyviä tietoja, mutta asia voitaisiin huomioida valintaa tehdessä. Jos myöhemmin muista syistä selviäisi, että työnhakija on antanut väärää tietoa työnhakutilanteessa, kohdistuisi tutkinta työntekijään ja tämän epärehelliseen lausumaan, ja sillä voisi olla työoikeudellisia seurauksia esimerkiksi työnsuhteen jatkoa arvioitaessa. Silloin käsittely perustuisi tietosuojalain (1050/2018) seitsemänteen pykälään. Taustojen tai lausumien todenperäisyyttä sellaisen työnhakijan osalta, joka ei ole tullut valituksi, ei olisi tarve tutkia. Eikä sille siten voisi olla lainmukaisuusperusteitakaan.

5.8 Sopimusoikeus

Oli kyse alihankinnasta tai suorasta toimeksiannosta, on kaiken toiminnan lähtökohta osapuolten välinen sopimus siitä, millaista palvelua asiakas saa ja millaisen vastikkeen palvelusta hänen täytyy suorittaa. Suomessa vallitsee sopimusvapaus, mikä tarkoittaa siitä, että kenellä tahansa on vapaus päättää, tekeekö sopimuksia ja kenen kanssa (Hemmo & Hoppu 2006, luku 4). Sopimusoikeuden osalta on muutama huomioitava asia, joilla voi olla vaikutusta joko asiakkaan hankkimaan yksityisetsiväpalveluun tai yksityisetsivän alihankintana toiselta yhtiöltä ostettuun työhön. Oikeustoimilain (228/1929) perusteella sopimuksen osapuoleksi voi tulla joko tekemällä suoraan itse tarjouksen tekijänä tai antajana tai valtuuttamalla jonkun toisen tekemään sopimus puolestaan (1 ja 10 §). Sopimus ei tarvitse olla kirjallinen, vaan sen voi tehdä myös suullisesti (Oikeustoimilaki 228/1929, 3 §). Tämä ei koske kuitenkaan kaikkea yksityisetsivätoimintaa, sillä kirjallinen sopimus vaaditaan silloin, kun on kyse rikoksen paljastamisesta tai selvittämisestä, mitkä kuuluvat vartioimisliiketoiminnan piiriin. Sopimus on tehtävä myös ennen tehtäviin ryhtymistä tai viimeistään toisena arkipäivänä tästä, jos tehtävän aloittaminen on kiireellistä. Sopimus tulee olla valvontaviranomaisen saatavilla selväkielisenä, vaikka se tehtäisiin sähköisesti. (Laki yksityisistä turvallisuuspalveluista 1085/2015, 73 §).

Toinen tilanne, jossa ainakin osa sopimuksesta on oltava kirjallisena, on aiemmin käsitelty henkilötietojen käsittely sopimussuhteessa. Tilanne, jossa osapuolet sopisivat kirjallisesti vain henkilötietojen käsittelystä, mutta eivät itse sopimuksen sisällöstä, voisi olla jälkeenpäin hankala tulkita. Esimerkiksi henkilötietojen käsittelyn tarkoitukset ja käsiteltävät henkilötietoryhmät riippuvat siitä, mistä osapuolten kesken on sovittu, jolloin hyvin suuri osa varsinaisen sopimuksen sisältöä on oltava kirjallisena. Lisäksi tulee huomioida se, että artiklassa 28 puhutaan henkilötietojen käsittelyyn liittyvästä sopimusvelvoitteesta tilanteissa, joissa tietoja käsitellään toisen lukuun (tietosuoja-asetus 679/2016, artikla 28, kohta 1). Siellä ei sanota, että kun henkilötietoja käsitellään kirjallisen sopimuksen perusteella. Vaikka alkuperäinen sopimus ei olisi kirjallisena, sovellettaisiin artiklaa 28 silti. Hemmon ja Hopun (2006) mukaan sopimuksiin sovelletaan normeja aina seuraavassa järjestyksessä (luku 3):

- Pakottava lainsäädäntö
- Sopimusehdot
- Osapuolten vakiintunut käytäntö
- Alalla vallitseva kauppatapa
- Tahdonvaltainen lainsäädäntö

Pakottavaa lainsäädäntöä on lähinnä maksutavoista ja esimerkiksi kuluttajansuojasta sopimussuhteissa, mutta ei esimerkiksi itse toimeksiantojen suorittamisen tavoista tai vastuista niihin liittyen (Hemmo & Hoppu 2006, luku 3). Seuraavaksi sovelletaan itse sopimusta, jonka ehdot ohittavat kaiken muun paitsi pakottavan lainsäädännön (Hemmo & Hoppu 2006, luku 3). Jos osapuolten välillä ei ole vakiintunutta käytäntöä tai osapuolet ovat täysin eri aloilla toimivia yrityksiä, kahta seuraavaa on hankala soveltaa. Lopuksi sovelletaan tahdonvaltaista lainsäädäntöä, joka esimerkiksi yksityisellä turvallisuusalalla ei edellä kuvattua enemmän sääntele sopimuksista. Käytännössä jäljelle jää oikeustapausten tulkitseminen tai analoginen muun lainsäädännön soveltaminen riita- tai erimielisyystilanteissa (Hemmo & Hoppu 2006, luku 3). Jos sopimus jäisi pelkästään ulkopuolisen tuomioistuimen tai muun sovitteluelimen tulkittavaksi eri laeista johdettavilla analogioilla, voidaan ajatella, että osapuolet eivät välttämättä itse enää kontrolloi sopimukseen liittyvää tahdonilmaisuaan. Sopimus tulisi siitä syystä olla kokonaisuudessaan aina kirjallinen.

Toinen perustelu kirjalliselle sopimukselle on aiemmin kuvatut eri lainsäädännöstä johtuvat vastuut osapuolten kesken ja oikeustoimilain toinen luku. Asiakkaan palkatessa yksityisetsivää esimerkiksi luotettavuusselvityksen tekemiseen, on kyse asiakkaan lukuun suoritettavasta toiminnasta, johon asiakas valtuuttaa etsivän edustamaan itseään ja suorittamaan oikeustoimia puolestaan (oikeustoimilaki 228/1929, luku 2, 10 §). Tehtävässä voidaan käyttää kameravalvontaa, asentaa uusia kameroita, hakea esiin sähköistä viestiliikennettä tai jopa seurata asianosaisia. Jos valtuutettu etsivä toimisi lainvastaisesti, vastaisi hän todennäköisesti

vahingoista, mutta jos vilpillisestä menettelystä on ollut hyötyä asiakkaalle, voi vastuu etsivän suorittamista lainvastaisuuksista kaatua myös asiakkaalle (Kauppakaari 3/1734, luku 18, 2 §). Jos asiakas valtuuttajana on ohjeistanut toiminnan ja etsivä rikkoisi ohjeistusta, ei se sitoisi asiakasta (oikeustoimilaki 228/1929, 11 §). Toisaalta jos edes sopimusta ei ole kirjallisena, on varmasti vaikea näyttää toteen ohjeistuksen sitovuutta, koska sopimus on usein ainoa tapa osoittaa esimerkiksi toimivalta (Hemmo & Hoppu 2006, luku 5).

Sopimuksen yksi olennainen osa on sopimuskumppanien valinta. Yhtä lailla niin asiakkaan kuin yksityisetsivänkin näkökulmasta ensimmäinen vaihe on varmistaa, että kyseinen sopimuskumppani on ensinnäkin olemassa ja että palkattavalla etsivällä on esimerkiksi riittävä toimivaltuus rikosten paljastamiseen. Myös sopimuskumppanien taloudellinen vastuunkantokyky ja sen tutkiminen voi olla tärkeää (Hemmo & Hoppu 2006, luku 4). Erityisesti tämän merkitys kasvaa, jos sopimussuhteessa käsitellään henkilötietoja. Tämä johtuu aiemmin Tietosuoja-asetus-luvussa käsitellystä vahinkovastuusta. Sen mukaan vahinkoa kärsineet rekisteröidyt voivat hakea täysimääräisesti korvauksia keneltä tahansa käsittelyketjuun osallistuneelta, joka on vähäisessäkään määrin vastuussa vahingoista. Kenen tahansa osapuolen virhe voi siis johtaa kaikkien vahinkovastuuseen suuremmasta vahingosta kuin mihin itse on syyllistynyt. Jos kirjallista sopimusta ei ole, tuskin yksikään osapuolista voi ainakaan aukottomasti todistaa vastuuvapauttaan käsittelystä. Jos ketjussa on toimijoita, joiden taloustilanne on heikko, tulee varautua siihen, että muut joutuvat kantamaan heidän taloudelliset vastuunsa.

Edelliseen kohtaan liittyy myös vaaranvastuu. Jos toimeksisaaja käyttää toimeksiantajan laitteistoa ja järjestelmiä, on vaaranvastuu usein niistä kuitenkin omistajalla (Hemmo & Hoppu 2006, luku 7). Myös vahingonkorvausvastuista, niiden suuruudesta ja sisällöistä kannattaa sopia – esimerkiksi yritysten välisissä sopimuksissa usein jätetään ulkopuolelle välilliset vahingot (Hemmo & Hoppu 2006, luku 4). Toisaalta kuluttajien kanssa tehtyjen sopimusten osalta kannattaa olla huolellisempi, koska sopimusehdot, jotka poikkeavat kuluttajansuojalaista tilaajan vahingoksi, ovat mitättömiä (kuluttajansuojalaki 38/1978, luku 8, 2 §). Vastuunrajoitukset eivät kuitenkaan oikeuta toimimaan miten tahansa, koska vakiintuneen periaatteen mukaisesti vastuunrajoitukset menettävät merkityksensä, jos sopimusrikkomus on tahallinen tai törkeän tuottamuksellinen (Hemmo & Hoppu 2006, luku 8).

Vahingonkorvausvastuissa etenkin toimeksisaajan tulee olla huolellinen, koska asiantuntijapalveluita tarjoavalta odotetaan usein korkeaa oman alansa osaamista. Siten asiantuntemuksen puutteellisuus ei ole lieventävä seikka. (Hemmo & Hoppu 2006, luku 16). Yksityisetsivää, joka mainostaa luotettavuusselvityksiä tai rikosten paljastamista, voidaan pitää alansa asiantuntijana, joka tuntee oman alansa käytänteet ja lainsäädännön ja vastuun voidaan siten ajatella olevan korkeampi toimeksiantoja suoritettaessa. Kuluttajien kanssa tulee huomioida myös mahdollisimman totuudenmukainen markkinointi ja toimeksiantojen

realistinen kuvaaminen, ettei syyllisty sopimattomaan menettelyyn tai kuluttajan harhaanjohtamiseen (kuluttajansuojalaki 38/1978, luku 2, pykälät 3 ja 6).

Asiantuntijapalveluissa on Hemmon ja Hopun (2006) mukaan hyvä sopia vähintään seuraavista asioista (luku 16):

- palvelun sisältö ja tavoite
- palvelun perustaksi annetut tiedot
- mahdolliset palvelun sisältöä koskevat rajoitukset ja toimeksiantajan itsensä hoidettavaksi jäävät tehtävät
- sovellettavat hinnoitteluperusteet ja mahdollinen kustannusarvio
- palvelun suorittamisaika
- palvelun suorittamisesta vastaavien henkilöiden yksilöinti
- toimeksisaajan vastuun sisältöä koskevat ehdot (vastuunrajoitukset ja määräykset vastuuvakuutuksesta).

Tämän työn havaintojen perusteella edellisen listaan tulisi sisältyä selvästi esimerkiksi lakisääteisten huolehtimisvelvoitteiden hoitaminen toimeksiantajan toimesta. Mitä paremmin ne on yksilöity sen parempi, koska asiantuntijapalveluiden osalta ei useinkaan odoteta asiakkaiden kykenevän arvioimaan toimenpiteiden sisältöjä (Hemmo & Hoppu 2006, luku 16). Esimerkiksi tilitoimiston, jonka tehtävänä oli laatia yhtiöosuuden luovutukseen liittyvät asiakirjat, olisi tullut osata ennakoida myös veroseuraamuksia, vaikka se ei kuulunut toimeksiantoon (KKO 2001:128, Hemmo & Hoppu 2006, luvun 16 mukaan). Toisessa esimerkissä tilitoimiston olisi tullut kyetä kyseenalaistamaan myös asiakkaalta saamiensa tietojen paikkansapitävyys asiantuntijana (KKO 1999:80, Hemmo & Hoppu, luvun 16 mukaan). Samankaltainen tulkinta käsiteltiin tässä työssä jo aiemmin henkilötietojen käsittelyn osalta Alankomaiden valvontaviranomaisen päätöksessä, jossa alihankkijana toimiva käsittelijä oli velvollinen varmistamaan myös asiakkaansa lainmukaisuusperusteet henkilötietojen käsittelylle (Autoriteit Persoongegevens 2015, päätös Z2015-00062).

Vastuiden lisäksi toimeksiannon sisällön ja tavoitteiden sopimisella voi olla vaikutusta siihenkin, mistä yksityisetsivä saa ylipäätään laskuttaa. Raportointi voi myös muodostua olennaiseksi osaksi tätä. Tämä käy ilmi esimerkiksi käräjäoikeuden päätöksestä, jossa toimeksiantaja oli riitauttanut toimeksiantoon kohdistuvan laskun sillä perusteella, että yksityisetsivä ei ollut toiminut sopimuksessa mainitulla tavalla eikä raportoinut riittävästi toimeksiantoon käytetystä ajasta. Toimeksiantaja oli olettanut yksityisetsivän toimittavan valokuvia, mutta koska valokuvaamista ei ollut kirjattu toimeksiantosopimukseen, ei toimeksiantoa voitu sillä perusteella riitauttaa. Yksityisetsivä oli myös huolehtinut raporttien lähettämisestä, eikä niiden perusteella ollut syytä epäillä myöskään toimeksiantoon käytettyä työaikaa. (Surakka 2021). Kääntäen voidaan ajatella, että jos sopimuksella olisi ollut

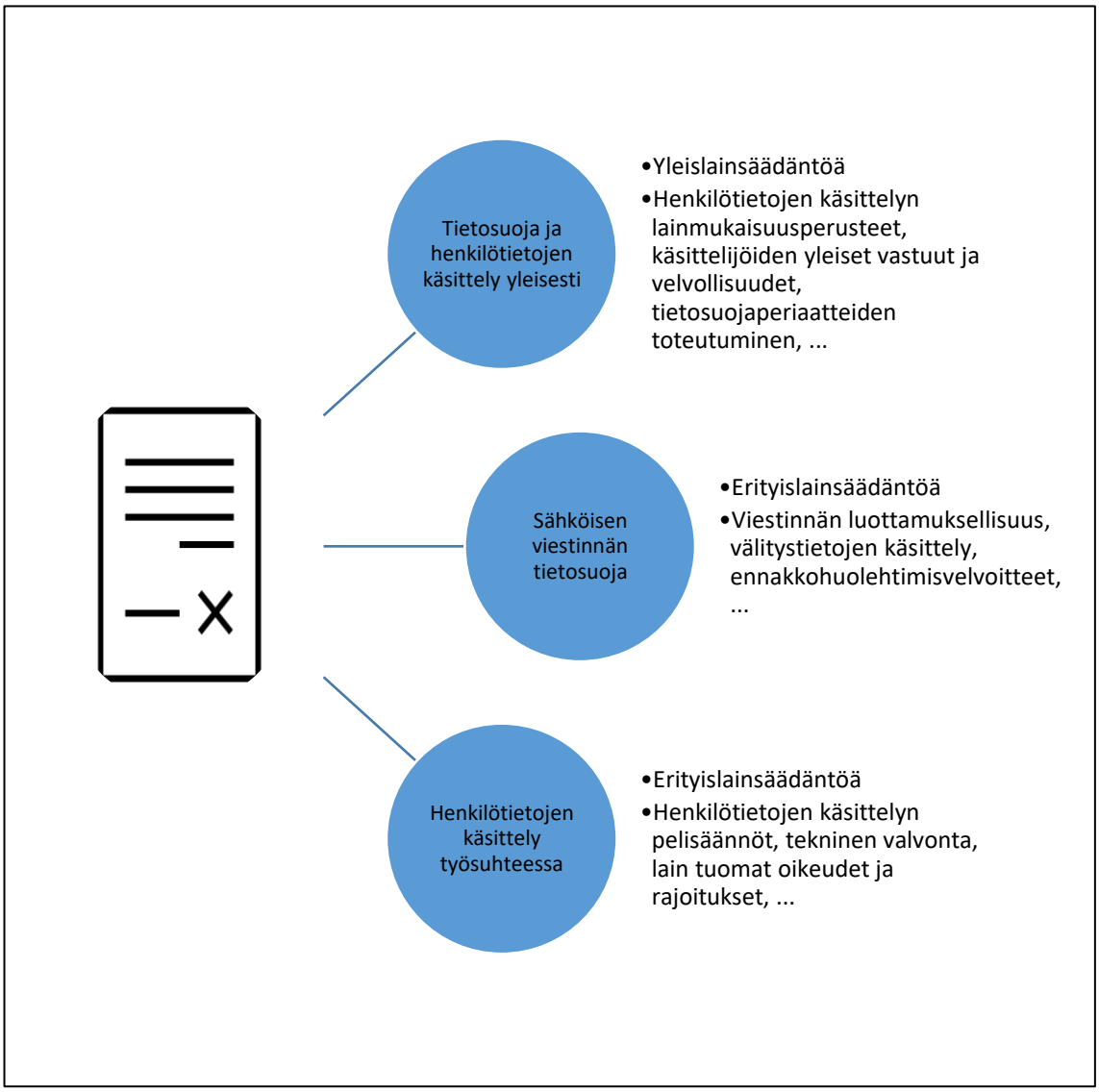
määriteltynä menetelmiä, tulisi huolehtia myös siitä, että kyseisiä menetelmiä käytetään. Jolloin palataan taas kysymykseen siitä, miten jakautuvat menetelmien käyttöön liittyvät vastuut ja kenen olisi pitänyt huolehtia niihin liittyvistä velvoitteista.

Edelliseen päätökseen liittyen kannattaa huomioida myös sopimuksella olevat hinnoitteluperusteet. Luvussa 5.4.6 käsiteltiin jo auditointien ja tarkastusten kustannuksia, joista Euroopan tietosuojaneuvosto oli maininnut näiden voivan muodostua kaupallisista lähtökohdista, mutta niiden ei saisi olla kohtuuttomia siten, että ne rajoittaisivat osapuolten mahdollisuuksia käyttää heille kuuluvia oikeuksiaan (EDPB 2021a, 41). Toimeksiantoihin voi liittyä muitakin tilanteita, joissa tietosuojalainsäädännön takia tarvitaan toisen osapuolen osallistumista. Tällainen tilanne voi tulla vastaan esimerkiksi edellä käsitellyssä menetelmien valinnassa. Kesken toimeksiannon voidaan joutua vaihtamaan menetelmiä, jotka muuttavat esimerkiksi henkilötietojen käsittelystä informointia toimeksiannon kohteille. Tällaisten tilanteiden varalle voi olla hyvä sopia etukäteen, kuka näistä tilanteista vastaa ja jos siihen tarvitaan toista osapuolta, miten sellaiset kustannukset jaetaan. Tietosuojaneuvoston kannanotto siihen, että kustannukset eivät saisi olla este tietosuojatakeiden toteutumiselle tarkoittaisi ehkä käytännössä sitä, että kustannusten tulisi perustua todellisiin kuluihin, eivätkä ne voisi olla korkeampia kuin toimeksiannon osalta muuten sovitut kustannukset (EDPB 2021a, 41).

Edellisten perusteella voidaan ajatella, että yksityisetsivän tulisi kyetä ohjeistamaan asiakkaansa sääntelystä johtuvista rajoituksista ja seuraamuksista, sekä varmistamaan, että asiakkaalta on saatu todenperäiset tiedot toimeksiannon suorittamiseksi. Sen lisäksi alihankkijalta voidaan odottaa myös käsittelyn lainmukaisuudesta varmistuminen. Edelliset huomioiden kovin yleisluontoinen lauseke ei ehkä tulisi kysymykseen. Pelkkä sopimuksella toteaminen, että ”asiakas huolehtii lakisääteisistä velvoitteistaan” ei ehkä riitä monimutkaisissa tapauksissa tuomaan toimeksisaajalle riittävää vastuuvapautta tilanteissa, joissa käytetään lukuisia erilaisia menetelmiä tai kohdistetaan toimia useisiin henkilöihin. Tämän vastuun vuoksi tässä työssä on käsitelty myös työnantajavelvoitteita, koska niillä voi olla merkitystä lainmukaisen ja riittävän laadukkaan yksityisetsiväpalvelun toimittamiseksi.

Kuten aiemmin luvussa Edellytykset, toimivaltuudet ja velvollisuudet rikoksen paljastamisessa todettiin, LYTP ei anna erityisiä toimivaltuuksia henkilötietojen käsittelyyn. Toisaalta ei myöskään rajoita sitä erityisesti. Mutta rikoksen paljastamisen yhteydessä se asettaa velvoitteen toimia kirjallisen sopimuksen perusteella. Vaikka toimeksianto ei perustuisi lakiin yksityisistä turvallisuuspalveluista, tulee huomioida luvussa 5.4.6 käsitelty velvollisuus henkilötietojen käsittelysopimuksesta. Sopimus taas rakentuu siten vähintään sen mukaan, mitä osapuolten välillä on sovittu henkilötietojen käsittelystä ja millaisessa kontekstissa käsittelyä suoritetaan: Esimerkiksi työsuhde, jossa luvussa 4 todettiin käsittelyä myös suoritettavan. Siten yksityisetsivätoiminnassa tapahtuvan henkilötietojen käsittelyn

lainsäädännöllinen viitekehys ja sopimuksella huomioitavat asiat näyttäisivät muodostuvan pääsääntöisesti alla olevan kuvion 9 mukaan.



Kuvio 9: Henkilötietojen käsittelyssä huomioitavat näkökulmat sopimuksilla ja toiminnassa yksityisetsivien toimeksiannoissa luvun 4 mukaan

6 Tulokset

Luvussa kolme kuvattiin suomalaista yksityisetsivätoimintaa lainsäädännön näkökulmasta. Luvussa neljä arvioitiin yksityisetsivien käytännön toimintaa ja toimijoita kansainvälisesti ja kansallisesti. Selvä johtopäätös on se, että lainsäädäntö Suomessa koskettaa vain osaa toiminnasta jättäen yksityisetsivätoiminnan kokonaisuuden sääntelemättä. Tämän ei todettu olevan sääntö Euroopassa, vaan toimintaa myös säännellään ja valvotaan joissain valtioissa

aktiivisesti. Yksityisetsivätoiminnassa sinällään ei nähty olevan merkittäviä poikkeamia kansallisen ja kansainvälisen toiminnan vertailussa. Suomalainen toiminta vaikutti saatavilla olevien tietojen perusteella hyvin samankaltaiselta kuin kansainvälinenkin. Suomalaisten toimijoiden kansainvälinen verkostoituneisuus tuli myös ilmi. Työn havaintojen perusteella ei voida myöskään päätellä, että luvussa neljä kuvatun kaltainen yksityisetsivätoiminta olisi sinällään laitonta tai mahdotonta. Viidennen luvun perusteella tosin selvä havainto on se, että ammattikuntaa koskeva sääntely on hajallaan useassa eri laissa.

Toimijoiden todettiin olevan kaikkialla pääsääntöisesti pieniä yrityksiä, joiden toiminta on kansainvälisesti verkottunutta. Luvussa neljä esitettiin myös kategorisointi, jolla pyritään kuvaamaan itse toimintaa ja sen luonnetta. Kategorisoinnin perusteella valittiin sekä määrällisin, että laadullisin perustein toimeksiannot, joiden osalta tehdään vielä tässä luvussa tarkempi analyysi. Ne on esitelty luvussa 6.2. Yksi neljännen luvun päähavaintoja oli kuitenkin se, että yksityisetsivätoiminnassa on ehkä yleistä turvallisuuskonsultointia lukuun ottamatta aina kyse henkilötietojen käsittelystä. Toisaalta turvallisuuskonsultointi esimerkiksi kameravalvonnasta voi johtaa henkilötietojen käsittelyyn. Siten myös siinä voidaan päätyä määrittelemään henkilötietojen käsittelyn keinoja ja tarkoituksia. Siten henkilötietojen käsittely liittyy lähes kaikkeen yksityisetsivätoimintaan.

Yksityisetsivätoiminta ja henkilötietojen käsittely ovat molemmat kytköksissä ihmisten perusoikeuksiin ja vapauksiin. Perinteisen omaisuuden vartioinnin osalta keskitytään laissa yksityisistä turvallisuuspalveluista (1085/2015) suojaamaan ihmisten koskemattomuutta säätelemällä tarkasti voimakeinojen käyttöä. Kuten neljännessä luvussa kuvattiin, tapahtuu rikosten ja väärinkäytösten selvittäminen luonnollisiin henkilöihin liittyviä tietoja – siis henkilötietoja – käsittelemällä. Toimeksiannoissa liikutaan aina yksityisyyden ja julkisen rajamaastossa ja toimeksiannoilla todettiin olevan oikeusvaikutuksia rekisteröityihin. Siinä mielessä henkilötietojen käsittely yksityisetsivätoiminnassa on tietyllä tavalla voimakeinojen käyttöä, joka kohdistuu yksityisyyteen. Tässä luvussa esitellään mallit, joilla pyritään pitämään huolta henkilötietojen lainmukaisesta käsittelystä ja käsittelyn oikeasuhtaisuudesta.

Työn alkuperäisenä tavoitteena oli tuottaa malli tai kehittämisehdotuksia siitä, mitä henkilötietojen käsittelyssä on huomioitava yksityisetsivätoiminnassa. Kehittämisehdotusten vaara on kuitenkin jäädä irrallisiksi huomioiksi tai pitkäksi luetteloksi vailla kiinnekohtaa toimintaan. Työn tuloksena ei voi myöskään esittää tyhjentävästi yhtä mallia, joka olisi yleispätevä kaikkiin tilanteisiin. Henkilötietojen käsittelyyn liittyvät vastuut ja velvollisuudet voivat poiketa paljonkin, jos yhtälössä muuttuu vain yksikin pieni tekijä. Esimerkkinä vaikka henkilöetsintä, jonka osalta lainmukaisuusperuste on täysin erilainen riippuen siitä, tehdäänkö etsintää metsään talvisäässä eksyneen ihmisen pelastamiseksi vaiko vain vanhan tutun löytämiseksi kuulumisten vaihtoa varten. Kaikkiin tilanteisiin soveltuvan mallin luonti

voisi olla sekavuutensa ja moniulotteisuutensa puolesta niin hankala, että sen ymmärrettävyys – saati hyödynnettävyys – olisi täysin olematon.

Sen vuoksi tuloksissa esitetään sekä toiminnan kuvaamisen perusteella (luku 4) ja siihen sovellettavan lainsäädännön (luku 5) pohjalta yksittäisiä malleja, jotka liittyvät merkittävimpiin velvoitteisiin tilanteissa, jotka tunnistettiin olennaisiksi. Näistä jäsentyy kokonaisuus, joka lähestyy ensin toimijaa ja toimijan roolia ja menee yksityiskohtaisemmaksi mitä lähemmäs tullaan itse käytännön toimeksiantoa. On vaikea vetää rajaa siihen, mikä on yksiselitteisesti toimeksisaajan ja mikä toimeksiantajan vastuulla. Avainasemassa on luvussa 5.9 käsitelty sopimus ja sen sisältö. Malleista kuitenkin saa ainakin viitteet siitä, mistä tulee sopia. Malleja voi hyödyntää esimerkiksi luvussa 3.1 viitattuun turvallisuusalan valvontayksikön tarkastuksen kohteena olevan toimintakäsikirjan luomisessa tai muuten oman toiminnan ja vastuiden tarkastamiseen ja toimintaohjeiden luomiseen.

Tuloksissa esitetyt kaaviot ovat yleisluontoisia malleja toimijaan kohdistuviin yleisiin tai erityisiin velvoitteisiin liittyen tai luvussa neljä tunnistettuihin yleisimpiin toimeksiantoihin. Kaaviot eivät ole tyhjentäviä, eikä niiden tehtävä ole olla yksityiskohtaisia ohjeita. Kaaviot ovat prosesseja, jotka toimijoiden on esitettyjä tilanteita varten käytävä läpi ja otettava vähintään niissä esitetyt asiat huomioon. Yksityiskohtaisemman analyysin huomioonotettavista asioista kaavion käyttäjä saa teoriaosan luvuista, joihin kaavion yhteydessä olevassa luvussa tai kaaviokuvassa viitataan. Teoriaosuuden käyttäminen ja tietosuojalainsäädännön yleisempi tuntemus on välttämätöntä kaavioiden hyödyntämiseksi. Esimerkiksi luvun 6.1 kaavion ensimmäinen päätöspiste on kysymys siitä, käsitelläänkö toimeksiannossa henkilötietoja. Tätä varten tulee tietää, mikä on tietosuojalainsäädännön näkökulmasta henkilötietoa ja asiaa voi joutua kertaamaan myös luvusta Tietosuoja-asetus. Siten tulokset muodostavat teoriaosansa ja tulosten kanssa yhdessä käytettävän kokonaisuuden.

Työn kirjoitusvaiheessa kaavioissa oli värein erotettu asiat, jotka kuuluvat käsittelijän vastuulle ja asiat, jotka kuuluvat rekisterinpitäjän vastuulle. Monet asiat kuitenkin kuuluvat molempien vastuulle, mutta vastuu ei ole aina silti yhtäläinen. Lisäksi voisi olla kiistanalaista, että mikä kuuluu asiantuntijapalveluita tuottavan erityisosaajan vastuulle ja mikä asiakkaan tulisi itse ymmärtää (vrt. luku Sopimusoikeus). Asioiden siirtäminen yleisesti sopimuksella ei ole välttämättä riittävää. Esimerkiksi tilanne, jossa sopimuksella sovittaisiin informoinnin olevan rekisterinpitäjän vastuulla, mutta käsittelijä tekisi jopa rekisterinpitäjän valtaan kuuluvia päätöksiä poiketa menetelmissä ilmoittamatta rekisterinpitäjälle. Tässä kohtaa sopimus ei enää riittäisi vastuiden tulkintaan. Todennäköisempi tilanne on sellainen, jossa sopimus on niin yleisluontoinen, että toinen osapuoli voi kiistää ymmärtäneensä sen sisältöä. Siksi kaavioissa on yleisesti esitetty asiat, joista tulee sopia ja jotka tulee määritellä parhaassa tapauksessa yhdessä osapuolten välillä. Siten kuin henkilötietojen käsittelystä tulee luvun 5.3.6 mukaan sopia; yksityiskohtaisesti. Värikoodit voisivat ohjata liian

yksinkertaistettuun tulkintaan ja saada toimijat sivuuttamaan mahdollisesti olennaisia ja tärkeitä velvoitteita.

Lukujen 6.1 ja 6.2 tuloksia tulkitessa tulee koko ajan muistaa muutama yleisjohtopäätös

1. EU-oikeus on etusijaista kansalliseen lainsäädäntöön nähden (Luku 5.2)
2. Rikoksiin liittyvät tai jopa puuttuvaan rikoshistoriaan liittyvät tiedot voidaan tulkita rikoksiin liittyviksi tiedoiksi (Luku 5.3)
3. Kaikki asiat on hyvä olla osoitusvelvollisuuden vuoksi paperilla (Luku 5.3.1)
4. Yksityisetsivätoiminnassa on huomioitava koko ajan, milloin ylitetään kynnys, jonka jälkeen rikosepäily on siirrettävä viranomaiselle (valmistelu vs. vaikutuksia aiheuttavat päätökset, luvut 3.3 ja 5.6)
5. Keinojen on oltava oikeasuhtaisia tavoiteltuun etuun sekä vartioimisliiketoiminnan yleisten periaatteiden, että henkilötietojen käsittelyn lainsäädännön näkökulmasta (esimerkiksi luvut 3.3, 5.3.2 ja 5.6.1)
6. Kaikkien henkilötietojen käsittely tulee perustua käyttötarkoituksen muodostamaan tarpeeseen. Etenkin työelämässä käsittelyn tarve tulee olla rajattu työsuhteen kannalta välittömästi tarpeelliseen. Siten toimeksiannoissa on huomioitava sen varmistaminen, ettei ylimääräisiä ja tarpeettomia tietoja kerry (luvut 5.3.1 ja 5.7)
7. Rekisteröidyt voivat hakea korvauksia henkilötietojen käsittelystä aiheutuneista vahingoista keneltä tahansa käsittelyketjuun osallistuneelta (luku 5.8).

6.1 Yksityisetsiviin kohdistuvat yleisemmät velvoitteet

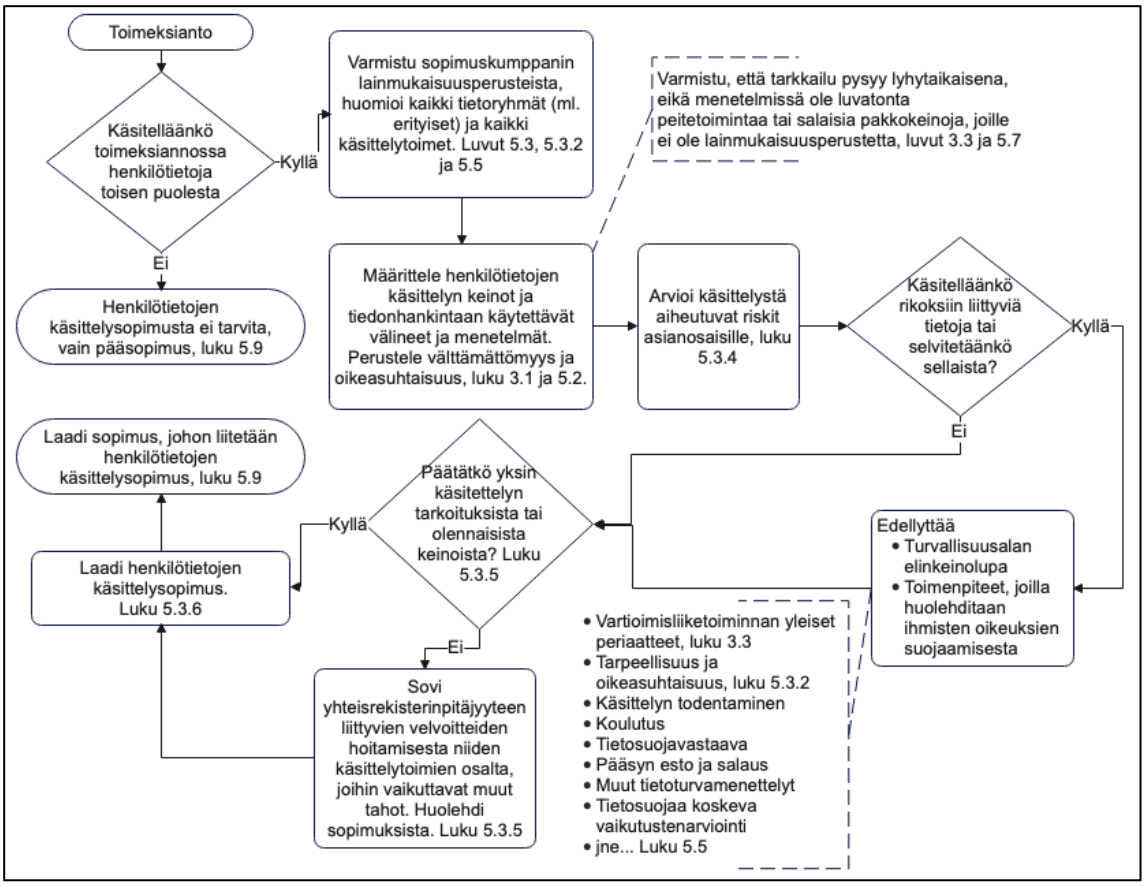
Luvussa 5.3.5 käsiteltiin rooleja henkilötietojen käsittelyn osalta. Siinä ja monessa muussakin yhteydessä on todettu velvoitteiden jakautuvan pääosin sen mukaan, mikä on toimijan rooli käsittelyssä. Luku 5.5 osoitti, että Suomessa ei ole laillista oma-aloitteisesti kerätä tai ylläpitää itsenäisesti henkilörekistereitä ilman lainmukaisuusperusteita. Se ei voisi tapahtua edes rikostorjunnan tai rikosten selvittämiseksi, koska luvussa 3.3 todettiin, että yleisen järjestyksen ja turvallisuuden ylläpito kuuluu kokonaan viranomaiselle. Siten ei ole nykylainsäädännön valossa todennäköistä, että yksityisetsivä voisi olla yhtä aikaa laillisesti toimiva ja rikoksia selvittävä itsenäinen rekisterinpitäjä. Poikkeuksena rekisterinpitäjyyteen on tietenkin yksityisetsivää itseään ja esimerkiksi sen henkilöstöä koskevien henkilötietojen käsittely, Niiden tietojen käsittelylle on olemassa lainmukaisuusperuste (työsuhde).

Kuten luvussa 5.3.5 todettiin, rekisterinpitäjän vastuut ja roolin voi saada vaikka käsittely olisikin laitonta. Alla olevien kaavioiden tarkoitus on kuitenkin pyrkiä varmistamaan, että henkilötietojen käsittely on laillista. Luvussa 5.3.6 todetun mukaan käsittelijän lainmukaisuusperuste taas voidaan johtaa rekisterinpitäjän lainmukaisuusperusteesta, jolloin yksityisetsivätoimeksiantojen suorittaminen toisen lukuun on mahdollista rekisterinpitäjän lainmukaisuusperusteeseen vedoten. Käsittelijänä toimimiselle olennainen tunnusmerkki oli

myös luvussa 5.3.5 käsitelty palvelun tuottaminen puhtaasti liiketoimintalähtöisesti rahallisen korvauksen saamiseksi. Siksi alla olevan kaavion lähtökohtana on se, että toimitaan toimeksiantoperusteisesti kuten luvun 4.3 mukaan toiminnalle onkin tyypillistä. On kuitenkin huomioitava luvussa 5.3.5 käsitellyt rekisterinpitäjän valtaan kuuluvista olennaisista elementeistä päättäminen, jossa todettiin tarvittavan molempien osapuolten yhteistyötä, että rekisterinpitäjyys säilyy alkuperäisellä tarkoitetulla rekisterinpitäjällä, eikä toimeksisaajasta muodostu itsenäistä rekisterinpitäjää. Henkilötietojen käsittelysopimuksen osalta on huomioitava luvussa 5.8 mainittu velvoite laatia se myös suullisten tai muussa muodossa tehtyjen toimeksiantojen osalta.

On toki mahdollista, että yksityisetsivä käyttäisi merkittävää valtaa henkilötietojen tarkoituksista ja keinoista päättämisessä. Tällainen tilanne voisi tulla eteen, jos tutkinnan edetessä yksityisetsivä tuloksia saadakseen päättäisi käsitellä sille luovutettuja henkilötietoja tarkoituksiin, joista toimeksiantaja ei ole tietoinen. Silloin tulee kuitenkin huomioida se, että yksityisetsivä vastaisi rekisterinpitäjänä kaikista tietosuoja-asetuksen rekisterinpitäjälle asetetuista velvoitteista. Koska yksityisetsivät ovat tyypillisesti pieniä toimijoita, voisi näihin velvoitteisiin vastaamisesta koitua suuri hallinnollinen ja sitä kautta taloudellinen taakka. Yksityisetsivän olisi näissä tilanteissa huolellisesti arvioitava sille tulevat vastuut ja niiden käytännön toteuttamismahdollisuudet. Myös luvussa 5.3.5 esiin nostettu vahingonkorvausvastuu kokonaisvahingoista voi olla sietämätön riski kannettavaksi pienelle yritykselle. Rekisterinpitäjän roolin ottaminen tulisi olla ainakin hyvin harkittu teko.

Siksi esimerkiksi rekisteröityjen oikeuksien toteuttamista ei käsitellä tuloksissa, koska luvussa 5.3.3 todettiin rekisteröityjen oikeuksien toteuttamisen olevan rekisterinpitäjän vastuulla. Tosin pitää muistaa samassa luvussa oleva huomio, että henkilön halutessa toimeksiantajalta jäljennöksiä itsestään tallennetuista tiedoista, koskee luovutusvelvollisuus myös yksityisetsivän keräämiä tietoja. Tietojen säilytykseen liittyviä asioita ei myöskään tarvitse käsitellä, koska niiden poistamisesta ja jatkokäyttötarkoituksista voi laillisesti päättää vain rekisterinpitäjä. Käytännössä käsittelijöiden on aina poistettava tai palautettava käsittelemänsä henkilötiedot käsittelyn tai sen tarpeen lakattua luvussa 5.3.6 todetun mukaan.



Kuvio 10: Sopimus on edellytys käsittelijänä toimimiselle

Kuvion 10 kaikissa vaiheissa tulee muistaa se, että sekä käytettyjen tutkintamenetelmien osalta johtuen laista yksityisissä turvallisuuspalveluissa ja henkilötietojen käsittelyssä johtuen tietosuoja-asetuksesta, kaikki keinot tulee olla tarpeellisia ja oikeasuhtaisia. Tämä pitää pystyä tarvittaessa osoittamaan jälkikäteen ja tästä tulee huolehtia myös, mikäli näihin tulee muutoksia kesken toimeksiannon. Lisäksi sopimuksen tulee luvussa 5.3.6 todetun mukaan sitoa käsittelijää rekisterinpitäjään, joten se tuskin voi olla kovin väljä tai vastuurajauksiltaan kapea.

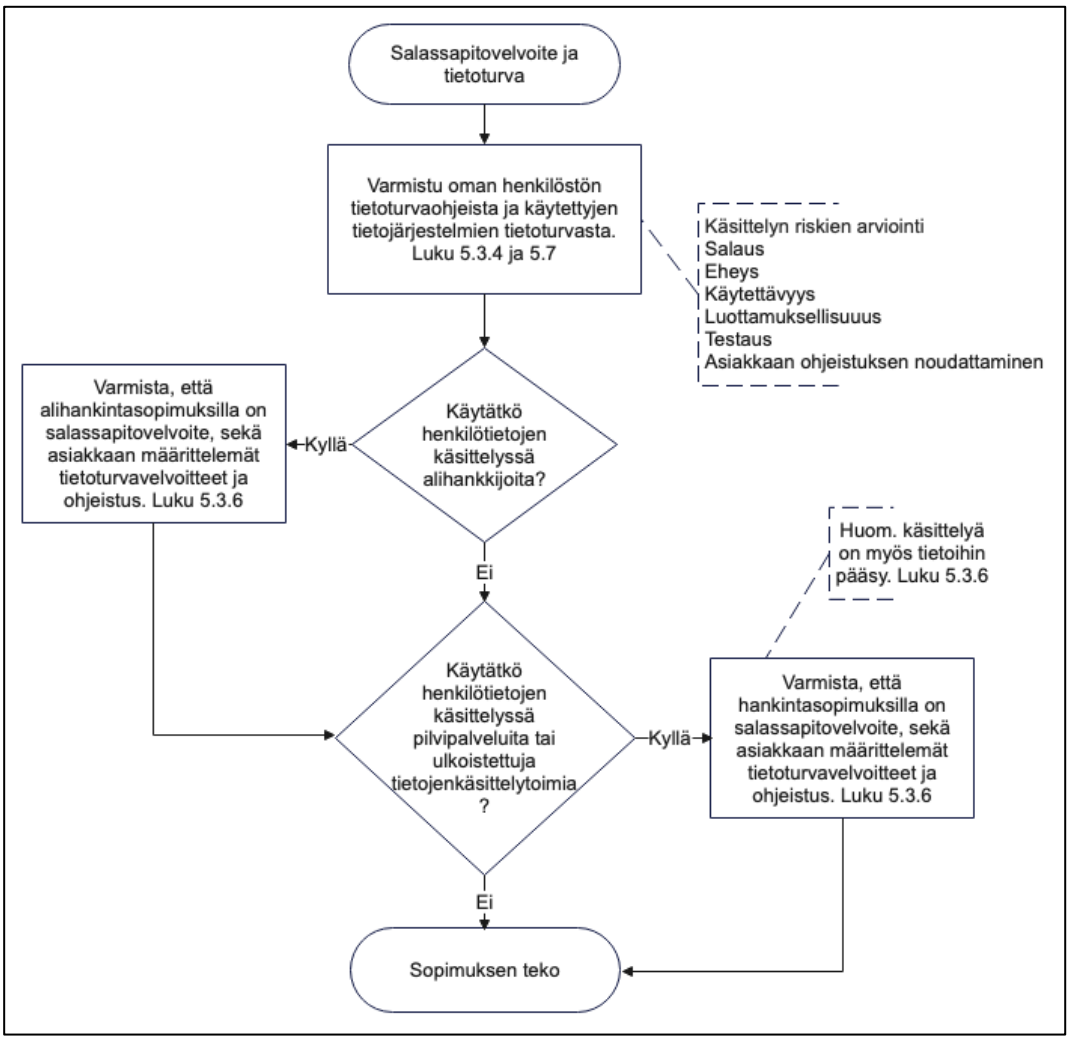
Luvussa 5.3.5 todetun mukaan yhteisrekisterinpitäjyys voisi tulla kyseeseen tilanteessa, jossa tutkinnan menetelmiä voisi määritellä jokin ammatillinen liitto tai yhdistys, jolloin käsittelyn rooli toimeksiantajaan nähden olisi silti käsittelijä. Silloin olennaisia juuri käsittelijään kohdistuvat velvoitteet. Nämä kohdistuvat kaikkiin yksityisetsivätoimintaa tekeviin, erityisesti rikosten paljastamisen yhteydessä, joka on laissa määritelty ansaintatarkoituksessa tapahtuvaksi toimeksiantajan lukuun suoritettavaksi tehtäväksi (Luku 3.1). Velvoitteita käsiteltiin luvussa 5.3.5 ja niiden todettiin olevan:

- Salassapitovelvoitteen olemassaolosta varmistuminen käsittelyä suorittavien osalta
- käsittelyn tietoturvasta varmistuminen

- rekisterinpitäjän avustaminen lainmukaisuuden toteuttamisessa
- käsittelytoimien selostetta vastuullaan olevista käsittelytoimista
- nimitettävä tietosuojavastaava tietyissä tilanteissa
- kansainvälisiä henkilötietojen siirtoja koskevat velvoitteet

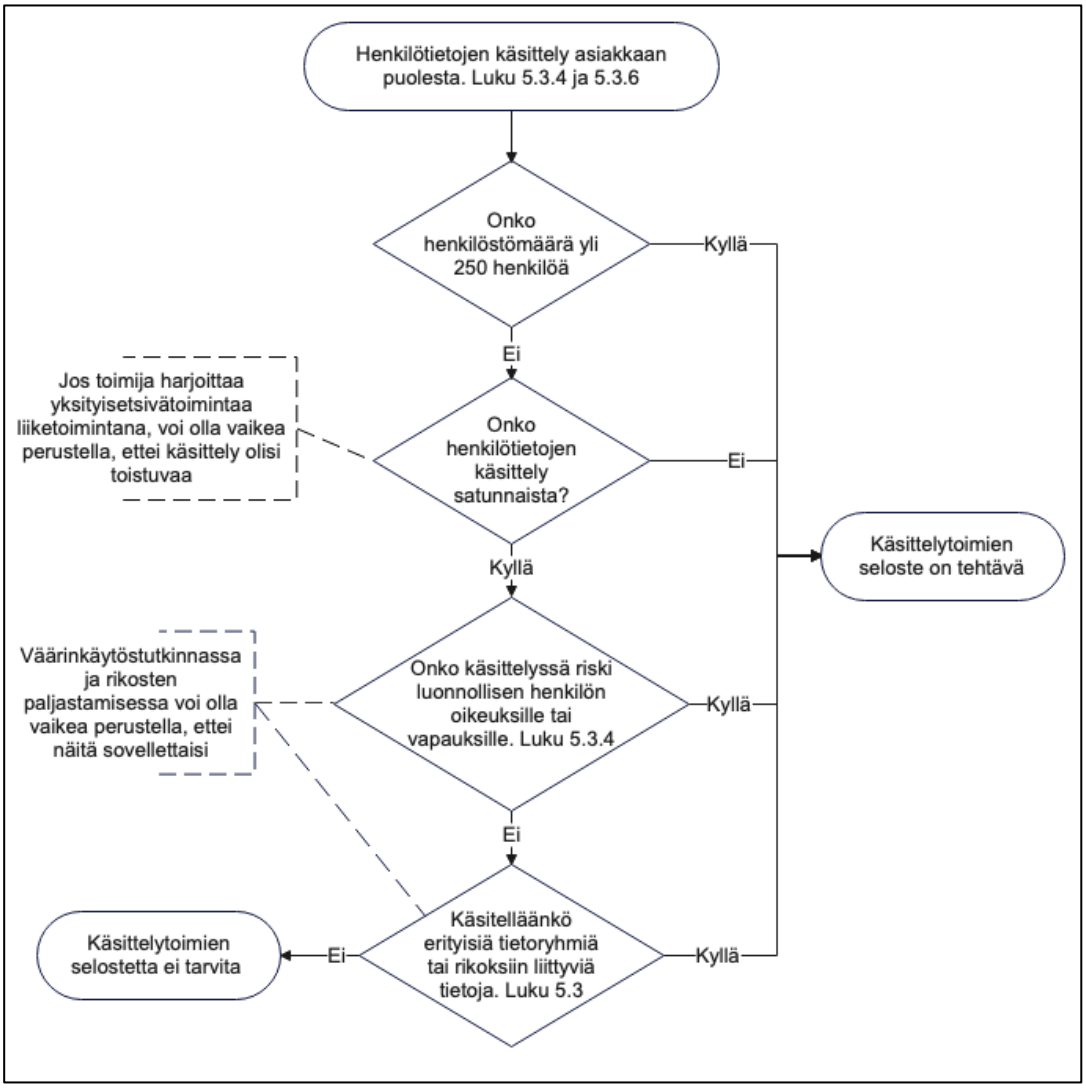
Yksinkertaisin edellisistä on rekisterinpitäjän avustamisvelvoite, jonka osalta mainittiin luvussa 5.3.6 tärkeää olevan lähinnä varautuminen rekisterinpitäjän avustamiseen ja niihin liittyvistä kustannuksista sopiminen.

Yksi keskeinen henkilötietojen suojaamisen periaate todettiin olevan salassapito. Yrityksillä on usein kumppaneita ja palveluita, joiden tuotteet tai palvelut voivat olla henkilötietojen käsittelyn osana. Siksi salassapidosta tulee huolehtia myös näiden osalta. Kuvio 11 valottaa tarkemmin alihankkijoiden tunnistamista yksityisetsivätoimintaa harjoittavan yrityksen toiminnassa.



Kuvio 11: Salassapidosta ja tietoturvamenettelyistä varmistuminen

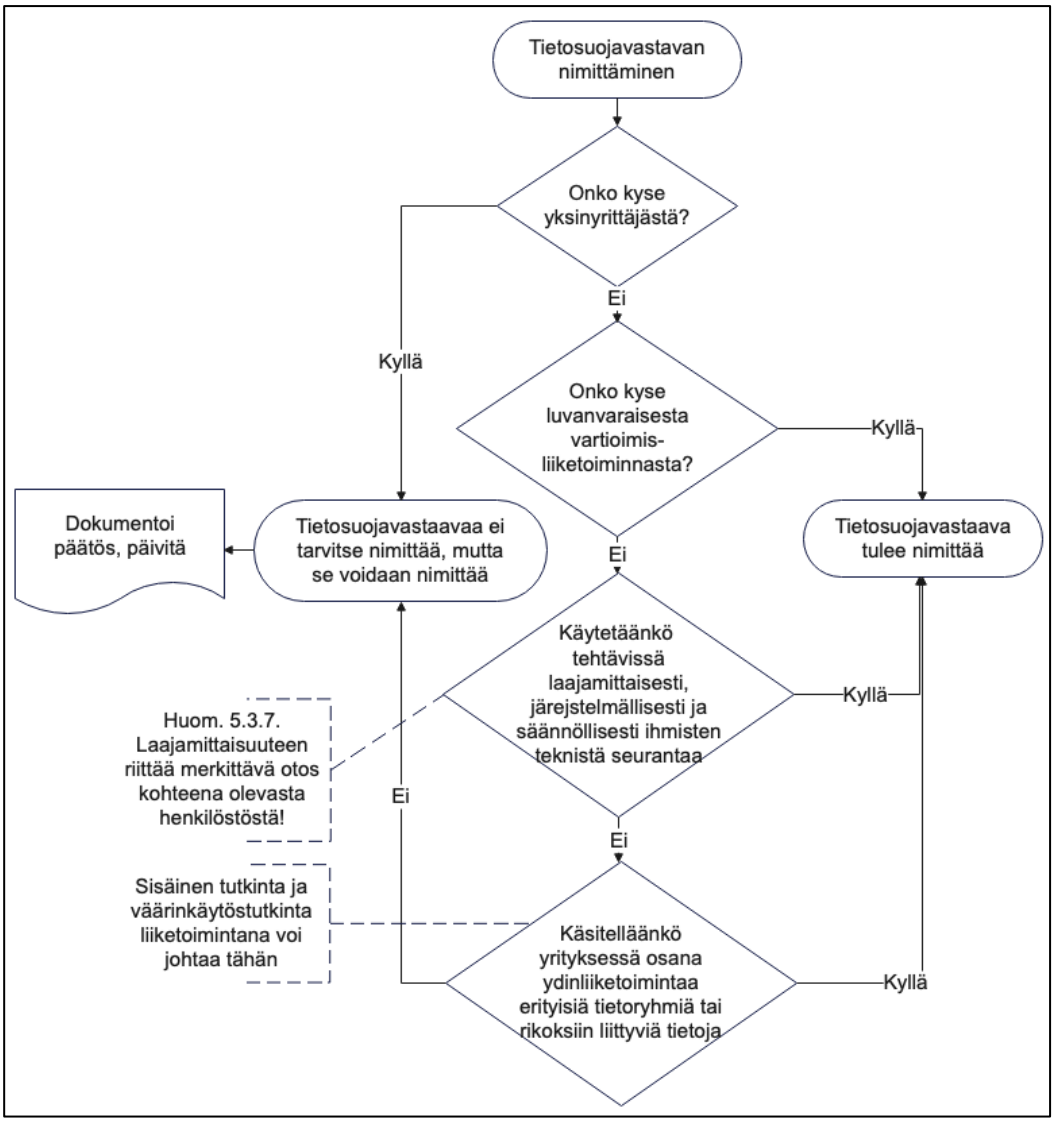
Käsittelytoimien selostetta sivuttiin luvussa 5.3.4. Käsittelijän ollessa kyseessä, seloste ei itsessään ole kovin haastava laatia ja siihen löytyy ohjeet ja mallipohjat Tietosuojavaltuutetun toimiston sivuilta (Tietosuojavaltuutetun toimisto 2021a, Seloste käsittelytoimista). Työn tavoitteiden kannalta oli olennaisempaa tunnistaa, milloin se tulee tehdä ja se on kuvattu alla kuviossa 12.



Kuvio 12: Käsittelytoimien selosteen laatimisvelvoitteesta päättäminen

Luvussa 3.1 todettiin, että hallitus on katsonut vartioimisliiketoimintaa harjoittavien olevan julkisen vallan käyttäjiä, jolloin tietosuojavastaavan nimittämisvelvollisuus koskisi vähintään luvanvaraista rikoksen paljastamista ja selvittämistä, koska määrittely on tehty lain tasolla. Tosin tavanomaisessa väärinkäytöstutkinnassa voi tilanne olla muunlainen. Luvussa 5.3.7 tunnistettiin kuitenkin muitakin tekijöitä, jotka velvoitteen voivat laukaista. koska perinteisissä kamera- ja kulunvalvontaratkaisuissa voidaan joutua käyttämään laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa, jota toimeksisaaja suorittaa osana

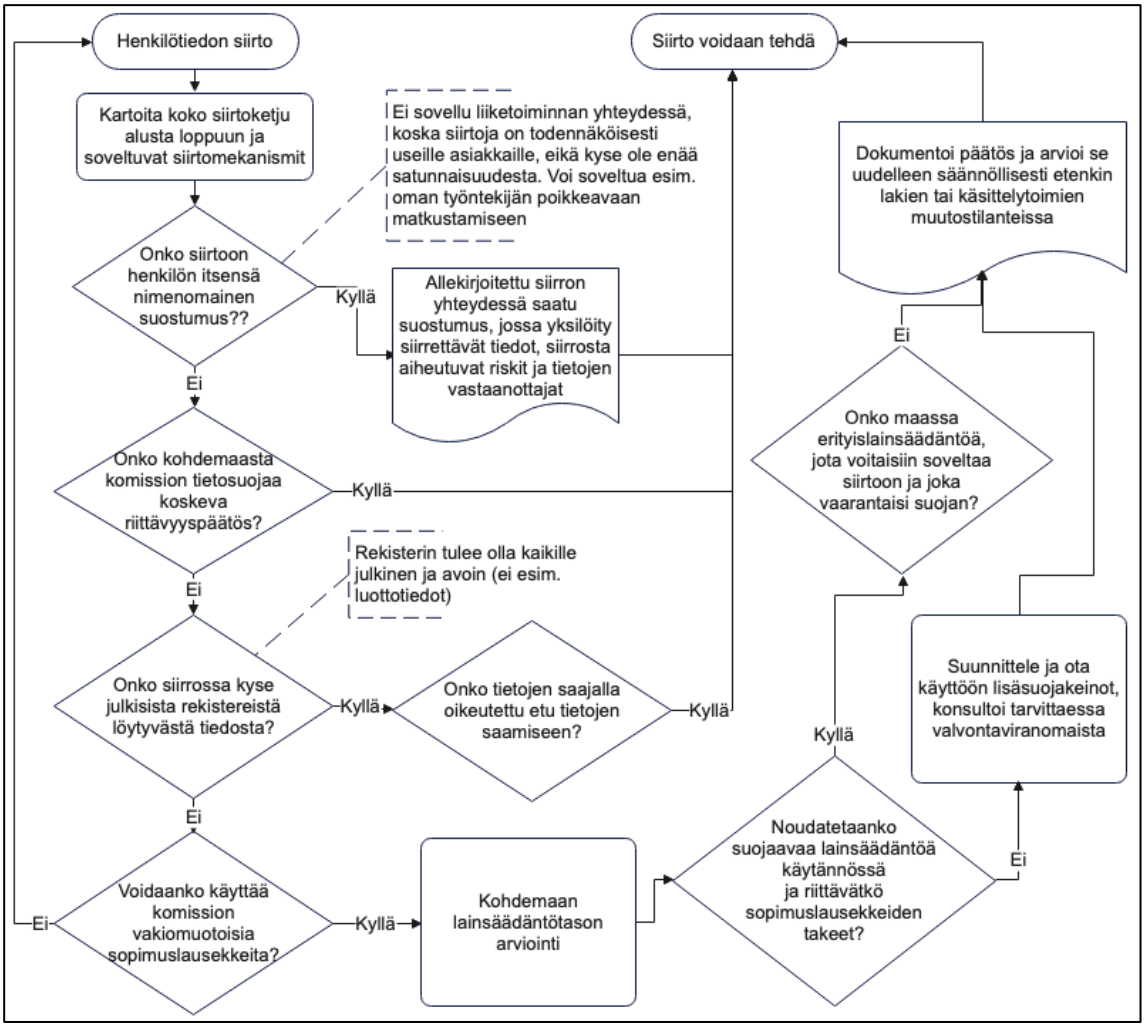
ydintehtäviään. Alla olevassa kuviossa 13 on vielä kerrattu olosuhteet nimittämisvelvoitteen taustalla.



Kuvio 13: Tietosuojavastaavan nimittämisvelvoite

Kansainväliset siirrot käsiteltiin luvussa 5.3.6 sopimusten yhteydessä ja olennaista yksityisetsivän näkökulmasta on huomata, että siirto tässä yhteydessä käsittää vain tietojen viemisen ETA-alueen ulkopuolelle. Henkilötietojen tuontiin ei rajoituksia ole johtuen luvussa 5.3 käsittelyn soveltamisalasta: koska tietosuoja-asetusta sovelletaan kaikkeen ETA-alueella tapahtuvaan käsittelyyn, sitä sovelletaan myös muualta tuotuihin tietoihin. Siksi siirto tässä kohtaa voidaan ymmärtää ikään kuin tietojen vientinä. Alla olevassa kuviossa 14 käsitellään yksittäistä henkilötiedon siirtoa, mutta kuvion velvoite tulee ymmärtää sovellettavaksi jokaiseen yksittäiseen siirtoon, miksi niiden kartoittaminen voi olla hyvä tehdä esimerkiksi aiemmin mainitulla käsitellyllä ja luvussa 5.3.6 ehdotetulla käsittelytoimien selosteella.

Kuten luvussa 5.3.6 todettiin, sovelletaan siirtoja koskevia velvoitteita myös käsittelijään. Mutta siirroista päättämisen todettiin luvussa 5.3.5 kuuluvan rekisterinpitäjän määräysvaltaan. Siksi ennen siirtoa tulee tarkistaa myös se, mitä sopimuksella on sovittu siirron toteuttamisesta, jos rekisterinpitäjä on itsekin sijoittunut ETA-alueelle. Ellei ole, vastaa käsittelijä yksin siirrosta. Kaaviosta on jätetty pois myös suojamekanismit, jotka luvussa 5.3.6 todettiin epätodennäköisiksi käytettäväksi yksityisetsivätoiminnassa, mutta tilanteessa, jossa vakiomuotoisten sopimuslausekkeiden käyttö ei sovellu, niitä voi olla syytä arvioida uudelleen. Yksityisetsivätoiminnassa on aina luvuissa 3.1 ja 4 todetun mukaan kyse sopimusperusteisesta käsittelystä, oli kyse sitten suoraan asiakkaalle tehtävästä toimeksiannosta tai alihankinnasta. Siten ei voida kovin helposti perustella sitä, etteivät sopimuslausekkeet soveltuisi, koska sopimus on tehtävä jollain tavalla joka tapauksessa. Siirto tulee arvioida luvun 5.3.6 mukaan alusta loppuun ja siinä tulee huomioida myös alihankkijoiden alihankkijat.



Kuvio 14: Henkilötietojen siirto ETA-alueen ulkopuolelle

6.2 Valittuihin tapauksiin liittyvät erityistilanteet

Edellä olevat kaaviot keskittyivät toimijoihin kohdistuviin velvoitteisiin riippumatta itse toimeksiannosta. Tässä luvussa käsitellään taas neljännessä luvussa valittuihin tapauksiin liittyvät velvoitteet. Näitä olivat:

1. Jäljitystehtävä, jossa sekä toimeksiantaja, että kohde ovat yksityishenkilöitä. Kummallakin osapuolella on siten lain takaamat perusoikeudet, jotka saattavat olla jopa ristiriidassa keskenään. Tällainen tilanne voi syntyä esimerkiksi silloin, kun vanhempi etsii täysi-ikäistä lastaan, tai aviopuoliso kumppaniaan, mutta toinen osapuoli ei halua tulla löydetyksi.
2. Rekrytointitilanteeseen liittyvä taustojen tarkistaminen. Tässä tilanteessa joudutaan tulkitsemaan oikeushenkilön tiedonsaantioikeutta ja valtaa henkilötietojen käsittelyssä suhteessa yksityishenkilöön. Tilanteessa joudutaan huomioimaan myös työoikeudellisia näkökulmia ja siten tällaisen tilanteen käsittely voi tuottaa enemmän kiinnostavaa informaatiota kuin toistaa edellisen tyyppiesimerkin tilanne.
3. Tutkintatoimeksiannoissa työantajaan kohdistuvan väärinkäytöksen selvittäminen.

Henkilöiden jäljitystehtävät ovat todennäköisesti ainoa tapauksiin liittyvä tilanne, jossa yksityisetsivä työn suorittajana voi käyttää merkittävää valtaa henkilötietojen käsittelyn keinoista päättämisessä. Koska kyse on kuitenkin kaupallisesta toimeksiannosta, on erittäin kyseenalaista, että yksityisetsivä voisi päättää kuitenkaan henkilötietojen käsittelyn tarkoituksista kuten luvussa 5.3.5 todettiin. Yksityisetsivätoiminnassa ei ole mitään erityisiä toimivaltuuksia kerätä tietoja muista ihmisistä varmuuden vuoksi tai perustamalla ihmisten seurantaan tai tarkkailuun perustuvia rekistereitä tai niiden osia kuten luvussa 5.5 todettiin. Näissä toimeksiannoissa on luonnollisesti huomioitava myös kuluttajansuojalaki (luku 5.8).

Yksityishenkilön tai yrityksen palkatessa yksityisetsivää jäljittämään jonkun yrityksen tai henkilön sijainti, voidaan tietoja hakea monista eri paikoista ja monin eri tavoin. Näitä keinoja ja menetelmiä voi olla mahdoton kuvata etukäteen tyhjentävästi, koska tietolähteitä voi olla julkisten rekisterien lisäksi myös henkilöiden haastattelut tai internetistä asianosaisten tai asiaan liittyvien ihmisten julkaisemat tiedot. Uusia tietolähteitä voi paljastua myös jäljityksen edetessä. Siten tilanne voi olla sellainen, jossa tilaajalla ei ole mahdollista määritellä keinoja etukäteen tyhjentävästi tai ohjeistaa käsittelyä riittävän tarkasti.

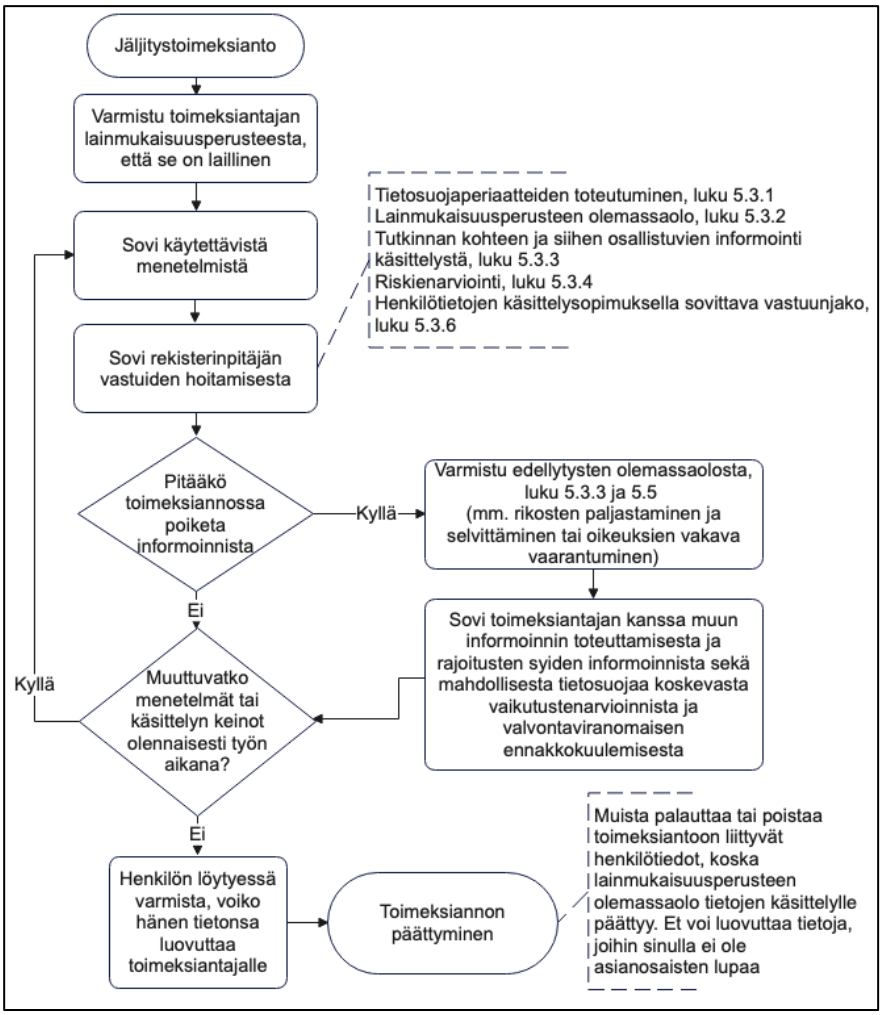
Tietojen karttuessa, uudella tiedolla voi olla merkitystä myös keinojen kehittymiseen tai uusi tieto voi jopa muuttaa käsittelyn tarkoituksia tai tuoda käsittelyyn tarkoituksia, joita ei ollut nimetty alkuperäisessä toimeksiannossa. Näiden pohjalta toimeksiantaja ja toimeksisaaja voivat tehdä joko yhteisiä päätöksiä, tai päättää yksipuolisesti henkilötietojen käsittelystä. Joka tapauksessa yhteistyön tulee olla tiivistä, että mahdollisista tarkoituksista ja keinoista

voidaan sopia siten, että asiasta tehdyn toimeksiantosopimuksen tarkoitus täyttyy ja osapuolet voivat toimia tarkoituksenmukaisissa rooleissaan. Näistä vastuista ja rooleista tulee myös sopia siten, että henkilöiden oikeus saada tietoja siitä käsitelläänkö heidän tietojaan ja mihin tarkoituksiin, toteutuisi (luku 5.3.2)

Tärkeintä jäljitystehtävän osalta on määritellä sen lainmukaisuusperuste. Tapauksen kiireellisyys, siinä käytettävät keinot ja mahdolliset riskit riippuvat paljon siitä, onko tarkoituksena pelastaa talvella metsään kadonnut ihminen, omatoiminen muistisairas kaupungista, tarkoituksella piilotteleva velallinen vai esimerkiksi varastettu omaisuus ja sen haltija. Lainmukaisuusperuste on aina sidottu tarkoitukseen, jolloin henkilötietojen käsittelyn alkuperäinen tarkoitus tulee toimeksiantajalta. Toimeksisaajalla tulisi olla jonkinlainen käsitys siitä, että tarkoitus on lainmukainen, ettei tehtävää suorittaessaan syyllisty henkilötietojen käsittelyyn ilman laillista perustetta (esimerkiksi luku 5.3.2). Etenkin yhteisrekisterinpitäjänä vastuu lainmukaisesta käsittelystä kuuluisi sekä toimeksiantajalle ja toimeksisaajalle yhtäläisesti. Toimeksiantaja voi olla myös tietämätön siitä, millaisia selvityksiä ylipäätään saa lain mukaan tehdä, jolloin sopimusoikeudellisesti toimeksisaajalla on todennäköisesti korkeampi vastuu toimituksen lainmukaisuudesta (luku 5.8).

Koska oikeus yksityisyyteen on kaikille kuuluva oikeus, on tämä oikeus myös henkilöillä, joihin jäljitys kohdistuu. Siten ihmisellä on oikeus myös kadota, kuten luvussa 4.5 todettiin. Siten yksityisetsivä joutuu väistämättä yksityishenkilöä jäljitettäessä tilanteeseen, joissa toimeksiantaja ei voi yksipuolisesti päättää henkilötietojen saamisesta ja tämä voi johtaa yksityisetsivän osalta kasvaneeseen vastuuseen. Itsenäistä rekisterinpitäjää toimeksianto ei yksityisetsivästä tee vain siksi, että toimeksiantajalla ei ole kaikkia yksityisetsivän tiedossa olevaa tietoa. Luvussa 5.3.5 todetun mukaan toimeksiantaja voi olla rekisterinpitäjä, vaikka hänellä ei olisi pääsyä käsiteltäviin henkilötietoihin. Riittää, että on voinut päättää käsittelyn tarkoituksista ja keinoista.

Toimeksiannon edetessä voidaan joutua keräämään kolmansien osapuolten henkilötietoja, eikä toimeksiantaja pysty välttämättä vaikuttamaan siihen, mitä heille kerrotaan heidän henkilötietojensa käsittelystä. Siksi osapuolten tulee sopia huolellisesti rekisterinpitäjälle kuuluvien vastuiden hoitamisesta ja menettelytavat, ettei yksityisetsivästä tule tahtomattaan ja vastoin toimeksiannon tarkoitusta itsenäistä rekisterinpitäjää. Näiden kolmansien osapuolten oikeuksien turvaamiseksi toimeksisaaja voi joutua toimimaan yhteisrekisterinpitäjänä toimeksiannon joissain vaiheessa, etenkin jos hän päättää olla luovuttamatta tietolähteidensä tietoja toimeksiantajalle tai toimeksiantajaansa tietolähteilleen. Silloin pitää huolehtia siitä, että rekisterinpitäjän vastuut tulee kuitenkin hoidettua. Osapuolten vastuiden ja velvoitteiden vuoksi on siis varmistettava ainakin kuviossa 15 esitellyt asiat.



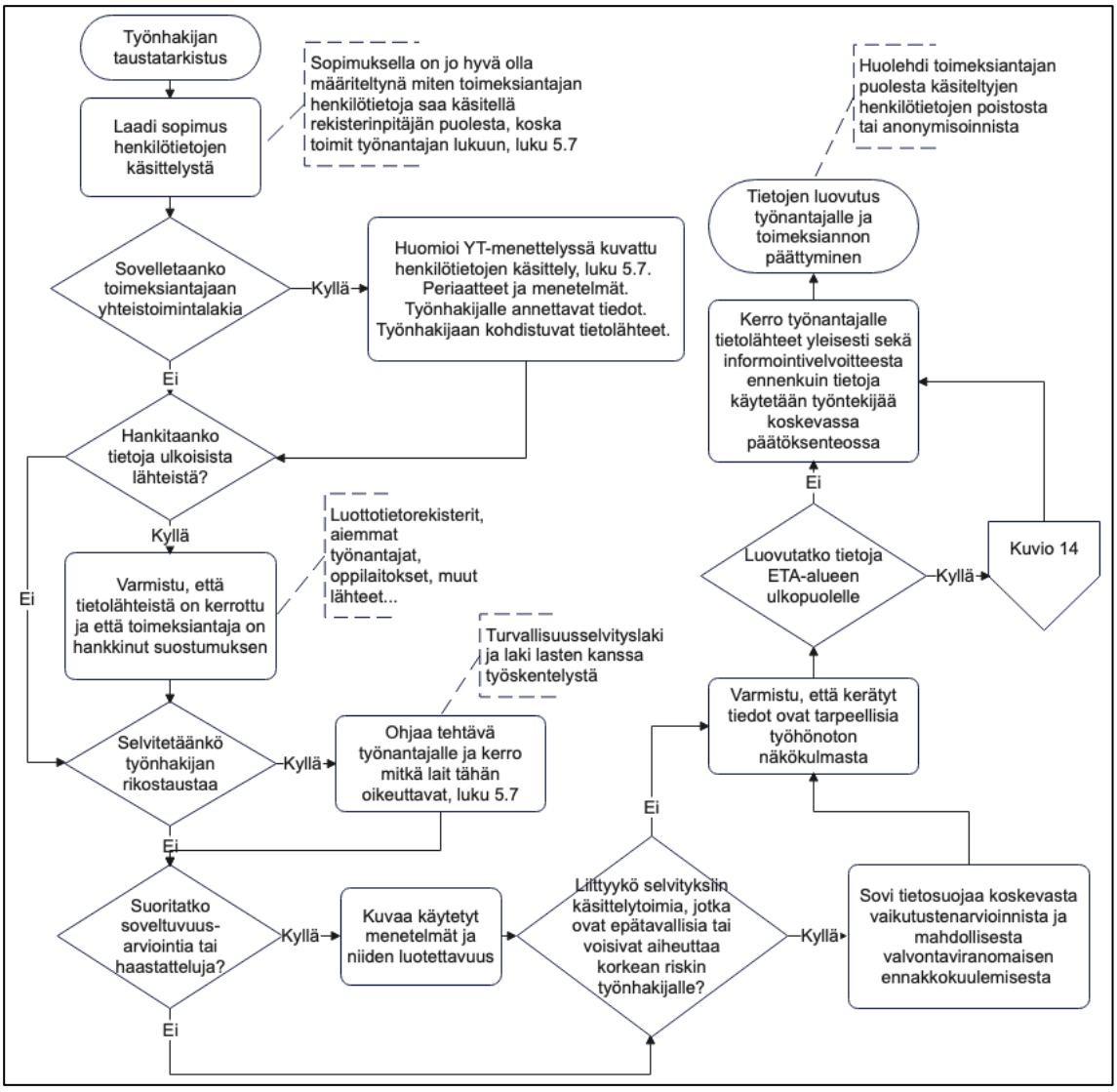
Kuvio 15: Jäljitystoimeksiannon suorittaminen

Yksityisetsivän selvitellessä työnhakijan taustoja, on käsittelyn tarkoitus luotettavuuden selvitys työn tilaajalle, jolloin tilaaja määrittelee tarkoituksen ja lainmukaisuusperusteen (luku 5.3.5). Työn suorittajalla tuskin on omaa intressiä, paitsi mikäli kyseessä oli rekrytointiin erikoistunut toimisto, joka käyttäisi selvityksiin myös omia tietokantojaan ja täydentäisi niitä tilaajilta saamillaan henkilötiedoilla. Tällöin olisi kyseessä itsenäinen rekisterinpitäjä, jolla tulisi olla oma lainmukaisuusperuste käsittelylle, informoida aktiivisesti rekisteröityjä käsittelystä ja kyetä toteuttamaan heidän oikeuksiaan suoraan heille. Rekisteri ei voisi kuitenkaan sisältää rikoksiin liittyviä tietoja. Tämä ei kuitenkaan ole tavanomaista yksityisetsivätoimintaa luvussa neljä esitettyjen esimerkkien perusteella.

Selvityksiä tekevä taho olisi tässäkin käsittelijä, koska kukaan ei voi kerätä oma-aloitteisesti tietoja ihmisistä ja ylläpitää rekisterejä heistä ja kyse on toimeksiantajan intressin palvelemisesta (luku 5.5). Joissain tilanteissa voi olla kyse tiedoista, joita hankitaan rekisterinpitäjiltä, jotka luvallisesti ylläpitävät tällaisia rekistereitä (esimerkiksi luottotiedot tai erilaiset ammattipätevyysrekisterit). Silloinkin yksityisetsivä toimii käsittelijänä

työnantajalle toimiessaan lähinnä ulkoa ostettuna työvoimana ja olisi siten käsittelijä (Luku 5.3.5). Työnantajalla on velvollisuus käsitellä YT-menettelyssä työnhakuun liittyvät henkilötietojen käsittelytoimet. Jos ne eivät olisi tiedossa, ei niitä olisi voitu käsitellä YT-menettelyssä. (Luku 5.7) Siten kaikissa selvityksissä työnantaja määrittelee henkilötietojen käsittelyn tarkoitukset ja suurimman osan keinoista.

Työantajalla on velvollisuus hankkia suostumus tietojen hankkimiseksi muualta, koska Työelämän tietosuojalainsäädäntö -luvussa ei tunnistettu mitään muita lainmukaisuusperusteita tätä varten. Käytännössä nämä tiedot voisivat olla todistusten aitoustarkistuksia, luottamustehtävien varmistamista tai edellisten työnantajien haastatteluja siinä määrin kuin niihin on saatu lupa työnhakijalta. Tätä tarkoitusta varten voidaan käyttää myös yksityisetsivää. Koska saaduista tiedoista tulee informoida työnhakijaa viimeistään ennen kuin tietoja käytetään häntä koskevassa päätöksenteossa, tulisi nämä tiedot ja tietojen lähteet olla työnantajan tiedossa. (Luku 5.5).



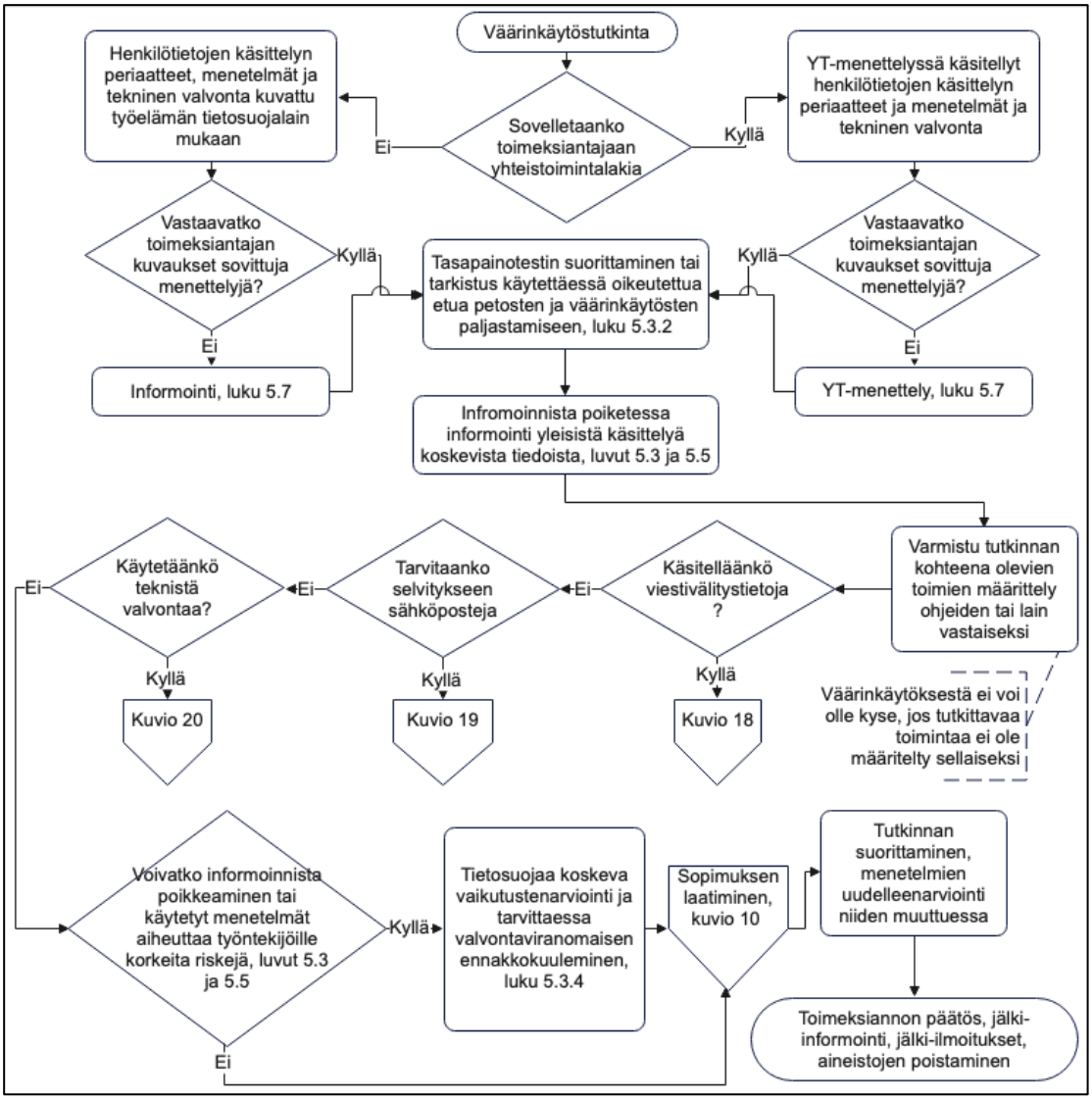
Kuvio 16: Työnhakijan taustaselvitys

Laki yksityisistä turvallisuuspalveluista ei määrittele erityisistä tiedonsaantioikeuksista tai niihin liittyvistä huolehtimis- tai valvontamekanismeista sähköiseen viestivälitykseen tai viestiliikenteeseen liittyen luvanvaraiselle toimijalle. Näiden asioiden sääntelyn on kuitenkin katsottu olevan kansallisessa lainsäädännössä edellytyksenä sille, että rikoksiin tai niiden selvittämiseen liittyviä tietoja voitaisiin pyytää, sen lisäksi, että rikosten tulee olla vakavia ja yksityisyyteen puuttumisen oikeasuhtaista rikosten vakavuuteen nähden. Näitä käsiteltiin perusteluineen tarkemmin luvussa Henkilötietojen käsittelyn ja tietosuojan kansainvälinen tausta ja kansallisen lainsäädännön osalta luvussa Viestintäpalvelulaki. Näiden seikkojen vuoksi yksityisetsivä voi turvautua vain sellaisiin toimivaltuuksiin, joita työantajalla toimeksiantajana on käytettävissään.

Työelämän tietosuojaa ja viestintäpalvelulakia koskevissa luvuissa todettiin henkilötietojen käsittelyyn liittyvän ennakkohuolehtimisvelvoitteita. Siten niitä tulisi työpaikoilla edeltää jo

organisaatiossa tapahtunut valmisteluvaihe. Ennakkohuolehtimisvelvoitteiden hoitaminen varmistaa tarvittavan keinovalikoiman olemassaolon, kun tutkintapäätöstä tehdään. Monet ennalta huolehdittavat asiat voivat viivästyttää tutkintaa ja jopa vaikuttaa sen onnistumiseen. Viestintäpalvelulakiin liittyi myös jälki-ilmoitusvelvollisuus esimerkiksi henkilöstöedustajille ja tietosuojavaltuutetulle. Vaikka nämä toimet ovat pääsääntöisesti organisaation itsensä vastuulla, todettiin sopimusoikeutta koskevassa luvussa yksityisetsivään asiantuntijapalveluita toimittavana kohdistuvan korkeampi vastuu toimeksiantojen lainmukaisuudesta ja asianmukaisuudesta. Siksi tämän luvun esimerkit toimivat muistilistana yksityisetsivälle, mutta myös kenelle tahansa yritykselle sen valmistautuessa väärinkäytöstutkintaan.

Kuviossa 17 on kuvattu tarkemmin väärinkäytöstutkintaan liittyvien asioiden valmistelu. Kuvion yksinkertaistamisen vuoksi kameravalvontaan, sähköpostien avaamiseen ja viestivälitystietojen käsittely on eritelty omiin kuvioihinsa.

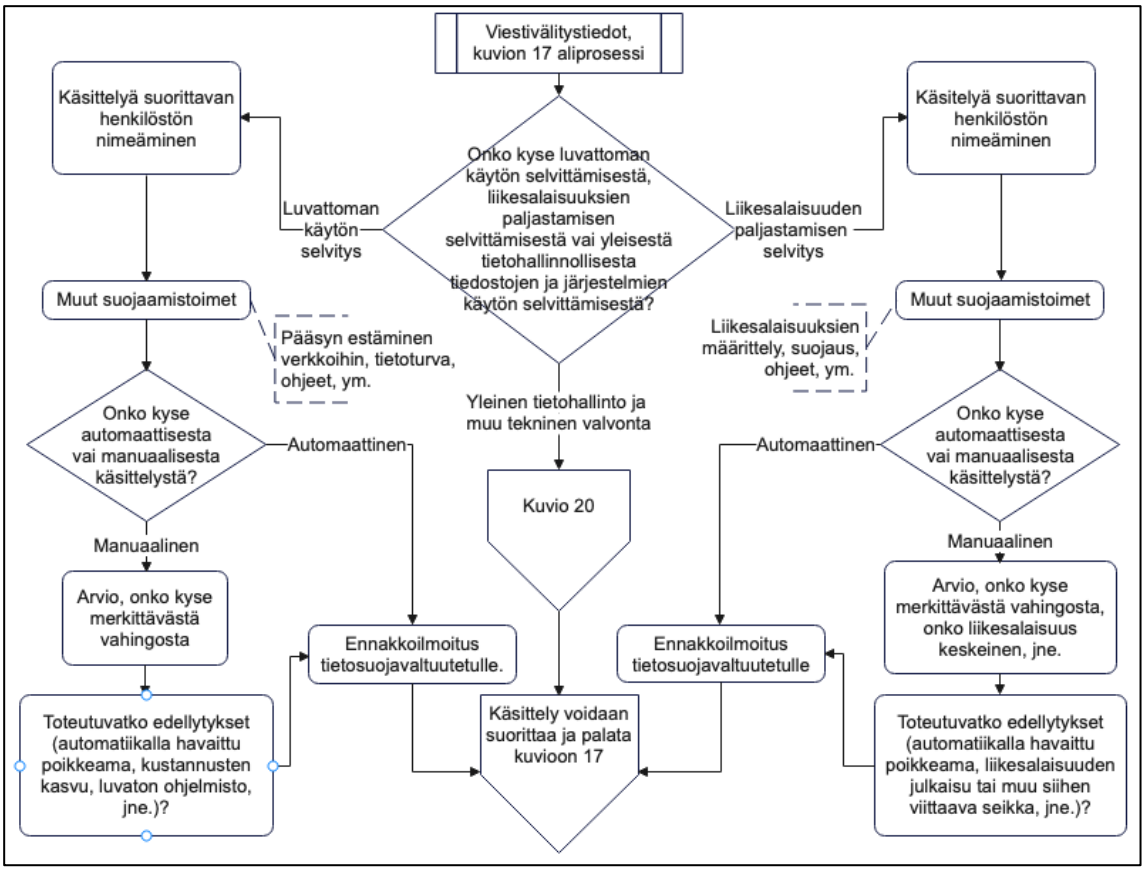


Kuvio 17: Työntekijöihin kohdistuva väärinkäytöstutkinta

Kuviossa 17 sopimuksen laatiminen on sijoitettu loppuun siksi, että ihannetilanteessa siinä kuvatut asiat olisi etukäteen määritelty ja helposti saatavilla jo sopimuksen teon yhteydessä. Jos sopimus tehdään kuitenkin aiemmin, tulee sopimuksella huomioida kuviossa 17 kuvatut menettelyt ja riittävä joustavuus ja vastuut niiden suorittamiseksi. Toimeksiannon loppuessa tulee huomioida muun muassa kuviossa 18 käsiteltyjen viranomaiselle tai henkilöstöedustajille tehtävien vuosi-ilmoitusten hoitaminen.

Koska luvun 5.6.1 tarkoittamat yleiset käsittelyoikeudet liittyvät vain tilanteisiin, joissa yksittäistä käyttäjää ei voida tunnistaa, eivät ne sovellu väärinkäytöstutkintaan rikosoikeudellisen vastuun selvittämiseksi. Väärinkäytöstutkintaan rikoksen paljastamiseksi ja selvittämiseksi soveltuu siten vain luvun 5.6.2 tarkoittamat erityiset oikeudet ja tässä käsitellään vain niitä. Tässä yhteydessä on hyvä huomauttaa vielä edellisten lukujen havainnoista, että itse viestisisältöjä tai selaimen välimuistitietoja ei saa käsitellä. Kannatta huomioida myös se, että koska prosessi on alisteinen kuvion 17 prosessille, tulee näiden aliprosessien osalta huomioida myös YT-menettely ja työelämän tietosuojalaki. Viestivälitystietojen käsittelyn osalta kuvion 10 huomiointi sopimuksen teon yhteydessä on tärkeää rikoksiin liittyen luvussa 5.2 esitettyjen edellytysten mukaan: Käsittelyn tulee olla välttämätöntä ja tapahtua riippumattoman hallinnollisen elimen valvonnassa. Välttämättömyys perustellaan keinoja valitessa kuvion 10 yhteydessä ja viestivälitystietojen käsittelyyn liittyvä valvonta tulee ennakko- ja jälki-ilmoitusten kautta Tietosuojavaltuutetun valvontaan.

Kuviossa on huomioitu myös muu tietotekninen valvonta, mutta kannattaa huomioida sen kuuluvan varsinaisesti kuvioon 20. Kaikki alla olevan kuvion 18 liittyviin kohtiin lisätiedot löytyvät luvusta 5.6.2.



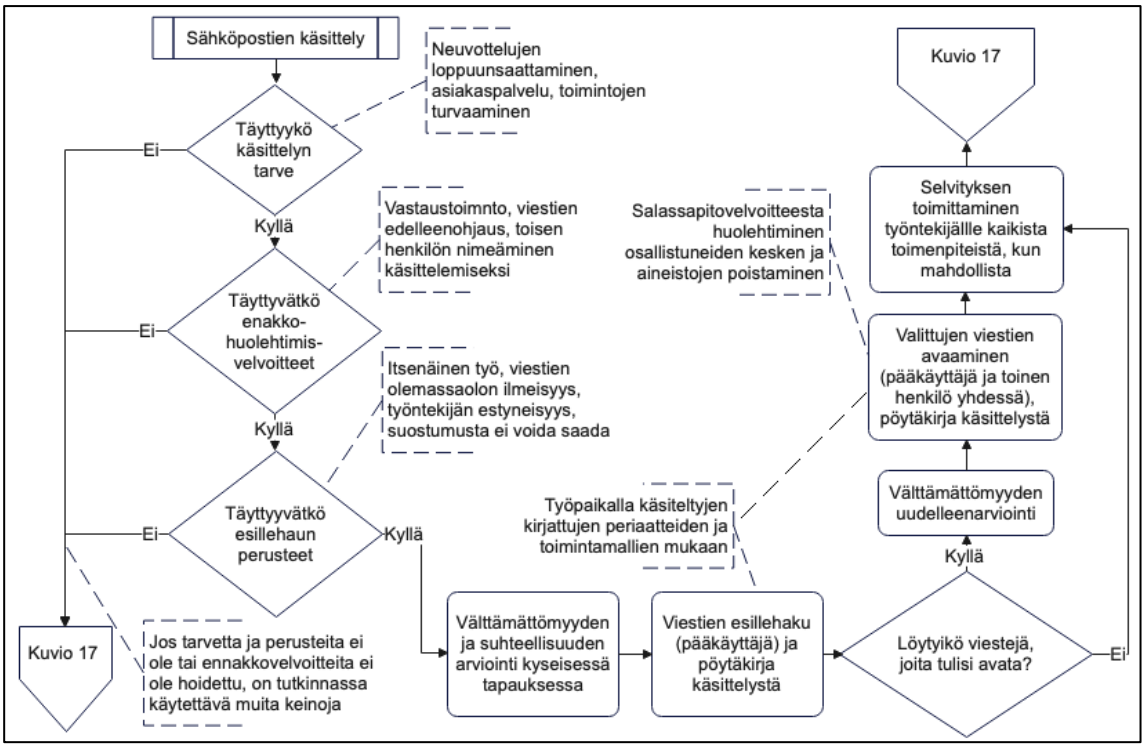
Kuvio 18: Viestivälitystietojen käsittely väärinkäytöstutkinnassa

Kuvion 18 osalta on huomioitava, että viestintäpalvelulaki laajentaa luvussa 5.6 esitetyn perusteella viestinnän luottamuksellisuuteen liittyvän oikeuden myös oikeushenkilöille. Siten esimerkiksi kumppanien ja alihankkijoiden välitystietoja on käsiteltävä luottamuksellisesti, vaikka kyse olisi yleisesti yhtiön liikenteestä verkoissa.

Kuten luvussa 5.7 todettiin, sähköposteja voi hakea esille ja avata, jos se on tarpeen työnantajan neuvottelujen loppuun saattamiseksi, asiakkaiden palvelemiseksi tai toimintojen turvaamiseksi. Tulee muistaa myös se, että väärinkäytöstutkinta ei automaattisesti anna oikeutta sähköpostien esillehakuun tai avaamiseen työelämän tietosuojaa koskevan luvun mukaan. Koska lainsäädäntö ei ole kovin tarkkarajainen siinä, mitä on työnantajan toimintojen turvaaminen, tulee erityisesti huolehtia välttämättömyydestä ja suhteellisuudesta yksityisyydensuojaan nähden. Suostumus ei ole välttämättä pätevä, kun käsitellään heikommassa asemassa olevia rekisteröityjä luvun 5.7 mukaan. Siksi nämä arviot syytä olla tehtynä, vaikka voitaisiin käyttää työntekijän suostumusta.

Kuvio 19 alla kuvaa prosessin sähköpostien käsittelyn osalta. Tämä on myös alisteinen prosessi kuviolle 17, koska käsittelyä suoritetaan väärinkäytöstutkinnan kontekstissa. Siksi kuvion 17 velvoitteet on huomioitava. Esimerkiksi sähköpostin käytön periaatteet on käsiteltävä YT-

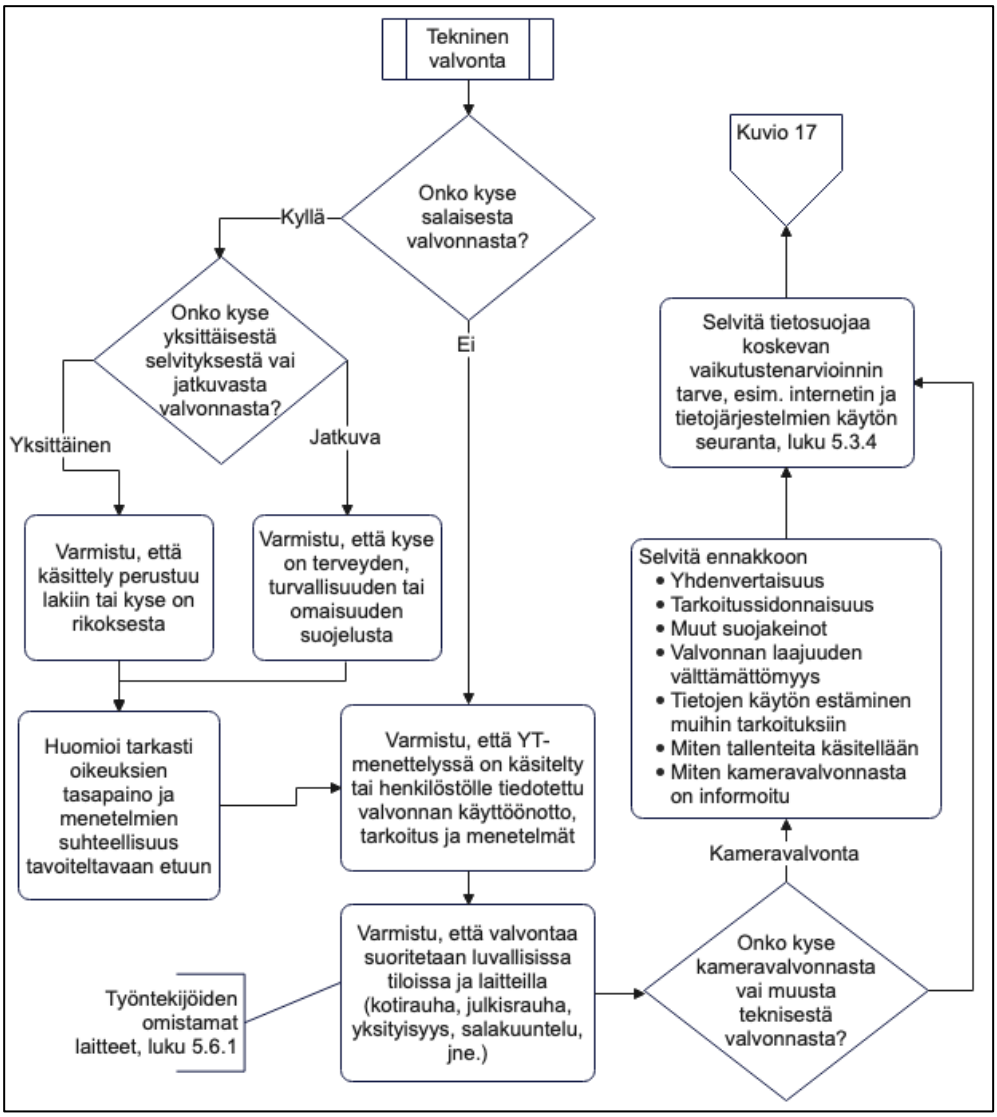
menettelyssä tai viestittävä työntekijöille luvun 5.7 mukaan. Siksi tätä ei ole enää huomioitu tässä kuviossa, koska se huomioidaan jo kuviossa 17.



Kuvio 19: Sähköpostien esillehaku ja avaaminen

Tämän luvun kaavio tulee sovellettavaksi, jos väärinkäytöstutkinnassa käytetään apuna teknistä valvontaa, kuten kulunvalvontaa tai kameravalvontaa. Luvussa 5.7 todettiin, että myös tietotekninen ja tietohallinnollinen valvonta kuuluu tekniseen valvontaan. Samoin esimerkiksi puhelinjärjestelmien tiedot ja tekninen paikantaminen. Teknisen valvonnan käsite on siis laaja. Siksi nämä käsitellään tässä samassa kaaviossa. Luvun 5.7 mukaan myös tämän luvun asiat kuuluvat käsiteltäväksi yhteistoimintamenettelyssä ja tiedotettava työelämän tietosuojalain mukaan ja siksi se on aina alisteinen kuviolle 17. Kaikki kuvioon 20 liittyvät velvoitteet on kuvattu tarkemmin luvussa 5.7, ellei toisin ole mainittu.

Alla esitetty kuvio 20 voi tulla sovellettavaksi väärinkäytöstutkinnassa joko ainoana keinona tai yhdessä tietojärjestelmiin kohdistuvien viestivälitystietojen tutkimisen yhteydessä. Jos kyse on kameravalvonnasta, tulee huomata, että jatkuva seuranta yksittäisen henkilöön kohdistuen ei ole mahdollista ilman muita perusteita, kuten henkilön omaa pyyntöä (luku 3.3). Tämä aliprosessi voi olla alisteinen myös kuviolle 18.



Kuvio 20: Teknisen valvonnan käyttö väärinkäytöstutkinnassa

6.3 Työn riskit ja tulosten epävarmuus

Jo luvussa Rajaukset todettiin, että toimijoihin kohdistuu useita satoja velvoitteita. Työn suurimpana riskinä on jonkin yksittäisen tärkeän velvoitteen unohtaminen tässä käsitellyistä. Tätä riskiä on pyritty välttämään usean lähteen tulkintatilanteissa. Tätä riskiä pienennetään myös lopputuloksen muodolla. Tuottamalla mallit eri velvoitteiden tunnistamiseksi erilaisissa tilanteissa, annetaan toimijoille joustavuutta täydentää tuota mallia milloin tahansa, jos se tunnistaa uusia omaan toimintaan sovellettavia velvoitteita. Työn tavoitteena ei ollut täydellisen oikeusvarmuuden tuottaminen toiminnan lainmukaisuudesta, vaan tukea toiminnan lainmukaisuuden vahvistamista kertomalla, mitä toimijoiden on vähintään huomioitava omassa toiminnassaan.

Liian tarkat ja yksityiskohtaiset mallit voisivat myös muodostaa riskin. Työssä todettiin monessa kohtaa, että monet tekijät ovat tilannesidonnaisia ja velvoitteiden laukeamiseen voi vaikuttaa useampi eri tekijä. Pelkästään lainmukaisuusperusteita voi olla useita yksittäisessä tapauksessa, koska jokainen käsittelytoimi ja erilaiset henkilötietoryhmät voivat vaatia omansa. Näin yksityiskohtaisten mallien luonti olisi työlästä tehdä ja tulkita. Niitä ei myöskään saisi koskaan niin varmoiksi, että ne voisivat huomioida kaikki elävän elämän tilanteet. Tulevaisuutta ei myöskään voi ennustaa esimerkiksi teknologian kehityksessä. Tulevaisuuden teknologiset kyvykkyydet voivat vaikuttaa paljon esimerkiksi teknisen valvonnan suorittamiseen tai oikeasuhtaisuuteen, jolloin harkintavaltaa tulee tilanteisiin jättää. Näin työn tulokset kestävät todennäköisesti myös paremmin aikaa.

Työssä on käytetty myös teleologista laintulkintaa arvioiden joitain tilanteita sen perusteella, mitä lainsäätäjä on saattanut tarkoittaa lakia säätäessään. Näiden osalta tulkinnat perustuvat tässä työssä esitettyihin oikeustapauksiin, lakien perusteluteksteihin ja kirjallisuuden lähteisiin. Koska työn tekijä ei ole suorittanut oikeustieteen opintoja, on olemassa vaara, että käytetyt lähteet ovat suppeita tai puoltavat tiettyä näkökulmaa. Työssä on kuitenkin pyritty haastamaan tiettyjä asioita useamman lähteen käytöllä suuremman varmuuden saamiseksi loppupäätelmistä. Työssä ei väitetä, että tulkinnat itsessään olisivat lopullisia tai oikeita tai toisivat varmaa menestystä esimerkiksi oikeudessa. Niitä ei tule siksi ottaa sellaisenaan lainopillisina neuvoina tai ohjeina. Päätarkoituksena on ollut pysyä toimijoiden ohjaamisessa realistiseen varautumiseen eri tilanteissa.

6.4 Jatkotutkimusaiheet

Lainsäätäjä on poistanut asetuksen yksityisetsivän ammatista, mutta jättämällä rikosten paljastamisen ja selvittämisen lainsäädäntöön, tarkoitus ei ole ilmeisesti ollut poistaa tällaisen toiminnan harjoittamisen mahdollisuutta. Tietosuoja-asetus antaa myös mahdollisuuden esimerkiksi rikoksiin liittyvien tietojen käsittelyyn viranomaisen valvonnassa. Vartioimisliiketoimintaa – samoin kuin asianajo- ja tilintarkastustoimintaa, suoritetaan viranomaisen valvonnassa. Näin voitaisiin nähdä tietosuoja-asetuksen vaatimuksen täyttyvän siitä, että lainsäädännöllä on rikoksiin liittyvien tietojen käsittelystä määritelty ja se tapahtuu viranomaisen valvonnassa. Euroopan tietosuojaneuvosto edellyttää kuitenkin tältä lainsäädännöltä tarkkarajaisuutta ja selkeyttä rekisteröityjen suuntaan myös heidän henkilötietojensa käsittelyssä. Kuten työssä todettiin, ovat monet asiat hajallaan eri laeissa. Avoimeksi jää siis, onko yksityisetsivän toiminnasta tai ylipäätään rikoksen paljastamisesta säädelty Suomessa niin selkeästi, että rekisteröidyille olisi selvää, milloin toimijat voisivat käsitellä esimerkiksi rikoksiin liittyviä tietoja kansallisen lain perusteella. Yksityisetsivätoiminnan rinnastaminen vartiointiin saman toimiluvan alle on myös kyseenalaista, koska tämänkin työn tulosten perusteella toiminta niissä on hyvin erilaista.

Aiemmin mainittiin epärehelliset tai rikolliset toimeksiannot tai rekisteröidyille aiheutuneet vahingot esimerkiksi väärinkäytösten paljastamisessa. On siis selvää, että rekisteröidyt tarvitsevat suojelua henkilötietojensa käsittelyn osalta suojautuakseen käsittelyn negatiivisilta vaikutuksilta heidän oikeuksiaan tai vapauksiaan kohtaan. Laki yksityisistä turvallisuuspalveluista ei määrittele mitään henkilötietojen käsittelyn suojakeinoista tai reunaehdoista rikoksen paljastamisen yhteydessä, muutoin kuin toimenpiteen perusteen ilmoittamisessa käytettäessä voimakeinoja (laki yksityisistä turvallisuuspalveluista 1085/2015, 7 §; HE 22/2014 vp, 33-34). Kyseinen laki ei myöskään koske muuta kuin rikosten paljastamista ja selvittämistä, jolloin muu yksityisetsivätoiminta jää sen ulkopuolelle. Työssä kuitenkin todettiin negatiivisia vaikutuksia olleen myös muussa väärinkäytöstutkinnassa.

Myös järjestäytyneen rikollisuuden on todettu hyödyntävän entistä enemmän yritystoimintaa rikollisuudessa (Rikostorjunnan tila 2018, 25). Samaan aikaan rikollisuus siirtyy tietoverkkoihin. Joidenkin arvioiden mukaan tietoverkoissa toteutetaan jo enemmän rikoksia kuin fyysisessä maailmassa (Rikostorjunnan tila 2018, 28). Valvonnasta huolimatta järjestäytyneen rikollisuuden on tiedetty Suomessa olevan yhteydessä jo yksityisturvapalveluihin (Hietanen 2015, Miljardibisnes Suomessakin: Näille aloille järjestäytynyt rikollisuus on soluttautunut; ja Iltalehti 2010, AL: Ammattirikolliset yrittävät soluttautua vartiointifirmoihin). Euroopassa rikollisuuden soluttautuminen ICT-yrityksiin on myös huomattu (Project Ariel Final report, 31).

Yksi työssä havaittu epävarmuus liittyy myös siihen, milloin yksityisetsivätoiminta on rikosten paljastamiseen liittyen valmistelua ja milloin julkisen vallan käyttöä. Tämä on oikeusvarmuutta horjuttava tekijä myös toimijan näkökulmasta, koska toiminta harmaalla alueella voi olla riski toimijan toimiluvalle tai laajemmin toimijoiden ammattiin kohdistuville mielikuville. Toimijat pääsääntöisesti pyrkivät toimimaan elinkeinonharjoittamisen yhteydessä lainmukaisesti, mistä kertoi muun muassa työssä esiin nostetut eri järjestöjen valmistelemat eettiset ohjeet, lainvalmisteluun osallistuminen ja aktiivinen jäsenistön kouluttaminen. Ammattikunnan tavoite on myös tuoda osaamista ja ammattitaitoa kenen tahansa saataville omien oikeuksiensa suojaamisessa silloin, kun esimerkiksi poliisin tutkintakynnys ei vielä ylity tai viranomaisen palveluita ei vielä ole käytössä. Siten yksityisetsivät lisäävät palveluillaan asiakkaidensa oikeusturvaa.

Turvallisuusalan valvonnan tehostamista ovat halunneet myös turvallisuusalan toimijat itse, kuten selviää vuonna 2012 julkaistusta kyselytutkimuksesta (Paasonen, Ellonen, Sutela 2012, 1224). Vaikka tutkimuksessa olikin kyse turvasuojaustoiminnasta, niin havainto on silti relevantti – turvasuojauksessa usein vasta suunnitellaan toimia ennaltaehkäisyn näkökulmasta, kun taas väärinkäytöstutkinnassa selvitetään jo yksilöihin kohdistuvia epäilyjä ja puututaan sitä kautta yksityisyydensuojaan. Asia on nostettu esiin myös Suomen Yksityisetsivä- ja Lakitoimistoliiton lausunnossa hallituksen esitykseen laiksi yksityisyyden

suojasta työelämässä annetun lain 4 §:n muuttamisesta. (TEM097:00/2020, Asiakirjat: Suomen yksityisetsivä- ja lakitoimistoliiton lausunto, 3-4).

Yksityisetsivät toimivat asiakkaidensa toimeksiannosta henkilötietojen käsittelijöinä. Rekisterinpitäjinä toimivat asiakkaat, omavartiointia suorittaessaan tai itseensä kohdistuvia rikoksia tutkiessaan, eivät kuulu viranomaisvalvonnan tai lupamenettelyn piiriin. Tämä voi johtaa tilanteeseen, jossa rikosten paljastamista tai väärinkäytöstutkintaa voidaan tehdä ilman minkäänlaista kokemusta tai osaamista toiminnasta. Tämä on saanut kritiikkiä siitä, että se jättää valvonnan ulkopuolelle toimijoita, jotka ammattimaisesti puuttuvat ihmisten perusoikeuksiin (Kerttula 2010, 124). Vartijoiden ja omavartiointia suorittavien henkilöiden oikeudet eivät poikkea paljon toisistaan ja ovat hyvin lähellä jokamiehenoikeuksia. Siten voisi nähdä, että omavartiointia tulisi myös säädellä julkisena hallintotehtävänä (Kerttula 2010, 15). Koska toiminta ei vaadi ennakkolupaa, se ei myöskään ole minkään koulutussuunnitelman piirissä, jolloin toimijoiden tuntemus luonnollisten henkilöiden oikeuksista ja vapauksista ei välttämättä ole sellaisella tasolla, joka takaisi laillisen ja oikeasuhtaisen menettelyn.

Vuona 2009 julkaistussa selvityksessä turvallisuusalasta oli kansalaiskyselyssä pohdittu toimivaltuuksien tarpeellisuutta vain perinteisten vartioimistehtävien näkökulmasta. Esimerkiksi toimivaltuuksien tarpeellisuuteen liittyvässä kyselyssä ei ollut eritelty rikosten paljastamista ollenkaan (Heinämäki 2009, 114). Kansalaisten mielipidettä oli kysytty myös siitä näkökulmasta, miten kansalaiset suhtautuisivat esimerkiksi rikosilmoitusten kirjaamiseen yksityisen turvallisuusalan toimijoiden tekemänä. Pääsääntöisesti suhteutuminen oli tähän negatiivista, tehtävää pidettiin vastaajista 54 %:n mukaan huonosti tai erittäin huonosti yksityiselle turvallisuusalalle sopivana (Heinämäki 2009, 116). Myös perinteisesti poliisin tehtäviin kuuluvat sakottaminen ja koti- ja ryöstöhälytystehtävien hoitaminen sai vastustusta vastaajilta (Heinämäki 2009, 120).

Kyselyssä oli kuitenkin kysytty vain yksittäisen tehtävän hoitamisesta. Kysymyksestä ”Mitkä näistä tehtävistä sopisivat mielestäsi tulvaisuudessa pääasiassa yksityisen turvallisuusalan hoidettavaksi?”, voi saada hyvin erilaisen kuvan, kuin mitä yksityisetsivätoiminta on (Heinämäki 2009, 120). Jos vastaaja ajattelisi sen johtavan siihen, että rikosilmoitukset tulisi jättää jatkossa pääasiassa vartioimisliikkeille, on helppo ymmärtää sekä mielipiteen negatiivisuus, mutta myös siihen sisältyvät perustuslailliset ongelmat. Kuten luvussa neljä todettiin, yksityisetsivätoimintaan liittyvät tehtävät ovat enemmän ennen poliisille ilmoittamista tehtäviä selvityksiä tai rikosten selvittämiseen liittyviä lisäselvityksiä. Mielipide olisi ehkä ollut toinen, jos olisi kysytty, haluttaisiinko yksityistä turvallisuusalaa käyttää poliisia täydentävänä vapaaehtoisuuteen perustuvana palveluna. Jos ammattikunta toimisi selkeän kaikkien saatavilla olevan lainsäädännön puitteissa, se voisi osaltaan lisätä luottamusta toimintaan.

Epävarmuustekijät vaikuttavat todennäköisesti myös liiketoiminnan kasvu- ja kehittymismahdollisuuksiin negatiivisesti. Edellisten perusteella yksi jatkotutkimusaiheita voisi olla seuraavat:

1. Tarvitseeko ammattikunta tarkemman kaikkien asianosaisten oikeusvarmuutta lisäävän lainsäädännöllisen kehikon ja millainen se voisi olla?
2. Tarvitseeko koko väärinkäytöstutkinnan ja rikosten paljastamiseen liittyvä toiminta lainsäädännöllisen kehikon riippumatta siitä, tapahtuuko se alihankintana vai niin sanottuna omavartiointina?
3. Voisiko ja miten Euroopan unionin alueella turvallisuuspalveluiden osalta sääntelyä yhdenmukaistaa siten, että näiden palveluiden vapaa liikkuvuus voisi toteutua Unionin alueella?
4. Lainsäädännön monimutkaisuus ja yksityisetsivätoimintaan erikoistuneiden yritysten pieni koko luovat melko suuren hallinnollisen taakan – onko se jopa kohtuuton ja miten sitä voisi keventää?

Pelkkä sääntely ei yksin ratkaise ongelmia, vaan alan toimijoille tulisi saada myös koulutusta. Laajemmat tehtävät ja toimivaltuuden edellyttävät myös perusteellista koulutusta tehtäviin (PeVL 22/2014 vp, 2). Henkilötietojen käsittely yksityisetsivätoiminnassa ei sisälly nykyiseen vartijakortin suorittamiseen (vastaavan hoitajan haastattelu 2021). Pelkästään tähän työhön sisältyvän lainsäädännön laajuuden kautta on helppo ajatella, ettei vartijan 120 tunnin mittainen koulutus voi kovin laajasti sisältääkään sitä muiden vartioimistehtävien ohella (Poliisi 2022, Korttihakemukset, kohta Vartijakortti).

Lähteet

Painetut

Aarnio, A.1997. Oikeussäännösten systematisointi ja tulkinta. kirjassa Minun metodini. toim. Juha Häyhä. Porvoo: WSOY.

Björne, L. 1986. Oikeusjärjestelmän kehityksestä. 2. uudistettu painos. Helsinki: Lakimiesliiton kustannus sekä Lars Björne.

Carey, P. 2015. Data Protection. A Practical Guide to UK and EU Law. 4. painos. Oxford: Oxford University Press.

Frände, D. 2005. Yleinen rikosoikeus. Helsinki: Edita.

Frände, D. & Wahlberg, M. 2018a. Julkisrauhan rikkominen. Teoksessa Frände, D., Matikkala, J., Tapani, J., Tolvanen, M., Viljanen, P., Wahlberg, M. Keskeiset rikokset. Keuruu: Otavan Kirjapaino Oy, 386-392.

Frände, D. & Wahlberg, M. 2018b. Kameravalvonnan rikosoikeudellinen sääntely. Teoksessa Frände, D., Matikkala, J., Tapani, J., Tolvanen, M., Viljanen, P., Wahlberg, M. Keskeiset rikokset. Keuruu: Otavan Kirjapaino Oy, 416-427.

Frände, D. & Wahlberg, M. 2018c. Salakuuntelu ja salakatselu. Teoksessa Frände, D., Matikkala, J., Tapani, J., Tolvanen, M., Viljanen, P., Wahlberg, M. Keskeiset rikokset. Keuruu: Otavan Kirjapaino Oy. 397-415.

Frände, D. & Wahlberg, M. 2018d. Voimassa oleva RL 24:1. Teoksessa Frände, D., Matikkala, J., Tapani, J., Tolvanen, M., Viljanen, P., Wahlberg, M. Keskeiset rikokset. Keuruu: Otavan Kirjapaino Oy, 370-384.

Heinämäki, A-K. 2009. Yksityinen turvallisuusala turvallisuuspalvelujen tuottajana. Selvitystyö yksityisen turvallisuusalan toimijoista, toimivaltuuksista ja toimintaympäristöstä. Poliisin ylijohdon julkaisusarja 8/2009. Sisäasiainministeriö.

Keravuori–Rusanen, M. 2008. Yksityinen julkisen vallan käyttäjänä: Valtiosääntöoikeudellinen tutkimus julkisen hallintotehtävän antamisesta muulle kuin viranomaiselle. Helsinki: Edita Prima Oy.

Kiikeri, M., Ylikoski, P. 2004. Tiede tutkimuskohteena: Filosofinen johdatus tieteentutkimukseen. Tampere: Gaudeamus.

Kuner, C., Bygrave, L., A., Docksey, C. 2020. The EU General Data Protection Regulation (GDPR) – A Commentary. Iso-Britannia: Oxford University Press.

Kurenmaa, T. 2018. Rikostorjunnan tila -selvityshankkeen loppuraportti. Poliisihallituksen julkaisusarja 1/2018. Poliisihallitus.

Laitinen, A., Aromaa, K. 2005. Rikollisuus ja kriminologia. Tampere: Vastapaino 2005.

Nyyssölä, M. 2020. Yksityisyyden suoja työsuhteessa. 9. uudistettu painos. Liettua: BALTO print.

Ojasalo, K., Moilanen, T., Ritalahti, J. 2018. Kehittämistyön menetelmät. Uudenlaista osaamista liiketoimintaan. Sanoma Pro Oy: Helsinki.

Paasonen, J. 2008. Yksityisen turvallisuusalan sääntely, Rikosoikeudellinen vastuu ja toimivaltuudet. Porvoo: Tietosanoma

Prenzler, T. 2006. Private Investigators. Teoksessa Gill, M. The Handbook of Security. 2006. Iso-Britannia: Palgrave Macmillan.

Susi, P. 2021. Yksityisetsivä, varjo kannoillasi. Docendo Oy. Liettua: Scandbook UAB.

Tikkanen, S., Aapio, L., Kaarnalehto, A., Kammonen, L., Laitinen, J., Mikkonen, J., Pisto, M.H. 2017. Ammattina turvallisuus. 3. uudistettu painos. Helsinki: Sanoma Pro

Ustaran, E. 2018. European Data Protection, Law and Practice. Portsmouth, USA: International Association of Privacy Professionals

Sähköiset

2/936/2005. Tietosuojavaltuutettu. 2006. Henkilötieto - Arkaluonteinen henkilötieto. Viitattu 1.10.2021. https://www.finlex.fi/fi/viranomaiset/ftie/2006/20060001

2477/161/21. Tietosuojavaltuutettu. 2021. Rekisteröidyn yleisen tietosuoja-asetuksen mukaiset oikeudet ym. ParkkiPate Oy. Viitattu 1.11.2021. https://tietosuoja.fi/documents/6927448/58640544/Seuraamuskollegion+p%C3%A4%C3%A4t%C3%B6s_henkil%C3%B6tietojen+k%C3%A4sittely+pys%C3%A4k%C3%B6inninvalvontamaksujen+yhteydess%C3%A4.pdf/9b105604-51e0-7beb-e21b-df1b504843e6/Seuraamuskollegion+p%C3%A4%C3%A4t%C3%B6s_henkil%C3%B6tietojen+k%C3%A4sittely+pys%C3%A4k%C3%B6inninvalvontamaksujen+yhteydess%C3%A4.pdf?t=1619763172841

2890/161/2021. Tietosuojavaltuutetun toimisto. 2021. Sähköinen suoramarkkinointi automatisoiduilla soittojärjestelmillä ja henkilötietojen käsittelysopimus. Viitattu 1.10.2021. https://finlex.fi/fi/viranomaiset/tsv/2021/20210863

3021/452/2017. Tietosuojavaltuutettu. 2017. Informointi asiakaspuheluiden tallentamisesta ja rekisteröidyn oikeus saada pääsy tietoihin. Viitattu 1.11.2021. https://finlex.fi/fi/viranomaiset/tsv/2020/20200501

3048/41/2015. Tietosuojavaltuutettu. Rikosrekisteritietojen tarkastaminen työelämässä. Viitattu 1.10.2021. https://finlex.fi/fi/viranomaiset/tsv/2015/20150187

3343/163/20. Tietosuojavaltuutettu. 2020. Rekisteröidyn oikeus saada pääsy tietoihin ja informoiminen keskusteluiden tallentamisesta. Viitattu 1.11.2021. https://www.finlex.fi/fi/viranomaiset/tsv/2021/20210763

344/45/2000. Tietosuojavaltuutettu. 2000. Ajoneuvon rekisterinumero, henkilötietolain mukainen päätös 344/45/2000. Viitattu 8.10.2021. https://www.finlex.fi/fi/viranomaiset/tsv/2000/20000041

3592/152/2019. Tietosuojavaltuutettu. 2021. Yksityisen elinkeinonharjoittajan oikeus tutustua tietoihin puhelutallenteen osalta ja annettavien tietojen muoto. Dnro: 3592/152/2019. Viitattu 1.11.2021. https://finlex.fi/fi/viranomaiset/tsv/2021/20211123

3818/161/2020. Tietosuojavaltuutettu. 2020. Henkilötietojen käsittelyn läpinäkyvyys ja rekisteröidylle toimitettavat tiedot silloin, kun henkilötietoja kerätään rekisteröidyltä itseltään. Viitattu 1.10.2021. https://tietosuoja.fi/documents/6927448/22406974/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf/b869b7ba-1a05-572e-d97a-

9c8a56998fc1/Henkil%C3%B6tietojen+k%C3%A4sittelyn+l%C3%A4pin%C3%A4kyvyys+ja+rekister%C3%B6idylle+toimitettavat+tiedot.pdf

3843/163/20. Tietosuojavaltuutettu. 2021. Työntekijän sijaintiin liittyvien henkilötietojen käsittely työajanseurannassa. Dnro: 3843/163/20. Viitattu 1.10.2021. https://finlex.fi/fi/viranomaiset/tsv/2021/20210943

4282/161/21. Tietosuojavaltuutettu. 2021. Käsittelyn turvallisuus, eheyden ja luottamuksellisuuden periaate,

sisäänrakennettu ja oletusarvoinen tietosuoja, oikeus tietojen poistamiseen. Viitattu 1.10.2021. https://tietosuoja.fi/documents/6927448/0/TSV+P%C3%A4%C3%A4t%C3%B6s+4282.161.21.pdf/8679d1a1-c3ae-a820-143c-5ae0cabfc6ff/TSV+P%C3%A4%C3%A4t%C3%B6s+4282.161.21.pdf?t=1643272760189

531/161/20. Tietosuojavaltuutettu. 2020. Työntekijöiden sijaintitietojen käsittely ja vaikutustenarviointi. Dnro 531/161/20. Tietosuojavaltuutetun ja seuraamuskollegion päätökset. Viitattu 1.11.2021. https://tietosuoja.fi/documents/6927448/22406974/Ty%C3%B6ntekij%C3%B6iden+sijaintitietojen+k%C3%A4sittely+ja+vaikutustenarviointi.pdf/2d04e545-d427-8a0d-3f4d-967de7b428ac/Ty%C3%B6ntekij%C3%B6iden+sijaintitietojen+k%C3%A4sittely+ja+vaikutustenarviointi.pdf?t=1590147001000

5417/163/20. Tietosuojavaltuutettu. 2020. Asiakkaiden henkilötietojen kerääminen asiakkaita tarkkailemalla. Päätös 5417/163/20. Viitattu 8.10.2021. https://finlex.fi/fi/viranomaiset/tsv/2021/20210963

6689/186/20. Tietosuojavaltuutettu. 2021. Rikostaustan selvittämiseen liittyvien henkilötietojen käsittely lasten tukihenkilötoiminnan yhteydessä, EU:n yleisen tietosuoja-asetuksen mukainen päätös 6689/186/20. Viitattu 8.10.2021. https://www.finlex.fi/fi/viranomaiset/tsv/2020/20200703työ

8393/161/2019. 2020. Tietosuojavaltuutettu. Apulaistietosuojavaltuutetun ja seuraamuskollegion päätökset. Viitattu 1.10.2021. https://tietosuoja.fi/documents/6927448/22406974/P%C3%A4%C3%A4t%C3%B6s+henkil%C3%B6tietojen+k%C3%A4sittelyn+lainmukaisuudesta/60115710-2513-a359-6261-e821818b9ee1/P%C3%A4%C3%A4t%C3%B6s+henkil%C3%B6tietojen+k%C3%A4sittelyn+lainmukaisuudesta.pdf

Aamulehti. 2020. Benjamin Särkkä ja muut suomalaiset valkohattuhakkerit selvittävät, millaisia jälkiä Vastaamo-tietomurron kiristäjä jätti itsestään verkkoon. Viitattu 1.10.2021. https://www.aamulehti.fi/uutiset/art-2000007439849.html

AEPD. 2022. Expediente Nº: PS/00267/2020. Viitattu 15.2.2022. https://www.aepd.es/es/documento/ps-00267-2020.pdf

Apulaisoikeuskansleri. 2021. Julkisen vallan käyttöön liittyvien tehtävien ulkoistaminen lastensuojelussa. Päätös OKV/292/10/2020. Viitattu 1.11.2021: https://www.okv.fi/media/filer_public/4a/ea/4aea3cba-2026-464d-8b5b-d0f62b23fe0a/ratkaisu_julkisen_vallan_kayttoon_liittyvien_tehtavien_ulkoistaminen_lastensuojelussa_okv_292_10_2020.pdf

Asetus yksityisetsivän ammatista. 112./1944. Viitattu 1.10.2021. https://www.finlex.fi/fi/laki/alkup/1944/19440112

Autoriteit Persoongegevens. 2015. Ontwerpbesluit inzake de verklaring omtrent de rechtmatigheid van de verwerking pre-employment screening van Adecco Group Nederland;

z2015-00062. Viitattu 1.11.2021.
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/ontwerpbesluit_adecco.pdf

C-131/12. 2014. Unionin tuomioistuin. Henkilötiedot – Yksilöiden suojelu henkilötietojen käsittelyssä – Direktiivi 95/46/EY – 2, 4, 12 ja 14 artikla – Asiallinen ja alueellinen soveltamisala – Internethakukoneet – Internetsivustoilla olevien tietojen käsittely – Kyseisten tietojen hakeminen, indeksointi ja tallentaminen – Hakukoneen ylläpitäjän vastuu – Jäsenvaltion alueella sijaitseva toimipaikka – Hakukoneen ylläpitäjän velvollisuuksien ja rekisteröidyn oikeuksien ulottuvuus – Euroopan unionin perusoikeuskirja – 7 ja 8 artikla. Viitattu 1.10.2021. https://curia.europa.eu/juris/liste.jsf?num=C-131/12

C-201/14. 2015. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Direktiivi 95/46/EY – Henkilötietojen käsittely – 10 ja 11 artikla – Rekisteröityjen informointi – 13 artikla – Poikkeukset ja rajoitukset – Se, että jäsenvaltion viranomainen siirtää henkilökohtaisia verotietoja niiden käsittelemiseksi toisessa viranomaisessa. Viitattu 1.11.2021. https://curia.europa.eu/juris/liste.jsf?num=C-201/14

C-207/16. 2018. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Sähköinen viestintä – Henkilötietojen käsittely – Direktiivi 2002/58/EY – 1 ja 3 artikla – Soveltamisala – Sähköisen viestinnän luottamuksellisuus – Suoja – 5 artikla ja 15 artiklan 1 kohta – Euroopan unionin perusoikeuskirja – 7 ja 8 artikla – Sähköisten viestintäpalvelujen tarjoamisen yhteydessä käsitellyt tiedot – Kansallisten viranomaisten oikeus saada tietoja tutkintaa varten – Rikoksen vakavuusaste, joka oikeuttaa tietojensaannin. Viitattu 1.11.2021. https://curia.europa.eu/juris/liste.jsf?num=C-207/16

C-210/16. 2018. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Direktiivi 95/46/EY – Henkilötiedot – Luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä – Määräys, joka koskee sellaisen Facebook-sivun (fan page) poistamista käytöstä, joka mahdollistaa kyseisellä sivulla kävijöihin liittyvien tiettyjen tietojen keräämisen ja käsittelyn – 2 artiklan d alakohta – Henkilötietojen käsittelystä vastuussa oleva taho – 4 artikla – Sovellettava kansallinen oikeus – 28 artikla – Kansalliset valvontaviranomaiset – Mainittujen viranomaisten toimintavaltuudet. ECLI:EU:C:2018:388. Viitattu 1.11.2021. https://eur-lex.europa.eu/legal-content/fi/TXT/?uri=CELEX:62016CJ0210

C-212/13. 2014. Unionin Tuomioistuin. Ennakkoratkaisupyyntö – Direktiivi 95/46/EY – Yksilöiden suojelu – Henkilötietojen käsittely – Yksinomaan henkilökohtaisen tai kotitaloutta koskevan toiminnan käsite. Viitattu 8.10.2021. https://curia.europa.eu/juris/liste.jsf?num=C-212/13

C-25/17. 2018. Unionin Tuomioistuin. Ennakkoratkaisupyyntö – Yksilöiden suojelu henkilötietojen käsittelyssä – Direktiivi 95/46/EY – Kyseisen direktiivin soveltamisala – 3 artikla – Henkilötietojen kerääminen, jonka uskonnollisen yhdyskunnan jäsenet suorittavat ovelta ovelle -saarnaamistyönsä yhteydessä – 2 artiklan c alakohta – Henkilötietojen rekisteröintijärjestelmän käsite – 2 artiklan d alakohta – Rekisterinpitäjän käsite – Euroopan unionin perusoikeuskirjan 10 artiklan 1 kohta. Viitattu 1.11.2021. https://curia.europa.eu/juris/documents.jsf?num=C-25/17

C-40/17. 2019. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä – Direktiivi 95/46/EY – 2 artiklan d alakohta – Rekisterinpitäjän käsite – Verkkosivuston ylläpitäjä, joka on sisällyttänyt sivustolle yhteisöliitännäisen, jolla voidaan välittää kyseisellä sivustolla kävijän henkilötietoja mainitun liitännäisen tarjoajalle – 7 artiklan f alakohta – Tietojenkäsittelyn laillisuus – Verkkosivuston ylläpitäjän vai yhteisöliitännäisen tarjoajan intressin huomioon ottaminen – 2 artiklan h alakohta ja 7 artiklan a alakohta – Rekisteröidyn suostumus – 10 artikla – Rekisteröidyn informointi – Kansallinen säännöstö, jossa sallitaan kuluttajansuojayhdistysten nostaa kanne. Viitattu 6.11.2021. https://curia.europa.eu/juris/liste.jsf?num=C-40/17

C-434/16. 2017. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Yksilöiden suojelu henkilötietojen käsittelyssä – Direktiivi 95/46/EY – 2 artiklan a alakohta – Henkilötietojen käsite – Ammatilliseen kokeeseen osallistujan laatimat kirjalliset vastaukset – Tarkastajan näitä vastauksia koskevat merkinnät – 12 artiklan a ja b alakohta – Rekisteröidyn tietojen saantia ja tietojen oikaisua koskevien oikeuksien laajuus. Viitattu 1.11.2021. https://curia.europa.eu/juris/documents.jsf?num=C-434/16

C-524/06. 2008. Unionin tuomioistuin. Henkilötietojen suojaaminen – Euroopan unionin kansalaisuus – Kansalaisuuden perusteella tapahtuvan syrjinnän kiellon periaate – Direktiivi 95/46/EY – Tarpeellisuuden käsite – Sellaisten unionin kansalaisten, jotka ovat toisen jäsenvaltion kansalaisia, henkilötietojen yleinen käsittely – Ulkomaalaisista pidettävä keskusrekisteri. Viitattu 1.11.2021. https://curia.europa.eu/juris/document/document.jsf?text=&docid=76077&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=34740453

C-582/14. 2016. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Henkilötietojen käsittely – Direktiivi 95/46/EY – 2 artiklan a alakohta – 7 artiklan f alakohta – Henkilötietojen käsite – Internetprotokollaosoitteet – Tallentaminen verkkomediapalvelujen tarjoajan toimesta – Kansallinen säännöstö, jonka mukaan rekisterinpitäjän oikeutettua intressiä ei voida ottaa huomioon. Viitattu 2.11.2021. https://curia.europa.eu/juris/document/document.jsf?docid=184668&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FI&cid=33740710

C-597/19. 2021. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Immateriaalioikeus – Tekijänoikeus ja lähioikeudet – Direktiivi 2001/29/EY – 3 artiklan 1 ja 2 kohta – Yleisön saataviin saattamisen käsite – Suojatun teoksen sisältävän tiedoston lataaminen vertaisverkosta (peer-to-peer-verkko) ja kyseisen tiedoston osien saattaminen samanaikaisesti saataviin niiden verkkoon lataamista varten – Direktiivi 2004/48/EY – 3 artiklan 2 kohta – Toimenpiteiden, menettelyjen ja oikeussuojakeinojen väärinkäyttö – 4 artikla – Henkilöt, joilla on oikeus pyytää toimenpiteiden, menettelyjen ja oikeussuojakeinojen soveltamista – 8 artikla – Tiedonsaantioikeus – 13 artikla – Vahingon käsite – Asetus (EU) 2016/679 – 6 artiklan 1 kohdan ensimmäisen alakohdan f alakohta – Luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä – Käsittelyn lainmukaisuus – Direktiivi 2002/58/EY – 15 artiklan 1 kohta – Lainsäädännölliset toimenpiteet, joilla rajoitetaan oikeuksien ja velvollisuuksien ulottuvuutta – Perusoikeudet – Euroopan unionin perusoikeuskirjan 7 ja 8 artikla, 17 artiklan 2 kohta ja 47 artiklan ensimmäinen kohta. Viitattu 8.10.2021. https://curia.europa.eu/juris/liste.jsf?num=C-597/19

C-673/17. 2019. Unionin tuomioistuin. Ennakkoratkaisupyyntö – Direktiivi 95/46/EY – Direktiivi 2002/58/EY – Asetus (EU) 2016/679 – Henkilötietojen käsittely ja yksityisyyden suoja sähköisen viestinnän alalla – Evästeet – Rekisteröidyn suostumuksen käsite – Suostumuksen antaminen valmiiksi rastitetulla ruudulla. Viitattu 1.11.2021. https://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=34725869

CMS. 2020. GDPR Enforcement Tracker. Viitattu 18.1.2022. https://www.enforcementtracker.com/

CNIL. 2021. The open source PIA software helps to carry out data protection impact assessment. Commission Nationale de l'Informatique et des Libertés. Viitattu 24.1.2021. https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

CoESS. 2013. Private Security services in Europe. CoESS Facts & Figures. Confederation of European Security Services. Viitattu 24.8.2021. https://www.coess.org/download.php?down=Li9kb2N1bWVudHMvZmYtMjAxMy1wcml2YXRlLXNlY3VyaXR5LXNlcnZpY2VzLWluLWV1cm9wZS1jb2Vzcy1mYWN0cy1hbmQtZmlndXJlcy5wZGY.

CoESS. 2021. Members. Confederation of European Security Services. Viitattu 24.8.2021. https://coess.org/about.php?page=members

Costa v. ENEL. 1964. Yhteisöjen tuomioistuimen tuomio 15 päivänä heinäkuuta 1964. - Flaminio Costa v. ENEL. - Giudice Conciliatore di Milanon esittämä ennakkoratkaisupyyntö. - Asia 6/64. ECLI:EU:C:1964:66. Viitattu 1.10.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A61964CJ0006

Dataguidance. 2022. Spain: AEPD fines Amazon Road Transport €2M for unlawful processing of criminal conviction data. Viitattu 15.2.2022. https://www.dataguidance.com/news/spain-aepd-fines-amazon-road-transport-2m-unlawful

Digi- ja väestötietovirasto. 2022. Jos läheinen katoaa. Viitattu 1.1.2022. https://www.suomi.fi/kansalaiselle/oikeudet-ja-velvollisuudet/turvallisuus-ja-jarjestys/opas/nain-toimit-hatatilanteissa/jos-laheinen-katoaa

ECHR 1725. 2010. Karin KOPKE v Germany - 420/07. Viitattu 1.11.2021. https://www.bailii.org/eu/cases/ECHR/2010/1725.html

Edilex uutinen. 2008. Yksityistä turvallisuusalaa koskeva lainsäädäntö uudistetaan. Viitattu 1.10.2021. https://www.edilex.fi/uutiset/18955

Edilex uutinen. 2009. Yksityistä turva-alaa koskeviin uudistusesityksiin voi ottaa kantaa. Viitattu 1.10.2021. https://www.edilex.fi/uutiset/21681

EDPB-EDPS. 2019. EDPB-EDPS Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection. Viitattu 1.11.2021. https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en

EDPB. 2010. Organisaatio. Euroopan unioniin virallinen verkkosivusto. Viitattu 1.10.2021. https://edpb.europa.eu/about-edpb/about-edpb/who-we-are_fi

EDPB. 2019. Ohjeet 2/2019 yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdan perusteella tapahtuvasta henkilötietojen käsittelystä rekisteröidyille tarjottavien verkkopalvelujen yhteydessä. Versio 2.0. Viitattu 1.11.2021. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22019-processing-personal-data-under-article-61b_fi

EDPB. 2018a. Endorsement 1/2018. Euroopan unionin virallinen verkkosivusto. Viitattu 1.10.2021. https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en

EDPB. 2018b. Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679. Adopted on 25 May 2018. Viitattu 1.1.2022. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf

EDPB. 2019. Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities Adopted on 12 March 2019. Viitattu 10.10.2021. https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en

EDPB. 2020a, Guidelines 07/2020 on the concepts of controller and processor in the GDPR, Version 1.0. Adopted on 02 September 2020. Viitattu 1.10.2020. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

EDPB. 2020b. Asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat 05/2020. Versio 1.1. Viitattu 1.11.2021. https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_fi.pdf

EDPB. 2020c. Suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista. Annettu 10. marraskuuta 2020. Viitattu 1.1.2022. https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_fi.pdf

EDPB. 2020d. Usein esitettyjä kysymyksiä, jotka koskevat Euroopan unionin tuomioistuimen tuomiota asiassa C-311/18 – Data Protection Commissioner vastaan Facebook Ireland Ltd ja Maximillian Schrems. Annettu 23. heinäkuuta 2020. Viitattu 1.1.2022. https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_fi.pdf

EDPB 2020e. Suositukset 2/2020 tiedustelua koskevista eurooppalaisista olennaisista takeista. Annettu 10. marraskuuta 2020. Viitattu 1.1.2022. https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_fi.pdf

EDPB. 2021a. Guidelines 07/2020 on the concepts of controller and processor in the GDPR. Viitattu 1.10.2021. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_en

EDPB. 2021b. Guidelines 10/2020 on restrictions under Article 23 GDPR. Version 2.0. Viitattu 1.11.2021. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-102020-restrictions-under-article-23-gdpr_en

EDPB. 2021c. Guidelines 01/2021 on Examples regarding Data Breach Notification. Adopted on 14 January 2021. Version 1.0. Viitattu 10.11.2021. https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

EDPB. 2021d. Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR. Viitattu 1.1.2022. https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

EDPB. 2021e. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. Version 2.0. Adopted on 18 June 2021. Viitattu 1.1.2022. https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf

EDPB. 2022. Code of conduct. Viitattu 1.1.2022. https://edpb.europa.eu/our-work-tools/our-documents/topic/code-conduct_en

EDPS. 2022. About. The European Data Protection Supervisor. Viitattu 1.1.2022. https://edps.europa.eu/about-edps_en

EIT 14.9.2010. Euroopan ihmisoikeustuomioistuin. 2010. Sanoma Uitgevers B.V.-tapaus (suuri jaosto) - Sananvapaus - Lähdesuoja – Laillisuusperiaate. Viitattu 1.11.2021. https://www.finlex.fi/fi/oikeus/eurooppa/feit/2010/20104120

Esitutkintalaki 805/2011. Viitattu 8.10.2021. https://www.finlex.fi/fi/laki/ajantasa/2011/20110805

Etelä-Savon turvamiehet. 2021. Turvallisuuspalvelut ja vartiointipalvelut. Viitattu 24.8.2021. https://www.esturvamiehet.com/news/turvallisuuspalvelut-ja-vartiointipalvelut/

Etsiväpalvelu Paananen. 2021. Etsiväpalvelut yrityksille. Viitattu 24.8.2021. https://www.etsivapalvelupaananen.fi/etsivapalvelut-yrityksille

Euroopan komissio. 2021a. Proposal for an ePrivacy Regulation. Viitattu 10.9.2021. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation

Euroopan komissio. 2021b. What constitutes data processing, 2021, Euroopan komissio, noudettu 8.10.2021: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

Euroopan komissio. 2021c. International transfers of personal data. 2021. Euroopan komissio. Viitattu 1.10.2021. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en

Euroopan komissio, 2021d, Mikä on rekisterinpitäjä tai tietojen käsittelijä?, noudettu 1.11.2021: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fi

Euroopan komissio. 2021e. Adequacy Decisions. Viitattu 19.12.2021. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

Euroopan neuvosto. 2021. Confidentiality of electronic communications: Council agrees its position on ePrivacy rules 2021. Viitattu 13.8.2021. https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/

Euroopan parlamentin ja neuvoston asetus 1215/2012. Tuomioistuimen toimivalta eri EU-maita koskevissa oikeustapauksissa. Viitattu 10.8.2021. https://eur-lex.europa.eu/legal-content/fi/LSU/?uri=CELEX%3A32012R1215

Euroopan unioni. 2021. Court of Justice of the European Union (CJEU). Euroopan unionin verkkosivusto. Viitattu 1.10.2021. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/court-justice-european-union-cjeu_en

Euroopan unionin virallinen lehti. 2016. C 202. 59. vuosikerta. Viitattu 1.10.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=OJ:C:2016:202:TOC

F-Secure. 2020. Vulnerability reward program. Viitattu 1.9.2021. https://www.f-secure.com/en/business/programs/vulnerability-reward-program

Finnsecurity ry. 2020. Tietoa toimialasta. Viitattu 25.8.2021. https://www.finnsecurity.fi/ajankohtaista/tietoa-toimialasta

Gottschalk, P. 2017. When private internal investigators turn against the whistleblower: The case of Norwegian police. International Journal of Police Science & Management. 2017;19(4). 229-237. Viitattu 8.10.2021. https://journals.sagepub.com/doi/abs/10.1177/1461355717730835

Halford v. The United Kingdom. 1997. Case of Halford v. The United Kingdom. (Application no. 20605/92). Judgement. European Court of Human Rights. Viitattu 1.8.2021. https://hudoc.echr.coe.int/eng#{%22appno%22:[%2220605/92%22]}

Hautamäki, T. 2016. Yksityisen turvallisuusalan valvonta. Väitöskirja. Acta Wasaensia 360. Vaasan yliopisto. Viitattu 24.8.2021. https://osuva.uwasa.fi/handle/10024/7317

HE 1/1998 vp. Hallituksen esitys Eduskunnalle uudeksi Suomen Hallitusmuodoksi HE 1/1998 vp. Viitattu 10.8.2021.
https://www.eduskunta.fi/fi/vaski/hallituksenesitys/documents/he_1+1998.pdf

HE 69/2001 vp. Hallituksen esitys Eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi. Viitattu 1.10.2021.
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_69+2001.pdf

HE 125/2003 vp. Hallituksen esitys Eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi. Viitattu 8.10.2021.
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_125+2003.pdf

HE 159/2021 vp. 2021. Hallituksen esitys eduskunnalle yhteistoimintalaiksi ja siihen liittyviksi laeiksi. Viitattu 1.11.2021.
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_159+2021.pdf

HE 162/2003 vp. 2003. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta. Viitattu 1.11.2021.
https://www.edilex.fi/he/fi20030162.pdf

HE 169/2003 vp. 2003. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiden siihen liittyvien lakien muuttamisesta. Viitattu 1.11.2021.
https://www.edilex.fi/he/fi20030162.pdf

HE 22/1990 vp. Hallituksen esitys Eduskunnalle ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen ja siihen liittyvien lisäpöytäkirjojen eräiden määräysten hyväksymisestä. Viitattu 8.10.2021.
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_22+1990.pdf

HE 22/2014 vp. Hallituksen esitys eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi. Viitattu 8.10.2021.
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_22+2014.pdf

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta. Viitattu 10.10.2021. https://www.edilex.fi/he/fi20130221.pdf

HE 235/2010 vp. Hallituksen esitys Eduskunnalle laeiksi tekijänoikeuslain 60 a §:n ja sähköisen viestinnän tietosuojalain muuttamisesta. Viitattu 1.1.2021.
https://www.finlex.fi/fi/esitykset/he/2010/20100235.pdf

HE 239/2009 vp. Hallituksen esitys Eduskunnalle laeiksi järjestyslain 22 §:n, järjestyksenvalvojista annetun lain ja yksityisistä turvallisuuspalveluista annetun lain muuttamisesta. Viitattu 1.10.2021. https://www.finlex.fi/fi/esitykset/he/2009/20090239.pdf

HE 254/2006 vp. 2006. Hallituksen esitys Eduskunnalle laiksi yhteistoiminnasta yrityksissä ja eräiksi siihen liittyviksi laeiksi. Viitattu 1.11.2021.
https://www.finlex.fi/fi/esitykset/he/2006/20060254.pdf

HE 309/1993 vp. 1993. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta. Viitattu 10.10.2021. https://www.edilex.fi/he/fi19930309.pdf

HE 42/2016 vp. 2016. Hallituksen esitys eduskunnalle laiksi yksityisistä turvallisuuspalveluista annetun lain muuttamisesta. Viitattu 1.10.2021.
https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_42+2016.pdf

HE 48/2008. 2008. Hallituksen esitys Eduskunnalle sähköisen viestinnäntietosuojalain ja eräiden siihen liittyvien lakien muuttamisesta. Viitattu 10.10.2021: https://www.edilex.fi/he/fi20080048.pdf

HE 49/2018 vp. 2018. Hallituksen esitys eduskunnalle liikesalaisuuslaiksi ja eräiksi siihen liittyviksi laeiksi. Viitattu 1.10.2021. https://www.edilex.fi/he/fi20180049.pdf

HE 75/2000 vp. 2000. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi. Viitattu 10.11.2021. https://www.edilex.fi/he/fi20000075.pdf

HE 85/1998. 1998. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta sekä eräiksi siihen liittyviksi laeiksi. Viitattu 10.10.2021. https://www.edilex.fi/he/fi19980085.pdf

HE 9/2018 vp. 2018. Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Viitattu 10.11.2021. https://www.edilex.fi/he/fi20180009.pdf

HE 96/1998 vp. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi. Viitattu 1.10.2021. https://www.edilex.fi/he/fi19980096.pdf

HE luonnos. 2021a. Hallituksen esitys eduskunnalle laiksi Euroopan unionin ja kansallisen oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta sekä siihen liittyviksi laeiksi. Viitattu 10.9.2021. https://api.hankeikkuna.fi/asiakirjat/0b6fed29-b91b-4574-86c7-6b1354d8fc0d/2f1d6051-20d9-4f77-a345-b245d916a80c/LAUSUNTOPYYNTO_20210702114644.PDF

HE luonnos. 2021b. Hallituksen esitys eduskunnalle laiksi yksityisyyden suojasta työelämässä annetun lain 4 §:n muuttamisesta. Viitattu 1.10.2021. https://www.lausuntopalvelu.fi/FI/Proposal/DownloadProposalAttachment?attachmentId=16229

Hemmo, M. & Hoppu, K. 2006. Sopimusoikeus. E-Kirja. Helsinki: WSOYpro.

Henkilörekisteriasetus 476/1987. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/alkup/1987/19870476#Pidm45237816607248

Henkilörekisterilaki 471/1987. Viitattu 10.10.2021. https://finlex.fi/fi/laki/alkup/1987/19870471

Henkilötietodirektiivi 95/46/EY. Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Viitattu 1.8.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:31995L0046

Henkilötietolaki 531/1999. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/ajantasa/kumotut/1999/19990523

Hietanen, E. 2015. Miljardibisnes Suomessakin: Näille aloille järjestäytynyt rikollisuus on soluttautunut. Viitattu 1.10.2021. https://www.mtvuutiset.fi/artikkeli/miljardibisnes-suomessakin-naille-aloille-jarjestaytynyt-rikollisuus-on-soluttautunut/4981254

ICO. 2021. What is criminal offence data. Information Commissioner’s Office. Viitattu 1.10.2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/criminal-offence-data/

IETF. 1983. Assigned numbers. RFC 870. Internet Engineering Task Force. Viitattu 1.10.2021. https://datatracker.ietf.org/doc/html/rfc870

IETF. 1997. Dynamic Host Configuration Protocol standard. RFC 2131. Internet Engineering Task Force. Viitattu 1.10.2021. https://datatracker.ietf.org/doc/html/rfc2131

Ihmisoikeuksien julistus. 1948. YK:n ihmisoikeuksien yleismaailmallinen julistus. Ihmisoikeusliitto. Viitattu 8.10.2021. https://ihmisoikeusliitto.fi/ihmisoikeudet/ihmisoikeuksien-julistus/

Ihmisoikeuskeskus. 2021. Euroopan neuvosto, EN. Viitattu 8.10.2021. https://www.ihmisoikeuskeskus.fi/ihmisoikeudet/euroopan-neuvosto-en-council-of-/

IKD. 2021. Archive. Internationale Kommission der Detektiv-Verbände. Viitattu 21.8.2021. https://www.i-k-d.com/index.php?page=archive

Ilmiantajien suojeludirektiivi 1937/2016. Euroopan parlamentin ja neuvoston direktiivi unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta. Viitattu 10.9.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32019L1937&from=FI

Iltalehti. 2010. AL: Ammattirikolliset yrittävät soluttautua vartiointifirmoihin. Viitattu 1.10.2021. https://www.iltalehti.fi/uutiset/a/2010120712823469)

Iltalehti. 2021a. Tosielämän salapoliisit. Viitattu 1.10.2021. https://www.iltalehti.fi/uutiset/a/2015011718870373

Iltalehti. 2021b. Kommentti: Aikuinen ihminen saa kadota vaikka omaisiltaan, jos hän niin tahtoo. Viitattu 1.11.2021. https://www.iltalehti.fi/kotimaa/a/daff3d35-ffde-40f2-b04a-129521eba80e

IMY. 2021. Brottsuppgifter. Integritetsskyds myndigheten. Viitattu 8.10.2021. https://www.imy.se/verksamhet/dataskydd/dataskydd-pa-olika-omraden/arbetsliv/tillaten-behandling--vilka-krav-galler/brottsuppgifter/

Isotalo, K. 2018. Rekisteritunnus on henkilötieto. Artikkeli sähköisessä lehdessä Positio 02/2018. Maanmittauslaitos. Viitattu 8.10.2021. https://www.maanmittauslaitos.fi/tietoa-maanmittauslaitoksesta/ajankohtaista/lehdet-ja-julkaisut/positio-lehti/rekisteritunnus-on-henkilotieto

IT 2018 käyttöohje. 2018. Keskuskauppakamari. Viitattu 1.11.2021. https://it-ehdot.fi/wp-content/uploads/2020/04/IT2018_kayttoohjeet.pdf

Italia v. komissio. 2016. Valtiontuki – Direktiivi 92/81/ETY – Kivennäisöljyjen valmisteverot – Alumiinioksidin valmistuksessa polttoaineena käytetyt kivennäisöljyt – Valmisteverovapautus – Toimenpiteen valikoivuus – Tuet, joiden voidaan katsoa soveltuvan yhteismarkkinoille – Valtiontuesta ympäristönsuojelulle annetut yhteisön suuntaviivat – Alueellisia valtiontukia koskevat vuoden 1998 suuntaviivat – Luottamuksensuoja – Oikeusvarmuus – Principe lex specialis derogat legi generali – Toimielinten toimien laillisuusolettamaa ja tehokasta vaikutusta koskeva periaate – Hyvän hallinnon periaate – Perusteluvelvollisuus. Tuomio. Viitattu 10.8.2021. https://curia.europa.eu/juris/document/document.jsf;jsessionid=5FB2B09FA95878170872B08A806B531B?text=&docid=176922&pageIndex=0&doclang=fi&mode=req&dir=&occ=first&part=1&cid=1501651

Jyväskylän yliopisto. 2020. Anonymisointi ja pseudonymisointi. Viitattu 9.10.2021. https://koppa.jyu.fi/avoimet/kirjasto/tutkimusaineistojenhallinta/henkilotiedot/anonymisointijapseudonymisointi

JUHTA. 2018. Liite 9. Erityisehtoja henkilötietojen käsittelystä (JIT 2015 – Henkilötiedot). Julkisen hallinnon tietohallinnon neuvottelukunta. Viitattu 1.11.2021.

https://www.suomidigi.fi/ohjeet-ja-tuki/jhs-suositukset/jhs-166-julkisen-hallinnon-it-hankintojen-yleiset-sopimusehdot-jit-2015

Kauppakaari 3/1734. Viitattu 1.11.2021.
https://www.finlex.fi/fi/laki/ajantasa/1734/17340003000#L18P3

Kauppalehti. 2021. Yritykset. Etsivätoiminta. Viitattu 27.8.2021.
https://www.kauppalehti.fi/yritykset/toimialat/etsiv%C3%A4toiminta/80300

Kerttula, T. 2010. Vartijat ja järjestyksenvalvojat julkisen vallan käyttäjinä. Yliopistopaino. Helsinki. Viitattu 10.9.2021.
https://helda.helsinki.fi/bitstream/handle/10138/18361/vartijat.pdf?sequence=2

Komission hyväksymät vakiolausekkeet. 2022. Tietosuojavaltuutetun toimisto. Viitattu 1.1.2022. https://tietosuoja.fi/komission-hyvaksymat-vakiolausekkeet

Komonen, OP. 2016. Mylly jauhaa yhä tekijänoikeuskirjeitä suomalaisille - yleensä joutuu maksamaan paljon tai enemmän. Tivi verkkojulkaisu. Viitattu 1.11.2021.
https://www.tivi.fi/uutiset/mylly-jauhaa-yha-tekijanoikeuskirjeita-suomalaisille-yleensa-joutuu-maksamaan-paljon-tai-enemman/bcabdd8b-b215-34f1-9304-464afca4a24f

Korpisaari, P. 2018. Henkilötiedot ja paikkatiedot. Miten tietosuojalainsäädäntö vaikuttaa paikkatietojen julkaisemiseen ja luovuttamiseen. Ympäristöministeriön raportteja 10/2018. Viitattu 8.10.2021.
https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160578/YMra_10_2018_Henkilotiedot_ja_paikkatiedot.pdf

Kuluttajansuojalaki 38/1978. Viitattu 1.11.2012.
https://www.finlex.fi/fi/laki/ajantasa/1978/19780038#L8

Käsikirja Euroopan tietosuojaoikeudesta. 2014. European Court of Human Rights. Viitattu 10.10.2021. https://www.echr.coe.int/Documents/Handbook_data_protection_FIN.pdf

Laki elinkeinon harjoittamisen oikeudesta 122/1919. Viitattu 8.10.2021.
https://www.finlex.fi/fi/laki/ajantasa/1919/19190122001

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä 1054/2018. Viitattu 1.1.2022.
https://www.finlex.fi/fi/laki/alkup/2018/20181054#Pidm45237816853008

Laki palvelujen tarjoamisesta 1116/2009. Viitattu 10.9.2021.
https://www.edilex.fi/lainsaadanto/20091166

Laki sähköisen viestinnän palveluista 917/2014.Viitattu 10.9.2021.
https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Laki tietoyhteiskuntakaaren muuttamisesta 68/2018. Viitattu 10.10.2021.
https://www.finlex.fi/fi/laki/alkup/2018/20180068

Laki varallisuusoikeudellisista oikeustoimista 228/1929. Viitattu 1.11.2021.
https://www.finlex.fi/fi/laki/ajantasa/1929/19290228

Lastensuojelulaki. 417/2007. Viitattu 8.10.2021.
https://www.finlex.fi/fi/laki/ajantasa/2007/20070417

Liikesalaisuusdirektiivi 943/2016. Euroopan parlamentin ja neuvoston direktiivi julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta

laittomalta hankinnalta, käytöltä ja ilmaisemiselta. Viitattu 1.11.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016L0943&from=FI

Liikesalaisuuslaki 595/2018. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/alkup/2018/20180595

Linnake, T. Kärkkäinen, H. 2018. Luvut julki: Operaattorit luovuttivat 200000 yhteystietoa piratismikirjeiden lähettäjille. Ilta-Sanomat verkkojulkaisu. Viitattu 1.11.2021. https://www.is.fi/digitoday/art-2000005526816.html

Oikaisu tietosuoja-asetukseen 679/2016. 2021. Euroopan parlamentin ja neuvoston asetukseen (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus) (Euroopan unionin virallinen lehti L 119, 4. toukokuuta 2016). Euroopan unionin virallinen lehti L74/35. 4.5.2021. Viitattu 8.10.2021. https://eur-lex.europa.eu/legal-content/EN-FI/ALL/?uri=CELEX:32016R0679R(03)&from=FI

Oikeudenkäymiskaari 4/1734. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/ajantasa/1734/17340004000#L17P20

Oikeusministeriö. 2018. Euroopan parlamentin ja neuvoston direktiivi unionin oikeuden rikkomisesta ilmoittavien henkilöiden suojelusta. OM028:00/2018 säädösvalmistelu. Viitattu 10.9.2021. https://oikeusministerio.fi/hanke?tunnus=OM028:00/2018

Oikeusministeriö 2021. Perustuslaki. Viitattu 1.10.2021. https://oikeusministerio.fi/perustuslaki

Oikeustoimilaki 228/1929. Laki varallisuusoikeudellisista oikeustoimista. Viitattu 1.11.2021. https://finlex.fi/fi/laki/ajantasa/1929/19290228#L2P11

Osakeyhtiölaki 624/2006. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/ajantasa/2006/20060624

Paasonen, J., Ellonen, V., Sutela, M. 2012. Yksityisen turvallisuusalan toimijoiden näkemyksiä turvasuojaustoiminnan sääntelystä. Lakimies 7–8/2012. Viitattu 10.9.2021. https://www.edilex.fi/lakimies/9262.pdf

Pakkokeinolaki 806/2011. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/alkup/2011/20110806

Palta. 2021. Tutkimukset ja julkaisut. Palvelualojen työnantajat Palta ry. Viitattu 24.8.2021. https://www.palta.fi/palvelualat-suomessa/tutkimukset-ja-julkaisut/

Palveludirektiivi 2006/123/EY. Euroopan parlamentin ja neuvoston direktiivi 2006/123/EY, annettu 12 päivänä joulukuuta 2006, palveluista sisämarkkinoilla. Viitattu 10.8.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A32006L0123

Perustuslaki 731/1991. Viitattu 10.10.2021. https://www.finlex.fi/fi/laki/ajantasa/1999/19990731#L2P10

PeVL 10/2006 vp. 2006. Perustuslakivaliokunnan lausunto 10/2006 vp. Hallituksen esitys laiksi järjestyksenvalvojista annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi. Viitattu 10.8.2021. https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_10+2006.pdf

PeVL 22/2014 vp. 2014. Perustuslakivaliokunnan lausunto 22/2014 vp. Hallituksen esitys eduskunnalle laiksi yksityisistä turvallisuuspalveluista sekä eräiksi siihen liittyviksi laeiksi.

Viitattu 10.8.2021.
https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_22+2014.pdf

PeVL 23/2020 vp. 2020. Perustuslakivaliokunnan lausunto PeVL 23/2020 vp hallituksen esitykseen 18/2020 vp. Viitattu 1.10.2021.
https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_23+2020.aspx

PeVL 30/2010 vp. 2010. Perustuslakivaliokunnan lausunto 30/2010. Hallituksen esitys valvontarangaistusta ja sähköistä valvontaa avolaitoksissa koskevaksi lainsäädännöksi. Viitattu 1.10.2021. https://www.eduskunta.fi/FI/vaski/Lausunto/Documents/pevl_30+2010.pdf

Pohjanoksa J, Stolt M, Suhonen R, Löyttyniemi E, Leino-Kilpi H. 2019a. Whistle-blowing process in healthcare: From suspicion to action. Nurse Ethics. 2019 March 26(2). 526-540. doi: 10.1177/0969733017705005. Epub 2017 May 11. PMID: 28494645. Viitattu 1.10.2021: https://journals.sagepub.com/doi/10.1177/0969733017705005

Pohjanoksa, J., Stolt, M., Suhonen, R., Leino-Kilpi, H. 2019b. Wrongdoing and whistleblowing in health care. Journal of Advanced Nursing Vol 75 2/2019. Blackwell Scientific Publications. Viitattu 10.9.2021.
https://research.utu.fi/converis/portal/detail/Publication/39844123?lang=fi_FI

Poliisi. 2021. Voimassa olevat turvallisuusalan elinkeinoluvat 20.8.2021. Viitattu 24.8.2021. https://poliisi.fi/documents/25235045/0/Voimassa-olevat-turvallisuusalan-elinkeinoluvat-20.8.2021.pdf/9b0bf085-b5bf-f2aa-70b0-f6c6f3c5e937/Voimassa-olevat-turvallisuusalan-elinkeinoluvat-20.8.2021.pdf?t=1629446386507

Prenzler, T. & King, M. 2002. The Role of Private Investigators and Commercial Agents in Law Enforcement. Trends and issues in crime and criminal justice 234. Viitattu 1.10.2021. https://www.aic.gov.au/publications/tandi/tandi234

Prenzler, T., Milroy, A. 2012. Recent inquiries into the private security industry in Australia: Implications for regulation. Security Journal (2012) 25, 342 – 355. doi: 10.1057/sj.2012.2. Viitattu 1.10.2021. https://www-proquest-com.nelli.laurea.fi/docview/1112276248/fulltextPDF/D6DB3EA9FFA8439APQ/1?accountid=12003

Private detective services act (ZDD-1). 2011. EU single market regulated professions database. Euroopan komissio. Viitattu 1.8.2021. https://ec.europa.eu/growth/tools-databases/regprof/index.cfm?action=regprof&id_regprof=21545&id_profession=9001&tab=countries&quid=2&mode=asc&pagenum=1

Project Ariel Final report. 2015. Organized Crime Infiltration of Legitimate Businesses in Europe: A Pilot Project in Five European Countries. Viitattu 1.10.2021.
https://www.researchgate.net/publication/305710696_Organized_Crime_Infiltration_of_Legitimate_Businesses_in_Europe_A_Pilot_Project_in_Five_European_Countries

PTK 36/2016/4. 2016. Eduskunnan lähetekeskustelu. Täysistunto. Tiistai 12.4.2016 klo 13.59—20.29. Viitattu 1.10.2021.
https://www.eduskunta.fi/FI/vaski/PoytakirjaAsiakohta/Sivut/PTK_36+2016+4.aspx

PwC. 2018. PwC's Global Economic Crime and Fraud Survey. PricewaterhouseCoopers Oy. Viitattu 1.10.2021. https://www.pwc.fi/fi/julkaisut/tiedostot/global-economic-crime-and-fraud-survey-suomi-2018.pdf

PwC. 2020. PwC's Global Economic Crime and Fraud Survey. PricewaterhouseCoopers Oy. Viitattu 1.10.2021. https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

Ratsula, N. 2016. Compliance – Eettinen ja vastuullinen liiketoiminta. E-kirja. Helsinki: Talentum.

Rikoslaki 39/1889. Viitattu 10.10.2021. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001

Rikostorjunnan tila. 2018. Selvityshankkeen loppuraportti. Poliisihallituksen julkaisusarja. Viitattu 1.10.2021. https://poliisi.fi/documents/25235045/42553324/rikostorjunnan_tila_selvityshankkeen_loppuraportti.pdf/3c8feabf-846c-0add-b732-4666ce3dc9ac/rikostorjunnan_tila_selvityshankkeen_loppuraportti.pdf?t=1604495170714

Räsänen, P. 2012. Ministeri Räsänen: Turvallisuuden parantamiseksi tarvitaan täsmätoimenpiteitä. IGEP-verkkosivusto. Viitattu 1.10.2021. https://igep.fi/en/-/1410869/minister-rasanen-specifika-insatser-behovs-for-att-forbattra-sakerheten

Räsänen, P. 2013. Yksityisen turvallisuusalan lainsäädäntö vaatii selkeyttämistä. Viitattu 1.10.2021. https://www.paivirasanen.fi/2013/03/yksityisen-turvallisuusalan-lainsaadanto-vaatii-selkeyttamista/

Safetion Oy. 2021. Yksityisetsivä. Viitattu 24.8.2021. https://www.safetion.fi/yksityisetsiva/

Savolainen, J. 2021. HTL Heikki Mansikka-ahon väitös: Poliisille yhden viraston malli ja kuntiin aluepoliisit asukasmäärän perusteella. Edilex uutiset. Julkisoikeus. Viitattu 1.10.2021. https://www.edilex.fi/uutiset/71398?allWords=Heikki+Mansikka-ahon&offset=1&perpage=20&sort=relevance&searchSrc=1&advancedSearchKey=1256952

Savolainen, M. 2021. Yksityisetsivät ovat korvaamaton apu monelle. Turvallisuus & Riskienhallinta, 36 vuosikerta, numero 4/2021. Turvallisuuden ja Riskienhallinnan (T&RH) Tietopalvelu Oy.

ScienceDirect. 2021. Mersenne Twister. Viitattu 8.10.2021. https://www.sciencedirect.com/topics/computer-science/mersenne-twister

Securitas. 2016. Etsivä löytää! Viitattu 25.8.2021. https://www.securitas.fi/media/nakoalapaikalla-blogi/etsiva-loytaa/

Securitas. 2021. Informaation tuottaminen. Viitattu 25.8.2021. https://www.securitas.fi/events/erikoisturvapalvelut/informaation-tuottaminennew-page/

Securitas. 2021. Turvallisuuspalvelut. Viitattu 25.8.2021. https://www.securitas.fi/turvallisuuspalvelut/

Sennewald, Charles A., Tsukayama, J. 2015. The Process of Investigation: Concepts and Strategies for Investigators in the Private Sector. E-kirja. Elsevier Science & Technology.

SopS 7/1976. Laki kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen eräiden määräysten hyväksymisestä 23.6.1975/107. Viitattu 8.10.2021. https://www.edilex.fi/valtiosopimukset/19760008

SopS 8/1976. Asetus kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen sekä siihen liittyvän valinnaisen pöytäkirjan voimaansaattamisesta 30.1.1976/108. Viitattu 8.10.2021. https://www.edilex.fi/valtiosopimukset/19760008

Standard Contractual Clauses. 2022. Euroopan komissio. Viitattu 1.1.2022. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en

Suomen Asiakastieto. 2021. AERTS. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/aerts/21315079/yleiskuva

Suomen Asiakastieto. 2021. AKM Consulting Oy. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/akm-consulting-oy/10281344/yleiskuva

Suomen Asiakastieto. 2021. AMCASE. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/amcase/25708056/yleiskuva

Suomen Asiakastieto. 2021. Kerberos Turvallisuuspalvelut. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/kerberos-turvallisuuspalvelut/18887455/yleiskuva

Suomen Asiakastieto. 2021. Nordic Security Services Ltd Oy. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/rosund-lillgard/13829221/yleiskuva

Suomen Asiakastieto. 2021. Opsec Oy. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/opsec-oy/22797583/yleiskuva

Suomen Asiakastieto. 2021. Patrikainen M.J. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/patrikainen-m-j/14247813/yleiskuva

Suomen Asiakastieto. 2021. Rösund Lillgård. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/rosund-lillgard/13829221/yleiskuva

Suomen Asiakastieto. 2021. Vercari Oy. Viitattu 27.8.2021.
https://www.asiakastieto.fi/yritykset/fi/vercari-oy/20161485/yleiskuva

Suomen Yksityisetsivä- ja Lakitoimistoliitto ry. 2021a. Jäsenet. Viitattu 24.8.2021.
http://www.yksityisetsiva.fi/2.0/index.php/jasenet/

Suomen Yksityisetsivä- ja Lakitoimistoliitto ry. 2021b. Eettiset säännöt. Viitattu 24.8.2021.
http://www.yksityisetsiva.fi/2.0/index.php/eettiset-saannot/

Suomen Yksityisetsivä- ja Lakitoimistoliitto ry. 2021d. Ajankohtaista. Viitattu 1.12.2021.
https://www.yksityisetsiva.fi/?page_id=98

Surakka, J. 2021. Mitä yksityisetsivän toimeksiannosta oli sovittu - käräjäoikeus arvioi. Edilex uutiset. Viitattu 8.10.2021. https://www.edilex.fi/uutiset/70054

Sähköisen viestinnän tietosuojadirektiivi 2002/58/EY. Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi). Viitattu 13.8.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32002L0058

Sähköisen viestinnän tietosuoja-asetus. 2017. Ehdotus. Euroopan parlamentin ja neuvoston asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). Viitattu 1.8.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:52017PC0010&from=fi

Taloushallintoliitto. 2021. Tilinpäätöksen julkisuus. Viitattu 27.8.2021.
https://taloushallintoliitto.fi/tilinpaatoksen-julkisuus

Tekijänoikeuslaki 404/1961. Viitattu 1.11.2021.
https://www.finlex.fi/fi/laki/ajantasa/1961/19610404#L7P60a

TEM097:00/2020, 2020. Hallituksen esitys laiksi yksityisyyden suojasta työelämässä annetun lain 4 §:n muuttamisesta. Asiakirjat: Suomen yksityisetsivä- ja lakitoimistoliiton lausunto. Viitattu 1.10.2021. https://tem.fi/hanke?tunnus=TEM097:00/2020

The Data Protection Commission. 2019. Guidance Note: Legal Bases for Processing Personal Data. Viitattu 1.11.2021. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20on%20Legal%20Bases.pdf

Tietosuoja-asetus 679/2016. Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Viitattu 1.8.2021. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Tietosuojalaki 1050/2018. Viitattu 10.10.2021. https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Tietosuojatyöryhmä WP 29. 2021. Euroopan unionin virallinen verkkosivusto. Viitattu 1.10.2021. https://europa.eu/about-edpb/more-about-edpb/article-29-working-party_fi

Tietosuojavaltuutetun toimisto. 2018. Luettelo vaikutustenarviointia edellyttävistä käsittelytoimista. Viitattu 1.11.2021. https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2020. Työelämän tietosuojan käsikirja. Viitattu 10.10.2021. https://tietosuoja.fi/documents/6927448/10594424/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+tietosuojavaltuutetun+toimisto.pdf/81dc78c3-6915-2893-5a19-62e3bc82988b/Ty%C3%B6el%C3%A4m%C3%A4n+tietosuojan+k%C3%A4sikirja+tietosuojavaltuutetun+toimisto.pdf?t=1600178022885)

Tietosuojavaltuutetun toimisto. 2021a. Seloste käsittelytoimista. Viitattu 1.11.2021. https://tietosuoja.fi/seloste-kasittelytoimista

Tietosuojavaltuutetun toimisto. 2021b. Usein kysyttyä työelämästä. Viitattu 1.11.2021. https://tietosuoja.fi/usein-kysyttya-tyoelama

Tietosuojavaltuutetun toimisto. 2021c. Vaikutustenarviointi. Viitattu 1.11.2021. https://tietosuoja.fi/vaikutustenarviointi

Tilastokeskus. 2008. Palvelualojen toimialakatsaus III/2007. Viitattu 24.8.2021. https://www.stat.fi/artikkelit/2008/art_2008-01-14_004.html?s=5

Tilastokeskus. 2021. Käsitteet. Mikroyritys. Viitattu 27.8.2021. https://www.stat.fi/meta/kas/mikroyritys.html

Traficom. 2021. Verkkotunnushaku. Viitattu 24.8.2021: https://www.traficom.fi/fi/viestinta/fi-verkkotunnukset/fi-verkkotunnushaku

TyVM 12/2018 vp. 2018. Hallituksen esitys eduskunnalle laeiksi yksityisyyden suojasta työelämässä annetun lain ja lasten kanssa työskentelevien rikostaustan selvittämisestä annetun lain 10 §:n muuttamisesta. Valiokunnan mietintö TyVM 12/2018 vp. Viitattu 10.11.2021. https://www.eduskunta.fi/FI/vaski/Mietinto/Sivut/TyVM_12+2018.aspx

Työelämän tietosuojalaki 759/2004. Laki yksityisyyden suojasta työelämässä 759/2004. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/ajantasa/2004/20040759

Työsopimuslaki 55/2001. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/ajantasa/2001/20010055

Työturvallisuuslaki 738/2002. Viitattu 1.11.2021.
https://www.finlex.fi/fi/laki/ajantasa/2002/20020738

Ustawa z dnia o ochronie osób zgłaszających naruszenia prawa. 2021. Rządowe Centrum Legislacji (Valtioneuvoston lainsäädäntökeskus). Viitattu 8.10.2021.
https://www.legislacja.gov.pl/docs/2/12352401/12822857/12822858/dokument525831.DOCX

Vainu.io. 2021a. Toimiala: Etsivätoiminta (80300). Viitattu 27.8.2021.
https://vainu.io/industry/FI/turvallisuus-vartiointi-ja-etsivapalvelut/etsivatoiminta/80300

Vainu.io. 2021b. Toimiala: Turvallisuus-, vartiointi- ja etsiväpalvelut (80). Viitattu 27.8.2021.
https://vainu.io/industry/FI/turvallisuus-vartiointi-ja-etsivapalvelut/80

W.A.D. 2021a. How to join W.A.D. World Association of Detectives. Viitattu 8.10.2021.
https://wad.memberclicks.net/join-wad

W.A.D. 2021b. Find an Investigator. World Association of Detectives. Viitattu 8.10.2021.
https://www.wad.net/find-an-investigator

What is an Intrusion Detection System? 2022. Barracuda Networks, Inc. verkkosivusto. Viitattu 1.8.2021. https://www.barracuda.com/glossary/intrusion-detection-system

Williams, P. 2022. FBI Director Wray says scale of Chinese spying in the U.S. 'blew me away'. NBC politics news. Haastattelun tallenne. Viitattu 2.2.2022.
https://www.nbcnews.com/politics/politics-news/fbi-director-wray-says-scale-chinese-spying-us-blew-away-rcna14369

WP 29. 2006. Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), 22 November 2006 (WP 128). Viitattu 1.10.2021. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf

WP 29. 2010. Opinion 1/2010 on the concepts of "controller" and "processor. Viitattu 1.10.2021. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_fi.pdf

WP 29. 2013. Opinion 03/2013 on purpose limitation. 00569/13/EN. WP 203. Viitattu 8.10.2021. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

WP 29. 2017a. Asetuksen 2016/679 mukaista suostumusta koskevat suuntaviivat, annettu 28. marraskuuta 2017. Viimeksi tarkistettu ja hyväksytty 10. huhtikuuta 2018. Viitattu 1.11.2021.
https://tietosuoja.fi/documents/6927448/8316711/Suostumus+fi/bd7605a0-5b37-4379-a681-57ba975a1ae7/Suostumus+fi.pdf?t=1535696147000

WP 29. 2017b. Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski". Viimeksi tarkistettu ja hyväksytty 4. lokakuuta 2017. Viitattu 1.11.2021.
https://tietosuoja.fi/documents/6927448/8316711/Vaikutustenarviointi+fi.pdf/af51e999-5326-4223-9deb-e21bdd2e0a63/Vaikutustenarviointi+fi.pdf?t=1527059635000

WP 29. 2017c. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. Viitattu 1.11.2021. http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

WP 29. 2017d. Tietosuojavastaavia koskevat ohjeet. WP 243 rev.01. Annettu 13. joulukuuta 2016. Viimeksi tarkistettu ja hyväksytty 5. huhtikuuta 2017. Viitattu 10.10.2021.
https://tietosuoja.fi/documents/6927448/8316711/Tietosuojavastaavia+koskevat+ohjeet+fi.p

df/3aad84e5-bb59-4e64-bdaf-adc1e5f2d719/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf/Tietosuojavastaavia+koskevat+ohjeet+fi.pdf?t=1527059636000

WP 29. 2018. Guidelines on transparency under Regulation 2016/679. WP260 rev.01. Viitattu 1.11.2021. https://ec.europa.eu/newsroom/article29/items/622227

Yhdistetyt tapaukset C-203/15 ja C-698/15. Unionin tuomioistuin. 2016. Ennakkoratkaisupyyntö – Sähköinen viestintä – Henkilötietojen käsittely – Sähköisen viestinnän luottamuksellisuus – Suoja – Direktiivi 2002/58/EY – 5, 6 ja 9 artikla sekä 15 artiklan 1 kohta – Euroopan unionin perusoikeuskirja – 7, 8 ja 11 artikla sekä 52 artiklan 1 kohta – Kansallinen lainsäädäntö – Sähköisten viestintäpalvelujen tarjoajat – Liikenne- ja paikkatietojen yleistä ja erotuksetta tapahtuvaa säilyttämistä koskeva velvollisuus – Kansalliset viranomaiset – Oikeus saada tietoja – Ei tuomioistuimen tai riippumattoman hallintoelimen ennakkovalvontaa – Yhteensoveltuvuus unionin oikeuden kanssa. Viitattu 1.11.2021. https://curia.europa.eu/juris/liste.jsf?num=C-203/15&language=fi

Yhdistetyt tapaukset C-92/09 ja C-93/09. Unionin tuomioistuin. 2010. Yksilöiden suojelu henkilötietojen käsittelyssä – Maataloustukien saajia koskevien tietojen julkaiseminen – Tällaisesta julkaisemisesta ja sen yksityiskohtaisista säännöistä annettujen unionin oikeuden säännösten pätevyys – Euroopan unionin perusoikeuskirja – 7 ja 8 artikla – Direktiivi 95/46/EY – 18 ja 20 artiklan tulkinta. Viitattu 10.11.2021. https://curia.europa.eu/juris/liste.jsf?num=C-92/09&language=fi

Yhteistoimintalaki 334/2007. Laki yhteistoiminnasta yrityksissä 334/2007. Viitattu 1.11.2021. https://www.finlex.fi/fi/laki/ajantasa/2007/20070334#L4P15

Yksityisetsivä Partes. 2021. noudettu 24.8.2021. https://www.yksityisetsivapartes.com/

YLE. 2015. "Aikuisella ihmisellä on oikeus kadota" – poliisi toivoo tervettä harkintaa katoamisilmoituksiin. Viitattu 1.11.2021. https://yle.fi/uutiset/3-8087764

YLE. 2019. Ammattihakkerit paljastavat: Suomalaisten tietoturva on heikoissa kantimissa. Viitattu 1.10.2021. https://yle.fi/aihe/artikkeli/2019/03/04/ammattihakkerit-paljastavat-suomalaisten-tietoturva-on-heikoissa-kantimissa

Yleissopimus 36/1992. YLEISSOPIMUS yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. Viitattu 8.10.2021. https://finlex.fi/fi/sopimukset/sopsteksti/1992/19920036/19920036_2

Yritystele. 2021. Luokittelu: Etsivätoiminta [80300]. Viitattu 27.8.2021. https://m.yritystele.fi/taxonomy/term/55336

Åstrand, C. 2020. Mitä due diligence tarkoittaa ja miksi se on yrityskaupoissa tärkeää? Talouselämä -lehden kumppaniblogit. Viitattu 8.10.2021. https://www.talouselama.fi/kumppaniblogit/bdo/mita-due-diligence-tarkoittaa-ja-miksi-se-on-yrityskaupoissa-tarkeaa/8be24e72-ec43-4135-92c9-03e81b69094e

Julkaisemattomat

Helsingin käräjäoikeus. 2005. Vartioimisliikerikos. Tuomio 05/11295.

Kiviniemi, P. 2020. Pari ajankohtaista GDPR-esimerkkiä oikeuskäytännöistä. Koulutus Digi- ja väestötietoviraston VAHTI tietosuojan kehittämisen työryhmän (TIKE) kokouksessa 1/2022. Julkaisematon.

Mikkola, J., Tietomurtotukinta käytännössä, tapausesimerkki, VAHTI viranomaistyöryhmän esitys digiturvaviikolla 2021, Verkkolähetys, Lähetyksen loppukysymyksissä esitettiin kysymys, että olisiko syyllinen ollut sisäpiirissä, mutta esittäjän vastaus kuului, että heidän ei ollut tarkoitus etsiä syyllistä vaikka ilmeisesti tietomurron kohteena ollut asiakas oli asian osalta tehnyt selvityksiä.

Turvallisuusalan valvontayksikön asiantuntija. 2021. Lupa-asioiden asiantuntijan haastattelu 12.8.2021. Poliisihallitus, turvallisuusalan valvontayksikkö. Puhelinhaastattelu.

Suomen Yksityisetsivä- ja Lakitoimistoliitto ry. 2021c. Jäsenrekisteri. Jäsenrekisteriin kohdistettu jäsenen tiedonsaantioikeuteen perustuva tarkastuspyyntö. Viitattu 6.8.2021.

SYL ry jäsenen asiantuntijahaastattelu. 2020. Suomen yksityisetsivä- ja lakitoimistoliiton jäsen ja yksityisetsivä. Suomen yksityisetsivä- ja lakitoimistoliitto. 24.10.2020. Etähaastattelu.

ÖDV-luottamushenkilön haastattelu. 2021. Österreichischer Detektiv-Verband -yhdistyksen luottamushenkilön haastattelu. 23.9.2021. Ljubljana.

Slovenialaisen etsivän haastattelu. 2021. 24.9.2021. Lubljana.

Vastaavan hoitajan haastattelu. 2021 Opsec Oy. 2021. 1.9.2021. Seinäjoki.

Viittaukset Tietosuoja-asetus -luvussa opinnäytetöihin, ei käytetty lähteenä työssä:

Lehtinen, E. 2017. Rekisterinpitäjän oikeutettu etu henkilötietojen käsittelyn oikeusperusteena tietosuoja-asetuksessa ja tietosuojalautakunnan ratkaisukäytännössä. Pro gradu –tutkielma. Helsingin yliopisto. http://urn.fi/URN:NBN:fi:hulib-201712185939

Räsänen, K.. 2018. EU:n yleisen tietosuoja-asetuksen oikeutettu etu henkilötietojen käsittelyn oikeusperusteena. Vaasan yliopisto.
https://osuva.uwasa.fi/handle/10024/9080Lukkarinen

Lukkarinen, K. 2019. HENKILÖTIETOJEN SUOJAN SUHTEESTA REKISTERINPITÄJÄN OIKEUTETTUUN ETUUN – miten oikeutettu etu toimii henkilötietojen käsittelyperusteena? Turun yliopisto. http://urn.fi/URN:NBN:fi-fe2019091928811

Kuviot

Taulukot

Liitteet

Liite 1: Turvallisuusalan sääntely Euroopassa

Maa	Turvallisuusalan luvanvaraisuus	Turvallisuusalalle oma lainsäädäntö	Yksityisetsivätoimintatunnistettu palveluna	Yksityisetsivätoiminnanluvanvaraisuus	Yksityisetsivätoimintaturvallisuusalankoulutuksessa	Laki yksityisetsivätoiminnasta
Itävalta	X		X	X		
Belgia	X	X			X	
Bosnia & Hertsegovina	X	X				
Bulgaria	X	X				
Kroatia	X	X			X	
Kypros	X	X				
Tšekin tasavalta	X					
Tanska	X	X				
Eesti	X	X				
Suomi	X	X				
Ranska	X	X				
Saksa	X	X				
Kreikka	X	X				
Unkari	X	X				
Irlanti	X	X				
Italia	X	X				
Latvia	X	X				X
Liettua	X	X				
Luxemburg	X	X				
Makedonia	X	X				
Malta	X	X				
Norja	X	X				
Puola	X	X				
Portugali	X	X				
Romania	X	X				
Serbia	X	X	X	X	X	
Slovakia		X				
Slovenia	X	X	X	X		X
Espanja	X	X			X	
Ruotsi	X	X				
Sveitsi	X	X	X			
Turkki	X	X				
Yhdistyneet kuningaskunnat		X				
Alankomaat	x	X			X	
Yhteensä	32	27	4	3	5	2

Liite 2: W.A.D. -listalla välitetyt toimeksiannot

ID	Assignment	Category	Client	Country	Target
1	investigator trace	other	na	15	na
2	insurance investigation	anti-fraud	company	75	na
3	investigator trace	other	na	72	na
4	background check	commercial	company	33	private
5	background check	legal work	na	France	private
6	Due diligence	legal work	na	108	na
7	background check	legal work	na	Netherlands	private
8	person trace	legal work	na	104	private
9	information acquisition	legal work	na	USA	na
10	person trace	legal work	na	Italy	na
11	surveillance	legal work	na	USA	na
12	asset trace	domestic	private	62	private
13	asset trace	legal work	na	37	private
14	background check	domestic	private	Mexico	private
15	information acquisition	legal work	na	51	company
16	background check	commercial	company	Turkey	private
17	information acquisition	legal work	na	USA	private
18	surveillance	legal work	na	France	na
19	lawyer search	domestic	private	USA	private
20	surveillance	legal work	na	USA	private
21	physical protection	commercial	company	Mexico	company
22	person trace	legal work	na	Japan	private
23	investigator trace	other	na	113	na
24	company trace	commercial	company	73	company
25	background check	legal work	na	52	private
26	insurance investigation	commercial	company	40	na
27	asset trace	legal work	na	45	na
28	information acquisition	legal work	na	Great Britain	private
29	crime forensics	legal work	na	92	na
30	lawyer search	legal work	na	USA	na
31	background check	legal work	na	USA	company
32	company trace	commercial	company	Great Britain	company
33	insurance investigation	anti-fraud	company	60	private
34	background check	legal work	na	Italy	private
35	background check	legal work	na	84	private

36	person trace	legal work	na	USA	private
37	person trace	legal work	na	61	private
38	investigator trace	other	na	42	na
39	person trace	legal work	na	USA	na
40	person trace	legal work	na	Great Britain	na
41	person trace	legal work	na	98	private
42	investigator trace	other	na	70	na
43	background check	legal work	na	19	private
44	lawyer search	domestic	na	USA	na
45	surveillance	legal work	na	56	na
46	asset trace	legal work	na	United Arab Emirates	company
47	surveillance	legal work	na	Thailand	na
48	background check	domestic	private	United Arab Emirates	private
49	information acquisition	legal work	na	7	private
50	debt collection	legal work	na	USA	na
51	lawyer search	domestic	private	USA	private
52	person trace	legal work	na	104	private
53	person trace	legal work	na	Portugal	private
54	person trace	domestic	private	Philippines	private
55	person trace	legal work	na	77	private
56	background check	legal work	na	United Arab Emirates	private
57	information acquisition	legal work	na	Mexico	na
58	TSCM	legal work	na	USA	na
59	credit check	commercial	company	Spain	private
60	company trace	legal work	na	3	company
61	person trace	legal work	na	23	private
62	surveillance	legal work	na	Spain	na
63	background check	legal work	na	USA	private
64	person trace	commercial	company	87	private
65	background check	legal work	na	98	private
66	person trace	legal work	na	43	private
67	information acquisition	domestic	private	87	private
68	information acquisition	legal work	na	na	na
69	surveillance	legal work	na	Great Britain	na
70	person trace	legal work	na	India	private
71	information acquisition	legal work	na	97	na
72	person trace	legal work	na	76	private
73	information acquisition	legal work	na	na	na

74	bank account	legal work	na	104	na
75	asset trace	legal work	na	25	private
76	background check	commercial	company	USA	company
77	background check	legal work	na	14	private
78	background check	legal work	na	43	private
79	information acquisition	legal work	na	Great Britain	private
80	person trace	legal work	na	USA	na
81	person trace	legal work	private	Turkey	private
82	investigator trace	other	na	68	na
83	information acquisition	legal work	na	na	na
84	person trace	legal work	na	France	na
85	trace	commercial	company	20	na
86	asset trace	legal work	na	USA	na
87	investigator trace	other	na	Mexico	na
88	infidelity	domestic	private	54	private
89	bank account	legal work	na	Portugal	na
90	background check	commercial	company	Germany	company
91	person trace	legal work	na	Germany	private
92	background check	legal work	na	94	company
93	asset trace	legal work	na	25	private
94	background check	legal work	na	USA	private
95	information acquisition	legal work	na	USA	na
96	information acquisition	legal work	na	71	private
97	person trace	legal work	na	Poland	na
98	investigator trace	other	na	67	na
99	person trace	legal work	na	27	private
100	background check	commercial	company	29	private
101	background check	legal work	na	12	private
102	person trace	domestic	private	83	private
103	credit check	commercial	company	India	private
104	person trace	legal work	na	USA	private
105	background check	legal work	public sector	110	company
106	person trace	legal work	na	60	private
107	person trace	domestic	private	94	private
108	background check	legal work	na	Philippines	private
109	IPR protection	commercial	company	Portugal	company
110	person trace	domestic	private	USA	private
111	investigator trace	other	na	Netherlands	na
112	bank account	legal work	na	60	private

113	background check	commercial	company	22	private
114	person trace	legal work	na	China	private
115	person trace	legal work	na	USA	na
116	background check	legal work	na	58	private
117	information acquisition	legal work	na	na	na
118	person trace	legal work	na	China	private
119	person trace	legal work	na	Netherlands	private
120	background check	commercial	company	Netherlands	private
121	background check	legal work	na	China	company
122	surveillance	legal work	na	USA	na
123	information acquisition	legal work	na	6	na
124	person trace	legal work	na	Thailand	private
125	repossession of property	legal work	na	Mexico	na
126	surveillance	commercial	company	Singapore	na
127	investigator trace	other	na	USA	na
128	bank account	legal work	na	USA	private
129	background check	legal work	na	100	company
130	background check	legal work	na	Germany	private
131	person trace	legal work	na	4	private
132	surveillance	legal work	na	USA	na
133	IPR protection	commercial	company	2	company
134	crime forensics	domestic	private	na	na
135	background check	legal work	na	USA	company
136	background check	legal work	na	19	company
137	Due diligence	commercial	company	13	company
138	information acquisition	legal work	na	Poland	private
139	information acquisition	legal work	na	na	na
140	surveillance	legal work	na	Germany	na
141	crime forensics	legal work	na	USA	private
142	company trace	legal work	na	China	company
143	background check	legal work	na	Poland	private
144	background check	legal work	na	103	na
145	information acquisition	commercial	company	USA	company
146	surveillance	legal work	na	USA	na
147	asset trace	legal work	na	Netherlands	company
148	surveillance	legal work	na	USA	private
149	surveillance	legal work	na	87	na
150	trace	legal work	na	Malta	na

151	person trace	legal work	na	77	na
152	person trace	legal work	na	Portugal	private
153	IPR protection	commercial	company	China	na
154	asset trace	legal work	na	17	na
155	background check	legal work	na	India	private
156	investigator trace	other	na	Taiwan	na
157	background check	legal work	na	USA	private
158	person trace	legal work	na	114	private
159	background check	legal work	na	63	company
160	asset trace	legal work	na	86	na
161	IPR protection	commercial	company	India	na
162	background check	legal work	na	Mexico	na
163	asset trace	legal work	na	Portugal	na
164	background check	legal work	na	110	private
165	surveillance	commercial	company	Great Britain	na
166	background check	legal work	na	30	private
167	person trace	legal work	na	27	private
168	information acquisition	legal work	na	88	private
169	investigator trace	other	na	84	na
170	person trace	legal work	na	France	private
171	lawyer search	domestic	na	USA	na
172	Due diligence	legal work	na	95	na
173	asset trace	commercial	company	China	company
174	information acquisition	domestic	private	52	private
175	investigator trace	other	na	19	na
176	person trace	legal work	na	Netherlands	private
177	person trace	commercial	company	Spain	private
178	background check	legal work	na	47	private
179	investigator trace	other	na	Philippines	na
180	asset trace	legal work	na	USA	na
181	background check	legal work	na	Canada	na
182	asset trace	legal work	na	Canada	na
183	lawyer search	commercial	company	USA	private
184	surveillance	commercial	company	USA	private
185	surveillance	legal work	na	66	private
186	person trace	legal work	na	Spain	private
187	lawyer search	legal work	na	20	na
188	credit check	commercial	company	40	private
189	person trace	legal work	na	Great Britain	na
190	background check	commercial	company	21	private

191	information acquisition	domestic	private	11	private
192	company trace	commercial	company	Turkey	company
193	person trace	legal work	na	31	na
194	information acquisition	commercial	company	Japan	private
195	person trace	legal work	na	India	private
196	person trace	legal work	na	17	private
197	background check	commercial	company	82	company
198	background check	legal work	na	Germany	private
199	information acquisition	legal work	na	USA	private
200	investigator trace	other	na	Singapore	na
201	background check	legal work	na	42	na
202	information acquisition	legal work	na	Philippines	na
203	person trace	domestic	private	10	private
204	information acquisition	legal work	na	Canada	na
205	surveillance	legal work	na	USA	na
206	insurance investigation	anti-fraud	company	USA	na
207	physical protection	other	na	Mexico	na
208	surveillance	legal work	na	China	na
209	asset trace	legal work	na	France	private
210	asset trace	legal work	na	Portugal	private
211	background check	legal work	na	United Arab Emirates	private
212	information acquisition	legal work	na	USA	na
213	background check	legal work	na	Malta	company
214	background check	commercial	company	52	private
215	person trace	legal work	na	USA	private
216	person trace	legal work	na	Spain	private
217	background check	legal work	na	India	private
218	IPR protection	commercial	company	43	company
219	asset trace	legal work	na	37	company
220	person trace	domestic	private	Great Britain	private
221	background check	legal work	na	USA	private
222	surveillance	legal work	na	86	na
223	asset trace	legal work	na	27	na
224	information acquisition	legal work	na	USA	na
225	person trace	legal work	na	France	private
226	investigator trace	other	na	na	na
227	person trace	legal work	na	103	private

228	person trace	legal work	na	81	private
229	information acquisition	domestic	private	Great Britain	private
230	background check	legal work	na	Netherlands	private
231	asset trace	legal work	na	36	na
232	person trace	legal work	na	65	na
233	person trace	legal work	na	50	na
234	information acquisition	legal work	na	na	private
235	asset trace	legal work	na	Great Britain	private
236	person trace	legal work	na	USA	private
237	person trace	legal work	na	62	company
238	person trace	domestic	private	110	private
239	information acquisition	legal work	na	USA	na
240	Due diligence	commercial	company	80	company
241	information acquisition	legal work	na	na	na
242	bank account	legal work	na	59	na
243	investigator trace	commercial	company	93	na
244	background check	legal work	na	Malta	na
245	information acquisition	domestic	private	25	private
246	person trace	legal work	na	Singapore	na
247	person trace	legal work	na	80	private
248	background check	commercial	company	79	private
249	information acquisition	legal work	na	na	na
250	TSCM	legal work	na	Mexico	na
251	information acquisition	legal work	na	na	private
252	information acquisition	legal work	na	France	na
253	person trace	legal work	na	105	private
254	person trace	commercial	company	22	private
255	Due diligence	legal work	na	93	na
256	background check	legal work	na	USA	private
257	company trace	legal work	na	9	company
258	background check	legal work	na	6	private
259	background check	legal work	na	16	company
260	background check	legal work	na	90	private
261	information acquisition	legal work	na	USA	na
262	surveillance	legal work	na	USA	na
263	person trace	legal work	na	Romania	private
264	person trace	domestic	private	57	private

265	surveillance	legal work	na	Portugal	private
266	person trace	legal work	na	55	private
267	information acquisition	legal work	na	38	na
268	background check	commercial	company	Canada	private
269	person trace	domestic	na	USA	private
270	investigator trace	other	na	na	na
271	person trace	legal work	na	Portugal	private
272	surveillance	legal work	na	USA	na
273	information acquisition	legal work	na	1	na
274	person trace	legal work	na	USA	private
275	background check	legal work	na	USA	private
276	information acquisition	legal work	na	USA	private
277	background check	commercial	company	30	private
278	information acquisition	legal work	na	na	private
279	background check	legal work	na	USA	company
280	Due diligence	legal work	na	10	na
281	background check	legal work	na	5	private
282	person trace	domestic	private	59	private
283	background check	domestic	private	35	private
284	background check	legal work	na	Great Britain	private
285	physical protection	other	na	Great Britain	na
286	surveillance	legal work	na	USA	na
287	background check	domestic	private	Thailand	private
288	information acquisition	domestic	private	France	private
289	person trace	legal work	na	39	na
290	person trace	domestic	na	Canada	private
291	person trace	legal work	na	Great Britain	private
292	person trace	legal work	na	Italy	private
293	Due diligence	legal work	na	9	na
294	surveillance	commercial	company	USA	private
295	background check	legal work	na	Romania	private
296	asset trace	legal work	na	Taiwan	na
297	Due diligence	commercial	company	99	company
298	person trace	legal work	na	India	private
299	person trace	legal work	na	na	private
300	person trace	domestic	private	Japan	private
301	asset trace	legal work	na	17	na
302	bank account	legal work	na	Poland	company
303	asset trace	domestic	private	Italy	private

304	investigator trace	commercial	company	43	company
305	credit check	commercial	company	Poland	private
306	investigator trace	legal work	na	28	na
307	background check	legal work	na	101	private
308	insurance investigation	commercial	company	USA	private
309	person trace	legal work	na	Romania	na
310	information acquisition	legal work	na	na	private
311	person trace	legal work	na	15	private
312	background check	legal work	na	Malta	na
313	lawyer search	domestic	na	USA	na
314	person trace	legal work	na	75	private
315	reputation protection	domestic	private	na	na
316	surveillance	legal work	na	19	na
317	bank account	legal work	na	96	na
318	investigator trace	commercial	company	84	na
319	background check	legal work	na	Netherlands	na
320	background check	legal work	na	Japan	private
321	person trace	legal work	na	22	private
322	information acquisition	legal work	na	USA	na
323	background check	legal work	na	21	private
324	bank account	legal work	na	83	na
325	investigator trace	legal work	na	Mexico	na
326	information acquisition	legal work	na	31	na
327	person trace	legal work	na	48	private
328	background check	legal work	na	China	company
329	background check	commercial	company	Great Britain	company
330	person trace	legal work	na	Turkey	private
331	surveillance	legal work	na	Taiwan	na
332	infidelity	domestic	private	Thailand	private
333	information acquisition	commercial	company	39	company
334	investigator trace	other	na	USA	na
335	person trace	domestic	private	92	private
336	background check	domestic	private	Philippines	private
337	person trace	legal work	na	USA	private
338	asset trace	legal work	na	91	na
339	person trace	legal work	na	Netherlands	na
340	surveillance	legal work	na	India	na
341	information acquisition	legal work	na	Singapore	na

342	asset trace	legal work	na	28	private
343	surveillance	legal work	na	90	private
344	lawyer search	domestic	na	USA	na
345	person trace	legal work	na	6	private
346	person trace	legal work	na	Taiwan	private
347	information acquisition	legal work	na	Germany	na
348	information acquisition	legal work	na	Japan	private
349	information acquisition	commercial	company	74	na
350	information acquisition	legal work	na	USA	na
351	investigator trace	legal work	na	46	na
352	investigator trace	legal work	na	Thailand	na
353	investigator trace	domestic	private	na	private
354	background check	commercial	company	Mexico	private
355	investigator trace	domestic	private	USA	na
356	person trace	legal work	na	39	na
357	person trace	legal work	na	52	private
358	person trace	legal work	private	China	private
359	company trace	legal work	na	na	company
360	trace	legal work	na	106	na
361	background check	legal work	na	Thailand	company
362	information acquisition	legal work	na	USA	private
363	bank account	domestic	private	Great Britain	private
364	person trace	legal work	na	Italy	private
365	investigator trace	commercial	company	France	company
366	asset trace	legal work	na	69	na
367	background check	legal work	na	111	private
368	person trace	legal work	na	51	private
369	asset trace	legal work	na	Romania	private
370	information acquisition	legal work	na	8	private
371	asset trace	legal work	na	Turkey	na
372	Due diligence	commercial	company	Portugal	company
373	asset trace	legal work	na	Italy	na
374	company trace	legal work	na	109	company
375	investigator trace	commercial	company	USA	na
376	asset trace	legal work	na	97	private
377	asset trace	legal work	na	40	na
378	investigator trace	other	na	85	na
379	asset trace	legal work	na	France	private

380	person trace	domestic	private	China	private
381	person trace	legal work	na	64	na
382	background check	legal work	na	84	na
383	person trace	domestic	private	USA	private
384	background check	legal work	na	18	company
385	lawyer search	domestic	na	USA	na
386	person trace	domestic	private	USA	private
387	background check	legal work	na	USA	private
388	bank account	legal work	na	27	company
389	background check	legal work	na	110	private
390	person trace	domestic	private	Germany	private
391	asset trace	legal work	na	44	private
392	investigator trace	other	na	55	na
393	person trace	legal work	na	110	private
394	investigator trace	legal work	na	96	na
395	child abduction	domestic	private	44	private
396	surveillance	legal work	na	USA	private
397	lawyer search	other	na	Canada	na
398	company trace	legal work	na	34	company
399	person trace	legal work	na	Mexico	private
400	person trace	legal work	na	United Arab Emirates	private
401	background check	commercial	company	Germany	private
402	background check	legal work	na	63	private
403	information acquisition	domestic	private	Great Britain	private
404	person trace	legal work	na	USA	private
405	asset trace	domestic	na	7	private
406	Due diligence	legal work	na	26	na
407	person trace	legal work	na	Spain	na
408	asset trace	legal work	na	75	private
409	person trace	legal work	na	Germany	private
410	investigator trace	other	na	102	na
411	asset trace	legal work	na	Germany	na
412	asset trace	legal work	na	Netherlands	company
413	background check	legal work	na	Thailand	company
414	investigator trace	other	na	5	na
415	asset trace	legal work	na	USA	private
416	asset trace	domestic	private	Great Britain	private
417	investigator trace	other	na	99	na
418	person trace	legal work	na	Canada	private
419	lawyer search	domestic	private	Germany	private

420	credit check	commercial	company	Italy	private
421	information acquisition	legal work	na	Italy	company
422	background check	commercial	company	24	private
423	person trace	legal work	na	Malta	private
424	surveillance	legal work	na	32	na
425	person trace	legal work	na	Turkey	private
426	asset trace	legal work	na	37	private
427	person trace	legal work	na	Japan	private
428	information acquisition	domestic	private	USA	private
429	person trace	domestic	private	40	private
430	credit check	commercial	company	Portugal	private
431	information acquisition	legal work	na	na	private
432	person trace	legal work	na	53	na
433	company trace	legal work	na	Canada	company
434	person trace	legal work	na	11	private
435	Due diligence	legal work	na	89	na
436	surveillance	legal work	na	USA	na
437	lawyer search	other	na	9	na
438	person trace	legal work	na	Italy	private
439	person trace	legal work	na	France	private
440	person trace	legal work	na	17	private
441	background check	legal work	na	92	private
442	information acquisition	legal work	na	68	company
443	infidelity	domestic	private	104	private
444	background check	commercial	company	Singapore	private
445	background check	legal work	na	India	private
446	person trace	legal work	na	Japan	private
447	person trace	legal work	na	Canada	private
448	information acquisition	legal work	na	na	na
449	person trace	legal work	na	5	private
450	investigator trace	other	na	USA	private
451	surveillance	legal work	na	38	na
452	person trace	legal work	na	41	na
453	person trace	legal work	na	Mexico	private
454	surveillance	legal work	na	USA	na
455	asset trace	legal work	na	Usa	na
456	background check	domestic	na	Romania	private
457	background check	legal work	na	112	private
458	background check	legal work	na	Canada	private

459	Due diligence	commercial	company	35	company
460	person trace	domestic	private	78	private
461	surveillance	domestic	private	USA	private
462	background check	legal work	na	Great Britain	private
463	person trace	legal work	na	29	private
464	background check	legal work	na	Japan	na
465	asset trace	legal work	na	113	na
466	person trace	legal work	na	Spain	na
467	person trace	domestic	private	Portugal	private
468	background check	legal work	na	Canada	private
469	background check	legal work	na	107	na
470	lawyer search	domestic	private	Taiwan	private