VAASAN YLIOPISTO
LASKENTATOIMEN JA RAHOITUKSEN YKSIKKÖ
TALOUSOIKEUS

Eveliina Palmroos

KYC-TIETOJEN KÄSITTELY PANKISSA

Rahanpesulain ja tietosuoja-asetuksen rajapinta

Talousoikeuden
pro gradu -tutkielma

ICT-juridiikan koulutusohjelma

VAASA 2018

SISÄLLYSLUETTELO **sivu**

VAASAN YLIOPISTO
Laskentatoimen ja rahoituksen yksikkö
Tekijä: Eveliina Palmroos
Tutkielman nimi: KYC-tietojen käsittely pankissa – Rahanpesulain ja tietosuoja-asetuksen rajapinta
Ohjaaja: Pekka Vainio
Tutkinto: Kauppatieteiden maisteri
Oppiaine: Talousoikeus
Koulutusohjelma: ICT-juridiikka
Aloitusvuosi: 2012
Valmistumisvuosi: 2018 **Sivumäärä: 86**

TIIVISTELMÄ

Asiakkaan tunteminen, eli KYC (Know Your Customer), on noussut viime aikoina mediassa esiin pankkien asiakkailleen esittämien kysymysten johdosta. Pankkien valvonnan lisääntyessä on kuitenkin myös huoli yksityisyyden säilymisestä kasvanut. Pankin tuleekin asiakkaan tuntemiseen liittyvissä prosesseissa ottaa huomioon sekä rahanpesulain että tietosuoja-asetuksen eriävät intressit.

Asiakkaan tunteminen on monipuolinen, koko asiakkuuden elinkaaren kattava prosessi. Alati muuttuva lainsäädäntö, dynaaminen rikosympäristö ja kahden, vastakkaisia intressejä ajavan lain noudattaminen luovat pankille oman haasteensa sopeutua viranomaisten asettamiin lukuisiin velvoitteisiin. Tutkimuksen tarkoituksena onkin ensinnäkin selvittää, millaisia lakisääteisiä velvollisuuksia pankilla on koskien henkilöasiakkaidensa tietojen käsittelyä asiakkaan tuntemisen näkökulmasta, tarkoituksena estää rahanpesua ja terrorismin rahoittamista. Toiseksi, tutkimus pyrkii selvittämään, miten rahanpesulaki ja tietosuoja-asetus suhteutuvat toisiinsa asiakkaan tuntemiseen kerättyjä henkilötietoja käsitellessä, ja millaisia haasteita näiden kahden lain yhteensovittaminen luo pankille.

Tutkielma perustuu tämänhetkisen oikeustilan systematisointiin ja tulkintaan, käyttäen hyväksi lainsäädännön ja viranomaislähteiden lisäksi sekä kotimaista että kansainvälistä oikeuskirjallisuutta. Tutkimuksessa käy ilmi, että pankki on haastavassa tilanteessa pyrkiessään samanaikaisesti soveltamaan kahta, täysin vastakkaisia intressejä ajavia lakeja. Siinä kuitenkin onnistuessaan pankki on osana luomassa aiempaa toimivampaa, turvallisempaa ja yksilöiden oikeuksia kunnioittavampaa yhteiskuntaa.

AVAINSANAT: Asiakkaan tunteminen, henkilötietojen käsittely, rahanpesu, terrorismin rahoittaminen, yksityisyyden suoja

LYHENNELUETTELO

EU	Euroopan unioni
HE	Hallituksen esitys
KYC	Know Your Customer
LuottoL	Laki luottolaitostoiminnasta 610/2014
RahanpesuL	Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017
Tietosuoja-asetus	Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)

1. JOHDANTO

1.1. Tutkimuskohteen kuvaus

Asiakkaan tunteminen, eli KYC, on noussut viime aikoina vahvasti esille etenkin pankkien esittämien, asiakkaan tuntemiseen liittyvien kysymysten johdosta[1]. Aihe on ihmetyttänyt ja puhututtanut ihmisiä, ja keskustelu aiheen ympärillä on usein ollut negatiivissävytteistä. Pankkien tiedustelut on koettu tungettelevina, syyttävinä ja tarpeettomina. Keskusteluista käy ilmi etteivät asiakkaat ole täysin tietoisia siitä, minkä vuoksi pankki kerää tietoa asiakkaistaan, ja onko tällainen toiminta laillista asiakkaiden yksityisyyden suojan näkökulmasta.

Yleisen keskustelun perusteella vaikuttaakin siltä, että asiakkaan tuntemiseen liittyvät kysymykset nähdään pankin vapaaehtoisesti harjoittamana toimintana, jonka uskotaan palvelevan pankin liiketoiminnallisia intressejä. Asia ei kuitenkaan ensisijaisesti ole näin. Pankin asiakkailleen esittämät kysymykset perustuvat ennen kaikkea pankin lakisääteiseen velvollisuuteen tuntea asiakkaansa[2]. Yrityksen oman edun sijaan kysymys on siis yhteiskunnallisesta hyvästä, sillä asiakkaan tuntemisella pyritään pääasiallisesti estämään rahanpesua ja torjumaan terrorismin rahoittamista. Pankilla, kuten muillakin finanssipalveluiden tarjoajilla, on lakiin perustuva velvollisuus sekä tunnistaa että tuntea asiakkaansa[3].

Asiakkaan tuntemisen tarkoituksena on mahdollistaa rahanpesun ja terrorismin rahoittamisen estäminen. Rahanpesulla tarkoitetaan rikoksella hankittujen varojen alkuperän häivyttämistä niin, että varojen alkuperä saadaan vaikuttamaan lailliselta[4]. Rikollisella toiminnalla hankittua omaisuutta pyritään siis peittelemään ja näin välttymään viranomaistoimenpiteiltä[5]. Varojen alkuperää, tosiallista luonnetta tai todellisia edunsaajia pyritään peittämään kierrättämällä varoja laillisen maksujärjestelmän kautta[6]. Rahanpesu edellyttää siis esirikoksen tapahtumista, eli varojen hankintaan laittomin toimin[7]. Terrorismin rahoittamisella sen sijaan tarkoitetaan varojen hankkimista tai keräämistä terroristista tarkoitusta varten. Terrorismin rahoittaminen poikkeaa rahanpesusta varojen alkuperän

[1] Savolainen 2016.
[2] Siikala 2015.
[3] Finanssivalvonta 2017 a.
[4] Seymour 2008: 374.
[5] Poliisi 2018.
[6] Sisäministeriö 2018.
[7] Poliisi 2018.

osalta siinä, että terrorismia voidaan rahoittaa sekä laillisesti että laittomasti hankituilla varoilla.[8]

Rahanpesua ja terrorismin rahoittamista koskeva lainsäädäntö on jatkuvassa muutoksessa muun muassa maksujärjestelmien monipuolistumisen, teknologian kehittymisen ja globalisoitumisen vuoksi. Rahanpesu kriminalisointiin Suomessa vuonna 1994[9]. Tämän jälkeen rahanpesulaki on muuttanut muotoaan muun muassa Euroopan unionin lainsäädännön myötä. Vuonna 2008 voimaan astunut laki rahanpesun ja terrorismin rahoittamisen estämisestä ja selvittämisestä kumottiin rahanpesulain kokonaisuudistuksen yhteydessä lailla rahanpesun ja terrorismin rahoittamisen estämisestä[10] heinäkuussa 2017[11]. Uusi kansallinen laki rahanpesun ja terrorismin rahoittamisen estämisestä perustuu voimassa olevaan, niin sanottuun neljänteen rahanpesudirektiiviin ja FATF:n[12] vuonna 2004 antamiin suosituksiin. Lainsäädännön dynaamisuutta ilmentää lisäksi hyvin Euroopan komission heinäkuussa 2016 antama ehdotus heinäkuussa 2017 kansallisesti voimaan saatetun neljännen rahanpesudirektiivin muutokseksi.[13]

Rahanpesu on yksi suurimmista esteistä toimivalle, kansainväliselle rahoitusjärjestelmälle. Rahanpesu on globaali ilmiö ja kansainvälinen haaste, johon liittyy usein monimutkaisia liiketoimia ja lukuisia ulkomaisilla lainkäyttöalueilla toimivia rahoituslaitoksia. Tästä johtuen sekä rahanpesua että terrorismin rahoittamista on erittäin vaikeaa tutkia ja tuomita.[14] Rahanpesu on olennainen osa järjestäytynyttä rikollisuutta. Integroituneen maailman johdosta rahanpesun ja terrorismin rahoittamisen torjunta ei ole kansallinen ongelma, vaan se on rajat ylittävä, kansainvälinen haaste.[15] Pankeilla on muiden finanssialalla toimivien yritysten ohella merkittävä asema rahanpesun estämisessä ja terrorismin rahoittamisen torjunnassa. Tämän vuoksi pankkeja velvoitetaankin aktiivisesti suojelemaan palveluitaan rahanpesuun ja terrorismin rahoittamiseen liittyviltä väärinkäytöksiltä.[16] Rahanpesu tapahtuu nimenomaan laillisten maksujärjestelmien[17], esimerkiksi pankkien kautta. Pankit voivat siis edesauttaa rahanpesun ja terrorismin rahoittamisen estämistä tunnistamalla ja tuntemalla asiakkaansa.

[8] Sisäministeriö 2018.
[9] Poliisi 2018.
[10] Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017.
[11] Eduskunta 2017.
[12] FATF on lyhenne sanoista Financial Action Task Force on Money Laundering.
[13] Valtiovarainministeriö 2018.
[14] Buchanan 2004: 115.
[15] Poliisi 2018.
[16] de Koker 2006: 28.
[17] Sisäministeriö 2018.

Vaikka asiakkaan tunteminen onkin aiheena yhteiskunnallisesti tärkeä nimenomaan rahanpesun ja terrorismin rahoittamisen estämisen näkökulmasta, liittyy siihen kääntöpuolena myös toinen tärkeä aihe, nimittäin yksityisyyden ja henkilötietojen suoja. Samalla kun pankkeja velvoitetaan täyttämään rahanpesulaissa asetetut, asiakkaan tuntemiseen liittyvät vaatimukset, tulee pankkien myös yhtä lailla ottaa huomioon henkilötietojen käsittelyä koskevat säännökset käsitellessään asiakkaan tuntemista varten kerättyjä henkilötietoja.

Henkilötietojen käsittelyn merkitys on noussut uudella tavalla esiin Euroopan unionin yleisen tietosuoja-asetuksen[18] myötä, jota on sovellettu 25.5.2018 lähtien. Ennen tietosuoja-asetusta henkilötietojen käsittelyyn on Suomessa sovellettu henkilötietolakia[19], joka on jo itsessään ollut sisällöltään hyvin kattava. Henkilötietolain periaatteet ovatkin vastanneet monilta osin tietosuoja-asetuksen säädöksiä, ja tietosuoja-asetus onkin lähinnä tuonut täsmennyksiä henkilötietolain sisältöön[20]. Tietosuoja-asetus tuo kuitenkin mukanaan myös uusia vaatimuksia ja tiukempia sanktioita tietosuojarikkeisiin, minkä voidaan nähdä olevan asiakkaan tuntemisen osalta pankille suuri haaste jo valmiiksi vahvasti säädellyssä lainsäädäntöympäristössä.

Maailma on muuttunut merkittävästi vuodesta 1999, jolloin henkilötietolaki astui voimaan. Teknologia on kehittynyt ja maiden väliset rajat ovat väistyneet globalisoitumisen myötä. Tietosuoja-asetuksella pyritäänkin vastaamaan muuttuneen maailman tarpeisiin yhtenäistämällä EU:n jäsenmaiden tietosuojaa koskevaa sääntelyä. Tietosuoja-asetuksen tarkoituksena on tehdä henkilötietojen käsittelystä avoimempaa ja läpinäkyvämpää, samalla lisäten rekisteröityjen mahdollisuutta valvoa henkilötietojensa käsittelyä.[21] Kaikkien tietosuoja-asetuksen sääntelyn piiriin kuuluvien toimijoiden on kiinnitettävä huomioita siihen, mitä tietoja yrityksellä on olemassa asiakkaistaan, missä ja miten tietoja säilytetään, onko tietojen säilyttämiselle oikeudellisia perusteita, ja ovatko tiedot turvassa kolmansilta osapuolilta[22]. Vaikka lainsäädäntö henkilötietojen käsittelyn suhteen on ollut esimerkiksi Suomen osalta jo ennestään hyvin kattava, jäsenmaiden lainsäädännön yhdenmukaistaminen edesauttaa sisämarkkinoiden digitaalitalouden kehitystä ja rakentaa luottamusta toimivaan yhteiskuntaan.[23]

[18] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus); esiintyy myöhemmin tekstissä terminä ”tietosuoja-asetus”.
[19] Henkilötietolaki 523/1999.
[20] Talus, Autio, Hänninen, Pihamaa & Kantonen 2017: 9-12.
[21] Talus ym. 2017: 9; Young 2017.
[22] Young 2017.
[23] Talus ym. 2017: 9.

Asiakkaan tunteminen on siis aiheena hyvin ajankohtainen ja tutkimuskohteena dynaaminen sekä moniulotteinen. Aihe on myös sekä kansallisesti että kansainvälisesti puhuttava, sillä asiakkaan tuntemistoimenpiteet koskevat jokaista maksujärjestelmien piirissä olevaa yksityishenkilöä ja yritystä. Kaksi hiljattain uudistunutta, vastakkaisia intressejä ajavat lainsäädännöt tuovat oman mielenkiintonsa aiheen tarkasteluun pankin näkökulmasta, sillä alati muuttuvat regulaatiot luovat pankeille haasteita sopeuttaa liiketoimintansa eri osa-alueet vastaamaan lain velvoittamia vaatimuksia.

1.2. Tutkimustehtävä ja sen rajaus

Tämän tutkielman tarkoituksena on ensinnäkin selvittää, minkälaisia velvoitteita laki asettaa pankeille koskien henkilötietojen käsittelyä asiakkaan tuntemisen näkökulmasta. Tutkielman tarkoituksena on myös selventää rahanpesulain ja tietosuoja-asetuksen rajapintaa: miten nämä toisiinsa nähden vastakkaisia intressejä ajavat lait suhteutuvat toisiinsa.

Yleislakina Euroopan unionin yleinen tietosuoja-asetus sääntelee luonnollisten henkilöiden henkilötietojen käsittelyä. Henkilötietojen käsittelyä säännellään tietosuoja-asetuksen lisäksi useissa erityislaissa, jotka ovat sovellettavuudeltaan ensisijaisia yleislakiin nähden. Erityislakien säännöksillä voi olla oleellinen vaikutus henkilötietojen käsittelyyn ja yksityisyyden suojaan.[24] Laki rahanpesusta ja terrorismin rahoittamisen estämisestä luo omat puitteensa erityislakina asiakkaan tuntemisen johdosta suoritettuun henkilötietojen käsittelyyn. Vaikkakin rahanpesulaki näyttäytyy tietosuoja-asetukseen nähden erityislakina, ei tietosuoja-asetusta voida sivuuttaa asiakkaan tuntemista varten kerättyjä henkilötietoja käsiteltäessä.

Tutkimus rajautuu pankkien velvollisuuteen tunnistaa ja tuntea henkilöasiakkaansa. Tutkimuksen ulkopuolelle jäävät siis muut, saman velvollisuuden piirissä olevat finanssipalveluita tarjoavat toimijat. Tutkimuksessa käsitellään lisäksi ainoastaan asiakkaan tuntemista luonnollisten henkilöiden osalta, jättäen oikeushenkilöt tutkimuksen ulkopuolelle. Asiakkaan tuntemisella tarkoitetaan tässä tutkielmassa ainoastaan pankkien lakiin perustuvaa velvollisuutta tunnistaa ja tuntea asiakkaansa rahanpesun ja terrorismin rahoittami-

[24] Tietosuojavaltuutetun toimisto 2013.

sen estämisen näkökulmasta. Mahdolliset muut pankkien lakisääteiset selonottovelvollisuudet tai liiketoiminnalliset intressit koskien asiakkaan tuntemista jätetään tämän tutkimuksen ulkopuolelle.

Tutkielma keskittyy kahden tutkimustehtävän käsittelyyn, jotka voidaan asettaa seuraavaan muotoon:

1) Millaisia lakisääteisiä velvollisuuksia pankilla on koskien henkilöasiakkaidensa tietojen käsittelyä asiakkaan tuntemisen (KYC) näkökulmasta, tarkoituksena estää rahanpesua ja terrorismin rahoittamista?

2) Miten rahanpesulaki ja tietosuoja-asetus suhteutuvat toisiinsa asiakkaan tuntemiseen kerättyjä henkilötietoja käsitellessä, ja millaisia haasteita näiden kahden lain yhteensovittaminen luo pankille?

1.3. Tutkimuksen metodit ja lähteet

Tutkimuksen tarkoituksena on selvittää tutkimusaihetta koskevien voimassaolevien oikeussääntöjen sisältöä. Voimassa olevien oikeussääntöjen sisällön selvittämisellä tarkoitetaan kahta asiaa: oikeuden voimassaolon toteamista ja oikeussäännön sisällön selvittämistä[25]. Tämän tutkielman metodina käytetäänkin lainopillista, eli oikeusdogmaattista metodia. Oikeusdogmaattisen metodin tarkoituksena on systematisoida ja tulkita voimassa olevia oikeusnormeja. Voimassaolevan oikeuden systematisoinnilla tarkoitetaan yksittäisten normien ja niiden tosiasiallisten tarkoitusten kokoamista yhdenmukaiseksi kokonaisuudeksi, kun taas tulkinnalla tarkoitetaan oikeuden sisällön selvittämistä.[26]

Tutkielmassa käytetyt lähteet koostuvat velvoittavuudeltaan eri asteisista oikeuslähteistä, primaarisista ja sallituista oikeuslähteistä[27]. Primaarisina, eli vahvasti velvoittavina lähteinä käytetään EU-lainsäädännön ja Suomen lain lisäksi lukuisia viranomaislähteitä, jotka ovat tutkielman kannalta erittäin keskeisessä asemassa. Primaaristen oikeuslähteiden tukena käytetään sallittuja oikeuslähteitä, eli oikeuskirjallisuutta sen eri muodoissa.

[25] Aarnio 1989: 47.
[26] Aarnio 1989: 48.
[27] Virolainen 2012: 4.

1.4. Tutkimuksen rakenne

Tutkimus muodostuu johdantokappaleen lisäksi viidestä erillisestä asiakokonaisuudesta ja tutkielman lopussa esitettävistä johtopäätöksistä. Tutkimus etenee kronologisessa järjestyksessä, käyden läpi asiakkaan tuntemiseen liittyvät moninaiset vaiheet ja osa-alueet koko asiakkuuden elinkaaren ajalta, aina asiakkuuden perustamisesta jatkuvaan seurantaan asti. Kaikkien asiakkaiden tuntemista koskevien vaiheiden lisäksi käydään läpi vain tiettyjä asiakkaita koskeva selonotto- ja ilmoitusvelvollisuus, ja niihin liittyvät toimenpiteet. Henkilötietojen käsittelyä koskeviin periaatteisiin ja määräyksiin syvennytään tarkemmin omassa kappaleessaan, vaikkakin aihe on mukana myös muissa tutkielman osioissa. Asiakkaan tuntemiseen liittyvän prosessin ja henkilötietojen käsittelyn lisäksi pohditaan miten rahanpesulaki ja tietosuoja-asetus suhteutuvat toisiinsa, ja millaisia haasteita pankki kohtaa pyrkiessään noudattamaan molempien lakien asettamia vaatimuksia.

Ensimmäisessä varsinaisessa osiossa (2. kappale) käsitellään tutkielmaan liittyvää normiperustaa ensin erikseen sekä rahanpesu- että tietosuojalainsäädännön näkökulmasta, minkä jälkeen käsitellään lyhyesti näiden kahden lain välistä rajapintaa.

Toisessa varsinaisessa osiossa (3. kappale) käsitellään asiakkaan tuntemiseen liittyviä tekijöitä yleisten periaatteiden, tunnistamisen ja tuntemistietojen hankkimisen ja tuntemisen eri tasojen osalta. Kappale on tutkielman kannalta hyvin keskeinen, sillä se kattaa kaikki ne toimenpiteet, joita pankeilta vaaditaan asiakkuudesta tai asiakkaan harjoittamasta toiminnasta riippumatta. Asiakkaan toiminta ei siis itsessään vaikuta juurikaan siihen, tuleeko pankin täyttää yllä mainitut vaatimukset asiakkaan tuntemiseen liittyen.

Kolmannessa varsinaisessa osiossa (4. kappale) käydään läpi, mitä asiakkaan tuntemistietojen käsittely käytännössä pitää sisällään. Yleisten tietojenkäsittelyä koskevien periaatteiden lisäksi kappaleessa esitellään myös muita tietojenkäsittelyyn liittyviä säädöksiä, sekä rekisteröidyn oikeuksia että rekisterinpitäjän velvollisuuksia. Kappaleessa tuodaan esiin rahanpesulain ja tietosuoja-asetuksen eriävät intressit ja se, miten nämä kaksi lakia suhteutuvat toisiinsa. Kappaleessa päästään paneutumaan tietojenkäsittelyyn muita kappaleita yksityiskohtaisemmin, vaikkakin näkökulma on vahvasti mukana myös tutkielman muissa kappaleissa.

Neljännessä varsinaisessa osiossa (5. kappale) paneudutaan pankin selonotto- ja ilmoitusvelvollisuuteen sekä jatkuvan seurannan toteuttamiseen. Selonotto- ja ilmoitusvelvol-

lisuuden täyttymiseen vaikuttaa pitkälti asiakkaan käyttäytyminen, minkä vuoksi se voidaankin nähdä poikkeuksellisesti toteutuvana, pankin harjoittamana toimenpiteenä kolmannessa kappaleessa esitettyihin, tavanomaisiin asiakkaan tuntemiseen liittyviin toimenpiteisiin nähden. Tämä kappale on hyvin mielenkiintoinen, sillä juurikin selonotto- ja ilmoitusvelvollisuus voidaan nähdä kiteyttävän koko asiakkaan tuntemisen funktion.

Viidennessä varsinaisessa kappaleessa (6. kappale) pohditaan millaisia haasteita pankki kohtaa pyrkiessään luovimaan kahden täysin erilaisia intressejä ajavan lain välillä. Tietosuoja-asetuksen soveltaminen on vasta alkumetreillä eikä kattavaa rahanpesu- ja tietosuojalainsäädäntöä vertailevaa tutkimusta ole saatavilla, joten kappaleessa esitetyt näkökulmat ovat yksittäisten artikkeleiden ja kirjoittajan omien näkemysten perusteella tehtyjä tulkintoja.

2. NORMIPERUSTA

2.1. Rahanpesulainsäädäntö

Rahanpesun ja terrorismin rahoittamisen estäminen on globaali haaste, jota pyritään torjumaan kansainvälisin standardein[28]. Rahanpesun ja terrorismin rahoittaminen eivät ole siis ainoastaan yksittäisten valtioiden sisäisiä ongelmia. Globalisoitumisen vuoksi haasteet ovat yhteisiä ja niiden torjumiseksi tarvitaan kansainvälisiä ja yhtenäisiä toimintatapoja. Finanssilaitoksilla asiakkaan tunteminen on selonotto- ja ilmoitusvelvollisuuden ohella tärkein rahanpesua ja terrorismin rahoittamista estävä toimenpide. Jotta rahanpesua ja terrorismin rahoittamista pystytään torjumaan, tulee asiakkaan tuntemista koskevien menettelytapojen olla globaalisti yhtenäisiä[29].

Asiakkaan tuntemista koskeva normiperusta rakentuu EU-lainsäädännöstä, Suomen lainsäädännöstä ja eri viranomaistahojen, kuten Finanssivalvonnan sääntelystä[30]. EU-lainsäädäntö perustuu FATF:n suosituksiin. FATF on taloudellisen yhteistyön ja kehityksen järjestö OECD:n[31] alaisuudessa toimiva, hallitusten välinen toimintaryhmä, joka työskentelee rahanpesun ja terrorismin rahoittamisen vastustamisen parissa kansainvälisellä tasolla. Kansallinen rahanpesun ja terrorismin rahoittamisen estämisestä annettu laki vastaavasti perustuu EU:n lainsäädäntöön, eli voimassa olevaan rahanpesudirektiiviin, ja FATF:n vuonna 2004 antamiin suosituksiin.[32]

2.1.1. EU-lainsäädäntö

EU-lainsäädännössä on yhteensä neljä voimassa olevaa asiakkaan tuntemista sekä rahanpesua ja terrorismin rahoittamisen estämistä säätelevää asetusta ja direktiiviä, jotka ovat niin sanottu neljännes rahanpesudirektiivi[33], niin sanottu toinen maksajan tiedot -asetus[34],

[28] Finanssivalvonta 2017 b.
[29] Finanssivalvonta 2017 b.
[30] Finanssivalvonnan standardi 2.4 2015.
[31] *OECD* on lyhenne sanoista Organisation for Economic Co-operation and Development.
[32] Valtiovarainministeriö 2018.
[33] Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/849, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen, Euroopan parlamentin ja neuvoston asetuksen (EU) N:o 648/2012 muuttamisesta sekä Euroopan parlamentin ja neuvoston direktiivin 2005/60/EY ja komission direktiivin 2006/70/EY kumoamisesta.
[34] Euroopan parlamentin ja neuvoston asetus (EU) 2015/847, varainsiirtojen mukana toimitettavista tiedoista ja asetuksen (EY) N:o 1781/2006 kumoamisesta.

direktiivi rahoitusjärjestelmän käytön estämisestä rahanpesutarkoituksiin sekä terrorismin rahoitukseen[35] ja EU:n komission täytäntöönpanodirektiivi[36].[37] Toukokuussa 2018 on lisäksi säädetty neljännen rahanpesudirektiivin muuttamiseksi niin sanottu viides rahanpesudirektiivi[38], joka on saatettava jäsenmaissa voimaan viimeistään tammikuussa 2020. Euroopan komissio on myös jo suunnittelemassa viidettä rahanpesudirektiiviä täydentävää, niin sanottua kuudetta rahanpesudirektiiviä[39].

Yllä mainittujen direktiivien ja asetusten lisäksi terrorismin rahoittamista pyritään estämään YK:n ja EU:n asettamilla finanssipakotteilla. Finanssipakotteet kohdistuvat niihin tahoihin, jotka ovat joko osallistuneet terroritekoihin tai edistäneet niitä. Suomessa ulkoasiainministeriö koordinoi näiden pakotteiden noudattamisen valvontaa. Kuten aiemmin mainittiin, EU:n rahanpesudirektiivit perustuvat FATF:n antamiin suosituksiin.[40]

2.1.2. Suomen lainsäädäntö

Keskeisen kansallinen asiakkaan tuntemiseen liittyvä laki on laki rahanpesun ja terrorismin rahoittamisen estämisestä[41]. Asiakkaan tuntemista käsitellään myös monissa muissa erikoislaeissa. Näistä laeista mainittakoon laki luottolaitostoiminnasta[42], joka on lain rahanpesusta ja terrorismin rahoittamisen estämisestä lisäksi oleellisin laki tämän tutkielman kannalta.

Kansallinen laki rahanpesun ja terrorismin rahoittamisen estämisestä pohjautuu ns. neljänteen rahanpesudirektiiviin ja FATF:n vuonna 2004 antamiin suosituksiin[43]. Suomessa rahanpesun ja terrorismin rahoittamisen vastaisesta lainsäädännön kehittämisestä vastaa

[35] Euroopan parlamentin ja neuvoston direktiivi 2005/60/EY, rahoitusjärjestelmän käytön estämisestä rahanpesutarkoituksiin sekä terrorismin rahoitukseen.
[36] Komission direktiivi 2006/70/EY, Euroopan parlamentin ja neuvoston direktiivin 2005/60/EY täytäntöönpanotoimenpiteistä ”poliittisesti vaikutusvaltaisen henkilön” määritelmän sekä yksinkertaistettuja asiakkaan tuntemismenettelyjä sekä satunnaisesti tai hyvin rajoitetusti harjoitetun rahoitustoiminnan perusteella myönnettyjä poikkeuksia koskevien teknisten perusteiden osalta.
[37] Finanssivalvonta 2017 b.
[38]Euroopan parlamentin ja neuvoston direktiivi (EU) 2018/843, rahoitusjärjestelmän käytön estämisestä rahanpesuun tai terrorismin rahoitukseen annetun direktiivin (EU) 2015/849 ja direktiivien 2009/138/EY ja 2013/36/EU muuttamisesta.
[39] O’Connor 2018.
[40] Finanssivalvonta 2017 b.
[41] Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017.
[42] Laki luottolaitostoiminnasta 610/2014.
[43] Valtiovarainministeriö 2018.

sisäministeriö[44]. Sisäministeriö koordinoi rahanpesulaissa esitettyjen toimivaltaisten viranomaisten keskinäistä yhteistyötä[45].

Sisäministeriön lisäksi muita rahanpesuun ja terrorismin rahoittamisen estämiseen liittyviä viranomaistahoja ovat esimerkiksi valtiovarainministeriö ja poliisin alaisuudessa toimiva rahanpesun selvittelykeskus. Valtiovarainministeriö osallistuu neljästi vuodessa Euroopan neuvoston rahanpesun ja terrorismin rahoituksen vastaiseen asiantuntijatyöryhmään, jonka tarkoituksena on tarkastella tämänhetkisiä lainsäädäntöhankkeita, markkinailmiöitä ja kansainvälisen yhteistyön tilaa[46]. Rahanpesun selvittelykeskus on keskusrikospoliisin alaisuuteen vuonna 1988 perustettu yksikkö, jonka toimialaan kuuluvat rahanpesun ja terrorismin rahoittamisen estämiseen liittyvät erinäiset tehtävät[47].

2.1.3. Finanssivalvonta

Finanssivalvonta on hallinnollisesti Suomen Pankin yhteydessä toimiva, päätöksenteossaan itsenäinen rahoitus- ja vakuutusvalvontaviranomainen. Pankit kuuluvat useiden muiden tahojen ohella finanssivalvonnan valvottavien piiriin. Finanssivalvonnan tarkoituksena on ylläpitää finanssimarkkinoiden vakautta, turvata asiakkaiden etuja ja edesauttaa finanssimarkkinoiden toimintaan kohdistuvan yleisen luottamuksen säilyttämistä.[48]

Finanssivalvonnalla on sekä oikeus antaa määräyksiä, että valvoa näiden määräysten ja muiden säännösten noudattamista. Finanssivalvonnalla on muun muassa oikeus antaa määräyksiä koskien asiakkaan tuntemista sekä rahanpesun ja terrorismin rahoittamisen estämistä. Finanssivalvonta saa antaa määräyksiä asiakkaan tuntemisessa noudatettaviin menettelytapoihin sekä rahanpesun ja terrorismin rahoittamisen estämiseen liittyvään riskienhallintaan. Oikeus yllä mainittujen määräysten antamiseen on kirjattu useampaan kansalliseen lakiin, joista tämän tutkielman kannalta tärkeimpänä mainittakoon laki luottolaitostoiminnasta.[49] Määräysten lisäksi Finanssivalvonnalla on laissa rahanpesun ja terrorismin rahoittamisen estämisestä annettu mandaatti valvoa finanssialalla toimivien tahojen säännösten ja määräysten noudattamista.

---

[44] Finanssivalvonta 2017 b.
[45] Sisäministeriö 2018.
[46] Valtiovarainministeriö 2018.
[47] Poliisi 2018.
[48] Finanssivalvonta 2017 c.
[49] Finanssivalvonnan standardi 2.4 2015.

2.2. Tietosuojalainsäädäntö

Noudattaessaan rahanpesulakia asiakkaan tuntemiseen liittyvissä toimenpiteissä pankki kohtaa myös toisen, päinvastaista intressiä ajavan lain: Euroopan unionin yleisen tietosuoja-asetuksen. Kuluttajien huoli yksityisyyden suojaa ja henkilötietojen käsittelyä kohtaan on kasvanut[50] verkostoituneessa yhteiskunnassamme, jossa henkilötietoja kerätään yhä kasvavassa määrin erilaisiin tarkoituksiin[51]. Yksityisyyden suoja ja henkilötietojen käsittely on vahvasti läsnä asiakkaan tuntemiseen liittyvissä toimenpiteissä, sillä kaikissa asiakkaan tuntemisen vaiheissa käsitellään asiakkaan henkilötietoja. Pankin toiminnan on siis oltava rahanpesulain lisäksi myös tietosuoja-asetuksen edellyttämien säännösten mukaista.

Tietosuojalainsäädäntö perustuu ensisijaisesti Euroopan unionin tietosuoja-asetukseen sekä tulevaan kansalliseen tietosuojalakiin. Lainsäädännön lisäksi tietosuojavaltuutetun toimistolla on merkittävä rooli valvojana sekä neuvojana tietosuoja-asioihin ja henkilötietojen käsittelyyn liittyvissä kysymyksissä[52].

2.2.1. EU-lainsäädäntö

Uudistunut tietosuojalainsäädäntö perustuu 25.5.2018 voimaan astuneeseen Euroopan unionin tietosuoja-asetukseen, jolla korvattiin vuoden 1995 henkilötietodirektiivi[53]. Tietosuoja-asetusta on sovellettava välittömästi sellaisenaan kaikissa jäsenmaissa[54]. Tietosuoja-asetuksella vahvistetaan säännöt luonnollisten henkilöiden suojelulle henkilötietojen käsittelyssä sekä säännöt, jotka koskevat henkilötietojen vapaata liikkuvuutta. Asetuksen tarkoituksena on suojella luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan.[55]

Siitä huolimatta, että kumotun tietosuojadirektiivin ja nykyisen tietosuoja-asetuksen välillä on reilusti yli kaksikymmentä vuotta, kuten tietosuojavaltuutettu Reino Aarniokin tuo esiin tietosuojavaltuutetun toimiston blogissaan, moni asia pysyy myös samana uuden asetuksen myötä[56]. Ennen tietosuoja-asetusta henkilötietojen käsittelyssä ensisijaisesti

[50] Graeff & Harmon 2002: 302.
[51] Pitkänen 2014: 202.
[52] HE 9/2018 vp: 10.
[53] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
[54] Tietosuojavaltuutetun toimisto 2018 a.
[55] Yleinen tietosuoja-asetus 2016/679: 1 artiklan 1 ja 2 kohta.
[56] Aarnio 2018.

sovellettu henkilötietolaki sisältää paljon samoja asioita kuin tietosuoja-asetus. Henkilötietolaissa kirjatut rekisteröidyn oikeudet pysyvät siis ennallaan. Näiden jo olemassa olevien oikeuksien rinnalle tulee myös uusia oikeuksia, jotka Eija Warman mukaan lisäävät rekisteröidyn mahdollisuuksia kontrolloida omia tietojaan[57].

2.2.2. Suomen lainsäädäntö

Hallitus on antanut eduskunnalle esityksen EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi, jossa ehdotetaan säädettäväksi tietosuojalaki. Lain tarkoituksena olisi täydentää ja täsmentää EU:n yleistä tietosuoja-asetusta.[58] Samalla kumottaisiin tämänhetkinen henkilötietolaki sekä laki tietosuojalautakunnasta ja tietosuojavaltuutetusta. Tietosuojalain käsittely on vielä eduskunnassa kesken. Lain valmistumiseen asti sovelletaan henkilötietolakia, poikkeuksena tietosuoja-asetuksen kanssa ristiriidassa olevat säädökset, joita ei EU-oikeuden etusijaperiaatteen vuoksi sovelleta.[59]

Tulevan tietosuojalain ja nykyisen henkilötietolain lisäksi henkilötietojen käsittelystä säädetään myös muissa kansallisissa erikoislaeissa. Näistä laeista pankin käsittelemien henkilötietojen kannalta tärkein on luottotietolaki[60], jota sovelletaan luottotietojen keräämiseen, tuottamiseen, tallettamiseen, luovuttamiseen, käyttöön ja muuhun käsittelyyn[61].

2.2.3. Tietosuojavaltuutetun toimisto

Tietosuojavaltuutetun toimisto on asiantuntijaorganisaatio, joka on perustettu vuonna 1987 turvaamaan ihmisten oikeuksia ja vapauksia henkilötietojen käsittelyssä. Tietosuojavaltuutetun toimisto on itsenäinen ja riippumaton viranomainen. Tietosuojavaltuutetun toimiston tarkoituksena on valvoa, että henkilötietoja käsitellään lainmukaisesti ja varmistaa tietosuojaoikeuksien toteutuminen. Tietosuojavaltuutetun toimiston tehtävänkuva on laaja, ulottuen aina valvonnasta hallinnollisten määräysten antamiseen, ja henkilötietojen käsittelyä koskevan tietoisuuden levittämiseen.[62]

---

[57] Juntunen 2016.
[58] HE 9/2018 vp: 1.
[59] Tietosuojavaltuutetun toimisto 2018 b.
[60] Luottotietolaki 11.5.2007/527.
[61] Luottotietolaki 11.5.2007/527: 1.1.
[62] Tietosuojavaltuutetun toimisto 2018 c.

Tietosuojavaltuutetun toimiston merkittävimpiä tehtäviä on valvoa tietosuoja-asetuksen ja muiden henkilötietojen käsittelyä koskevien lakien noudattamista, sekä määrätä hallinnollisia seuraamuksia, jos henkilötietojen käsittelyssä ilmenee rikkomuksia. Näiden tehtävien lisäksi tietosuojavaltuutetun toimistolla on lukuisia muita toimenkuvia, joista mainittakoon tietoisuuden edistäminen henkilötietojen käsittelyä koskevissa kysymyksissä, sekä yhteistyö muiden EU:n tietosuojaviranomaisten kanssa.[63]

2.3. Rahanpesulain ja tietosuoja-asetuksen rajapinta

Rahanpesu- ja tietosuojalainsäädännöllä on toisiinsa nähden hyvin erilaiset tarkoitusperät. Rahanpesulainsäädännön tavoitteena on estää rahanpesua ja terrorismin rahoittamista, edistää tällaisen toiminnan paljastamista ja selvittämistä sekä tehostaa rikoksen tuottaman hyödyn jäljittämistä ja takaisinsaantia[64]. Tietosuoja-asetuksen tarkoituksena on vastaavasti suojella luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan[65]. Rahanpesulainsäädännön tarkoituksena on siis kiteytettynä estää rahanpesua ja terrorismin rahoittamista, kun taas tietosuojalainsäädännön tarkoituksena on suojella luonnollisten henkilöiden yksityisyyttä ja henkilötietojen käsittelyä.

Rahanpesun ja terrorismin rahoittamisen takana on aina luonnollinen henkilö, vaikka oikeushenkilöitä käytettäisiinkin rikollisten tarkoitusperien saavuttamiseen. Jotta rikollinen toiminta pystytään joko havaitsemaan tai poissulkemaan, tulee mahdollisten tekojen takana olevasta luonnollisesta henkilöstä kerätä mahdollisimman paljon tietoa. Tietosuojalainsäädännön tarkoituksena taas on suojella luonnollisten henkilöiden yksityisyyttä henkilötietojen käsittelyn sääntelyn kautta.

Suurimmat ongelmat ja ristiriidat rahanpesu- ja tietosuojalainsäädännön yhdistämisestä pankin näkökulmasta kulminoituvat ensisijaisesti kerätyn tiedon käsittelyyn lukuisista eri näkökulmista katsottuna. Juurikin tieto, sen kerääminen ja käsittely ovat tekijöitä, jotka aiheuttavat intressikonfliktin näiden kahden lain välille. Lainsäädännön vastakkaisten intressien ydin onkin yksityisyyden suojan ja yhteiskunnan turvallisuuden vastakkainasettelussa, mikä aiheuttaa väistämättä ristiriitoja.

---

[63] Tietosuojavaltuutetun toimisto 2018 c.
[64] RahanpesuL 1:1.
[65] Yleinen tietosuoja-asetus 2016/679: 1 artiklan 1 kohta.

Rahanpesu- ja tietosuojalainsäädännön vertaileminen on tutkimuskohteena hyvin uusi tuoreiden lainsäädäntöjen vuoksi, eikä vertailevaa, tieteellistä materiaalia näin ollen juurikaan ole saatavilla. Tästä johtuen tutkimuskysymyksiin ei ole olemassa valmiita vastauksia, vaan oikeudentila on jokseenkin määrittelemätön ja tulkinnanvarainen. Tutkimuskysymyksiin pyritään löytämään vastaus perehtymällä lukuisiin eri oikeuslähteisiin ja tekemällä näiden perusteella tulkintoja, päätelmiä ja kannanottoja.

3. ASIAKKAAN TUNTEMINEN

3.1. Asiakkaan tuntemisen taustaa

Rahanpesun torjunta muodostuu sekä ennaltaehkäisevistä että jälkikäteisistä toimista. Ennaltaehkäisevät, eli preventiiviset toimenpiteet ovat muotoutuneet alun perin rahoituslaitosten kansainvälisen yhteistyön myötä, kun taas jälkikäteisillä, eli repressiivisillä keinoilla on pyritty estämään rikollisella toiminnalla saatujen varojen saattaminen joko esirikoksen suorittaneen tahon käyttöön tai uusien rikosten rahoittamiseen. Merkittävä preventiivinen keino rahanpesun ja terrorismin rahoittamisen torjumiseksi on laissa rahanpesun ja terrorismin rahoittamisen estämisestä erinäisille yhteisöille ja elinkeinonharjoittajalle asetettu ilmoitusvelvollisuus, jonka perusteella esimerkiksi pankkien on ilmoitettava rahanpesun selvittelykeskukselle havaitsemistaan epäilyttävistä liiketoimista.[66] Jotta epäilyttävien liiketoimien havaitseminen ja siitä ilmoittaminen on mahdollista, tulee pankkien muiden rahanpesulaissa esitettyjen toimijoiden ohella tuntea asiakkaansa.

Asiakkaan tunteminen muodostaakin rahanpesulain keskeisen velvoitteen[67], sillä ilman asiakkaan tuntemiseen liittyviä toimenpiteitä ei myöskään pystytä havaitsemaan epäilyttävään liiketoimeen viittaavia poikkeavia tapahtumia ja käyttäytymismalleja. Pankkien tulee tuntea asiakkaansa koko asiakassuhteen keston ajan; ei riitä, että tiedot päivitetään kertaalleen asiakassuhdetta perustettaessa. Asiakkaan käyttäytymismallit voivat lain ohella muuttua asiakassuhteen aikana, minkä vuoksi on tarpeellista päivittää asiakkaan tuntemistietoja säännöllisin väliajoin. Rahanpesulain asettamien velvoitteiden lisäksi myös tietosuoja-asetus edellyttää, että asiakkaasta kerättävät tiedot ovat tarpeellisia ja virheettömiä, joten on huolehdittava siitä, että tiedot ovat sekä oikein että ajan tasalla.[68]

Asiakkaan tuntemisen velvoitteet perustuvat EU:n lainsäädäntöön, Suomen lainsäädäntöön ja Finanssivalvonnan sääntelyihin[69]. Laissa rahanpesun ja terrorismin rahoittamisen estämisessä on säädetty tarkat vähimmäistiedot, jotka pankin on hankittava asiakkaistaan täyttääkseen velvoitteensa asiakkaan tuntemisesta. Osa rahanpesulain tiedoista on yksityiskohtaisia, kun taas osa kohdista on jätetty väljemmiksi, mahdollistaen näin pankkien

[66] Lahti & Koponen 2007: 151-152.
[67] Finanssivalvonnan standardi 2.4 2015.
[68] Finanssivalvonta 2016.
[69] Finanssivalvonnan standardi 2.4. 2015.

riskiperusteisen harkinnan.[70] Pankeilla tulee olla valtuudet arvioida kuhunkin asiakkuuteen liittyvät riskit, ja arvionsa perusteella tehdä päätös asiakkaasta kerättävän tiedon määrästä ja laadusta. Toimimalla näin pankit sekä optimoivat rajallisten resurssiensa käytön että asiakkaan yksityisyyden säilymisen. Rahanpesun ja terrorismin rahoittamisen ilmenemismuotoja on lisäksi mahdotonta ennakoida, minkä vuoksi lainsäädäntö ei voi olla yksiselitteinen ja joustamaton. Antamalla pankeille valtuudet tietyissä rajoissa päättää myös esitetyistä kysymyksistä varmistetaan, että pankit voivat sopeuttaa asiakkaan tuntemiseen liittyvät toimenpiteet kulloiseenkin tilanteeseen sopivaksi.

Seuraavassa alaluvussa 3.2. määritellään tarkemmin, mitä asiakkaan tuntemisella tarkoitetaan ja millaisia tekijöitä asiakkaan tunteminen pitää sisällään. Luvussa esitellään asiakkaan tunnistamisen ja tuntemisen käsitteet, sekä asiakassuhteen perustamisen edellytykset. Luvussa sivutaan lyhyesti myös asiakkaan jatkuvaa seurantaa, tietojen käsittelyä ja dokumentointia, sekä selonotto- ja ilmoitusvelvollisuutta.

3.2. Asiakkaan tuntemisen määritelmä

Kuten aiemmassa kappaleessa kävi jo ilmi, pankeilla on lakiin perustuva velvollisuus sekä tunnistaa että tuntea asiakkaansa, mikä muodostaa rahanpesulain keskeisen velvoitteen[71]. Asiakkaan tuntemisella tarkoitetaan pankin velvollisuutta sekä tunnistaa että tuntea asiakkaansa ja tämän toiminnan laadun ja laajuuden. Asiakkaan tunteminen käsittää sekä asiakkaan tunnistamisen että asiakkaan kokonaisvaltaisen tuntemisen. Asiakkaan tunnistamisella tarkoitetaan asiakkaan oikeasta henkilöllisyydestä varmistumista henkilöllisyyden todentamisen avulla. Asiakkaan kokonaisvaltainen tunteminen tarkoittaa asiakkaan toiminnan ja taustojen tuntemista asiakassuhteen vaatimalla laajuudella.[72] Asiakkaan tunteminen edellyttää myös riskien hallintaa uusien asiakkuuksien avaamisen kohdalla, transaktioiden monitorointia ja eri asiakkuuksille suunnattuja menettelytapoja[73].

Asiakkaan tunteminen alkaa siitä hetkestä, kun asiakas haluaa avata asiakkuuden pankissa. Asiakas ja pankki sopivat asiakkuuden ehdoista, minkä jälkeen asiakas luovuttaa

[70] Finanssivalvonta 2017 a.
[71] Finanssivalvonnan standardi 2.4. 2015.
[72] Finanssivalvonnan standardi 2.4. 2015.
[73] Parra Moyano & Ross 2017: 412.

pankille pankin tarvitsemat tiedot asiakkaan tunnistamiseksi ja tuntemiseksi. Pankki analysoi saamansa tiedot, joiden perusteella luodaan sisäinen dokumentaatio[74] asiakkuudesta. Dokumentaation tarkoituksena on todentaa viranomaisille, että asiakkuus on joko hyväksytty tai hylätty, ja asiakkaan tuntemistiedot on asianmukaisesti kerätty ja dokumentoitu.[75]

Asiakkaan tunteminen on koko asiakassuhteen ajan kestävä, jatkuva prosessi, eikä asiakkaan tunteminen siten rajoitu ainoastaan hetkeen, jolloin asiakassuhde perustetaan. Asiakkaan tuntemisen tulee lain mukaan olla jatkuvaa ja tietojen on oltava sekä oikeita että ajan tasalla.[76] Asiakassuhdetta ei siten tule perustaa tai ylläpitää, jos asiakkaan tuntemistiedot ovat pankin oman riskiperusteisen arvion perusteella puutteellisia[77]. Asiakkaan jatkuva tunteminen on tärkeää, sillä asiakkaan käyttäytyminen voi muuttua asiakassuhteen keston aikana. Asiakassuhteen perustamishetken käytös voi olla lainmukaista, kun taas myöhemmät tapahtumat saattavat indikoida rahanpesua tai terrorismin rahoittamista. Myös pankin monitorointijärjestelmät kehittyvät alati, minkä vuoksi epäilyttäviä toimia ei välttämättä ole pystytty vielä asiakassuhteen alussa havaitsemaan nykyhetken näkökulmasta puutteellisten järjestelmien takia.

Asiakkaan tunnistamisen ja tuntemistietojen hankkimisen lisäksi asiakkaan tuntemistietoja tulee siis päivittää säännöllisin väliajoin ja asiakkuuden kehittymistä on seurattava koko asiakassuhteen keston ajan. Tuntemistiedot on dokumentoitava asiallisesti ja niitä tulee säilyttää lain asettamaan määräaikaan asti. Yllä mainittujen toimien lisäksi asiakkaan tuntemiseen liittyvät toimenpiteet kattavat myös selonotto- ja ilmoitusvelvollisuuden.

Pankin on kaikissa asiakkaan tuntemisen vaiheissa, mukaan lukien selonotto- ja ilmoitusvelvollisuuteen liittyvissä toimenpiteissä, otettava huomioon tietosuoja-asetuksen mukaiset vaatimukset tietojenkäsittelylle. Edellä mainitut toimenpiteet sisältävät hyvin erilaisia tietojenkäsittelyn muotoja, joihin kohdistuu täten erilaisia velvollisuuksia. Näitä velvollisuuksia käsitellään tarkemmin luvussa 4.

[74] *Sisäisellä dokumentaatiolla* tarkoitetaan asiakkaan KYC-tietolomaketta.
[75] Parra Moyano & Ross 2017: 412.
[76] Finanssivalvonta 2016.
[77] Finanssiala ry 2016.

Seuraavassa alaluvussa 3.3. käydään läpi pankkien harjoittamaa riskiperusteista arviointia asiakkaan tuntemisen toimenpiteissä. Luvussa tuodaan esiin asiakkuuksiin kohdistuvien riskien arvioinnin välttämättömyys, sekä riskiarvion suorittamiseen kehitetyt työkalut.

3.3. Riskiperusteinen arviointi

Pankeilla on suuri riski altistua käytettäväksi rahanpesullisiin tarkoituksiin, minkä vuoksi pankkien on tärkeää pystyä arvioimaan asiakkaisiinsa kohdistuvat riskit[78]. Rahanpesulain mukaan pankin on asiakassuhteeseen liittyviä rahanpesun ja terrorismin rahoittamisen riskejä arvioidessaan otettava huomioon asiakkaisiin, maihin tai maantieteellisin alueisiin, tuotteisiin, palveluihin ja liiketoimiin sekä jakelukanaviin liittyvät rahanpesun ja terrorismin rahoittamisen riskit[79]. Pankin tulee siis suhteuttaa asiakkaan tuntemiseen liittyvät toimenpiteet ottaen huomioon kokonaisvaltaisesti asiakkaan aiheuttamat riskit rahanpesun ja terrorismin rahoittamisen näkökulmasta. Jos pankki arvioi, että asiakkuuteen liittyy kesimääräistä suurempi väärinkäytösriski rahanpesun ja terrorismin rahoittamisen näkökulmasta, tulee asiakkaaseen tällöin kohdistaa tehostettuun tuntemiseen liittyviä toimenpiteitä[80].

Pankille ei ole tarkoituksenmukaista tai rajallisten resurssien puitteissa edes mahdollista monitoroida jokaista asiakkuutta samalla laajuudella ja tarkkuudella. Pankin tuleekin fokusoitua niihin asiakkuuksiin, jotka vaativat sekä lain että pankin oman riskiarvion perusteella tarkempaa valvontaa[81]. Pankilla on kuitenkin velvollisuus kohdistaa asianmukaiset toimenpiteet myös niihin asiakkuuksiin, joiden voidaan nähdä muodostavan rahanpesun ja terrorismin rahoittamisen näkökulmasta alhaisemman riskin. Näihin asiakkuuksiin voidaan kuitenkin kohdistaa standardoidumpia tuntemistoimenpiteitä.[82]

Tarkoituksenmukaisuuden ja resurssienhallinnan lisäksi pankin tulee ottaa toiminnassaan huomioon myös tietosuoja-asetuksen asettamat velvoitteet tietojenkäsittelylle. Tietosuoja-asetuksen oletusarvoista tietosuojaa[83] käsittelevän 25 artiklan toisen kohdan perus-

[78] Mat Isa, Sanusi, Haniff, Barnes 2015: 7.
[79] RahanpesuL 3:1:2.
[80] Finanssivalvonnan standardi 2.4. 2015.
[81] Ramage 2012: 273.
[82] de Wit 2007: 161.
[83] Oletusarvoinen tietosuoja tunnetaan paremmin englanninkielisenä terminä *privacy by default*.

teella rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa.

Oletusarvoisen tietosuojan noudattaminen on oleellista riskiperusteista arviota suorittaessa, sillä tehostetun tuntemisen tason valinta vaikuttaa merkittävästi erityisesti kerättyjen henkilötietojen määrään, laajuuteen ja käsittelyaikaan. Yksi oletusarvoisen tietosuojan pääperiaatteista on tiedon minimointi, jolla tarkoitetaan henkilötietojen käsittelyn rajaamista mahdollisimman minimaaliseen määrään[84]. Tietojen rajaamisella mahdollisimman pieneen määrään tarkoitetaan sitä, että asiakkaasta tulisi kerätä vain tiettyä, rajattua tarkoitusta varten oleellinen määrä tietoa.[85] Oli kyseessä sitten yksinkertaistettu tai tehostettu tunteminen, tulee kerättyjen tuntemistietojen tuntemisen tasosta huolimatta vastata sitä tarkoitusta, mihin tiedot on kerätty.

Pankin tulee siis pystyä tunnistamaan asiakkuuksiin liittyvät riskit, jotta voidaan tehdä päätös sen suhteen, täyttääkö asiakkuus korkean riskin asiakkaan tunnusmerkit, vai voidaanko asiakas luokitella vähäisen riskin asiakkaaksi. Ensimmäinen arvio tehdään luonnollisesti uusien asiakkuuksien kohdalla asiakassuhdetta perustettaessa. Asiakkuuden perustamisen jälkeen asiakkaan jatkuva tunteminen etenee asiakkuuden muodostamien riskien puitteissa, missä pankin sisäiset, monitorointiin tarkoitetut järjestelmät ovat tärkeässä asemassa.[86]

Pankilla tulee olla käytössään asianmukaiset järjestelmät sen arvioimiseen, millaisia riskejä asiakkaat aiheuttavat liiketoiminnalle. Näiden järjestelmien tarkoituksena on tukea asiakkaan tuntemiseen liittyviä toimintatapoja sekä estää väärinkäytöksiä. Järjestelmien ei tarvitse muodostaa muusta liiketoiminnasta erillistä kokonaisuutta, vaan ne voivat olla osa pankin yleistä riskienhallintaa ja sisäistä tarkastusta.[87] Järjestelmien tarkoituksena on muun muassa mahdollistaa transaktioiden automaattinen monitorointi, jota ei ole mahdollista suorittaa rajallisten resurssien vuoksi manuaalisesti henkilöstön voimalla[88].

Järjestelmien käyttö keinona havainnoida rahanpesua ja terrorismin rahoittamista kohtaa haasteita tietosuoja-asetuksen näkökulmasta, sillä järjestelmän tuottama automaattinen

[84] Romanou 2018: 103.
[85] Koops, Hoepman & Leenes 2013:679.
[86] de Wit 20017: 158.
[87] Finanssivalvonnan standardi 2.4. 2015.
[88] de Wit 2007: 159.

data voidaan nähdä tietosuoja-asetuksen mukaisena profilointina. Tietosuoja-asetuksessa profiloinnilla tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin.[89] Rahanpesun ja terrorismin rahoittamisen estämisen näkökulmasta profiloinnin kieltämisellä voitaisiin olla ajautumatta vääriin ja virheellisiin tulkintoihin[90], ja näin ollen suojella asiakkaiden henkilötietoja.

Vaikkakin profilointi voidaan nähdä ongelmallisena rahanpesun ja terrorismin rahoittamisen estämisen, ja sitä tukevan tutkinnan kontekstissa, on automaattisen tietojenkäsittelyn käyttämättä jättäminen käytännössä mahdotonta suurien tietomassojen takia. On myös otettava huomioon mahdollisen profiloinnin pois jättämisen vaikutukset asiakkaiden henkilötietojen käsittelyyn. Ilman profilointia pankki joutuisi manuaalisesti tarkistamaan kaikkien asiakkaiden tiedot, jolloin asiakkaiden yksityisyyden suoja vaarantuisi huomattavasti enemmän. Mahdollinen ratkaisu profiloinnin luomiin ongelmiin olisikin kehittää automaattista tietojenkäsittelyä havaitsemaan paremmalla tarkkuudella epäilyttävät tapahtumat normaalista, jolloin tosiasiallisesti ei-rikollisten asiakkaiden henkilötietoja ei jouduttaisi käsittelemään.

Rahanpesun ja terrorismin rahoittamisen estämisen tekee haastavaksi muun muassa kyseisten aktiviteettien monimuotoisuus, kansainvälisyys ja jatkuvasti muuttuva toimintaympäristö. Pankkien osalta näiden haasteiden selättämisessä keskeisessä asemassa ovat monitorointiin tarkoitetut järjestelmät ja pankin oma riskiperusteinen arvio. Riskiperusteisen arvion avulla pystytään keskittymään niihin asiakkuuksiin, joiden kohdalla nähdään kohonnut riski. Riskiperusteinen arvio mahdollistaa resurssien keskittämisen epäilyttäviin tapahtumiin, unohtamatta kuitenkaan myös muiden asiakkuuksien rutiininomaisempaa seurantaa. Kyse on siis riskienhallinnasta ja resurssien tarkoituksenmukaisesta kohdentamisesta. Riskiperusteinen arvio onkin yksi neljännen rahanpesudirektiivin keskeisistä muutoksista aiempaan direktiiviin verrattuna.

Seuraavassa alaluvussa 3.4. syvennytään tarkemmin asiakkaan tunnistamiseen ja tuntemiseen, ja määritellään näiden kahden käsitteen välinen ero. Luvussa perehdytään myös pankin riskiperusteiseen arviointiin näitä toimia suorittaessa.

[89] Yleinen tietosuoja-asetus 2016/679: 4 artiklan 4 kohta.
[90] Koops ym. 2013: 685.

3.4. Tunnistaminen ja tuntemistietojen hankkiminen

Pankeilla on lakiin perustuva velvollisuus sekä tunnistaa että tuntea asiakkaansa. Asiakkaan tunteminen kattaa kaikki asiakkaasta kerätyt tiedot ja tietojen käsittelyyn liittyvät toimenpiteet koko asiakassuhteen kattamalta ajalta. Asiakkaan tunnistaminen sisältyy asiakkaan tuntemiseen, mutta on itsessään asiakkaan tuntemista suppeampi käsite. Lain mukaan asiakas on tunnistettava ja tämän henkilöllisyys todennettava vakituista asiakassuhdetta perustettaessa[91]. Asiakas on lisäksi tunnistettava ja tämän henkilöllisyys todennettava muun muassa silloin, jos aiemmin todennetun asiakkaan henkilöllisyyden todentamistietojen luotettavuutta tai riittävyyttä on syytä epäillä[92]. Asiakkaan tunnistamisella tarkoitetaan siis asiakkaan henkilöllisyydestä varmistumista vakituista asiakassuhdetta perustettaessa ja muissa laissa määritetyissä erityistilanteissa. Finanssivalvonnan mukaan vakituiseksi asiakkuudeksi määritellään sellainen asiakas, joka muun muassa avaa tilin, ryhtyy luottosuhteeseen tai solmii arvopaperivälityssopimuksen pankin kanssa[93].

Pankeilla on pääsääntöisesti velvollisuus tarjota asiakkaille peruspankkipalvelut, eli talletustili ja maksukortti. Luottolaitostoiminnasta annetussa laissa on kuitenkin määrätty poikkeus tähän, sillä talletuspankki saa kieltäytyä tavanomaisen talletustilin avaamisesta ja tilin käyttöön tarkoitetun välineen myöntämisestä tai maksupalvelua koskevan toimeksiannon hoitamisesta ETA-valtiossa laillisesti oleskelevalle luonnolliselle henkilölle vain, jos kieltäytymiselle on painava peruste. Perusteen tulee liittyä asiakkaaseen, hänen aiempaan käyttäytymiseensä tai siihen, ettei asiakassuhteelle ilmeisesti ole todellista tarvetta. Kieltäytymisen peruste on ilmoitettava asiakkaalle.[94]

Yksi esimerkki painavasta syystä on se, ettei pankki pysty tunnistamaan asiakastaan. Pankilla on oikeus kieltäytyä asiakassuhteen perustamisesta esimerkiksi sellaisen tahon kanssa, joka kieltäytyy antamasta riittäviä tietoja itsestään tai toiminnastaan. Pankilla ei siis lain mukaan saa olla tunnistamattomia, eli anonyymeja asiakkaita, mikä onkin yksi esimerkki painavasta syystä kieltäytyä tarjoamasta asiakkaalle edes vähimmäisvaatimuksen mukaisia peruspankkipalveluita. Myös asiakassuhteen tai toimeksiannon muodostaessa kesimääräistä suuremman riskin rahanpesun tai terrorismin osalta, voidaan asiakassuhde jättää perustamatta tai toimeksianto suorittamatta.[95]

---

[91] RahanpesuL 3:2:1.
[92] RahanpesuL 3:2:1:n 4 kohta.
[93] Finanssivalvonta 2017 b.
[94] LuottoL 15:6 :1.
[95] Finanssivalvonnan standardi 2.4. 2015.

Asiakas tunnistetaan ja henkilöllisyys todennetaan asiakkaan toimittaman asiakirjan perusteella. Asiakkaan on oltava asiakirjasta tunnistettavissa ja henkilötiedot yksiselitteisesti todennettavissa. Asiakkaan henkilöllisyys voidaan todentaa joko viranomaisen myöntämän henkilöllisyystodistuksen tai vahvan sähköisen tunnistautumisen kautta, riippuen siitä, tapahtuuko asiakkuuden perustaminen asiakkaan ollessa henkilökohtaisesti läsnä vai etänä verkkotapaamisen yhteydessä. Pankki voi oman riskienhallintaperiaatteensa mukaan päättää, mitkä asiakaskirjat hyväksytään henkilöllisyyden todentamiseksi. Yleisesi kuitenkin katsotaan, että passi ja henkilökortti ovat niiden myöntämisprosessin osalta esimerkiksi ajokorttia varmempi henkilöllisyyden todentamisen väline.[96]

Henkilöllisyystodistuksia käsitellessä tulee olla erityisen tarkka, sillä henkilöstä otetut kasvokuvat, joita käytetään esimerkiksi passeissa ja ajokorteissa, luetaan biometrisiksi tiedoiksi[97] niissä esiintyvien, yksilöllisen tunnistamisen mahdollistavien fyysisten piirteiden vuoksi[98]. Biometrisillä tiedoilla tarkoitetaan kaikkia luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa[99].

Lähtökohtaisesti biometristen tietojen käyttäminen on kiellettyä tietosuoja-asetuksen 9 artiklan 1 kohdan nojalla. Artikla esittää kuitenkin poikkeustilanteita, joissa kyseisten tietojen käsittely on sallittua. Asiakkaan tuntemista koskevissa toimenpiteissä voidaan nähdä täyttyvän artiklan 2 kohdan 1 alakohta, jonka mukaan tietoja saa käsitellä, jos rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten, sillä asiakkaalle tulee ilmoittaa tietojen käyttämisestä rahanpesun ja terrorismin rahoittamisen estämiseen[100].

Kansainvälisissä rahanpesuun liittyvissä regulaatioissa on kiinnitetty huomiota etenkin asiakassuhteen perustamishetkeen, joka on asiakkaan ja pankin välisen suhteen kannalta erittäin tärkeä ja ratkaiseva. Perustamishetkellä hankittua tietoa käytetään päivitettävien tietojen ohella koko asiakassuhteen keston ajan, joten asiakkaan henkilöllisyydestä ei saa

[96] Finanssivalvonta 2017 a.
[97] Romanou 2018: 104.
[98] Tikkinen-Piri, Rohunen & Markkula 2018:139.
[99] Yleinen tietosuoja-asetus 2016/679: 4 artiklan 14 kohta.
[100] RahanpesuL 3:3.4.

olla epäilyksiä[101] ja asiakkaan tuntemistietojen tulee olla virheettömiä. Asiakkaan tunnistamiseen liittyvien prosessien lisäksi pankin tulee myös tuntea asiakkaansa, eli olla tietoinen asiakkuuteen liittyvistä oleellisista asioista, kuten varallisuudesta ja maksuliikenteestä.[102] Kun asiakkaan käyttäytyminen on pääpiirteittäin pankin tiedossa, pystytään välttämättään mahdolliset epäselvyydet liittyen asiakkaan maksuliikenteeseen. Jos asiakkaan monitoroinnin yhteydessä huomataan esimerkiksi ulkomaille kohdistuvia suorituksia, ei asiakasta tarvitse välttämättä tavoitella tapahtumiin liittyen, jos tiedot ulkomaanmaksuliikenteestä on jo kirjattu asiakkaan tuntemistietoihin.

Rahanpesulaissa määritellään ne tiedot, joita pankin on hankittava asiakkaistaan, jotta voidaan katsoa asiakkaan tuntemisen täyttyneen. Osa tiedoista on määritelty yksiselitteisesti, kun taas joidenkin tietojen kohdalla on jätetty myös pankille varaa toteuttaa omaa riskiperusteista arviotaan. Kun asiakkaalle avataan peruspankkipalvelut, eli maksutili, maksukortti ja verkkopankki, tulee pankin tietää asiakkaastaan perustietojen[103] lisäksi, onko asiakas poliittisesti vaikutusvaltainen henkilö tai kuuluuko asiakas tällaisen henkilön lähipiiriin, mikä on asiakkaan taloudellista elämäntilannetta kuvaava status[104], onko kyseessä asiakkaan pääasiallinen pankkiasiakkuus ja mistä asiakkaan varallisuus on peräisin. Pankin on myös saatava asiakkaalta tämän arvio säännöllisen maksuliikenteen määrästä sekä mahdollisista ulkomaanmaksuista ja niiden perusteista.[105]

Näiden tietojen lisäksi pankilla on oikeus kysyä asiakkaalta tuntemiseen liittyviä lisäkysymyksiä asiakkuuden laadun ja laajuuden perusteella. Pankilla on lisäksi tarvittaessa oikeus pyytää asiakkaalta dokumentaatiota selvityksen tueksi.[106] Tämä korostuu etenkin selonottovelvollisuuden yhteydessä, kuten jäljempänä kappaleessa 5.2. ilmenee.

Henkilötietoja kerätessä ja käsiteltäessä on huomioitava, että tietoja tulee kerätä vain tehtävän vaativa tarpeellinen määrä[107], minkä lisäksi henkilötietojen on oltava asianmukaisia ja olennaisia[108]. Henkilötietoja ei voi siis kerätä ylettömissä määrin tai varmuuden vuoksi, vaan kerättävien tietojen tulee perustua johonkin nimenomaiseen tarkoitukseen, ja tietojen keräämisen tarkoituksena tulee olla jonkin tietyn tehtävän suorittaminen.

---

[101] Demetriades 2016: 80.
[102] de Wit 2007: 159.
[103] Perustietoja ovat esimerkiksi henkilön nimi, osoite, henkilötunnus ja kansalaisuus.
[104] Elämäntilannetta kuvaava status voi olla esimerkiksi opiskelija, eläkeläinen ja palkansaaja.
[105] Finanssivalvonta 2017 a.
[106] Finanssivalvonta 2017 a.
[107] Tikkinen-Piri ym. 2018:139; Lindroos-Hovinheimo 2018: 62.
[108] Yleinen tietosuoja-asetus 2016/679: 5 artiklan 1 kohdan c alakohta.

Seuraavissa alaluvuissa (3.5., 3.5.1., 3.5.2. ja 3.5.3.) käsitellään tarkemmin asiakkaan tuntemisen tasoja ja tuntemisen tasoon vaikuttavia tekijöitä. Luvuissa korostetaan pankin oman riskiarvion merkitystä tuntemistason valinnassa, unohtamatta lakiin perustuvia vaatimuksia.

3.5. Tuntemisen tasot

Asiakkaan tuntemiseen liittyvät toimenpiteet määräytyvät riskiperusteisesti asiakkuudesta riippuen. Asiakkuuteen liitettävää riskiä voidaan määritellä muun muassa asiakastyypin, asiakkaan yritysyhteyksien ja tilitapahtumien perusteella[109]. Jotta pankki pystyy tunnistamaan epäilyttävän ja mahdollisesti rikollisen toiminnan normaalista, tulee pankin ymmärtää epäilyttäviltä vaikuttavien, poikkeavien toimintatapojen lisäksi myös mikä on normaalia ja rehellistä käyttäytymistä asiakkailta. Vain näin pystyään erottamaan asiakasmassan joukossa olevat poikkeavuudet. Kun poikkeavuudet osataan tunnistaa, pystytään kehittämään pankin sisäisiä due diligence[110], KYC ja tilitapahtumien monitorointiprosesseja. Kun nämä prosessit ovat kunnossa, on rahanpesua ja terrorismin rahoittamista indikoivia elementtejä mahdollista huomata jo ennenaikaisesti jälkikäteisen havainnoinnin sijaan.[111]

Normaalia huolellisuutta tulee noudattaa silloin, kun asiakkuuteen ei liitetä korkeariskisiä tekijöitä. Normaalin huolellisuuden yhteydessä puhutaan yksinkertaisesta asiakkaan tuntemisesta. Erityistä huolellisuutta, eli asiakkaan tehostettua tuntemista tulee noudattaa niiden asiakkaiden kohdalla, joiden nähdään muodostavan pankille korkeamman riskin.[112] Pankeilla on mandaatti harjoittaa toiminnassaan riskiperusteita arviointia, sillä kaikkia riskitekijöitä ei pystytä ottamaan huomioon laissa. Rahanpesun ja terrorismin rahoittamisen keinot muuttuvat jatkuvasti, ja riskitekijät elävät luonnollisesti näiden muutoksien mukana. Laissa on määritelty tiettyjä riskitekijöitä, jotka on otettava huomioon, jättäen kuitenkin tilaa pankkien omalle, riskiperusteiselle arviolle. Riskiperusteinen arvio mahdollistaa resurssien allokoinnin korkeariskisiin asiakkaisiin, mikä tukee sekä pankin että valtion intressejä. Pankki pystyy tällöin toimimaan tarkoituksenmukaisesti ja kustannustehokkaasti, mikä johtaa siihen, että epäilyttävät tapahtumat huomataan suuremmalla todennäköisyydellä ja ne voidaan saattaa viranomaisten tietoon.

---

[109] de Koker 2006: 28.
[110] Käsitteellä *due diligence* tarkoitetaan asianmukaista huolellisuutta.
[111] Lowe 2017: 478.
[112] de Koker 2006: 28; Ramage 2012: 278.

Riskiperusteinen arviointi kytkeytyy vahvasti myös yhteen tietosuoja-asetuksen ydinkäsitteeseen, vaatimuksen oletusarvoisesta tietosuojasta. Tietoja kerätessä pitää perusteellisesti harkita, onko kerättävä tieto aidosti keräykseen kohdistuvan tarkoituksen kannalta oleellista, ja kuinka kauan tietoja on tarpeen säilyttää.[113] Tuntemisen tason valinnalla on suuri vaikutus kerättävän tiedon määrään, laatuun ja säilytysaikaan, joten riskiarviota tehdessä tulee kiinnittää huomiota myös tietosuoja-asetuksen vaatimuksiin.

3.5.1. Yksinkertaistettu tunteminen

Rahanpesulain mukaan ilmoitusvelvollinen noudattaa yksinkertaistettua menettelyä asiakkaan tuntemiseksi, jos ilmoitusvelvollinen arvioi, että asiakassuhteeseen tai yksittäiseen liiketoimeen liittyy vähäinen rahanpesun ja terrorismin rahoittamisen riski. Ilmoitusvelvollisen on kuitenkin seurattava asiakassuhdetta poikkeuksellisten tai epätavallisten liiketoimien havaitsemiseksi.[114] Laissa ei määritellä tarkemmin, milloin asiakkaan voidaan katsoa muodostavan vain vähäisen riskin rahanpesun tai terrorismin rahoittamisen näkökulmasta. Paljon jätetään siis pankkien oman, riskiperusteisen arvion varaan.

Jos asiakkaan maksuliikenne koostuu pääosin henkilöasiakkaalle tyypillisistä tilitapahtumista, kuten palkkatuloista ja päivittäiseen elämiseen liittyvistä kustannuksista, ei asiakkuuden pääsääntöisesti voida nähdä muodostavan suurta riskiä rahanpesun tai terrorismin rahoittamisen näkökulmasta. Tällöin on sekä pankin resurssienhallinnan että asiakkaan yksityisyydensuojan näkökulmasta tarkoituksenmukaista soveltaa asiakkaaseen yksinkertaistettua tuntemista. Näin mahdollistetaan resurssien kohdistaminen korkeariskisiin asiakkaisiin ja varmistetaan, että asiakkaan tietoja käsitellään vain välttämättömässä mittakaavassa.

3.5.2. Tehostettu tunteminen

Tehostettua menettelyä asiakkaan tuntemiseksi on lain mukaan sovellettava, jos arvioidaan, että asiakassuhteeseen tai yksittäiseen liiketoimeen liittyy tavanomaista suurempi rahanpesun ja terrorismin rahoittamisen riski, tai jos asiakkaalla tai liiketoimella on liittymäkohta valtioon, jonka rahanpesun ja terrorismin rahoittamisen estämis- ja selvittely-

[113] Dickie & Yule 2017: 101.
[114] RahanpesuL 3:8:1.

järjestelmä muodostaa komission arvion mukaan merkittävän riskin EU:n sisämarkkinalle tai ei täytä kansainvälisiä velvoitteita.[115] Näiden tekijöiden lisäksi poliittisesti vaikutusvaltainen henkilö tai tällaisen henkilön perheenjäsen tai yhtiökumppani on asetettava tehostetun tuntemisen piiriin.[116]

Edellä mainittujen tekijöiden lisäksi on myös muita asioita, joiden voidaan nähdä muodostavan korkean riskin rahanpesun ja terrorismin rahoittamisen näkökulmasta. Käteisperusteinen asiointi on yksi hyvä esimerkki korkeariskisestä tekijästä. Koska käteisen alkuperää tai käyttötarkoitusta on varmuudella vaikea selvittää, voidaan käteisten runsas käyttö nähdä korkeana riskinä. Käteisen käyttö, kuten myöskään poliittinen vaikutusvaltaisuus tai yhteys korkeariskiseen valtioon, ei itsessään indikoi rikollista toimintaa, mutta on kuitenkin tekijä, jonka perusteella asiakkaan tuntemisessa on hyvä noudattaa erityistä huolellisuutta.

Seuraavassa alaluvussa 3.6. pohditaan tarkemmin, millaisiin tekijöihin asiakkaan tuntemisen tason valinta voi perustua.

3.6. Tuntemisen tason valinta

Koska laki ei tarjoa yksittäisiä tilanteita lukuun ottamatta yksiselitteisiä vastauksia tuntemisen tason valintaan, tulee pankin tehdä päätös tuntemisen tasosta oman, riskiperusteisen arvioinnin pohjalta. Riskiperusteinen harkinta ja päätöksenteko perustuu pitkälti asiakkaasta saatavilla olevaan tietoon. Asiakkaalta saatujen tietojen lisäksi tilitapahtumat ovat varteenotettava vaihtoehto riskiä arvioidessa, sillä tilitapahtumien perusteella asiakkaan toiminnasta voidaan muodostaa totuudenmukaisen kuvan. Tilitapahtumien monitorointi onkin avainasemassa epäilyttävien tapahtumien havaitsemisessa[117]. Asiakkuuteen liittyvät mahdolliset korkeariskiset tekijät saattavatkin tulla huomatuksi vasta pankkien tilitapahtumien monitorointiin tarkoitettujen järjestelmien havaitsemien poikkeavuuksien myötä. Näiden järjestelmien kautta havaitut poikkeavuudet, joko yksittäiset tai systemaattiset, ovat riskejä, joita ei tyhjentävästi pystytä kartoittamaan laissa tai asiakkaan tuntemiseen liittyvien kysymysten muodossa. Tämä ilmentää hyvin sitä, ettei rahanpesu ja terrorismin rahoittaminen ole rikoslajina staattista tai ennakoitavaa.

[115] RahanpesuL 3:10:1; Hughes 2018: 2, 8.
[116] RahanpesuL 3:13:3:n 3 kohta; Demetriades 2016: 85.
[117] Lucchetti 2018: 4.

Tilitapahtumien tarkastelun lisäksi korkeariskisten asiakkaiden jäljille voi päästä ymmärtämällä miksi ja mihin tarkoitukseen rikolliset tarvitsevat pankin tarjoamia palveluita. Jotta voidaan ymmärtää mihin rikollinen pyrkii suorittamillaan tilitoimilla, on tiedettävä, millaisia motiiveja rikollisilla on ja mihin asioihin heidän päätöksentekonsa perustuu. Näiden asioiden ymmärtämiseksi pankki voi analysoida aiemmissa tutkinnoissa esiin nousseita tapauksia ja jakaa näistä saatua tietoa, sekä muodostaa erilaisia kuvioita käyttäytymismalleista.[118] Poikkeavat ja epäilyttävät tapahtumat eivät ole siis välttämättä aina räikeitä, selkeästi havaittavissa olevia tapahtumia, vaan epäilyttävän käytöksen huomaaminen voi vaatia laajempaa ymmärrystä rikollisten toiminnan taustalla olevasta logiikasta.

Laki ei yksinään siis pysty määrittelemään yksiselitteisiä rajoja asiakkaan tuntemisen tasoille, vaan pankeilla tulee olla hallussaan omia sisäisiä, riskien tunnistamiseen tarkoitettuja monitorointijärjestelmiä. Riskien tunnistaminen ja rikollisen toiminnan estäminen edellyttää tiedon keräämistä, arvioimista ja analysointia, minkä avulla pystytään hahmottaan pankin kohtaamia riskejä[119]. Riskien analysoinnin avulla pystytään myös muodostamaan selkeämpi käsitys toimintamallien ohella siitä, mitkä asiakkuudet muodostavat korkean riskin pankin liiketoiminnalle rahanpesun ja terrorismin rahoittamisen näkökulmasta. Oppiminen, joka tapahtuu sekä ulkoisten lähteiden ja tietojen, että sisäisessä tutkinnassa karttuneen kokemuksen avulla, on tärkeässä asemassa asiakkaan toiminnan ymmärtämisessä ja siten onnistuneen riskiarvion luomisessa.

[118] Lowe 2017: 478.
[119] Lowe 2017: 478.

4. TUNTEMISTIETOJEN KÄSITTELY

4.1. Henkilötietojen käsittelyn taustaa

Teknologisesti kehittyneet kaupungit älykkäine infrastruktuureineen nähdään usein merkittävänä tilaisuutena yhteiskunnalle ja taloudelle. Lukuisten positiivisten tekijöiden ohella tällaisilla yhteiskunnilla on kuitenkin myös kääntöpuolensa. Merkittävänä haasteena tietoyhteiskunnassa[120], jossa kerätään jatkuvasti valtavia määriä informaatiota, voidaan nähdä yksilöiden perusoikeuksien, kuten yksityisyyden ja henkilötietojen onnistunut suojaaminen.[121]

Viimeisten vuosien aikana tietojenkäsittelyyn liittyvät riskit ovat muuttaneet muotoaan. Aiempi huoli valtion tarkkailusta on saanut ohelleen huolen henkilötietojen väärinkäyttämisestä taloudellisen hyödyn tavoittelemiseen ilman yksilön suostumusta. Informaation keskeisen roolin myötä myös huoli syrjinnästä on kasvanut, ja tietoon perustuvat päätöksentekoprosessit voidaankin nähdä hyvin ongelmallisena tasa-arvoisen kohtelun näkökulmasta esimerkiksi tietojen automaattisen käsittelyn kohdalla.[122] Liiketoiminnan näkökulmasta tietojen automaattinen käsittely on manuaaliseen käsittelyyn verrattuna huomattavasti nopeampaa, ja näin ollen luonnollisesti kustannustehokkaampaa. Yrityksen hyötyessä automaattisen käsittelyn tuomista eduista, yksilön oikeudet saattavat kuitenkin kärsiä.

Yleinen tietosuoja-asetus on luotu ensisijaisesti ja ennen kaikkea EU-kansalaisten tietojen turvaamista varten. Kaikki asiakastieto on yksilön omaisuutta, mikä onkin tietosuoja-asetuksen ydinsanoma. Yksilö voi tarjota tietojaan yritykselle, mikä ei kuitenkaan tarkoita sitä, että yksilö samalla luopuisi oikeuksistaan antamiinsa tietoihin. Tietojen luovuttamisessa yritykselle on kyse ennemminkin tietojen lainaamisesta.[123] Henkilötiedot ovat nykyaikana valtava liiketoiminnallinen resurssi, joita ilman harva yritys pärjäisi. Jotta yrityksellä on oikeus liiketoiminnassaan hyödyntää henkilötietoja, on sen muutettava toimintaansa niin, että henkilötietoja käsitellään turvallisesti ja yksilön oikeuksia kunnioittaen. Henkilötietojen asianmukaisen ja laillisen käsittelyn on siis mentävä yrityksen liiketoiminnallisten intressien edelle.

---

[120] *Tietoyhteiskunnalla* tarkoitetaan yhteiskuntaa, jossa informaation tuottaminen, jakelu ja käyttäminen on merkittävä osa taloutta ja kulttuuria.
[121] van Dijk, Tanas, Rommetveit & Raab 2018: 230.
[122] Mantelero 2017: 593.
[123] O'Connor 2017: 52-54.

Uudistunut, yleinen tietosuoja-asetus ei ole muuttanut asetusta edeltäneen tietosuojadirektiivin pääelementtejä, sillä henkilötietojen suojelu perustuu edelleen pääasiallisesti yksilön oikeuksiin ja niiden turvaamiseen. Rekisteröidyn informointi ja suostumuksen edellytys käsittelyn lähtökohtana muodostavat edelleen tärkeän oikeudellisen pohjan tietojenkäsittelylle. Näiden pääperiaatteiden lisäksi tietosuoja-asetuksella pyritään vahvistamaan rekisteröidyn oikeuksia esimerkiksi minimoimalla ja rajoittamalla tietojen käsittelyä.[124]

Keskustelu uudistuneen tietosuoja-asetuksen ympärillä on viimeisten kuukausien aikana keskittynyt pitkälti asetuksen oikeudelliseen viitekehykseen. Hyvin vähän on keskitytty niihin vaikutuksiin, joita asetuksella on yrityksen tosiasialliseen liiketoimintaan. Yritykset eivät voi enää suhtautua henkilötietojen käsittelyyn välinpitämättömästi, sillä tietosuoja-asetuksen noudattaminen on liiketoiminnan kannalta välttämätöntä.[125] Yrityksen on siis ryhdyttävä konkreettisiin toimiin täyttääkseen tietosuoja-asetuksen vaatimukset. Tietosuoja-asetus näyttäytyy yrityksen toiminnassa sisäisten toimien lisäksi erilaisina velvoitteina asiakkaita ja viranomaisia kohtaan.

Jo entuudestaan haastavaan kombinaatioon oman lisänsä tuo henkilötietojen käsittely asiakkaan tuntemisen näkökulmasta. Enää yhtälössä ei ole mukana ainoastaan liiketoiminnan ja tietosuoja-asetuksen yhdistäminen, vaan henkilötietojen käsittelyä tulee harjoittaa rahanpesulainsäädäntö ja sen mukaiset velvoitteet mielessä pitäen. Tietosuoja- ja rahanpesulainsäädännön yhdistämisessä on otettava huomioon käsittelyn vaikutukset kolmeen erilliseen tahoon: pankkiin, asiakkaaseen ja yhteiskuntaan. Lainsäädäntöympäristö on tässä kontekstissa poikkeuksellisen haastava, sillä kaikilla osapuolilla on omat intressinsä tietojen käsittelyn suhteen.

Seuraavassa alaluvussa 4.2. käydään läpi, mitkä toiminnot voidaan katsoa henkilötietojen käsitellyksi, ja mitkä tiedot voidaan lukea henkilötiedoiksi. Luvussa käsitellään lisäksi lyhyesti tietosuoja-asetuksen ja henkilötietolain välistä eroa henkilötietojen käsittelyn määritelmässä.

4.2. Henkilötietojen käsittelyn määritelmä

Tietosuoja-asetuksen määritelmä henkilötietojen käsittelystä on henkilötietolakia kattavampi ja käsittää näin ollen useammat tietojen käsittelyn muodot ja tilanteet. Tietosuoja-

[124] Mantelero 2017: 586.
[125] Jackson 2018.

asetuksen 4 artiklan 2 kohdan mukaisesti käsittelyllä tarkoitetaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista.

Tietosuoja-asetuksessa henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijainti tiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella.[126]

Valtaosa tietosuoja-asetuksen artikloista on jo aiemmin sisällytetty jäsenmaiden kansallisiin lainsäädäntöihin. Tietosuoja-asetuksen tarkoituksena on kuitenkin harmonisoida tietosuojalainsäädäntöä Euroopassa ja luoda jäsenmaille tasapuoliset toimintaedellytykset.[127] Suurin osa näistä edellä mainituista käsittelyn muodoista onkin jo sisällytetty Suomen kansalliseen lainsäädäntöön, eli henkilötietolakiin. Tietosuoja-asetuksen määritelmä henkilötietojen käsittelystä ja sen eri muodoista on kuitenkin hieman henkilötietolain 3§:n 2 kohtaa laajempi, sillä henkilötietojen jäsentämistä, hakua, kyselyä ja rajoittamista ei ole yksilöity henkilötietolaissa.

Asiakkaan tuntemista varten kerättävät tiedot koostuvat asiakkaan henkilötiedoista, minkä vuoksi tietojen käsittelyyn sovelletaan tietosuoja-asetusta[128]. Kaikki asiakkuuden elinkaaren vaiheet, aina asiakkuuden perustamisesta jatkuvaan seurantaan, sekä mahdollisten selonotto- ja ilmoitusvelvollisuuden täyttämiseen, ovat kokonaisuudessaan henkilötietojen käsittelyä. Tietosuoja-asetuksen ollessa rahanpesulakiin nähden yleislaki, ristiriitatilanteissa tulee rahanpesulaki ensisijaisesti sovellettavaksi. Tällaisissakin tilanteissa on kuitenkin otettava huomioon tietosuoja-asetuksen mukaiset vaatimukset ja suhteuttava toiminta niin, että asiakkaan tietoja käsitellään mahdollisuuksien rajoissa tietosuoja-asetuksen säännöksiä kunnioittaen.

[126] Yleinen tietosuoja-asetus 2016/679: 4 artiklan 1 kohta.
[127] O'Connor 2017: 52-54.
[128] Hughes 2018: 7.

Seuraavassa alaluvussa 4.3. esitellään tietosuoja-asetuksen mukaiset henkilötietojen käsittelyn yleiset kuusi periaatetta. Periaatteita käsitellään tarkemmin alaluvun jälkeisissä alaotsikoissa sekä tietosuoja-asetuksen että rahanpesulainsäädännön näkökulmasta.

4.3. Henkilötietojen käsittelyn yleiset periaatteet

Tietosuoja-asetuksen 5 artiklan 1 kohdan mukaisesti tietoja käsitellessä on noudatettava kuutta periaatetta, jotka ovat lainmukaisuus, kohtuullisuus ja läpinäkyvyys, tietojen minimointi, täsmällisyys, säilytyksen rajoittaminen sekä eheys ja luottamuksellisuus. Näitä kuutta periaatetta on lähtökohtaisesti noudatettava kaikessa toiminnassa, jossa jollain tavalla käsitellään henkilötietoja. Rekisterinpitäjän on 5 artiklan 2 kohdan mukaisesti osoitusvelvollisuuden nojalla pystyttävä todistamaan, että näitä periaatteita noudatetaan tietoja käsitellessä.

On kuitenkin tilanteita, joissa noudattaminen on ristiriidassa jonkin erityislain kanssa, jolloin periaatteiden noudattaminen ei ole aina yksiselitteistä. Esimerkiksi läpinäkyvyyden noudattaminen on ristiriidassa rahanpesulain epäilyttäviä liiketoimia koskevan salassapitovelvollisuutta käsittelevän 4 luvun 4§:n kanssa, jolloin tietojen käsitteleminen täysin läpinäkyvästi ei ole mahdollista. Tällaisissa tilanteissa on pyrittävä toimimaan niin, että erityislain vaatimukset toteutuvat, mutta myös yleislain säännökset otetaan mahdollisimman hyvin toiminnassa huomioon.

Seuraavissa alaluvuissa (4.3.1., 4.3.2., 4.3.3., 4.3.4., 4.3.5., 4.3.6. ja 4.3.7.) käsitellään tarkemmin kutakin periaatetta. Periaatteita käsitellessä otetaan myös huomioon, miten kukin periaate näyttäytyy rahanpesulainsäädännön näkökulmasta, ja ovatko periaatteet täysin sovellettavissa sellaisinaan, vai velvoittaako rahanpesulainsäädäntö tekemään periaatteiden soveltamiseen poikkeuksia. Joidenkin periaatteiden kohdalla tietosuoja-asetusta pystytään soveltamaan sellaisenaan, kun taas joidenkin periaatteiden kohdalla rahanpesulain ja tietosuoja-asetuksen välillä on selkeitä ristiriitoja.

4.3.1. Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

Tietosuoja-asetuksen mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi[129]. Tietojenkäsittelyn laillisuus kulminoituu

[129] Yleinen tietosuoja-asetus 2016/679: 5 artiklan 1 kohdan a alakohta.

ensisijaisesti asiakkaan antamaan suostumukseen tietojen käsittelylle[130]. Asiakkaan tietojen käsittelyyn antaman suostumuksen on perustuttava vapaaehtoisuuteen, minkä lisäksi suostumuksen on oltava yksilöity, yksiselitteinen ja tietoisesti tehty[131]. Suostumuksen lisäksi asiakkaalla on lähtökohtaisesti aina oikeus määrätä tietojenkäsittely keskeytettäväksi.[132]

Lainmukaisen tietojenkäsittelyn ja -hallinnan edellytyksenä on siis se, että tietojen kerääjä on pyytänyt ennen tietojen keräämistä asiakkaalta nimenomaista ja tiedostettua suostumusta tietojen käsittelyyn[133]. Asiakkaalle tulee lisäksi kertoa selkeästi ja ymmärrettävällä tavalla, mihin tarkoitukseen tietoja kerätään, ja miten tietoja tullaan jatkossa käsittelemään. Näiden toimien lisäksi rekisterinpitäjän tulee huolehtia siitä, että tietoja käsitellään turvallisesti asiakkaan yksityisyyttä kunnioittaen. Kun asiakas tietää mihin tarkoitukseen hänestä kerättyjä tietoja käytetään, asiakkaalla on mahdollisuus tehdä tosiasiallisiin tietoihin perustuva päätös siitä, haluaako hän antaa rekisterinpitäjälle oikeuden käsitellä henkilötietojaan.[134]

Tietosuoja-asetuksen tietojenkäsittelyn määritelmän on erittäin laaja, minä vuoksi asetusta sovelletaan lukuisissa erilaisissa tilanteissa. Tietosuoja-asetuksessa mahdollisimman moni henkilötietojen käsittelyn muoto ja toiminto onkin pyritty sisällyttämään tietojen käsittelyn määritelmään. Rekisterinpitäjän on ennen mahdollista tietojen käsittelyä kartoitettava, onko kyseessä nimenomaisesti henkilötietojen käsittely, minkä jälkeen on varmistuttava siitä, löytyykö käsittelylle oikeudellisia perusteita. Käsittelyn oikeudelliset perusteet selviävät tietosuoja-asetuksen yksityiskohtaisista määräyksistä.[135]

Myös asiakkaan tuntemista varten kerätyissä tiedoissa on noudatettava lainmukaisuutta. Rahanpesulain 3 luvun 3 §:n 4 momentin mukaan asiakkaalle on ilmoitettava, että asiakkaan tuntemistietoja ja muita henkilötietoja voidaan käyttää rahanpesun ja terrorismin rahoittamisen estämiseen, paljastamiseen ja selvittämiseen sekä rahanpesun ja terrorismin rahoittamisen ja sen rikoksen, jolla rahanpesun tai terrorismin rahoittamisen kohteena oleva omaisuus tai rikoshyöty on saatu, tutkintaan saattamista varten.

[130] Pitkänen, Tiilikka & Warma 2013: 83.
[131] Talus ym. 2017: 20.
[132] Alvarez 2017: 20.
[133] Hughes 2018: 9; Pitkänen ym. 2013: 83.
[134] Garcia-Rivadulla 2016: 235-236.
[135] Lindroos-Hovinheimo 2018: 60.

Tietojen keräämisen on siis perustuttava ensisijaisesti asiakkaan suostumukseen. Pankilla on rahanpesulain nojalla velvollisuus tuntea asiakkaansa ja kerättävä asiakkaasta tarvittava määrä tietoa. Tästä huolimatta asiakkaalla on kuitenkin mahdollisuus kieltäytyä tietojen antamisesta, sillä uhalla, ettei pankki enää pysty kieltäytymisen jälkeen jatkamaan asiakassuhdetta. On huomioitavaa, ettei pankki ole viranomainen, eikä näin ollen voi vasten asiakkaan tahtoa kerätä asiakkaasta tietoja.

Pankin on otettava myös kohtuullisuus huomioon kerätessään tietoja asiakkaasta. Tietojen keräämisen tulee perustua tiettyyn käyttötarkoitukseen, minkä lisäksi tietoja tulee kerätä vain välttämättömissä määrin. Tietojen käyttötarkoitussidonnaisuutta ja minimointia käsitellään tarkemmin jäljempänä alaluvuissa 4.3.2. ja 4.3.3.

Lainmukaisuuden ja kohtuullisuuden toteutuessa, täydellistä läpinäkyvyyttä ei rahanpesua ja terrorismin rahoittamisen estämistä varten kerättyjen tietojen kohdalla pystytä noudattamaa. Tietosuoja-asetuksen 15 artiklan 1 kohdan mukaisesti rekisteröidyllä on oikeus saada pääsy omiin tietoihinsa. Rahanpesulain 4 luvun 4 §:n 1 momentissa on kuitenkin määrätty salassapitosäännökset, joiden mukaan asiakkaalle ei saa paljastaa, jos hänestä on tehty ilmoitus epäilyttävästä liiketoimesta. Rahanpesulaki voidaan nähdä tässä kohdin tietosuoja-asetukseen nähden erityislakina, ja siten ensisijaisesti sovellettavana lakina rahanpesuun ja terrorismin rahoittamiseen liittyvissä tapauksissa. Myös jatkuvan seurannan aikana saadut tiedot voidaan katsoa kuuluvan osaksi pankin riskienhallintaa, ja tämän myötä lukeutuvan tiedoksi, johon asiakkaalla ei ole tarkistusoikeutta[136]. Vaikkei asiakkaalla itsellään ole oikeutta saada tietoonsa asiakkaasta tehtyä epäilyttävää liiketoimi-ilmoitusta koskevia tietoja, voi tietosuojavaltuutettu asiakkaan pyynnöstä tarkastaa asiakasta koskevien tietojen lainmukaisuuden[137].

4.3.2. Käyttötarkoitussidonnaisuus

Pankin velvollisuus tietojenkäsittelyn suhteen alkaa usein velvollisuudesta kertoa asiakkaalle, mihin tarkoitukseen tietoja kerätään ja miten tietoja käsitellään[138]. Tietosuoja-asetus määrääkin, että henkilötiedot on kerättävä tiettyä, nimenomaista ja laillista tarkoitusta varten, eikä niitä saa käsitellä myöhemmin näiden tarkoitusten kanssa yhteensopimattomalla tavalla[139]. Käyttötarkoitussidonnaisuus pätee myös asiakkaan tuntemista varten ke-

[136] Finanssivalvonnan standardi 2.4. 2015.
[137] RahanpesuL 7:8:4.
[138] Dockeray & Westbrook 2018: 56-58.
[139] Yleinen tietosuoja-asetus 2016/679: 5 artiklan 1 kohdan b-d alakohdat.

rättyihin tietoihin. Rahanpesulain 3 luvun 3§:n 5 momentin mukaan asiakkaan tuntemistietoja tai muita henkilötietoja, jotka on hankittu ainoastaan rahanpesun ja terrorismin rahoittamisen estämiseksi ja paljastamiseksi, ei saa käyttää tarkoitukseen, joka on yhteensopimaton näiden tarkoitusten kanssa.

Käyttötarkoitussidonnaisuuden periaate tulisi rahanpesun ja terrorismin rahoittamisen estämisen kontekstissa ottaa huomioon myös suunnitellessa mitä lisätietoja asiakkaalta tulisi saada asiakkaan toiminnan selvittämiseksi[140]. Käyttötarkoitussidonnaisuus tässä kontekstissa liittyy myös vahvasti tietojen minimointiin, jota käsitellään tarkemmin alaluvussa 4.3.3. Asiakkaalta ei ole tarkoituksenmukaista kysyä varmuuden vuoksi mahdollisimman paljon tietoa sen kartoittamiseksi, onko asiakkaan toiminta epäilyttävää. Pankin tulisi sen sijaan tarkkaan harkita, mitä tietoja asiakkaalta on tosiasiassa pyydettävä. Harkinta tietoja pyydettäessä palvelee sekä asiakasta että pankkia, sillä tällöin suojellaan asiakkaan yksityisyyttä, ja vastaavasti hallitaan pankin rajallisia resursseja sekä ajankäytön että kustannusten suhteen.

4.3.3. Tietojen minimointi

Yksi tärkeistä tietosuoja-asetuksen myötä esiinnousseista pääperiaatteista on tietojen minimointi. Tietosuoja-asetuksen mukaan henkilötietojen on oltava asianmukaisia ja olennaisia ja rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään[141]. Käsiteltävän tiedon määrän minimoinnilla pyritään turvaamaan henkilötietoja ja sitä kautta suojelemaan asiakkaan yksityisyyttä[142]. Kerätyn ja käsitellyn tiedon rajaaminen ainoastaan laadullisesti ja määrällisesti tarpeelliseen määrään tietoa suojelee asiakasta sekä tietoturvariskeiltä että yksityisyyden vaarantumiselta.

Tietosuoja-asetuksen minimointiperiaatteen perusteella vain välttämätön määrä tietoa tulisi kerätä tietyn tarkoituksen suorittamista varten[143]. Rahanpesulain 3 luvun 4§:n 1 momentin perusteella pankin on vastaavasti hankittava kokonaisvaltaisesti tietoa asiakkaan toiminnasta. Rahanpesulainsäädäntö ei kuitenkaan määrittele kuinka paljon asiakkaasta on kerättävä tietoa asiakkaan perustietojen lisäksi, joten tämä jää pankin harkinnan varaan. Pankin onkin tietoja hankkiessaan harkittava, kuinka paljon asiakkaasta tosiasiallisesti tarvitaan tietoa rahanpesulainsäädännön velvoitteiden noudattamiseksi.

---

[140] Vanto 2011: 53.
[141] Yleinen tietosuoja-asetus 2016/679: 5 artiklan 1 kohdan c alakohta; Hughes 2018: 9.
[142] Camp 2015: 27-28.
[143] McCallister, Zanfir-Fortuna & Mitchell 2018: 39.

Tietosuojalain mukaisesti tietoja ei tulisi hankkia varmuuden vuoksi, vaan kerättyjen tietojen tulisi juurikin olla olennaisia. Pankin on huomioitava tämä rahanpesulainsäädännön määräyksistä huolimatta. Tilanne on pankin kannalta haastava, sillä on mahdotonta yksiselitteisesti pystyä määrittelemään, kuinka paljon tietoa on kerättävä, jotta asiakkaan toiminnasta pystyään muodostamaan ymmärrettävä kuva sen suhteen, onko toiminta laillista vai laitonta. Pankille kertyneen kokemuksen voidaan nähdä olevan merkittävässä asemassa tietojen keräämisen oikeasuhteisuuden varmistamisessa. Kokemuksen myötä pankki pystyy hahmottamaan, milloin asiakkaalta tulisi saada lisätietoa toiminnan selvittämiseksi, ja vastaavasti milloin jo olemassa olevilla tiedoilla pystyään tekemään päätös toiminnan luonteen suhteen.

Tietojen minimointi ei ole ainoastaan tärkeää asiakkaan yksityisyyden säilymisen ja tietoturvariskien minimoinnin näkökulmasta. Tietojen minimoiminen voidaan nähdä myös liiketoiminnallisena etuna pankille, sillä tietojen kerääminen ja asianmukainen käsittely aiheuttaa pankille valtavasti kuluja. Noudattamalla tietosuoja-asetuksen minimointiperiaatetta, tietojenhallintaprosessit keventyvät ja pankki pystyy toimimaan aiempaa kustannustehokkaammin.

Toinen merkittävä hyöty kerätyn tiedon minimoinnissa on asiakkaan tuntemiseen ja etenkin selonottovelvollisuuteen kuluvan ajan vähentyminen. Pankin tehtävänä on ainoastaan havaita epäilyttäviä liiketoimia ja raportoida tehdyistä huomioista eteenpäin rahanpesunselvittelykeskukselle. Pankin tarkoituksena ei siis ole suorittaa rikostutkintaa ja kerätä ylettömiä määriä tietoja asiakkaasta. Keräämällä ainoastaan ilmoituksen kannalta tarpeellisen määrän tietoa, pankki pystyy suorittamaan tutkintaprosessin nopeammin ja keskittymään laajempaan määrään epäilyttäviä tapauksia.

4.3.4. Täsmällisyys

Tietosuoja-asetuksen mukaisesti henkilötietojen on oltava täsmällisiä, virheettömiä ja tarvittaessa päivitettyjä[144]. Pankin on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä[145]. Myös rahanpesulaki edellyttää pankkia tuntemaan asiakkaansa koko asiakassuhteen keston ajan[146].

[144] O'Connor 2017: 52-54.
[145] Yleinen tietosuoja-asetus 2016/679: 5 artiklan 1 kohdan d alakohta.
[146] RahanpesuL 3:4:2.

Pankin olisi tietosuoja-asetuksen nojalla huolehdittava, ettei asiakkaasta kerätä tai tallenneta virheellisiä, epätäydellisiä tai vanhoja tietoja. Tiedot olisikin lähtökohtaisesti hyvä saada asiakkaalta itseltään, tai muita luotettavia lähteitä hyväksikäyttäen.[147] Vaatimus tietojen täsmällisyydestä, virheettömyydestä, ja ajantasaisuudesta sekä luotettavien tietolähteiden käyttämisestä on osittain kuitenkin haastavaa asiakkaan tuntemisen kontekstissa. Pankin käyttäessä sisäisten lähteiden lisäksi myös ulkoisia lähteitä, ei tietojen tarkkuudesta tai virheettömyydestä pystytä varmistumaan. Näin ollen asiakkaasta kerätyt tiedot ja tietojen perusteella muodostettu profiili asiakkaasta voi perustua ainakin osittain virheellisiin ja epätarkkoihin tietoihin.

Tietojen ajantasaisuus kuitenkin toteutuu asiakkaan tuntemisen kohdalla ainakin sisäisten tietojen osalta, sillä myös rahanpesulainsäädäntö velvoittaa pitämään asiakkaan tuntemisen tiedot ajan tasalla jatkuvan seurannan nojalla. Ulkoisten tietojen osalta, esimerkiksi avoimen haun avulla saatujen tietojen kohdalla, ei aina voida varmistua tietojen ajantasaisuudesta. Sen sijaan ulkoiset, viralliset rekisterit, kuten Suomen Asiakastieto Oy ja Väestörekisterikeskus ovat useimmiten kuitenkin luotettavia tietolähteitä ajantasaisuudenkin osalta, sillä päivämäärät, joihin tiedot perustuvat, ovat usein ilmoitettu.

4.3.5. Säilytyksen rajoittaminen

Henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten[148]. Lähtökohtaisesti rekisterinpitäjän tulisi siis säilyttää tietoja vain sen aikaa kuin on tarpeellista kunkin tehtävän loppuun saattamiseksi[149]. Koska pankin toimintaa asiakkaan tuntemisen suhteen säätelee kuitenkin tietosuoja-asetuksen ohella ensisijaisesti rahanpesulainsäädäntö, tulee pankin säilyttää tietoja rahanpesulain määräämän ajan.

Rahanpesulain 3 luvun 3 §:n 1 momentissa määrätään, että asiakkaan tuntemistietoja on säilytettävä luotettavalla tavalla viiden vuoden ajan vakituisen asiakassuhteen päättymisestä. Rahanpesulain 3 §:ssä on määritelty tarkemmin yksityiskohtaiset tiedot, jotka asiakkaasta on säilytettävä. Tällaisia tietoja ovat muun muassa asiakkaan perustiedot, henkilöllisyyden todentamisessa käytetyn asiakirjan tiedot[150] sekä asiakassuhteen aikaiseen toimitaan liittyvät tiedot, kuten tiedot tilille talletettujen varojen alkuperästä ja käyttötarkoituksesta.

---

[147] Pitkänen ym. 2013: 104.
[148] Yleinen tietosuoja-asetus 2016/679: 5 artiklan 1 kohdan e alakohta.
[149] Dockeray & Westbrook. 2018: 56-58; Jackson 2018; McCallister, Zanfir-Fortuna & Mitchell 2018: 39.
[150] Hughes 2018: 8.

Rahanpesulain 4 luvun 3§:n 1 momentin mukaan pankin on asiakkaan tuntemista varten kerättyjen tietojen lisäksi säilytettävä viiden vuoden ajan epäilyttävää liiketoimi-ilmoitusta varten hankitut välttämättömät tiedot sekä näihin liittyvät asiakirjat. Tiedot ja asiakirjat on pidettävä erillään asiakasrekisteristä eikä niitä saa käyttää muuhun kuin tässä laissa säädettyyn tarkoitukseen. Tiedot ja asiakirjat on poistettava viiden vuoden kuluttua asiakassuhteen päättymisestä tai epäilyttävän liiketoimen suorittamisesta, jollei niiden edelleen säilyttäminen ole tarpeen rikostutkinnan, vireillä olevan oikeudenkäynnin tai ilmoitusvelvollisen tai sen palveluksessa olevan oikeuksien turvaamiseksi.

4.3.6. Eheys ja luottamuksellisuus

Henkilötietojen käsittelyssä tulee noudattaa luottamuksellisuutta. Tällä tarkoitetaan sitä, että henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia[151].

Eheys ja luottamuksellisuus ovat tietojen saatavuuden ohella kiinteästi sidoksissa tietojenhallintaan. Luottamuksellisuudella tarkoitetaan tietojen saatavuuden rajoittamista sellaisilta henkilöiltä tai osapuolilta, joilla ei ole lupaa saada pääsyä tietoihin. Saatavuuden rajoittamisella pyritään juurikin estämään luvaton pääsy tietoihin muilta kuin tahoilta, joiden kohdalla tietojen käsittely on perustelua. Tietojen eheydellä sen sijaan tähdätään siihen, että tiedot ovat oikein ja ajan tasalla koko tietojen käsittelyä koskevan ajanjakson ajan, joka kattaa kaikki tietojen käsittelyyn liittyvät vaiheet ja toimenpiteet aina tietojen keräämisestä tietojen hallintaan ja muuttamiseen. Saatavuudella pyritään siihen, että tiedot ovat saatavilla niitä prosesseja varten, joiden vuoksi tiedot on alun perin kerätty. Tiedon saatavuuteen liittyvien turvatoimenpiteiden ja toimintojen tulee olla tarkoituksenmukaisia tietojen suojaamiseksi.[152]

Jotta pankki voi kerätä asiakkaalta tietoja tuntemistoimenpiteitä varten, pankin on ryhdyttävä tarvittaviin toimenpiteisiin suojellakseen tietoja mahdollisilta tietoturvariskeiltä.[153] Asiakkaan tuntemiseen liittyvien tietojen käsittelyssä luottamuksellisuus voi käytännön tasolla tarkoittaa sitä, että asiakkuuteen liittyvistä asioista keskustellaan ainoastaan asianmukaisten osapuolien kesken tilanteen vaatimassa laajuudessa. Tietojen

[151] Yleinen tietosuoja-asetus 2016/679: 5 artiklan 1 kohdan f alakohta.
[152] Laybats & Tredinnick 2016: 78.
[153] O'Connor 2017: 52-54.

eheydestä tulee myös huolehtia tietosuoja-asetuksen lisäksi rahanpesulain 3 luvun 3§:n 1 momentin ja 4 luvun 3§:n 1 momentin nojilla, sillä kyseiset kohdat vaativat säilyttämään asiakkaan tuntemiseksi sekä epäilyttävän liiketoimi-ilmoituksen laatimiseksi kerätyt tiedot vähintään viiden vuoden ajan asiakassuhteen päättymisestä tai vastaavasti vähintään viiden vuoden ajan epäilyttävän liiketoimi-ilmoituksen laatimisesta.

Seuraavassa alaluvussa 4.4. käsitellään tarkemmin, mitä erityisillä henkilötietoryhmillä tarkoitetaan, ja miten niitä koskevia tietoja tulee käsitellä. Luvussa tuodaan esiin sekä arkaluontoisten tietojen että biometristen tietojen käsittelyn periaatteet, sekä näiden tietojen käsittelyn näyttäytyminen asiakkaan tuntemista varten kerättyjen tietojen näkökulmasta.

4.4. Erityisiä henkilöryhmiä koskeva käsittely

Erityisten henkilötietoryhmien käsittelyksi luetaan tietosuoja asetuksen 9 artiklan 1 kohdan mukaisesti sellaiset henkilötiedot, joista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys. Myös geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen tai luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista koskevien tietojen käsittely lukeutuvat erityistä henkilötietoryhmää koskeviksi tiedoiksi.

Tietynlaiset tiedot ovat arkaluontoisempia kuin toiset. Esimerkiksi terveyteen, rotuun ja etnisyyteen liittyvät tiedot tiettyjen biometristen tietojen ohella lukeutuvat arkaluontoisiin tietoihin.[154] Arkaluontoisten ja biometristen tietojen käyttö voi aiheuttaa vakavia uhkia asiakkaan yksityisyydelle. On kuitenkin otettava huomioon, että on tilanteita, joissa tällaisten tietojen käsittelyllä pyritään suojaamaan joko yhteiskunnallisia tai rekisteröidyn yksityisiä intressejä. Rikostutkinta ja yleisen järjestyksen ylläpitäminen ovat hyviä esimerkkejä yhteiskunnallisista intresseistä, kun taas erilaisten teknologisten järjestelmien ja tietojen turvaaminen ulkopuolisilta palvelee usein rekisteröidyn yksityisiä intressejä. Tällaisissa tilanteissa edellä mainittujen tietojen käyttäminen voidaan nähdä laillisena yksityisyyteen puuttumisena.[155] Arkaluontoisten tietojen kerääminen rahanpesun ja terrorismin rahoittamista varten voidaan nähdä juurikin yhteiskuntaa palvelevana toimintana,

[154] Dockeray & Westbrook. 2018: 56-58.
[155] Štitilis & Laurinaitis 2017: 619.

sillä asiakkaan tuntemiseen liittyvillä toimenpiteillä pyritään takaamaan yhteiskunnallisen stabiiliuden säilyminen.

Erityisten henkilötietoryhmien kohdalla henkilötietojen oikeudellinen sääntely, soveltaminen ja tulkinta on äärimmäisen tärkeää. Jossain tilanteissa esimerkiksi biometrisen teknologian käyttö on kannustettavaa, kun taas tilanteissa, joissa on havaittu piilevän riski yksityisyyden loukkaamiselle, käyttöä tulisi rajoittaa.[156] Biometristen tietojen käytöstä osana liiketoimintaa on tullut arkipäivää yrityksille[157]. Biometristen tietojen käytön lisääntyminen myös henkilökohtaisissa kulutustottumuksissa ja hallitusten valvonnassa on peruuttamatonta.[158] Arkaluontoiset ja biometriset tiedot ovat oleellinen osa myös asiakkaan tuntemisen prosessia, sillä rahanpesulainsäädännön mukaan asiakas pitää olla yksiselitteisesti tunnistettavissa henkilöllisyystodistuksen avulla.

Erityisiksi henkilötietoryhmiksi luokiteltavien henkilötietojen käsittely ei lähtökohtaisesti ole sallittua. Erityisiä henkilötietoryhmiä käsittäviä tietoja on kuitenkin lupa käsitellä, jos tietosuoja-asetuksen 6 artiklassa säädetyn perusteen lisäksi myös jokin asetuksen 9 artiklassa olevista määräyksistä toteutuu.[159] Tämän lisäksi erityisten henkilötietoryhmien kohdalla henkilötietojen käsittely on sallittua silloin, kun suostumus henkilötietojen käsittelyyn on nimenomainen [160].

Rahanpesun ja terrorismin rahoittamisen estämiseksi on kerättävä valtava määrä tietoa, josta osa voidaan nähdä olevan tietosuoja-asetuksen mukaisia, erityisiä henkilöryhmiä koskettavia, arkaluontoisia tietoja. Rahanpesun ja terrorismin rahoittamisen estämiseksi kerättyjen tietojen käsittely on kuitenkin tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohdan mukaista lainmukaista käsittelyä, sillä henkilötietojen käsittely tähän tarkoitukseen on pankeille laissa asetettu vaatimus, ja siten käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Käsittelyn voi katsoa olevan laillista myös tietosuoja-asetuksen 9 artiklan 2 kohdan a alakohdan nojalla, jonka mukaisesti tietoja saa käsitellä, jos rekisteröity on antanut nimenomaisen suostumuksensa kyseisten henkilötietojen käsittelyyn yhtä tai useampaa tiettyä tarkoitusta varten.

[156] Štitilis & Laurinaitis 2017: 619.
[157] Štitilis & Laurinaitis 2017: 620.
[158] Kindt 2018: 523.
[159] Talus ym. 2017: 19.
[160] Kindt 2018: 537; Talus ym. 2017: 20.

Pankilla on lakiin perustuen kerättävä asiakkaasta tietoja, joiden perusteella esimerkiksi asiakkaan rotu ja etnisyys tulevat pankin tietoon. Tällaisia tietoja voivat olla juurikin asiakkaan henkilöllisyystodistus ja tieto asiakkaan synnyinmaasta. Vaikka pankeilla onkin lakiin perustuva velvollisuus käsitellä erityisiä henkilötietoryhmiä koskevia tietoja, tulee pankin siitä huolimatta noudattaa tietosuoja-asetuksen mukaisia yleisiä periaatteita tietojen käsittelyn suhteen.

Seuraavaa alaluku 4.5. käsittelee asiakkaan tietojen automaattista käsittelyä, eli profilointia. Profilointia koskevien yleisten periaatteiden lisäksi tulkitaan lainsäädännön merkitystä asiakkaan tuntemiseen liittyvien toimenpiteiden näkökulmasta, sillä profilointi linkittyy vahvasti asiakkaan tuntemisessa apuna käytettyyn transaktioiden monitorointiin.

4.5. Profilointi

Tietosuoja-asetuksen 4 artiklan 1 kohdan 4 alakohdan mukaisesti profiloinnilla tarkoitetaan mitä tahansa henkilötietojen automaattista käsittelyä, jossa henkilötietoja käyttämällä arvioidaan luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin.

Yksilöiden ja ryhmien automaattinen profilointi on tavanomainen käytäntö nykyisessä informaatioyhteiskunnassamme. Tiedonlouhinnan[161] kasvava kehitys on merkittävä tekijä automaattisen profiloinnin toteuttamisessa. Usein profiloinnin ja tiedonlouhinnan vaikutukset mielletään uhkana tietosuojalle ja yksityisyydelle. Tietosuoja-asetuksen profilointia koskevilla määräyksillä pyritäänkin ensisijaisesti suojelemaan rekisteröityjen yksityisyyttä. Samalla kun tiedonlouhinta ja profilointi nähdään uhkana tietosuojalle ja yksityisyydelle, voivat profiloinnin muut uhat, kuten yksilöllisyyden unohtuminen, tietojen epäsymmetria ja syrjintä olla yksityisyyttä suurempia uhkia.[162]

Syrjintä on usein yksi profiloinnin ja tiedonlouhinnan lieveilmiöistä. Syrjintä on lähtökohtaisesti aina kuitenkin laitonta, tai vähintäänkin epäeettistä. Syrjintä on laitonta silloin,

[161] *Tiedonlouhinnalla* tarkoitetaan menetelmiä, joilla pyritään löytämään haluttu tieto suuresta tietomassasta.
[162] Schermer 2011: 45-46.

kun se perustuu henkilön etnisyyteen, sukupuoleen, uskontoon ja seksuaaliseen suuntautumiseen. Aiemmin kuvailtuja profilointiin ja tiedonlouhintaan liittyviä riskejä pyritään minimoimaan vetoamalla tietosuojaan ja yksityisyyteen. Tietosuojan ydinajatuksena on juurikin rekisteröidyn oikeus ja mahdollisuus suojella omia henkilötietojaan kolmansilta osapuolilta.[163] Pankin on joissain asiakkaan tuntemista koskevissa tilanteissa välttämätöntä käsitellä edellä mainitun tapaisia, arkaluonteisia tietoja. Tällöin ei kuitenkaan ole kyse syrjinnästä, sillä pankin tekemät päätökset eivät perustu asiakkaan henkilökohtaisiin ominaisuuksiin vaan asiakkaan toimintaan ja siitä muodostettuun kokonaiskuvaan.

Tietosuoja-asetus kieltää tietyin poikkeuksin automaattisen profiloinnin, jonka seurauksena yksilö kohtaa oikeusvaikutuksia tai joilla on vastaavalla tavalla merkittävä vaikutus yksilöön. Automaattista profilointia harjoittaessaan rekisterinpitäjän on huolehdittava asianmukaisista toimenpiteistä rekisteröidyn vapauksien, oikeuksien ja etujen suojelemiseksi. Erityisiin henkilötietoihin kohdistuva profilointi sen sijaan on kiellettyä tiettyjä poikkeustilanteita lukuun ottamatta.[164] Pankin on välttämätöntä ulottaa profilointi myös arkaluontoisiin tietoihin, sillä rahanpesulainsäädäntöä noudatettaessa tulee kiinnittää huomiota etenkin asiakkaisiin, joilla on yhteys rahanpesun ja terrorismin rahoittamisen näkökulmasta korkean riskin maihin[165].

Automaattisella tietojen käsittelyllä, eli profiloinnilla, on vaikutusta siihen, miten yritykset suhtautuvat asiakkaisiinsa. Hyvä esimerkki automaattisesta tietojen käsittelystä ovat luottoluokitukset, joiden avulla määritellään todennäköisyys sille, pystyykö henkilö, jolle luotto on myönnetty, maksamaan velkansa takaisin.[166] Automaattisella tietojen käsittelyllä on pitkä historia. Rahoituslaitokset ovat käyttäneet tilastoihin perustuvaa luottoluokitusjärjestelmää jo vuosien ajan, ja järjestelmien kehittymisen myötä automaattisen tietojen käsittelyn ja päätöksenteon myötä syntyneet tulokset ovat olleet ihmisen tekemiä päätöksiä tarkempia.[167] Näin on myös rahanpesun ja terrorismin rahoittamisen estämiseen käytettyjen monitorointijärjestelmien kohdalla. Järjestelmät pystyvät seulomaan suuresta massasta tietoa epäilyttäviä tapahtumia ja käyttäytymismalleja, joita ihmisten olisi mahdotonta pystyä seulomaan manuaalisesti.

[163] Schermer 2011: 47-48.
[164] Talus ym. 2017: 27-28.
[165] RahanpesuL 3:10:1.
[166] Vanto 2011: 136.
[167] Kingston 2017: 439.

Päätöksentekoon vaikuttavaa automaattista profilointia on rajoitettu tietosuoja-asetuksen myötä. Tietosuoja-asetuksen 13-15 artikloiden mukaan rekisteröidylle on annettava riittävät tiedot siitä, miten tietoja käsitellään ja säilytetään, mukaan lukien tieto siitä, mihin tarkoitukseen tietoja kerätään. Jos tietoja käytetään automaattisen päätöksentekoon ja profilointiin, on rekisteröidylle kerrottava, millaisiin tekijöihin automaattinen päätöksenteko perustuu, ja kuinka suuria ja oletettuja vaikutuksia päätöksenteolla on rekisteröidyn asemaan. Artiklan 22 mukaan vaatimusten tarkoituksena on suojella rekisteröityä joutumasta ainoastaan automaattisen tietojenkäsittelyn ja profiloinnin perusteella tehdyn päätöksenteon kohteeksi, etenkin tilanteissa, joissa päätöksenteolla on oikeudellisia tai vastaavasti merkittäviä vaikutuksia rekisteröidyn asemaan.[168]

Rahanpesulainsäädännön perusteella pankin on ilmoitettava asiakkaalle, että asiakkaan tuntemiseksi kerättyjä tietoja käytetään rahanpesun ja terrorismin rahoittamisen estämiseksi tarkoitettuja toimenpiteitä varten. Tässä kontekstissa asiakkaan tietoihin kohdistuvia, mahdollisesti ilmoitusvelvollisuuteen johtavia toimenpiteitä ei kuitenkaan perusteta yksinomaan automaattisen monitorointijärjestelmän perusteella saatuihin tietoihin, joten profilointi ei itsessään aiheuta asiakkaan asemaan kohdistuvia merkittäviä vaikutuksia.

Oikeus omien henkilötietojen suojaamiseen on erittäin tärkeää, sillä siten yksilöllä on mahdollisuus suojella omia henkilötietojaan väärinkäytöiltä. Tietojen ja yksityisyyden suojeleminen ei kuitenkaan ole aiheena yksiulotteinen, sillä se linkittyy yksilön lisäksi myös esimerkiksi teknologisiin, oikeudellisiin ja sosiaalisiin aspekteihin. Rekisteröidyn suostumus automaattiseen tietojenkäsittelyyn ja profilointiin voi tuoda haasteita läpinäkyvyyden kannalta. Vaikka rekisteröity antaisi suostumuksensa tietojen käsittelylle ja profiloinnille, on rekisteröidyn kuitenkin todennäköisesti vaikeaa arvioida ja ymmärtää käsittelyn laajuutta ja profiloinnin vaikutusta rekisteröityyn. Tästä johtuen rekisteröidyt voivat aliarvioida automaattiseen profilointiin liittyviä riskejä.[169]

Seuraavassa alaluvussa 4.6. käsitellään oletusarvoista tietosuojaa, jolla on vahvoja liittymäkohtia jo aiemmissa alaluvuissa käsiteltyihin henkilötietojen käsittelyn periaatteisiin.

[168] Kingston 2017: 439.
[169] Schermer 2011: 48-49.

4.6. Oletusarvoinen tietosuoja

Oletusarvoisella tietosuojalla tarkoitetaan sitä, että rekisterinpitäjän on oletusarvoisesti käsiteltävä ainoastaan kunkin tehtävän suorittamisen kannalta tarpeellisia tietoja. Oletusarvoinen tietosuoja ei kata ainoastaan tietojen laatua, vaan myös tietojen määrää, käsittelyn laajuutta, tietojen säilytysaikaa ja saatavuutta. Rekisterinpitäjän on lisäksi huolehdittava siitä, ettei tietoja saateta sellaisten osapuolien käyttöön, joille rekisteröity ei ole antanut suostumustaan.[170] Oletusarvoinen tietosuoja linkittyykin vahvasti aiemmin alaluvuissa 4.3.2., 4.3.3., 4.3.5. ja 4.3.6. käsiteltyihin käyttötarkoitussidonnaisuuteen, tietojen minimointiin, säilytyksen rajoittamiseen, eheyteen ja luottamuksellisuuteen.

Tietosuoja-asetuksen määräys sisäänrakennetusta ja oletusarvoisesta tietosuojasta pyrkii siihen, että tietojärjestelmät rakennettaisiin jo alun perin tukemaan ja valvomaan yksityisyyden ja tietosuojan toteutumista. Oletusasetusten tulisi automaattisesti minimoida tiedon kerääminen, säilyttäminen ja jakaminen, ja käsitellä tietoja ainoastaan siinä laajuudessa kuin on tarpeellista tietyn tehtävän suorittamiseksi.[171] Rekisterinpitäjän täytyy ottaa käyttöönsä juurikin tällaiset mekanismit, joiden avulla varmistutaan oletusarvoisesti siitä, että ainoastaan kunkin käsittelyn kannalta välttämättömiä tietoja todellisuudessa käsitellään. Näiden mekanismien tarkoituksena on varmistaa, ettei tietoja kerätä, käsitellä tai säilytetä pidempään kuin on tarpeellista. Näiden toimien lisäksi mekanismien on erityisesti varmistettava, ettei määräämätön määrä ihmisiä saa tietoja käyttöönsä ilman rekisteröidyn hyväksyntää.[172] Oletusarvoisen tietosuojan voidaan nähdä helpottavan tietojenhallintaa, tekevän tietojen käsittelystä tietoturvallisempaa sekä automaattisuuden johdosta myös kustannustehokkaampaa.

Seuraavassa alaluvussa 4.7. määritellään, mitä henkilötietojen turvallisuudella tarkoitetaan ja millaisia toimenpiteitä henkilötietojen suojaaminen vaatii. Luvussa käsitellään myös turvallisuuteen liittyvien riskien arvioimista ja turvallisuustoimien soveltamista kulloisenkin riskin mukaisesti.

[170] Talus 2017: 13.
[171] Koops & Leenes 2013: 160.
[172] Tikkinen-Piri ym. 2018: 142.

4.7. Henkilötietojen turvallisuus

Henkilötietojen turvallinen käsittely on tärkeää henkilötietojen suojaamisen näkökulmasta. Tietojen suojaamisella tarkoitetaan tietojen, palvelujen ja järjestelmien ja tietoliikenteen suojaamista niin, että tietojen käsittely kaikissa käsittelyn muodoissa on mahdollista ainoastaan tietojen käsittelyyn oikeutettujen henkilöiden osalta.[173] Henkilötietojen turvallisuutta uhkaavien riskien arvioinnin ja hallinnan haasteellisuus riippuu täysin siitä, millaisia tietoja käsitellään. Yksilöllisesti ja kollektiivisesti vähäriskisten tietojen käsittely ei vaadi ajallisesti tai kustannuksellisesti paljon resursseja. Tietojen käsittelyn vaatimat resurssit kasvavat sen mukaan, mitä riskisempiä tietoja käsitellään.[174] Tietosuoja-asetuksen 32 artiklan 1 kohdan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet, ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit.

Pankin on huolehdittava, että tietoja käsitellessä noudatetaan asianmukaisia teknisiä ja organisatorisia toimenpiteitä. Tekniset ja organisatoriset toimenpiteet liittyvät henkilötietojen suojaamiseen. Tällaisia toimenpiteitä voi esimerkiksi olla henkilöstön kouluttaminen, henkilöstölle annetut ohjeet ja määräykset, salassapitosopimukset, erilaiset valvontatoimenpiteet, järjestelmien tietoturva ja tietojen salaus. Rekisterinpitäjän on itse määriteltävä asianmukaiset toimenpiteet, käytettävissä oleva tekniikka, kustannukset, käsiteltyjen tietojen luonne, laajuus, asiayhteys ja käsittelyn tarkoitus huomioon ottaen. Toimenpiteitä laadittaessa on myös otettava huomioon rekisteröidyn oikeuksin ja vapauksiin kohdistuvien riskien suuruus.[175] Myös rahanpesulain 9 luvun 1§:n 1 momentin mukaan pankin on huolehdittava henkilöstön kouluttamisesta lain noudattamisen varmistamiseksi. Lisäksi sekä laki luottolaitostoiminnasta[176] että rahanpesulaki[177] edellyttävät, että asiakkaan tiedot, mukaan lukien epäilyttäviä liiketoimia koskevat tiedot, on pidettävä salassa.

Rekisterinpitäjän tulee arvioida tietojen käsittelyyn kohdistuvat riskit ja toimittava niin, että mahdolliset riskit pystyään minimoimaan. Toimimalla näin, rekisteripitäjä pystyy

[173] Pitkänen ym. 2013: 215.
[174] Mantelero 2017: 595.
[175] Pitkänen ym. 2013: 215; Talus ym. 2017: 31.
[176] LuottoL 15:14:1.
[177] RahanpesuL 4:4:1.

varmistamaan, että toiminta noudattaa asianmukaista turvallisuustasoa. Henkilötietojen turvallisuuden varmistaminen edellyttää myös käsittelyn säännöllistä seurantaa ja valvontaa.[178] Säännöllinen seuranta ja valvonta on linjassa myös rahapesulain asettamien, jatkuvaan seurantaan[179] liittyvien vaatimusten kanssa.

Tietosuoja-asetuksen mukaan rekisterinpitäjällä on oikeus harjoittaa tietojen käsittelyssä riskiperusteista lähestymistapaa. Riskiperusteisella lähestymistavalla tarkoitetaan tietojen käsittelyyn liittyvien velvoitteiden ja tietoihin kohdistettujen suojatoimien suhteuttamisten rekisteröidyn oikeuksiin ja mahdollisiin vapauksiin kohdistuviin riskeihin. Riskiperusteisen lähestymistavan avulla pyritään kohdistamaan oikeasuhteiset toimenpiteet tietojen suojeluun kulloisenkin käsittelyn riskin mukaisesti. Tietojen käsittelyn riski voi olla korkeampi tapauksissa, joissa käsitellään esimerkiksi arkaluontoisia, eli erityisiä henkilötietoryhmiä käsittäviä tietoja. Myös usein rekisteröityjen tai suurten tietomäärien käsittely voi nostaa henkilötietojen käsittelyn riskiä. Lisäksi henkilökohtaisten ominaisuuksien arviointi, eli henkilöprofiloinnin suorittaminen, voi kasvattaa käsittelyn riskisyyttä.[180]

Asiakkaan tuntemiseksi kerätyt tiedot käsittävät arkaluontoisia tietoja, minkä lisäksi profilointi on osa asiakkaan tuntemista transaktioiden monitoroinnin kautta. Käsitellyt tietoja asiakasmäärät ovat myös suuria pankin toiminnassa. Näin ollen henkilötietojen turvallisuuteen liittyvä riski asiakkaan tietoja käsitellessä merkittävä, minkä vuoksi riskien hallinta vaatii pankilta erityisen paljon toimenpiteitä.

Seuraava alaluku 4.8. käsittelee rekisteröidyn oikeuksia, etenkin tietojen läpinäkyvyyden ja avoimuuden, käsittelyn rajoittamisen ja estämisen sekä rekisterinpitäjän informointivelvollisuuden näkökulmasta.

4.8. Rekisteröidyn oikeudet

Rekisteröidyn oikeuksien lisääminen on tietosuoja-asetuksen tärkeimpiä prioriteetteja. Tietosuoja-asetuksen myötä rekisterinpitäjän tulee informoida rekisteröityä laajemmin, ja yhä useampi toimi edellyttää rekisteröidyn suostumusta. Henkilötietolakiin jo aiemmin sisältyneiden, tietosuoja-asetuksen myötä tehostuneiden oikeuksien lisäksi tietosuoja-

[178] Talus ym. 2017: 31.
[179] RahanpesuL 3:4:2.
[180] Alvarez 2017: 20; Talus ym. 2017: 16.

asetuksessa on määrätty rekisteröidyille myös uusia oikeuksia.[181] Rekisteröidyn oikeuksien lisääminen aiheuttaa haasteita rahanpesulainsäädännön näkökulmasta, sillä rahanpesulaki on etenkin epäilyttä liiketoimi-ilmoitusten osalta vahvasti salassapitoon painottuvaa.

Tietosuoja-asetuksen myötä rekisteröidyn oikeudet omiin henkilötietoihin ovat kasvaneet. Tietosuoja-asetuksen määrää yksilöille oikeuden saada pääsy omiin tietoihinsa, oikeuden korjata virheellisiä tai puutteellisia tietoja ja oikeuden sekä vastustaa että rajoittaa tietojen käsittelyä.[182] Lisäksi huomattava muutos aiempaan, poikkeustilanteita lukuun ottamatta, on rekisteröidyn oikeus pyytää poistettavaksi kaikki rekisteröityä itseään koskevat tiedot, eli oikeus tulla unohdetuksi.[183]

Tietosuoja-asetuksen yksi pääpainoista on henkilötietojen käsittelyn avoimuus, mikä näkyy rekisterinpitäjään kohdistuvissa yksityiskohtaisissa määräyksissä, jotka koskevat rekisterinpitäjän informointivelvollisuutta ja rekisteröidyn oikeuksien toteutumista. Tietosuoja-asetuksen 15 artiklassa määrätään rekisteröidyn oikeudesta saada pääsy omiin tietoihinsa.[184] Rekisteröidyn pyytäessä rekisterinpitäjän on toimitettava rekisteröidylle henkilötietojen käsittelyä koskevat tiedot kompaktissa, läpinäkyvässä, helposti ymmärrettävässä ja saatavissa olevassa muodossa kuukauden kuluessa asiakkaan esittämästä pyynnöstä.[185] Rahanpesulainsäädännön nojalla asiakkaalle ei voida paljastaa kaikkea asiakkaasta kerättyjä tietoa. Pankki voi ilmoittaa asiakkaalle tästä kerätyt perustiedot, mutta asiakkaalla ei ole oikeutta saada pääsyä epäilyttävästä liiketoimesta tehtyä ilmoitusta koskeviin tietoihin.

Tietojenkäsittelyn avoimuuden lisäksi rekisteröidyllä on tietosuoja-asetuksen nojalla oikeus vaatia rekisterinpitäjää rajoittamaan rekisteröityjä koskevien tietojen käsittelyä. Rekisteröidyllä on oikeus tällaiseen vaatimukseen muun muassa silloin, kun rekisteröity pyytää rekisterinpitäjää oikaisemaan tai poistamaan tietoja. Näin toimimalla rekisteröity ilmaisee, etteivät tiedot ole paikkaansa pitäviä. Henkilötietojen käsittelyä voidaan rajoittaa esimerkiksi estämällä käyttäjien pääsy tiettyihin henkilötietoihin. Rekisteröidyllä on myös oikeus vastustaa tietojen käsittelyä. Rekisterinpitäjällä ei ole lähtökohtaisesti enää

[181] Hughes 2018: 5; Poullet 2018: 775.
[182] Dockeray & Westbrook 2018: 56-58.
[183] O'Connor 2017: 52-54; Talus ym. 2017: 24-25; Young 2017.
[184] Alvarez 2017: 20; Gonçalves 2017: 92.
[185] Talus ym. 2017: 23-24.

oikeutta käsitellä henkilötietoja sen jälkeen, kun asiakas on käyttänyt vastustamisoikeuttaan. Vastustamis- ja käsittelykiellosta voidaan kuitenkin tietosuoja-asetuksen nojalla tietyin edellytyksin poiketa.[186]

Asiakkaalla on oikeus myös asiakkaan tuntemista varten kerättyjen tietojen kohdalla pyytää tietojaan korjattavaksi, jos ne ovat virheellisiä tai vanhentuneita. Asiakkaalla ei kuitenkaan ole oikeutta rajoittaa tietojen käsittelyä takautuvasti, sillä rahanpesulaki edellyttää asiakkaan tietojen säilyttämistä vähintään viiden vuoden ajan. Asiakas ei voi myöskään pyytää rahanpesulain vaatimusten vuoksi tietojaan poistettavaksi, eikä tältä osin voi tulla unohdetuksi[187], ennen kuin viisi vuotta on kulunut asiakassuhteen päättymisestä tai vastaavasti epäilyttävän liiketoimi-ilmoituksen tekemisestä.

Rekisteröidyllä on myös oikeus saada lyhyessä ajassa vastaus rekisterinpitäjältä rekisteröidyn tietojen käsittelyä koskeviin kysymyksiin. Rekisterinpitäjän on lisäksi selitettävä automaattisen päätöksenteon taustalla oleva logiikka ja ne tekijät, joihin tällainen päätöksenteko perustuu. Näiden uudistusten avulla rekisteröidyllä on todennäköisesti pienempi kynnys puuttua hänen henkilötietoja koskevaan käsittelyyn.[188] Myös rahanpesulaki velvoittaa kertomaan asiakkaalle, että asiakkaasta kerättyjä tuntemistietoja voidaan käyttää rahanpesun ja terrorismin rahoittamisen estämistä varten tarvittaviin toimenpiteisiin.

Vaikka tietosuoja-asetus perustuukin vahvasti yksilön yksityisyyden ja henkilötietojen suojaamiseen, on asetuksessa myös määrätty henkilötietojen suojaa rajoittavia tekijöitä. Tietosuoja-asetuksen 23 artiklan mukaan on tiettyjä tilanteita, joissa henkilötietoja voidaan poikkeuksellisesti käsitellä niin, että henkilötietoihin kohdistuva suoja on normaalia heikompi. Myös tällaisissa poikkeustilanteissakin on toimittava keskeisiltä osin yksilön perusoikeuksien ja -vapauksien mukaisesti ja niitä kunnioittaen. Jos henkilötietojen suojaa joudutaan rajoittamaan, on käsittelyn tällöin oltava demokraattisessa yhteiskunnassa välttämätön toimenpide, minkä lisäksi käsittelyn on oltava tarkoitukseen nähden oikeasuhteinen. Tällainen poikkeava käytäntö voi tulla vastaan esimerkiksi tilanteessa, jossa kansallinen puolustus ja turva on taattava, tai kun kyseessä on rikoksen ennalta ehkäiseminen tai muu julkista intressiä palveleva päämäärä.[189] Rahanpesulainsäädännön asettamat velvoitteet voidaan juurikin nähdä poikkeavana käytäntönä, jonka takia asiakkaan oikeuksia joudutaan tietyissä tapauksissa rajoittamaan.

[186] Talus ym. 2017: 26-27.
[187] Hughes 2018: 6.
[188] Poullet 2018: 775.
[189] Lindroos-Hovinheimo 2018: 61.

Seuraava alaluku 4.9. käsittelee rekisterinpitäjän velvollisuuksia. Tietosuoja-asetuksen noudattaminen on jo itsessään rekisterinpitäjän päällimmäinen velvollisuus. Luvussa kuitenkin käsitellään muutamaa, rekisterinpitäjään kohdistunutta velvollisuutta tarkemmalla tasolla.

4.9. Rekisterinpitäjän velvollisuudet

Pankki kohtaa useita velvollisuuksia käsitellessään tietoja asiakkaan tuntemista varten. Osa velvollisuuksista on sisällytetty jo aiempaan henkilötietolakiin, kun taas osa on uusia, tietosuoja-asetuksen myötä tulleita velvoitteita. Pankin velvoitteisiin lukeutuvat muun muassa tietojen käsittelyn dokumentointi, dokumentoitujen tietojen luovuttaminen viranomaisille ja tietojenkäsittelyn vaikutuksenarvioinnin laatiminen.

Tietosuoja-asetuksen myötä tulleet, uudet tietojenhallintavaatimukset eivät kosketa ainoastaan itse tietojenkäsittelyä. Pankin on pystyttävä osoittamaan, millaisiin valmisteluihin tietojen käsittelemiseksi on ryhdytty ja miten tietojenkäsittely on dokumentoitu.[190] Pankilla on lisäksi aiempaa suurempi vastuu pystyä jälkikäteen osoittamaan, miten yrityksen tietojenkäsittely on tosiasiassa hoidettu. Pankin täytyy esimerkiksi pystyä määrittämään, kuinka kauan tietoja säilytetään ja selvittämään, mihin tietojenkäsittely tosiasiallisesti perustuu.[191] Tietojen säilyttämisen ja käsittely perustuu asiakkaan tuntemisen tietojen osalta rahanpesulain säädöksiin, joita pankin on toiminnassaan noudatettava.

Pankin tulee dokumentoida asianmukaisesti miten tietoja on käsitelty ja olla valmis tarvittaessa esittämään dokumentit myös tietosuojaviranomaisille. Pankin täytyy siis pystyä todistamaan noudattavansa toiminnassaan tietosuoja-asetuksen mukaisia määräyksiä.[192] Myös rahanpesulaki määrää, että ilmoitusvelvollisen on salassapitosäännösten estämättä ilman aiheetonta viivytystä toimitettava valvontaviranomaiselle maksutta sen pyytämät tiedot ja selvitykset, jotka ovat välttämättömiä rahanpesulaissa tai sen nojalla annetuissa säännöksissä tai määräyksissä tarkoitetun tehtävän hoitamiseksi.[193] Pankin on siis pystyttävä toimittamaan tarvittavat dokumentit sekä tietosuojaviranomaisille, että rahanpesulain mukaiselle valvontaviranomaiselle, joka pankin tapauksessa on Finanssivalvonta.

[190] O'Connor 2017: 52-54.
[191] O'Connor 2017: 52-54.
[192] Dockeray & Westbrook 2018: 56-58; Talus 2017: 14.
[193] RahanpesuL 7:1:1.

Pankin tulee lisäksi toteuttaa tietosuojaa koskevan vaikutustenarviointi, jonka tulee sisältää yksityiskohtainen kuvaus olennaisista järjestelmistä ja prosesseista, arvio rekisteröityjen yksityisyyttä uhkaavista riskeistä sekä suunnitellun käsittelyn välttämättömyydestä ja oikeasuhteisuudesta. On myös otettava huomioon, että tietosuoja-asetuksen myötä pelkkä määräysten noudattaminen ei riitä. Tietosuoja-asetus painottaa nimenomaan hyvää hallintotapaa ja vastuullisuutta, minkä vuoksi yritysten on asetuksen noudattamisen lisäksi pystyttävä osoittamaan noudattavansa määräyksiä.[194]

[194] Dickie & Yule 2017: 101.

5. SELONOTTO- JA ILMOITUSVELVOLLISUUS

5.1. Selonotto- ja ilmoitusvelvollisuuden taustaa

Rahanpesuregulaatiot asettavat huomattavia velvoitteita pankeille. Asiakkaan tuntemiseen liittyvien tietojen keräämisen ja dokumentoinnin lisäksi pankkeja velvoitetaan kouluttamaan henkilökuntaa havainnoimaan mahdollisia epäilyttäviä tapahtumia ja käyttäytymismalleja sekä ilmoittamaan näistä huomioista tarvittaessa eteenpäin[195], ellei toiminnalle saada selvitystä tai se herättää epäilyksiä selvityksen saamisen jälkeenkin. Aiemmin kolmannessa luvussa esitellyt asiakkaan tuntemiseen liittyvät toimenpiteet ovat keskeisessä asemassa epäilyttävien tapahtumien selvittämisen ja niistä raportoimisen, eli selonotto- ja ilmoitusvelvollisuuden kannalta. Huolellisesti kerätyt ja dokumentoidut asiakkaan tuntemistiedot mahdollistavat etenkin selonottovelvollisuuden toteutumisen, minkä avulla pystytään myöhemmin täyttämään ilmoitusta koskevat velvollisuudet.

Selonotto- ja ilmoitusvelvollisuuden täyttyminen edellyttää epäilyttävien tapahtumien tunnistamisen suuresta massasta tapahtumia[196], jotka sisältävät myös paljon normaalia käyttäytymistä. Jotta epäilyttäviä tapahtumia on mahdollista tunnistaa, tulee asiakkaan tuntemistietojen olla ensinnäkin kunnossa. Tuntemistietojen lisäksi pankilla tulee olla käytössä epäilyttävien tapahtumien monitorointiin tarkoitettu järjestelmä[197], minkä avulla pystytään seulomaan tapahtumia ja käyttäytymismalleja, joiden voidaan katsoa olevan riskisiä ja indikoivan epäilyttävää toimintaa. Asiakastiedot ja monitorointijärjestelmät eivät kuitenkaan yksinään riitä havaitsemaan todellisia epäilyttäviä tapahtumia, vaan niiden lisäksi pankilla tulee olla työllistettynä ammattilaisia, joiden tehtävänä on manuaalisesti arvioida ja analysoida tapahtumia[198].

Selonotto- ja ilmoitusvelvollisuus edellyttävät pankilta hyvin laaja-alaista ja kattavaa henkilötietojen käsittelyä. Selonotto- ja ilmoitusvelvollisuutta noudattaessa useampikin tietosuoja-asetuksen 4 artiklan 2 alakohdan tietojen käsittelyä koskevista määritelmistä toteutuu, sillä selonotto- ja ilmoitusvelvollisuuden täyttäminen edellyttää muun muassa tietojen keräämistä, tallentamista, hakua, kyselyä, käyttöä sekä tietojen luovuttamista. Rahanpesulainsäädännön määräämien velvoitteiden lisäksi on siis otettava myös tietosuoja-asetuksen määräykset huomioon. Pankin on harkittava kuinka paljon ja millaista tietoa

[195] Sica 2000: 53.
[196] Doughty 2005: 248.
[197] Doughty 2005: 248.
[198] Doughty 2005: 248; Mat-Isa ym. 2015: 7.

on kerättävä, jotta on mahdollista erottaa epäilyttävä tapahtumat normaalista toiminnasta, vaarantamatta kuitenkaan tarpeettomasti asiakkaan yksityisyyttä, tai vastaavasti laiminlyömättä pankin lakisäädännäistä selonotto- ja ilmoitusvelvollisuutta.

Seuraavassa alaluvussa 5.2. perehdytään tarkemmin siihen, mihin selonottovelvollisuus perustuu ja millaisia toimia sekä tietolähteitä selonottovelvollisuuteen sisältyy.

5.2. Selonottovelvollisuus

Selonottovelvollisuudella tarkoitetaan pankeille asetettua vaatimusta hankkia lisää tietoa epätavallisista tai epäilyttävistä tilitapahtumista tai muusta vastaavasta toiminnasta. Pankkien on otettava selvää, mihin epäilyttävät tapahtumat perustuvat, ja saatujen tietojen perusteella tehdä päätös siitä, tuleeko toiminnasta ilmoittaa eteenpäin rahanpesunselvittelykeskukselle.[199] Selonottovelvollisuutta täyttäessä on otettava huomioon pankin ja lainvalvontaviranomaisten välinen ero. Pankilla ja sen työntekijöillä ei ole lainvalvontaviranomaisia vastaavaa koulutusta, auktoriteettiasemaa tai missiota, eikä näin ollen myöskään kompetenssia tai valtaa tehdä olettamuksia tai päätöksiä sen suhteen, onko jokin käytös rikollista toimintaa vai ei. Tästä huolimatta pankilla on kuitenkin alan osaamiseen ja kokemukseen perustuvaa asiantuntijuutta, minkä avulla se pystyy tunnistamaan mitkä tilitapahtumat ovat epätavallisia ja epäilyttäviä, sekä millaiset toimintamallit ovat rationaalisesta taloudellisesta toiminnasta poikkeavia.[200]

Pankilla on oikeus pyytää asiakkaalta tarkempia tietoja liittyen asiakkaan asiointiin ja maksuliikenteeseen. Esimerkiksi tilille tulevien varojen alkuperästä, varojen käyttötarkoituksesta ja maksuliikenteen perusteista voidaan pyytää tarkempia, kirjallisia selvityksiä. Selvityksen tueksi voidaan pyytää dokumentteja, kuten kauppakirjoja tai muita asiakirjoja, joiden avulla tapahtumat pystytään luotettavasti todentamaan.[201]

Selonottovelvollisuutta noudattaessaan pankin on otettava rahanpesulainsäädännön asettamien velvoitteiden lisäksi huomioon myös tietosuoja-asetuksen vaatimukset henkilötietojen käsittelystä, sillä selonottovelvollisuuden toteutuminen edellyttää asiakastietojen käsittelyä ja keräämistä, kuten kyselyä, hakua ja tallentamista. Asiakkaalta voidaan esi-

[199] Finanssivalvonta 2017 b.
[200] Axelrod 2017: 462.
[201] Finanssivalvonta 2017 a.

merkiksi kysellä tietoja tämän maksuliikenteestä, minkä lisäksi tietoja voidaan hakea tapahtumien selvittämiseksi tai päätöksenteon tueksi ulkoisista lähteistä. Pankin on tietojen keräämisen lisäksi pystyttävä todentamaan, mihin se on perustanut päätöksensä asiakkaan toiminnasta. Todentamisen vuoksi asiakkaalta saadut tiedot on tallennettava mahdollisia myöhempiä, viranomaisten suorittamia valvontatoimenpiteitä varten. Tietosuojalainsäädännön huomioiminen on erittäin tärkeää, sillä tutkinnan yhteydessä kerättyjä tietoja käsitellessä pankilla on potentiaalisen rikollisen toiminnan havaitsemisen ohella riskinä vaarantaa asiakkaan yksityisyys keräämällä tietoja tarpeettomasti ja harkitsemattomasti.

Jotta epäilyttäviä tapahtumia pystytään havaitsemaan ja raportoimaan eteenpäin, on osattava erottaa epäilyttävä käyttäytyminen normaalista. Epäilyttävät tapahtumat eivät ole aina yksiselitteisiä ja objektiivisesti määriteltävissä. On kuitenkin joitakin suuntaa-antavia tekijöitä, joista voi olla apua tapahtumia tarkasteltaessa. Rahanpesulain 3 luvun 4 §:n 3 momentin mukaan ilmoitusvelvollisen on erityisesti kiinnitettävä huomiota liiketoimiin, jotka rakenteeltaan tai suuruudeltaan taikka ilmoitusvelvollisen koon tai toimipaikan osalta poikkeavat tavanomaisesta. Samoin on meneteltävä, jos liiketoimilla ei ole ilmeistä taloudellista tarkoitusta tai ne eivät sovi yhteen sen kokemuksen tai tietojen kanssa, jotka ilmoitusvelvollisella on asiakkaasta.

Pankkien asiakasmäärät ovat pääsääntöisesti niin suuria, ettei tapahtumien läpikäyminen manuaalisesti ole mahdollista. Tämän vuoksi pankeilla tulee olla käytössään tähän tarkoitukseen suunniteltu ohjelmisto, joka seuloo tapahtumat automaattisesti ja erottaa epänormaalin käyttäytymisen normaalista. Transaktioiden monitorointiin tarkoitetut ohjelmistot ovat suunniteltu juurikin tähän tarkoitukseen.[202] Ohjelmistossa tulisi yhdistyä reaaliaikainen maksuseulonta, transaktioiden monitorointi sekä asiakkaiden tarkastus muun muassa pakotelistoja vastaan. Ohjelmisto analysoi tapahtumia hyödyntäen sekä kontekstuaalista että historiallista tietoa. Näin pystytään tunnistamaan yksittäisiä riskitekijöitä sekä tiedossa olevia, rahanpesuun ja terrorismin rahoittamiseen liittyviä toimintamalleja.[203]

Tilitapahtumien automaattinen käsittely epänormaalin toiminnan havaitsemiseksi herättää kysymyksiä tietosuoja-asetuksen automatisoituja yksittäispäätöksiä ja profilointia käsittelevän 22 artiklan näkökulmasta. Vaikkei tietojen automaattisen käsittelyn voida rahanpesulainsäädännön kontekstissa nähdä olevan yksiselitteisesti artiklan mukaista profilointia, ei toiminta ole ongelmatonta asiakkaan yksityisyydensuojan näkökulmasta. Tietynlaisten transaktioiden ja käyttäytymiskaavojen tuottamat hälytykset eivät itsessään ole

[202] Ramage 2012: 276.
[203] Amicelle 2011: 167.

epäilyttäviä, vaan tapahtumien epäilyttävyyden tunnistaminen vaatii aina myös manuaalisen tutkinnan. Manuaalisen tutkinnan johtaessa esimerkiksi siihen tulokseen, ettei toiminta ole epäilyttävää, on asiakkaan tietoja ehditty mahdollisesti käsitellä jo hyvinkin laajasti. Tällöin asiakkaan yksityisyys on joutunut uhatuksi automaattisen profiloinnin johdosta, ilman että asiakkaan toiminta olisi tosiasiallisesti ollut epäilyttävää. Kuten aiemmin riskiperusteista arviointia käsittelevässä alaluvussa 3.3. on todettu, automaattista tietojenkäsittelyä on mahdotonta rahanpesun ja terrorismin rahoittamisen estämisen kontekstissa kieltää, mutta profilointia harjoittavia tietojärjestelmiä sen sijaan olisi hyvä kehittää epäilyttävän toiminnan havaitsemisen osumatarkkuuden osalta.

Monitorointiin tarkoitettujen järjestelmien lisäksi asiakkaasta on mahdollista saada tietoa myös julkisista lähteistä. Tällaisia lähteitä ovat esimerkiksi uutisartikkelit ja tuomioistuinten päätökset. Myös muista lähteistä voi löytyä tietoa, jonka perusteella on syytä epäillä asiakkaan mahdollisesti piilottelevan pankin liiketoiminnan tai riskihalukkuuden kannalta oleellisia asioita.[204] Esimerkiksi Suomen Asiakastieto Oy:stä saatavat yritysyhteys- ja henkilöluottotiedot voivat paljastaa asiakkaasta pankkisuhteen perustamisen tai jatkamisen kannalta epäedullisia asioita. Jos asiakkaan menneisyydestä paljastuu aiempia rikkomuksia, voidaan sen nähdä indikoivan myös vastaavanlaisia käytösmalleja sekä tässä hetkessä että tulevaisuudessa. Tämän takia tiedot asiakkaan aiemmasta toiminnasta ovat erittäin arvokkaita pankille, sillä ne ovat merkittävässä asemassa riskiarviointia tehdessä.[205]

Tietosuoja-asetuksen 5 artiklan 1 kohdan d alakohdan mukaan henkilötietojen tulee olla täsmällisiä. Vaatimus näyttäytyy haastavana joidenkin rahanpesua ja terrorismin rahoittamisen estämistä varten kerättyjen tietojen kohdalla, sillä tietoja kerättäessä pankki voi käyttää myös ulkoisia lähteitä asiakkaan tilitapahtumien ja käyttäytymisen selvittämisen tukena. Pankilla ei ole ulkoisten lähteiden kohdalla varmuutta siitä, ovatko tiedot täsmällisiä, tarkkoja tai pitävätkö ne ylipäätään paikkansa. Ulkoisia lähteitä käyttäessä syntyykin riski siitä, käsitteleekö pankki mahdollisesti virheellisiä tietoja asiakkaan vahingoksi ja perustetaanko päätös asiakkaan toiminnan luonteesta potentiaalisesti vääriin tietoihin.

[204] Lowe 2017: 475.
[205] Lowe 2017: 475.

Laki ja lainvalvontaviranomaiset kuitenkin edellyttävät, että epäilyttävä toiminta on tutkittava tarkasti, jotta pankki voi varmistua siitä, edellyttääkö toiminta raportoimista rahanpesunselvittelykeskukselle.[206] Pankit pystyvät tunnistamaan epätavalliset ja epäilyttävät tapahtumat joutumatta kuitenkaan käymään läpi samoja prosesseja, joita lainvalvontaviranomaiset joutuvat varmistaakseen, onko toiminta laitonta vai ei. Lainvalvontaviranomaisen tehtäväksi jää siis suorittaa tarkempi ja kattavampi tutkinta eri tietoja ja tietokantoja hyödyntäen.[207] Pankin tehtävä onkin havaita poikkeavat ja epäilyttävät tapahtumat ja jättää mahdolliset jatkoselvitykset viranomaisille. Usein epäilyttävyyden havaitseminen ei vaadi yhtä kattavia toimenpiteitä kuin sen yksiselitteinen toteaminen, onko toiminta rikollista vai ei. Tämän näkemyksen valossa pankin olisi harkita kuinka paljon asiakkaasta tosiasiallisesti on kerättävä tietoa toiminnan selvittämistä varten.

Seuraavassa alaluvussa 5.3. perehdytään tarkemmin selonottovelvollisuudesta seuraavaan ilmoitusvelvollisuuteen. Luvussa käsitellään ilmoitusvelvollisuutta sekä lain velvoittamien tilanteiden että pankin oman riskiperusteisen arvion ja harkinnan näkökulmasta.

5.3. Ilmoitusvelvollisuus

Valtio on saanut pankit mukaan rahanpesun ja terrorismin rahoittamisen torjuntaan velvoittamalla pankkeja ilmoittamaan epäilyttävistä liiketoimista tai asiakkuuksista[208]. Pankin on lakiperusteisen velvollisuuden nojalla ilmoitettava tällaisista tapahtumista tai toiminnasta eteenpäin rahanpesunselvittelykeskukselle, joka voi tarpeen katsoessaan aloittaa pankin toimittamien tietojen perusteella tarkemman tutkinnan, tai vastaavasti saadun informaation avulla täydentää jo olemassa olevan rikostutkinnan tietoja.[209]

Mahdollisien rahanpesuun liittyvien epäilyttävien tapahtumien ilmoittaminen onkin yksi rahanpesun ja terrorismin rahoittamisen estämisen päätekijöistä. Tällaisten tapahtumien raportointi on välttämätöntä, jos halutaan tehokkaasti vaikuttaa rahanpesun torjuntaan. Rahanpesua harjoitetaan usein sellaisten järjestelmien kautta, joihin viranomaisilla ei ole pääsyä, minkä takia pankit ovat tärkeässä roolissa mahdollistaen viranomaisten tiedonsaannin.[210]

---

[206] Burt 2005: 18-19.
[207] Axelrod 2017: 466.
[208] Sica 2000: 53.
[209] Axelrod 2017: 462.
[210] Stessens 2000: 159-160.

Epäilyttävästä tai poikkeavasta liiketoimesta, joka voi mahdollisesti viitata rahanpesuun tai terrorismin rahoittamiseen, on tehtävä viipymättä ilmoitus rahanpesun selvittelykeskukselle. Aika on tärkeä tekijä ilmoitusta laadittaessa, sillä nopealla reagoinnilla varmistetaan, ettei varoja ehditä siirtää viranomaisten ulottumattomiin. Usein tilanne voi kuitenkin olla se, että epäilyttävät tapahtumat huomataan vasta jälkikäteen. Myös tällaisissa tilanteessa ilmoitus tulee tehdä heti, kun tapahtumat on huomattu.[211]

Jotta pankki voi täyttää ilmoitusvelvollisuutensa, tulee sen ensin olla perillä epäilyttävien ja poikkeavien tapahtumien tai käytöksen perusteista. Tämä tarkoittaa sitä, että pankin on otettava tarkemmin selvää sellaisista liiketoimista, jotka poikkeavat normaalista esimerkiksi maksujen suuruuden tai rakenteen osalta, tai eivät sovi muutoin yhteen asiakkaan profiilin kanssa[212]. Jos asiakkaalta ei saada tilanteen edellyttämiä riittäviä tietoja, on tapahtumien suorittamisesta jatkossa kieltäydyttävä ja tarpeen vaatiessa harkittava asiakassuhteen lopettamista. Tällaiset asiakkaan tuntemista estävät tekijät ja toimenpiteet palveluiden rajoittamiseksi luonnollisesti velvoittavat lisäksi tekemään ilmoituksen epäilyttävästä liiketoimesta rahanpesun selvittelykeskukselle.[213]

Jos asiakkaalta saadaan selvitys poikkeaville ja epäilyttäville tapahtumille, mutta käytös herättää vielä selvityksen jälkeenkin epäilyksiä, tulee rahanpesun selvittelykeskukselle tehdä ilmoitus epäilyttävästä liiketoimesta. Ilmoitus on myös tehtävä silloin, jos aiemmin normaaliksi katsottu käyttäytyminen herättää epäilyksiä uusien, esiin nousseiden seikkojen valossa. Jos pankki suorittaa epäilyttävän liiketoimen tarkoituksenaan edesauttaa epäilyttävän tapahtuman selvittämistä, tai jos pankki vastaavasti kieltäytyy suorittamasta epäilyttävää liiketoimea, tulee luonnollisesti myös näissä tapauksissa ilmoittaa eteenpäin viranomaiselle.[214]

Pankkeja velvoitetaan ilmoittamaan eteenpäin viranomaisille kaikista epäilyttävistä liiketoimista[215]. Koska laki ei tarjoa yksiselitteistä vastausta siihen, millaisen toiminnan voidaan katsoa olevan epäilyttävää, on pankeilla usein vastuu tiettyjen, annettujen raamien puitteissa itse määritellä, mikä on epäilyttävää ja mikä ei.[216] Epäilyttävä liiketoimi onkin siten hyvin subjektiivinen käsite, ja jättää pankille ja etenkin tapausta tutkivalle henkilölle paljon tulkinnanvaraa. Tosiasia kuitenkin on, että pankeilla on vain rajallinen määrä tietoa

[211] Finanssivalvonta 2017 b.
[212] Finanssivalvonta 2017 b.
[213] de Koker 2006: 31.
[214] Finanssivalvonta 2017 b.
[215] Doughty 2005: 249.
[216] Stessens 2000:169.

liittyen asiakkaaseen ja tämän toimintaan. Pankeilla ei myöskään ole yksityisenä tahona oikeutta vaatia asiakkaalta toimintaa selventäviä tietoja, toisin kuin esimerkiksi viranomaistahoilla on. Pankki voi ainoastaan pyytää asiakkaalta toivomiaan tietoja.

Vaikka laki edellyttääkin pankkia raportoimaan epäilyttävistä liiketoimista, valvontaviranomaiset kuitenkin toivovat, ettei pankki lähetä ilmoituksia ilman tarkkaa harkintaa ja tutkintaa. Vielä aiemmin pankit saivat palautetta siitä, ettei ilmoituksia epäilyttävistä liiketoimista tehdä tarpeeksi. Tilanne on kuitenkin muuttunut, ja ilmoituksia lähetetään nykyään huomattavasti aiempaa enemmän.[217] Syy ilmoituksien lisääntymiselle voi olla pankkien valveutuneisuuden lisääntymisessä. Valveutumisen lisäksi kysymys voi olla myös tarpeettomista, varmuuden vuoksi tehdyistä ilmoituksista. Tapahtumia on saatettu raportoida ilman huolellista tutkintaa, jonka avulla olisi ollut mahdollista huomata, ettei kyseessä ole aidosti epäilyttävä liiketoimi[218].

Puutteellisesta tutkinnasta johtuvien turhien ilmoitusten tekeminen on johtanut siihen, etteivät viranomaiset pysty käsittelemään kaikkia saapuvia ilmoituksia. Lainsäätäjät ja lainvalvontaviromaiset edellyttävät, että pankeilla on asiakkaan tuntemisen liittyvän prosessin myötä tarvittavat tiedot asiakkaistaan, minkä lisäksi pankkien tulee asianmukaisesti olla perillä asiakkaan tosiasiallisista tilitapahtumista tilitapahtumien monitoroinnin avulla.[219]

Koska asiakkaasta saatavilla olevat tiedot ovat rajallisia, eikä laki anna yksiselitteistä määritelmää epäilyttävälle liiketoiminnalle, perustuu päätös epäilyttävän liiketoiminnan ilmoittamiseen yksinomaan pankin tiedossa oleviin seikkoihin, aiempaan kokemukseen ja tapausta tutkivan työntekijän henkilökohtaiseen näkemykseen. Epäilyttävän liiketoimen väljä määritelmä tarjoaakin sekä mahdollisuuksia että haasteita pankille. Ilmoitusten tekeminen on toisaalta tehokkaampaa, kun voidaan luottaa koulutetun henkilökunnan kokemukseen ja harkintaan, kun taas toisaalta resursseja voidaan kohdistaa vääriin asioihin, kun tutkinnalla ei ole tarkkaa, lain asettamaa fokusta.

Ilmoitusvelvollisuutta noudattaessaan pankin on otettava rahanpesulainsäädännön ohella huomioon tietosuojalainsäädännön asettamat velvoitteet tietojen käsittelylle. Ilmoitusvelvollisuuden kääntöpuolena onkin yksilön oikeus yksityisyyteen ja sen suojaan – vaarannetaanko yksityisyyden suoja antamalla viranomaisille suuri määrä tietoa ilman virallisia

[217] Burt 2005: 18-19.
[218] Burt 2005: 18-19.
[219] Burt 2005: 18-19.

haasteita tai muita vastaavia, tiedon saannille asetettuja esteitä.[220] Rahanpesulain velvoittamana epäilyttävistä liiketoimista on luonnollisesti ilmoitettava eteenpäin rahanpesunselvittelykeskukselle. Pankilla on kuitenkin mahdollisuus harkita potentiaalisesti epäilyttäviä tapahtumia tutkiessaan, missä määrin asiakkaan tilitapahtumia ja muita henkilötietoja on tarpeellista tutkia, jotta saadaan selvitettyä, onko kyseessä aidosti epäilyttävä tapahtuma, vai löytyykö alun perin epäilyttävältä vaikuttaneen toiminnan taustalta selventäviä tekijöitä, joiden myötä pankki välttyisi tarpeettoman ilmoituksen tekemiseltä.

Ilmoitusvelvollisuuden yhteydessä tulee huomioida, ettei pankilla, sen johdolla tai henkilökunnalla ole missään tilanteessa oikeutta paljastaa asiakkaalle tai kolmannelle osapuolelle, että asiakkaan tiedot on luovutettu viranomaisille, tai että asiakas on tutkinnan alla epäiltynä rahanpesusta tai terrorismin rahoittamisesta.[221] Jos asiakkaan palveluita esimerkiksi päädytään ilmoituksen johdosta rajoittamaan, asiakkaalle ei saa ilmoittaa rajoituksen johtuvan ilmoituksen tekemisestä. Tietoja ei saa myöskään asiakkaan nimenomaisesta vaatimuksesta huolimatta luovuttaa, vaikka asiakkaalla onkin tietosuoja-asetuksen 15 artiklan 1 kohdan mukaan oikeus saada pääsy omiin tietoihin. Tämä johtuu siitä, että rahanpesulaki ja sen 4 luvun 4 §:n ensimmäisen momenttia voidaan pitää erityislakina ja ensisijaisesti sovellettavana tietosuoja-asetuksen 15 artiklaan nähden.

Seuraavassa alaluvussa 5.4. perehdytään asiakkaan jatkuvaan seurantaan. Asiakkaan jatkuva seuranta on tärkeää tietosuoja-asetuksen asettamien velvollisuuksien valossa, minkä lisäksi myös rahanpesulaki velvoittaa pankkia tuntemaan asiakkaansa koko asiakassuhteen keston ajan.

5.4. Jatkuva seuranta

Velvoite asiakkaan jatkuvalle seurannalle perustuu sekä rahanpesulakiin että tietosuoja-asetukseen. Pankin on rahanpesulain 3 luvun 4 §:n 2 momentin mukaan järjestettävä asiakkaan toiminnan laatuun ja laajuuteen, asiakassuhteen pysyvyyteen ja kestoon sekä riskeihin nähden riittävä seuranta sen varmistamiseksi, että asiakkaan toiminta vastaa sitä kokemusta ja tietoa, joka ilmoitusvelvollisella on asiakkaasta ja tämän toiminnasta. Tietosuoja-asetuksen 5 artiklan 1 kohdan d alakohdassa sen sijaan tuodaan esiin täsmällisyysvaatimus, jonka mukaan henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitet-

[220] Axelrod 2017: 466.
[221] Stessens 2000: 163.

tyjä, minkä lisäksi on toteutettava kaikki mahdolliset kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden epätarkat ja virheelliset henkilötiedot poistetaan tai oikaistaan viipymättä.

Asiakkaan tuntemisen velvoitteet eivät siis koske yksinomaan uusia asiakkuuksia. Myös olemassa olevien asiakkaiden tuntemisen tiedot tulee olla virheettömiä ja ajan tasalla. Pankki voi käyttää riskiin perustuvaa harkintaa päättäessään asiakkaan tuntemisen tasosta ja tuntemistietojen päivittämisen tiheydestä.[222] Asiakassuhteen kehitystä ja palveluiden käyttöä on seurattava kuitenkin koko asiakassuhteen ajan. Asiakkaan jatkuva tunteminen on tärkeä osa pankin riskienhallintaa ja sisäistä valvontaa.[223]

Asiakkuuden riskitason määrittäminen on asiakkaan tuntemisen kannalta keskeinen tekijä, sillä sen perusteella pystytään arvioimaan, kuinka usein asiakkaan tietoja tulee päivittää ja millä aikavälillä asiakkaan tilitapahtumia on seurattava[224]. Riskiarviolla on suuri merkitys jatkuvaan seurantaan liittyvien tekijöiden osalta. Tilitapahtumien seuranta on pidettävä mahdollisimman tarkoituksenmukaisena ja luonnollisesti myös kustannustehokkaana, koska kyse on lain asettamista velvoitteista huolimatta liiketoiminnasta. Jotta molemmat edellä mainituista vaatimuksista täyttyisivät, tulee pankeilla olla käytössään tilitapahtumien monitorointiin suunnitellun ohjelmiston lisäksi myös hyvin koulutettuja työntekijöitä, jotka pystyvät ohjelmiston tuottaman datan perusteella analysoimaan tietoa ja havaitsemaan poikkeukselliset ja epäilyttävät tapahtumat normaalien tapahtumien joukosta.[225]

Kaikkia asiakkaita ei siis tarvitse seurata saman ajanjakson välein samalla tarkkuudella, vaan asiakas on luokiteltava asiakkaan sen hetkisen riskitason mukaisesti joko normaalin tai korkean riskin asiakkaaksi. Asiakkaiden jaottelu riskien perusteella on juurikin tarkoituksenmukaista ja kustannustehokasta resurssien hallintaa. Toimimalla näin, säilytetään myös suurempi yksityisyyden suoja niillä asiakkailla, joiden kohdalla tiheä monitorointi ja tietojen päivittäminen ei ole välttämätöntä. Jatkuva seuranta kaikkien asiakkuuksien kohdalla kuitenkin takaa sen, että mahdolliset muutokset asiakkaan käyttäytymisessä tulevat huomatuiksi, ja asiakas voidaan tarvittaessa nostaa tehostettuun seurantaan, jos asiakkaan nähdään täyttävän korkean riskin asiakkaan tuntomerkit.

[222] de Koker 2016: 31.
[223] Finanssivalonta 2017 b.
[224] de Wit 2007: 159.
[225] de Wit 2007: 159,

Koska pankkien palveluiden käyttäminen rahanpesun ja terrorismin rahoittamisen välikätenä on valitettavan yleistä, on pankkien pystyttävä hallitsemaan ja vähentämään palveluidensa väärinkäytön riskiä. Kuten aiemmin on käynyt jo ilmi, muiden asiakkaan tuntemiseen liittyvien toimenpiteiden ohella riskiä pystytään minimoimaan monitoroimalla asiakkaiden tapahtumia. Monitoroinnin avulla on mahdollista tunnistaa poikkeuksellisia tilitapahtumia tai käytösmalleja, jotka voivat indikoida rahanpesua tai terrorismin rahoittamista.[226]

Talousrikollisten toiminta noudattaa usein sen hetkisen tilanteen trendejä. Tämän vuoksi on mahdollista kehittää erilaisia skenaarioita, joihin toteutuneita tapahtumia voidaan verrata[227]. Aiemmin esitellyt monitorointiin tarkoitetut ohjelmistot voivat havaita tällaisia epäilyttäviä tai riskisiä kaavoja[228], ja nostaa niitä esiin tarkempaa tutkintaa varten. Vaikka kaavat ovat hyödyllisiä ja käyttökelpoisia tapoja seurata epäilyttäviä tapahtumia, eivät ne kuitenkaan ota huomioon rahanpesun ja terrorismin rahoittamisen tunnusmerkillistä ominaisuutta: dynaamisuutta. Rahanpesun ja terrorismin rahoittamisen keinot muuttuvat alati, minkä takia yksinomaan jälkikäteisellä seurannalla ei päästä riittäviin tuloksiin. Jälkikäteen tapahtuvan seurannan rinnalle olisi hyvä kehittää ennakoivia järjestelmiä. Myös tämän takia on tärkeää, että kaikkia asiakkaita monitoroidaan säännöllisin väliajoin, sillä aiemmin normaalilta vaikuttanut käyttäytyminen voidaan nähdä riskisenä uusien tietojen ja trendien valossa.

[226] de Wit 2007: 159.
[227] Böszörmenyi & Schweighofer 2015: 68.
[228] Favarel-Garrigues, Godefroy & Lascoumes 2011: 183.

6. HAASTEET PANKILLE

6.1. Lainsäädäntöjen vastakkaiset intressit

Fundamentaalisin haaste rahanpesulain ja tietosuoja-asetuksen yhteensovittamisessa on näiden kahden lainsäädännön täysin vastakkaiset intressit. Rahanpesulainsäädäntö velvoittaa pankkia hankkimaan tietoja maksimaalisissa määrin, kun taas tietosuoja-asetus pyrkii rajoittamaan käsitellyn tiedon määrää. Kuten Reese[229] toteaa, rahanpesu- ja tietosuojalainsäädännön intressikonfliktista johtuen lainsäädäntöjen samanaikainen soveltaminen aiheuttaa väistämättä haasteita pankille. Vaikka tietosuoja- ja rahanpesulainsäädännän väliset haasteet eivät itsessään ole uusia, ovat niiden väliset ristiriidat korostuneet tietosuoja-asetuksen myötä.

Rahanpesulainsäädäntö edellyttää pankkia hankkimaan, käsittelemään ja analysoimaan suuria määriä henkilötietoja. Henkilötietojen käsittelyn tarkoituksena rahanpesulainsäädännön näkökulmasta on suojella rahoitusalaa ja yhteiskuntaa kokonaisuudessaan rahanpesulta ja terrorismin rahoittamiselta. Tietosuoja-asetus sen sijaan määrittelee miten, milloin ja miksi henkilötietoja tulee kerätä, käsitellä ja käyttää. Näiden määräysten lisäksi tietosuoja-asetuksen myötä henkilötietojen käsittelyn määritelmä on laajentunut. Laajentuneen määritelmän mukaisesti lähes kaikki rahanpesulainsäädännön nojalla kerätyt tiedot lukeutuvat tietosuoja-asetuksen piiriin.[230] Rahanpesulain ja tietosuoja-asetuksen väliset intressit voidaan nähdä siis tietojen käsittelyä perustavanlaatuisempana haasteena. Rahanpesulainsäädäntö pyrkii suojelemaan yhteiskuntaa, kun taas tietosuoja-asetuksen tarkoituksena on suojella yksilöitä.

Rahanpesu- ja tietosuojalainsäädännön tarkoitusperien eroavaisuuksien lisäksi jatkuvasti muuttuvat lainsäädännöt, ja muutokset jo olemassa oleviin lainsäädäntöihin ovat jo itsessään haaste pankille[231]. Organisaatioiden onkin pyrittävä löytämään tasapaino rahanpesu- ja tietosuojalainsäädännön välillä varmistaen, että rahanpesulainsäädännön noudattamiseksi käsitellyt tiedot ovat linjassa tietosuoja-asetuksen kanssa[232]. Tasapainon löytäminen on pankeille suuri haaste lainsäädäntöjen intressikonfliktin ja lainsäädäntöympäristön dynaamisuuden lisäksi myös siksi, että molemmat lainsäädännöt ovat hyvin uusia eikä

[229] Reese 2018.
[230] Reese 2018.
[231] Preziosi 2017.
[232] Khan 2016.

vakiintunutta oikeuskäytäntöä vielä ole saatavilla näiden kahden lain välisten eroavaisuuksista syntyvien ongelmien ratkaisemiseksi.

6.2. Pankin ja viranomaisten ero

Ainoastaan pankkien ei pidä asennoitua uudelleen tietosuoja-asetuksen myötä muuttuneeseen lainsäädäntöön ja sen aiheuttamiin haasteisiin. Ennen kun pankkien voi olettaa muuttavan ajatusmaailmaansa, tulee viranomaisten ottaa vastuuta lainsäädäntöympäristön systematisoinnista. Pankkien on mahdotonta luovia näiden kahden lainsäädännön välillä niin kauan, kun oikeudentila on epäselvä. Epäselvän oikeustilan lisäksi rahanpesun ja terrorismin rahoittamisen estäminen vaikuttaa edelleen olevan viranomaisille yksilön tietojen ja yksityisyyden suojaamista tärkeämpi missio.[233] Pankki onkin erittäin haastavassa tilanteessa yrittäessään noudattaa sekä rahanpesulain että tietosuoja-asetuksen vaatimuksia tilanteessa, jossa edes viranomaiset eivät osaa antaa yksiselitteisiä vastauksia lakien välisen intressikonfliktin selvittämiseen.

Tietosuoja-asetuksen myötä pankkien on väistämättä otettava jossain määrin vähemmän vastuuta epäilyttävien tapahtumien selvittämisessä. Pankki ei voi enää tietojen keräämisen minimoinnin näkökulmasta kerätä asiakkaista valtavia määriä tietoja epäilyttävyyden varmistamiseksi tai viranomaisia hyödyttävän kattavan tutkinnan ja selvittelyn tekemiseksi. Pankin olisikin jatkossa hyvä keskittyä ainoastaan rahanpesulain noudattamisen kannalta olennaisten ja mahdollisimman vähäisen tietomäärän keräämiseen, ja jättää vastuu laajemmasta tutkinnasta viranomaisille.

6.3. Tietojen määrä ja laatu

Tietosuoja-asetuksen näkökulmasta asiakkaan tuntemiseksi kerättyjä tietoja ei tulisi käsitellä varmuuden vuoksi tarpeettoman laajasti edes rahanpesulain velvoitteiden täyttämiseksi. Pankin on pystyttävä todentamaan, että asiakkaasta kerätyt tiedot ovat linjassa asiakkaan riskitason kanssa. Tämä ei ole tärkeää ainoastaan viranomaisvalvonnan näkökulmasta, vaan myös asiakkaiden näkökulmasta. Vaikka pankki ei saa paljastaa asiakkaalle arvioimaansa riskitasoa, on pankin hyvä pystyä tarvittaessa näyttämään toteen, ettei se ole kerännyt tarpeettomissa määrin tietoa asiakkaan muodostamaan riskitasoon

[233] Preziosi 2017.

nähden.[234] Tietosuoja-asetuksen mukaisesti asiakkaan tietoja saa käsitellä vain tarvittavissa määrin tietyn tarkoituksen suorittamista varten. Jos riskiarvion jälkeen päädytään siihen, että asiakas kuuluu yksinkertaistetun tuntemisen piiriin, on asiakkaasta mahdollisesti jo ehditty kerätä tarkoitukseen nähden liian paljon tietoa[235]. Toisaalta tietoa ei olisi voitu kerätä yhtään vähempää päästääkseen tähän lopputulokseen, sillä muuten riskiarvion suorittaminen ei olisi mahdollista. Kerätyn tiedon määrää onkin haastavaa rajata asiakkaan tuntemiseen liittyviä toimenpiteitä suorittaessa, sillä asiakkaan muodostamasta riskistä on asiakassuhdetta perustettaessa pystyttävä muodostamaan riittävän selkeä kuva.

Tietojenkäsittely tulee ottaa huomioon myös selonotto- ja ilmoitusvelvollisuutta täyttäessä. Selonotto- ja ilmoitusvelvollisuuden kohdalla pankilla on muihin asiakkaan tuntemiseen liittyviin vaiheisiin verrattuna hieman paremmat edellytykset harkita, kuinka paljon asiakkaasta tulisi kerätä tietoa. Pankin on punnittava, millaisia riskejä ja hyötyjä kerätyn tiedon määrä aiheuttaa etenkin ilmoitusvelvollisuuden täyttämisen näkökulmasta. Pankin kerätessä asiakkaasta kattavasti tietoja selonottovelvollisuuden täyttämiseksi ja epäilyttävältä vaikuttavan toiminnan selvittämiseksi, pankki voi välttyä epäilyttävän liiketoimi-ilmoituksen tekemiseltä toiminnan muuttuessa ymmärrettäväksi kerätyn tiedon valossa. Tällaisessa tilanteessa pankki välttyy turhien tietojen luovuttamiselta viranomaisille, näin ollen onnistuen asiakkaan yksityisyyden suojelemisessa. Varjopuolena kuitenkin on, että pankki on selvitystä tehdessään mahdollisesti kerännyt asiakkaasta myös tarpeettoman paljon tietoa, vaarantaen asiakkaan yksityisyyden säilymisen.

Vastaavasti pankin kerätessä selonottovelvollisuutta noudattaessaan asiakkaasta mahdollisimman suppeasti tietoa, pankki voi vähäisen tiedon valossa päätyä ilmoittamaan todellisuudessa ymmärrettävän toiminnan epäilyttävänä liiketoimena viranomaisille. Tällöin pankilla on hallussaan vain vähän tietoa asiakkaasta, mutta tieto voi olla tämän jälkeen pankin lisäksi myös kolmannen osapuolen hallussa mahdollisesti täysin perusteetta. Tällöin ollaan taas tilanteessa, jossa on voitu sekä suojella että vaarantaa asiakkaan yksityisyys.

Selonottovelvollisuutta varten kerätyn tiedon määrän lisäksi onkin myös harkittava, kuinka paljon tietoa viranomaisille halutaan luovuttaa ilmoitusvelvollisuutta täyttäessä. Pankin on lakiin perustuen luovutettava ainoastaan tapauksen kannalta oleelliset tiedot,

[234] Preziosi 2017.
[235] Khan 2016.

viranomaisen voidessa jälkikäteen tarpeen mukaan pyytää lisätietoja tapauksen selvittämiseksi. Pankin on siis noudatettava rahanpesulainsäädännön vaatimuksia, huolehtien samalla kuitenkin asiakkaiden yksityisyyden suojaamisesta.

Tiedon määrän lisäksi pankin tulisi kiinnittää huomiota kerätyn tiedon laatuun. Tietoja ei tulisi yrittää löytää luotettavien lähteiden lisäksi kaikista mahdollisista ulkoisista lähteistä[236], vaan tietojen keräämisessä tulisi keskittyä ennen kaikkea tiedon laatuun ja ajantasaisuuteen. Huonolaatuisen tiedon käyttäminen ei ainoastaan vie tutkinnan fokusta pois oleellista asioista, vaan virheellisen tai epätäydellisen tiedon käsittelyllä voi olla myös vaikutuksia asiakkaan tosiasialliseen tilanteeseen. Esimerkiksi asiakkaan tili tai maksuväline voi joutua jäädytetyksi puutteellisen tai virheellisen tiedon pohjalta tehdyn väärän tulkinnan johdosta.[237]

Asiakkaan tuntemiseen liittyvien prosessien myötä pankkien kustannukset ovat nousseet, mikä on muiden tekijöiden ohella merkittävä haaste pankille.[238] Jo yksinomaan asiakkaan tuntemistietojen käsittely kuormittaa pankin toimintaa useassa eri portaassa. Tietosuoja-asetuksen määräämien vaatimusten noudattaminen tuo mukanaan merkittäviä hallinnollisia kustannuksia[239] jo entuudestaan raskaaseen prosessiin. Tietosuoja-asetuksen velvoitteet voidaan kuitenkin lukuisten haasteiden ohella nähdä myös positiivisessa valossa pankin toiminnan kannalta. Pankilla on erinomainen mahdollisuus käydä tietosuoja-asetuksen valossa tietojaan läpi ja punnita, ovatko kaikki olemassa olevat ja mahdollisesti tulevaisuudessa kerättävät tiedot tarpeellisia asiakkaan tuntemisen näkökulmasta.[240] Tarpeettomien tietojen karsiminen keventää tietojen- ja ajanhallintaprosessien lisäksi sekä kustannusrakennetta että pankin compliance-toimintoja[241].

6.4. Toiminnan kehittäminen tulevaisuudessa

Rahanpesulain ja tietosuojalainsäädännön velvoitteiden onnistunut yhteensovittaminen pankin asiakkaan tuntemisen toiminnoissa edellyttäisi ennen kaikkea lainsäädäntöympäristön systematisointia ja selkeyttämistä viranomaisten taholta. Viranomaisten tulisi pys-

[236] Hughes 2018: 9.
[237] Preziosi 2017.
[238] Parra Moyano & Ross 2017: 411.
[239] O'Connor 2017: 52-54.
[240] Preziosi 2017.
[241] *Compliance-toiminnoilla* tarkoitetaan yrityksen toimia, joilla pyritään lakien, sääntöjen ja määräysten noudattamiseen.

työ tarjoamaan pankeille nykyistä selvempiä linjavetoja tietojen oikeaoppisen ja -suhtaisen käsittelyn varmistamiseksi. Muiden tietojenkäsittelyn muotojen ohella etenkin kerätyn tiedon määrä ja laatu aiheuttaa pankille haasteita, joihin tulisi saada apua ja tukea viranomaisilta.

Oikeudentilan ollessa epäselvä, pankkien on kuitenkin pyrittävä oman osaamisensa puitteissa luovimaan rahanpesulain ja tietosuoja-asetuksen välillä parhaalla mahdollisella tavalla. Tässä onnistuakseen merkittävä tekijä on ajatusmaailman muuttaminen pankin sisällä. Pankin on luonnollisesti jatkossakin huolehdittava rahanpesulain asettamien velvoitteiden noudattamisesta asianmukaisin asiakkaan tuntemisen toimin. Tietosuoja-asetuksen myötä pankin on kuitenkin alettava aiempaa enemmän käyttää harkintaa sen suhteen, miten tietojen käsitellään, kuinka paljon ja millaista tietoa kerätään, ja mitä tietoja ilmoitetaan viranomaisille.

Ajatusmaailman muutoksen ohella pankin jatkuvasti kerryttämällä kokemuksella on suuri merkitys rahanpesulainsäädännön ja tietosuoja-asetuksen onnistuneessa yhteensovittamisessa. Kokemuksen kertyessä pankin mahdollisuudet riskiperusteiseen arviointiin paranevat, mikä näkyy myös tietojenkäsittelyssä. Osaamisen myötä pankilla on valmiudet hahmottaa aiempaa paremmin epäilyttävä toiminta normaalista, jolloin käsitellyn tiedon määrää pystytään myös minimoimaan. Jotta kokemusta ja osaamista pystytään hyödyntämään, tulee pankin huolehtia henkilöstön säännöllisestä ja riittävästä kouluttamisesta. Haasteettomaksi rahanpesulainsäädännön ja tietosuoja-asetuksen yhteensovittaminen tuskin tulee kuitenkaan muuttumaan, sillä tietojen käsittelyyn etenkin tietojen keräämisen osalta on mahdotonta löytää yksiselitteistä ratkaisua, jolla ei olisi varjopuolia joko yhteiskunnan turvallisuuden tai asiakkaan yksityisyyden vaarantumisen kannalta.

Pankin on siis muistettava huolehtia yhteiskunnallisten intressien toteutumisen lisäksi myös yksilön oikeuksista parhaan osaamisensa ja mahdollisuuksiensa mukaan. Pankkien pääasiallinen funktio on kuitenkin harjoittaa liiketoimintaa, mikä ei olisi mahdollista ilman asiakkaita. Tämän vuoksi pankin onkin tärkeä pitää myös huoli asiakkaiden tyytyväisyydestä huolehtimalla näiden yksityisyyden säilymisestä. Jotta pankki pystyy omalta osaltaan huolehtimaan yhteiskunnan turvallisuudesta, tulee sen ensiksi pystyä harjoittamaan kannattavaa liiketoimintaa.

7. JOHTOPÄÄTÖKSET

Tutkimuksessa on käyty läpi kronologisessa järjestyksessä asiakassuhteen eri vaiheet, ja pyritty selvittämään tutkimuskysymyksen mukaisesti, millaisia lakisääteisiä velvollisuuksia pankilla on koskien henkilöasiakkaidensa tietojen käsittelyä asiakkaan tuntemisen näkökulmasta, tarkoituksena estää rahanpesua ja terrorismin rahoittamista. Rahanpesulain asettamia velvoitteita on lisäksi peilattu tietosuoja-asetuksen mukaisiin vaatimuksiin, ja näin ollen toisen tutkimuskysymyksen mukaisesti pyritty selvittämään, miten rahanpesulaki ja tietosuoja-asetus suhteutuvat toisiinsa asiakkaan tuntemiseen kerättyjä henkilötietoja käsitellessä, ja millaisia haasteita näiden kahden lain yhteensovittaminen luo pankille.

Asiakkaan tuntemiseen liittyy lukuisia eri vaiheita, joilla jokaisella on oma tarkoituksensa rahanpesun ja terrorismin rahoittamisen estämisen näkökulmasta. Asiakassuhde alkaa aina asiakkaan tunnistamisella. Asiakkaan tunnistamista seuraa asiakkaan tuntemiseen liittyvien tietojen kerääminen ja dokumentointi. Asiakkaan tunnistaminen ja tunteminen on vaiheena tärkeä, sillä näiden tietojen perusteella suoritetaan asiakkaan profilointi, eli muodostetaan kokonaisvaltainen ja eheä käsitys asiakkaan toiminnasta ja siihen liittyvistä riskeistä.

Tuntemistietojen keräämisen ja analysoinnin jälkeen päätetään, tuleeko asiakkaan tuntemisessa noudattaa normaalia vai erityistä huolellisuutta, eli asetetaanko asiakas yksinkertaistetun vai tehostetun tuntemisen piiriin. Pankilla on oikeus, erinäiset lain asettamat vaatimukset huomioon ottaen, soveltaa päätöksessään omaa, riskiperusteista harkintaa. Päätös tuntemisen tasosta vaikuttaa asiakkaan jatkuvan seurannan toteuttamiseen. Korkeariskisiä asiakkaita tulee seurata normaalin riskin asiakkaita tiheämmin ja asiakkaan tuntemistietoja on päivitettävä tavanomaista useammin.

Asiakkaan tuntemiseen ja tunnistamiseen liittyvät vaiheet ja toimenpiteet voidaan nähdä osittain standarditoimina, sillä vaiheita sovelletaan jokaiseen asiakkaaseen tämän toiminnasta riippumatta. Toisin on selonotto- ja ilmoitusvelvollisuuden laita. Selonotto- ja ilmoitusvelvollisuus voidaan nähdä poikkeustilanteina, sillä niiden täyttyminen edellyttää aina poikkeuksellista tai epäilyttävää toimintaa asiakkaan puolelta. Selonotto- ja ilmoitusvelvollisuuteen kulminoituukin rahanpesulain perimmäinen tarkoitus: potentiaalisen rikollisen toiminnan huomaaminen ja siitä viranomaisille eteenpäin raportoiminen tarpeen vaatiessa. Selonotto- ja ilmoitusvelvollisuus ovat riippuvaisia aiemmin suoritetuista

asiakkaan tuntemisen toimenpiteistä, sillä ilman näitä edeltäviä vaiheita poikkeuksellisten tapahtumien havaitseminen ei olisi mahdollista.

Asiakkaan tunteminen on aiheena sekä ajankohtainen että dynaaminen. Asiakkaan tuntemista koskeva lainsäädäntö on jatkuvan muutoksen alla – uuden lain astuessa voimaan suunnitellaan jo seuraava lakia, joka parantaisi edellistä. Lainsäädännön lisäksi myös rahanpesu ja terrorismin rahoittaminen on rikoslajina alati muuttuva. Lainsäädännön tiheät muutokset voidaankin nähdä reaktiona ympäristössä tapahtuviin muutoksiin. Toimintatapojen lisäksi myös toimintaympäristö muuttuu ja laajenee. Rahanpesu ja terrorismin rahoittaminen ei ole enää kansallinen ongelma, sillä globalisoitumisen myötä siitä on tullut rajat ylittävä, kansainvälinen ilmiö ja yhteinen haaste.

Rahanpesulain määräysten lisäksi pankin velvoitteet ovat kasvaneet tietosuoja-asetuksen myötä. Asiakkaan tuntemiseen liittyvien prosessien sopeuttaminen vastaamaan tietosuoja-asetuksen mukaisia edellytyksiä on työläs ja aikaa vievä prosessi. Kyse ei ole ainoastaan tietojärjestelmien muokkaamisesta, vaan ennen kaikkea yrityskulttuurin ja ajatusmaailman muuttamisesta[242]. Pankki voi kuitenkin valita, suhtautuuko se tietosuoja-asetukseen ja sen määräyksiin kielteisesti vai myönteisesti. Kielteisessä näkemyksessä korostuvat tietosuoja-asetuksen byrokraattisuus, kustannukset ja muut negatiiviset tekijät. Myönteisen asenteen avulla voidaan sen sijaan nähdä tietosuoja-asetuksen positiiviset puolet ja mahdollisuudet pankille. Tietosuoja-asetuksen myötä pankki joutuu päivittämään, poistamaan ja järjestelemään hallussaan olevia tietoja, sekä miettimään entistä tarkemmin, mitä tietoja jatkossa tulisi käsitellä ja miten. Vaikka prosessi on hidas, sen myötä tietojenhallinta sekä paranee että kevenee, ja pankkien toiminnasta tulee aiempaa kustannustehokkaampaa. Tietojen läpikäynnin yhteydessä pankilla on lisäksi hyvä mahdollisuus olla yhteydessä asiakkaisiinsa, mahdollistaen entistä paremman ja tiiviimmän yhteistyön.[243]

Pankkien asema alati muuttuvan lainsäädännön ja toimintaympäristön keskellä on vähintäänkin haastava. Pankkien on täytettävä rahanpesulain mukainen lakisääteinen velvollisuutensa, sekä pidettävä huoli siitä, että toiminta on myös pankin liiketoiminnan kannalta kustannustehokasta ja tarkoituksenmukaista. Pankkien on lisäksi otettava huomioon tietosuoja-asetuksen asettamat vaatimukset henkilötietojen käsittelyn suhteen, ja huolehdittava siitä, että toiminta on samanaikaisesti sekä rahanpesulain että tietosuoja-asetuksen näkökulmasta laillista.

[242] Preziosi 2017.
[243] O'Connor 2017.

Pankkien rooli rahanpesun ja terrorismin rahoittamisen torjunnassa on kasvattanut viime vuosien aikana huomattavasti merkitystään viranomaisten asettamien vaatimusten kasvaessa. Koska vaatimukset ovat suhteellisen uusia, on pankkien aika kulunut tähän asti lähinnä totutellessa jatkuviin muutoksiin ja kasvaviin velvoitteisiin. Nyt kun aikaa on kulunut ja pankeille on karttunut kokemusta, on mielenkiintoista nähdä, millaiseksi pankin rooli tulee tulevaisuudessa muokkautumaan. Toiminta on muuttunut huomattavasti jo aiemmasta, sillä pankkien ilmoitusvelvollisuus perustuu nykyään raja-arvojen sijaan epäilyttävin tapahtumiin[244], minkä lisäksi pankeille on annettu uuden lainsäädännön myötä enemmän valtuuksia riskiperusteiseen arviointiin. Voidaan siis nähdä, että ollaan kulkemassa kohti tulevaisuutta, jossa pankkien omaan harkintakykyyn ja asiantuntijuuteen luotetaan yhä enemmän.

Vaikka rahanpesusta on tullut aiempaa hankalampaa rahoitusalan valvonnan kehittymisen myötä, ei rahanpesu kuitenkaan itsessään ole vähentynyt[245]. Herääkin kysymys, millainen rooli pankeilla tulisi tulevaisuudessa olla, jotta rahanpesua ja terrorismin rahoittamista pystyttäisiin aidosti torjumaan nykyistä enemmän. Rahoitusalla on viime aikoina lisätty valtavasti resursseja lainsäädännön asettamien vaatimusten täyttämiseksi ja etenkin jälkikäteinen seuranta on leimannut pankkien toimintaa. On otettava huomioon, ettei rahanpesu ja terrorismin rahoittaminen ole rikoslajina staattinen, sillä rikollisten toiminta muuttuu sitä mukaan, kun vanhat toimintatavat eivät enää tuota tulosta.

Pankkien olisi tulevaisuudessa hyvä olla enenevissä määrin perillä rahanpesun ja terrorismin rahoittamisen ajankohtaisista trendeistä, minkä lisäksi jälkikäteisen seurannan rinnalle tulisi saada ennakoivampi ja analyyttisempi ote. Näin varmistettaisiin, että pankki pystyisi toimimaan kustannustehokkaasti, allokoimaan resurssejaan ja hyödyntämään karttunutta asiantuntijuuttaan. Rahanpesulain säädösten noudattamisen ohella asiakkaan yksityisyyden suojaamisen tulisi olla prioriteetti pankille. Rahanpesulain ja tietosuoja-asetuksen samanaikainen noudattaminen on haastavaa tasapainoilua yhteiskunnan etujen ja yksilön oikeuksien välillä. Siinä kuitenkin onnistuessaan, pankki on osana luomassa aiempaa toimivampaa, turvallisempaa ja yksilöiden oikeuksia kunnioittavampaa yhteiskuntaa.

[244] Lowe 2017: 475.
[245] Lowe 2017: 475.

LÄHDELUETTELO

Euroopan unionin lainsäädäntö:

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

Suomen lainsäädäntö:

Laki luottolaitostoiminnasta 610/2014

Laki rahanpesun ja terrorismin rahoittamisen estämisestä 444/2017

Virallislähteet:

Eduskunta (2017). *Rahanpesulainsäädännön kokonaisuudistus* [online] [siteerattu 2018-01-15]. Saatavana World Wide Webistä: <URL: https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/rahanpesulainsaadannon-kokonaisuudistus.aspx>.

Finanssivalvonta (2017 a). *Asiakkaan tunnistaminen ja tunteminen* [online] [siteerattu 2018-02-15]. Saatavana World Wide Webistä: <URL: http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Finanssialan_palveluita/Pages/asiakkaan_tunnistaminen.aspx>.

Finanssivalvonta (2017 b). *Rahanpesun ja terrorismin rahoittamisen estäminen* [online] [siteerattu 2018-02-15]. Saatavana World Wide Webistä: <URL: http://www.finanssivalvonta.fi/fi/Valvonta/Rahanpesun_estaminen/Pages/Default.aspx>.

Finanssivalvonta (2017 c). *Tietoa Finanssivalvonnasta* [online] [siteerattu 2018-02-15]. Saatavana World Wide Webistä: <URL: http://www.finanssivalvonta.fi/fi/Fiva/Pages/Default.aspx>.

Finanssivalvonta (2016). *Usein kysytyt kysymykset* [online] [siteerattu 2018-02-15]. Saatavana World Wide Webistä: <URL: http://www.finanssivalvonta.fi/fi/Finanssiasiakas/Finanssialan_palveluita/Pages/Usein_kysytyt_kysymykset.aspx>.

Finanssivalvonnan standardi 2.4 (2015). *Asiakkaan tunteminen – rahanpesun ja terrorismin rahoittamisen estäminen* [online] [siteerattu 2018-01-13]. Saatavana World Wide Webistä: <URL: http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Uusi/Documents/2.4.std5.pdf>.

Hallituksen esitys eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi HE 9/2018

Poliisi (2018). *Rahanpesun torjunta* [online] [siteerattu 2018-01-13]. Saatavana World Wide Webistä: <URL: http://www.poliisi.fi/rahanpesu>.

Sisäministeriö (2018). *Rahanpesun ja terrorismin rahoituksen torjunta* [online] [siteerattu 2018-01-12]. Saatavana World Wide Webistä: <URL: http://intermin.fi/rahanpesun-ja-terrorismin-rahoituksen-torjunta>.

Tietosuojavaltuutetun toimisto (2018 a). *EU:n tietosuojauudistus* [online] [siteerattu 2018-05-20]. Saatavana World Wide Webistä: <URL: http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html>.

Tietosuojavaltuutetun toimisto (2018 b). *Henkilötietolaki* [online] [siteerattu 2018-06-10]. Saatavana World Wide Webistä: <URL: https://tietosuoja.fi/henkilotietolaki>.

Tietosuojavaltuutetun toimisto (2018 c). *Tietosuojavaltuutetun toimisto* [online] [siteerattu 2018-06-10]. Saatavana World Wide Webistä: <URL: https://tietosuoja.fi/tietosuojavaltuutetun-toimisto>.

Tietosuojavaltuutetun toimisto (2013). *Muiden lakien merkitys henkilötietojen käsittelyssä* [online] [siteerattu 2018-01-18]. Saatavana World Wide Webistä: <URL: http://www.tietosuoja.fi/fi/index/rekisterinpitajalle/muutlaitsuhteessahenkilotietolakiin.html>.

Valtiovarainministeriö (2018). *Rahanpesun estäminen rahoitusmarkkinoilla* [online] [siteerattu 2018-01-16]. Saatavana World Wide Webistä: <URL: http://vm.fi/rahanpesun-estaminen-rahoitusmarkkinoilla>.

Kirjallisuus:

Aarnio, Aulis (1989). *Laintulkinnan teoria.* 1. painos. Juva: Werner Söderström Oy. 315 s. ISBN 951-0-15493-8.

Alvarez, Daniel K. (2017). The EU General Data Protection Regulation Is Coming - Is Your Client Ready? *Practical Lawyer* 63:5 [online] [siteerattu 2018-07-10], 19-22. Saatavana World Wide Webistä: <URL: https://search-proquest-com.proxy.uwasa.fi/docview/1945666719?accountid=14797>.

Amicelle, Anthony (2011). Towards a ‘new’ political anatomy of financial surveillance. *Security Dialogue*, 42:2, 161-178. doi: 10.1177/0967010611401472

Axelrod, Robert M. (2017). Criminality and suspicious activity reports. *Journal of Financial Crime,* 24:3, 461-471. doi: 10.1108/JFC-03-2017-0019

Buchanan, Bonnie (2004). Money laundering - a global obstacle. *Research in International Business and Finance,* 18:1, 115-127. doi: 10.1016/j.ribaf.2004.02.001

Burt, Sue (2005). The dos and don'ts of suspicious activity reporting. *Texas Banking* 94:8 [online] [siteerattu 2018-09-12], 18-19. Saatavana World Wide Webistä: <URL: https://search-proquest-com.proxy.uwasa.fi/docview/209743889/?pq-origsite=primo>.

Böszörmenyi, Janos & Erich Schweighofer (2015). A review of tools to comply with the Fourth EU anti-money laundering directive. *International Review of Law, Computers & Technology*, 29:1, 63-77. doi: 10.1080/13600869.2015.1016276

Camp, Jean L (2015). Respecting people and respecting privacy. *Communications of the ACM* 58:7 [online] [siteerattu 2018-08-09], 27-28. Saatavana World Wide Webistä: <URL: http://delivery.acm.org.proxy.uwasa.fi/10.1145/2780000/2770892/p27-camp.pdf?ip=193.166.96.80&id=2770892&acc=ACTIVE%20SERVICE&key=74A0E95D84AAE420%2E47B562B2B23DBB74%2E4D4702B0C3E38B35%2E4D4702B0C3E38B35&__acm__=1533821718_f9c2ff2ee66714aa68c184993a6ffb3b>.

de Koker, Louis (2006). Money laundering control and suppression of financing of terrorism: Some thoughts on the impact of customer due diligence measures on financial exclusion. *Journal of Financial Crime*, 13:1, 26-50. doi: 10.1108/13590790610641206

Demetriades, George (2016). Is the person who he claims to be? Old fashion due diligence may give the correct answer! *Journal of Money Laundering Control*, 19:1, 79-91. doi: 10.1108/JMLC-11-2014-0041

de Wit, Jos (2007). A risk-based approach to AML: A controversy between financial institutions and regulators. *Journal of Financial Regulation and Compliance*, 15:2, 156-165. doi: 10.1108/13581980710744048

Dickie, Nancy & Andrew Yule, (2017). Privacy by design prevents data headaches later. *Strategic HR Review*, 16:2, 100-101. doi: 10.1108/SHR-01-2017-0008

Doughty, Caroline (2005). Know your customer: Automation is key to comply with legislation. *Business Information Review*, 22:4, 248–252. doi: 10.1177/0266382105060603

Favarel-Garrigues, Gilles, Thierry Godefroy & Pierre Lascoumes (2011). Reluctant partners? Banks in the fight against money laundering and terrorism financing in France. *Security Dialogue*, 42:2, 179-196. doi: 10.1177/0967010611399615

Garcia-Rivadulla, Sandra (2016). Personalization vs. privacy: An inevitable trade-off? *IFLA Journal*, 42:3, 227-238. doi: 10.1177/0340035216662890

Gonçalves, Maria E. (2017). The EU data protection reform and the challenges of big data: remaining uncertainties and ways forward. *Information & Communications Technology Law*, 26:2, 90-115. doi: 10.1080/13600834.2017.1295838

Graeff, Timothy R. & Susan Harmon (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, 19:4, 302-318. doi: 10.1108/07363760210433627

Kindt, E.J (2018). Having yes, using no? About the new legal regime for biometric data. *Comupter Law & Security Review: The International Journal of Technology Law and Practice*, 34:3, 523-538. doi: 10.1016/j.clsr.2017.11.004

Kingston, John (2017). Using artificial intelligence to support compliance with the general data protection regulation. *Artificial Intelligence and Law*, 25:4, 429-443. doi: 10.1007/s10506-017-9206-9

Koops, Bert-Jaap, Jaap-Henk Hoepman & Ronald Leenes (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, 29:6, 676-688. doi: 10.1016/j.clsr.2013.09.005

Lahti, Raimo & Pekka Koponen (2007). *Talousrikokset.* 2. painos. Vaajakoski: Gummerus Kirjapaino Oy. 305 s. ISBN 978-951-855-276-8.

Laybats, Claire & Luke Tredinnick (2016). Information security. *Business Information Review*, 33:2, 76.80. doi: 10.1177/0266382116653061

Lindroos-Hovinheimo, Susanna (2018). Henkilötietojen suoja EU-oikeudessa - yksityisyyttä yhteisön kustannuksella? *Lakimies* 1/2018 [online] [siteerattu 2018-06-20], 52-75. Saatavana World Wide Webistä: <URL: https://www-edilex-fi.proxy.uwasa.fi/lakimies/18564.pdf>.

Lowe, Richard J. (2017). Anti-money laundering – the need for intelligence. *Journal of Financial Crime*, 24:3, 472-479. doi: 10.1108/JFC-04-2017-0030

Mantelero, Alessandro (2017). Regulating big data. The guidelines of the Council of Europe in the context of the European data protection framework. *Computer Law & Security Review*, 33:5, 584-602. doi: 10.1016/j.clsr.2017.05.011

Mat Isa, Yusarina, Zuraidah Mohd Sanusib, Mohd Nizal Haniffa & Paul A. Barnesc (2015). Money Laundering Risk: From the Bankers' and Regulators Perspectives. *Procedia Economics and Finance* 28 [online] [siteerattu 2018-04-02], 7-13. Saatavana World Wide Webistä: <URL: https://ac-els-cdn-com.proxy.uwasa.fi/S2212567115010758/1-s2.0-S2212567115010758-main.pdf?_tid=5dec61cb-4cac-470e-94a4-0837f2f306a0&acdnat=1522765665_7795a5b30551c2695a1babcfabc58151 >.

McCallister, Jennifer, Gabriela Zanfir-Fortuna & Jennifer Mitchell (2018). Getting ready for the EU's stringent data privacy rule. *Journal of Accountancy* 225:1 [online] [siteerattu 2018-08-09], 36-40. Saatavana World Wide Webistä: <URL: https://search-proquest-com.proxy.uwasa.fi/docview/1987380644?accountid=14797>.

O'Connor, Billy (2017). The final countdown to GDPR. *Accountancy Ireland* 49:4 [online] [siteerattu 2018-08-13], 52-54. Saatavana World Wide Webistä: <URL: https://search-proquest-com.proxy.uwasa.fi/business/docview/1973329972?pq-origsite=primo>.

Parra Moyano, José & Omri Ross (2017). KYC Optimization Using Distributed Ledger Technology. *Business & Information Systems Engineering*, 59:6, 411-423. doi: 10.1007/s12599-017-0504-2

Pitkänen Olli, Päivi Tiilikka & Eija Warma (2013). *Henkilötietojen suoja*. 1. painos. Alma Talent. 332 s. ISBN: 9789521420580.

Pitkänen, Olli (2014). Sinun tietosi eivät ole sinun: rekisteröidyn oikeus hyödyntää omia henkilötietojaan. *Oikeus* 2/2014 [online] [siteerattu 2018-05-20], 202-214. Saatavana World Wide Webistä: <URL: https://www-edilex-fi.proxy.uwasa.fi/oikeus/13599.pdf>.

Poullet, Yves (2018). Is the general data protection regulation the solution? *Computer Law & Security Review*, 34:4, 773-778. doi: 10.1016/j.clsr.2018.05.021

Ramage, Sally (2012). Information techonology facilitating money laundering. *Information & Communications Technology Law*, 21:3, 269-282. doi: 10.1080/13600834.2012.744226

Romanou, Anna (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review*. 34:1, 99-110. doi: 10.1016/j.clsr.2017.05.021

Schermer, Bart W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law and Security Review: The International Journal of Technology and Practice*, 27:1, 45-52. doi: 10.1016/j.clsr.2010.11.009

Seymour, Brian (2008). Global Money Laundering. *Journal of Applied Security Research,* 3:3-4, 373-387. doi: 10.1080/19361610801981001

Sica, Vincent (2000). Cleaning the Laundry: States and the Monitoring of the Financial System. *Millenium: Journal of International Studies*, 29:1, 47-72. doi:10.1177/03058298000290010801

Stessens, Guy (2000). *Money Laundering: A New International Law Enforcement Model.* 1st ed. Cambridge: Cambridge University Press. 460 p. ISBN 0-521-78104-3.

Štitilis, Darius & Marius Laurinaitis (2017). Treatment of biometrically processed personal data: Probelm of uniform practice under EU personal data protection law. *Computer Law & Security Review*, 33:5, 618-628. doi: 10.1016/j.clsr.2017.03.012

Tikkinen-Piri, Christina, Anna Rohunen & Jouni Markkula (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, 34:1, 134-153. doi: 10.1016/j.clsr.2017.05.015

van Dijk, N., A. Tanas, K.Rommetveit & C. Raab (2018). Right engineering? The redesign of privacy and personal data protection. *International Review of Law,*

Computers & Technology, 32:2-3, 230-256. doi: 10.1080/13600869.2018.1457002

Vanto, Jarno (2011). *Henkilötietolaki käytännössä*. 1 painos. Sanoma Pro Oy. 210 s. ISBN 978-951-0-36933-3.

Virolainen, Jyrki (2012). Oikeuskirjallisuus oikeuslähteenä ja tuomion perusteluissa. *Lakimies* 1/2012 [online] [siteerattu 2018-01-13], 3-32. Saatavana World Wide Webistä: <URL: https://www-edilex-fi.proxy.uwasa.fi/lakimies/8624.pdf>.

Muut:

Aarnio, Reijo (2018). Mitä GDPR:n jälkeen? *Tietosuojavaltuutetun toimisto* [online] [siteerattu 2018-06-11]. Saatavana World Wide Webistä: <URL: https://tietosuoja.fi/artikkeli/-/asset_publisher/mita-gdpr-n-jalkeen>.

Dockeray, Jane & Nick Westbrook (2018). ARE YOU READY FOR GDPR? *The Estates Gazette* [online] [siteerattu 2018-08-13], 56-58. Saatavana World Wide Webistä: <URL: https://search-proquest-com.proxy.uwasa.fi/business/docview/2056022495?pq-origsite=primo>.

Finanssiala ry (2016). *Fiva: Asiakassuhdetta ei voi ylläpitää, jos tuntemistiedoissa puutteita*. [online] [siteerattu 2018-01-03]. Saatavana World Wide Webistä: <URL: http://www.finanssiala.fi/uutismajakka/Sivut/Fiva-Asiakassuhdetta-ei-voi-yllapitaa-jos-tuntemistiedoissa-puutteita.aspx>.

Hughes, Jessica R. (2018). The Importance of Incorporating Data Privacy into Anti-Money Laundering and Anti-Corruption Compliance Programs. *ACAMS* [online] [siteerattu 2018-09-16]. Saatavana World Wide Webistä: <URL: https://www.acams.org/aml-white-paper-data-privacy-anti-corruption-regulations/>.

Jackson, Olly (2018). GDPR: on the right path? *International Financial Law Review* [online] [siteerattu 2018-07-11]. Saatavana World Wide Webistä: <URL:

https://search-proquest-com.proxy.uwasa.fi/docview/2045017398/abstract/6AA93C950DAE4C1APQ/1?accountid=14797>.

Juntunen, Ritva (2016). Uusi tietosuoja-asetus luo oikeuksia ja velvollisuuksia. *Lakimiesuutiset* [online] [siteerattu 2018-06-11]. Saatavana World Wide Webistä: <URL: https://lakimiesuutiset.fi/uusi-tietosuoja-asetus-luo-oikeuksia-ja-velvollisuuksia/>. Perustuu Eija Warman haastatteluun.

Khan, Sana (2016). The Fourth AML Directive and the EU's Approach to Data Protection: A Precautionary Warning. *ACAMS Today* [online] [siteerattu 2018-09-16]. Saatavana World Wide Webistä: <URL: https://www.acamstoday.org/fourth-aml-directive-eus-approach-to-data-protection/>.

Lucchetti, Umberto (2018). AML Rule Tuning: Applying Statistical and Risk-Based Approach to Achieve Higher Alert Efficiency. *ACAMS* [online] [siteerattu 2018-02-14]. Saatavana Word Wide Webistä: <URL: http://www.acams.org/wp-content/uploads/2015/08/AML-Rule-Tuning-Applying-Statistical-Risk-Based-Approach-to-Achieve-Higher-Alert-Efficiency-U-Luccehtti.pdf>.

O'Connor, Denis (2018). EU Sixth Anti-money Laundering Directive (6AMLD) – Expert Analysis of New EU Measures. *KYC360* [online] [siteerattu 2018-09-15]. Saatavana World Wide Webistä: <URL: https://kyc360.com/article/6amld-eu-sixth-anti-money-laundering-directive/>.

Preziosi, Camilleri (2017). Finding the balance betwen data protection and AML requirements. *Lexology* [online] [siteerattu 2018-09-16]. Saatavana World Wide Webistä: <URL: https://www.lexology.com/library/detail.aspx?g=8aabfbf8-33c1-456d-869b-ef1f56ec0e08>.

Reese, Bernadine (2018). GDPR and EU AML Directives - A Regulatory Tug-of-War. *Protiviti* [online] [siteerattu 2018-09-16]. Saatavana World Wide Webistä: <URL: https://blog.protiviti.com/2018/05/24/gdpr-eu-aml-directives-regulatory-tug-war/>.

Savolainen, Jukka (2016). Tietosuojavaltuutettu selvittää kyselevätkö pankit jo liikaa asiakkailta rahanpesulain varjolla. *Edilex* [online] [siteerattu 2018-01-15]. Saatavana World Wide Webistä: <URL: https://www-edilex-fi.proxy.uwasa.fi/uutiset/47415?allWords=asiakkaan+tunteminen&offset=1&perpage=20&sort=relevance&typeIds[]=127%3Afi&searchSrc=1&advancedSearchKey=653520>.

Siikala, Kristiina (2015). Miksi pankki kysyy? - Oletko poliittisesti vaikutusvaltainen? *Finanssiala ry* [online] [siteerattu 2018-01-01]. Saatavana World Wide Webistä: <URL: http://www.finanssiala.fi/uutismajakka/Sivut/Miksi_pankki_kysyy_Oletko_poliittisesti_vaikutusvaltainen.aspx>.

Talus, Anu, Elina Autio, Anna Hänninen, Heljä-Tuulia Pihamaa, Heljä-Tuulia & Silja Kantonen (2017). Miten valmistautua EU:n tietosuoja-asetukseen? *Oikeusministeriön julkaisu* 4/2017. [online] [siteerattu 2018-07-01]. Saatavana World Wide Webistä: <URL: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79316/OMSO_04_2017_OM_TSV_EU_tietosuoja.pdf?sequence=1>.

Young, Tom (2017). PRIMER: General data protection regulation. *International Financial Law Review* [online] [siteerattu 2018-08-21]. Saatavana World Wide Webistä: <URL: https://search-proquest-com.proxy.uwasa.fi/business/docview/1944972348?pq-origsite=primo>.