jamk.fi

Pilvipalveluiden käyttöönotto asian-ajotoimistoissa

Suvi-Maaria Westerlund

Opinnäytetyö
Joulukuu 2016
Yhteiskuntatieteiden, liiketalouden ja hallinnon ala
Tradenomi (AMK), liiketalouden tutkinto-ohjelma

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Westerlund, Suvi-Maaria	Opinnäytetyö, AMK	Joulukuu 2016
	Sivumäärä 53	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Pilvipalveluiden käyttöönotto asianajotoimistoissa

Tutkinto-ohjelma
Liiketalouden tutkinto-ohjelma

Työn ohjaaja(t)
Riikka Ahlgren

Toimeksiantaja(t)
Suomen Asianajajaliiton Keski-Suomen osasto

Tiivistelmä

Tutkimuksen aiheena oli pilvipalveluiden käyttöönottoon liittyvät oikeudelliset kysymykset. Tavoitteena oli selvittää, miten voidaan varmistaa tietosuojan ja tietoturvan säilyminen asianajotoimistojen siirtyessä käyttämään pilvipalvelupohjaisia ratkaisuja. Tämän lisäksi tavoitteena oli tutkia Suomen Asianajajaliiton säädösten huomioimista pilvipalveluiden käyttöönotossa.

Tutkimus toteutettiin kvalitatiivisena eli laadullisena tutkimuksena, ja tiedonkeruumenetelmänä käytettiin teemahaastatteluita. Haastattelut toteutettiin lokakuussa 2016, ja haastateltavina oli Jyväskylän alueella toimivia eri kokoisia asianajotoimistoja. Haastatteluita tehtiin yhteensä viisi kappaletta, joissa käsiteltiin kolmea eri teemaa: pilvipalveluita, tietosuojaa ja tietoturvaa sekä asianajajaliiton säädöksiä.

Tutkimustulosten perusteella asianajotoimistot pitävät palveluntarjoajan luotettavuutta tärkeimpänä tekijänä tietosuojan ja tietoturvan säilymiselle pilvipalveluissa. Palveluntarjoajan luotettavuutta lisää yrityksen kotimaisuus, muiden toimistojen kokemukset kyseisestä yrityksestä ja palveluntarjoajan kanssa tehtävä salassapitosopimus. Lisäksi palvelimen sijaitsemista Suomessa pidettiin tärkeänä, jotta voidaan välttyä lainsäädännöllisiltä ongelmilta.

Asianajajaliiton säädösten osalta saatiin selville, että ne vaikuttavat omalta osaltaan pilvipalveluiden käyttöönottoon. Säädökset ovat melko ympäripyöreät, mutta jos jotain tarkkaa on määrätty, sen mukaan toimitaan. Avoimet kohdat jäävät toimistojen oman harkinnan mukaan ratkaistaviksi. Tuloksista voidaan päätellä, että tekijät, jotka toimistot kokivat tärkeiksi tietosuojan ja tietoturvan kannalta, kohtasivat hyvin asianajajaliiton säädösten kanssa.

Avainsanat (asiasanat)
Pilvipalvelut, tietosuoja, tietoturva, asianajotoimisto, Suomen Asianajajaliitto

Muut tiedot

jamk.fi

Description

Author(s)	Type of publication	Date
Westerlund, Suvi-Maaria	Bachelor's thesis	December 2016
		Language of publication: Finnish
	Number of pages 53	Permission for web publication: x

Title of publication
Introduction of cloud computing in law firms

Degree programme
Business Administration

Supervisor(s)
Ahlgren, Riikka

Assigned by
Finnish Bar Association Chapter of Central Finland

Abstract

The subject of the study was the judicial questions in introduction of cloud computing. The aim was to establish how the remaining of data privacy and data protection could be ensured when law firms start to use cloud computing solutions. In addition, the aim was to study how Finnish Bar Association´s guidelines will be taken into consideration when starting to use cloud computing solutions.

The approach of the study was qualitative and the collection of data was conducted by theme interviews. The interviews were implemented in October 2016 and the interviewees were law firms of different sizes in Jyväskylä. Five interviews were made consisting of three themes: cloud computing, data privacy and data protection as well as the Finnish Bar Association´s guidelines.

Based on the results of the study the law firms find service provider´s reliability the most important factor when thinking of the remaining of data privacy and data protection in cloud computing. Things that increase service provider´s reliability are that the firm is domestic, other offices have knowledge of the firm and that a confidentiality agreement is made with the service provider. Also it was important to the offices that the server is located in Finland so that there would not be any legislative issues.

The Bar Association´s guidelines have also an impact on introduction of cloud computing. The guidelines are mainly quite general but the offices have to act according to any specific issues in the guidelines. The open questions are left into offices´ own consideration. It can be concluded from the results that the factors that the offices held important in the remaining of data privacy and data protection were similar to the Bar Association´s guidelines.

Keywords/tags (subjects)
Cloud computing, data privacy, data protection, law firm, Finnish Bar Association

Miscellaneous

Sisältö

1 Johdanto 2
2 Tutkimusasetelma 3
2.1 Tutkimusongelma ja tavoitteet 3
2.2 Tutkimusmenetelmät 5
3 Asianajotoimisto ja pilvipalvelut 9
3.1 Asianajoala 10
3.2 Aineistopankkihanke AIPA 12
3.3 Pilvipalvelut 14
4 Oikeudelliset kysymykset pilvipalveluissa 17
4.1 Lainsäädäntö 18
4.2 Tietosuoja 22
4.3 Tietoturva 26
5 Tutkimuksen toteutus ja tutkimustulokset 30
5.1 Tutkimuksen toteutus 30
5.2 Tietosuojan ja tietoturvan säilyminen 33
5.3 Asianajajaliiton säädösten huomioiminen 36
6 Johtopäätökset 38
7 Pohdinta 44
Lähteet 48
Liitteet 52

Kuviot

Kuvio 1. Rikosasian papereiden eteneminen 13
Kuvio 2. Tietoturvallisuuden osatekijät 27
Kuvio 3. Litteroinnin teemat 32
Kuvio 4. Pääteemat tutkimuskysymyksiä mukaillen 33

1 Johdanto

Digitalisaatio eli prosessi kohti digitaalista liiketoimintaa (Digitalization n.d.) tulee muuttamaan yritysten liiketoimintaprosesseja entistä enemmän, esimerkiksi erilaisin tietoteknisin ratkaisuin. Viime vuosien aikana pilvipalveluista on kehittynyt yksi nopeimmin kasvavista tietotekniikan osa-alueista. Kasvua on kuitenkin hidastanut huoli pilvipalveluympäristön turvallisuudesta. (Subashini & Kavitha 2011.) Yrityksissä liikkuu paljon salassa pidettävää ja luottamuksellista tietoa, minkä takia tietosuojan ja tietoturvan säilyminen on olennaista.

Pilvipalveluille on ominaista, että käyttäjä ei välttämättä tiedä pilvipalvelimen konkreettista sijaintia. Tämän takia ajatus dokumenttien tallentamisesta pilveen saattaa herättää käyttäjässä epävarmuutta. Myöskin se, että asiakirjat eivät ole enää omassa hallinnassa, voi esiintyä jarruttavana tekijänä pilvipalveluiden käyttöönotolle. Asianajotoimistoissa syntyy toimeksiantojen yhteydessä paljon asiakirjoja, jotka sisältävät arkaluontoista ja salassa pidettävää tietoa. Asiakirjoja käsiteltäessä tulee ottaa huomioon niiden sisältämän tiedon luonne, ja niitä tulee säilyttää rikkomatta asianajajan salassapitovelvollisuutta.

Asianajotoimistoissa liikkuvan tiedon luonteen ja asianajajan salassapitovelvollisuuden vuoksi pilvipalveluita ei ole vielä hyödynnetty paljoa suomalaisissa asianajotoimistoissa. Sen sijaan pilvipalveluita on käytetty maailmalla asianajotoimistoissa jo pidemmän aikaa. Esimerkiksi Yhdysvalloissa on useita pilvipalveluntarjoajia, joiden palvelut on suunniteltu nimenomaan asianajotoimistoille. Palvelut voivat erota hyvinkin paljon turvallisuuden ja palveluominaisuuksien osalta verrattuna ”tavallisiin” pilvipalveluihin. (Kimbro & Mighell 2011.) Uudessa-Seelannissa puolestaan paikallinen lakiyhdistys (New Zealand Law Society) on tehnyt jäsenilleen ohjeistuksen pilvipalveluista ja niiden käytöstä. Se sisältää yleistä tietoa pilvipalveluista ja huomioitavista asioista pilvipalvelun käyttöönotossa. (Practice briefing: cloud computing guidelines for lawyers 2014.)

Suomessa asianajotoimistojen toimintaa valvoo Suomen Asianajajaliitto, jonka tekemät säädökset ja ohjeet sisältävät asianajotoimistojen tietoturvaoppaan. Tietoturvaopas sisältää yleiset ohjeet it-palveluiden ulkoistamisesta ja pilvipalveluiden käytöstä. Ohjeet ovat kuitenkin tehty yleisellä tasolla, sillä pilvipalveluiden käyttö asianajotoimistoissa on vielä melko uusi asia.

2 Tutkimusasetelma

Luvussa 2.1 kuvataan tutkimuksen taustat, tutkimusongelma ja tavoitteet sekä esitellään aikaisempia tutkimuksia. Tutkimusmenetelmät-osiossa käsitellään tutkimusotetta, tiedonkeruu- ja analysointimenetelmiä sekä luotettavuuden varmistusta. Käytettävät menetelmät perustellaan tutkimusongelman kannalta. Lisäksi luvun lopussa on lyhyt kuvaus opinnäytetyön toimeksiantajasta.

2.1 Tutkimusongelma ja tavoitteet

Tutkimusongelma

Opinnäytetyön aiheena on asianajotoimistojen tietosuojan ja tietoturvan säilyminen sekä asianajajaliiton säädösten huomioiminen siirryttäessä pilvipalveluiden käyttöön. Tutkimuksen tarve nousi esille työelämästä. Opinnäytetyön tekijä oli vuonna 2016 pidemmän harjoittelujakson töissä asianajotoimistossa, jonka jälkeen vielä kesätöissä kyseisessä toimistossa. Aihetta pilvipalveluiden käyttöönotosta asianajotoimistossa mietittiin jo harjoittelun alussa ja opinnäytetyön kirjoittamisen alkaessa sitä muokattiin opinnäytetyöaiheeksi sopivaksi.

Tutkimusaihe on ajankohtainen, sillä oikeusministeriö on käynnistänyt vuonna 2010 aineistopankkihankkeen (AIPA), joka on syyttäjälaitoksen ja yleisten tuomioistuinten asian- ja dokumentinhallinnan kehittämishanke. Sen myötä oikeuslaitos on siirtymässä sähköiseen työskentelyyn (Mikkonen 2015), mikä omalta osaltaan painostaa myös asianajotoimistoja miettimään sähköistä asiankäsittelyä. Aihe on opinnäytetyön tekijälle mielenkiintoinen, koska hän on työskennellyt asianajotoimistossa, ja osaa käytännössä miettiä aihetta itse työn kannalta. Esimerkiksi miettiä sitä, miten työnteko muuttuu sähköisten järjestelmien lisääntyessä, ja kuinka tärkeitä tietosuoja- ja tietoturva-asiat ovat käsiteltäessä henkilötietoja ja muita arkaluontoisia tietoja sisältäviä asiakirjoja.

Tutkimuksen tutkimusongelmana on Miten tietosuoja ja tietoturva sekä asianajajaliiton säädökset huomioidaan asianajotoimistojen siirtyessä pilvipalveluiden käyttöön? Tutkimusongelmasta johdetaan tutkimuskysymys tai -

kysymyksiä ja niiden vastauksista saadaan vastaus itse tutkimusongelmaan (Kananen 2008, 51). Tutkimuskysymyksiksi on määritelty:

- Miten voidaan varmistaa tietosuojan ja tietoturvan säilyminen asianajotoimistoissa olevien tietojen siirtyessä pilveen?
- Millä tavalla asianajajaliiton säädökset vaikuttavat pilvipalveluiden käyttöönottoon?

Tavoitteet

Pilvipalveluiden käyttöönottoon liittyy monia huomioitavia seikkoja, joista yksi on pilvipalveluiden hyödyntämisen oikeudelliset esteet. Ne voivat liittyä tietosuojaan, tietoturvaan, tekijänoikeuksiin ja standardointiin. (Kalli, Argillander, Talvitie & Luoma 2013, 32.) Opinnäytetyö on rajattu tietosuojaan ja tietoturvaan liittyviin kysymyksiin, sillä niiden säilyminen yrityksissä on erittäin tärkeää. Lisäksi ne ovat asioita, jotka yleisimmin nousevat esiin epävarmuustekijöinä pilvipalveluiden käyttöönotossa. Asianajotoimistoissa käsitellään paljon luottamuksellisia ja salassa pidettäviä asiakirjoja, jotka sisältävät henkilötietoja. Tämän takia on luontevaa keskittyä tietosuojan ja tietoturvan säilymiseen.

Yleisen tietosuojaa ja tietoturvaa koskevan lainsäädännön lisäksi on huomioitava toimialakohtaiset säädökset. Asianajajaliitto on julkaissut tietoturvaoppaan, jossa on säädöksiä ja ohjeita pilvipalveluiden käytöstä asianajotoimistoissa. Käytössä on otettava huomioon erityisesti salassapidon asettamat vaatimukset, joita asianajajalta edellytetään. (Tietoturvaopas 2012, 11.) Opinnäytetyössä tutkitaan myös sitä, miten asianajotoimistot käytännössä huomioivat nämä asianajajaliiton ohjeet. Tutkimuksessa ei siis pyritä selvittämään pilvipalveluihin ja niiden käyttöönottoon liittyviä teknisiä kysymyksiä, vaan se on nimenomaan rajattu käsittelemään käyttöönottoon liittyviä oikeudellisia kysymyksiä sekä asianajajaliiton säädösten ja ohjeiden huomioonottamista.

Työn nimellisenä toimeksiantajana on asianajajaliiton Keski-Suomen osasto. Tutkimuksen myötä syntyy käytännön kuvaus tietosuojan, tietoturvan ja asianajajaliiton säädösten huomioimisesta pilvipalveluiden käyttöönotossa. Näiden pohjalta tehdään toimeksiantajalle kehittämisehdotus liittyen pilvipalveluiden käyttöönoton ohjeisiin. Tutkimuksen pohjalta asianajajaliitto saa tietoa,

miten asianajotoimistot kokevat ja huomioivat heidän antamansa ohjeet pilvipalveluiden käytöstä. Lisäksi se saa yleistä tietoa pilvipalveluiden käytöstä asianajotoimistoissa. Asianajotoimistot saavat myös tietoa tietosuojan ja tietoturvan säilymisestä pilvipalveluiden käytössä sekä pilvipalveluiden tarjoajat saavat tietoa, miten heidän tarjoamansa palvelut soveltuvat asianajotoimistojen käyttöön. Tieto on ajankohtaista, sillä yhä useammat asianajotoimistot ovat siirtymässä pilvipalveluiden käyttöön lähivuosien aikana.

Aikaisemmat tutkimukset

Opinnäytetyön aiheesta ei ole suoranaisesti aikaisempia tutkimuksia. Pilvipalveluympäristöjen turvallisuutta ovat tutkineet esimerkiksi Subashini ja Kavitha (2011) sekä Fernandes, Soares, Gomez, Freire ja Inácio (2014). Nämä tutkimukset keskittyvät kuitenkin pilvipalveluiden turvallisuuden tekniseen puoleen. Tilastokeskus on tehnyt vuosittain tutkimuksia tietotekniikan käytöstä yrityksissä, mihin on kahtena viime vuotena otettu mukaan pilvipalveluiden käyttö yrityksissä.

Pilvipalveluiden käyttöönotosta on tehty myös opinnäytetöitä. Lähimpänä opinnäytetyön aihetta on Tomi Viitalan 2016 keväällä kirjoittama opinnäytetyö, joka käsittelee organisaation (LAMK) tietojen tietosuojan säilymisestä siirryttäessä pilvipalveluihin. Anne Hankosalo on vuonna 2012 tehnyt opinnäytetyön, jossa käsitellään tietosuojan oikeudellisia ja teknisiä kysymyksiä yritysten ottaessa käyttöön pilvipalvelupohjaisia ratkaisuja. Terveydenhuoltoalalle on puolestaan tehty useampia opinnäytetöitä tietosuojan ja tietoturvan säilymisestä käsiteltäessä potilastietoja, mutta niissä ei ole tutkittu pilvipalveluiden käyttöä. Tutkimusta, joka olisi kohdistunut juuri asianajoalalle, ei löytynyt.

2.2 Tutkimusmenetelmät

Tutkimusote

Yksinkertainen tutkimusotteiden jaottelu jakaa ne kvantitatiiviseen ja kvalitatiiviseen tutkimusotteeseen (Kananen 2010, 36–37). Opinnäytetyö toteutetaan kvalitatiivisena eli laadullisena tutkimuksena. Opinnäytetyössä on perusteltua käyttää laadullista tutkimusta, sillä aiheesta ei ole aikaisempaa tutkimusta ja

tutkimuskohde halutaan kuvata mahdollisimman hyvin. Opinnäytetyössä ei pyritä testaamaan mitään hypoteesia tai teoriaa vaan tutkimusongelmasta halutaan kokonaisvaltainen ymmärrys.

Kanasen (2008, 24–25) mukaan laadullinen tutkimus on tutkimuskohteen kuvaamista ja ymmärtämistä, eikä sillä pyritä yleistyksiin vaan ilmiön syvällisempään selittämiseen. Kohdetta pyritään tutkimaan mahdollisimman kokonaisvaltaisesti. Lähtökohtana on aineiston yksityiskohtainen tarkastelu, eikä teorian tai hypoteesien testaaminen. (Hirsjärvi, Remes & Sajavaara 2009, 164.) Metsämuuronen (2008, 14) puolestaan määrittelee yhdeksi laadullisen tutkimuksen käyttötilanteeksi sen, kun ollaan enemmän kiinnostuneita jonkun tapahtuman yksityiskohtaisesta rakenteesta, kuin niiden yleisluotoisesta jakaantumisesta.

Laadullinen tutkimus ei etene samanlaisen kaavan mukaan kuin määrällinen tutkimus, vaan se on joustavampi tutkimusote (Kananen 2008, 27). Tutkimussuunnitelmaa voidaan joutua muokkaamaan olosuhteiden mukaisesti (Hirsjärvi ym. 2009, 164). Kaavamaisuuden puuttuessa tutkimuksessa voidaan toimia ja edetä tilanteen mukaan, mutta toisaalta joustavuus voi johtaa umpikujaan, jos mahdollisuuksia on liikaa (Kananen 2008, 27).

Tiedonkeruumenetelmät

Kuten tutkimusotteen valinnassakin, on myös tiedonkeruumenetelmän valinnassa tärkeä kiinnittää huomiota tutkittavaan ilmiöön. Laadullisessa tutkimuksessa aineisto kootaan luonnollisissa tilanteissa. Tärkeimmät laadullisen tutkimuksen tiedonkeruumenetelmät havainnointi, haastattelu sekä erilaiset dokumentit. (Hirsjärvi ym. 2009, 164; Kananen 2010, 48.) Tässä tutkimuksessa käytetään tiedonkeruumenetelmänä teemahaastattelua, sillä teemojen rajaus pitää saadun aineiston maltillisena ja helpommin analysoitavana. Teemahaastattelu antaa myös sijaa odottamattomille asioille, jotka saattavat nousta esille haastateltavien puheesta.

Metsämuuronen (2008, 39) kuvaa haastattelun sopivan moneen tilanteeseen, ja sitä tulisi käyttää laadullisessa tutkimuksessa aina kun se on järkevä tapa hankkia tietoa. Erityisen hyvin se sopii tiedonkeruumenetelmäksi, kun halutaan kuvaavia esimerkkejä aiheesta (mts.). Teemahaastattelu on yksi haastat-

telumuodoista ja se kohdennetaan tiettyihin teemoihin, joista haastattelussa keskustellaan. Haastattelu ei etene yksityiskohtaisten kysymysten mukaan, jolloin haastateltavien tulkinnat asioista ja heidän asioille antamansa merkitykset pääsevät esille. (Hirsjärvi & Hurme 2000, 48.) Teemahaastattelun etuna on juurikin tarkkojen kysymysten puuttuminen, mikä antaa tilaa haastateltavien puheelle. Teemat kuitenkin rajaavat haastattelua, jolloin sitä on kohtuullisen helppoa ryhtyä analysoimaan teemoittain. (Saaranen-Kauppinen & Puusniekka 2006.)

Haastateltavat valitaan harkinnanvaraisesti, eli tutkijan asettamien kriteerien perusteella. Heidän tulisi olla sopivia tutkimusongelman kannalta ja tietää mahdollisimman paljon ilmiöstä. (Kananen 2008, 35–37, 73; Saaranen-Kauppinen & Puusniekka 2006.) Tutkimuksen teemahaastatteluissa haastatellaan eri kokoisia Jyväskylässä toimivia asianajotoimistoja. Osa heistä on siirtynyt kokonaan tai osittain pilvipalveluiden käyttöön ja osalla ei ole pilvipalveluita käytössä ollenkaan. Tietoa kerätään myös toimistoista, joissa ei ole pilvipalveluita käytössä, sillä juuri nämä tietosuoja- ja tietoturvakysymykset saattavat olla tekijöitä, jotka vaikuttavat siihen, ettei pilvipalveluita ole otettu käyttöön. Yhteensä haastatteluita tehdään viisi kappaletta.

Analyysimenetelmät

Aineiston analyysillä voidaan tarkoittaa esimerkiksi aineiston järjestelyä, sisällön erittelyä, jäsentämistä ja pohtimista. Analyysi voi tarkoittaa myös aineiston sisällön luokittelemista teemojen perusteella. Tarkoituksena on tiivistää haastatteluiden sisältöä tai rakennetta ja tarkastella tutkimusongelman kannalta olennaisten asioiden esiintymistä. Analyysin avulla tutkija tiivistämisen lisäksi tulkitsee aineistoa ja yhdistää teoriaa, empiriaa ja omaa ajatteluaan. (Saaranen-Kauppinen & Puusniekka 2006.) Aineiston teksti luetaan useampaan kertaan ja tutkija tekee aineistosta tulkinnan. Tekstistä etsitään tutkimusongelman kannalta olennaisimmat asiat ja ne tiivistetään asiakokonaisuuksiksi. (Kananen 2010, 63–64.)

Litteroinnin eli haastatteluiden puhtaaksikirjoittamisen jälkeen voidaan aloittaa varsinainen aineiston analyysi. Tässä tutkimuksessa käytetään analysointimenetelmänä teemoittelua, sillä teemahaastatteluiden jälkeen on luontevaa

analysoida tulokset teemoittain. Teemat eivät välttämättä vastaa ennakkoon asetettuja teemoja, sillä haastatteluista on saattanut nousta esiin eri teemoja, jotka jäsentävät tutkimusaihetta paremmin (Saaranen-Kauppinen & Puusniekka 2006). Teemoittelun avulla tehty analyysi voi jäädä vain haastatteluiden auki kirjoittamiseksi ilman tulkintaa ja johtopäätöksiä (Kananen 2008, 91). Tämän välttämiseksi tutkimustulosten esittelyssä käytetään maltillisesti sitaatteja ja teemojen käsittelyssä yhdistetään eri haastatteluista saatuja tuloksia, jolloin tulosten esittäminen ei koostu vain haastatteluiden auki kirjoittamisesta.

Luotettavuuden varmistus

Kaikissa tutkimuksissa tulisi arvioida tehdyn tutkimuksen luotettavuutta. Tavallisesti puhutaan tutkimuksen reliabiliteetista eli tulosten toistettavuudesta ja validiteetista eli tutkimuksen pätevyydestä. Edellä mainitut ovat määrällisessä tutkimuksessa käytettyjä mittareita, mutta niiden sopivuudesta laadullisen tutkimuksen luotettavuuden arviointiin ollaan montaa mieltä. Kvalitatiivisessa tutkimuksessa luotettavuuden kannalta oleellista on tarkka selostus tutkimuksen toteuttamisesta sen kaikissa vaiheissa. (Hirsjärvi ym. 2009, 232.) Myös oikeiden tutkimusmenetelmien valitseminen on tärkeää. Tutkimuksen tulisi olla objektiivista, mutta tutkijan tekemät valinnat vaikuttavat aina tutkimustuloksiin. Tämän takia subjektiivisuuden tiedostaminen tutkimusprosessin eri vaiheissa on tärkeää objektiivisuuden syntymiseksi. (Kananen 2008, 121– 123).

Kananen (2008, 124) kuvaa Mäkelän (1990) ehdottamia kvalitatiivisen tutkimuksen arviointiperusteita, jotka ovat aineiston riittävyys, analyysin kattavuus, arvioitavuus ja toistettavuus. Aineiston voidaan katsoa olevan riittävä eli saturoitunut, kun uuden tapauksen lisääminen ei tuo muutosta tuloksiin. Analyysin kattavuus puolestaan tarkoittaa, että tulkintoja ei ole perustettu satunnaisiin aineiston osiin, vaan tulkinta tapahtuu aineistoista löytyneiden yhtäläisyyksien perusteella. Analyysin arvioitavuus ja toistettavuus liittyvät toisiinsa. Tutkimus tulee dokumentoida tarkasti, jotta ulkopuolinen henkilö voi jälkikäteen tarkastella ratkaisuja ja päätelmiä. Näin ollen myös tutkimus voidaan teoriassa toistaa, kun tutkimusasetelma ja prosessit on dokumentoitu. (Mts. 36, 124–125.)

Tämän tutkimuksen luotettavuus varmistetaan valitsemalla oikeat menetelmät tutkimusongelman kannalta, jotka ovat aiemmin raportissa perusteltu. Tarkka

selostus tutkimuksen toteuttamisesta varmistetaan kuvaamalla haastatteluolosuhteet selvästi sekä nauhoittamalla haastattelut pelkkien muistiinpanojen tekemisen sijasta. Näin varmistutaan siitä, että haastatteluiden litterointi on tarkkaa. Aineiston analysointivaiheessa tulosten teemoittelu kuvataan huolellisesti ja tulkintaa tehdessä kerrotaan, millä perusteella kyseinen tulkinta on tehty. Tutkijan oman roolin vaikutus tutkimustuloksiin minimoidaan tiedostamalla se jokaisessa tutkimuksen vaiheessa. Näin pyritään varmistumaan siitä, että tutkijan omat asenteet ja näkemykset eivät sekoitu tutkimusmateriaaliin ja sen tulkintaan. Tutkimuksen luotettavuutta arvioidaan pohdinta-osiossa.

Toimeksiantaja

Suomen Asianajajaliitto on vuonna 1919 perustettu julkisoikeudellinen yhteisö. Sen tehtävänä on edistää oikeudellisten palveluiden saatavuutta varallisuudesta riippumatta. Vuonna 1959 se sai hoitaakseen myös lakisääteisiä tehtäviä, kun laki asianajajista (496/1958) säädettiin. (Suomen Asianajajaliitto n.d.) Asianajajaliiton tehtävänä on säännellä ja valvoa asianajotoimintaa, edistää asianajopalveluiden laatua, kouluttaa ja tukea asianajajia sekä kehittää oikeusoloja ja oikeusturvaa. Asianajajaliiton jäseneksi hyväksytään vain kokeneita lakimiehiä ja liiton jäsenmäärä on noin 2 100. Kaikki suomalaiset asianajajat kuuluvat asianajajaliittoon. (Asianajajaliitto lyhyesti n.d.) Asianajajaliitto jakautuu kahteentoista paikallisosastoon, joidenka puheenjohtajat ja muut jäsenet toimivat Asianajajaliiton paikallisina yhteyshenkilöinä. Keski-Suomen osasto on yksi näistä kahdestatoista paikallisosastosta. (Asianajajaliiton paikallisosastot n.d.)

3 Asianajotoimisto ja pilvipalvelut

Alhavan (2016, 22) mukaan digitalisaation tuloa on tärkeä miettiä myös asianajoalalla. Pilvipalveluihin siirtymisen puolesta puhuu käytettävyyden parantuminen, etätyöskentelymahdollisuus, hankintakustannusten edullisuus ja nopea käyttöönotto. Alhava (2016, 22) kertoo, että TrademarkNow’n toimitusjohtajan Anne Ronkaisen mukaan käytettävyys paranee dokumenttien hallinnan myötä, kun niitä on mahdollista hallita ja muokata eri laitteilla eri paikoissa.

Midpointedin toimitusjohtajan Olli Rikalan mukaan edullisuus mahdollistaa sen, että pienet ja keskisuuret toimistot voivat käyttää samoja palveluita kuin isotkin toimistot (mts.).

3.1 Asianajoala

Suomen oikeuslaitoksen tehtävänä on antaa oikeusturvaa, joka kuuluu ihmisen perusoikeuksiin. Oikeusturva tarkoittaa oikeuttaa saada asia käsitellyksi tuomioistuimessa asianmukaisesti. Asianajajalaitos kuuluu oikeuslaitokseen yhdessä tuomioistuimien, oikeusaputoimistojen, syyttäjälaitoksen, ulosottoviranomaisten ja Rikosseuraamuslaitoksen kanssa. Poliisi ei kuulu oikeuslaitokseen, mutta se on tiiviissä yhteistyössä oikeuslaitoksen kanssa, sillä sen tehtäviin kuuluu esitutkinta, josta alkaa rikoksen oikeudellinen selvittäminen. (Oikeuslaitos 2015.) Asianajajalaitokseen puolestaan kuuluu asianajajakunta, joka omalta osaltaan myötävaikuttaa oikeusturvan toteutumiseen (Ylöstalo & Tarkka 2001, 30).

Asianajaja on lailla suojattu ammattinimike ja sitä voi käyttää vain asianajajaliittoon hyväksytyt jäsenet (Suomen Asianajajaliitto n.d.). Noin 10 prosenttia suomalaisista lakimiehistä on asianajajia (Asianajajaliitto lyhyesti n.d.). Asianajaja voi työskennellä asianajotoimistossa tai julkisena oikeusavustajana (Asianajaja n.d.). Asianajajaliiton (2015) mukaan asianajotoimistoja on Suomessa vajaa 800 ja asianajajien lisäksi asianajotoimistoissa työskentelee yli 800 muuta lakimiestä. Keskimäärin toimistot ovat pieniä, 1–2 juristin toimistoja. Suuret toimistot ovat keskittyneet Helsinkiin. (Asianajajaliitto lukuina 2015.) Tämä vastaa hyvin asianajajaliiton vuonna 2012 julkaiseman asianajajatutkimuksen tulosta, jonka vastanneista hieman yli puolet asianajajista toimii Helsingissä. Keski-Suomessa toimii asianajajista 3 %. (Laukkanen & Järvenpää 2012, 7.)

Asianajotoimistoissa työskentelee asianajajien ja lakimiesten lisäksi yleensä asianajoassistentti tai -assistentteja toimiston koosta riippuen. Asianajotoimistoissa voidaan hoitaa yksityishenkilöiden, yhteisöjen tai yritysten toimeksiantoja. Esimerkkeinä hoidettavista asioista ovat oikeudenkäynnit, asuntokaupat, avioehtosopimukset, työsuhdetta koskevat asiat, perunkirjoitus- ja perinnönja-

kotilanteet sekä konkurssipesien hoito. Usein toimistojen toiminta painottuu tiettyihin oikeudellisiin tehtäväalueisiin. Toimeksiantojen myötä asianajotoimistoissa syntyy paljon kirjallista aineistoa, joka tulee säilyttää. (Asianajaja n.d.)

Asianajajaliiton säädöksissä ja ohjeissa on annettu asianajotoiminnassa kertyvän asiakirja-aineiston säilyttämistä koskeva suositus. Samasta säädöksestä löytyy hyvää asianajajatapaa koskevat ohjeet, jonka 5.11 kohdan mukaan asianajajan tulee toimeksiannon päättyessä palauttaa asiakkaalle hänelle kuuluvat asiakirjat. Tässä ohjeessa säädetään asianajotoimistoon jäävistä asiakirjoista. Säilytettävä aineisto on jaoteltu viiteen eri osaan asiakirjojen luonteen perusteella. (Asiakirjojen säilyttämistä koskeva suositus 2012, 1.)

Lain tai muiden säännösten mukaan säilytettäväksi määrätty aineisto täytyy arkistoida niin kuin laissa tai muissa säännöksissä on säädetty. Tällaisia asiakirjoja voivat olla esimerkiksi kirjanpitolaissa tarkoitetut tositteet. Samoin asianajajan tekemän erityisen sopimuksen nojalla säilytettävän aineiston arkistoinnissa tulee noudattaa sopimuksessa määriteltyä tapaa ja aikaa. Esimerkiksi testamenttien tai osakekirjojen säilyttämisestä voi olla tehty erityinen sopimus. (Mts.)

Muut alkuperäisluontoiset asiakirjat, kuten oikeudenkäyntipöytäkirjat tai kauppakirjat, annetaan toimeksiannon päättyessä päämiehelle. Muu asiakirja-aineisto, joka ei ole lain, säädöksen, tai sopimuksen perusteella määrätty säilytettäväksi, on suositeltavaa arkistoida kymmeneksi vuodeksi toimeksiannon päättymisestä. Esimerkiksi kirjeenvaihto tai jäljennökset alkuperäisistä asiakirjoista ovat edellä mainittuja asiakirjoja. (Mts. 1–2.)

Viimeisenä säädetään pesänselvityksen, perinnönjaon ja konkurssipesien hoidon yhteydessä syntyvästä sekä muusta vastaavasta erityisestä aineistosta. Pesänselvityksessä ja perinnönjaossa syntyvä aineisto suositellaan säilytettävän kymmenen vuotta. Konkurssivelallisen kirjanpitoaineisto suositellaan annettavaksi velalliselle, ja sen säilytyksessä tulee noudattaa kirjanpitolain määräyksiä. Muiden konkurssivelallisen asiakirjojen sekä konkurssipesän hoidosta syntyvien asiakirjojen säilytysajaksi suositellaan kymmentä vuotta. Erotuksena on konkurssipesän hoidon aikainen kirjanpitoaineisto, jossa noudate-

taan kirjanpitolain ohjeita. Muun erityisaineiston säilyttämisestä suositellaan vastaavia säilytysaikoja soveltuvin osin. (Mts.)

Riippumatta säilytettävän asiakirja-aineiston laadusta, on aineisto arkistoitava rikkomatta asianajajan salassapitovelvollisuutta. Samoin tulee menetellä asiakirjoja hävitettäessä. Jo vuonna 2006 ohjeisiin on lisätty kohta asiakirjojen sähköisestä arkisoinnista. Sen mukaan aineiston voi myös arkistoida sähköisesti, jos se on mahdollista säilytyksen vaarantumatta. Sähköisesti arkistoidut asiakirjat tulee luetteloida tai muulla tapaa jäsennellä selkeästi sähköiseen arkistoon. (Mts. 2–3.)

3.2 Aineistopankkihanke AIPA

Aineistopankkihankkeen eli AIPA-hankkeen takana on pyrkimys kehittää syyttäjälaitoksen ja yleisten tuomioistuinten toimintaa sekä luoda niille yhtenäinen asian- ja dokumentinhallinnan tietojärjestelmäkokonaisuus. Hankkeen tavoitteena on kehittää oikeushallinnon sisäisiä työvälineitä, mikä puolestaan tehostaa ja nopeuttaa lainkäyttöasioiden käsittelyä. Lisäksi se mahdollistaa poikkihallinnollisen yhteistyön muiden viranomaisten, kuten poliisin, kanssa. Aineistopankin myötä asiakirja-aineisto ja asianosaistiedot siirtyvät sähköisesti viranomaisten välillä. (Aineistopankkihanke 2012; Syyttäjänlaitoksen ja yleisten tuomioistuinten asian- ja dokumentinhallinnan kehittämishanke (AIPA) 2016.)

Hanke on laitettu vireille jo vuonna 2007, kun oikeusministeriö perusti yleisten tuomioistuinten asianhallinnan kehittämistyöryhmän. Hanke käynnistyi varsinaisesti vuonna 2010. (Syyttäjänlaitoksen ja yleisten tuomioistuinten asian- ja dokumentinhallinnan kehittämishanke 2010.) Se etenee vaiheittain niin, että järjestelmän on tarkoitus olla kokonaan käytössä vuoden 2018 aikana. Aineistopankin käyttöönotto aloitetaan rikosasioista, ja vuoden 2018 aikana rikosasioiden lisäksi riita- ja hakemusasiat hoidetaan oikeudessa sähköisesti. (OM: Rikos- ja riita-asioiden käsittely muuttuu vähitellen sähköiseksi 2014.)

13.3.2014 julkaistussa uutisessa asianajajaliiton sivuilla kävi ilmi, että käräjäoikeuksien oli tarkoitus siirtyä vuoden 2015 lopussa käsittelemään vangitsemisasioita sähköisesti. Myös syyttäjänvirastoissa oli tarkoitus samaan aikaan

ottaa ensimmäiset AIPAn ominaisuudet, eli sakkoihin liittyvät asiat, käyttöön. (OM: Rikos- ja riita-asioiden käsittely muuttuu vähitellen sähköiseksi 2014.) Käyttöönotto kuitenkin lykkääntyi ja hankkeen toteuttamista oikeusministeriössä johtavan Marko Loisan mukaan arvioitu vangitsemisasioiden sähköinen käyttöönotto siirtyy syksyyn 2017. Syyttäjänvirastoissa sakkomenettelyä voidaan käyttää jo tämän vuoden lopulla. (Vallisaari 2016.)

Aineistopankkihankkeen myötä luotavassa uudessa järjestelmässä syyttäjänvirastot ja yleiset tuomioistuimet käsittelevät kaikki vireille tulevat asiat sähköisesti aina niiden ratkaisemiseen ja arkistointiin asti. AIPA-järjestelmällä korvataan tällä hetkellä käytössä olevat erilliset järjestelmät. (Syyttäjänlaitoksen ja yleisten tuomioistuinten asian- ja dokumentinhallinnan kehittämishanke (AIPA) 2016.) Suurin muutos oikeushallinnon työtavoissa on paperisesta asiakirjojen käsittelystä sähköiseen työskentelyyn siirtyminen. Papereiden kopioiminen, postittaminen ja arkistointi loppuvat, ja myös asiakkaat voivat asioida sähköisesti syyttäjänvirastojen ja yleisten tuomioistuinten kanssa niin halutessaan. (Aineistopankkihanke 2012.)

Seuraavana kuvataan (kuvio 1) esimerkki rikosasian käsittelyyn liittyvien papereiden etenemisestä viranomaiselta toiselle.

Kuvio 1. Rikosasian papereiden eteneminen

Rikosasian käsittelyssä syntyy paljon paperista aineistoa ennen kuin asiaan tulee ratkaisu. Se alkaa poliisin esitutkintamateriaalista, josta se etenee syyttäjänvirastoon ja sieltä käräjäoikeuteen. Lisäksi rikosasiaan liittyy myös muita asianosaisten käräjäoikeudelle toimittamia asiakirjoja, joita ovat asianomistajan käräjäoikeudelle ilmoittamat korvausvaatimukset sekä vastaajan vastaus vaatimuksiin. Oikeuden istuntoihin toimitetaan paperiset kutsut haastemiehen tai postin välityksellä ja käsittelyn jälkeen ratkaisu toimitetaan asianosaisille kirjallisesti. Mahdollinen muutoksenhaku ratkaisuun siirtää aineiston seuraavaan oikeusasteeseen. (Vallisaari 2016.)

AIPA-järjestelmän myötä edellä kuvattu prosessi tapahtuu kokonaan sähköisesti yhdessä järjestelmässä. Tämä vaikuttaa asianajotoimistojen arkeen, sillä asioiden käsittelyn sähköistyessä muissa oikeuslaitoksen osissa myös asianajotoimistojen on vastattava ennemmin tai myöhemmin tähän uudistukseen. Tämä voi tapahtua esimerkiksi ottamalla pilvipalveluita käyttöön.

3.3 Pilvipalvelut

Pilvitoimintamalli on suhteellisen uusi ilmiö, vaikka sen varhainen kehitys on alkanut jo aiemmin. Varsinaisesti pilvitoimintamallin kehityksen katsotaan alkaneen 2000-luvun alussa ja pilvipalvelumarkkinoiden odotetaan kasvavan nopeasti. (Heino 2010, 33; Salo 2012, 11.) Pilvipalvelut eivät ole pelkästään teknologinen muutos, vaan myös liiketaloudellisen ajatustavan muutos siitä, miten tietotekniikkaa voidaan hyödyntää liiketoiminnassa. Tietotekniikan palvelullistamisen myötä yritykset voivat alentaa it-investointien kokonaiskustannuksia ja liikkuvan työn tekeminen helpottuu. Myös vahvasti pinnalla olevat ympäristöarvot otetaan paremmin huomioon, sillä pilvipalvelut kasvattavat resurssien käyttöastetta, vähentävät tilan- ja energian tarvetta sekä vähentävät työperäisen matkustamisen tarvetta. (Salo 2012, 16.)

Yritykset hankkivat yhä useammin tietojärjestelmäratkaisuja palveluina, sillä niiden vähäiset kustannukset, nopea käyttöönotto ja fyysisiin laitteisiin sitoutumattomuus houkuttaa. Suurimpana jarruttavana tekijänä näiden palveluiden ostossa on epätietoisuus siitä, kuka pääsee käsittelemään organisaation tietoja ja missä niitä konkreettisesti säilytetään. Tietoturvakysymykset tuleekin ot-

taa tarkasti huomioon miettiessä, minkälaiset ratkaisut soveltuvat toteutettavaksi pilvipalveluina. (Andreasson & Koivisto 2013, 17–18.)

Vaikka pilvipalveluiden hyödyt ovat tiedossa, ei käsitteen määrittely ole täysin yksiselitteistä. Yhtä yleisesti hyväksyttyä määritelmää käsitteelle ei ole. (Salo 2010, 16.) Yleiskielellä puhuttaessa pilvipalvelut tarkoittavat pilvipohjaisia it-palveluita, jotka voivat olla internetistä hankittua tietokonekapasiteettia, sovelluksia tai muita palvelusuoritteita. Ammattilaisten keskuudessa tarkempi määrittely ei pidä pilvipalveluita pelkästään palveluina, vaan kokonaan uutena toimintatapana. Tämän määritelmän mukaan pilvipalvelut ovat toimintamalli, jonka kautta ei enää tarvita fyysisiä konesaleja. Pilvipalvelut voivat korvata tai täydentää yrityksen omia ydinjärjestelmiä. (Andreasson & Koivisto 2013, 26; Heino 2010, 32.)

National Institute of Standards and Technology:n (NIST) määritelmä pilvipalveluille on yksi yleisimmin käytettyjä (Salo 2010, 17).

> *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.* (Mell & Grance 2011, 2.)

Salo (2010, 17) on kääntänyt NIST:n määritelmän niin, että pilvipalvelu on ”toimintamalli, joka mahdollistaa pääsyn vapaasti konfiguroitaviin ja skaalautuviin tietotekniikkaresursseihin, jotka voidaan ottaa käyttöön tai poistaa käytöstä helposti ja nopeasti”. Määritelmän lisäksi NIST on nimennyt viisi pilvipalveluiden ominaispiirrettä, joita ovat itsepalvelullisuus, pääsy palveluihin eri päätelaitteilla, resurssien yhteiskäyttö, nopea joustavuus ja käytön tarkka mittaaminen (mts.).

Itsepalvelullisuus tarkoittaa sitä, että tietotekniikkaresurssit saa käyttöön ja käytön voi lopettaa ilman tarvetta olla yhteydessä palveluntarjoajaan. Asiakas voi ostaa käyttöönsä tarpeensa mukaan palvelinaikaa ja tallennuskapasiteettia. Palvelut ovat saatavissa internetin välityksellä ja niiden käyttö onnistuu eri laitteilla, kuten puhelimella, tabletilla tai kannettavalla tietokoneella. Näin ollen palvelut eivät ole sidottu vain yhteen päätelaitteeseen, joka sijaitsee työpaikalla. (Mell & Grance 2011, 2; Salo 2010, 18.)

Resurssien yhteiskäyttö tarkoittaa asiakkaan kannalta sitä, että asiakas ei tarvitse eikä yleensä saa tietoa siitä, millä tavoin ja missä palvelut toteutetaan. Useiden asiakkaiden käytössä on siis sama laitteisto- ja ohjelmistokapasiteetti toisistaan tietämättä ja riippumatta, mikä mahdollistaa palvelun edullisen hinnan. Nopea joustavuus mahdollistaa tarjottujen palveluiden mukautumisen ylös- ja alaspäin, jolloin kapasiteettirajoitetta ei asiakkaan näkökulmasta käytännöstä ole. Myös uusien sovellusten käyttöönotto ja kehittäminen nopeutuvat ja esimerkiksi tallennuskapasiteetin lisääminen onnistuu tarvittaessa lähes välittömästi. Pilvipalveluiden käyttöä voidaan seurata, valvoa ja raportoida, mikä mahdollistaa läpinäkyvyyden sekä palveluntarjoajalle että palvelun käyttäjälle. Kun käyttöä mitataan tarkasti, asiakas maksaa vain käyttämästään kapasiteetista. (Mell & Grance 2011, 2; Salo 2010, 18.)

NIST:n pilvipalvelumääritelmään kuulu edellä kuvattujen ominaispiirteiden lisäksi kolme palvelumallia (Mell & Grance 2011, 2). Kolme yleisintä tyyppiä ovat Platform as a Service (PaaS), Infrastructure as a Service (Iaas) ja Software as a Service (SaaS) (Heino 2010, 50). Palveluita käyttävän yrityksen kannalta ei ole väliä, mitä yllä mainituista lyhenteistä pilvipalveluista käytetään, sillä niillä kaikilla on aiemmin mainitut NIST:n listaamat ominaisuudet. Pilvipalvelut mahdollistava tekniikka ei ole yrityksen näkökulmasta keskeinen asia, vaan tärkeämpää on tekniikan kyky mahdollistaa liiketoimintaprosessit ja näin ollen tuki koko yrityksen liiketoiminnalle. (Salo 2010, 22–23.)

Pilvipalveluita tuottaa pilvipalveluntarjoaja tai pilvitoimija. Käsitteet on syytä erottaa toisistaan, sillä pilvipalveluntarjoaja on yritys tai yhteisö, jonka kanssa on tehty jonkinlainen sopimus etukäteen määritellystä palvelusta. Pilvitoimija on puolestaan sellainen, jonka palveluita hyödynnetään, mutta jonka kanssa ei ole tehty käytetyn kapasiteetin perusteella veloitukseen johtavaa sopimusta. Esimerkiksi Facebook on pilvitoimija. (Heino 2010, 34.)

Palvelutasosopimus eli SLA (service level agreement) on palveluntarjoajan lupaus palvelun tasosta. Sopimus tehdään palveluntarjoajan ja asiakkaan välille ja tason toteutumista valvotaan erilaisilla sovituilla mittareilla ja seurantapalavereilla. Mikäli sovittu palvelutaso alitetaan, voi siitä seurata sanktio, jos siitä on sopimuksessa määritelty. (Andreasson & Koivisto 2013, 25.) Sanktio voi esimerkiksi olla hyvityslasku tai alennus seuraavasta laskusta. Yleensä

sanktio on siis sidottu palvelusta maksettavaan korvaukseen, eikä yritykselle aiheutuvaan haittaan. Ilman SLA-sopimusta ei käytännössä ole sovittua lupausta palvelun toiminta-ajoista, huoltokatkojen enimmäispituuksista tai vikatilanteessa korjauksiin vievän ajan maksimikestosta. (Heino 2010, 35–36.)

4 Oikeudelliset kysymykset pilvipalveluissa

Tilastokeskuksen vuonna 2014 tekemässä tutkimuksessa on tutkittu tietotekniikan käyttöä eri toimialoja ja yrityskokoja edustavissa yrityksissä. Yrityksen koko minimissään oli kymmenen henkilöä työllistävä. Yhtenä tutkimuksen osa-alueena oli pilvipalveluiden käyttö yrityksissä. Tuloksena saatiin, että hieman yli puolet yrityksistä käyttää pilvipalveluita ja yleisimmin käytetyt pilvipalveluratkaisut ovat sähköposti, tiedostojen tallennus ja kirjanpitosovellukset. Kolmannes pilvipalveluita käyttävistä yrityksistä koki tietoturvariskit käyttöä rajoittavina tekijöinä. Myös yritykset, jotka eivät käytä pilvipalveluita, kokivat tietoturvariskit ja epävarmuuden oikeudellisissa kysymyksissä esteinä pilvipalveluiden käytölle. (Tietotekniikan käyttö yrityksissä 2014, 5, 14, 17.)

Vaikka asianajoalaa ei ole eritelty vastanneiden yritysten toimialoista, on huomattavaa, että yritykset kokivat pilvipalveluita rajoittavina tai käyttöä estävinä tekijöinä tietoturvariskejä sekä epävarmuutta oikeudellisista kysymyksistä. Alhavan (2016, 22) mukaan tietoturvatason säilyminen on lähinnä ollut huolena pilvipalveluissa asianajoalan näkökulmasta. Kuitenkin Alhavan (2016, 22) mukaan Midpointedin toimitusjohtajan Olli Rikalan mielestä isojen pilvipalvelutoimijoiden tietoturva on parempi kuin perinteisessä ”mapit hyllyssä” toimintatavassa. Niiden palvelimet eivät ole paikallisia, vaan kokonaan asiakkaan käytössä. On olemassa toimialakohtaisia it-ratkaisuja ja helpointa on valita valmiiksi asianajotoimistoille suunnattu järjestelmä. (Mts.)

Tässä luvussa kuvataan tietosuojaan ja tietoturvaan liittyvä keskeisin lainsäädäntö ja asianajajaliiton säädökset pilvipalveluiden käyttöön liittyen. Tämän lisäksi määritellään tietosuoja ja tietoturva käsitteinä sekä liitetään niihin tärkeimmät kohdat lainsäädännöstä.

4.1 Lainsäädäntö

Pilvipalvelut ovat globaaleja, mutta niillä ei ole yhtä yhtenäistä lainsäädäntöä. Niiden lainsäädännöllinen kenttä on hajaantunut ja yrityksen toimintamaasta riippuen lainsäädäntö voi olla erilaista. Eroja voi olla esimerkiksi siinä, voiko yritys tallentaa asiakastietojaan toimintamaansa rajojen ulkopuolella sijaitsevaan palvelinkeskukseen. (Salo 2010, 107.) Pilvipalveluille on ominaista, että ne eivät rajaudu vain tietyn maan rajojen sisäpuolelle. Näin ollen yrityksille voi olla epäselvää, minkä maan lakia noudatetaan EU:n sisällä ja erityisesti EU:n ulkopuolella tapahtuvissa mahdollisissa kiistoissa. (Kalli ym. 2013, 32.)

Erilaiset asetukset ja standardit säätelevät yrityksen liiketoimintaprosesseja ja sitä, mitä tietoja ja miten niitä tulee säilyttää. Tämän takia yrityksen on ensin selvitettävä, mitä asetuksia ja standardeja sen tulee noudattaa, mitä asiakkaat tai yhteistyökumppanit vaativat noudatettavan, mitä yritys haluaa vapaaehtoisesti noudattaa sekä mitä järjestelmiä vaaditut asetukset ja standardit koskevat. Näiden lisäksi myös kansallinen ja kansainvälinen lainsäädäntö tulee ottaa huomioon. (Salo 2010, 106–107.)

Tietosuojalainsäädäntö antaa raamit asiakkaiden henkilötietojen käsittelyyn ja näin ollen määrittää sähköisen liiketoiminnan oikeudellisia perusteita. Sähköinen liiketoiminta tarkoittaa sitä, että yrityksen palvelut ja liiketoimintaprosessit on usein toteutettu tietojärjestelmillä, joissa käsitellään asiakkaiden henkilötietoja. Yrityksen kehittäessä sähköistä liiketoimintaa sen täytyy tehdä liiketoiminnallisten ja teknisten päätösten lisäksi myös oikeudellisia päätöksiä. Sähköisessä liiketoiminnassa henkilötietojen käsittely on kriittinen osa yritysten liiketoimintaa. Yritysten vastuullisuus yksityisyyden suojaamisesta vahvistaa asiakkaiden luottamusta. (Salminen 2009, 9, 23.)

Tietosuojalainsäädännön kannalta keskeistä on yksityisyyden suoja. Tärkeimpiä lakeja niin yleisessä tietosuojalainsäädännössä kuin pilvipalveluiden tietosuojassa ovat henkilötietolaki (523/1999), laki yksityisyyden suojasta työelämässä (759/2004), tietoyhteiskuntakaari (917/2014), laki sähköisestä asioinnista viranomaistoiminnassa (13/2003) ja laki viranomaisten toiminnan julkisuudesta (621/1999). Osa näistä laeista koskee kaikkia organisaatioita, mutta

osa säätelee ainoastaan julkisyhteisöjen toimintaa. (Heino 2010, 98–99; Lait 2015.)

Euroopan unionin asettamat direktiivit vaikuttavat jäsenmaidensa lainsäädäntöön siten, että ne tulee panna täytäntöön kansallisessa lainsäädännössä. Tämä edesauttaa yhdenmukaista lainsäädäntöä EU:n alueella. (EU-lakien suhde Suomen lakiin 2015.) Salmisen (2009, 43) mukaan Suomen perustuslaki (731/1999) määrittelee ihmisen perusoikeudet, joihin yhtenä osana kuuluu oikeus yksityisyyden suojaan. Samoin siinä määritellään, että henkilötietojen suojasta säädetään tarkemmin lailla, joka on henkilötietolaki. Euroopan parlamentin ja neuvoston asettaman henkilötietodirektiivin velvoitteet on tuotu osaksi henkilötietolakia. Toinen Euroopan unionin antama tietosuojaan liittyvä direktiivi on sähköisen viestinnän tietosuojadirektiivi. Sen velvoitteet on saatettu voimaan osana sähköisen viestinnän tietosuojalakia (516/2004). (Mts. 43–45.) Sähköisen viestinnän tietosuojalaki on nykyisin osana tietoyhteiskuntakaarta.

Liiketoiminnan sähköistyessä myös tietosuojalainsäädäntö on laajentunut. Tietosuojalainsäädäntö on melko uutta verrattuna moneen muuhun lainsäädännön alueeseen, sillä laissa on ratkottu tietosuojaa koskevia kysymyksiä vasta viime vuosikymmeninä. Tietosuojalainsäädännön vaikutus yritysten toiminnassa tulee kasvamaan sitä mukaa, kun uusia sähköisen liiketoiminnan teknologioita otetaan käyttöön. Myös asiakastietojen käsittelyn merkitys liiketoiminnassa tulee olemaan entistä tärkeämpää. (Salminen 2009, 19–20.)

Tekniikan nopea kehitys ja globalisoituminen ovat omalta osaltaan luoneet uusia haasteita henkilötietojen suojaamiseen. Tämän takia käynnissä on Euroopan unionin tietosuojauudistus, joka tulee vaikuttamaan henkilötietojen käsittelyyn. Uudella tietosuoja-asetuksella kumotaan EU:n henkilötietodirektiivi ja sitä aletaan soveltaa 25.5.2018 jälkeen. (EU:n tietosuojauudistus 2015.) EU:n on luotava kattava ja johdonmukainen lähestymistapa takaamaan yksilön tietosuojaa koskevan perusoikeuden noudattamisen sekä EU:n alueella että sen ulkopuolella. Tavoitteena on luoda Euroopan unionille ajanmukainen ja yhtenäinen tietosuojakehys, jolla voidaan parantaa luottamusta sähköisiin palveluihin. (Euroopan unionin tietosuojalainsäädännön uudistaminen 2016).

Asetus sisältää kansallista liikkumavaraa, eli Suomessa voidaan tietyiltä osin tehdä siihen kansallisia ratkaisuja asetuksen kokonaisvaltaisen soveltamisen sijaan. Lopullinen asetusteksti vaatii vielä selvennystä ja sen kansallinen täytäntöönpano kuuluu oikeusministeriön toimialaan. (EU:n tietosuoja-asetus muuttaa henkilötietojen käsittelyä 2016) Oikeusministeriö on asettanut helmikuussa 2016 työryhmän, joka selvittää, minkälaisia lainsäädäntötoimia asetus edellyttää. Se valmistelee myös ehdotuksen mahdolliseksi yleiseksi tietosuojalainsäädännöksi. (Tietosuojalainsäädäntö n.d.) Asetuksen myötä henkilötietojen käsittelyyn tullaan soveltamaan asetustekstiä, uudistettua henkilötietolakia ja julkisuuslakia, joiden lisäksi erityissääntelyn tietosuojakohtiin tullaan tekemään muutoksia (EU:n tietosuoja-asetus muuttaa henkilötietojen käsittelyä 2016).

Asianajajaliiton säädökset

Yleisen tietosuoja- ja tietoturvalainsäädännön lisäksi asianajotoimintaa velvoittaa asianajajaliiton säädökset ja ohjeet. Näiden säädösten kohdassa B 5.1 on määritelty tietoturvallisuusohjeet ja kohdasta B 5.2. löytyy tietoturvaopas. Tietoturvallisuusohjeeseen on koottu 10 tietoturvallisuuteen liittyvää kohtaa, joista asianajajan on huolehdittava. Pilvipalveluihin siirtymisen kannalta keskeisin ohje on, että erityisesti sopimukset ulkoistetuista it-palveluista tulee täyttää tietoturvavaatimukset. Asiakirjojen tallennus, säilytys, arkistointi ja hävitys tulee tapahtua tietoturvallisella tavalla. Lisäksi asiakkaan kanssa käytävään sähköiseen viestintään tulee olla asiakkaan hyväksyntä. (Tietoturvallisuusohje 2013.)

Tietoturvaoppaassa on määritelty tarkemmin tietoturvallisuusohjeen sisältämät kohdat ja siinä kerrotaan asianajotoimistojen tietoturvallisuusvaatimukset. Toimistoissa on muun muassa otettava huomioon laitteiden sijoittaminen niin, etteivät asiakkaat näe esimerkiksi tulostettavia asiakirjoja. Lisäksi on huolehdittava tietokoneiden salauksesta, käyttöjärjestelmien päivittämisestä uusimpaan versioon ja asiakirjojen varmuuskopioinnista. Tietoturvaoppaasta löytyy myös erikseen kohta it-palveluiden ulkoistamisesta ja pilvipalveluista. It-palveluiden ulkoistaminen tarkoittaa sitä, että tietoja käytetään ja säilytetään palveluntarjoajan palvelimella. (Tietoturvaopas 2012, 1–2, 11.)

Ulkopuolisen it-tuen käyttö jossain muodossa on usein välttämätöntä, sillä it-palvelusopimuksia syntyy lähes huomaamatta internetin palveluita käytettäessä. Esimerkiksi sähköposti, www-sivut, sähköinen kalenteri, laskutus sekä asiakas- ja toimeksiantorekisteri käyttävät ulkoista palvelintilaa. Suurin kysymys it-palveluiden ulkoistamisessa on asianajosalaisuuksia sisältävän tiedon säilytys, käyttö ja siirto tietokoneilla, jotka eivät ole vain asianajajan hallinnassa. Tämän takia palveluita hankittaessa on kiinnitettävä erityisesti huomiota asianajajan salassapitovaatimuksiin. Palveluntarjoajan tulee sitoutua täydelliseen tietojen salassapitoon, eikä tietoihin saa päästä kukaan muu kuin asianajaja ja hänen toimistonsa henkilökunta. (Mts. 11.)

Palveluntarjoajan kanssa tulee tehdä salassapitosopimus, jolla varmistetaan tietojen luottamuksellisuus. Palveluntarjoajan teknisen tietoturvatason tulee olla riittävän korkea ja sen lisäksi on suositeltavaa tarkistaa yrityksen taustat ja vakavaraisuus. Palveluntarjoajaa valitessa tulee kiinnittää huomiota palvelimen sijaintimaahan, sillä palvelimet saattavat sijaita eri puolilla maailmaa. Lisäksi varmuuskopioinnin taso, tiedostojen palautettavuus ja tietojen saatavuus tietoliikenneyhteyksien pettäessä ovat asioita, jotka tulee ottaa huomioon. (Mts. 12–13.)

Asianajajaliiton tietoturvaoppaassa säädetään myös pilvipalveluiden käytöstä. Niiden tietoturvan laatuun liittyvät vaatimukset eivät käytännössä poikkea edellä mainituista ulkoistettujen palveluiden käyttöönoton vaatimuksista. Osa tarjotuista pilvipalveluista on ilmaisia tai erittäin edullisia ja niissä käytetään käyttöönottosopimuksessa vakiosopimusta. Tällaisiin palveluihin ei kannata tallentaa luottamuksellista tietoa, sillä palveluntarjoaja saattaa seurata tiedostojen sisältöä ja tallentaa tietoja itselleen. Toisaalta tietojen käsittely ja säilyttäminen luotettavan palveluntarjoajan pilvipalveluissa voi olla tietoturvallisin ratkaisu. Luottamuksellisen tiedon pitäminen pilvipalveluissa mahdollistaa sen, ettei tietoa tarvitse säilyttää tietokoneella tai puhelimessa. Näin ollen yksittäisen laitteen häviäminen tai rikkoutuminen ei aiheuta tietoturvavahinkoja. (Mts.)

Edellä mainituista säädöksistä ja ohjeista koskien ulkoistamista asianajajaliitto on tehnyt yhteenvedon, joka sisältää asiat, joista tulisi ainakin huolehtia. Etäyhteyden käyttäminen ei saa vaarantaa asianajotoimiston tietoturvaa ja etäyhteyden käytöstä on oltava päätäntävalta asianajajalla, palvelutarjoajan

kanssa on tehtävä salassapitosopimus sekä on ajateltava tietoturvallisesti. (Mts. 13.)

Tietoturvaoppaassa on säädetty myös sähköisestä viestinnästä. Sähköpostiviestit ovat luottamuksellisia, ellei niitä ole nimenomaisesti tarkoitettu julkiseksi. Laki suojaa sähköistä viestintää kuten muutakin luottamuksellista viestintää. Asianajajan on suositeltavaa käyttää sähköpostiviestin lopussa luottamuksellisuusilmoitusta. Erityisesti silloin kun sähköposti sisältää henkilötietoja, on noudatettava erityistä huolellisuutta. Sähköpostin palveluntarjoajalla tulee olla korkea tietoturvan taso sekä sopimuksellisesti että tosiasiallisesti. (Mts.) Andreasson ja Koivisto (2013, 135) muistuttavat, että sähköpostijärjestelmän ylläpito on usein ulkoistettu ulkopuoliselle palveluntuottajalle, minkä takia sopimuksessa on syytä määritellä yksityiskohtaisesti tietosuoja ja tietoturva.

4.2 Tietosuoja

Tietosuojasta ja tietoturvasta puhutaan usein samassa yhteydessä, mutta käsitteet tulee erottaa toisistaan. Niiden erona on se, että tietosuojan piiriin kuuluu lähinnä yksityisyyden suojaaminen ja henkilötietojen käsittelyn toimintatavat, kun taas tietoturvaan kuuluu erityisesti tietojen luottamuksellisuuden, eheyden ja käytettävyyden varmistaminen. (Salminen 2009, 81.) Järvisen (2012, 12) mukaan tietoturvassa suojataan itse tietoja ja tietojärjestelmiä, kun taas tietosuojassa kohteena ovat ihmisten henkilötiedot. Tietoturvassa pyritään varmistamaan järjestelmien toiminta olosuhteista riippumatta ja käytön turvallisuus. Tietosuojalla pyritään varmistamaan ihmisen oikeus yksityisyyteen ja estämään hänen tietojensa väärinkäyttö. (Mts.)

Tietosuoja ei siis pelkästään tarkoita yksityisyyden suojaa, vaan se on käsitteenä laajempi. Se tarkoittaa kansalaisen yksityisyyden suojan ja oikeusturvan huomioonottamista tietojen rekisteröinnissä. Siihen kuuluu myös tiedostojen suojaaminen ulkopuoliselta käytöltä ja henkilön oikeus saada tietää itseään koskevista rekisteritiedoista. Laissa on säädetty sekä julkisten että salassa pidettävien henkilötietojen käsittelystä. (Andreasson & Koivisto 2013, 27.) Tietosuojalainsäädäntö luo henkilötietojaan luovuttaville henkilöille oikeuksia, sillä se suojaa yksilöä ja hänen oikeuksiaan tietoihinsa. Se suojaa myös yksilöä

hänen henkilötietojensa vahingolliselta käytöltä. Henkilötietoja käsitteleville yrityksille eli rekisterinpitäjille tietosuojalainsäädäntö puolestaan asettaa velvollisuuksia. On otettava huomioon, että tietosuojalainsäädäntö ei suojaa itse tietoa, vaan yksilöä ja hänen oikeuksiaan omiin tietoihinsa. (Salminen 2009, 15.)

Henkilötietolaki on tärkein tietosuojaan liittyvä laki. Sen tarkoituksena on toteuttaa yksityiselämän suojaa henkilötietoja käsiteltäessä ja edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. Lakia on noudatettava aina henkilötietoja käsiteltäessä ja sitä sovelletaan henkilötietojen automaattiseen käsittelyyn ja muuhun henkilötietojen käsittelyyn, kun ne muodostavat henkilörekisterin tai sen osan. Henkilötietolakia sovelletaan niiden henkilötietojen käsittelyyn, joissa rekisterinpitäjän toimipaikka on Suomen alueella tai muulla tavalla Suomen oikeudenkäytön pirissä. Lakia sovelletaan myös silloin, kun rekisterinpitäjän toimipaikka ei ole Euroopan unionin jäsenvaltioiden alueella, mutta rekisterinpitäjä käyttää henkilötietojen käsittelyssä Suomessa sijaitsevia laitteita. Tällöin rekisterinpitäjän tulee nimetä Suomessa oleva edustaja, jonka vastuulla on rekisterinpitäjälle kuuluvat velvollisuudet Suomessa. (L 22.4.1999/523; Vanto 2011, 36.)

Tietosuojaan liittyvien tärkeiden termien ja määritelmien tunteminen on tarpeellista arvioitaessa tietosuojalainsäädännön vaikutuksia yrityksen toimintaan. Määritelmät on kuvattu henkilötietolain 3 §:ssä. Laajasti katsottuna **henkilötiedoilla** tarkoitetaan kaikkea luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota yrityksen toiminnassa käsitellään. (Salminen 2009, 17.) Yksinkertaisimmillaan henkilötieto on esimerkiksi henkilötunnus, mutta toisaalta henkilötieto voi olla myös auton rekisterikilpi tai sähköpostiosoite. Henkilötietolain soveltamisen kannalta on tärkeää arvioida, onko tieto sellainen, jonka perusteella henkilö tunnistetaan. (Vanto 2011, 22–23.)

Henkilötietojen käsittelyllä tarkoitetaan puolestaan esimerkiksi henkilötietojen keräämistä, tallentamista, käyttöä, luovuttamista, säilyttämistä ja tuhoamista (Salminen 2009, 17). Käytännössä siis kaikki henkilötietoihin kohdistuva toimenpide on henkilötietojen käsittelyä ja siinä on noudatettava henkilötietolakia (Vanto 2011, 28–29). **Henkilörekisteri** on käyttötarkoituksensa vuoksi yhteenkuuluvista merkinnöistä muodostuva henkilötietoja sisältävä tietojouk-

ko. Sitä voidaan käsitellä joko kokonaan tai osittain automaattisen tietojenkäsittelyn avulla tai se voi olla järjestetty esimerkiksi kortistoksi tai luetteloksi. Henkilörekisteristä voidaan helposti löytää tiettyä henkilöä koskevat tiedot. (Salminen 2009,17–18.) Esimerkiksi asianajotoimiston asiakkaille laatimat muistiot tai asiakirjat, joihin sisältyy henkilötietoja, eivät vielä sellaisenaan muodosta lain tarkoittamaa rekisteriä. Niistä muodostuu rekisteri, kun ne tallennettu järjestelmään, jossa tiedostoista voidaan hakea tietoa niiden sisältämien henkilötietojen perustella. (Vanto 2011, 29.)

Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan. Rekisterinpitäjällä on oikeus määrätä henkilörekisterin käytöstä tai rekisterinpito on voitu myös säätää lailla rekisterinpitäjän tehtäväksi. **Rekisteröity** puolestaan on henkilö, jonka henkilötietoja käsitellään. (Salminen 2009, 18.) **Sivullinen** on jokin muu henkilö, yhteisö, laitos tai säätiö kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai kahden viimeksi mainitun lukuun henkilötietoja käsittelevä. **Suostumus** tarkoittaa kaikenlaista vapaaehtoista, yksilöityä ja tietoista tahdonilmausta, jolla rekisteröity hyväksyy tietojensa käsittelyn. Suostumuksen ei välttämättä tarvitse olla kirjallinen, mutta se on suositeltavaa rekisterinpitäjän kannalta. Näin hän voi todistaa suostumuksen olemassa olon. (L 22.4.1999/523; Vanto 2011, 33, 35.)

Myös työntekijän yksityisyyden suojasta työelämässä säädetään erikseen laissa. Siinä säädetään työntekijää koskevien henkilötietojen käsittelystä, työntekijälle tehtävistä tarkastuksista, teknisestä valvonnasta työpaikalla sekä työntekijän sähköpostiviestin avaamisesta. Lain tarkoituksena on toteuttaa yksityiselämän suojaa työelämässä. Sen mukaan työnantaja saa käsitellä vain työntekijän työsuhteen kannalta tarpeellisia henkilötietoja ja henkilötiedot tulee kerätä henkilötiedot työntekijältä itseltään. (L 13.8.2004/759.)

Tietoyhteiskuntakaaren yhtenä tavoitteena on sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutumisen takaaminen (L 7.11.2014/917). Yritysten tulisi kiinnittää huomiota sähköpostin käyttöön, sillä se kuuluu nykypäivänä yritysten jokapäiväiseen toimintaan (Andreasson & Koivisto 2013, 134). Viestintäverkot ja -palvelut ja niihin liitettävät viestintäverkot ja -palvelut on suunniteltava niin, että sähköinen viestintä on tekniseltä

laadultaan hyvää ja tietoturvallista. Kenenkään tietosuoja, tietoturva eikä muut oikeudet saa vaarantua. (L 7.11.2014/917.) Tietosuojan turvaamiseksi tulisi välttää salassa pidettävien asiakirjojen ja muiden luottamuksellista tietoa sisältävien dokumenttien lähettämistä suojaamattomalla sähköpostiyhteydellä. Tieto voi helposti joutua vääriin käsiin, jos sähköpostia käytetään varomattomasti. (Andreasson & Koivisto 2013, 136.) Tietoyhteiskuntakaaren 136 § mukaan vastaanottaja, joka on saanut sähköpostin, jota ei ole hänelle tarkoitettu, ei saa ilman viestinnän osapuolen suostumusta käyttää hyväksi viestin sisältöä (L 7.11.2014/917).

Monien sähköpostijärjestelmien yhteyteen on liitetty sähköinen kalenteri. Myös siihen tehtävissä kalenterimerkinnöissä tulee muistaa tietosuoja. Salassa pidettävää aineistoa ei saisi liittää kalenterikutsun yhteyteen siten että ulkopuoliset voivat nähdä sitä. Sähköposti ja sähköinen kalenteri on mahdollista synkronoida myös matkapuhelimeen, jolloin siihen kopioituu sähköposteja ja kalenterimerkintöjä. Matkapuhelin tulisi suojata pääsykoodilla, jotta puhelimen katoaminen tai vääriin käsiin joutuminen ei aiheuta tietosuojauhkaa. (Andreasson & Koivisto 2013, 147–149.)

Tietojenkäsittelyn ja yksityisyyden suojaamisen riskit ovat kasvaneet arjen tietoyhteiskunnan myötä. Tietotekniikka on tullut osaksi jokaisen ihmisen arkipäivää ja tietojenkäsittelyä tapahtuu kaikkialla kaiken aikaa. Toisaalta tekniikan kehittyminen on tuonut ja tuo jatkuvasti uusia tietojenkäsittelyyn perustuvia mahdollisuuksia. Yritykset ovat ottaneet käyttöön tietojärjestelmiä, joita ei ollut aiemmin mahdollista toteuttaa. Se on lisännyt henkilötietojen keräämisen ja käsittelyn määrää yrityksissä, mikä puolestaan kasvattaa tietosuojan huomioimisen tarpeita. (Salminen 2009, 18–19.)

Pilvipalveluissa säilytetään lähes aina henkilötietoja ja henkilötietolain vaatimukset ulottuvat myös ulkoistettuihin palveluihin. EU:n sisällä ja ETA-alueella on Euroopan unionin mukainen tietojen vapaa liikkuvuus, joten henkilötietoja saa siirtää näillä alueilla sekä EU:n komission hyväksymissä riittävän tietosuojatason maissa. (Salminen 2009, 83.) Lähtökohtaisesti kohdemaassa tulee olla sama tietosuojan taso kuin lähtömaassa, sillä pilveen tallennettuihin tietoihin pätee sijaintimaan laki (Castrén 2010). Henkilötietolain 22 § mukaan henkilötietoja saa siirtää EU:n jäsenvaltioiden alueen tai Euroopan talousalu-

een (ETA) ulkopuolelle vain silloin, kun kyseisessä maassa on riittävä tietosuojan taso (L 22.4.1999/523).

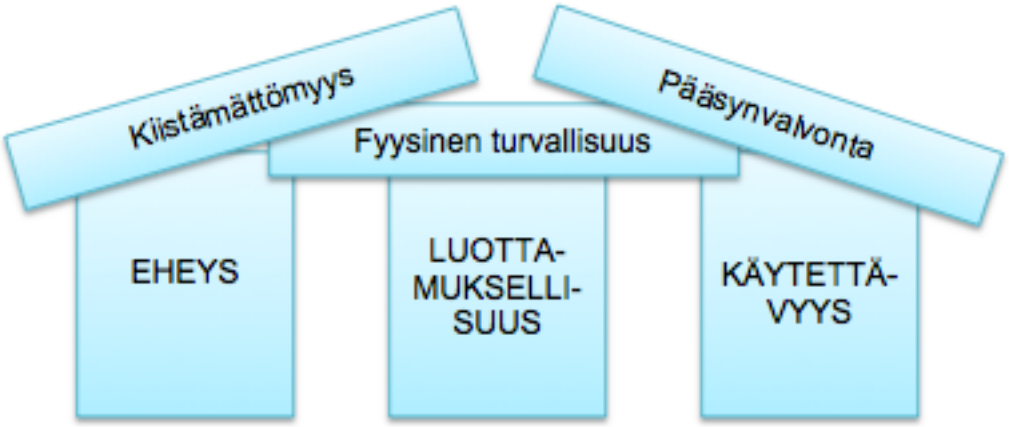
Euroopan komission mukaan tällä hetkellä riittävän tietosuojatason maita ovat Andorra, Argentiina, Kanada, Färsaaret, Guernsey, Israel, Mansaari, Jersey, Uusi-Seelanti, Sveitsi ja Uruguay (Adequacy decisions 2016). Lisäksi poikkeusperiaatteena on esimerkiksi henkilötietojen siirtojen tapahtuminen komission hyväksymiä mallisopimuslausekkeita käyttäen (L 22.4.1999/523). Jos palveluntarjoaja ei voi varmistaa tietojen säilytyspaikkaa, ollaan tietosuojan kannalta hankalassa tilanteessa. Tiedot voivat sijaita sellaisessa maassa sijaitsevalla palvelimella, jossa ei ole samanlaisia tietosuojavelvoitteita kuin Suomessa. (Castrén 2010.)

Yhdysvaltain tietosuojan taso on EU:n komission mukaan riittämätön, joten vuonna 2000 tehtiin niin kutsuttu turvasatamasopimus (Safe Harbor), jossa on sovittu toimintaperiaatteista liittyen tietoturvavaatimuksiin. Sopimus mahdollistaa sen, että EU-direktiivien mukaiset tietoturvavaatimukset täyttyvät myös Yhdysvalloissa, mikä mahdollistaa henkilötietojen säilyttämisen yhdysvaltalaisyritysten Yhdysvalloissa sijaitsevilla palvelimilla. (Pynnä 2015; Salo 2012, 45.) Kesällä 2016 EU hyväksyi Safe Harbor-sopimuksen jatkajaksi Privacy Shield -sopimuksen, jota ennen oltiin hetki ilman sopimusta EU:n ja Yhdysvaltojen välillä. Pilvipalveluiden kannalta on olennaista, että EU:n ja Yhdysvaltojen välillä on olemassa sopimus, sillä useat pilvipalvelut siirtävät henkilötietoja Yhdysvaltoihin tallennettavaksi. (Korhonen 2016.)

4.3 Tietoturva

Tietoturvallisuudelle on useita erilaisia määritelmiä, mutta kaikki niistä lähtevät samasta perusajatuksesta. Yrityksen tärkein ominaisuus on tieto, joka halutaan pitää luotettavana sekä nopeasti, oikeassa muodossa, ja oikeiden henkilöiden saatavilla. Klassisen määritelmän mukaan tietoturvallisuus koostuu kolmesta osatekijästä, joita ovat luottamuksellisuus, eheys ja käytettävyys. Tietoja tulee suojata tahallisten väärinkäytösten, laitteisto- ja tietoverkkovikojen sekä erilaisten luonnontapahtumien aiheuttamilta uhilta ja vahingoilta. (Hakala, Vainio & Vuorinen 2006, 4; Salminen 2009, 81.) Klassista määritel-

mää on myöhemmin laajennettu ottamaan huomioon myös kiistämättömyys ja pääsynvalvonta (Hakala ym. 2006, 5). Kuviossa 2 kuvataan sekä klassisen määritelmän että laajennetun määritelmän mukaiset tietoturvallisuuden osatekijät.



Kuvio 2. Tietoturvallisuuden osatekijät (Hakala ym. 2006, 6.)

Luottamuksellisuudella tarkoitetaan sitä, että tiedot ja tietojärjestelmät ovat vain henkilöiden käytössä, joilla on niihin käyttöoikeus. Tietojen ja tietojärjestelmien tulee olla eheitä, eli luotettavia, oikeita ja ajantasaisia. Sähköpostit, yrityssalaisuudet ja henkilötiedot eivät saa vuotaa julkisuuteen. Käytettävyys puolestaan tarkoittaa, että tietojen ja tietojärjestelmien palveluiden tulee olla niiden käyttöön oikeutettujen käytössä riittävän nopeasti. (Järvinen 2012, 10; Salminen 2009, 81–82.) Käytettävyyteen liittyy myös vaatimus palvelun jatkuvuudesta ja häiriöiden ratkaisuajasta (Andreasson & Koivisto 2013, 79).

Luottamuksen varmistamiseksi tietojärjestelmien laitteet ja tietovarastot suojataan käyttäjätunnuksin ja salasanoin. Eheyttä tavoitellaan pääasiassa ohjelmointiteknisin ratkaisuin ja käytettävyyttä puolestaan ylläpidetään tieto- ja tietoliikennejärjestelmien laitteiden tehokkuudella. Lisäksi käytettävien ohjelmistojen tulisi soveltua mahdollisimman hyvin järjestelmään tallennettujen tietojen käsittelyyn. (Hakala ym. 2006, 4–5.)

Kiistämättömyydellä tarkoitetaan tietojärjestelmän kykyä tunnistaa ja tallentaa järjestelmää käyttävän henkilön tiedot. Siihen pyritään pääasiassa kahden seikan takia. Ensimmäiseksi halutaan varmistaa tiedon alkuperä. Toiseksi halutaan tunnistaa olemassa olevien tietojen luvaton käyttö tilanteissa, joissa

tietojärjestelmien omistaja joutuu mahdollisesti käyttämään oikeudellisia toimia järjestelmän käyttäjää vastaan. Pääsynvalvonnalla sen sijan tarkoitetaan niitä menetelmiä, joilla rajoitetaan varsinaisiin tietoihin pääsyä ulkopuolisilta henkilöiltä. Tämä kuuluu omalta osaltaan myös luottamuksellisuuden ylläpitoon. (Mts. 5.)

Tietoturvallisuus jaetaan usein pienempiin osiin, jotta sitä on helpompi käsitellä. Tavallisin tapa on erotella seuraavat osa-alueet: hallinnollinen turvallisuus, fyysinen turvallisuus, henkilöturvallisuus, tietoaineistoturvallisuus, ohjelmistoturvallisuus, laitteistoturvallisuus ja tietoliikenneturvallisuus. Hallinnollisella turvallisuudella tarkoitetaan tietoturvan kehittämistä ja johtamista. Tärkeässä asemassa ovat esimerkiksi lainsäädännön ja palvelusopimusten vaikutusten arviointi yrityksen tietoturvakäytäntöihin. Fyysinen turvallisuus puolestaan tarkoittaa tilojen ja niissä sijaitsevien laitteiden suojaamista erilaisilta fyysisiltä uhilta kuten murroilta tai vesivahingoilta. (Mts. 11.)

Henkilöturvallisuuteen liittyy ne toimet, joilla varmistetaan henkilöstön osaaminen käyttää tietojärjestelmiä sekä rajaus heidän mahdollisuuksistaan käyttää tietojärjestelmiä ja yrityksen tietoja. Tietoaineistoturvallisuus kattaa tietojen säilyttämisen, varmistamisen, palauttamisen ja tuhoamisen toimet. Myös ohjelmistoihin ja laitteisiin liittyvät seikat tulee ottaa huomioon. Sovellusten ja laitteiden tulee olla käyttötarkoitukseen sopivia sekä ajanmukaisia. Tietoliikenneturvallisuuteen kuuluu tiedonsiirtoratkaisujen ja viestintäjärjestelmien turvallisuuden. (Mts. 11–12.)

Tietoturvaa koskevat vaatimukset perustuvat henkilötietojen suojaamisen osalta henkilötietolakiin ja sähköisen viestinnän tietoturvan osalta sähköisen viestinnän tietosuojalakiin, sillä Suomessa ei ole erillistä tietoturvalakia (Salminen 2009, 81). Tietoyhteiskuntakaari on 1.1.2015 voimaan tullut laki, joka kumosi sähköisen viestinnän tietosuojalain (516/2004) sekä lain tietoyhteiskunnan palvelujen tarjoamisesta (458/2000). Lain tarkoituksena on edistää sähköisen viestinnän palveluiden tarjontaa ja käyttöä sekä varmistaa, että ne ovat turvallisia. (L 7.11.2014/917.) Lisäksi tavoitteena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköistä kaupankäyntiä Euroopan talousalueella (Tietoyhteiskuntakaarta sovelletaan internetin yhteisö- ja ajanvietepalveluihin 2015).

Henkilötietolaki säätää tietoturvallisuudesta ja tietojen säilytyksestä. Sen mukaan rekisterinpitäjän on toteutettava tarpeelliset toimenpiteet henkilötietojen suojaamiseksi asiattomien pääsyltä tietoihin. Velvoite koskee myös henkilötietojen hävittämistä, muuttamista, luovuttamista ja siirtämistä. Toimenpiteiden toteuttamisessa tulee ottaa huomioon käytettävissä olevat tekniset mahdollisuudet, kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta. (L 22.4.1999/523.)

Rekisterinpitäjältä siis odotetaan tietoturvan varmistamista kohtuullisin uhrauksin. Suojauksen tason tulee kuitenkin olla riittävä myös mahdollisissa poikkeusolosuhteissa. Näin ollen rekisterinpitäjän vastuulle jää käytännön riskien ja tarpeellisten toimenpiteiden arviointi. Rekisterinpitäjällä on myös velvollisuus näyttää, että toiminnassa on noudatettu riittävää huolellisuutta ja että tietojen suojaamisen varmistamiseksi on tehty riittävät toimenpiteet. (Salminen 2009, 82.)

Henkilötietojen käsittelijää koskee vaitiolovelvollisuus, eli hän ei saa luovuttaa saamiaan tietoja sivullisille (L 22.4.1999/523). Vaitiolovelvollisuus koskee kaikkia henkilötietojen käsittelijöitä ilman erillisiä salassapito- tai vaitiolosopimuksia. Salassapito- ja vaitiolovelvollisuutta voidaan kuitenkin laajentaa erillisillä sopimuksilla ja joillakin toimialoilla voi olla lisäksi erityislainsäädännöstä johtuvia salassapito- ja vaitiolovelvoitteita. (Salminen 2009, 83.) Asianajajien toimintaa koskee laki asianajajista, jonka 5 c § säädetään salassapitovelvollisuudesta (L 12.12.1958/496).

Lain mukaan asianajaja tai hänen apulaisensa ei saa luovuttaa sellaista yksityisen henkilön tai perheen salaisuutta eikä liike- tai ammattisalaisuutta, josta hän on saanut tiedon tehtävää hoitaessaan (L 12.12.1958/496). Lisäksi asianajajan tulee noudattaa hyvää asianajajatapaa. Sen kohdassa 3.4 säädetään asianajajan vaitiolovelvollisuudesta. Asianajaja ei saa luvattomasti kertoa muita tietoja, joita hän on saanut tietää asiakkaasta ja hänen oloista tehtävää hoitaessaan. Asianajajan salassapito- ja vaitiolovelvollisuus on ajallisesti rajoittamatonta ja ne koskevat kaikkia samassa asianajotoimistossa työskenteleviä. (Hyvää asianajajatapaa koskevat ohjeet 2012, 3–4, 14.)

Tietoturva on osa organisaatioiden päivittäistä toimintaa ja se tulee hoitaa asianmukaisesti. Tavoitteena on estää tietojen ja tietojärjestelmien oikeudeton käyttö, tietojen tuhoutuminen tai vääristyminen tahattomasti tai tahallisesti ja minimoida mahdolliset aiheutuvat vahingot. Tietoturvan huomioiminen on erityisen tärkeää silloin kun ulkoistetaan tietojenkäsittelyä ja tietotekniikan ylläpitoa, otetaan käyttöön uusia toimintamalleja tai kun tehdään uusia hankintoja ja määritellään niihin liittyviä vaatimuksia. (Andreasson & Koivisto 2013, 29.)

Andreasson ja Koivisto (2013, 26) ovat määritelleet pilvipalveluiden keskeisiä kysymyksiä tietoturvan kannalta. Huolta tietoturvallisuudesta aiheuttaa palveluiden ja niissä olevan tiedon siirtyminen yrityksen verkon ja hallinnan ulkopuolelle. Keskeistä on selvittää, missä tiedot konkreettisesti sijaitsevat ja kuinka tiedot suojataan. Olennaista on myös se, kuka pääsee käsittelemään tietoja ja kuinka käyttöä valvotaan. Edellä mainittujen asioiden takia palvelusopimuksen sisältöön ja sen tietoturva-asioiden riittävään huomioonottamiseen tulee kiinnittää huomiota. Tietoturvan on vastattava asiakkaan vaatimuksia, ja esimerkiksi palveluntarjoajan ”standardisopimus” ei välttämättä riitä. Ennen pilvipalveluihin siirtymistä kannattaa ottaa huomioon myös käytännön mahdollisuudet siirtyä pois palvelusta tai vaihtaa palveluntarjoajaa. (Mts.)

5 Tutkimuksen toteutus ja tutkimustulokset

Tässä luvussa kuvataan tutkimuksen toteutus ja esitellään tärkeimmät haastatteluista saadut tulokset. Tutkimustulokset on jaettu kahteen eri osaan, joista toisessa keskitytään tietosuojan ja tietoturvan säilymiseen pilvipalveluissa, ja toinen käsittelee asianajajaliiton säädöksiä.

5.1 Tutkimuksen toteutus

Tutkimusaineisto kerättiin tekemällä teemahaastatteluita. Haastattelut toteutettiin lokakuussa 2016 ja niitä tehtiin yhteensä viisi. Haastateltavina oli neljä Jyväskylän alueella toimivaa asianajotoimistoa, ja haastatteluita kertyi yhteensä viisi, sillä yhdestä toimistosta haastateltiin sekä asianajajaa että asianajoassis-

tenttia. Muista toimistoista haastateltiin asianajoassistentteja. Assistentit valikoituivat haastateltaviksi, sillä näissä toimistoissa assistentti selvittää kyseisiä asioita ja esittelee ne juristeille. Haastatteluista sovittiin etukäteen puhelimitse tai sähköpostitse, jolloin haastateltaville esiteltiin opinnäytetyön aihe ja sovittiin haastatteluaika.

Haastateltavat toimistot valittiin sen perusteella, että tutkimukseen saataisiin mahdollisimman monenlaisia näkökulmia aiheesta. Toimistot edustivat eri kokoluokkia: pienimmässä toimistossa työskentelee yksi juristi ja yksi assistentti ja suurimmassa neljä juristia ja yksi assistentti. Muut toimistot ovat kooltaan jotain tältä väliltä. Toimistot erosivat myös pilvipalveluiden käytön suhteen. Kahdella toimistolla ei ollut käytössään minkäänlaisia pilvipalvelupohjaisia ratkaisuja, yksi toimisto oli kokonaan siirtynyt pilvipalveluihin ja yhdellä toimistolla oli sähköposti pilvipalvelupohjaisella ratkaisulla sekä aikomus ottaa pilvipalvelut käyttöön lähitulevaisuudessa.

Haastattelut toteutettiin yksilöhaastatteluina sillä erotuksella, että yhden toimiston haastattelussa asianajaja ja asianajoassistentti olivat hetken yhtä aikaa haastateltavina. Tätä ennen oli haastateltu asianajajaa ja sen jälkeen jatkettiin vielä assistentin kanssa yksilöhaastattelua. Kaikki haastattelut nauhoitettiin litteroinnin ja analysoinnin helpottamiseksi. Nauhoittamiseen kysyttiin haastateltavien lupa ennen jokaisen haastattelun alkua.

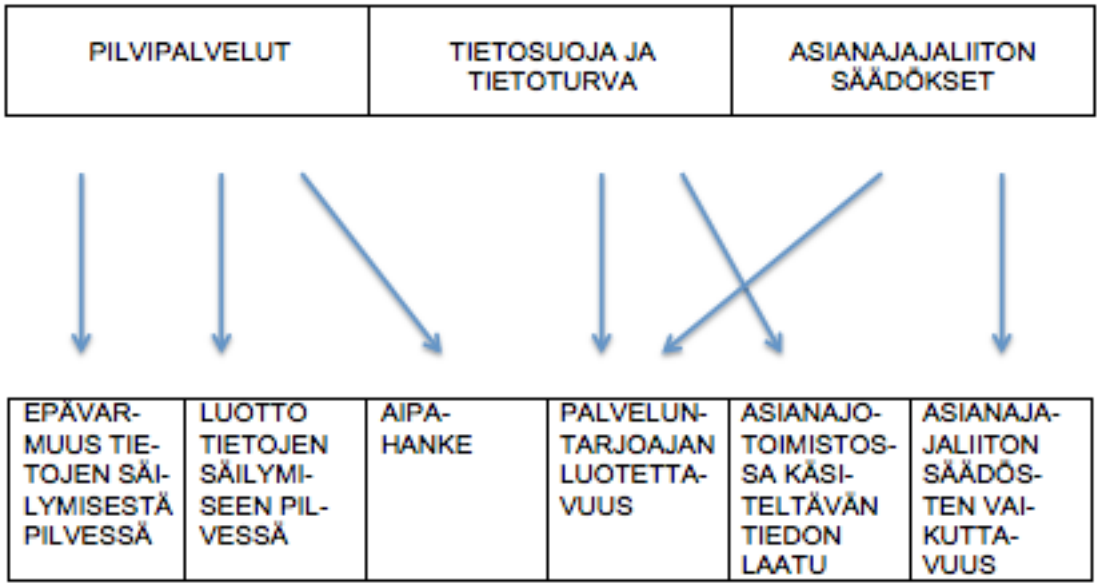
Teemahaastatteluita varten laadittiin teemahaastattelurunko (ks. liite 1), joka sisälsi **kolme teemaa**: pilvipalvelut, tietosuoja ja tietoturva sekä asianajajaliiton säädökset. Teemat valittiin sen perusteella, että haastattelun vastauksista saataisiin vastaukset tutkimuskysymyksiin ja sitä kautta tutkimusongelmaan. Teemojen alle oli listattu tarkentavia alakysymyksiä helpottamaan teemojen käsittelyä. Tarkentavat alakysymykset olivat asioita, jotka teoriasta nousivat olennaisina asioina liittyen kyseisiin teemoihin.

Haastattelurunkoa ei annettu haastateltaville, vaan heille kerrottiin haastatteluiden etenevän kolmen teeman mukaan. Haastattelusta riippuen teemojen käsittelyjärjestys saattoi vaihdella hieman. Haastatteluista merkattiin ylös haastateltavan nimi ja asema, toimisto ja toimiston koko sekä haastattelun

kesto. Kesto vaihteli 25 ja 30 minuutin välillä. Haastatteluiden jälkeen aineisto litteroitiin ja analysoitiin teemoittelun avulla.

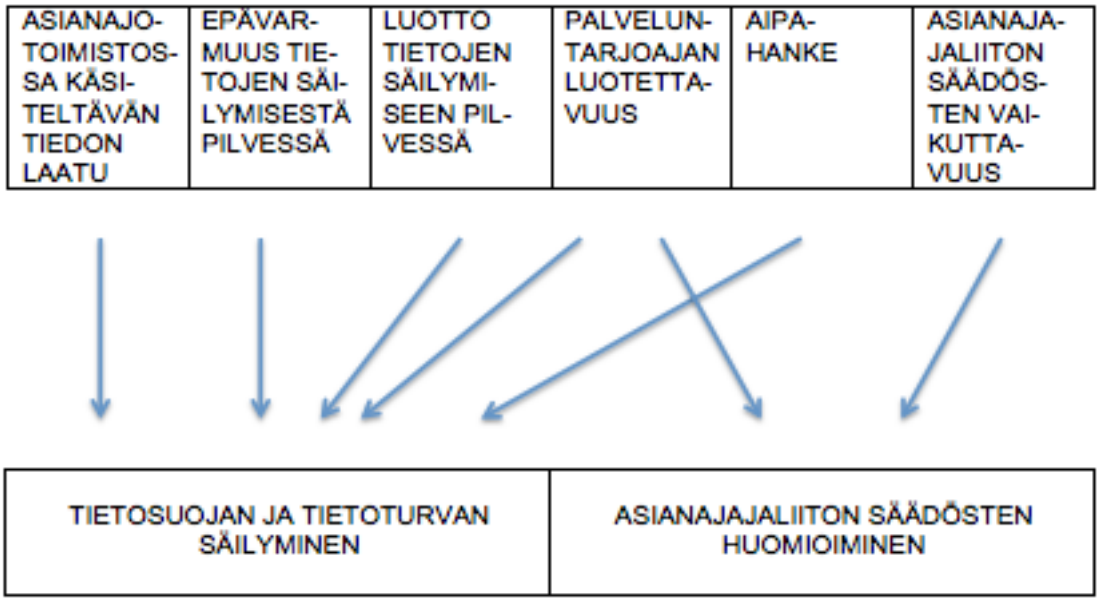
Pilvipalvelut-teemassa käsiteltiin haastateltavien suhtautumista pilvipalveluihin ja kartoitettiin, onko käytössä pilvipalvelupohjaisia ratkaisuja. Osiossa käytiin läpi asianajotoimistossa käsiteltäviä asiakirjoja ja mitä niiden käsittelyssä tulee ottaa huomioon, sillä nämä olisivat niitä dokumentteja, joita pilvipalveluihin siirrettäisiin. Lisäksi käsiteltiin AIPAn vaikutusta asianajotoimistoihin. Tietosuojaa ja tietoturvaa käsittelevässä teemassa käytiin ensin läpi yleisesti asianajotoimiston tietosuojaan ja tietoturvaan liittyviä asioita sekä sitä, miten tietosuojasta ja tietoturvasta tällä hetkellä toimistoissa huolehditaan. Tällä pohjustettiin haastateltavien käsitystä tietosuojasta ja tietoturvasta pilvipalveluissa. Viimeisessä teemassa, eli asianajajaliiton säädöksissä, käsiteltiin ensin yleisesti säädösten noudattamista, jonka jälkeen käytiin läpi it-palveluiden ulkoistamista koskevia säädöksiä, ja niiden vaikutusta pilvipalveluiden käyttöönottoon.

Litteroitua haastatteluaineistoa tutkittaessa aineistosta nousi esille **kuusi pääteemaa**. Teemoja olivat asianajotoimistoissa käsiteltävän tiedon laatu, AIPA-hanke, epävarmuus tietojen säilymisestä pilvessä, luotto tietojen säilymisestä pilvessä, pilvipalveluntarjoajan luotettavuus ja asianajajaliiton säädösten vaikuttavuus. Alla on havainnollistettu (kuvio 3), miten haastattelun kolmesta pääteemasta syntyi kuusi teemaa.



Kuvio 3. Litteroinnin teemat

Tämän jälkeen näiden kuuden teeman alle kirjattiin haastatteluista ilmenneitä tekijöitä kuhunkin teemaan liittyen. Teemoissa esiintyvistä tekijöistä huomattiin yhtäläisyyksiä, jotka koottiin **kahden pääteeman** alle tutkimusongelman tutkimuskysymyksiä mukaillen. Kuviossa 4 on kuvattu litteroinnin teemojen kohdistuminen kahteen pääteemaan.



Kuvio 4. Pääteemat tutkimuskysymyksiä mukaillen

Tutkimustulokset esitetään näiden kahden pääteeman mukaan. Ensimmäisessä luvussa käsitellään tekijöitä, jotka edesauttavat tietosuojan ja tietoturvan säilymistä pilvipalveluissa. Toisessa luvussa käsitellään asianajajaliiton säädösten huomioimista pilvipalveluiden käyttöönotossa.

5.2 Tietosuojan ja tietoturvan säilyminen

Asianajotoimistoissa käsiteltävät asiakirjat sisältävät arkaluontoista tietoa, jonka takia tietosuojan ja tietoturvan säilyminen on olennaisen tärkeää, oli sitten pilvipalveluita käytössä tai ei. Kaikki asiakkailta saatava tieto on salassa pidettävää ja luottamuksellista, ja lisäksi asianajotoimistoilla on lain nojalla salassapitovelvollisuus. Toimistoissa käsitellään ihmisten henkilökohtaisia tietoja, eli esimerkiksi henkilötunnuksia ja tulotietoja. Näitä arkaluontoisia tietoja sisältävät asiakirjat ovat juuri niitä dokumentteja, joita pilvipalveluissa säilytettäisiin.

> *--tiedothan ei saa vuotaa minnekään. Niin että 7 päivää -lehden lööppeihin ei varsinaisesti ole suotavaa päätyä. (Haastateltava 3.)*

Tietojen luonteen vuoksi osassa toimistoissa suhtauduttiin pilvipalveluiden käyttöönottoon hieman skeptisesti. Haastatteluista nousi esille suurimpina epävarmuustekijöinä samat asiat, kuin mitä Andreasson ja Koivistokin (2013, 18) ovat todenneet: ovatko pilveen laitettavat tiedot tallessa ja turvassa siellä, pääseekö joku muu niihin käsiksi ja missä tiedot oikeasti sijaitsevat. Ajatus siitä, että tiedot eivät ole omassa hallinnassa aiheutti epävarmuutta tietosuojan ja tietoturvan säilymiseen.

> *Ihan semmonenkin, että mitä jos tää ylläpitäjä menee vaikka konkurssiin, kenen ne loppujen lopuksi on ne asiakirjat, mitä jos käykin niin, että ne sanoo että tää kaikki on pesän omaisuutta. (Haastateltava 1.)*

Useammassa haastattelussa nousi esille palveluntarjoajan konkurssitilanne. Tämän takia luotettavan palveluntarjoajan löytäminen on keskeisessä roolissa tietosuojan ja tietoturvan säilymisen kannalta. Luotettavuus on usean tekijän summa, ja keskeisimpinä asioina nousivat esille se, että yritys olisi kotimainen ja että jollain muullakin olisi siitä tietoa tai kokemusta. Toisten toimistojen positiivisesti kokemukset palveluntarjoajasta lisäävät kyseisen palveluntarjoajan luotettavuutta. Muutamasta haastattelusta nousi esille myös mahdollisuus saada palveluntarjoajalta nopeasti apua ongelmatilanteissa. Palveluntarjoajan ollessa kotimainen voi ongelmista keskustella omalla kielellä.

Kotimaisuuden ja muiden toimistojen kokemusten lisäksi haastateltaville oli tärkeää, että myös konesali sijaitsisi Suomessa. Näin voitaisiin varmistaa, että tietojen säilyttämisessä ei tulisi lainsäädännöllisiä ongelmia, sillä sovellettava laki määräytyy palvelimen sijaintimaan mukaan. Esimerkiksi ylempänä mainitussa konkurssitilanteessa olisivat tiedot Suomen lainsäädännön piirissä, ja palvelimelta vielä saatavissa.

Palvelutarjoajaa valittaessa hyvä taustatyö on olennaista, jotta voidaan välttyä mahdollisilta riskitilanteilta. Luottotietojen tarkistuksella voidaan varmistaa, että yritys on elinkykyinen, jolloin konkurssitilanteen syntyminen on epätodennäköistä. Jos kyseisen yrityksen kanssa ei ole tehty aiemmin yhteistyötä, on hyvä tarkistaa mitä, palveluita yritys ylipäätänsäkin tarjoaa. Tämän lisäksi tulisi selvittää tarkasti, minkälainen palvelu, jonka hankkimista suunnitellaan, on

kyseessä. Luotettavuutta lisää se, että palveluntarjoajan kanssa tehdään tarkka sopimus, jossa sovitaan esimerkiksi salassapidosta.

Palveluntarjoajan oma tietoturvaopas ja tietoturvavarmistukset lisäävät luottoa tietosuojan ja tietoturvan säilymiseen. Laitesalien kulunvalvontajärjestelmillä voidaan kontrolloida, kuka siellä käy ja ettei kuka tahansa pääse palvelimiin käsiksi. Myös palveluntarjoajan oma perehtyneisyys asianajajaliiton tietoturvasäädöksiin lisää luotettavuutta. Jos palveluntarjoaja pystyy markkinoimaan tarjoamaansa pilvipalvelua sellaisena, jonka asianajajaliitto hyväksyy, on toimistojen helpompi pitää kyseistä palveluntarjoajaa luotettavana.

Toimistossa, jossa pilvipalvelu oli käytössä, ei ollut tullut vielä vastaan tietoa, josta olisi pitänyt miettiä sopiiko se pilveen laitettavaksi. Muut haastateltavat olivat samoilla linjoilla. Jos tehtäisiin ratkaisu, että pilvipalvelua käytetään, olisi vaikea alkaa luokittelemaan, mikä tieto olisi sellaista, ettei sitä voisi laittaa pilveen.

> *Ylipäätään jos sinne pannaan mitään niin kyllä se sitten ois myös arkaluontoisia kaiken tasoisia, et me vaan varmistettais se sitten et se ois semmonen paikka et se soveltuis meille. Koska sitten tavallaan hirveen vaikee on kategorisoida, että mikä on sitten vähemmän arkaluontosta ja mikä enemmän, kun ne on kaikki. (Haastateltava 4.)*

Pilvipalveluiden tietosuojaan ja tietoturvaan voi myös omalta osaltaan vaikuttaa palveluntarjoajan valitsemisen jälkeen. Kun tietokoneen avaamiseen tarvitsee yhden salasanan ja pilvipalveluihin kirjautumiseen toisen, voi salasanojen avulla rajata käyttäjät, jotka pääsevät palvelimelle. Näin voidaan omalla toiminnalla varmistaa, että tietoihin pääsee vain ne henkilöt, joille ne kuuluvat. Samoin palvelun etäkäytössä esimerkiksi puhelimella, on tärkeää suojata myös puhelin salasanalla tai sormenjälkitunnistuksella.

Edellä on kuvattu tärkeimmät tutkimustulokset liittyen tekijöihin, jotka parantavat tietosuojaa ja tietoturvaa pilvipalveluissa. Toisaalta haastatteluista tuli myös esille näkökulma siitä, miksi pilvipalvelut olisivat turvallisempia kuin omalla koneella tai palvelimella pidettävä tieto. Jos oma kone tai palvelin rikkoutuu, monia tärkeitä tietoja saattaa kadota. Tietojen ollessa pilvessä oman koneen hajoaminen ei vaikuta tietojen säilymiseen, sillä ne saadaan käyttöön

palvelimelta. Pilvipalveluissa on omat riskinsä, mutta on olemassa myös riski, että toimistoihin murtaudutaan tai postilaatikosta viedään postia.

> *Mä henkilökohtaisesti oon sitä mieltä, että tekniikka kehittyy ja maailma menee eteenpäin, ja jos me emme mihinkään voi luottaa niin mitä tää on. (Haastateltava 3.)*

Haastatteluista selvisi, että asianajotoimistojen tietoisuus AIPA-hankkeesta on vielä melko vähäistä. Asianajajaliittokin oli vasta hiljattain ”herännyt” siihen, että AIPA-hanke on jo melko pitkällä, minkä takia joka osastosta oli valittu yksi AIPA-vastaava. Jatkossa myös asianajajaliitto menee mukaan esimerkiksi hankkeesta järjestettäviin koulutuksiin, jotta asianajajatkin pystyvät vaikuttamaan siihen, että järjestelmä toimii myös toimistojen ja tuomioistuimien välillä. Tämän myötä saadaan enemmän tietoa asianajotoimistoilta ”vaadittavista” toimenpiteistä kyseiseen hankkeeseen liittyen, jonka myötä toimistojen tietoisuus aiheesta tulee varmasti lisääntymään lähitulevaisuudessa

Toimistoissa ei vielä tässä vaiheessa osattu konkreettisesti sanoa, miten AIPA tulee vaikuttamaan asianajotoimistojen arkeen ja dokumenttien hallintaan. Epäilyksenä kuitenkin oli, että järjestelmän tultua täysin käyttöön, tulee se varmasti jollain tapaa vaikuttamaan. Dokumentoinnin siirtyessä sähköiseksi toimistojen tulee miettiä omaa asiakirjojen käsittelyä, vaikka ketään ei tietenkään voi pakottaa ottamaan käyttöön tiettyä järjestelmää. Ajankohtaista tulee kuitenkin jossain vaiheessa olemaan, tulisiko asiakirjojen käsittelyn siirtyä sähköiseksi esimerkiksi pilvipalveluita käyttämällä, koska toimistojen omille palvelimille ei mahdu loputtomasti dataa.

5.3 Asianajajaliiton säädösten huomioiminen

Asianajajaliiton säädöksissä ja ohjeissa on määritelty tietoturvavaatimukset asianajotoimistoille. Säädöksistä löytyy myös erikseen kohta it-palveluiden ulkoistamiselle ja pilvipalveluiden käytölle. Pääasiassa pilvipalveluiden tietoturvavaatimukset eivät poikkea muunlaiselle ulkoistamiselle asetetuista vaatimuksista. Säädöksiä velvoitetaan noudattamaan, mutta ne jättävät toimistoille jonkun verran tulkinnan varaa. Säädöksiä on vähän siellä täällä, eikä esimerkiksi palvelimen sijaintimaasta ole listaa, joissa palvelin saisi olla tai ei. Haas-

tatteluista kuitenkin ilmeni, että Yhdysvalloissa sijaitsevalle palvelimelle ei saa tallentaa tietoa. Tämän oli eräs pilvipalveluiden tarjoaja selvittänyt asianajajaliitolta.

Säädöksissä ja ohjeissa ei ole erikseen tarkkoja ohjeita eri tilanteiden varalle. Jos miettii jotain yksittäistä asiaa it-palveluiden ulkoistamiseen liittyen, liitolta voi varmistaa, onko heillä tarkentavaa ohjetta. Esimerkiksi toimistossa, jossa sähköposti on pilvipalvelimella, oli ennen käyttöönottoa mietitty, voivatko he ottaa kyseisen palvelun käyttöön. He olivat kysyneet liitolta tarkentavaa ohjeistusta ja vastauksena oli, että he eivät yksittäisen toimiston kanssa selvitä jokaista yksityiskohtaa. Tämä jättää toimistojen harkintaan, miten kyseisessä tilanteessa olisi kannattavaa ja järkevää toimia.

> *Niin kyllähän me katotaan, että onko täällä määrätty jotakin tiettyä. Että sitten jos ei oo, niin sittenhän me keskenämme vähän katotaan mikä se on, ja sitten noilla monesti onkin vähän sitä kokemusta tai tietoa, että miten jossakin toimistossa tehään tai on tehty, että sitten vähän sen mukaan mietitään näitä asioita. (Haastateltava 5.)*

Ohjeet kuitenkin vaikuttavat päätöksentekoon asianajotoimistossa, sillä ohjeita ja säädöksiä on noudatettava, vaikka ne ovatkin melko ympäripyöreitä. Uusia it-ratkaisuja mietittäessä toimistoissa katsotaan, mitä säädöksissä on määrätty ja toimitaan niiden ohjeiden mukaan. Avoimet kohdat jäävät jokaisen toimiston itse mietittäväksi. Varsinkin pilvipalveluiden osalta ohjeet ovat yleiset ja suuntaa-antavat. Tämän arveltiin johtuvat suurimmaksi osaksi siitä, että pilvipalvelut ovat vielä melko vierasta aluetta, minkä takia niiden käyttöön on yleisluontoiset ohjeet.

Säädöksissä on kuitenkin muutamia tarkempia ohjeita. Niissä esimerkiksi edellytetään tekemään palveluntarjoajan kanssa salassapitosopimus. Eräästä haastattelusta selvisi, että asianajajaliitto tekee kerran vuodessa toimistotarkastuksia ja Keski-Suomen osastossa se tarkoittaa kahta toimistoa vuosittain. Tarkastettavat toimistot arvotaan ja kyseessä olevan toimiston tulee esimerkiksi esitellä salassapitosopimus ja sen sisältö, jos it-palvelut on ulkoistettu. Kaikki haastateltavat pitivät itsestään selvänä, että palveluntarjoajan kanssa tehtäisiin salassapitosopimus ilman liiton säädöksiäkin. Tietosuojan ja tietotur-

van säilyminen on luonnollisestikin toimistoille tärkeää, ja salassapitosopimus edesauttaa niiden säilymistä.

Kuten luvussa 5.2 tuli ilmi, pitivät toimistot tärkeänä selvittää palveluntarjoajan taustat ja mahdollisesti muiden toimistojen kokemukset kyseisestä palveluntarjoajasta. Lisäksi palvelimen sijaintimaa nousi tärkeään rooliin palveluntarjoajaa valitessa. Edellä mainitut tekijät, eli palveluntarjoajan taustojen ja teknisen tietoturvan taso sekä palvelimen sijaintimaa, kuuluvat asianajajaliiton säädöksiin, joissa kehotetaan tarkistamaan kyseiset asiat. Ennen kuin suurimmassa osassa haastatteluista päästiin tähän kohtaan, oli jo käynyt selväksi, että nämä asiat tarkistettaisiin ilman liiton säädöksiäkin.

Toimistoilta edellytetään säännöllistä varmuuskopiointia tiedostoista, riippumatta onko tiedot pilvessä vai eivät. Varmuuskopioinnista sovitaan palveluntarjoajan kanssa tehtävässä sopimuksessa. Esille tuli myös tietojen palautettavuus ja käytettävyys, jotka varmistettaisiin palveluntarjoajan kanssa käytävien neuvotteluiden yhteydessä. Toimistoilla ei ollut käytössä internetistä helposti käyttöönotettavia ilmaisia pilvipalveluja, koska kaikille toimistoille oli tärkeää, että palveluntarjoaja ei ole netissä käyttöönotettava palvelu. Niiden tietoturvataso ei riitä arkaluontoisten tietojen säilyttämiseen, eikä niitä koettu tarpeelliseksi muistiinpanojen tekemisellekään.

Esimerkkinä asianajajaliiton säädösten vaikuttavuudesta tuli esille salatun sähköpostiviestin käyttö. Mielipiteet koskien salattua sähköpostiviestiä vaihtelivat. Yksi toimisto oli ottanut sen hiljattain käyttöön, ja toinen toimisto mietti sen käyttöönottoa. Muut haastateltavat eivät kokeneet sitä tarpeelliseksi, ja yhtenä perusteluna oli, ettei asianajajaliittokaan sitä velvoita käyttämään. Jos sellainen kohta tulisi liiton säädöksiin, olisi selvää, että salattu sähköposti otettaisiin toimistoissa käyttöön.

6 Johtopäätökset

Opinnäytetyön tarkoituksena oli tutkia tietosuojan ja tietoturvan säilymistä sekä asianajajaliiton säädösten vaikuttavuutta pilvipalveluiden käyttöönotossa.

Tutkimusongelmana oli Miten tietosuoja ja tietoturva sekä asianajajaliiton säädökset huomioidaan asianajotoimistojen siirtyessä pilvipalveluiden käyttöön? Siitä johdettuja tutkimuskysymyksiä olivat

- Miten voidaan varmistaa tietosuojan ja tietoturvan säilyminen asianajotoimistoissa olevien tietojen siirtyessä pilveen?
- Millä tavalla asianajajaliiton säädökset vaikuttavat pilvipalveluiden käyttöönottoon?

Luvuissa 5.2 ja 5.3 esitetyistä tutkimustuloksista voidaan tehdä johtopäätöksiä sekä tietosuojan ja tietoturvan säilymisestä että asianajajaliiton säädösten huomioimisesta. Tässä luvussa esitetään johtopäätökset tutkimuskysymysten kannalta käytännön kuvauksena. Tämän lisäksi esitetään tutkimuksen konkreettinen hyöty toimeksiantajalle.

Tietosuojan ja tietoturvan säilyminen pilvessä

Haastatteluita tehtäessä ilmeni, että pilvipalvelut eivät ole vielä laajasti käytössä Jyväskylän alueen asianajotoimistoilla. Haastateltavista vain yksi toimisto oli kokonaan siirtynyt käyttämään pilvipalveluita. Myös haastateltavat olivat sitä mieltä, että pilvipalveluiden käytöstä on ollut puhetta jo jonkun aikaa, mutta harva on vielä oikeasti ottanut tai on suunnitellut ottavansa niitä käyttöön. Asianajoala on toimialana hieman vanhahtava ja asiat on totuttu tekemään tietyllä tavalla. Tämän takia muutokset voivat tuntua jollain tapaa hankalilta ja näin ollen turhilta.

Toisena syynä on nimenomaan epävarmuus pilvipalveluiden tietosuojasta ja tietoturvasta. Tätä tulosta tukee hyvin luvussa 4 mainittu Tilastokeskuksen tutkimus tietotekniikan käytöstä yrityksissä, josta käy ilmi, että juuri nämä seikat ovat usein esteenä pilvipalveluiden käytölle (Tietotekniikan käyttö yrityksissä 2014, 2). Haastatteluissa korostui toimistoissa liikkuvan tiedon olevan salassa pidettävää, minkä takia sitä käsiteltäessä ja arkistoidessa tulee noudattaa erityistä huolellisuutta. Jos pilvipalveluiden turvallisuuteen ei luoteta, ei sinne myöskään haluta siirtää minkäänlaista tietoa.

Haastatteluista saaduista vastauksista pystyttiin päättelemään, että käsitykset pilvipalveluista erosivat sen mukaan, onko niitä käytössä vai ei. Toimistossa,

jossa oli otettu pilvipalvelut käyttöön, oli käyttöönotto venynyt pitkään turvallisuuteen liittyvien epävarmuustekijöiden takia. Pilvipalveluihin oli suhtauduttu epäluuloisesti, ennen kuin assistentti oli tehnyt kattavan taustaselvityksen niihin liittyen. Perehtyneisyys aiheeseen lisää selkeästi luottoa tietosuojan ja tietoturvan säilymiseen pilvipalveluissa. Tätä tulkintaa vahvisti myös yhden haastateltavan toteamus siitä, että koska hän ei ole perehtynyt tarkemmin aiheeseen, hänen uhkakuvansa eivät välttämättä ole todellisia.

Toimistosta riippumatta luotettavan palveluntarjoajan valinta nousi tärkeimmäksi tekijäksi puhuttaessa tietosuojan ja tietoturvan säilymisestä pilvipalveluissa. Mutta millä tavalla sitten voidaan varmistua palveluntarjoajan luotettavuudesta? Tärkeänä tekijänä pidettiin sitä, että palveluntarjoajan tulee olla niin sanotusti ”todellinen”, eikä vain internetin välityksellä ostettu palvelu. Vaikka pilvipalveluiden luonteeseen kuuluu, että ne saa käyttöön ilman yhteyttä palveluntarjoajaan (Mell & Grance 2011, 2), on helpompi luottaa toimijaan, jonka kanssa voi konkreettisesti käydä neuvotteluita. Näin ollen palvelun ostaja saa kattavammin tietoa ostettavasta palvelusta ja pystyy vaikuttamaan palveluntarjoajan kanssa tehtävän sopimuksen sisältöön. Lisäksi mahdollisen ongelmatilanteen tullessa eteen, palveluntarjoajalta saa yksityiskohtaisempaa apua tilanteen ratkaisemiseen.

Palveluntarjoajan kotimaisuus ja pilvipalvelimen sijaitseminen Suomessa nousivat esille lähes jokaisesta haastattelusta. Suomalaisen palveluntarjoajan kanssa on helpompi käydä neuvotteluita esimerkiksi sopimusta tehtäessä. Neuvottelu sopimuksen sisällöstä on tärkeää, jotta pilvipalvelu on varmasti asianajotoimiston käyttöön soveltuva. Tämän takia palveluntarjoajan kanssa kannattaa käydä kunnolla läpi, miten he varmistavat tietosuojan ja tietoturvan säilymisen. Esimerkiksi konesalin kulunvalvonta ja kontrollointi estävät ulkopuolisten pääsyn konesaliin.

Kun palveluntarjoajan tietosuoja- ja tietoturvavarmistukset ovat konkreettisesti selvillä, tietojen suojaukseen on helpompi luottaa. Lisäksi palveluntarjoajan kanssa tehtävä salassapitosopimus on ehdoton, jotta voidaan varmistaa tietojen olevan vain niiden käytössä, joille ne kuuluvat. Vielä asteen paremman ja luotettavamman palveluntarjoajasta tekee se, jos he ovat ottaneet itse selvää, että heidän palvelunsa ovat soveltuvia asianajotoimiston käyttöön.

Konesalin sijaitessa Suomessa voidaan välttyä monilta lainsäädännöllisiltä ongelmilta. Pilvipalveluiden ominaispiirteenä on, että asiakas ei välttämättä saa tai tarvitse tietoa palvelimen konkreettisesta sijainnista (Mell & Grance 2011, 2). Tarkkaa sijaintia ei ole välttämätöntä tietää, mutta sijaintimaan tietäminen on olennaista siirrettäessä arkaluontoisia henkilötietoja. Vaikka lakien mukaan konesali voisi sijaita esimerkiksi Euroopassa, pidettiin sen sijaitsemista Suomessa silti tärkeänä. Tämä minimoi ongelmat lainsäädännön kannalta, sillä konesalin sijaitessa Suomessa, on selvää, että tietojen säilytykseen sovelletaan Suomen lakia.

Näiden lisäksi muiden toimistojen kokemuksia kyseisestä palveluntarjoajasta pidettiin tärkeänä. Kollegojen kanssa käyty keskustelu on avainasemassa, jotta saadaan esimerkiksi käyttäjäkokemuksia kyseisestä yrityksestä. Ihanteellisin tilanne olisi, jos palveluntarjoajan kanssa olisi aikaisemmin tehnyt yhteistyötä, tai jos jollain toisella toimistolla olisi positiivisia kokemuksia palveluntarjoajasta. Näin ollen voitaisiin ainakin varmistua siitä, että kyseiset pilvipalvelut sopivat asianajotoimiston käyttöön. Aina tällainen tilanne ei kuitenkaan ole mahdollinen, jolloin keskiöön nousee tarkka selvitys palveluntarjoajan taustoista. Kannattaa esimerkiksi ottaa selvää, minkälaisia palveluita palveluntarjoaja yleisesti ottaen tarjoaa ja selvittää palveluntarjoajan vakavaraisuus.

Palveluntarjoajan valinta on asia, johon voi itse vaikuttaa. Neuvotteluista ja asianmukaisista sopimuksista eteenpäin palvelun ostajan ei auta muuta kuin luottaa, että palveluntarjoaja hoitaa tietosuojan ja tietoturvan lupaamallansa tavalla. Itse voi kuitenkin vaikuttaa ja tuleekin vaikuttaa myös siihen, että suojaa koneet asianmukaisilla salasanoilla. Tämä koskee niin ikään matkapuhelinta ja pilvipalvelimelle pääsyä. Näillä keinoilla pilvipalvelun käyttäjä pystyy rajaamaan palvelimelle pääsyn vain niille henkilöille, joille tiedot kuuluvat, ja näin ollen vaikuttamaan siihen, ettei tietosuoja ja tietoturva vaarannu käyttäjästä riippuvista tekijöistä.

Asianajajaliiton säädösten vaikutus pilvipalveluiden käyttöönottoon

Vaikka toimistojen käsitykset koskien pilvipalveluiden tietosuojaa ja tietoturvaa erosivat, asianajajaliiton säädösten kannalta toimistojen mielipiteet olivat yhtenäiset. Kaikista vastauksista oli havaittavissa, että niiltä osin, kun säädök-

sissä ja ohjeissa on määrätty jotain tarkkaa, niitä noudatetaan. Palveluntarjoajan valinnan osalta säädökset vaikuttavat pilvipalveluiden käyttöönottoon seuraavalla tavalla:

- palveluntarjoajan kanssa tehdään salassapitosopimus
- palveluntarjoajan taustat selvitetään
- palvelusopimuksessa määritellään varmuuskopioinnista
- arkaluontoisten tietojen säilyttämiseen ei käytetä internetistä käyttöön otettavia ilmaisia palveluita.

Pääosin säädökset ja ohjeet ovat siis suuntaa-antavat ja ohjailevat, jolloin ne jättävät toimistoille myös tulkinnan varaa. Säädökset kehottavat yleiseen huolellisuuteen ja varovaisuuteen pilvipalveluiden käytössä. Niiltä osin, kun jotain tarkkaa ei määrätä, toimistojen harkintaan jää, mitä kussakin tilanteessa kannattaa tehdä. Toimistoilla voi esimerkiksi olla tiedossa jokin hyväksi havaittu toimintatapa, jota muut toimistot ovat käyttäneet, ja toimia sen mukaan.

Tarkasteltaessa tutkimustuloksia tutkimuskysymysten kannalta voidaan huomata, että asianajajaliiton säädökset sisältävät tekijöitä, jotka koettiin myös tietosuojan ja tietoturvan säilymisen kannalta olennaisiksi. Esimerkiksi juuri salassapitosopimuksen tekeminen ja palveluntarjoajan taustojen selvittäminen nousivat esille jokaisessa haastattelussa. Tämän osoittaa sen, että asianajajaliiton säädökset ja toimistojen mielikuvat tietosuojan ja tietoturvan säilymisestä pilvipalveluissa kohtaavat hyvin, minkä takia säädösten noudattamista ei koeta hankalana.

Hyöty toimeksiantajalle

Asianajajaliitto on tehnyt linjauksen, että yksityiskohtaisten ohjeiden tekeminen ei ole tarpeellista. Osasyy säädösten yleisluontoisuuteen on myös se, että pilvipalveluiden käyttö asianajotoimistoissa on vielä melko uusi asia, jonka takia ei ole vielä tullut ajankohtaiseksi tehdä tarkempia ohjeita. Toisaalta on vaikeaa tehdä tarkkaa listaa siitä, mitä saa ja mitä ei saa tehdä. Asianajajaliitto voisi tehdä asianajotoimistoja varten samankaltaisen oppaan pilvipalveluista,

kuin mitä luvussa 1 mainitun Uuden-Seelannin lakiyhdistyksen tekemä ohjeistus on.

Ohjeistus voisi lisätä asianajotoimistojen tietoisuutta pilvipalveluiden hyödyistä ja riskeistä sekä niiden käyttöönotossa huomioitavista asioista, mikä saattaisi edesauttaa luottamusta pilvipalveluiden tietosuojaan ja tietoturvaan. Lähitulevaisuudessa pilvipalveluiden käyttöönotto tulee varmasti kasvamaan myös suomalaisissa asianajotoimistoissa. Ohjeistuksen avulla asianajotoimistojen voisi olla helpompi siirtyä käyttämään pilvipalveluita.

Ohjeistuksissa voisi olla ensin yleistä tietoa pilvipalveluista sekä niiden hyödyistä ja riskeistä. Tämän jälkeen se voisi sisältää tarkastuslistan asianajotoimistoille helpottamaan pilvipalveluiden käyttöönottoa. Lista voisi olla esimerkiksi seuraavan lainen:

- Perehdy pilvipalveluiden hyötyihin ja riskeihin.
- Mieti, mihin tarkoitukseen pilvipalvelua käytettäisiin toimistossanne.
- Varmista, että palveluntarjoaja on luotettava ja asianajotoimiston käyttöön soveltuva. Esimerkiksi seuraavat tekijät lisäävät palveluntarjoajan luotettavuutta:
    - palveluntarjoaja on ”todellinen” toimija, eikä internetin välityksellä käyttöönotettava palvelu
    - palveluntarjoaja on kotimainen
    - pilvipalvelin sijaitsee Suomessa, jolloin ollaan Suomen lainsäädännön piirissä
    - palveluntarjoajalla on konkreettisesti esittää heidän tietosuoja- ja tietoturvavarmistukset
    - palveluntarjoajan kanssa tehdään salassapitosopimus, jotta voidaan varmistaa, etteivät tiedot vuoda minnekään
    - palveluntarjoaja tietää asianajajaliiton vaatimukset tietosuojalle ja tietoturvalle

    - muiden asianajotoimistojen positiiviset kokemukset kyseisestä palveluntarjoajasta
    - palveluntarjoajan taustojen selvitys
- Neuvottele mahdollisen palveluntarjoajan kanssa, jotta voit varmistua edellä mainituista tekijöistä.
- Pilvipalveluiden ollessa käytössä, suojaa koneet, matkapuhelimet ja pilvipalvelimelle pääsy asianmukaisilla salasanoilla.

Lista sisältäisi käytännön ohjeita esimerkiksi palveluntarjoajan valintaan. Se olisi nimenomaan tehty pilvipalveluiden käyttöönoton avuksi, eikä sellaiseksi, mitä olisi pakko yksityiskohtaisesti noudattaa. Lista auttaisi pilvipalveluiden käyttöönottoa suunnittelevia toimistoja oikeille jäljille. Ohjeistukseen voisi mahdollisesti myös yhdistää luettelon asianajajaliiton suosittelemista pilvipalveluntarjoajista, jotka ainakin täyttävät asianajajaliiton vaatimukset tietosuojalle ja tietoturvalle.

7 Pohdinta

Opinnäytetyön tavoitteena oli saada käytännön kuvaus tietosuojan, tietoturvan ja asianajajaliiton säädösten huomioimisesta pilvipalveluiden käyttöönotossa asianajotoimistoissa. Tutkimuksen voidaan todeta olleen onnistunut, sillä sen myötä saatiin kuvaus konkreettisista toimenpiteistä tietosuojan ja tietoturvan säilymiseksi pilvipalveluiden käyttöönotossa. Lisäksi asianajajaliiton säädösten ja ohjeiden huomioimisesta saatiin kuvaus asianajotoimistojen näkökulmasta. Näin ollen saatiin myös vastaukset tutkimuskysymyksiin ja sitä kautta tutkimusongelmaan. Tutkimus tuotti toimeksiantajalle uutta tietoa pilvipalveluista sekä keskustelujen ja pohdinnan aihetta. Tutkimustulosten myötä toimeksiantajalle tehtiin luvussa 6 esitetty kehittämisehdotus ohjeistuksesta helpottamaan pilvipalveluiden käyttöönottoa asianajotoimistoissa.

Vaikka laadullisen tutkimuksen päätavoitteena ei ole tutkimustulosten yleistettävyys, voidaan tutkimuksesta saatuja tuloksia yleistää koskemaan myös mui-

ta asianajotoimistoja. Asianajotoimistot ovat työympäristönä samanlaisia, vaikka koko ja hoidettavat toimeksiannot saattavat vaihdella. Tietosuoja- ja tietoturvavaatimukset ovat kaikissa toimistoissa samanlaiset, minkä takia pilvipalveluilta vaaditaan samoja ominaisuuksia toimistosta riippumatta. Myös asianajajaliiton säädökset koskevat kaikkia asianajotoimistoja. Näin ollen tutkimuksen tulokset ovat myös sovellettavissa muihin asianajotoimistoihin.

Tutkimuksen luotettavuus

Tutkimuksen luotettavuutta arvioidaan laadullisen tutkimuksen luotettavuuskriteerien mukaisesti, jotka on kuvattu tarkemmin tutkimusmenetelmät-osiossa. Yksi tärkeimmistä laadullisen tutkimuksen luotettavuutta lisäävistä tekijöistä on tarkka dokumentaatio, joka tarkoittaa kaikkien ratkaisujen perustelemista tutkimuksen eri vaiheissa (Kananen 2010, 69). Tutkimuksen luotettavuus varmistettiin valitsemalla oikeat tutkimusmenetelmät tutkimusongelman kannalta ja perustelemalla nämä valinnat. Tämän lisäksi tutkimuksen toteutus dokumentoitiin tarkasti jokaisessa tutkimusvaiheessa.

Haastatteluiden luotettavuus varmistettiin kertomalla haastatteluiden lähtökohdat ja perustelemalla haastateltavien valinta. Haastatteluiden määrä päätettiin etukäteen, mutta niitä olisi voinut tehdä enemmän, jos se olisi katsottu tarpeelliseksi. Haastatteluiden edetessä tuloksista oli kuitenkin havaittavissa samankaltaisia piirteitä, minkä takia haastatteluiden määrän katsottiin olevan sopiva. Haastatteluiden luotettavuutta lisättiin nauhoittamalla haastattelut. Tämän myötä vuorovaikutus haastateltavan kanssa oli hyvä, koska muistiinpanojen kirjoittaminen ei vienyt huomiota pois haastateltavan vastauksista.

Haastatteluiden nauhoittaminen edesauttoi tarkan litteroinnin tekemistä. Haastattelut litteroitiin heti haastattelun jälkeen tai seuraavana päivänä, jolloin haastattelu oli vielä tuoreessa muistissa. Nauhoittamisen avulla haastatteluihin pystyttiin palaamaan aineiston analysointivaiheessa, millä varmistettiin aineiston tarkka analysointi. Aineiston analysointivaiheessa tulosten teemoittelu kuvattiin ja tulkintaa tehdessä tulkinnat perusteltiin haastatteluista nousseiden asioiden pohjalta. Tämän avulla voitiin osoittaa, että tulkinnat pohjautuivat haastateltavien näkemyksiin.

Tutkimustulosten myötä saatiin vastaus tutkimusongelmaan, minkä takia aineistonkeruu voidaan katsoa onnistuneeksi. Tutkimustuloksia olisi kuitenkin voinut vielä parantaa se, että haastateltavista jollain toisellakin toimistolla olisi ollut pilvipalvelut käytössä. Näin ollen oltaisiin saatu lisää näkökulmia itse käyttöönoton toteutukseen sekä tietosuojan, tietoturvan ja asianajajaliiton säädösten huomioimiseen. Tällöin oltaisiin saatu enemmän tietoa käyttöönoton suunnittelusta edellä mainittujen tekijöiden kannalta.

Haastateltavien tulisi olla sellaisia, joilla on mahdollisimman paljon tietoa tutkimusaiheesta (Kananen 2008, 35–37). Tässä tutkimuksessa osa haastateltavista ei ollut perehtynyt pilvipalveluihin paljoa, joten tältä kannalta katsottuna kaikki haastateltavat eivät olleet optimaalisimpia haastateltavia. Asianajotoimistoilla tuntui olevan yleisesti ottaen melko vähän tietoa pilvipalveluista, jonka takia haastateltaviksi valikoitui myös muutama henkilö, jotka eivät olleet asiaan perehtyneet. Toisaalta heidän haastatteluista löytyi samankaltaisia vastauksia kuin asiaan enemmän perehtyneiltäkin, josta voitiin tehdä myös päätelmiä.

Tutkijan oman roolin vaikutus tutkimustuloksiin tiedostettiin jokaisessa tutkimuksen vaiheessa. Tutkimuksen haastateltavista yksi oli tuttu opinnäytetyön tekijälle, mikä vaikutti haastatteluun siten, että haastattelu eteni tuttavallisemmin, kuin muut haastattelut. Tämä ei kuitenkaan vaikuttanut tutkimustuloksiin, sillä haastattelurunko oli jokaisessa haastattelussa sama. Opinnäytetyön tekijä pyrki olemaan kaikissa haastatteluissa samanlaisessa roolissa, eli johdattelemaan haastattelun kulkua vaikuttamatta haastattelijoiden vastauksiin. Tämän takia sen ei voida katsoa heikentävän tutkimuksen luotettavuutta. Opinnäytetyön tekijän omat asenteet ja näkemykset pyrittiin pitää erossa tutkimusmateriaalin tulkinnasta siten, että tulkintoihin löytyy perustelut haastatteluaineistosta.

Jatkotutkimusaiheet

Tutkimuksessa kävi ilmi, että melko harva toimisto on vielä siirtynyt pilvipalveluiden käyttöön. Haastateltavat olivat kanssani samoilla linjoilla ja syyksi epäiltiin muun muassa sitä, että alalla on totuttu tekemään asiat pitkään tietyllä tapaa, jonka takia muutos epäilyttää. Tämän takia olisi kiinnostavaa tehdä kvan-

titatiivisena tutkimuksena toteutettava kartoitus siitä, kuinka moni toimisto käyttää pilvipalveluita ja miksi toimistot käyttävät tai eivät käytä niitä. Kartoituksen voisi tehdä esimerkiksi Keski-Suomen alueen toimistoista. Tutkimuksesta saataisiin yleistettävämpiä tuloksia käyttöä rajoittavista tai estävistä tekijöistä asianajotoimistojen näkökulmasta.

Toisaalta olisi myös kiinnostavaa tehdä yllä kuvatun kaltainen tutkimus Helsingin alueella sijaitseville toimistoille, sillä hieman yli puolet kaikista asianajajista toimii Helsingissä. Keski-Suomeen alueen vastaava osuus on noin 3 %. Näin ollen, jos tutkimus tehtäisiin vain Keski-Suomen alueella, ei määrällisen tutkimuksen kannalta tulisi välttämättä tarpeeksi vastauksia, jotta niitä saataisiin mielekkäästi analysoitua. Jos tutkimuksen saisi toteutettua pääkaupunkiseudulla, olisivat tulokset kattavampia.

Toisena jatkotutkimusaiheena voisi olla AIPAn vaikuttavuus asianajotoimistojen sähköiseen asiakirjakirjojen käsittelyyn ja sitä kautta pilvipalveluiden hyödyntämiseen. Tämän tutkimuksen voisi tosin tehdä vasta silloin, kun AIPA on täysin käytössä, eli tämän hetkisellä aikataululla vasta vuonna 2018. Vielä tällä hetkellä asianajotoimistojen ja asianajajaliiton tietoisuus AIPAsta on melko vähäinen, mutta se tulee varmasti lisääntymään lähiaikoina, ja vuonna 2018 aiheesta osattaisiin varmasti sanoa huomattavasti enemmän.

Lähteet

Adequacy decisions. 2016. European Commission. Viitattu 1.10.2016. http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

Aineistopankkihanke. 2012. Oikeusministeriön muistio. Viitattu 23.9.2016. http://www.oikeusministerio.fi/material/attachments/om/valmisteilla/kehittamishankkeet/NMmokEaIp/AIPA_JulkinenTavoitetila_2012_11_23.pdf.

Alhava, S. 2016. Toimisto pilveen. Advokaatti 1/2016, 22.

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Asiakirjojen säilyttämistä koskeva suositus. 2012. Asianajotoimintaa koskevia säädöksiä ja ohjeita. Viitattu 26.9.2016. http://www.asianajajaliitto.fi/files/838/B_10_Asiakirjojen_sailyttamista_koskeva_suositus.pdf.

Asianajaja. N.d. Ammattinetti. Viitattu 26.9.2016. http://www.ammattinetti.fi/ammatit/detail/116_ammatti.

Asianajajaliiton paikallisosastot. N.d. Suomen Asianajajaliiton www-sivut. Viitattu 28.9.2016. http://www.asianajajaliitto.fi/asianajajaliitto/organisaatio/paikallisosastot.

Asianajajaliitto lukuina. 2015. Suomen Asianajajaliiton www-sivut. Viitattu 26.9.2016. http://www.asianajajaliitto.fi/files/2923/Vuosikatsausliite2016_final.pdf.

Asianajajaliitto lyhyesti. N.d. Suomen Asianajajaliiton www-sivut. Viitattu 22.9.2016. http://www.asianajajaliitto.fi/asianajajaliitto/liitto_lyhyesti.

Castrén, K. 2010. Pilvipalvelut: Sopimalla saat turvallisemman. Tietosuoja 3/2010. Viitattu 28.9.2016. https://www.tietosuoja-lehti.fi/index.php?mid=2&pid=32&aid=2751.

Digitalization. N.d. Gartner IT Glossary. Viitattu 27.9.2016. http://www.gartner.com/it-glossary/digitalization/.

Euroopan unionin tietosuojalainsäädännön uudistaminen. 2016. Oikeusministeriö. Viitattu 23.9.2016. http://www.oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html.

EU-lakien suhde Suomen lakiin. 2015. Ulkoasiainministeriön eurooppatiedotus.fi -sivusto. Viitattu 29.9.2016. http://www.eurooppatiedotus.fi/public/default.aspx?contentid=272243&contentlan=1.

EU:n tietosuoja-asetus muuttaa henkilötietojen käsittelyä. 2016. Suomen kuntaliitto. Viitattu 29.9.2016.

http://www.kunnat.net/fi/tietopankit/uutisia/2016/Sivut/EUn-tietosuoja-asetus-muuttaa-henkilotietojen-kasittelya.aspx.

EU:n tietosuojauudistus. 2015. Tietosuojavaltuutetun toimisto. Viitattu 29.9.2016. http://www.tietosuoja.fi/fi/index/euntietosuojauudistus.html.

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo.

Heino, P. 2010. Pilvipalvelut. Helsinki: Talentum.

Hirsjärvi, S. & Hurme, H. 2000. Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.

Hirsjärvi, S., Remes, P., Sajavaara, P. 2009. 15. uud. p. Tutki ja kirjoita. Helsinki: Tammi.

Hyvää asianajajatapaa koskevat ohjeet. 2012. Asianajotoimintaa koskevia säädöksiä ja ohjeita. Viitattu 1.10.2016. http://www.asianajajaliitto.fi/files/1660/B_01_Hyvaa_asianajajatapaa_koskevat_ohjeet_tammikuu_2013.pdf.

Järvinen, P. 2012. Arjen tietoturva. Vinkit & Ratkaisut. Jyväskylä: Docendo.

Kalli, S., Argillander, T., Talvitie, J. & Luoma, E. 2013. Suomalainen Pilvimaisema. Helsinki: Liikenne- ja viestintäministeriö. Viitattu 23.9.2016. https://www.lvm.fi/documents/20181/799435/Julkaisuja+14-2013/1721c985-6737-41af-ab36-d439649681a4?version=1.0.

Kananen, J. 2008. Kvali: kvalitatiivisen tutkimuksen teoria ja käytänteet. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kananen, J. 2010. Opinnäytetyön kirjoittamisen käytännön opas. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Kimbro, S. & Mighell, T. 2011. Popular Cloud Computing Services for Lawyers: Practice Management Online. Law Practice, 37, 5. Viitattu 31.10.2016. https://www.americanbar.org/publications/law_practice_magazine/2011/september_october/popular_cloud_computing_services_for_lawyers.html.

Korhonen, S. 2016. Teknologiajätit huokaisevat helpotuksesta: EU hyväksyi Safe Harborin korvaavan sopimuksen. Mikro Bitti. Viitattu 23.9.2016. http://www.mikrobitti.fi/2016/07/teknologiajatit-huokaisevat-helpotuksesta-eu-hyvaksyi-safe-harborin-korvaavan-sopimuksen/.

Lait. 2015. Tietosuojavaltuutetun toimisto. Viitattu 28.9.2016. http://www.tietosuoja.fi/fi/index/lait.html.

Laukkanen, J. & Järvenpää, E. 2012. Asianajajatutkimus. Viitattu 26.9.2016. http://www.asianajajaliitto.fi/files/1628/Asianajajatutkimus2012.pdf.

L 22.4.1999/523. Henkilötietolaki. Viitattu 28.9.2016. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

L 12.12.1958/496. Laki asianajajista. Viitattu 23.9.2016. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

L 13.8.2004/759. Laki yksityisyyden suojasta työelämässä. Viitattu 28.9.2016. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

L 7.11.2014/917. Tietoyhteiskuntakaari. Viitattu 28.9.2016. Valtion säädöstietopankki Finlex. http://www.finlex.fi, ajantasainen lainsäädäntö.

Mell, P. & Grance, T. 2011. The NIST Definition of Cloud Computing. Viitattu 29.9.2016. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf.

Metsämuuronen, J. 2008. Laadullisen tutkimuksen perusteet. Helsinki: International Methelp.

Mikkonen, E. 2015. Viestinviejänä AIPA-hankkeessa. Oikeusministeriön Oikeus.fi:n Arkea&Ajatuksia -sivut. Viitattu 16.9.2016. www.oikeus.fi/arkeaajatuksia.

Oikeuslaitos. 2015. Oikeusministeriön oikeus.fi -sivusto. Viitattu 25.9.2016. http://www.oikeus.fi/fi/index/esitteet/oikeuslaitos.html.

OM: Rikos- ja riita-asioiden käsittely muuttuu vähitellen sähköiseksi – Tietojärjestelmän toimittaja valittu. 2014. Suomen Asianajajaliitto. Oikeudelliset uutiset, Kotim. tietolähteet, arkisto 2014. Viitattu 23.9.2016. http://www.asianajajaliitto.fi/viestinta/oikeudellisia_uutisia/kotimaiset_tietolahteet/2014/om_rikos-_ja_riita-asioiden_kasittely_muuttuu_vahitellen_sahkoiseksi_-_tietojarjestelman_toimittaja_valittu.7686.news.

Practice briefing: cloud computing guidelines for lawyers. 2014. New Zealand Law Society. Viitattu 31.10.2016. https://www.lawsociety.org.nz/practice-resources/practice-briefings/Cloud-Computing-2014-07-21-v2.pdf.

Pynnä, P. 2015. EU päätti tietojen siirrosta Yhdysvaltoihin - sammutammeko valot? ASML. Viitattu 23.9.2016. http://www.asml.fi/blogi/safe-harbor-kaatui-mita-seuraavaksi/.

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. Viitattu 27.9.2016. http://www.fsd.uta.fi/menetelmaopetus/.

Salminen, M. 2009. Tietosuoja sähköisessä liiketoiminnassa. Helsinki: Talentum.

Salo, I. 2010. Cloud computing: palvelut verkossa. Jyväskylä: Docendo.

Salo, I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo.

Subashini, S. & Kavitha, V. 2011. A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applica-

tions, 34, 1, 1-11. Viitattu 30.10.2016. http://www.sciencedirect.com/science/article/pii/S1084804510001281.

Suomen Asianajajaliitto. N.d. Suomen Asianajajaliiton www-sivut. Viitattu 22.9.2016. http://www.asianajajaliitto.fi/asianajajaliitto.

Syyttäjänlaitoksen ja yleisten tuomioistuinten asian- ja dokumentinhallinnan kehittämishanke. 2010. Oikeusministeriön asettamispäätös. Viitattu 23.9.2016. http://www.oikeusministerio.fi/material/attachments/om/valmisteilla/kehittamishankkeet/NAw6c1t5b/AIPA_asettamispaatos_syko_asianhallinta_2010_02_16.pdf.

Syyttäjänlaitoksen ja yleisten tuomioistuinten asian- ja dokumentinhallinnan kehittämishanke (AIPA). 2016. Oikeusministeriö. Viitattu 23.9.2016. http://www.oikeusministerio.fi/fi/index/valmisteilla/kehittamishankkeita/syyttajalaitoksenjayleistentuomioistuintenasian-jadokumentinhallinnankehittamishanke.html.

Tietosuojalainsäädäntö. N.d. Elinkeinoelämän keskusliitto. Viitattu 1.10.2016. http://ek.fi/mita-teemme/yrityslainsaadanto/tietosuojalainsaadanto/.

Tietotekniikan käyttö yrityksissä 2014. Tilastokeskus. Viitattu 23.9.2016. https://www.stat.fi/til/icte/2014/icte_2014_2014-11-25_fi.pdf.

Tietoturvallisuusohje. 2013. Asianajotoimintaa koskevia säädöksiä ja ohjeita. Viitattu 23.9.2016. http://www.asianajajaliitto.fi/files/1733/B_05.1_Tietoturvallisuusohje_10.1.2013.pdf.

Tietoturvaopas. 2012. Asianajotoimintaa koskevia säädöksiä ja ohjeita. Viitattu 23.9.2016. http://www.asianajajaliitto.fi/files/1734/B_05.2_Tietoturvaopas_14.12.2012.pdf.

Tietoyhteiskuntakaarta sovelletaan internetin yhteisö- ja ajanvietepalveluihin. 2015. Viestintävirasto. Viitattu 28.9.2016. https://www.viestintavirasto.fi/kyberturvallisuus/palveluidenturvallinenkaytto/palveluntarjoajanyhteystiedot.html.

Vallisaari, E. 2016. Digitalisaatio muuttaa työtä myös oikeuslaitoksessa. Oikeusministeriön Oikeus.fi:n Arkea&Ajatuksia -sivut. Viitattu 23.9.2016. www.oikeus.fi/arkeaajatuksia.

Vanto, J. 2011. Henkilötietolaki käytännössä. Helsinki: WSOYpro.

Ylöstalo, M. & Tarkka, O. 2001. Asianajajan käsikirja. Helsinki: Werner Söderström lakitieto.

Liitteet

Liite 1. Teemahaastattelurunko ja tarkentavat kysymykset

Käsiteltävät teemat:

- **Pilvipalvelut**
- **Tietosuoja ja tietoturva**
- **Asianajajaliiton säädökset**

1. Pilvipalvelut

- Mitä mieltä olette pilvipalveluista? (mitä hyvää, mitä huonoa, mitä riskejä)
- Onko käytössä pilvipalvelupohjaisia ratkaisuja?
    - Jos on, niin mitä ja miksi on päädytty niihin?
    - Jos ei, niin miksi ei ole otettu käyttöön?
- Onko suunnitteilla ottaa käyttöön lähitulevaisuudessa? (jos on niin mitä ja miksi, jos ei niin miksi ei)
- Käsiteltävät/arkistoitavat asiakirjat ja niiden sisältämä tieto (=mitä pilveen siirrettäisiin)
    - Minkä tyyppisiä asiakirjat ovat?
    - Mitä tietoa ne sisältävät, ovatko ne salaisia?
    - Mitä tulee huomioida niitä käsiteltäessä, arkistoidessa ja tuhotessa?
- Sopiiko mielestänne kaikenlainen tieto säilytettäväksi pilvessä?
    - Minkälainen tieto ei välttämättä sovi?
- Mitä tiedätte AIPA-hankkeesta, vaikuttaako se jotenkin pilvipalveluihin?

2. Tietosuoja ja tietoturva

- Miten miellätte käsitteet tietosuoja ja tietoturva?
- Kuinka tärkeää em. mainittujen tekijöiden säilyminen on asianajotoimistossa?
- Millä tavalla yksityisyyden suojaaminen hoidetaan toimistossanne? (salassapitosopimukset, asiakkaiden henkilötietojen käsittely, salaiset asiakirjat)
- Käytetäänkö salattua sähköpostiviestiä? (milloin sitä pitäisi käyttää)
- Miten tietoturvallisuudesta huolehditaan? (laitteiden käyttö ja salaus, päivitykset)

- Millaiseksi koette tietosuojan ja tietoturvan pilvipalveluissa?
    - Liittyykö sen käyttöönottoon jotain huolia, esim. palvelimen sijaintimaa, mihin maihin saa siirtää tietoja, kuka pääsee tietoihin käsiksi?
    - Mitkä tekijät parantavat tietosuojaa ja tietoturvaa?

3. Asianajajaliiton säädökset

- Kuinka tarkasti säädöksiä velvoitetaan noudattamaan, kuinka paljon on tulkinnan varaa?
- Säädökset it-palveluiden ulkoistamisesta (miten vaikuttavat pilvipalveluiden käyttöön):
    - Asianajosalaisuuksia sisältävän tiedon säilytys, käyttö ja siirto tietokoneilla, jotka eivät ole asianajajan yksinomaisessa hallinnassa. (salassapitosopimukset)
    - Palveluntarjoajan tekninen tietoturvataso ja taustat, palvelimen sijaintimaa. (tarkistettava)
    - Palveluntarjoajan varmuuskopioinnin taso ja tiedostojen palautettavuus.
    - Ilmaiset/erittäin edulliset palvelut, joissa käytetään käyttöönottosopimuksessa vakiosopimusta. (ei luottamuksellista tietoa, muistiinpanoihin soveltuu)
    - Ulkoistus ei saa vaarantaa asianajotoimiston tietoturvaa, salassapitosopimus, päätösvalta etäyhteyden käytöstä, tietoturvallinen ajattelu.