Juho Kantola

IMMATERIAALIOIKEUKSIEN HALLINTA PILVIPALVELUISSA TEKNOLOGIAN JA PILVIPALVELUIDEN OMINAISPIIRTEIDEN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2016

TIIVISTELMÄ

Kantola, Juho
Immateriaalioikeuksien hallinta pilvipalveluissa teknologian ja pilvipalveluiden ominaispiirteiden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2016, 33 s.
Tietojärjestelmätiede, kandidaatintutkielma
Ohjaaja: Halttunen, Veikko

Pilvipalvelut tarjoavat yksityisille kuluttajille ja organisaatioille mahdollisuuden kasvattaa tehokkuutta. Vaikka pilvipalvelut tarjoavat etuja, on niihin liittyviä omistus- ja immateriaalioikeuksia käsitelty alan kirjallisuudessa joko vähän tai niitä on käsitelty muun tietoturvan ohella. Tässä tutkielmassa pyritään löytämään niitä pilvipalveluille ominaisia piirteitä, jotka vaikuttavat immateriaali- ja omistusoikeuksien määräytymiseen kirjallisuuskatsauksen avulla ja vastaamaan mitä pilvipalvelun potentiaalisen asiakkaan tulisi tehdä pitääkseen nämä omistus- ja immateriaalioikeudet itsellään.

Tutkielman tuloksia ovat kirjallisuuskatsauksen avulla tehty pilvipalveluiden ominaispiirteiden ja teknologisten ominaisuuksien kokoaminen, joilla on potentiaalista merkitystä immateriaalioikeuksien hallinnan kannalta. Tuloksista käy muun muassa ilmi, että teknologisen kehityksen johdosta voimassa olevalla lainsäädännöllä voi olla lain alkuperäisen tarkoituksen vastaisia vaikutuksia.

Toisaalta teknologisesta näkökulmasta katsoen ei esimerkiksi ole kehitetty ratkaisuja, jotka varmistaisivat asiakkaan tiedon salauksen niin, että tietoon voi kohdistaa monimutkaisia operaatioita pitäen tiedon sisällön ainoastaan asiakkaan hallussa.

Asiasanat: Pilvipalvelut, omistusoikeus, immateriaalioikeudet, immateriaalioikeuksien hallinta, pilvipalvelujen teknologia

ABSTRACT

Kantola, Juho

Jyväskylä: University of Jyväskylä, 2016, 33 p.
The management of immaterial rights in cloud computing services from the perspective of technology and characteristics of cloud computing services
Information Systems, Bachelor's Thesis
Supervisor: Halttunen, Veikko

Cloud services offer private consumers and organizations a chance to grow their efficiency. Cloud services offer benefits, but the ownership and immaterial rights related to cloud services have been discussed to a limited degree, or in the context of information security in general. This thesis seeks to discover unique characteristics of cloud services that affect the determination of immaterial and ownership rights with the help of a literacy review, and answer what a potential customer of a cloud service should do in order to keep these ownership and immaterial rights to himself.

By doing a literary review, this thesis seeks to compile technological attributes and characteristics of cloud services which have a potential bearing on the management of immaterial rights. The results for example show that due to technological advancement current legislation may have effects that are contrary to the original intent of the law.

Further, looking at the technological point of view, there have been no solutions developed for cloud services to ensure the encryption of a client's data in a manner that allows the application of complex operations while holding the content of the data solely in the client's possession.

Keywords: Cloud services, ownership, immaterial rights, management of immaterial rights, cloud computing technology

KUVIOT

SISÄLLYS

1 JOHDANTO

Pilvipalvelut yleistyvät niiden joustavuuden ja siihen liittyvien säästöjen ansiosta. Kalyvas, Overly ja Karlyn (2013) mainitsevat esimerkiksi elastisuuden eli mahdollisuuden lisätä palvelun kapasiteettia hyvin nopeasti, ja skaalautuvuuden eli mahdollisuuden käyttää hyvin suuria resursseja ilman, että pilvipalvelun käyttäjälle koituu pysyviä kustannuksia infrastruktuurihankintojen johdosta. Kuitenkin pilveen tallennetun tiedon omistusoikeudet ja immateriaalioikeudet eivät ole aina yksiselitteisiä. Jaeger, Lin, ja Grimes (2008) toteavatkin, että pilvipalvelut nostavat esille huomattavia kysymyksiä muun muassa yksityisyydestä, turvallisuudesta, anonyymiudesta sekä pilvipalveluihin pätevien lakien toimivuudesta.

Sekä yksityiset kuluttajat että suuryritykset saattavat ladata pilveen sisältöä, joihin sisältyy omistus- ja immateriaalioikeuksia. Nämä oikeudet saattavat liittyä esimerkiksi valokuvan tekijänoikeuteen, tai immateriaalioikeuksiin, jotka voivat liittyvät esimerkiksi logoon tai tuotekehitystietoihin.

Patibandla, Kurra ja Mundukur (2012) mainitsevat, että pilvipalveluiden käyttöön sisältyy luontaisesti riskejä käyttäjälle, koska käyttäjän syötteet ja ladatut tiedot pilvipalvelussa voivat olla salaamattomassa muodossa. Tämä voi altistaa asiakkaan pilvipalvelussa olevan tiedon pilvipalveluntarjoajan työntekijöille tai ulkopuolisille tahoille.

Pilvipalvelut voivat myös varastoida tietoa valtioissa, joissa viranomaiset voivat päästä käsiksiin tietoihin lain mukaan tietyissä tilanteissa. Vaikka valtio olisikin jopa sama, missä pilvipalvelun käyttäjä sijaitsee, tiedon keskittyminen palveluntarjoajalle voidaan olettaa asettavan tiedon riskialttiimmaksi, koska tällöin yhdessä lähteessä eli palveluntarjoajan tiloissa on suurempi hyöty tiedon erilaisille väärinkäytöksille.

Myös itse tietoverkon turvallisuus, eli asiakkaan ja palveluntarjoajan välinen yhteys on riskikysymys. Tiedon eheys palveluntarjoajalla voi asettaa riskejä asiakkaalle. On myös luontevaa kysyä, miten palveluntarjoaja vastaa asiakkaan todentamisesta, ja miten käyttöoikeudet tietoon jaetaan palveluntarjoajan puolesta ja asiakkaan organisaation sisällä. Myös pilvipalvelujen saatavuus kunakin käyttöhetkenä voi olla riskinä asiakkaalle verrattuna perinteisiin toteutuksiin. (Subashini, Kavitha, 2010.).

Pilvipalveluiden luonne asettaa haasteita tiedon luottamuksellisuudelle, koska asiakkaan tieto kulkee lähes aina kolmansien osapuolten hallitsemien tietoverkkojen kautta. Marston, Li, Bandyopadhyay, Zhang, ja Ghalsasi (2011) kertovat, että pilvipalvelut muuttavat käsityksiä tiedon paikasta ja omistajuudesta, koska tiedon haltijat antavat tietonsa palveluntarjoajille, jotka ovat vastuussa tiedon tallennuksesta ja hallinnoinnista. Perinteisesti kuluttajat ja liikeyritykset sekä omistavat että hallitsevat tietoansa: hallitsemiseen kuuluu muun muassa se, miten ja mihin tieto on fyysisesti varastoitu. Pilvipalvelujen käyttö kuitenkin muuttaa näitä oletuksia

Googlen käyttöehdot ovat aiheuttaneet kohua suomalaisessakin mediassa käyttöehtoihin liittyvien epäselvyyksien vuoksi. (Linnake, 2012). Kappale, joka on aiheuttanut kohua, on alla (Google, 2014):

> Kun lataat, lähetät tai tallennat sisältöä Palveluihin tai niiden kautta tai vastaanotat sisältöä Palveluista tai niiden kautta, annat Googlelle (ja yhteistyökumppaneillemme) maailmanlaajuisen oikeuden käyttää, ylläpitää, tallentaa, jäljentää, muokata, välittää, julkaista, esittää ja levittää kyseistä sisältöä, asettaa sitä julkisesti esille sekä luoda siitä johdannaisteoksia (esimerkiksi teoksia, jotka syntyvät kääntämällä, sovittamalla tai tekemällä teokseen muita muutoksia, joiden avulla sisältö saadaan toimimaan Palveluissa paremmin). (...)

Google kuitenkin perustelee näitä käyttöehtoja käyttöehdoista löytyvällä seuraavalla kappaleella. (Google, 2014):

> Sinulla on mahdollisuus ladata, lähettää tai tallentaa sisältöä joihinkin Palveluihin ja vastaanottaa sisältöä niistä. Säilytät mahdolliset sisältöä koskevat immateriaalioikeudet itselläsi eli sisällön lähettäminen ei perusta immateriaalioikeuksien siirtymistä.

Google siis perustelee käyttöehdoissa palveluntarjoajalle tai sen kumppaneille annettua oikeutta käyttää käyttäjän lataamaa sisältöä sillä, että se mahdollistaa palvelujen tarjoamisen asiakkaalle. Monet muutkin palveluntarjoajat käyttävät lähes identtisiä käyttöehtoja omissa palveluissaan.

Tällaiset epäselvyydet tiedon omistuksesta osoittavat, että pilvipalveluihin liittyviin omistusoikeus- ja immateriaalioikeuskysymyksiin ei ole yksiselitteisiä vastauksia. Sen lisäksi aiheeseen liittyvä kirjallisuus ja artikkelit eivät yksittäisiä poikkeuksia lukuun ottamatta keskity nimenomaan omistus- ja immateriaalioikeuksiin liittyviin kysymyksiin, vaan käsittelevät niitä yleensä osana suurempaa riskien kokonaisuutta, joihin luetaan muun muassa tietoturvakysymykset. Tämän takia kirjallisuuskatsaus aiheesta on perusteltu.

Natunen (2014) on käsitellyt tekijänoikeus- ja omistusoikeuskysymyksiä pilveen liittyen omassa pro gradu -tutkielmassaan, mutta hän rajaa oman teoriaosuutensa hyvin tarkkaan käsittelemään ainoastaan sopimuskäytäntöä, käyttöehtosopimuksia ja kansallista sekä kansainvälistä lainsäädäntöä. Natunen käsittelee näitä kysymyksiä nimenomaan yksittäisten pilvipalvelujen näkökulmasta. Natunen (2014) ei siis syvenny esittelemään minkälaisia haasteita pilvipalveluille ominaiset tekniset ominaisuudet luovat, joita itse esittelen omassa tutkielmassani.

Tässä tutkielmassa käsitellään ensimmäiseksi kirjallisuuskatsauksen avulla erilaisia normeja, lainsäädäntöä ja käyttöehtoja, jotka vaikuttavat osaltaan omistusoikeuden määräytymiseen pilvipalveluissa. Tämän jälkeen määrittelen teknisiä seikkoja ja lainsäädäntöä, jotka ovat ominaisia nimenomaan pilvipalveluille tai omaavat yhteisiä seikkoja esimerkiksi tietokonesovellusten kanssa. Tämän jälkeen käsittelen ilmi tulleita seikkoja tarkemmin, sekä mitä asiakas voi tehdä varmistaakseen immateriaalioikeuksien ja omistusoikeuden säilymisen itsellään käyttäessään pilvipalveluita. Tutkimusongelman muodostavat siis seuraavat kysymykset:

1. Mitkä pilvipalveluille ominaiset piirteet ja tekniset ominaisuudet liittyvät omistus- ja immateriaalioikeuksiin pilvipalveluissa?

2. Ottaen huomioon esille tulleet normit ja tekniset seikat, mitä asiakas voi tehdä pyrkiäkseen hallitsemaan omistus- ja immateriaalioikeuksia?

Toisessa luvussa käsitellään erilaisia pilvipalveluita sekä niihin liittyviä lakeja ja normeja. Kolmannessa luvussa kuvaillaan niitä teknisiä ja ei-teknisiä ominaispiirteitä jotka vaikuttavat pilvipalvelujen omistus- ja immateriaalioikeuksien hallintaan ja pohditaan niitä alustavasti. Nämä ominaispiirteet on valittu lukemalla alan akateemisia artikkeleita ja listaamalla niitä seikkoja, joita artikkeleissa käsitellään. Yhteenvedossa pohditaan miten kolmannessa luvussa ilmi tulleiden seikkojen valossa immateriaali- ja tekijänoikeuksia voidaan pilvessä hallita, ja pohditaan edellisten lukujen sisältöä.

2 PILVIPALVELUT JA NIIHIN LIITTYVÄT LAIT JA NORMIT

Esittelen tässä luvussa kaksi tapaa jaotella pilvipalveluja, sekä lait ja normit, joiden voidaan nähdä muodostavan perustan asiakasta ja palveluntarjoajaa sitovalle suhteelle. Ensin käsitellään kaksi yleisintä tapaa jakaa pilvipalveluja eri tyyppeihin, jonka jälkeen kuvaillaan lyhyesti immateriaali- ja omistusoikeuksia sekä sopimuksia.

2.1 Pilvipalvelujen palvelumallit ja palvelutyypit

Kalyvas ym. (2013) jaottelevat pilvipalvelumalleja kolmeen eri kategoriaan:

1. Software-as-a-Service (SaaS)
2. Platform as-a-Service (PaaS)
3. Infrastructure-as-a-Service (IaaS)

SaaS-palvelut ovat palveluntarjoajan ohjelmistoja, joita toimitetaan Internetin välityksellä (Kalyvas ym., 2013). Marston ym. (2011) mainitsevat lisäksi, että asiakkaiden ei tarvitse asentaa tai ajaa SaaS-sovelluksia omalla koneellaan Liu ym. (2011) määrittelevät, että SaaS-sovellusten käyttäjiä voivat olla organisaatiot, jotka tarjoavat jäsenilleen pääsyn sovelluksiin, loppukäyttäjät jotka käyttävät sovellusta ilman välikäsiä, tai ylläpitäjät jotka konfiguroivat SaaS-sovelluksia loppukäyttäjiä varten.

PaaS-palvelut tarkoittavat esimerkiksi palveluntarjoajan kehitysalustaa, joka toimitetaan sovelluskehittäjälle Internetin välityksellä. Sovelluskehittäjä voi käyttää palvelua kehittääkseen, testatakseen ja ottaakseen käyttöön kehittämiänsä sovelluksia, jotka toimivat sen jälkeen palveluntarjoajan infrastruktuurin päällä (Kalyvas ym., 2013). Marston ym. (2011) tarjoavat esimerkeiksi PaaS-palveluista seuraavia: Microsoft:in Azure Services Platform, Salesforce:n Force.com, Google App Engine, Amazonin Relational Database Services ja Rackspace:n Cloud Sites.

IaaS-palvelut antavat asiakkaalle pääsyn virtuaalikoneisiin, verkon kautta käsiksi päästävään tallennustilaan, prosessoreihin ja muuhun perustavanlaatuiseen IT-infrastruktuuriin, jonka avulla ylläpitäjät ja kehittäjät voivat luoda erilaisia IT-kokonaisuuksia (Liu ym., 2011). IaaS-palvelut antavat asiakkaalle pääsyn lähimmäksi ns. rautatasoa verrattuna muihin palvelumalleihin ja mahdollistavat suurimman muokkausvaran kaikista kolmesta palvelumallista. Kerr ja Teng (2010) kertovat, että asiakkaalle annetaan täysi hallinta jonkin palvelimen osasta. Sen sijaan, että asiakas käyttäisi jotain valmiiksi konfiguroitua virtuaalikoneen ilmentymää, asiakas voi pyörittää itsensä luomaa ja muokkaamaa virtuaalikonetta.

Pilvipalveluiden palvelutyyppejä on kolmenlaisia: private, hybrid ja public cloud, eli yksityinen, hybridi ja julkinen pilvi. Marston ym. (2011) mainitsevat, että julkinen pilvi on sellainen pilvipalvelutyyppi, jossa palvelu on ulkopuolisen palveluntarjoajan tarjoama ja siihen on pääsy Internetin kautta. Julkinen pilvi tarjoaa joustavuutta esimerkiksi kustannuksissa, koska ne eivät ole asiakkaan itsensä ylläpitämiä. Marston ym. (2011) mainitsevat, että Google Apps on yksi hyvä esimerkki julkisesta pilvestä, ja että julkiset pilvet ovat hyödyllisiä pienemmille yrityksille.

Yksityinen pilvi taas tarjoaa suurempaa kontrollia pilvipalvelun infrastruktuurille, ja se voi olla asiakkaan itse hallitsema. Yksityinenkin pilvi voi kuitenkin olla kolmannen osapuolen hallitsema – eli asiakas ostaa palvelun palveluntarjoajalta, mutta yksityinen pilvi on täysin eroteltuna julkisista pilvipalveluista. Hybridi pilvi on taas julkisen ja yksityisen pilven yhdistelmä, jossa esimerkiksi epäkriittiset tiedot ja palvelut voivat olla hybridin pilven julkisella puolella (Marston ym., 2011.).

Kalyvas ym. (2013) määrittelevät myös yhteisöpilven, jossa pilvipalvelun infrastruktuuri on jaettu usean organisaation välillä, joilla on esimerkiksi jokin yhteinen tavoite. Yhteisöpilvessäkin pilvi voi olla yksityisen pilven tapaan myös kolmannen osapuolen tarjoama.

2.2 Omistus- ja immateriaalioikeudet sekä sopimukset

Perinteisen omistusoikeuden kohteena on Haarmann ja Mansala (2012, 16–17) mukaan konkreettinen esine, jota omistaja voi hallita ja käyttää. Omistusoikeuteen kuuluu myös oikeus luovuttaa omistusoikeuden kohde esimerkiksi sopimuksella ja valta päättää omistusoikeuden kohteen paikasta.

Immateriaalioikeudet jaetaan Suomessa kahteen osaan: tekijänoikeuteen ja teollisuusoikeuteen. Teollisoikeudet ovat teknisiä, edellyttävät yleensä rekisteröintiä, ja ne suojaavat esimerkiksi keksintöä, mallia ja yrityksen tunnusta tai logoa. (Haarmann & Mansala, 2012, 16-17.).

Suomessa tekijänoikeus suojaa kirjallisten ja taiteellisten teosten luojia. Suojan saaminen kuitenkin edellyttää teokselta teoskynnyksen ylittämistä eli riittävää itsenäisyyttä ja omaperäisyyttä. Tekijänoikeuteen kuuluu taloudellisia oikeuksia, kuten kappaleiden valmistamisen oikeus, ja oikeus saattaa teos yleisön saataviin, sekä moraalisia oikeuksia kuten isyys- ja respektio-oikeus, jotka määrittelevät tekijän henkilökohtaista suhdetta teokseen. (Haarmann, 2005, 90-93).

Moraaliset oikeudet määrittelevät esimerkiksi teoksen tekijän oikeutta julkistaa, ja oikeutta päättää milloin teos julkistetaan. Oikeudet käsittelevät myös tekijän oikeutta päästä teoksen luokse ja erilaisia loukkaamattomuusoikeuksia, joihin sisältyy muun muassa tekijän oikeus tulla mainittuna teoksen tekijänä, sekä teoksen muuntelemattomuus loukkaavalla tavalla (Haarmann, 2005, 138–151).

Euroopan Unioni vaikuttaa myös säädöksillään ja direktiiveillään pilvipalveluiden omistus- ja immateriaalioikeuksiin. EU on asettanut muun muassa direktiivejä, jotka määräävät esimerkiksi henkilötietojen siirrosta eri maihin. Svantesson ja Clarke (2010) viittaavatkin yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annettuun Euroopan parlamentin ja neuvoston direktiivin 95/46/EY artiklaan 25, joka edellyttää sitä, että henkilötietojen siirron tapahtuessa kolmanteen maahan tietoa koskee tarpeeksi tyydyttävä tietosuoja kohdemaassa.

Sopimuksen keskeisiä käsitteitä on tarjous-vastaus-mekanismi. Mekanismi tarkoittaa sitä, että sitova sopimus syntyy, kun on esitetty tarjous ja siihen on vastattu myöntävästi. Vastatarjous syntyy silloin, kun vastaus sisältää muutoksia annettuun tarjoukseen, ja se on sitova niin, että alkuperäisen tarjouksen antaja voi hyväksyä sen ja tehdä sopimuksesta pätevän (Hemmo, Könkkölä & Norros, 2006, 73–82).

Suomessa sopimusoikeutta käsittelee lähinnä Laki varallisuusoikeudellisista oikeustoimista. (Laki varallisuusoikeudellisista oikeustoimista, 1929). Käyttöehtosopimukset ovat käyttäjän hyväksymiä, yleensä vakiomuotoisia sopimuksia, joiden hyväksymistä palveluntarjoaja edellyttää palvelun käyttämiseksi. Varsinkin suurilla yrityksillä on tosin yleensä mahdollisuus neuvotella sopimusehdoista palvelua hankkiessaan toisin kuin pienillä tai keskisuurilla yrityksillä tai yksityisillä kuluttajilla.

Lemley (2006) määrittelee ”shrinkwrap”, ”clickwrap” ja ”browsewrap”-sopimukset käyttöehtosopimuksiksi, koska ne kontrolloivat – tai ne olettavat kontrolloivansa käyttäjien pääsyä sisältöön tai ohjelmistoon. Shrinkwrap-sana viittaa ohjelmistojen muovikelmupakkauksiin, clickwrap taas ”Hyväksyn”-painikkeen käyttämiseen käyttöehdoissa jotka ovat elektronisessa muodossa, ja browsewrap viittaa esimerkiksi verkkosivun käyttöehtojen hyväksymistä pelkästään selailemalla verkkosivun sisältöä.

3 IMMATERIAALIOIKEUKSIIN LIITTYVÄT TEKNISET OMAINAISPIIRTEET

Tässä luvussa esitellään pilvipalveluihin kuuluvia teknisiä ominaispiirteitä ja normeja, jotka yhdessä vaikuttavat omistus- ja immateriaalioikeuksien hallintaan. Luvussa pohditaan myös sitä, miten nämä ominaispiirteet ovat riskejä näiden oikeuksien hallinnalle, ja miten käyttäjän sekä mahdollisesti palveluntarjoajan pitäisi toimia reagoidakseen näihin riskeihin.

3.1 Metatieto ja tiedon arvo

Mitä on metatieto pilvessä? Akateemiset julkaisut eivät määrittele kokonaisvaltaisesti, mitä metatieto juuri pilvessä tarkoittaa. Lassila (1998) käyttää muun muassa seuraavia ominaisuuksia kuvaamaan metatietoa: Metatieto on tietoa esimerkiksi dokumentin tekijästä, dokumentin luomisajasta ja muusta kuvailevasta tiedosta. Metatieto määritellään yleensä tiedoksi tiedosta. Esimerkiksi tiedostojärjestelmä voi hallita metatietoa hallinnoidakseen kansion tai tiedostojen käyttöoikeuksia. Metatieto myös auttaa järjestelemään tietoa. Metatiedolla on yleensä ottaen myös tietynlainen syntaksi, joka tekee siitä konetulkittavaa (Lassila, 1998). Prabavathy, Devi ja Babu (2013) kuvailevat deduplikaatiota eli samanlaisten tiedostojen kaksoisilmentymien poistamista pilvipalveluissa. Tässä yhteydessä he mainitsevat, että tiedoston metatieto voi koskettaa tiedoston fyysistä paikkaa tallennuslaitteessa.

Näiden määritelmien avulla voidaan lähteä määrittelemään, mitä metatieto on pilvipalvelussa. Metatieto pilvipalveluissa voidaan nähdä olevan kaikkea sitä tietoa, mikä ei ole itse käyttäjän lataamaa sisältöä ja joka muodostuu yleensä automaattisesti käyttäjän toimien ja niiden tiedostojen perusteella mitä käyttäjä lataa pilvipalveluun. Jos pilvipalvelu luo automaattisesti esimerkiksi jonkinlaista lokitiedostoa käyttäjien toimista, voidaan sen katsoa olevan metatietoa. Pilvipalveluissa on myös luonnollisesti perinteistä metatietoa, joka liittyy tiedostoihin tai tietorakenteisiin. Tämä metatieto sisältää esimerkiksi tiedoston luonti- ja muokkauspäivät, omistajan, viimeisen muokkaajan, jne. Metatieto voi liittyä myös pilvipalveluissa tiedon fyysiseen sijaintiin tallennusmedialla. Metatieto voi myös pilvipalvelussa kuvailla itse sisältöä luokitellen sen esimerkiksi johonkin genreen. Esimerkiksi YouTube (2015b) määrittelee metatiedoksi jopa videon annetun nimen ja kuvauksen. Tämä ei välttämättä vastaa kaikissa tilanteissa metatiedon määritelmää, mutta toisaalta YouTube:n tag-toiminto, jolla voi antaa lyhyitä kuvauksia niistä aiheista, joita video käsittelee, vastaa hyvin metatiedon käsitettä, koska se auttaa järjestelemään ja luokittelemaan tietoa, vaikkakin se luodaan käyttäjän toimesta. Metatietoa ilmenee siis monella tasolla. Rautatasolla metatieto voi määritellä tiedon sijaintia tallennusmedialla ja abstraktilla tasolla se voi luokitella esimerkiksi videon aihealueita.

Lassila (1998) kertoo, että toisen ohjelman metatieto voi olla toisen ohjelman varsinaista prosessoitavaa tietoa. YouTube esimerkiksi käyttää sekä videon otsikkoa ja tageja videon indeksoimiseen hakuja varten. Myös ns. tilastollinen tieto, joka kertoo esimerkiksi käyttäjän virtuaalikoneen prosessorin ja muistin kuormittamisesta voidaan nähdä olevan metatietoa pilvipalveluissa. Tällaista tietoa voidaan käyttää muun muassa käyttäjän laskuttamiseksi. Tiedot esimerkiksi käyttäjän virtuaalikoneiden instansseista PaaS- ja IaaS-palveluissa voidaan myös luokitella olevan metatietoa.

Reed (2010) lähestyy metatiedon määritelmää toisella tavalla: Hänen yhtenä tutkimuskysymyksenään on se, luovatko pilvipalvelut uudenlaista informaatiota, ja jos sellaista informaatiota syntyy, kuka, ja millä perustein tieto omistetaan? Reed lähestyy metatiedon ja varsinaisen sisällön erottelun ongelmaa ajatusleikillä 1930-luvun teknologiaa hyödyntävästä yrityksestä, jolle hän antaa nimen ”Efficient Office Company” (EOC), joka matkii palvelukonseptillaan nykyajan pilvipalveluja. Tämä lähestymistapa vähentää hahmotusongelmia, jotka johtuvat pilvipalvelujen osittain abstraktista luonteesta. Reed (2010) jaottelee nämä yrityksen käyttämät tietotyypit neljään luokkaan:

1. Dokumentit, jotka asiakas vastaanottaa ja jotka ovat sen jälkeen EOC:n säilytyksessä.

2. Dokumentit, joita EOC lähettää asiakkaan puolesta vastaanottajille.

3. Dokumentit, joita EOC luo palvelunsa osana – esimerkiksi kopiot lähetetyistä viesteistä.

4. Tietoa, jota EOC tuottaa omiin tarkoituksiinsa, esimerkiksi laskutusta varten.

Ensimmäisenä mainitut dokumentit ovat Reed (2010) mukaan yksiselitteisesti asiakkaan omistamia. Toisena mainittuja hän pitää vastaanottajan fyysisenä omaisuutena. Fyysisellä omaisuudella viitataan tällöin omistusoikeuteen, kun taas tekijänoikeudet lähetetyistä viesteistä kuuluvat Reedin mukaan asiakkaalle itselleen. Reed (2010) esittää, että kolmantena mainitut dokumenttien kopiot voivat olla palveluntarjoajan fyysisessä hallinnassa, mutta nämä dokumentit ovat kuitenkin oletettavasti asiakkaan omistusoikeuden alaisia, jolloin asiakkaalla on oikeus vaatia näitä dokumentteja itselleen, jos asiakassuhde palveluntarjoajan kanssa päättyy. Viimeisenä Reed (2010) käsittelee tietoa, jota voidaan pitää metatietona. Tässäkin tapauksessa metatieto syntyy siis tavallaan oheistuotteena varsinaisen sisällön oheistuotteena. Metatiedolla voidaankin harkita olevan lähes aina jonkinlainen isyyssuhde sen tiedon tai toiminnan kanssa, jota se on muodostunut kuvailemaan. Reed (2010) argumentoi, että tämä metatieto kuuluu kylläkin EOC:lle, mutta EOC:n tulisi ottaa huomioon, että tätä tietoa ei pitäisi luovuttaa kellekään kolmannelle osapuolelle, jos asiakas on siitä pääteltävissä.

Esimerkiksi Surden (2013) mainitsee Yhdysvalloissa käytetyn liiketoimintasalaisuuksia suojaavan lain, joka suojaa liikesalaisuuksia asiattomalta liiketoimintatietojen kuten tuotantoprosessien ja kemiallisten kaavojen urkkimiselta. Tämä laki siis suojaa tiedon luottamuksellisuutta vain niin pitkään, kuin se pysyy liikesalaisuutena. Tämä osoittaa sen, että tiedon luottamuksellisuutta voidaankin

pitää omistusoikeuden ja immateriaalioikeuksien lisäksi kolmantena oleellisena ominaisuutena, jota asiakas haluaa varjella, kun hän lataa sisältöä pilvipalveluun. Pearson (2009) mainitsee yksityisyyteen liittyviä tietoja, joita tulisi ottaa huomioon pilvipalveluja suunnitellessa, tai kun niiden käyttöönottoa harkitaan. Näen, että näistä Pearson (2009) mainitsemista seikoista kolme on relevantteja pilvipalvelujen tietojen yksityisyyden kannalta:

> 1. Henkilötietoja, joita voidaan käyttää tunnistamaan tai paikantamaan henkilö tai tietoa, jota voidaan yhdistää muun tiedon kanssa henkilön tunnistamiseksi kuten luottokorttitiedot, IP-osoite ja postinumero.
>
> 2. Käyttötietoja, joita on kerätty esimerkiksi laitteista kuten tulostimista ja tietoja käyttäjien käyttäytymisestä esimerkiksi verkkosivuilla.
>
> 3. Laitteiden tunnistamiseen tähtääviä tietoja, joilla voidaan tunnistaa jokin tietty laite, kuten IP-osoitteet, RFID-tiedot, tai vain tiettyä laitetta koskeva tunnistustieto.

Edellä käsitellyt tiedon ominaisuudet voidaan luokitella noin kolmeen eri osa-alueeseen: Tiedon omistusoikeus, tietoon sisältyvät immateriaalioikeudet ja tiedon luottamuksellisuus tai yksityisyys. Näitä kolmea ominaisuutta voidaan pitää pilvessä esiintyvän tiedon kolmena eri arvona, jotka voivat esiintyä yhdessä tai erikseen.

Palveluntarjoajalla on kuitenkin intressejä hyödyntää metatietoa muun muassa taloudellisten syiden sekä oman palvelunsa suorituskyvyn parantamisen vuoksi. Muun muassa Patibandla, Kurra ja Mundukur (2012) mainitsevat, että pilvipalvelujen tarjoajien yksi vakionomainen ansaintamalli on toissijaisen tiedon hyväksikäyttö. Yksi yleisimmistä toissijaisen tiedon käyttötavoista on mainosten kohdentaminen avainsanojen avulla. Patibandla ym. (2012) myös kuitenkin mainitsevat, että tämä toissijainen tiedon käyttö voi olla asiakkaan tahdon vastaista. Tällaista tahdon vastaista tiedon käyttöä voi olla esimerkiksi yritysasiakkaan myyntitietojen jälleenmyynti kilpailijoille. Pearson (2009) mainitsee myös omassa artikkelissaan myyntitietojen analysoinnin. Pearson pitää riskinä esimerkiksi Salesforce.com:n tarjoamien myyntitietojen keskittämiseen tähtääviä palveluja, koska kyseisiä tietoja voidaan varastaa vihamielisten tunkeilijoiden toimesta, ja näitä tietoja – kun ne sisältävät asiakasdataa – voidaan myydä esimerkiksi kilpailijoille tai identiteettivarkaille. Pearson ei mainitse palveluntarjoajia itseään riskinä, mutta lienee syytä harkita palveluntarjoajankin motivaatioita käyttää asiakkaansa tietoa tällä tavoin.

Pearson (2009) mainitsee myös räätälöidyn käyttäjäkokemukseen liittyvän tiedonkeruun, jonka avulla käyttäjälle voidaan tarjota juuri hänelle relevanttia sisältöä, kuten tietoa esimerkiksi siitä, ketkä käyttäjän kavereista ovat lähistöllä. Tällaisten ominaisuuksien tarjoaminen voidaan nähdä yhtenä argumenttina siitä, miksi pilvipalveluntarjoajat käyttävät niin laajoja käyttöehtoja kuin edellä mainittiin.

Myös Bradshaw, Millard ja Walden (2011) mainitsevat, että ns. ”ilmaiset” palvelut saattavat asettaa ei-rahallisia kustannuksia asiakkaalle, kuten kontekstuaalisen mainonnan tarjoaminen, tai jopa käyttöehtoja, jotka mahdollistavat asiakkaan tiedon uudelleenkäytön.

Bradshaw ym. (2011) esittelevät myös toisenlaista metatiedon käyttöä, jota palveluntarjoajat harjoittavat. Tämä on asiakkaiden toiminnan valvonta niin, että palveluntarjoaja voi käyttöehtojen mukaan seurata esimerkiksi asiakkaan verkon käyttöä. Artikkeli mainitsee tämän lisäksi kaksi muuta syytä: tilastollisen analyysin, jota Microsoft harjoittaa käyttöehtojensa mukaan SQL Azure -tietokannoissaan. Artikkeli ei lähde tarkemmin kuvailemaan mitä tämä tilastollinen analyysi tarkoittaa – ehto onkin melko häilyvä. Artikkeli mainitsee kolmanneksi syyksi asiakkaiden valvonnalle käyttöehtojen vastaisten toimien seuraamisen. Bradshaw ym. (2011) mukaan usein käyttöehdoista ei käy ilmi, onko tämä valvonta ennakoivaa, vai tapahtuuko sitä vasta, kun epäillään, että käyttöehtoja olisi rikottu.

3.2 Tiedon ja lisenssien siirreltävyys

Lock-in merkitsee pilvipalveluissa asiakkaan vaikeutta siirtyä toisen kilpailevan palvelun käyttöön tiedon tai sovellusten huonon siirrettävyyden vuoksi. Pilvipalveluissa on vielä nykypäivänä puutetta yhteensopivuusstandardeista. Kilpailevat pilvipalveluiden tarjoajat kehittävät omia de facto -standardeja. Tästä johtuvia rajoitteita on muun muassa se, että pilvipalveluilla ei ole yhteisesti hyväksyttyjä dataformaatteja tai standardimuotoista tapaa keskustella keskenään. Tästä johtuen pilvipalvelusta toiseen siirtyminen tai pilvipalveluun varastoidun tiedon tuominen asiakkaan oman verkon sisälle prosessoitavaksi voi olla vaikeaa (Pearson, 2013.).

Armbrust ym. (2009) toteavat, että pilvipalvelujen käytössä olevat rajapinnat ovat toimittajastandardien vallitsemia, eli eivät avoimesti hyödynnettäviä. Tämä johtaa siihen, että asiakkaat eivät voi Armbrust ym. (2009) mukaan helposti ottaa omaa dataansa ja sovelluksia ulos tietystä pilvipalvelusta ja siirtää sitä käyttökelpoiseen muotoon muualle. Tällainen toimintatapa on houkuttelevaa palveluntarjoajille. Asiakkaan lukittuminen tietyn omistajan standardin alle tekee asiakkaan haavoittuvaiseksi palveluntarjoajan toiminnan lopettamiselle. Armbrust ym. (2009) mainitsevatkin tämän argumentin tukemiseksi esimerkin ”The Linkup” -nimisestä pilvipalvelusta joka tarjosi tallennustilaa. Tämä pilvipalvelun tarjoaja onnistui menettämään jopa 45 % asiakkaiden datasta. Tämä palveluntarjoaja taas käytti toista palveluntarjoajaa varsinaisen tiedon varastoimiseen. Armbrust ym. (2009) argumentoivatkin, että jos tällaisen pilvipalvelun tarjoaja käyttäisi standardeja rajapintoja, olisi sen helpompi hajauttaa tieto useaan kolmannen osapuolen pilvipalveluun varmistaakseen tiedon eheyden. Armbrust ym. (2009) mainitsevat lopuksi vielä sen, että rajapintojen standardisointi mahdollistaa kuormantasausta, koska samaa ohjelmistoinfrastruktuuria voitaisiin käyttää sekä yksityisessä että julkisessa pilvessä. Tämä voidaan nähdä viittaavan esimerkiksi siihen, että organisaatio voisi käyttää ulkoista palveluntarjoajaa oman yksityisen pilven kuorman tasaamiseen, jos standardit sen mahdollistaisivat.

Jaeger ym. (2008) esittelevät hypoteesia, joka liittyy kuormantasaukseen. He argumentoivat, että alueittain muuttuva lainsäädäntö vaikeuttaa kuormantasauksen hyödyntämistä. Tässä hypoteesissa he vertaavat kuormantasausta nykypäivän sähköverkkojen kuormantasaukseen. Jaeger ym. (2008) esittelevät tilanteen, jossa kuormantasauksesta voisi olla hyötyä: Palveluntarjoajalla ei ole enää kapasiteettia palvella omia asiakkaitaan esimerkiksi huippukuormituksen aikana. Tämä palveluntarjoaja voisi olla sopimuksessa toisen palveluntarjoajan kanssa, joka tarjoaa omia resurssejaan alkuperäisen palveluntarjoajan asiakkaalle rajallisella aikamääreellä. Juurikin tällaisessa tilanteessa edellä mainittu standardisointi hyödyttäisi kutakin osapuolta. Tällainen standardisointi yltäisi tässä esimerkissä myös teknisten standardien lisäksi yhteiseen lainsäädännölliseen pohjaan.

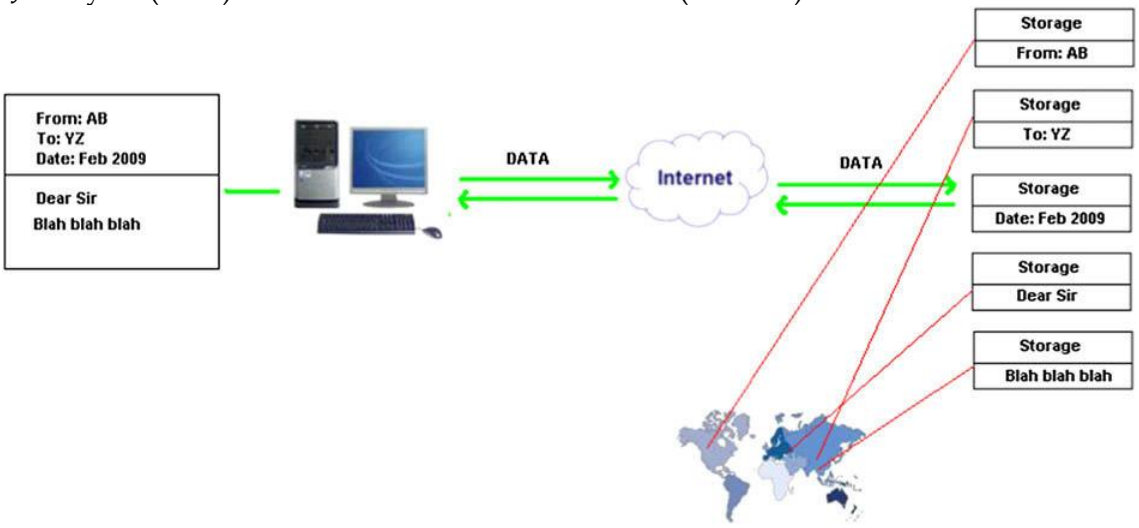
Jaeger ym. (2008) tuovat kuitenkin esille ongelman, jota olen jo esitellyt, eli käyttäjien tiedon hyödyntäminen palveluntarjoajien toimesta. Tässä esimerkissä palveluntarjoaja antaisi siis asiakkaan tietoja – mahdollisesti ilman mitään ilmeistä varoitusta – kolmannelle osapuolelle mahdollistaakseen kuormantasausta. Tällöin siis toistuvat ongelmat muun muassa käytönvalvonnasta ja metatiedon hyödyntämisestä. Cunningham ja Reed (2013) siteeraavat tähän liittyen sopimattomista elinkeinoharjoittajien ja kuluttajien välisistä kaupallisista menettelyistä sisämarkkinoilla annettua Euroopan parlamentin ja neuvoston direktiivin 2005/29 artiklaa 5 ja 6, joissa käsitellään muun muassa tuotteen koostumusta ja kelpoisuutta ja niiden totuudenmukaista esittämistä asiakkaalle. He tuovat esille näihin artikloihin liittyviä argumentteja asiakkaan tosiasiallisesta tietämyksestä pilvipalveluista ja niiden rakenteesta. Cunningham ja Reed siis esittävät, että pilvipalvelualan yksi yleisistä tavoista on ”teettää alihankintana” joitain osia pilvipalvelusta. Tällöin asiakas hankkii PaaS-palvelun ja palvelun toimittaja hankkii alihankintana esimerkiksi IaaS-puolen eli ”perustan” asiakkaalle tarjotusta PaaS-palvelusta. Tällöin Cunningham ja Reed (2013) mukaan voi olla vaikeata esittää kuka on tosiasiallisesti vastuussa palvelun luotettavuudesta. Tämän lisäksi voi olla vaikeata antaa tarkkaa kuvaa palvelun rakenteesta asiakkaalle. Näiden syiden johdosta voidaan jopa kyseenalaistaa voiko pilvipalvelun tarjoaja tehdä väitteitä palvelun kelpoisuudesta markkinoitua tarkoitusta varten. Tästä voidaan tehdä johtopäätös, että pilvipalvelun tarjoajan tulee esittää asiakkaalle selonteko palveluntarjoajan käyttäessä jonkinlaista alihankintaa tai kuormantasausta, joka hyödyntää kolmansien osapuolien kapasiteettia, koska se voi esimerkiksi johtaa asiakkaan tietojen tilapäiseen luovutukseen kolmannelle osapuolelle.

Pilvipalveluihin saattaa kuulua jo olemassa olevia lisenssejä ns. normaaleihin sovelluksiin. Koska esim. PaaS- ja IaaS-palveluissa virtuaalikoneissa voidaan ajaa sovelluksia, joihin kuuluu lisenssiehtoja, voi olla kiinnostavaa harkita miten nämä lisenssiehdot pätevät pilvessä virtuaalikoneissa pyöritettäviin sovelluksiin. Jaeger ym. (2008) kirjoittavatkin juuri tästä kysymyksestä. He mainitsevat, että ohjelmistolisenssit yleensä kieltävät jälleen jakamisen. Heidän mielestään onkin kiinnostava kysymys, voidaanko ohjelmiston käyttämistä pilvessä mieltää jälleen jakamiseksi. Tieto ja sovellukset saatetaan lähettää kolmannelle osapuolelle eli pilvipalveluntarjoajalle, mutta pilvipalveluntarjoaja ei varsinaisesti käytä

näitä lisensoituja sovelluksia. Armbrust ym. (2009) taas listaavat eri syitä, miksi jokin yritys saattaa ryhtyä pilvipalveluntarjoajaksi, mistä yksi on ns. olemassa olevan tuotteen tai brändin aseman puolustaminen. Armbrust ym. väittävät – tosin lähteettä – että Microsoft Azure tarjoaa polkuja jo olemassa oleville yritysasiakkaille siirtyä pilvipalveluiden käyttöön. Osana tällaista olemassa olevien tuotteiden aseman puolustamista voidaan esimerkiksi pitää Microsoftin pilvessä toimivaa Office 365:ä, jolla yritys pyrkinee pitämään kiinni olemassa olevista Office-käyttäjistään ja houkuttelemaan esimerkiksi Google Docs -käyttäjiä siirtymään Microsoftin tuotteiden pariin.

3.3 Tiedon fyysinen sijainti

Pilvipalvelussa varastoitava tieto voi olla varastoituna useaan eri paikkaan. Tämä asettaa tiedon omistusoikeudelle erilaisia haasteita, jotka johtuvat muun muassa siitä, että pilvipalveluissa varastoitu tieto voi ylittää eri valtioiden rajoja, ja eri maissa saatetaan pilvipalveluihin soveltaa erilaista lainsäädäntöä. Pilvipalveluun varastoitu tieto voi olla varastoituna myös useaan eri paikkaan samanaikaisesti, tai yksi tiedon entiteetti kuten tiedosto voi olla varastoituna sirpaloituneesti. Joint, Baker ja Eccles (2009) mainitsevatkin, että pilvipalveluntarjoajien tapa varastoida tietoa saattaa johtaa siihen, että yksi tiedosto tai tietorakenne voi olla sirpaleinen. Tiedoston eri paloja voi olla siis varastoituna samanaikaisesti eri paikkoihin. Joint ym. (2009) väittävät, että sen päättely, missä tiedoston osat ovat voi olla vaikeaa riippuen käytetystä järjestelmästä. Huomionarvoista on, kuten Joint ym. (2009) mainitsevatkin, että tämä sirpaloituminen voi olla edullista tietoturvan suhteen, koska yksi sijainti ei sisällä kokonaiskuvaa asiakkaan varastoimasta tiedosta, vaikka se ei yksinään varsinaista riittävää tietoturvaa tarjoaisikaan. Joint ym. (2009) havainnollistavat tätä kuvalla. (kuvio 1).



KUVIO 1 Pirstaloitunut tieto (Joint ym., 2009).

Svantesson ja Clarke (2010) esittävät, että pilvipalvelun tarjoajat asettavat itsensä alttiiksi kaikkien maiden lainsäädännölle, joissa ne toimivat. Onkin kyseenalaista, onko pilvipalvelutarjoajien edes mahdollista noudattaa kaikkien niiden alueiden lainsäädäntöä, missä palveluntarjoajien asiakkaat sijaitsevat.
Svantesson ja Clarke (2010) jakavat pilvet yhden maan pilviksi ja rajojen ylittäviksi pilviksi. Yhden maan pilvi sijaitsee fyysisesti nimenomaan yhdellä alueella, kun taas rajojen ylittävät pilvet voivat sijaita usealla eri lainsäädäntöä noudattavalla alueella. Svantesson ja Clarke (2010) mainitsevat, että monessa eri lainsäädännössä erotellaan nimenomaan organisaatioiden välistä tiedonsiirtoa maantieteellisten seikkojen sijasta. Tällöin lainsäädäntö ei välttämättä rajoita yhden organisaation kuten pilvipalvelutarjoajan toimintaa joka sijoittaa asiakkaan tietoa eri lainsäädäntöä noudattaville alueille. Toisaalta, tietynlainen tieto saattaa olla tiukemman lainsäädännön alaista. Svantesson ja Clarke (2010) siteeraavatkin Australian lainsäädäntöä ja sitä, miten 1988 säädetty yksityisyyslaki kattaa Australian ulkopuolisia alueita ainoastaan, kun seuraavat kaksi ehtoa täyttyvät:

> 1. Tieto käsittelee Australian kansalaista tai henkilöä Australiassa, jonka oleskelulle Australiassa ei ole asetettu minkäänlaista ajallista rajoitetta.
>
> 2. Organisaatio joka käsittelee tätä henkilötietoa omaa vahvan siteen Australiaan, esimerkiksi tekemällä liiketoimintaa Australiassa.

Kuitenkin Svantensson ja Clarke (2010) mainitsevat, että kun lainsäädäntö pyrkii toteuttamaan itseään valtion rajojen ulkopuolella, voi sen toteutus osoittautua vaikeaksi, ellei mahdottomaksi. Käyttäjille asettaa haasteita muun muassa eri valtioiden tiedusteluelimien ja tuomioistuimien kiinnostus käyttäjän tiedoista ja ladatusta sisällöstä. Jaeger, Lin, Grimes ja Simmons (2009) mainitsevat julkaisussaan PATRIOT Act:n mahdollistaman tiedonkeruun, jonka avulla valtio voi painostaa palveluntarjoajia luovuttamaan tietoa käyttäjistä. Jaeger ym. (2009) huomioivat myös niin kutsutun lakishoppailun: pilvipalvelutarjoajilla voi olla intressejä toimia alueilla, joissa lait eivät rajoita pilvipalveluntarjoajien toimintaa tiedonkeräyksen osalta. Jaeger ym. (2009) mainitsevatkin, että moni hallintoalue voi olla kiinnostunut asettamaan erityisen väljiä lakeja pilvipalvelujen tarjoajia kohtaan, jotta he voivat houkutella pilvipalveluntarjoajia omille hallintoalueilleen.

Sekä yritys- että yksityiskuluttajalle voi olla haastavaa ylipäätään hallinnoida maantieteellisistä seikoista koostuvia haasteita. Käyttäjäorganisaation jäsenet voivat olla yhdessä tai useassa eri maassa, palvelinkeskukset toisessa, ja pilvipalvelun palveluntarjoajan avainhenkilöt kolmannessa. Akateemiset artikkelit eivät yllätyksekseni edes käsitelleet sitä seikkaa, että pilvipalvelujen hallinnoijien sijainti voi olla jopa merkityksellisempää kuin itse varastoidun tiedon sijainti – koska näitä hallinnoijia voidaan painostaa esimerkiksi kotimaansa viranomaisten taholta. Ainakin joidenkin kuluttajien mielestä tiedon hallinnoijien sijainnilla on ratkaisevaa merkitystä: F-Secure myi oman SaaS-pohjaisen, Younited-nimisen pilvitallennuspalvelunsa yhdysvaltalaiselle Synchronos-nimiselle yritykselle. (Toivonen, 2015). F-Secure kertoi lisää myynnistä omilla keskustelu-

palstoillaan, joilla mainitaan, että pilvipalvelun tiedot eivät poistu heidän eurooppalaisesta pilvestään. (F-Secure, 2015). Ilmeisesti F-Secure ei nähnyt tarpeelliseksi keskustelupalstan viestien perusteella informoida asiakkaitaan myynnistä heti sähköpostin avulla. Myös digitoday otti yhdysvaltalaisen yrityksen osallistumisen F-Securen pilvitallennuspalveluun puheeksi omassa artikkelissaan. (Kärkkäinen, 2015). Onkin siis ilmeistä, että asiakkaat näkevät ehkä syystäkin merkittäväksi sen, missä tiedon hallinnoijat sijaitsevat.

3.4 Lainsäädäntö ja käyttöehdot

Kaiken uuden teknologian saralla kohdataan ongelmia lainsäädännön muuttumisen hitauden vuoksi. Koska lainsäätäjät eivät pysty reagoimaan teknologiseen muutokseen tarpeeksi nopeasti tai ymmärrä teknologisen muutoksen vaikutuksia, saattaa myös pilveen liittyviin omistus- ja immateriaalioikeuksiin liittyä paineita, jotka sotivat perinteisiä käsityksiä vastaan, koska säädetyt lait eivät toimi tarkoituksenmukaisesti.

Surden (2013) esittelee teknologisen kustannuksen termin, joka kuvaa miten jotkin teknologiset rajoitteet ovat rajoittaneet kopioinnin edullisuutta. Tämä termi on Surdenin mukaan tärkeä, koska teknologinen muutos vaikuttaa esimerkiksi tekijänoikeuslakeihin. Omistusoikeuteen ja immateriaalioikeuteen liittyviä lakeja laadittaessa saatetaan olettaa, että tietyn suuruiset teknologiset kustannukset ovat voimassa. Teknologian kehittyessä nämä kustannukset saattavat alentua triviaalin suuruisiksi, jolloin alkuperäiset immaterialioikeuteen liittyvät lait saattavat muuttua vaikutuksiltaan. Surden (2013) havainnoikin tätä kuvailemalla tutkijoille tarkoitettua periaatetta, jossa tutkijoilla on mahdollisuus kopioida kirjastossa olevia kirjoja tutkimuskäyttöön. Tätä periaatetta laadittaessa on todennäköisesti oletettu tutkijan pystyvän ottamaan vain rajallisen määrän kopioita rajallisesta määrästä materiaalia sen vuoksi, kuinka työlästä kopiointi periaatetta noudattaessa oli. Voidaankin potentiaalisesti olettaa, että teknologisten rajoitteiden vuoksi on oletettu kopioinnin määrän olevan rajallinen. Surden (2013) kertoo, että usea eri akateeminen tutkija on todennut, että tekijänoikeuksiin liittyvä tasapaino muuttui huomattavasti 1990-luvulla, kun luovat työt siirtyivät analogisesta muodosta digitaaliseen.

Robison (2010) esittelee omassa artikkelissaan esimerkin siitä, kuinka lainsäädäntö ei monesti toimi loogisesti pilvipalvelualalla. Robison analysoi yhdysvaltalaista Stored Communications Act:a, joka säädettiin vuonna 1986. Siinä määritellään kaksi palvelua, joita tällä lailla halutaan säädellä:

1. Elektroniset kommunikaatiopalvelut (Electronic communication services), jotka käsittelevät tiedon välitystä ja elektronista postia.

2. Etänä käytettäviä tiedonkäsittelypalveluita (remote computing services), jotka tarjoavat ulkoistettua tiedon varastointia ja prosessointia.

Robison (2010) siis ilmaisee, että kongressi päätti, että näille kahdelle palvelutyypille sovelletaan erilaisia yksityisyysperiaatteita. Elektroniset kommunikaatiopalvelut ovat palveluita, jotka tarjoavat käyttäjilleen mahdollisuuden lähettää tai vastaanottaa elektronista kommunikaatiota, ja niiden täytyy pitää niitä elektronisessa säilössä, joka on väliaikainen, ja sen tarkoitus on mahdollistaa viestien lähetys ja kopiointi varmuuskopioita varten. Etänä käytettävät tiedonkäsittelypalvelut taas merkitsevät kolmansien osapuolten tarjoamia palveluja jotka tarjoavat hienostuneita tiedonkäsittelypalveluita asiakkaille etänä. Jotta palvelu voidaan luokitella etänä käytettäväksi tiedonkäsittelypalveluksi, sen täytyy täyttää seuraavat ehdot:

1. Palveluntarjoajan tulee tarjota tallennustilaa tai tiedonkäsittelypalveluita yleisölle elektronisen kommunikaatiokanavan kautta.

2. Tieto täytyy vastaanottaa elektronisesti asiakkaalta.

3. Palveluntarjoaja saa ylläpitää tai kantaa sisältöä vain sitä tarkoitusta varten, että palveluntarjoaja pystyy tarjoamaan tallennustilaa ja tiedonkäsittelypalveluita asiakkaalle.

4. Palveluntarjoajalla ei tule olla lupaa päästä asiakkaan sisältöön mitään muuta tarkoitusta kuin tallennuspalveluiden ja tiedonkäsittelypalveluiden tarjoamista varten.

Robison (2010) kertookin, että elektronisille kommunikaatiopalveluille on asetettu löyhemmät tietosuojaperiaatteet verrattuna elektronisiin tiedonkäsittelypalveluihin. Mielestäni lainsäädäntö selkeästi kuvaa vanhentunutta ajattelua muun muassa sen takia, koska tietosuojakäytänteet voivat joidenkin tulkintojen mukaan muuttua sen perusteella, onko sähköposti esimerkiksi luettu vai ei.

Kiinnostavampi kysymys lienee kuitenkin se, että kontekstuaalinen mainonta voidaan nähdä olevan ristiriidassa etänä käytettävien elektronisen tiedonkäsittelypalveluiden kolmannen ja neljännen edellytyksen kanssa. Robison (2010) argumentoikin, että näiden kahden periaatteen vuoksi kontekstuaalista mainontaa tarjoavia pilvipalveluita ei voida pitää etänä käytettävinä elektronisina tiedonkäsittelypalveluina. Voidaan myös olettaa, että kaikenlaista tiedonlouhintaa saatetaan pitää näiden edellytysten vastaisina.

Robisonin (2010) tekemät päätelmät ja hänen määrittelemänsä teknologisen kustannuksen termi osoittavat, että on luonnollista, ellei lähes väistämätöntä, että vanha lainsäädäntö ei välttämättä noudata lain alkuperäistä henkeä. Tosin tilanne voi joskus olla jopa edullinen pilvipalveluja käyttävän tiedon omistajan kannalta. Voidaan myös kysyä, onko lainsäädännön vanhentuminen ja sen muuttumattomuus uhkana varsinkin yksityiskäyttäjille, joilla ei välttämättä ole samanlaista mahdollisuutta painostaa tai lobata lainsäätäjiä kuin esimerkiksi suuryrityksillä?

Yksityisillä asiakkailla ja organisaatioilla on epäyhtäläinen mahdollisuus neuvotella pilvipalveluihin liittyvien sopimusten ehdoista. Yksityiset asiakkaat joutuvat hyväksymään yleensä ns. yhtenäissopimuksia jotka ovat valmiiksi luotuja. Koska pilvipalvelujen käyttöehdot ovat itsekin Internetissä, palveluntarjoajalla voi olla pienempi kynnys muuttaa niitä. Bradshaw ym. (2011) kirjoittavatkin käyttöehtojen muuttumisesta, ja siitä, miten jotkin palveluntarjoajat eivät

välttämättä tiedota käyttöehtojen muuttumisesta esimerkiksi sähköpostitse. Jotkin palveluntarjoajat eivät edes mainitse, mikä luetaan käyttöehtojen muuttumisen hyväksymiseksi ja miten palveluntarjoajat mahdollisesti tiedottavat muutoksesta. Bradshaw ym. (2011) toteavatkin, että vain kolme heidän tutkimuksessaan ollutta pilvipalveluntarjoajaa mainitsee, että muutokset käyttöehtosopimukseen tulee hyväksyttää kirjallisesti molemmilla sopimuksen osapuolilla. Se, että käyttöehdot eivät ole kirjoitettuna muuttumattomina paperilla saattaa aiheuttaa asiakkaalle haasteita käyttöehtoihin liittyvään riskien hallintaan.

Pilvipalvelut määrittelevät yleensä käyttöehdoissaan lainkäyttöalueen, jonka lakien mukaan esimerkiksi kanteet tulisi antaa. Lainkäyttöalueella on yleensä jokin maantieteellinen sidonnaisuus esimerkiksi pilvipalveluntarjoajan pääkonttoria kohtaan. Kuitenkin tällaisia käyttöehtoja voidaan pitää epäreiluina, koska ne rajoittavat käyttäjän mahdollisuuksia oikeudellisiin toimiin palveluntarjoajaa vastaan. Asiakkaan lainkäyttöalueella toimivat tuomioistuimet voivatkin pitää tällaisia käyttöehtoja epäreiluina ja määrätä mahdollisen käyttöehtosopimuksen ainakin niiltä osin pätemättömäksi. (Cunningham ja Reed, 2013.).

3.5 Tiedon yhdistely ja uudelleenkäyttö

Google Books on esimerkki siitä, mitä nykyaikaisella järjestelmällä saadaan aikaan, ja minkälaisia immateriaalioikeuksiin liittyviä haasteita sellainen järjestelmä voi tuoda esille. Surden (2013) kertoo, että Google teki yhteistyötä monen suuren yliopiston kirjaston kanssa muuntaakseen näiden kirjastojen kirjat digitaaliseen muotoon. Google käytti optisia skannereita skannatakseen miljoonien kirjojen jokaisen sivun, ja nämä sivut muutettiin digitaaliseksi optista merkinlukua käyttäen. Tämä mahdollistaa minkä tahansa tekstinpätkän etsimisen Google Books:n tietokannasta löytyvästä kirjasta. Google käyttää näyttäessään hakutuloksia ns. ”reilun käytön” periaatetta, jossa tekijänoikeudella suojatusta teoksesta voidaan näyttää rajattuja katkelmia ei-kaupallista käyttöä varten. Googlen tämän periaatteen käyttö niin laajassa muodossa aiheuttaa epäilyksiä, vastaako Googlen periaatteen noudatus reilun käytön periaatteen alkuperäistä tarkoitusta. Myös Jaeger ym. (2008) mainitsevat, että Google Booksin kaltaiset projektit pystyvät jatkamaan lainsäädännöllisen epävarmuuden vuoksi – Eli he väittävät, että Google on voinut kehittää palvelua osittain pienentyneen teknologisen kustannuksen vuoksi, ja koska tällainen massiivinen kopiointi ja tiedon näyttäminen eivät ole tulleet harkituksi lainsäädännössä.

Marston ym. (2011) esittelevät termin ”mashup”, jota käytetään kuvailemaan yhdistettyä sisältöä monesta lähteestä web-kehityksessä. Yhdistetyn sisällön ideana on pilvipalvelujen mahdollistaman sisällön yhdistely useasta ulkoisesta lähteestä tavalla, joka eroaa niiden alkuperäisestä tarkoituksesta. Mashup voisi olla esimerkiksi web-palvelu, joka yhdistelee tekstipohjaisia bussiaikataulutietoja graafiseen käyttöliittymään ja hakupalveluun. Jotkin organisaatiot jopa

vapauttavat sellaista tietoa, joka on ideaalia mashup-palveluiden käyttöön. Esimerkiksi Suomen maanmittauslaitos jakaa vapaasti osaa tiedoistaan. (Maanmittauslaitos, 2015) Tällainen toiminta voi olla kuitenkin ongelmallista. Mainitsin jo aiemmin Lemley ym. (2006) artikkelin, joka käsittelee erilaisia käyttöehtoja. Jotkin web-sivujen ylläpitäjät sisällyttävät eri tavoin käyttöehtoja esimerkiksi verkkosivujensa yhteyteen, jolla he yrittävät välttää verkkosivujensa materiaalin uudelleenkäytön. Näillä materiaalin omistajilla voi olla perusteltu syy kieltää sisällön uudelleenkäyttö. Lemley ym. (2006) tuovat esimerkkinä tapauksen, jossa tapahtumiin lippuja myyvä verkkosivu tarjosi linkkejä kilpailevaan palveluun, kun asiakas yritti etsiä lippuja tapahtumiin, joihin kilpailevalla palvelulla oli yksinoikeus. Vaikka kilpaileva palvelu tiesi, että se sai lippumyyntituloja toisen palvelun suoran linkittämisen välityksellä, päätti se kieltää tämän linkittämisen sillä perusteella, että linkittävän palvelun markkinaosuus saattaisi pienentyä.

Lemley ym. (2006) mainitsevat myös, että alkuperäisen tiedon omistajat saattavat yrittää estää sen tietoja käyttäviä toisia organisaatioita pääsemästä omistajien verkkosivuilla säilytettyyn tietoon teknisten keinojen avulla – varsinkin, jos tietoa hyödyntävä organisaatio käyttää tiedon keräämiseen automaattisia keinoja. Kun tiedon kerääjä yrittää kiertää näitä keinoja, voidaan olettaa tiedon kerääjän olevan tietoinen siitä, että tiedon omistaja vastustaa tiedon keräystä. Siten tällainen tekninenkin estäminen voi joissain oikeusistuimissa omata myös oikeudellisen puolen.

Lemley ym. (2006) huomasivat artikkelissaan, että tuomioistuimet Yhdysvalloissa näyttivät tuomitsevan tapauksia niin, että käyttöehtojen ei katsottu sitovan kuluttajaa niin usein kuin toista yritystä.

Monilla kaupallisilla tiedon haltijoilla voikin olla intressejä kieltää kaikki oman tietonsa uudelleenkäyttö samanlaisista syistä, miksi moni yritys vahtii omia immateriaalioikeuksiaan ja tavaramerkkejään tarkasti. Vaikka jollekin tietylle tiedolle ei olisi juuri nyt käyttöä, niin luvan antaminen tiedon käyttöön voi johtaa siihen, että kaupallisella toimijalla ei ole enää mahdollista käyttää omaa yksinoikeuttaan hallitsemaansa tietoon taloudellisesti hyväksi. Esimerkiksi tutkijat saattavat siis kerätä tiedon pilvipalveluun, mutta vasta tiedon analysointi ja uudelleenkäyttö saattavat synnyttää tiedolle varsinaista arvoa.

3.6 Tiedon säilyvyys

Bradshaw ym. (2011) mainitsevat artikkelissaan, että tiedon säilyvyys pilvipalveluissa on kaksijakoinen ongelma: Yhtäältä asiakas haluaa, että hänellä on pääsy tietoon tietyissä tapauksissa jopa sopimuksen päätyttyä, tai vaikka palveluntarjoajan varsinaisesti lopetettua toimintansa esimerkiksi konkurssin takia. Toisaalta asiakas haluaa varmistaa, että palveluntarjoaja ei säilytä asiakkaan tietoja, kun sopimus palveluntarjoajan kanssa loppuu. Asiakas voi edellyttää tiedon poistumista palveluntarjoajan palvelimilta tiedon yksityisyyden, rahallisen arvon, tai muun merkittävän syyn takia. Bradshaw ym. (2011) löytävätkin niistä 25 pilvipalveluista, joita he tutkivat, kolme kategoriaa tiedon säilyvyyden suhteen.

1. Palveluntarjoajat jotka tarjoavat noin kuukauden verran aikaa, jonka aikana entinen asiakas pääsee käsiksi omiin tietoihinsa. Tämä varoaika saattaa olla voimassa ainoastaan, jos käyttöehtosopimusta ei ole rikottu asiakkaan osalta. Tämä varoaika saattaa myös sisältää maksuja noudetun tiedon säilytyksen ja siirron osalta asiakkaalle.

2. Palvelut, jotka kertovat, että kun pilvipalveluun liittyvä tili lopetetaan, asiakas menettää pääsyn palveluun ja kaikkeen siellä varastoituun tietoon.

3. Palvelut, jotka eivät takaa, että tiedostoja on olemassa, kun sopimus on päättynyt, mutta ei myöskään takaa, että tiedostot poistettaisiin palveluntarjoajan palvelimilta välittömästi.

Jotkin ilmaiset palvelut, joille ei ole asetettu sopimusaikaa, saattavat poistaa tiedot, jos käyttäjä ei ole käyttänyt palvelua tietyn aikavälin sisällä. Kuitenkin pilvipalveluiden tarjoajat harvoin vakuuttavat, että käyttäjän tiedot tuhotaan sopimuksen loputtua. Kalyvas ym. (2013) kertovat omassa artikkelissaan, että palveluntarjoajan ei tulisi evätä pääsyä pilvipalveluun perustuen esimerkiksi maksuihin liittyviin epäselvyyksiin, vaan ilmoittaa siitä asiakkaalle, ja jos asiakas ei korjaa asiaa, irtisanoa palvelu.

Asiakkaan tulisi perehtyä käyttöehdoissa mainittuihin seikkoihin tiedon säilyvyydestä. Yhtäältä asiakkaan tulisi varmistaa, että hänen on mahdollista noutaa omat tietonsa poikkeustilanteessakin, ja toisaalta varmistaa se, että palveluntarjoajalle ei jää asiakkaan ladattua tietoa asiakassuhteen loputtua – mahdollisesti esimerkiksi poistaen kaiken palvelussa olevan tiedon niitä menetelmiä noudattaen, jotka palvelulle parhaiten sopivat. IaaS- ja SaaS-palveluille tämä käytäntö on todennäköisesti hyvin erilainen. IaaS-palveluissa asiakkaan on todennäköisemmin mahdollista poistaa omat tietonsa hyvin matalalta tasolta lähtien johtuen virtuaalikoneiden tai palvelinten syvemmälle ulottuvasta hallinnasta.

3.7 Teknisiä riskejä ja mahdollisuuksia tiedon suojaamiselle

Pilvipalvelut pyörivät yleensä alustalla, joka muodostaa rautatasolla kokonaisuuden, jota käyttää usea asiakas. Englanniksi ilmiötä kuvaava sana multitenancy voitaisiin ehkä kääntää suomeksi ”monikäyttäjäisyys”. (Subashini & Kavitha, 2011.). Jaeger ym. (2008) kuitenkin mainitsevat, että käyttäjät olettavat, että he pääsevät itse käsiksi omiin tietoihinsa. Asiakas myös olettaa, että hän pääsee tietoonsa käsiksi milloin ja missä tahansa, kuitenkin niin, että palveluntarjoaja huolehtii siitä, että hänen immateriaalioikeutensa ovat turvattuja. (Jaeger ym., 2008.).

Bhadauria, Chaki, Chaki, ja Sanyal (2011) mainitsevatkin, että SaaS-palveluissa asiakas on riippuvainen siitä, että palveluntarjoaja toimii tietoturvan suhteen asiallisesti niin, että käyttäjät eivät näe toistensa tietoa. Tämä johtaa heidän

mukaansa siihen, että käyttäjän on vaikeata varmistaa, että käyttäjän pilveen lataama tieto on turvattua. Monikäyttäjäisyyden johdosta usea käyttäjä voi varastoida tietoa samassa paikassa. Tämä voi Bhadauria ym. (2011) mukaan mahdollistaa asiattoman pääsyn toisten asiakkaiden tietoihin. SaaS-palveluiden tulisikin heidän mukaansa varmistaa selkeä raja käyttäjien tiedoissa sekä rauta- että sovellustasolla.

Descher, Masser, Feilhauer, Tjoa ja Huemer (2009) kirjoittavat artikkelissaan, että pilvipalvelujen käytön huonoja puolia voidaan verrata kovalevyjen irrottamiseen omista palvelinkeskuksista ja niiden lähettämistä ulkoiselle palveluntarjoajalle. Heidän mukaansa siitä seuraa muun muassa se, että asiakkaan lataama tieto on manipuloitavissa, ja tiedon kontrolli poistuu – eli mahdollisten virtuaalikoneiden toiminta ja kommunikaatio ovat lopulta palveluntarjoajan hallinnassa. Descher ym. (2009) mukaan on olemassa useita projekteja jotka pyrkivät lisäämään turvallisuutta virtualisaatiossa, mutta pääkäyttäjällä eli palveluntarjoajan edustajalla on mahdollisuus rajoittamattomaan pääsyyn. Esimerkiksi Descherin siteeraama Sailer ym. (2005) tekemä IBM:n tutkimusportti paneutuu lähinnä eri virtuaalikoneinstanssien erottamiseen toisistaan ja välttämään niille liiallisten oikeuksien antamiseen siinä järjestelmässä missä ne pyörivät. Descher ym. (2009) mainitsevatkin, että palveluntarjoajiin luottaminen on yleinen käytäntö, ja kirjoittajat keskittyvät pilvipalveluresurssien koskemattomuuteen. He kuvailevat salattuun virtuaalikoneeseen pohjautuvaa menetelmää, jota ei voitaisi modifioida ilman virtuaalista avainta.

Ryan (2013) kertoo, että tiedon omistajan on mahdollista salata lähetettävä tieto, ennen kuin hän lataa sen pilveen. Kuitenkin normaalin salauksen kanssa tämä estää lähes kaikenlaisen tiedon modifioinnin, rajoittaen pilven käytön pelkästään tallennustilana toimimiseen. Homomorphinen salaus mahdollistaa Ryanin (2013) mukaan ainakin joidenkin operaatioiden tekemisen ladatulle tiedolle – jolloin tiedolle tehdyt operaatiot kääntyvät oikein myös salaamattomalle tiedolle, jolloin sillä on sama lopputulos molemmissa. Toinen Ryan (2013) kuvailema lähestymistapa on rautapohjainen turvallisuus, jossa varmistettaisiin asiakkaan tiedon yksityisyys käyttämällä erikoisvalmisteista rautaa käyttäjän tietojen isännöimiseksi. Nämä palvelimet toimisivat Ryan (2013) mukaan ainoastaan tietyn ohjelman kautta, josta asiakkaalla ja palveluntarjoajalla olisi sopimus. Asiakas lataisi ensin avaimen palvelimelle, mikä on sidottu tiettyyn ohjelmaan. Tämän jälkeen asiakas lataisi tiedon joka on salattu annetulla avaimella, jolloin palvelin voi käyttää sovittua ohjelmaa käsittelemään ladattua tietoa. Tämä ratkaisu toimisi ainoastaan sitä varten räätälöidyllä raudalla, joka estää tiedon käytön muilta kuin sovituilta ohjelmilta. Vaikka Ryan (2013) mainitseekin joitain konkreettisia esimerkkejä, hän myös toteaa, että edellä mainittuja periaatteita seuraavien ratkaisujen toteuttaminen on osoittanut hankalaksi, ja ne mahdollistavat vain melko yksinkertaisia operaatioita tiedolle. Sen lisäksi todellisen luottamuksen osoittaminen asiakkaalle voi osoittautua vaikeaksi.

Santos, Gummadi ja Rodrigues (2009) mainitsevat, että mitä kauempana pilvipalvelun alustatyyppi on IaaS-tasosta, sitä vaikeampi asiakkaan on varmis-

taa tiedon luottamuksellisuutta, koska SaaS-palvelut kuten Google Docs manipuloivat asiakkaan tietoa suoraan asiakkaan puolesta. IaaS-palveluissa asiakkaan tiedon turvaaminen on siis heidän mukaansa helpompaa, koska asiakas pääsee lähemmäksi palvelun rautapintaa. He keskittyvät artikkelissaan järjestelmänvalvojien tekemien hyökkäysten estämiseen – kuitenkin huomauttaen, että järjestelmänvalvojan ei oleteta tässäkään tapauksessa omaavan rajaamatonta pääsyä esimerkiksi pilvipalveluntarjoajan fyysiseen laitteistoon, jolloin heidän menetelmänsä ei nähtävästi toimisi asiakkaan tiedon turvaamisessa, jos palveluntarjoaja ei ole luotettava. Lindell ja Pinkas (2009) puhuvat kryptografiassa ilmenevästä turvallisesta, usean henkilön suorittamasta laskennasta, jossa ideana on se, että laskentaan osallistuvat osapuolet pystyvät vain päättelemään oikean tuloksen, mutta eivät edes tekemällä yhteistyötä pystyisi keräämään tietoa itse annetusta tiedosta. Tämä kryptografinen ongelma kuvailee tilannetta, jossa hajautetaan esimerkiksi yksi laskutoimitus tapahtuvaksi useassa ulkoisessa kohteessa. Tällaisten ongelmien ratkaisut voivat olla tähdellisiä myös pilvipalveluille.

Chen ja Zhao (2012) mainitsevat artikkelissaan tiedon salauksen. Heidän mukaansa avaimen vahvuus ja salaukseen käytetty algoritmi ovat tärkeitä tiedon turvallisuuden varmistamiseksi – kuitenkin huomioiden salattavan tiedon määrä. Toinen ongelma Chen ja Zhao (2012) mukaan on avainten hallinta. Vaikkakin ideaalissa maailmassa tiedon omistajat hallitsivat itse avaimia, monesti tiedon omistajilla ei ole tarvittavaa osaamista niiden hallitsemiseen, vaan niitä hallinnoivat yleensä pilvipalvelujen tarjoajat.

Tietojen salaamisen ideaali tilanne olisi se, että asiakas voisi kohtuullisen tai olemattoman haitan kustannuksella käyttää pilvipalveluja ainakin IaaS-tasolla turvallisesti. Tällä tarkoitetaan sitä, että tiedot jotka ovat palveluntarjoajan laitteilla, eivät olisi muunnettavissa selkokieliseen muotoon palveluntarjoajalle muuten kuin poikkeustilanteessa asiakkaan luvalla. Ryan (2013) artikkeli osoittaa, että tutkimusta alalla asiasta on, mutta ainakaan ns. täydellistä tiedon abstraktointia palveluntarjoajan näkökulmasta ei ole näkyvissä.

SaaS-sovellusten luotettavuus voisi ehkä parantua tarjoamalla käyttäjälle ulkoisen tahon validoima sovellus niin, että palveluntarjoaja ei voi muuttaa asiakassovelluksen toimintaa ilman jonkin puolueettoman tai luotettavan tahon hyväksyntää ja auditointia. Tämä mahdollistaisi esimerkiksi tietojen lähetyksen salatusti ja helppokäyttöisesti niin, että asiakas pystyisi luottamaan sovelluksen toimintaan joka salaisi tiedot ennen kuin se lähettää ne palveluntarjoajalle. Tällainen toiminta tosin mahdollistaa miltei ainoastaan vain laajennetun tallennustilan käytön pilvipalveluiden avulla.

4 YHTEENVETO

Tutkielman tarkoituksena oli etsiä, mitkä pilvipalveluille ominaiset piirteet vaikuttavat immateriaali- ja omistusoikeuksien määräytymiseen, ja mitä pilvipalvelujen potentiaalinen asiakas voi tehdä hallitakseen näitä oikeuksia. Käsittelen aluksi, mitä seikkoja tuli ilmi 3. luvussa kirjallisuuskatsauksen osalta, ja siirryn sen jälkeen pohtimaan näistä seuraavia johtopäätöksiä hieman syvemmin.
Metatiedon osalta tuli ilmi, että käyttäjän tulisi pohtia, miten palveluntarjoaja hyödyntää käyttäjää ja hänen tietojaan kuvailevaa metatietoa. Tähän metatietoon kuuluu arvoa, jota palveluntarjoajalla on intressi hyödyntää. Jos palvelu on ilmainen, on käyttäjän metatiedon hyödyntäminen todennäköisempää esimerkiksi kontekstuaalisen mainonnan johdosta. Tiedon hyödyntämisellä voi olla myös yllättäviä vaikutuksia esimerkiksi lainsäädännön tarjoamaan suojaan, kuten luvussa 3.4 tuli ilmi.

Pilvipalvelun käyttö esimerkiksi tietystä sijainnista tai tiettynä kellonaikana voi kertoa käyttäjästä tietoja, joita käyttäjä ei välttämättä halua paljastaa palveluntarjoajalleen. Käyttäjän tiedostoihin saattaa myös kuulua metatietoa, joka voi olla tärkeää esimerkiksi omistussuhteiden osoittamiseksi tai automaattisen tiedonkäsittelyn vuoksi. Käyttäjän tulisi pohtia miten pilvipalvelun metatiedot siirtyvät käyttäjän halutessa vaihtaa palvelua. Palveluntarjoajan tulisikin asiakkaan näkökulmasta varmistaa ns. varsinaisen sisällön lisäksi myös metatiedon säilyvyys. Chen ja Yoon (2010) suosittelevat, että asiakkaiden tulisi selvittää poistumisstrategia pilvipalvelusta.

Asiakkaan tulisi valita palveluntarjoaja sen perusteella, tarjoaako palveluntarjoaja helppoa tapaa saada kaikki asiakkaan tieto pilvipalvelusta pois sekä toisen pilvipalvelun hyödyntämään muotoon. Tässä tulee ottaa huomioon myös mahdollinen metatieto, ja rakenteet, miten tieto on varastoitu pilvipalvelussa, koska itse tietorakenteet ja miten ne ovat säilytetty pilvipalvelussa voivat olla merkittäviä asiakkaalle.

Palveluntarjoajan etu voi olla jopa noudattaa standardeja, jotta palveluntarjoaja voi hyödyntää kolmansien osapuolten kuormantasaukseen liittyvää tarjontaa. Asiakkaiden houkuttelu standardeja noudattelevalla palvelulla on myös mahdollisuus palveluntarjoajan liiketoiminnan kasvattamiselle. Asiakkaan tulisi edellyttää pilvipalvelun tarjoajan osalta standardien noudattamista, jotta asiakkaan on helpompi siirtyä tarvittaessa toisen pilvipalvelun käyttöön, ja jotta palveluntarjoaja voi hyödyntää kuormantasausta mahdollistaen pilvipalvelun suuremman toimintavarmuuden myös kysyntäpiikkien aikana. Toisaalta kolmansien osapuolien hyödyntäminen kuormantasauksessa tai jonkin osa-alueen tai palvelutason tarjoaminen ns. aliurakoitsijan avulla asettaa asiakkaan riskialttiiksi sekä tietoturvan että tiedon hyödyntämisen suhteen – Tässä tilanteessa tietoa täytyy kulkea palveluntarjoajan ja aliurakoitsijan sekä aliurakoitsijan ja asiakkaan välillä jolloin pelkästään tiedon siirtyminen synnyttää lisää riskejä. Asiakkaan tulisikin kartoittaa tästä johtuvat riskit.

Asiakkaan tulisi ohjelmistohankintoja tehdessään selvittää, mitä ohjelmistojen lisenssiehdot sanovat tuotteen käytöstä pilvipalveluissa, sekä harkita sellaisia tuotteita jotka sen mahdollistavat, jos se vähentää kustannuksia verrattuna tilanteeseen, jossa asiakas mahdollisesti hankkii paikallisilla laitteilla ja pilvessä ajettavat ohjelmistot erikseen. Ohjelmistoja tuottavien yritysten tulisi taas tehdä tutkimusta siitä, miten pilvipalvelujen yleistyminen vaikuttaa heidän tuotteisiinsa ja harkita ns. ”pilvivalmiiden” sovellusten kehittämistä.

Käyttäjän tulee pyrkiä selvittämään, missä pilvipalvelun tietoa säilytetään, missä maassa pilvipalveluntarjoajan organisaatio ja sen jäsenet toimivat ja asuvat, ja ottaa nämä asiat huomioon palveluntarjoajaa valittaessa. Palveluntarjoajan pitäisi katsoa velvollisuudekseen säilyttää tietoa sellaisissa paikoissa, mikä varmistaa asiakkaan tietojen säilymisen asiakkaalla itsellään sekä niiden luottamuksellisuuden.

Teknologinen kehitys ja lainsäädännön suhteellinen muuttumattomuus aiheuttavat ongelmia sekä asiakkaille että palveluntarjoajille. Asiakkaiden tulisi aktiivisesti edellyttää, että lainsäädäntöä kehitetään oikeudenmukaiseen suuntaan. Yritys- ja yksityisasiakkaiden tulee myös mahdollisuuksien mukaan kartoittaa tarkoin lainsäädäntöä, koska on ilmeistä, että se voi toimia epäintuitiivisesti asiakasta kohtaan.

Yritysten kannalta on perusteltua pyrkiä niihin toimiin, jotka asettavat todistettavat lähtökohdat sille, että yritys on toimittanut esimerkiksi mahdollisille omilla verkkosivuillaan käyville henkilöille tiedot, jotka esittävät minkälaisia omistus- ja immateriaalioikeuksia yrityksen sivuilla esitettyihin tietoihin kuuluu. Toisaalta tietojen ulkopuolinen hyödyntäminen voi joskus myös hyödyntää yritystä tarjoten esimerkiksi asiakkaille helpomman pääsyn yrityksen tarjoamiin tietoihin, joka taas voi edistää yrityksen liiketoimintaa. Yksityisiä kuluttajia omistusoikeuksien suojaaminen tiedon yhdistelyn varalta ei koske niin paljon kuin organisaatioita, mutta myös yksityiset henkilöt voivat soveltaa jossain määrin samoja periaatteita.

Asiakkaan tulisi tutkia, mitä käyttöehtosopimus sanoo käyttöehtojen muuttumisesta ja muutosten ilmoittamisesta, sekä mahdollisesti pyrkiä käyttämään palveluntarjoajaa, joka toimittaa asiakkaalle käyttöehtosopimuksissa ilmenevät mahdolliset muutokset niin, että asiakkaan on myös mahdollista noutaa oma sisältönsä pilvipalvelusta ilman hyväksymättä uusia käyttöehtosopimuksia. Suurempien organisaatioiden tulisi taas hyödyntää mahdollisuuttaan neuvotella käyttöehtosopimukset paremmin omia tarpeita vastaaviksi.

Bhadauria ym. (2011) käsittelevät muun muassa käyttäjien valtuuttamisen kysymystä, ja he mainitsevat, että organisaatiolla on todennäköisesti sisäiset käytänteet kelle, millä perusteella ja miten tieto annetaan jollekin organisaation jäsenelle käytettäväksi. Näitä periaatteita tulisikin Bhadauria ym. (2011) noudattaa myös pilvipalveluissa. Tietorakenteet, jotka hallitsevat käyttäjien valtuutusta pilvipalveluissa eivät ole välttämättä integroituina suoraan organisaation muihin tietojärjestelmiin. Tämän vuoksi pilvipalveluita käyttävien organisaatioiden tulisikin Bhadauria ym. (2011) mukaan huolehtia käyttäjäoikeuksien päivittämisestä esimerkiksi työsuhteen päättyessä.

Asiantuntevien asiakkaiden tulisi mahdollisuuksien mukaan suosia IaaS-palveluita, koska ne mahdollistavat paremmin tietojen salaamisen. Yksityisasiakas voi ainakin luottamuksellisimpien tietojensa osalta salata ne ennen pilvipalveluun lataamista.

Edellisissä kappaleissa käsiteltiin kokoavasti aikaisempien lukujen sisältöä. Seuraavaksi käsittelen pohtivasti tästä sisällöstä johtuvia suosituksia ja johtopäätöksiä sekä kirjallisuuskatsauksen ulkopuolisia näkökulmia.

Palveluntarjoajien osalta suuntaa-antavana ohjeena voisi pitää esimerkiksi Pearson (2009) artikkelia, jossa hän käy läpi listaa yksityisyysperiaatteista, joista seuraavien hyödyntäminen myös omistus- ja immateriaalioikeuksien suojelemiseksi mielestäni perusteltua:

> 1. Kuka tahansa, joka kerää käyttäjien tietoa, tulisi kertoa käyttäjille, mitä he keräävät, miten he käyttävät kerättyä tietoa, miten pitkään he säilyttävät kerättyä tietoa, kenen kanssa he jakavat kerättyä tietoa ja mihin muihin tarkoituksiin he aikovat käyttää kerättyä tietoa. Tietojen jakamisesta myös kolmansille osapuolille pitää kertoa.
>
> 2. Käyttäjille tulee antaa päätäntävalta heidän tietojensa keräyksestä.
>
> 3. Vain sellaista tietoa, joka vastaa mainittua tarkoitusta, tulisi kerätä.
>
> 4. Käyttäjille pitää antaa mahdollisuus tutustua, minkälaisia tietoja heistä on varastoitu, ja mahdollisuus varmistaa se, että tiedot käyttäjästä ovat oikeelliset.

Pearson (2009) myös mainitsee, että yksityisyysvaatimusten kartoittaminen kehittäjän osalta tulisi aloittaa jo tuotteen kehityksen alussa, jatkaa sitä kehityksen aikana ja jatkaa yksityisvaatimusten kartoittamista tuotteen käytön poistamiseen asti.

Pilvipalvelujen potentiaalisen asiakkaan tulisi harkita onko pilvipalvelujen käyttäminen kannattavaa kolmannessa luvussa tulleiden syiden perusteella ja vaarantavatko ne asiakkaan immateriaali- ja omistusoikeuksia, kuitenkaan unohtamatta potentiaalisia ulkoisesti näkymättömiä riskejä, joita mainitaan tässä yhteenvedossa. Potentiaalisen asiakkaan tulisi pohtia kunkin pilvipalveluntarjoajan hyötyjä ja riskejä myös erikseen.

Pienet- ja keskisuuret yritykset saavat erityistä kilpailuetua pilvipalveluiden mahdollistaman elastisuuden ja skaalautuvuuden vuoksi. Suuretkin organisaatiot todennäköisesti hyötyvät taloudellisesti pilvipalvelujen käytöstä. Toisaalta suurilla organisaatioilla on todennäköisesti osaamista ja resursseja tuottaa oma yksityinen pilvi varsinkin kriittisiä tietoja varten, ja ne ovatkin todennäköisimmin alttiina esimerkiksi kilpailijoiden teollisuusvakoilulle, jonka vuoksi omien yksityispilviratkaisujen toteuttaminen on perusteltua.

Myös palveluntarjoajien tulisi toimia niin, että asiakkaan on mahdollista säilyttää immateriaali- ja omistusoikeudet itsellään. Tässä tutkielmassa keskityttiin enemmän palveluntarjoajan asemaan riskitekijänä asiakkaan lataamien omistusoikeuksien ja immateriaalioikeuksien hallinnalle.

Eri näkökulmaa immateriaalioikeuksien suojaamiselle tuovat esimerkiksi käyttäjän pilveen, varsinkin julkiseen kulutukseen lataama sisältö, jonka immateriaalioikeudet eivät kuulu käyttäjälle itselleen. Muun muassa YouTube käyttää

automaattista sisällöntunnistusjärjestelmää näiden sisältöjen tunnistamiseen ja jatkotoimenpiteiden suorittamiseen. (YouTube, 2015a). Yhdysvalloissa on myös käytössä Digital Millenium Copyright Act, DMCA, jota immateriaalioikeuksien haltijat usein käyttävät myös Internetissä ns. luvattoman sisällön poistamiseen.

Kuten aikaisemmissa luvuissa on todettu, pilvipalveluiden tarjoajilla voi olla intressejä hyväksikäyttää asiakkaan tietoja. Voidaan kuitenkin kyseenalaistaa, perustuuko tiedon mahdollinen hyväksikäyttö pelkästään yrityksen välittömille taloudellisille intresseille. Voiko pilvipalveluiden luvallinenkin tiedon analysointi ja hyväksikäyttö saavuttaa sellaisen kattavuuden, että sen voidaan katsoa karanneen taloudellisten realiteettien ulkopuolelle? Voiko esimerkiksi sisällön kustomointi käyttäjälle mennä liian pitkälle?

Tutkielmassani olen käsitellyt pilvipalvelujen tarjoajien argumentteja tiedon hyväksikäyttämisestä niitä kyseenalaistamatta, mutta on kuitenkin perusteltua harkita, mitä pilvipalvelujen tarjoajat voivat tehdä asiakkaiden tiedoilla. Pilvipalveluiden tarjoajat ovat suurelta osin liikeyrityksiä, joiden on tarkoitus tuottaa mahdollisimman paljon voittoa. Mikä siis estää pilvipalveluntarjoajaa suoraan hyväksikäyttämästä esimerkiksi asiakkaan tuotekehitys-, myynti- tai yksityistietoja? Palveluntarjoaja voi myydä valittuja tietoja eteenpäin esimerkiksi asiakkaan kilpailijalle sillä tavoin, että asiakkaan on lähes mahdotonta tai vaikeaa havainnoida tai todistaa tietojen käyttöä tällä tavoin. Esimerkiksi tuotekehitystietojen pitäminen yrityksen omassa yksityisessä pilvessä tai tietojärjestelmissä voi olla perusteltua tällaisten uhkakuvien johdosta.

Perusteita muihinkin kuin taloudellisesti motivoituneihin uhkakuviin on olemassa: Greenwald ja MacAskill (2013) kirjoittivat The Guardian:n kuuluisaksi tulleessa artikkelissaan Yhdysvaltojen tiedustelupalvelun National Security Agency harjoittamasta tiedonkeruuohjelmasta joka tunnetaan nimellä PRISM. Kyseinen ohjelma keräsi Edward Snowdenin paljastusten mukaan tietoja suoraan suurten palveluntarjoajien, kuten Googlen ja Applen palvelimilta. Nämä paljastukset väittivät, että kyseiset yritykset auttoivat NSA:ta tietojenkeruussa. Ackerman, Ball ja Rushe (2013) kuitenkin raportoivat myös The Guardianissa, että suuret teknologiayritykset kiistävät, että he edesauttaisivat tietojenkeruuta millään tavalla. Kuitenkin Ackerman (2014) raportoi, että NSA:n asianajaja Rajesh De väitti, että muun muassa Yahoo, Apple ja Google tiesivät ja saivat laillisia vaateita tiedonkeruusta. On varmasti aiheellista suhtautua epäilevästi Rajeshin väitteisiin teknologiayritysten tietämyksestä, mutta ei olisi yllättävää, jos nämä yritykset tekivät yhteistyötä Yhdysvaltojen tiedusteluelinten kanssa. Ottaen huomioon nämä kiistämiset, ja mahdolliset taloudelliset edut Yhdysvaltojen liittovaltion kanssa yhteistyön tekemisestä, voidaan pilvipalvelujen tarjoajien motiiveja – joista suuri osa on yhdysvaltalaisia – pitää riskialttiina ei pelkästään suoraan taloudellisten, vaan myös ns. kansallisten etujen vuoksi.

Jatkotutkimuksena tälle tutkielmalle voisi olla muun muassa potentiaalisille asiakkaille suunnattu tiekartta tai menetelmä, jolla asiakas voisi kartoittaa johdonmukaisesti kunkin pilvipalveluntarjoajan asiakuuden kannattavuutta esi-

merkiksi omistus- ja immateriaalioikeuksien hallinnan näkökulmasta. Tämä menetelmä voisi hyödyntää esimerkiksi luvussa 3 ja tässä yhteenvedossa ilmi tulleita seikkoja.

LÄHTEET

Ackerman, S. (2014). US tech giants knew of NSA data collection, agency's top lawyer insists. The Guardian. Haettu 3.6.2015 osoitteesta http://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de

Ackerman, S., Ball, J., Rushe, D. (2013). Reports that NSA taps into Google and Yahoo data hubs infuriate tech giants. Haettu 3.6.2015 osoitteesta http://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links 3.6.2015.

Armbrust, A., Fox, A., Griffith, R., Joseph, A., Katz, R., Konwinski, A., Lee, G., Patterson D.A., Rabkin, A., Stoica, I., & Zaharia, M. (2009). Above the clouds: A Berkeley view of cloud computing. Department of Electrical Engineering and Computer Sciences, University of California, Berkeley.

Bhadauria, R., Chaki, R., Chaki, N., & Sanyal, S. (2011). A survey on security issues in cloud computing.

Bradshaw, S., Millard, C., & Walden, I. (2011). Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services. *International Journal of Law and Information Technology, 19*(3), 187-223.

Chen, Z., Yoon, J. (2010). IT auditing to assure a secure cloud computing. SERVICES-1. *2010 IEEE 6th World Congress on Services*, 253-259.

Chen, D. ja Zhao, H. (2012). Data security and privacy protection issues in cloud computing. Computer Science and Electronics Engineering (ICCSEE), *2012 International Conference on Computer Science and Electronics Engineering* (1) 647-651.

Cunningham, A. & Reed, C. (2013). Caveat Consumer?–Consumer Protection and Cloud Computing Part 2–The Application of ex ante and ex post Consumer Protection Law in the Cloud. Queen Mary University of London, School of Law.

Descher, M., Masser, P., Feilhauer, T., Tjoa, A.M., & Huemer, D. (2009). Retaining data control to the client in infrastructure clouds. *2009 International Conference on Availability, Reliability and Security*.

F-Secure. (2015) F-SECURE SELLS YOUNITED PERSONAL CLOUD TO SYNCHRONOSS Noudettu osoitteesta https://community.f-secure.com/t5/Using-younited/F-SECURE-SELLS-YOUNITED-PERSONAL/td-p/66613/highlight/false 5.5.2015.

Greenwald, G., MacASkill, E. NSA Prism program taps in to user data of Apple, Google and others. (2013). Haettu 3.6.2015 osoitteesta http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Haarmann, P. (2005). *Tekijänoikeus ja lähioikeudet*. (3. uud. painos). Helsinki: Talentum.

Haarmann, P., Mansala, M. (2012). *Immateriaalioikeuden perusteet*. (2. uud. painos). Helsinki: Talentum.

Hemmo, M., Könkkölä, J., Norros, O. (2006) *Sopimusoikeuden oppikirja*. Helsinki: Talentum.

Googlen palveluehdot. (2014). Haettu 29.4.2015 osoitteesta https://www.google.com/intl/fi/policies/terms/

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: Computing in a policy cloud? *Journal of Information Technology & Politics, 5*(3), 269-283.

Jaeger, P.T., Lin, J., Grimes, J.M. & Simmons, S.N. (2009). Where is the cloud? Geography, economics, environment, and jurisdiction in cloud computing. *First Monday 14*(5).

Joint, A., Baker, E., & Eccles, E. (2009). Hey, you, get off of that cloud? *Computer Law & Security Review, 25*(3), 270-274.

Kalyvas, J.R, Overly, M.R., & Karlyn, M.A. (2013). Cloud Computing: A Practical Framework for Managing Cloud Computing Risk–Part I. *Intellectual Property & Technology Law Journal, 25*(3). 7-18.

Laki varallisuusoikeudellisista oikeustoimista. 13.6.1929/228. Haettu 9.4.2015 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/1929/19290228

Lassila, O. (1998). Web metadata: a matter of semantics. *Internet Computing, IEEE. 2*(4). 30-37.

Lemley, M.A. Terms of Use. (2006) *Minnesota Law Review*, 91

Lindell, Y. & Pinkas, B. (2009). Secure multiparty computation for privacy-preserving data mining. *Journal of Privacy and Confidentiality, 1*(1), 5.

Linnake, T. (2012). Drive pelästytti : Viekö Google tietosi? It-viikko. Haettu 22.4.2015 osoitteesta http://www.itviikko.fi/uutiset/2012/04/25/drive-pelastyttivieko-google-tietosi/201228134/7

Liu, F., Tong, J., Mao, J., Bohn, R., Messina, J., Badger, L. ja Leaf, D. (2011). NIST cloud computing reference architecture. *National Insitute of Standards and Technology special publication*, 500-292.

Maanmittauslaitos. Mitä on Maanmittauslaitoksen avoin data? Haettu 10.5.2015 osoitteesta http://www.maanmittauslaitos.fi/avoindata/mita-avaaminen-tarkoittaa

Ryan, M. D. (2013). Cloud computing security: The scientific challenge, and a survey of solutions. *Journal of Systems and Software, 86*(9), 2263-2268.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J., & Ghalsasi, A. (2011). Cloud computing—The business perspective. *Decision Support Systems, 51*(1), 176-189.

Natunen, A. (2014). *Tiedon omistajuus pilvipalveluissa tietoturvan, lainsäädännön ja käyttöehtojen näkökulmasta*. Tietojärjestelmätieteen pro gradu –tutkielma. Jyväskylän yliopisto.

Patibandla, R.L., Kurra, S.S., & Mundukur, N.B. (2012). A study on scalability of services and privacy issues in cloud computing. *Distributed Computing and Internet Technology*. 212-230. Berlin Heidelberg: Springer.

Pearson, S. (2013). Privacy, security and trust in cloud computing. Privacy and Security for Cloud Computing. 3-42. Lontoo: Springer.

Pearson, S. (2009). Taking account of privacy when designing cloud computing services. *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*. 44-52. IEEE Computer Society.

Prabavathy, B., Devi, M., ja Babu, C. (2013, July). Multi-index technique for metadata management in private cloud storage. *Recent Trends in Information Technology (ICRTIT), 2013 International Conference on*. 84-89.

Reed, C. (2010). Information 'Ownership' in the Cloud. Queen Mary School of Law.

Robison, W. J. (2010). Free at what cost? Cloud computing privacy under the stored communications act. *Georgetown Law Journal, 98*(4).

Sailer, R., Valdez, E., Jaeger, T., Perez, R., Van Doorn, L., Griffin, J. ja Berger, S. (2005). sHype: Secure hypervisor approach to trusted virtualized systems. Thomas J. Watson Research Center. IBM Research Division.

Santos, N., Gummadi, K. P., & Rodrigues, R. (2009). Towards trusted cloud computing. *HotCloud* 9 (2009): 3-3.

Sopimattomista elinkeinoharjoittajien ja kuluttajien välisistä kaupallisista menettelyistä sisämarkkinoilla annettu Euroopan parlamentin ja neuvoston direktiivi 2005/29. Haettu 28.4.2015 osoitteesta http://eur-lex.europa.eu/legal-content/fi/ALL/?uri=CELEX:32005L0029

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of network and computer applications, 34*(1), 1-11.

Surden, H. (2013) Technological Cost as Law in Intellectual Property. *Harvard Journal of Law and Technology, 27*(1), 135-202.

Svantesson, D. ja Clarke, R. (2010). Privacy and consumer risks in cloud computing. *Computer Law & Security Review, 26*(4), 391-397.

Toivonen, Ulla (2015). F-Secure Sells Younited Personal Cloud to Synchronoss; Redoubles Security Focus. Haettu 5.5.2015 osoitteesta https://www.f-secure.com/en/web/press_global/news-clippings/-/journal_content/56/1075444/1179552?p_p_auth=768Zjrct

Yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta annettu Euroopan parlamentin ja neuvoston direktiivi 95/46. Haettu 28.4.2015 osoitteesta http://eur-lex.europa.eu/legal-content/fi/ALL/?uri=CELEX:31995L0046

YouTube (2015a) How Content ID works. Haettu 12.6.2015 osoitteesta https://support.google.com/youtube/answer/2797370?hl=en

YouTube (2015b) Metadata. Haettu 11.6.2015 osoitteesta https://www.youtube.com/yt/playbook/metadata.html