

Antti Natunen

**TIEDON OMISTAJUUS PILVIPALVELUISSA  
TIETOTURVAN, LAINSÄÄDÄNNÖN JA  
KÄYTTÖEHTOJEN NÄKÖKULMASTA**



JYVÄSKYLÄN YLIOPISTO  
TIETOJENKÄSITTELYTIETEIDEN LAITOS  
2014

## TIIVISTELMÄ

Natunen, Antti

Tiedon omistajuus pilvipalveluissa tietoturvan, lainsäädännön ja käyttöehtojen näkökulmasta

Jyväskylä: Jyväskylän yliopisto, 2014, 49 s.

Tietojärjestelmätiede, pro gradu -tutkielma

Ohjaajat: Ojala, Arto

Tässä pro gradu -tutkielmassa käsitellään tiedon omistajuutta ja käyttöoikeuksia pilvipalveluissa. Tutkielman tarkoitus oli selvittää käyttöehtojen ja lainsäädännön vaikutuksia tiedon omistajuuteen pilvipalveluissa tietoturvan näkökulmasta. Tutkielmassa oli myös tarkoituksena selvittää, miten palveluntarjoajat vaikuttavat pilvipalveluiden käyttöehdoissa niihin tallennetun tiedon omistajuuteen ja mitä vaikutuksia tällä on tietoturvaan. Lisäksi oli tarkoitus selvittää, mitä lainsäädäntöä pilvipalveluihin sovelletaan. Tutkielman aihe on tärkeä, koska tiedon omistajuutta ja siihen liittyviä kysymyksiä etenkin tietoturvan näkökulmasta ei juurikaan ole käsitelty aiemmissä tutkimuksissa. Tiedon omistajuuteen ja kontrolliin liittyviä seikkoja pidetään tutkitusti yhtenä merkittävimmistä ongelmista pilvipalveluissa. Tutkielman kirjallisuusosassa tarkasteltiin pilvipalveluiden käyttöehtojen vaikutuksia niihin tallennetun tiedon omistajuuteen. Lisäksi tarkasteltiin Suomen, Euroopan unionin ja Yhdysvaltojen lainsäädännön vaikutuksia tiedon omistajuuteen pilvipalveluissa. Tutkielman empiirisessä osassa tehtiin tapaustutkimus, jossa tutkittiin kahdeksaa julkista pilvipalvelua, joista selvitettiin niiden käyttöehtosopimuksia analysoimalla niihin tallennetun tiedon omistajuutta sekä niihin sovellettavaa lainsäädäntöä. Tämän tutkielman tuloksena saatiin katsaus tiedon omistajuuteen kahdeksan tunnetun julkisen pilvipalvelun osalta. Tutkimuksen johtopäätöksiä todettiin, että pilvipalveluissa on suurta kirjavuutta tiedon omistajuuden sekä sovellettavan lainsäädännön osalta. Kaikki tutkitut pilvipalvelut antoivat käyttäjän pitää omistusoikeutensa niihin tallentamaansa tietoon, mutta puolesta tapauksista pilvipalvelun tarjoaja sai varsin laajojakin käyttöoikeuksia käyttäjien niihin tallentamaan tietoon. Myös tutkittuihin pilvipalveluihin sovellettavassa lainsäädännössä todettiin olevan paljon hajontaa, kuitenkin siten, että valtaosin niihin sovellettavaksi ilmoitettiin Yhdysvaltojen lainsäädäntö. Johtopäätöksenä todettiin myös, että on erittäin tärkeää tietää, miten käytetyn pilvipalvelun tarjoaja suhtautuu siihen tallennetun tiedon omistajuuteen.

Asiasanat: pilvipalvelu, tietoturva, lainsäädäntö, tiedon omistajuus

## ABSTRACT

Natunen, Antti

Data ownership in cloud services from security, law and end-user license agreement perspectives

Jyväskylä: University of Jyväskylä, 2014, 49 p.

Information Systems, pro gradu

Supervisor: Ojala, Arto

This pro gradu -thesis covers data ownership and access rights on cloud services. This report investigated what effects end-user license agreements and applicable laws have concerning the data ownership on cloud services. The purpose of this report was to find out the effects of end-user license agreements and legislation concerning the data ownership on cloud services. The topic of this report is important, because it was covered very briefly at most in the earlier research. Also questions about data ownership and control on cloud computing services are proved to be one of the most important aspects of them. In literature part of this thesis a topic is discussed from perspective of end-user license agreement, law and security. Theory part also discussed the effects of Finnish, European union and United States law to data ownership on cloud services. Second part of this thesis is empirical part and it uses case study as research method. The Case Study discusses the analysis of the end user license agreements of the eight very commonly used and public cloud-computing services. The end user agreements are analyzed in the perspective of data ownership and applicable law. The results of this thesis are the review of data ownership and applicable law of the eight commonly used and public cloud-computing services. At conclusions there was presented the fact that there is a lot of variation between the public cloud-computing services what comes to the data ownership in them. Also applicable law point of view there was variation between the services. Still majority of the services states the US law as the applicable law. All eight studied cloud-computing services let the users keep the ownership of the data that they save on those services but a half of them also makes users to gave providers the usage rights to the that data. Also conclusion was made that it is very import to know how the provider of the used cloud-computing service concerns about ownership and privacy of users data.

Keywords: cloud computing, data ownership, Software as a Service, security, law

## **KUVIOT**

KUVIO 1 Yksinkertainen kaavio pilvipalvelukonseptista .....	12
KUVIO 2 Jericho pilvikuutiomalli .....	15

## **TAULUKOT**

TAULUKKO 1 Tapaustutkimuksen tärkeimmät havainnot .....	41
---	----

# SISÄLLYS

TIIVISTELMÄ  
ABSTRACT  
KUVIOT

1	JOHDANTO .....	7
1.1	Taustaa .....	7
1.2	Tutkimusongelman esittely sekä tutkimuksen tarkoitus, tavoitteet ja tarve.....	8
1.3	Tutkielman rakenne ja tutkimusmenetelmä .....	8
1.4	Aiempi tutkimus .....	9
1.5	Tutkielman tulokset .....	10
2	TIEDON OMISTAJUUS PILVIPALVELUISSA .....	11
2.1	Käsitteet .....	11
2.2	Pilvipalvelutyypit.....	14
2.3	Tiedon omistajuus ja pilvipalvelut .....	16
2.4	Pilvipalveluiden käyttöehtojen vaikutus tiedon omistajuuteen ja tietoturvaan.....	16
2.5	Lainsäädännön vaikutus tiedon omistajuuteen pilvipalveluissa.....	17
2.5.1	Suomen lainsäädäntö.....	18
2.5.2	Lainsäädäntö muualla ja kansainvälinen lainsäädäntö.....	20
3	METODOLOGIA .....	24
4	TIEDON OMISTAJUUS TUNNETUISSA PILVIPALVELUISSA .....	26
4.1	Google Apps .....	26
4.1.1	Pilvipalvelun kuvaus .....	26
4.1.2	Käyttöehdot.....	27
4.1.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	28
4.2	Microsoft Office 365 .....	29
4.2.1	Pilvipalvelun kuvaus .....	30
4.2.2	Käyttöehdot.....	30
4.2.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	31
4.3	F-Secure Younited .....	32
4.3.1	Pilvipalvelun kuvaus .....	32
4.3.2	Käyttöehdot.....	32
4.3.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	33
4.4	Dropbox .....	33
4.4.1	Pilvipalvelun kuvaus .....	33
4.4.2	Käyttöehdot.....	34
4.4.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	34
4.5	iCloud.....	34
4.5.1	Pilvipalvelun kuvaus .....	35
4.5.2	Käyttöehdot.....	35
4.5.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	36

4.6	GitHub .....	36
4.6.1	Pilvipalvelun kuvaus .....	36
4.6.2	Käyttöehdot.....	37
4.6.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	37
4.7	Adobe Creative Cloud.....	37
4.7.1	Pilvipalvelun kuvaus .....	38
4.7.2	Käyttöehdot.....	38
4.7.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	38
4.8	Amazon Web Services .....	39
4.8.1	Pilvipalvelun kuvaus .....	39
4.8.2	Käyttöehdot.....	39
4.8.3	Lainsäädäntö ja mahdolliset oikeustapaukset .....	40
4.9	Tulokset ja johtopäätökset .....	40
5	YHTEENVETO.....	42
	LÄHTEET.....	45

# 1 JOHDANTO

Tässä luvussa esitellään tutkielman taustaa ja tutkimusongelma sekä asetetaan tutkimuskysymykset, joihin tutkielmassa haetaan vastauksia. Luvussa määritellään myös tutkielman tarkoitus ja tavoitteet. Näiden lisäksi luvussa esitellään tutkielman rakenne ja käsitellään aihealueen aiempaa tutkimusta. Lopuksi luvussa esitetään saavutetut tulokset.

## 1.1 Taustaa

Pilvipalveluiden yleistymisen vuoksi niiden käyttämisen yhdeksi suurimmista kysymyksistä viimevuosina on noussut niiden tietoturvaongelmat. IDC:n vuonna 2008 tekemässä kyselyssä (Awodele, Ibikunie & Kuyoro, 2011), johon vastasi 244 yritysten it-johtajaa, merkittävimmäksi kysymykseksi pilvipalveluissa nostettiin juuri tietoturvaongelmat. Kysely uusittiin vuonna 2009 ja tällä kertaa siihen vastasi 263 it-johtajaa. Tietoturvaongelmia pidettiin edelleen merkittävimpänä kysymyksenä pilvipalveluissa. (Eloff, Ramgovind & Smith, 2010.) Prosessorivalmistaja Intel teki puolestaan vuonna 2012 kyselyn liittyen pilvipalveluihin ja niiden käyttämiseen. Siihen vastasi 800 it-johtajaa Iso-Britanniasta, Kiinasta, Saksasta ja Yhdysvalloista. Myös tässä kyselyssä pilvipalveluiden tietoturvaa pidettiin ongelmana. 69 prosenttia vastaajista kertoi olevansa huolissaan tai erittäin huolissaan yksityisten pilvipalveluiden tietoturvasta. Samassa kyselyssä julkisten pilvipalveluiden tietoturvasta oli huolissaan tai erittäin huolissaan peräti 87 prosenttia vastanneista. (Peer research: What's holding back the cloud, 2012.) Pilvipalveluiden tietoturvaongelmat nostaa tärkeimpinä esiin artikkelissaan myös Bhadauria, Chaki, Chaki & Sanyal (2011), jossa tietoturva määritellään perusasiaksi, joka määrittää uuden tietojenkäsittelytekniikan menestyksen.

Pilvipalveluiden tietoturvaongelmista tärkeimpiä ovat niihin tallennetun tiedon omistajuuteen ja käyttöoikeuksiin liittyvät kysymykset. Intelin vuoden 2012 kyselytutkimuksen mukaan yli puolet vastanneista piti tiedon ja siihen pääsyn kontrollin puutetta yhtenä kolmesta suurimmasta tietoturvaongelmasta

pilvipalveluissa. (Peer research: What's holding back the cloud, 2012.) Tiedon omistajuuteen pilvipalveluissa ei ole kiinnitetty tarpeeksi huomiota ja monet pilvipalveluiden käyttäjät eivät edes ole ajatelleet sitä käyttäessään pilvipalveluita. Myös nimenomaan pilvipalveluita koskevan lainsäädännön puuttuminen on ongelma pilvipalveluiden käyttämisessä. Tämä tulee selkeästi esiin mm. Antwerpenin yliopiston professori Eecken (2010) esittämästä EU:n nykyisen lainsäädännön ja teknologian kehittymistahdin eroa kuvaavasta kaaviosta. Monet pilvipalveluihin ja etenkin niiden käyttämiseen liittyvät kysymykset ovat miltei mahdottomia ratkaista pilvipalveluja koskevan lainsäädännön puuttumisen takia.

## 1.2 Tutkimusongelman esittely sekä tutkimuksen tarkoitus, tavoitteet ja tarve

Tässä tutkielmassa on tarkoitus alla asetettuihin ja lueteltuihin tutkimusongelmiin ratkaisuja hakemalla selvittää pilvipalveluihin tallennetun tiedon omistajuutta tietoturvan kannalta ja selvittää, mitä vaikutuksia pilvipalveluiden käyttöehdoilla sekä lainsäädännöllä on tiedon omistajuuteen.

1. Pilvipalvelun käyttöehtojen vaikutus tiedon omistajuuteen ja tiedon käyttöoikeuksiin pilvipalveluissa tietoturvan näkökulmasta.
2. Kansallisen ja kansainvälisen lainsäädännön vaikutus tiedon omistajuuteen pilvipalveluissa tietoturvan näkökulmasta.

Tutkielman tavoitteena on selvittää miten pilvipalvelun tarjoaja voi vaikuttaa tiedon omistajuuteen pilvipalvelussa käyttöehtosopimuksen kautta ja miten se vaikuttaa tietoturvaan. Lisäksi tutkielmassa on tavoitteena selvittää pilvipalveluihin liittyvän lainsäädännön olemassaoloa ja vaikutuksia tiedonomistajuuteen ja tietoturvaan.

Tutkielma on tarpeen, koska tiedon omistajuuteen ja käyttöoikeuksiin eli tiedon ja siihen pääsyn kontrollointiin liittyviä kysymyksiä pidetään tutkitusti (What's holding back the cloud, 2012) yhtenä suurimmista ja tärkeimmistä ongelmista pilvipalveluiden käyttämisessä. Tiedon omistajuuteen pilvipalveluissa ei myöskään kiinnitetä tarpeeksi huomiota, eikä sitä ole aiemmassa tutkimuksessa käsitelty kovinkaan laajalti. Etenkin pilvipalveluihin tallennetun tiedon omistajuuden tietoturvanäkökohtia on syytä tuoda esiin.

## 1.3 Tutkielman rakenne ja tutkimusmenetelmä

Tässä pro gradu -tutkielmassa käsitellään pilvipalveluihin tallennetun tiedon omistajuutta ja siihen liittyviä kysymyksiä tietoturvan, lainsäädännön ja käyttöehtojen näkökulmasta. Tutkielma sisältää johdannon, käsittelyosan ja yh-



teenvedon. Käsittelyosassa määritellään ensin tutkielman aiheen kannalta keskeiset käsitteet. Tämän jälkeen käsitellään tiedon omistajuutta pilvipalvelukontekstissa. Tutkielmassa perehdytään pilvipalveluiden käyttöehtojen vaikutuksiin tiedon omistajuuteen ja käyttämiseen. Lisäksi tarkastellaan myös kansallisen ja kansainvälisen lainsäädännön vaikutuksia tiedon omistajuuteen pilvipalveluissa.

Tutkimusmenetelmänä tutkielman kirjallisuusosassa käytetään kirjallisuuskatsausta, joka on kohdistettu aihepiiriä käsittelevään lähdekirjallisuuteen sekä aiempiin tutkimuksiin. Lähdemateriaali on haettu kirjastojen aineistohauilla sekä Google Scholar -artikkelihauilla. Lähdemateriaali on valittu sen perusteella, että se on mahdollisimman relevanttia tutkielman aiheen kannalta. Lisäksi lähdemateriaalivalinnoissa on pyritty huomioimaan tutkielmaan haluttu tietoturvanäkökulma.

Tutkielman toisessa eli empiirisessä osassa käytetään tutkimusmenetelmänä tapaustutkimusta, jossa on perehdytty tutkielman aiheeseen joidenkin tunnettujen pilvipalveluiden osalta. Tapaustutkimukseen on pyritty valitsemaan eri tyyppisiä pilvipalveluita, jotka ovat myös hyvin tunnettuja ja paljon käytettyjä. Tapaustutkimuksessa selvitetään, miten tutkielman teoriaosassa esitetyt tiedon omistajuuteen pilvipalvelukontekstissa liittyvät seikat toteutuvat tutkimuksen kohteeksi valituissa pilvipalveluissa.

## 1.4 Aiempi tutkimus

Pilvipalveluita käsittelevää tutkimusta on tehty melko paljon. Näissä tutkimuksissa on tutkittu myös pilvipalveluiden tietoturvaa. Aiempaa tutkimusta nimenomaan tiedon omistajuudesta ja siihen liittyvistä tietoturvaseikoista pilvipalvelukontekstissa ei kuitenkaan juurikaan ole. Pilvipalveluiden tietoturvaa sinänsä käsittelevissä tutkimuksissa tiedon omistajuuteen liittyvät seikat jäävät yleensä pelkän maininnan tasolle, eikä niihin siten ole perehdytty tarkemmin.

Pilvipalveluiden tietoturvaa on laajemmin ja yleisemmin käsitelty viime vuosina mm. joissakin artikkeleissa, kuten esimerkiksi Grobauerin, Stöckerin ja Walloschekin (2011) artikkelissa, joka käsittelee pilvipalveluiden haavoittuvuuksia tai Ahnin, Joshin ja Takabin (2010) artikkelissa, joka puolestaan käsittelee pilvipalveluympäristöön liittyviä tietoturvaasteita. Nämä artikkelit eivät kuitenkaan käsittele tiedon omistajuutta tai siihen liittyviä tietoturvaseikkoja sen tarkemmin.

Pilvipalveluiden käyttöehdoista ja käyttöehtosopimuksista on jonkin verran aiempaa tutkimusta, jossa tiedon omistajuutta ainakin sivutaan. Esimerkiksi Bradshawn, Millardin ja Waldenin Lontoon Queen Maryn yliopistossa tekemässä tutkimuksessa he vertailevat ja analysoivat pilvipalveluiden käyttöehtoja. (Bradshaw, Millard & Walden, 2011.)

Pilvipalveluihin liittyvää lainsäädäntöä käsittelevä tutkimus on erittäin niukkaa, koska kyseinen lainsäädäntö puuttuu suurelta osin kokonaan. Pilvipalveluiden tietoturvaa käsittelevissä tutkimuksissa lainsäädännön osa jää myös samoista syistä suppeaksi.

## 1.5 Tutkielman tulokset

Tämän tutkielman tuloksena saadaan selvitys pilvipalveluihin tallennetun tiedon omistajuudesta sekä pilvipalveluiden käyttöehtojen vaikutuksista siihen. Lisäksi saadaan selvitys pilvipalveluihin tallennetun tiedon omistajuuteen liittyvän lainsäädännön olemassaolosta ja sen vaikutuksista tiedon omistajuuteen. Tutkielman empiirisenä osana olevan tapaustutkimuksen tuloksena saadaan katsaus tiedon omistajuuden toteutumiseen ja sovellettavaan lainsäädäntöön kahdeksan tunnetun julkisen pilvipalvelun osalta.

## 2 TIEDON OMISTAJUUS PILVIPALVELUISSA

Ensimmäisenä tässä luvussa määritellään tutkielman aiheen kannalta keskeiset käsitteet. Tämän jälkeen käsitellään pilvipalveluiden tyyppejä. Seuraavaksi luvussa perehdytään tiedonomistajuuden käsitteeseen pilvipalvelukontekstissa. Sitten luvussa käsitellään pilvipalveluiden käyttöehtojen vaikutuksia tiedon omistajuuteen pilvipalveluissa. Lopuksi luvussa perehdytään Suomen, Euroopan unionin ja Yhdysvaltojen lainsäädäntöön pilvipalveluiden ja etenkin niihin tallennetun tiedon omistajuuden osalta.

### 2.1 Käsitteet

#### **Kansainvälinen lainsäädäntö**

Kansainvälisellä lainsäädännöllä tarkoitetaan monikansallisia eli kahta tai useampaa valtiota koskevia lakeja ja määräyksiä (Merriam-Webster: Definition of International Law, 2014). Tässä tutkielmassa tarkastellaan kansainvälisen lainsäädännön osalta lähinnä Euroopan unionin lainsäädäntöä eli käytännössä EU-direktiivejä ja asetuksia.

#### **Kansallinen lainsäädäntö**

Kansallisella lainsäädännöllä tarkoitetaan tietyn yksittäisen ja itsenäisen valtion lainsäädäntöä eli lakeja, säädöksiä ja asetuksia. Kansallisen lainsäädännön pohjana on yleensä perustuslaki. Perustuslakia täydentävät normaalit lait ja asetukset. (Merriam-Webster: Definition of law, 2014.)

Tässä tutkielmassa kansallisen lainsäädännön osalta keskitytään etupäässä Suomen valtion lainsäädäntöön. Tutkielmassa tarkastellaan myös Yhdysvaltojen lainsäädäntöä.

#### **Käyttöehdot**

Käyttöehdoilla eli loppukäyttäjän lisenssisopimusehdoilla (End User License Agreement, EULA) viitataan jonkin ohjelmiston tai palvelun käyttämiseen liittyviin ehtoihin, jotka ko. ohjelmiston tai palvelun käyttäjän on hyväksyttävä

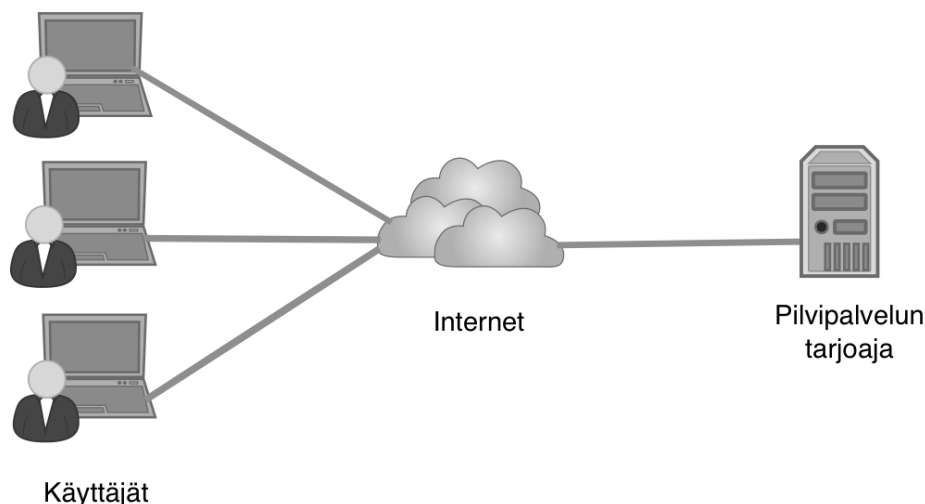
sitä käyttääkseen. Näissä käyttöehdoissa ohjelmiston tai palvelun tuottaja voi määritellä hyvin tarkkaan, kuka ja miten hänen tuotettaan saa käyttää ja mitä ehtojen rikkomisesta tai noudattamatta jättämisestä seuraa. Käyttöehdoissa myös määritellään, minkä maan lainsäädäntöä ohjelmiston tai palvelun käyttämisessä tai siihen liittyvissä mahdollisissa riitatilanteissa sovelletaan. (PC-Mag Encyclopedia: Eula, 2014.)

### Julkinen pilvipalvelu

Julkisella pilvipalvelulla (Public Cloud) tarkoitetaan julkisessa verkossa eli yleensä internetissä olevaa pilvipalvelua, joka on kenen tahansa käytettävissä, joko ilmaiseksi tai maksua vastaan. Tunnetuimmat ja käytetyimmät pilvipalvelut ovat julkisia pilvipalveluita. Julkisen pilvipalvelun vastakohta on yksityinen pilvipalvelu. (Chang, Dillon & Wu, 2010.)

### Pilvipalvelu

Pilvipalvelulla tässä tutkielmassa tarkoitetaan ohjelmisto palveluna (Software as a Service, SaaS) -konseptia, jossa ohjelmisto tarjotaan palveluna verkkoyhteyden välityksellä (kuvio 1). Yksi usein kirjallisuudessa viitattu määritelmä pilvipalvelulle on Yhdysvaltojen kansallisen standardi- ja teknologiainstituutin (NIST, National Institute of Standards and Technology) vuonna 2011 antama määritelmä. Sen mukaan pilvipalvelu on malli, joka mahdollistaa paikkariippumattoman, kätevän ja tarvelähtöisen pääsyn jaettuihin verkkoresursseihin kuten tallennustilaan tai sovelluksiin, joita voidaan nopeasti ottaa käyttöön ja vapauttaa käytöstä vähäisellä hallinnointitarpeella tai palveluntarjoajan toimenpiteillä. Saman määritelmän mukaan pilvipalvelumalli koostuu viidestä erityispiirteestä, kolmesta palvelumallista ja neljästä julkaisumallista. (Grance & Mell, 2011.)



KUVIO 1 Yksinkertainen kaavio pilvipalvelukonseptista

Nimitys pilvipalvelu juontaa juurensa verkkotopologiakaaviossa internetiä kuvaamaan käytetystä pilvikuviosta. Pilvipalvelussa ohjelmisto sijaitsee palvelun tarjoajan palvelimilla. Pilvipalvelun käsite sisältää SaaS:n lisäksi myös muita

pilvipalvelun tyyppinä. Näitä ovat pilviohjelmistoalustat (Platform as a Service, PaaS) ja pilvi-infrastruktuurit (Infrastructure as a Service, IaaS). Ensin mainituksa PaaS -tyypissä palveluntarjoaja tarjoaa pilvessään ohjelmistoalustaa, jossa asiakas voi käyttää siihen kehittämäänsä sovelluksia. IaaS -pilvipalvelutyypissä puolestaan palvelun tarjoaja tarjoaa ainoastaan verkkolaite eli palvelininfrastruktuurin asiakkaan käyttöön ja asiakas itse rakentaa sen päälle ohjelmistoalustan ja varsinaiset sovellukset. (Ransome & Rittinghouse, 2010.)

Pilvipalveluiden suurin etu on tiedon saatavuus. Tieto voi olla tallennettuna toisella puolella maailmaa sijaitsevaan palvelinkeskukseen maantieteellisistä ja valtiollisista rajoista riippumatta ja silti käyttäjän saatavilla, milloin ja missä tahansa hän sitä tarvitsee. Pilvipalvelun käyttäjä voi käyttää palvelua ja sinne tallentamia tietoja usealla eri päätelaitteella kuten tietokoneella ja älypuhelimella tai tablettitietokoneella samanaikaisesti. Pilvipalveluita käytettäessä käyttäjän ei myöskään tarvitse huolehtia ohjelmiston päivityksistä ja ylläpidosta, koska ohjelmisto sijaitsee palveluntarjoajan palvelimilla. (Elsenpeter, Valte & Valte, 2010.)

### **Tiedon käyttöoikeudet**

Käyttöoikeuksilla tallennetun tiedon kohdalla tarkoitetaan niitä oikeuksia, jotka on annettu jollekin henkilölle tai taholle tiettyä tallennettua tietoa kohtaan sen käyttämistä näiden käyttöoikeuksien mukaisella tavalla. Käyttöoikeus on siinä mielessä laaja käsite, että sillä voidaan viitata useisiin eri tyyppisiin käyttöoikeuksiin. Yksinkertaisimmillaan tallennetun tiedon käyttöoikeus voi olla pelkkä tiedon lukuoikeus. Tallennetun tiedon käyttöoikeudet voivat sisältää eri tyyppisiä tallennetun tiedon edelleen käyttöoikeuksia eri tarkoituksiin, kuten kaupalliseen käyttöön. Tallennetun tiedon käyttöoikeudet voivat sisältää myös oikeudet alkuperäisen tiedon muokkaamiseen tai kopioimiseen. (PC-Mag Encyclopedia: Access rights, 2014.)

### **Tiedon omistajuus**

Tiedon omistajuudella tarkoitetaan sitä, kenen tallennettu tieto on ja kuka sitä hallinnoi ja saa käyttää. Tiedon omistajuutta ei pidä sekoittaa tiedon käyttöoikeuksiin. Lähtökohtaisesti tallennetun tiedon omistaa sen luoja, mutta etenkin pilvipalveluympäristössä näin ei välttämättä todellisuudessa ole. Tässä tutkielmassa tarkastellaan tiedon omistajuutta erityisesti pilvipalveluiden tapauksessa. (Brathwaite, 1983.)

### **Tietoturva**

Tietoturva on käsite, jolla viitataan yleensä digitaalisten järjestelmien ja palveluiden ja niiden sisältämän datan turvallisuuteen. Tietoturvasta puhuttaessa se mielletään usein tietojärjestelmien, tietoliikenneväylien tai tietokoneiden suojaamiseksi ja turvaamiseksi. Tietoturvan ydin ja päätarkoitus on kuitenkin tallennetun tiedon säilyvyyden turvaaminen ja saatavuuden varmistaminen käyttöoikeuksien haltijoille tiedon tallennusmuodosta ja -paikasta riippumatta. Tietoturva kattaa siis digitaalisen tiedon ja järjestelmien lisäksi myös perinteiset paperiset arkistot ja muut tietovarastot. (Mattord & Whitman, 2012.)

Pilvipalvelukontekstissa tietoturva käsittää useita osa-alueita. Pilvipalvelun tietoturvaan kuuluu palvelun luotettavuus, selviytymiskyky, luottamuksellisuus, yhtenäisyys ja saatavuus. Pilvipalvelun luotettavuudella tarkoitetaan sitä, että palvelussa ei ole tietoturva-aukkoja tai heikkouksia, jotka altistavat palvelun väärinkäytöksille tai muulle haitalliselle käytölle. Pilvipalvelun selviytymiskyky tarkoittaa palvelun sietokykyä mahdollisia hyökkäyksiä vastaan mahdollisimman vähän haittaa käyttäjille aiheuttaen. Luottamuksellisuus on tärkeä osa myös pilvipalveluita. Luottamuksellisuudella pilvipalveluissa tarkoitetaan mm. immateriaalioikeuksien ja tekijänoikeuksien kunnioittamista ja palvelun tietojen ja tietoliikenteen salausta. Yhtenäisyydellä pilvipalveluissa tarkoitetaan sitä, että vain autentikoiduilla tahoilla (eli käytännössä tiedon omistajalla ja niillä tahoilla, joilla on käyttöoikeuksia tietoon) on pääsy palveluun tallennettuun tietoon lukemista tai muokkaamista varten. Pilvipalvelun saatavuudella tarkoitetaan, sitä että pilvipalvelu ja siihen tallennettu tieto on ajasta ja paikasta riippumatta luotettavasti ja tarvittaessa saatavilla. (Kavitha & Subashini, 2011.)

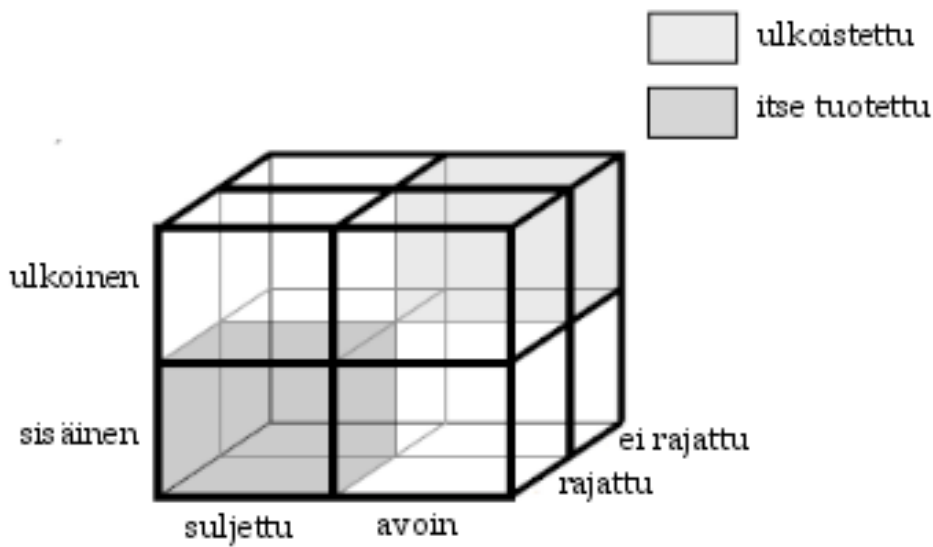
### **Yksityinen pilvipalvelu**

Yksityinen pilvipalvelu on pilvipalvelutyyppejä, jossa pilvipalvelu sijaitsee yksityisillä palvelimilla muodostaen suljetun ympäristön. Yksityisellä pilvipalvelulla on lisäksi rajattu käyttäjäryhmä eli se ei ole julkisesti saatavilla. Yksityiset pilvipalvelut sijaitsevat yleensä yritysten ja organisaatioiden omissa sisäisissä verkoissa ja ovat siten vain niiden itsensä käytettävissä. Yrityksen tai organisaation edustajilla voi olla pääsy pilveen myös julkisen internetin kautta esimerkiksi VPN (Virtual Private Network) -teknologian avulla. (Carlin & Curran, 2011.)

## **2.2 Pilvipalvelutyypit**

Tässä tutkielmassa tarkasteltavat ohjelma palveluna (Software as a Service) -pilvipalvelut jakautuvat hyvin eri tyyppisiin pilvipalveluihin. Yksittäinen pilvipalveluiden tarjoaja voi tarjota myös useamman erillisen tai eri tyyppisen pilvipalvelun yhdistelmää (vrt. Googlen pilvipalvelut). Pilvipalveluiden tarjonta on jatkuvassa kasvussa ja niiden valikoima onkin tällä hetkellä jo varsin laaja. Pilvipalvelutarjonnasta löytyy mm. ilmaisia kenen tahansa käyttöön otettavissa olevia palveluita kuten verkkotallennustilapalvelut Google Drive ja Dropbox, erilaisen tiedon synkronointipalvelut Google Calendar ja iCloud) sekä ryhmä- tai yhteistyön mahdollistavat palvelut Google Docs ja MS Office 365. Pilvipalveluista löytyy myös kaupallisia ja erityisesti yrityskäyttäjille suunniteltuja palveluita kuten toiminnanohjausjärjestelmiä ja muita liiketoimintaa tukevia järjestelmiä esimerkiksi taloushallinnon järjestelmiä. Kaupallisista ja ammattimaisemmista pilvipalveluista mainittakoon myös luovien ohjelmistojen kokonaisuus Adobe Creative Cloud. Nykyisin yhä useammat aiemmin varsin hinnakat ja laajat tietojärjestelmät on mahdollista hankkia pilvipalveluna. (Bradshaw ym., 2011.)

Yksi väline pilvipalvelutyyppejen eroja kuvaamaan on Jericho -foorumin luoma pilvipalveluiden pilvikuutiomalli (Jericho Cloud Cube Model). Vuonna 2004 useista eri it-alan toimijoista koostuva it-turvallisuusliitto muodosti Jericho -foorumin pohtimaan tietotekniikan rajojen ja rajoitusten poistumisesta aiheutuvia tietoturvaongelmia, etenkin internetin yli tapahtuvien yritysten välisiin transaktioihin liittyen. Jericho -foorumi julkaisi vuonna 2009 pilvipalveluiden tekniseen toteutukseen liittyviä eroja kuvaavan pilvikuutiomallin (kuvio 2). Jericho -foorumin pilvikuutiomalli kuvaa pilvipalvelun perusominaisuuksiltaan neliulotteisena objektina. Jericho -foorumin pilvikuutiomallia voidaan hyödyntää mm. pilvipalveluiden luokittelussa ja ryhmittelyssä. Malli on suunnattu organisaatioiden käyttöön pilvipalveluiden käyttöönoton suunnittelun apuvälineeksi. Mallin kuvaamat neljä ulottuvuutta ovat sisäinen - ulkoinen, suljettu - avoin, rajattu - ei rajattu ja itse tuotettu - ulkoistettu. Sisäinen - ulkoinen -ulottuvuudella tarkoitetaan palveluun tallennetun tiedon fyysistä sijaintia eli sijaitseeko data palvelua käyttävän organisaation tiloissa vai ei. Suljettu - avoin -ulottuvuus tarkoittaa, käyttääkö palvelu avoimia vai suljettuja standardeja ja järjestelmiä. Rajattu - ei rajattu -ulottuvuus puolestaan tarkoittaa sitä, toimiiko pilvipalvelu vain eristettynä organisaation sisäisesti vai tarjoaako se mahdollisuuden vuorovaikutukseen ulkopuolisten palveluiden kanssa. Mallin neljäs ja viimeinen ulottuvuus eli itse tuotettu -ulkoistettu -ulottuvuus tarkoittaa sitä, vastaako palvelun ylläpitämisestä organisaation oma henkilöstö vai ulkopuolinen taho. (Kruz & Russell, 2010.)



KUVIO 2 Jericho pilvikuutiomalli (Kruz & Russell, 2010, 52)

## 2.3 Tiedon omistajuus ja pilvipalvelut

Perinteisesti kun tietoa tallennetaan paikallisesti analogisille tai digitaalisille medioille tai tallenteille, omistaa tallennetun tiedon sen luonut henkilö tai taho. Mikäli tallennettu tieto muodostaa teoksen, sitä suojaa lisäksi lakisääteiset tekijänoikeudet. Paikallisesti tallennetun tiedon omistajuuden ja käyttöoikeuksien hallinta on luonnollisesti selkeää ja helposti kontrolloitavaa. (Jaszi, 1991.)

Maaailman digitalisoituessa tietoa luodaan ja tallennetaan enemmän kuin koskaan aiemmin. Tallennettavan tiedon määrän kasvaessa ja tiedon liikuteltavuuden sekä saatavuuden vaatimusten lisääntyessä internetin myötä on syntynyt tarve keskitetyille tallennusratkaisuille, joissa tieto on saatavilla ajasta ja paikasta riippumatta. Tähän tarpeeseen ovat pilvipalvelut syntyneet. Pilvipalvelut ovat kiistatta käteviä ja helpottavat elämää monessa tilanteessa. Niitä käytettäessä herää kysymys tiedon omistajuudesta, kun tieto on tallennettu ulkopuolisen tahon hallinnoimaan tietovarastoon. (Reed, 2010.)

Tiedon tallentamiseen ulkopuolisen tahon tarjoamaan pilvipalveluun eli käytännössä yleensä ulkomailla sijaitseville palvelimille tai vähimmilläänkin sellaiseen tallennusjärjestelmään, jonka kontrolli ei ole tiedon tallentajan omilla käsissä asettaa rajoituksia sen suhteen, missä tilanteissa ja millaisen datan tallentamiseen niitä voidaan käyttää. Esimerkiksi Suomessa on tiukkoja lakisääteisiä rajoituksia siihen, mihin ja miten tietyn tyyppistä tietoa saa tallentaa. (Henkilötietolaki, 1999.)

## 2.4 Pilvipalveluiden käyttöehtojen vaikutus tiedon omistajuuteen ja tietoturvaan

Pilvipalveluiden käyttöehdot (EULA, End User License Agreement) on palvelun käyttöehtosopimus, joka määrittelee sekä palvelun käyttäjän että sen tarjoajan oikeudet ja velvollisuudet palvelua käytettäessä. Pilvipalveluissa käyttöehdoissa määritellään, kuka ja mihin tarkoituksiin pilvipalvelua saa käyttää. Käyttöehdoissa määritellään myös palveluun tallennetun tiedon omistajuus ja käyttöoikeudet. (PC-Mag Encyclopedia: Eula, 2014.)

Harva tavallinen pilvipalveluiden tai muunkaan palvelun tai ohjelmiston käyttäjä lukee pitkiä ja usein vaikeaselkoisiakin käyttöehtoja läpi vaan hyväksyy ne lukematta ajatellen, että ei niissä mitään ihmeellistä kuitenkaan ole. Käyttöehtoihin perehtymisen merkitys korostuu pilvipalveluissa niiden sisältämien tiedon käyttöoikeuksiin liittyvien seikkojen vuoksi. Joissain tapauksissa pilvipalvelun käyttöehdot saattavat sisältää osia, jotka estävät pilvipalvelun käyttöönottamisen kokonaan. Tällainen tilanne on todennäköisin yrityksissä tai muissa organisaatioissa. (Lau, 2003.)

Monissa pilvipalveluissa käyttäjä säilyy palveluun tallennetun tiedon omistajana ainakin muodollisesti. Pilvipalvelun käyttäjä on myös vastuussa palveluun lataamastaan tiedosta siten, että ladatessaan tiedon palveluun vastuu



tiedon laillisuudesta ja siihen liittyvistä tekijänoikeuksista on palvelun käyttäjällä. Eli jos pilvipalvelun käyttäjä lataa palveluun tietoa, joka on lainvastaista tai johon tällä ei ole oikeuksia, on siitä vastuussa palvelun käyttäjä ei palvelun tarjoaja. Vaikka pilvipalvelun käyttäjä yleensä säilyykin palveluun lataamansa tiedon omistajana, luovuttaa pilvipalvelun käyttäjä kyseisen palvelun tarjoajalle ja mahdollisesti myös tämän yhteistyökumppaneille käyttöehdoissa määritellyt käyttöoikeudet palveluun ladattuun tietoon. Nämä pilvipalvelun tarjoajalle luovutetut käyttöoikeudet ovat useissa pilvipalveluissa erittäin laajat ja monipuoliset. Pilvipalveluun tallennettuun tietoon liittyvät luovutetut käyttöoikeudet voivat sisältää oikeuksia kyseisen tiedon muokkaamiseen, julkaisuun, esittämiseen ja levittämiseen. Tästä herääkin kysymys, omistaako käyttäjä pilvipalveluun tallentamaansa tietoa, jos on luovuttanut sen käyttämiseen ja hyödyntämiseen lähes rajattomat oikeudet jollekin toiselle osapuolelle. Yleensä nämä oikeudet on kuitenkin käyttäjien onneksi rajattu kyseisen pilvipalvelun edelleen kehittämiseen tai saman palveluntarjoajan uusien palvelujen kehittämiseen eli käytännössä siis pilvipalveluntarjoajan sisäiseen käyttöön. (Bradshaw ym., 2011.)

Monien pilvipalveluiden kohdalla näyttääkin olevan palveluntarjoajien trendinä hankkia käyttöehtosopimuksen avulla varmuuden vuoksi enemmän ja laajempia oikeuksia käyttäjien palveluun tallentamaan tietoon, kuin mitä todellisuudessa normaaliolosuhteissa tarvittaisiin. Näin palveluntarjoaja välttyy mahdollisilta ongelmilta koskien puuttuvia oikeuksia, jos tälle tulee pystyä hyödyntämään palveluun tallennettua tietoa jollain uudella tavalla. Pilvipalveluiden käyttöehdoissa määritellyistä asioista tiedon omistajuuden ja tietoturvan kannalta olennainen seikka on myös se, kuinka kauan käyttöehtosopimus on voimassa ja etenkin se, päättyykö palveluntarjoajan käyttöoikeudet palveluun tallennettuun tietoon, kun käyttäjä poistaa tiedon palvelusta tai lopettaa koko palvelun käyttämisen. (Bashir, Hayes, Kesan & Zielinski, 2011.)

## **2.5 Lainsäädännön vaikutus tiedon omistajuuteen pilvipalveluissa**

Kansallinen ja kansainvälinen lainsäädäntö vaikuttaa merkittävästi myös tiedon omistajuuteen ja etenkin tiedon käyttöoikeuksiin pilvipalveluissa. Jotkin kansalliset lait tai asetukset saattavat ohittaa käyttöehdoissa määritellyn asian, kun ehtoja sovelletaan käytännössä. Tämä johtuu siitä, että ensin sovelletaan maan lainsäädäntöä ja vasta seuraavaksi sovelletaan palvelun käyttöehtoja. Vaikka lainsäädäntö useimmiten tarjoaa turvaa pilvipalveluiden käyttäjille voi se myös kääntyä heitä vastaan. Toisin sanoen lainsäädännöllä voidaan myös heikentää yksittäisen pilvipalvelun käyttäjän asemaa ja palvelun käytön turvallisuutta mahdollistamalla esimerkiksi viranomaisille tai muulle taholle pääsyoikeudet pilvipalveluun tallennettuun tietoon. Pilvipalveluun ja siihen tallennettuun tietoon sovelletaan lähtökohtaisesti sen maan lainsäädäntöä, jossa kyseisen pilvipalvelun palvelimet sijaitsevat. Jos pilvipalvelulla on palvelimia useassa maassa

(vrt. Google) sovelletaan niihin tallennettuun tietoon sen maan lainsäädäntöä, jossa palvelimet sijaitsevat. (Millard, 2013.)

Yleinen ongelma pilvipalveluihin liittyvässä lainsäädännössä on, että sitä on todella vähän tai ei lainkaan. Lisäksi olemassa olevan lainsäädännön soveltaminen pilvipalveluihin on hankalaa tai vaikeaa. Tämä ongelma ei koske pelkästään Suomea vaan tilanne on sama kaikkialla. Tämä johtuu suurelta osin siitä, että pilvipalvelut ovat varsin nuori teknologia. Pilvipalveluita koskeva lainsäädäntö olisi tarpeen laatia mahdollisimman nopeasti, koska sillä voitaisiin ennaltaehkäistä tulevia epäselvyyksiä ja riitatilanteita sekä ylipäättään selkeyttää pilvipalveluiden käyttämistä ja hyödyntämistä eri tilanteissa. Pilvipalveluihin tallennetun tiedon omistajuuteen liittyviä tai vaikuttavia lakeja ovat tietosuojalait, henkilötieto- ja henkilörekisterilait, sopimusoikeus eli sopimuksia koskevat lait ja tietenkin mahdollinen nimenomaisesti pilvipalveluita koskevat lait. (Reed, 2010.)

### 2.5.1 Suomen lainsäädäntö

Suomessa pilvipalveluiden tilanne lainsäädännön kannalta on ongelmallinen, koska Suomen lainsäädännöstä puuttuu vielä tällä hetkellä nimenomaisesti pilvipalveluja koskevat lait. Tästä seikasta johtuen pilvipalveluihin liittyviin asioihin sovelletaan eräitä muita lakeja niiltä osin kuin ne ovat sovellettavissa. Tällaisia lakeja ovat mm. henkilötietolaki, sähköisen viestinnän tietosuojalaki ja tekijänoikeuslaki sekä laki varallisuus oikeudellisista oikeustoimista. Tiedon omistajuuteen pilvipalveluissa (tai yleensäkin verkkopalveluissa) vaikuttavia tai soveltuvia lainkohtia on nykyisissä laeissa varsin vähän tai ei lainkaan.

Suomen viranomaisilla ei vielä ole suoraa, lain turvaamaa ja automaattista pääsyä suomalaisiin tai suomalaisilla palvelimilla olevien verkkopalveluihin tallennettuun dataan.

#### **Perustuslaki**

Suomen perustuslaki takaa suomen kansalaisille tietosuojan perustuslaillisena oikeutena. Tämä perustuslaillinen tietuoja kuuluu perustuslain 7§ määrittämään oikeuteen henkilökohtaiseen vapauteen ja koskemattomuuteen (Suomen perustuslaki, 2. luku, 7 §). Perustuslain henkilökohtainen vapaus kattaa fyysisen vapauden lisäksi myös vapaan tahdon sekä itsemääräämisoikeuden. Nämä puolestaan koskevat myös kansalaisten tietoa ja tieto-omaisuutta. Perustuslaki tarjoaa Suomen kansalaisille myös oikeuden luottamukselliseen viestintään (Suomen perustuslaki, 2. luku, 10 §). Pilvipalveluiden tapauksessa tällä on merkitystä, jos pilvipalveluun liittyy käyttäjän ja jonkin toisen osapuolen välistä viestintää. (Suomen perustuslaki, 1999.)

#### **Sähköisen viestinnän tietosuojalaki**

Sähköisen viestinnän tietosuojalain tarkoituksena on suojata sähköisen viestinnän luottamuksellisuus ja yksityisyys. Tietyn tyyppiset pilvipalvelut sisältävät sähköistä viestintää, joten niiden tapauksessa sähköisen viestinnän tietosuojalakea voidaan soveltaa. Sähköisen viestinnän tietosuojalaki määrittelee sähköisen

viestin, joka voi olla sähköisessä muodossa oleva teksti, puhe, video tai muu viesti, sekä siihen liittyvät tunnistamistiedot luottamuksellisiksi. Sähköisen viestinnän tietosuojalain mukaan sähköisen viestin tai sen tunnistamistietojen käsittely vaatii aina viestinnän osapuolen suostumuksen. Sähköistä viestintää sisältävien pilvipalveluiden osalta palveluntarjoajat ovat yleensä huomioineet nämäkin oikeudet palvelun käyttöehdoissa, mikäli katsovat kyseisten tietojen käsittelyn tarpeelliseksi. Sähköisen viestinnän tietosuojalaki määrittelee kuitenkin tarkkaan sen, mihin tarkoituksiin sähköisen viestin tunnistamistietoja saa käsitellä. Tunnistamistietoja saa käsitellä palvelun toteuttamista ja käyttöä, laskutusta, markkinointia, teknistä kehittämistä ja tilastollista analysointia varten. Kuitenkin tunnistamistietoja saa käsitellä vain siinä määrin kuin se on tarpeen. Sähköistä viestintää sisältävän palvelun käyttäjällä on kuitenkin sähköisen viestinnän tietosuojalain nojalla oikeus suojata viestiään ja sen tunnistamistietoja käytettävissä olevilla teknisillä keinoilla näin halutessaan. (Sähköisen viestinnän tietosuojalaki, 2004.)

Pilvipalveluiden ja etenkin niiden tietoturvan kannalta onkin tärkeää käyttää mikäli mahdollista pilvipalveluita, jotka tarjoavat tietojensalausta ja salattua tietoliikennettä ominaisuuksinaan. Vähintäänkin on hyvä varmistaa käyttävänsä palvelun mahdollisesti tarjoamia tiedonsalausominaisuuksia, mikäli ne eivät oletusarvoisesti ole käytössä. (Sähköisen viestinnän tietosuojalaki, 2004.)

#### **Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista**

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista velvoittaa palveluntarjoajan huolehtimaan, että tämän tarjoama palvelu täyttää henkilötietolain 32 § edellyttämän tietojen suojaamisen tason ja riittävän tietoturvan. Pilvipalveluiden osalta tämä tarkoittaa sitä, että pilvipalvelun käyttäjän on voitava luottaa siihen, että pilvipalveluntarjoaja on palvelussaan huomioinut lain vaatiman tietojen ja yksityisyyden suojaamisen. Pilvipalveluun tallennetut tiedot voivat tästä huolimatta olla palveluntarjoajan käytettävissä palvelun käyttöehtosopimuksessa määriteltyjen ehtojen mukaisesti. (Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista, 2009.)

#### **Tekijänoikeuslaki**

Tekijänoikeuslain tarkoitus on suojata teoksia, ovatpa ne sitten digitaalisessa tai fyysisessä muodossa. Tekijänoikeuslaki vaikuttaa tiedon omistajuuteen pilvipalvelussa, kun käyttäjän siihen tallentama tieto on tekijänoikeuksien piirissä. Tämä toteutuu esimerkiksi, kun tallennettu tieto täyttää teoksen tunnusmerkit (kuten kirja tai musiikkikappale). Vaikka tekijänoikeuslaki suojaakin käyttäjän niihin tallentamaa tietoa silloin, kun se on tämän itsensä luomaa, ei laki useinkaan suojaa palveluun tallennetun tiedon käyttämiseltä. Tämä johtuu siitä seikasta, että pilvipalvelun käyttöehtosopimuksella käyttäjä nimenomaan luovuttaa käyttö-oikeuksia omistamaansa tietoon. Näin ollen pilvipalveluntarjoaja ei riko tekijänoikeuksia hyödyntäessään käyttäjän palveluun tallentamaa tietoa käyttöehtosopimuksessa määriteltyjen tapojen mukaisesti. (Tekijänoikeuslaki, 1961.)

## **Henkilötietolaki**

Henkilötietolaki ei vaikuta suoraan varsinaiseen tiedon omistajuuteen pilvipalveluissa, mutta se on silti merkityksellinen, koska se vaikuttaa rajoittavasti siihen mitä niihin voi tallentaa. Henkilötietolaki ja erityisesti sen henkilötietorekistereitä koskevat osat määrittelevät, mihin henkilötietorekistereitä voidaan tallentaa. (Henkilötietolaki, 1999.)

Henkilötietolain tarkoitus on suojata yksilön henkilötietojen yksityisyyttä henkilötietojen käsittelyssä. Henkilötietolaki määrittelee, että henkilötietojen joukko muodostaa henkilötietorekisterin, jos sitä käsitellään automaattisella tietojen käsittelyllä tai se on järjestetty luetteloksi. Henkilötietolaki määrittelee myös, että jos henkilötietorekisteri sijaitsee Suomessa (esimerkiksi Suomessa olevilla palvelimilla) tai rekisterin ylläpitäjällä on toimipaikka Suomessa, on kyseisen henkilötietorekisterin pitäjän noudatettava henkilötietolaissa määritellyjä periaatteita. (Henkilötietolaki, 1999.)

Henkilötietolain mukaan henkilötietorekisterin hallinnointi ja käyttö pitää olla suunniteltua, perusteltua ja huolellista. Henkilötietolaki määrittelee myös mitä henkilötietoja henkilötietorekisteriin voidaan tallentaa. Esimerkiksi arkaluontoisten tietojen, kuten etnisyyteen tai terveyteen liittyvien, käsittely ja tallentaminen on kielletty. (Henkilötietolaki, 1999.)

## **Sopimusoikeus**

Pilvipalveluita käytettäessä käyttäjä hyväksyy palvelun käyttöehtosopimuksen eli tällöin palvelun käyttäjän ja tarjoajan välille syntyy palvelun käyttöä koskeva sopimus. Suomen lainsäädännön perusta sopimusoikeudessa on laki varallisuusosoikeudellisista oikeustoimista, joka määrittelee yleisesti, miten ja milloin kahden osapuolen välinen sopimus syntyy. Laki on kuitenkin peräisin jo vuodelta 1929, joten se tuntee vain yhden sopimuksen syntyvän (tarjouspyyntö-tarjous-tilaus). Näin ollen laki on varsin vanhentunut. (Laki varallisuusosoikeudellisista oikeustoimista, 1929.)

Käyttäjän hyväksyessä pilvipalvelun käyttöehdot syntyvä sopimus on sinänsä juridisesti pätevä osapuolia sitova sopimus siinä missä mikä tahansa muukin kirjallinen sopimus. Etenkin yksityisen käytön osalta pilvipalveluiden käyttöehtosopimuksissa käyttäjällä ei ole käytännössä mahdollisuutta neuvotella sopimusehdoista, vaan mikäli tämä haluaa palvelua käyttää on hänen hyväksyttävä kyseisen palvelun käyttöehdot. Yritys- ja organisaatiokäyttäjien osalta ainakin osassa palveluita (esimerkiksi räätälöidyt pilvipalvelut) voi olla mahdollista neuvotella palvelun tarjoajan kanssa tietyistä ehdoista. (Laki varallisuusosoikeudellisista oikeustoimista, 1929.)

### **2.5.2 Lainsäädäntö muualla ja kansainvälinen lainsäädäntö**

#### **Euroopan unionin lainsäädäntö**

Euroopan unionissa on säädetty sen jäsenmaita koskevia direktiivejä, jotka ohjaavat jäsenmaiden lainsäädännön kehittämistä. Näillä direktiiveillä pyritään yhtenäistämään EU:n jäsenmaiden lainsäädäntöä. Euroopan unionin perussopimus velvoittaa jäsenmaat muuttamaan lainsäädäntöään noudattamaan direk-

tiivejä. Tästä johtuen myös Euroopan unionin jäsenmaiden, myös Suomen, on täytynyt muokata tietosuojalainsäädäntöään. Euroopan unionin nykyiset direktiivit ovat vanhentuneita, eivätkä näin huomioi esimerkiksi pilvipalveluita tai sosiaalista mediaa. Tähän on kuitenkin tulossa muutos kun Euroopan unionissa suunnitelmassa on saattaa uudistetut tietosuojadirektiivit voimaan lähivuosina. Uudistuksen suunnittelu on aloitettu jo vuonna 2010. Uudistusta koskevat neuvottelut ovat kesken, eikä direktiivien lopullista muotoa ole vielä päätetty. Uudistuksen tarkoituksena on, että tietosuojadirektiivit vastaisivat paremmin olemassa oleviin ja uusiin tietosuojahaasteisiin ja uhkiin. Uudistettuun tietosuojadirektiivin on tarkoitus huomioda myös pilvipalvelut ja niiden käyttäminen sekä niiden tietoturva. (Euroopan unionin tietosuojalainsäädännön uudistaminen, 2014.)

Euroopan unionin tietosuojadirektiivi on säädetty EU:n alkuaikoina eli jo vuonna 1995 (EU-direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 95/46/EY, 1995). Se on siis auttamatta vanhentunut teknologian kehittyttyä vauhdilla sen jälkeen. Tämä direktiivi on tarkoitus kumota ja korvata uudistetulla direktiivillä lähitulevaisuudessa. Euroopan unionilla on myös sähköisen viestinnän tietosuojadirektiivi (EU-direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 2002/58/EY, 2002).

Euroopan unionin tietosuojadirektiivin tarkoitus on ennen kaikkea turvata jäsenmaiden kansalaisille henkilötietojen käsittelyssä heidän oikeutensa yksityisyyteen. Tietosuojadirektiivi estää myös jäsenvaltioita kieltämästä ja rajoittamasta henkilötietojen vapaata liikkuvuutta jäsenvaltioiden välillä edellä mainittuun yksityisyyden turvaamiseen liittyvistä syistä. Tietosuojadirektiivin tarkoituksena on myös taata EU/ETA -alueella sijaitsevien palveluiden EU/ETA -alueen valtioiden välisten tiedonsiirtojen tietoturva ja tietosuoja sekä määrittää tietojensiirron vaatimat periaatteet. (EU-direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, 1995.)

EU-direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla velvoittaa Euroopan unionin jäsenmaat kansallisen lainsäädännön avulla takaamaan sähköisten viestintäpalveluiden välityksellä tapahtuvan viestinnän ja sen tunnistetietojen luottamuksellisuus. Tämä koskee myös niitä pilvipalveluita, jotka sisältävät sähköistä viestintää. (EU-direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, 2002.)

### **Yhdysvaltojen lainsäädäntö**

Yhdysvaltojen lainsäädäntö pilvipalveluihin sovellettavilta osin on esimerkiksi Suomen vastaavaan verrattuna huomattavasti laajempi ja moninaisempi. Yhdysvaltojen lainsäädäntö koki suuria muutoksia vuoden 2001 syyskuun 11. päivän terrori-iskujen jälkeen. Tällöin myös pilvipalveluita koskeva tai niihin sovellettava lainsäädäntö muuttui merkittävästi. Terrori-iskujen jälkeen Yhdysvalloissa tehtiin nopealla aikataululla lakiin useita muutoksia ja lisäyksiä, joilla annettiin mm. Yhdysvaltojen liittovaltion tiedusteluelimille eli keskustiedustelupalvelu CIA:lle ja kotimaan turvallisuusvirasto NSA:lle oikeudet päästä käsiksi mm. yhdysvaltojen kautta kulkevaan internetliikenteeseen ja erilaisiin in-

ternetin yhdysvaltalaisten verkkopalveluiden sisältöihin terrorismin vastaisen taistelun nimissä. Yksi keskeisimmistä tällaisista lisäyksistä tai muutoksista on ns. Patriot Act -laki (Qian, Zhou, Zhou, Zhang & Xie, 2010).

Näiden lakimuutosten ja -lisäysten vuoksi Yhdysvaltojen tiedusteluviranomaisilla on käytännössä pääsy myös Yhdysvaltalaisiin pilvipalveluihin tallennettuun tietoon. Tähän tiedon keruuseen NSA:lla on vuoden 2001 terrori-iskujen jälkeen käynnistetty salainen PRISM-ohjelma, jolla NSA kerää verkkopalveluihin tallennettuja käyttäjille kuuluvia tietoja. NSA on kerännyt PRISM-ohjelmalla tietoja ainakin Googlen, Yagoon ja Microsoftin palveluista sekä Facebookista. (Kopstein & Sottek, 2013.)

### **Tietosuojalait yhdysvalloissa**

Yhdysvalloissa on olemassa kansallinen tietosuojalainsäädäntö, mutta se poikkeaa rakenteensa puolesta oleellisesti Suomen tai Euroopan unionin tietosuojalainsäädännöstä. Yhdysvaltojen tietosuojalainsäädännön pohjana on Yhdysvaltojen perustuslain 4. lisäys, joka takaa Yhdysvaltojen kansalaisille oikeuden olla suojassa tarpeettomalta tiedonkeruulta. Yhdysvalloissa on käytössä ns. toimialakohtainen tietosuojalainsäädäntö, johon kuuluu lakien lisäksi sääntely ja itesesäätely. Tämän rakenteen yhtenä keskeisenä ideana on, että alakohtainen itesesäätely ratkaisee uuden teknologian tuomat haasteet ja ongelmat. Yhdysvaltojen tietosuojalainsäädännön yksi merkittävä piirre pilvipalveluiden osalta on se, että se koskee ainoastaan yhdysvaltalaisten pilvipalveluiden yhdysvaltalaisia käyttäjiä eikä siten suojaa kyseisten pilvipalveluiden ulkomaalaisia käyttäjiä. Tätä yksityiskohtaa yhdysvalloissa myös hyödynnetään tehokkaasti tietoverkkourkintaan terrorismin torjunnan nimissä. (Clancy, 1998)

### **Patriot Act ja muut lisäykset**

Patriot Act on ehkä kansainvälisestikin tunnetuin syyskuun 2001 terrori-iskujen jälkeen tehty lisäys Yhdysvaltojen lainsäädäntöön. Pilvipalveluiden kannalta merkittävimpana seikkana tämä lisäys antoi yhdysvaltojen tiedusteluviranomaisille oikeuden päästä käsiksi yhdysvaltalaisten pilvipalveluiden muiden kuin yhdysvaltalaisten käyttäjien niihin tallentamiin tietoihin. Muita mm. pilvipalveluita ja niihin tallennettua tietoa koskevia lisäyksiä Yhdysvaltojen tietosuojalainsäädäntöön ovat ainakin Stored Communications Act (SCA) ja Foreign Intelligence Surveillance Act (FISA). Stored Communications Act on lähikohtaisesti tietosuojaa parantava laki, joka suojaa sähköisen viestinnän viestijä ja tunnistetietoja tiedonkeruuta vastaan. Laki sisältää kuitenkin määritelmät poikkeuksille, joissa tietyt hallinnolliset elimet saavat oikeudet edellä mainittujen tietojen keräämiseen esimerkiksi teleoperaattoreilta. Foreign Intelligence Surveillance Act on lisäys, joka antaa FBI:lle mahdollisuuden kerätä kolmansilta osapuolilta esimerkiksi pilvipalveluihin tallennettuja tietoja ulkomaisen tiedustelun ja kansainvälisen terrorismin torjunnan tarpeisiin. Merkittävää lisäyksessä on, että Yhdysvaltojen presidentti voi määrätä edellä mainitun tiedonkeruun ilman oikeuden määräystä. FISA:aa ja Patriot Act:ia pidetään kansainvälisesti Yhdysvaltojen tietosuojalainsäädännön pahimpina uhkina pilvipalveluihin tallennetulle tiedolle. (Bashir ym., 2011.)

**Edward Snowdenin paljastukset yhdysvaltojen tietourkinnasta**

Ehdottomasti huolestuttavin seikka yhdysvaltojen lainsäädännön lisäyksissä koskien tiedusteluviranomaisten pääsyä yhdysvaltalaisiin pilvipalveluihin tallennettuun tietoon on se, että lisäyksen tuomien oikeuksien hyödyntämisen laajuudesta ei kenelläkään ainakaan julkisesti ollut oikeastaan mitään tietoa ennen kuin entinen yhdysvaltojen tiedustelupalvelu CIA:n ja kansallisen turvallisuuspalvelu NSA:n teknikko Edward Snowden erosi tehtävistään ja paljasti medialle yhdysvaltojen tietourkinnan todellisen laajuuden (Rowen, B. 2013). Snowdenin paljastukset ovat muuttaneet myös käyttäjien suhtautumista tiedon tallentamiseen pilvipalveluihin. Paljastukset ovat herättäneet pilvipalveluiden käyttäjät miettimään niiden tietosuojaan ja tietoturvaan liittyviä seikkoja uudelleen ja huomattavasti entistä tarkemmin. Jos käyttäjät eivät voi luottaa pilvipalveluiden tarjoajiin, että heidän palveluun tallentamansa tiedot ovat turvassa, vahingoittaa se koko pilvipalvelu konseptia ja sen ympärille muodostunutta liiketoimintaa. Yrity maailman muuttuneet asenteet mm. pilvipalveluihin NSA-tietourkinnan paljastuttua selviävät mm. Yhdysvaltaisen NTT Communicationin teettämästä tuoreesta kyselystä, joka kohdistettiin yli 1000 it-yritykseen Iso-Britanniassa, Ranskassa, Saksassa, Hong Kongissa ja Yhdysvalloissa paljasti, että yritykset haluavat tietonsa säilytettävän paikallisemmin myös pilvipalveluiden tapauksessa. Lisäksi kysely paljasti, että yksi kuudesta vastanneesta yrityksestä siirtää tai peruu pilvipalveluiden käyttöönottoon liittyviä hankkeita. (NSA After-Shocks, 2014.)

### 3 METODOLOGIA

Tässä luvussa kuvataan tässä tutkielmassa käytetty tutkimusmenetelmä ja tiedonkeruutavat. Luvussa kuvataan myös kerätyn tiedon analysointiin käytetyt menetöt. Tämän tutkielman empiirinen osa toteutettu tapaustutkimuksena.

#### **Tapaustutkimus**

Tutkielman empiirinen osa on toteutettu tapaustutkimuksena. Tapaustutkimus on kvalitatiivinen eli laadullinen tutkimusstrategia, jossa paneudutaan tapauksiin sellaisenaan huomioiden kuitenkin asiayhteys. Sitä suositaan tutkimuksissa, joissa ”miten” ja ”miksi” kysymykset on esitetty, tutkijan vaikutus tapahtumiin on vähäinen ja joissa keskitytään tietyn ajan tapahtumiin todellisessa kontekstissa. Tämän kaltaista selittävää tapaustutkimusta voidaan lisäksi täydentää tutkivilla ja kuvailevilla tapaustutkimuksilla. (Yin, 2003.) Tutkielman empiirinen osa toteutettiin tapaustutkimuksena, koska se täyttää Yinin edellä mainitut kriteerit tapaustutkimukseksi soveltuvalle tutkimukselle. Tämän tutkimuksen kohteena on rajattu joukko pilvipalveluita, jotka käsitellään itsenäisinä toisistaan riippumattomina yksiköinä eli tapauksina. Lisäksi tämän tutkielman tutkimusongelmat voidaan nähdä ”miten” kysymyksinä ja tässä tutkielmassa tutkija ei vaikuta tutkimuksen kohteisiin. Tapaustutkimus soveltuu esimerkiksi kyselytutkimusta paremmin tämän tutkielman tutkimusongelmiin, koska tutkimuksen kohteena olevat pilvipalvelut on käsin valittuja ja koska niistä kerätävä aineisto on vapaasti niiden internetsivuilta saatavissa. Tapaustutkimuksen tapauksiksi on pyritty valitsemaan pilvipalveluita, jotka ovat hyvin tunnettuja ja käytettyjä. Pilvipalveluiden käytettyyden arvioinnissa on hyödynnetty Cloud Security Alliancen internetsivujen listausta kahdestakymmenestä yrityksissä käytetyimmästä pilvipalvelusta (Cook, 2014). Tapaustutkimukseen valittiin lopulta kahdeksan julkista pilvipalvelua ja ne pyrittiin valitsemaan siten, että ne edustavat eri tyyppisiä pilvipalveluita, jotta tapaustutkimuksen otanta edustaisi laajempaa pilvipalveluiden kenttää. Näistä tapaustutkimuksen kohteeksi valituista pilvipalveluista laadittiin palvelun kuvaus ja analysoitiin niiden käyttöehtodokumentteja. Käyttöehtodokumenttien analyysissä niistä käytiin läpi niiden tiedon omistajuutta ja käyttöoikeuksia sekä lainsäädäntöä koskevat osat. Tapaustutkimuksen aineiston analyysimenetelmänä käytettiin laadullista teo-



rialähtöistä analyysimetodia, jossa aineistoa analysoidaan määritellyn valmiiksi olemassa olevan teorian tai mallin avulla (Saaranen-Kauppinen & Puusniekka, 2006). Käytännössä tässä tutkielmassa tapaustutkimuksen aineistoa analysoitiin tutkielman teoriaosassa esitettyjen näkökohtien valossa. Menetelmä valittiin, koska tapaustutkimuksessa haluttiin tutkia, miten tutkielman teoriaosassa esitetyt pilvipalveluiden tiedon omistajuuteen ja käyttöoikeuksiin liittyvät seikat toteutuvat käytännössä tutkimuksen kohteeksi valituissa pilvipalveluissa. Aineisto palvelun kuvausta ja käyttöehtodokumenttien analyysiä varten hankittiin kyseisten pilvipalveluiden verkkosivuilta.

## 4 TIEDON OMISTAJUUS TUNNETUISSA PILVIPALVELUISSA

Tässä luvussa tarkastellaan tiedon omistajuutta muutamissa tunnetuissa pilvipalveluissa. Tarkastelussa keskitytään tutkielman kirjallisuusosassa esitettyihin näkökohtiin. Tarkasteluun valituista pilvipalveluista analysoidaan palvelun käyttöehtojen vaikutus tiedon omistajuuteen niissä ja palvelun tietoturvaan. Lisäksi tarkastellaan lainsäädännön vaikutuksia tiedon omistajuuteen näissä palveluissa. Myös mahdollisia tiedon omistajuuteen näissä pilvipalveluissa liittyviä oikeuden ennakkotapauksia tai muutoin julkitulleita tapauksia kartoitetaan. Jokainen tarkastelluista pilvipalveluista käsitellään omassa alaluvussaan. Nämä alaluvut jakautuvat edelleen kolmeen osaan. Ensimmäisenä osana on pilvipalvelun kuvaus. Seuraavana on pilvipalvelun käyttöehtojen analyysi. Viimeisenä osana on pilvipalveluun liittyvän lainsäädännön ja oikeustapausten kartoitus.

### 4.1 Google Apps

Tässä luvussa käsitellään Google Apps -pilvipalvelukokonaisuutta. Pilvipalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoikeuksia koskevat osat. Pilvipalvelusta käsitellään myös siihen soveltuvaa tiedon omistajuuteen liittyvää lainsäädäntöä sekä Tanskan tietosuojaviranomaisen antamaa pilvipalvelua koskevaa lausuntoa.

#### 4.1.1 Pilvipalvelun kuvaus

Google Apps on Googlen tarjoama pilvipalveluiden tai sovellusten kokonaisuus. Kokonaisuuteen kuuluu pilvisovelluksia niin viestintään kuin yhteis- ja ryhmätyön avuksikin. Google Appsin historia yltää vuoteen 2006, jolloin saataville tuli Googlen sähköpostin Gmailin yritysversio. Vuonna 2007 Google Apps laajeni Google Docsilla eli toimistosovelluksilla. Google Appsiin lisättiin Google

Drive verkkotallennuspalvelu vuonna 2012 ja mobiiliversiot Googlen pilvitoimistosovelluksista tulivat puolestaan tarjolle vuonna 2014. Google Apps on kehittynyt ja kasvanut merkittävästi kahdeksan vuoden historiansa aikana saaden aika ajoin uusia ominaisuuksia samalla kun vanhoja on kehitetty ja parannettu. (Google Apps for Work, 2014.)

Google Appsista on ilmainen versio yksityiseen käyttöön sekä kaupalliset versiot yrityksiä ja muita organisaatioita sekä oppilaitoksia varten. Google Apps -pilvipalveluiden käyttäminen edellyttää aina käyttäjätiliä eli Google tiliä. Yksityisen käyttäjän tapauksessa käyttäjä voi hallinnoida omaa tiliään Googlen sallimissa rajoissa. Organisaatiokäyttäjien, kuten yritysten ja oppilaitosten, tapauksessa käyttäjätiliä hallinnoi yleensä organisaation sisältä joku taho, joka ylläpitää kaikkia organisaation Google Apps -tilejä. Google Apps sisältää Google Docs -toimistosovellukset eli Docs -tekstinkäsittely-, Sheets -taulukkolaskenta- ja Slides -esitysgrafiikkasovelluksen. Lisäksi Google Appsista löytyy Forms -sovellus lomakkeiden ja kyselyiden laatimiseen. Edellä mainitut sovellukset höydyntävät Google Apps -kokonaisuuteen kuuluvaa Google Drive -pilvitallennuspalvelua. Näiden lisäksi Google Apps -kokonaisuuteen kuuluvat Gmail -sähköposti ja Calendar -kalenteripalvelut sekä Hangouts -pikaviestisovellus. Google Apps -kokonaisuuden toimistosovellukset, kalenteri- ja pilvitallennuspalvelu on suunniteltu ennen kaikkea ryhmä- ja tiimityöskentelyn apuvälineiksi. Pilvitallennuspalvelu mahdollistaa tiedostojen ja dokumenttien jakamisen helposti ryhmän tai tiimin jäsenten kesken. Pilvitallennuspalvelu mahdollistaa myös kevyen dokumenttien versionhallinnan. Google Apps -toimistosovellukset puolestaan mahdollistavat jopa saman dokumentin samanaikaisen muokkaamisen reaaliajassa ryhmän tai tiimin jäsenten kesken. (Google Apps for Work, 2014.)

#### 4.1.2 Käyttöehdot

Google Apps -pilvipalvelukokonaisuus käyttää käyttöehtoinaan Googlen yleisiä heidän tarjoamiaan palveluita koskevia palveluehtoja. Lisäksi erillisessä tietosuojakäytäntö -dokumentissa määritellään Googlen tietosuojakäytännöt, joissa on myös tiedon omistajuuteen liittyviä seikkoja (Googlen tietosuojakäytäntö, 2014). Googlen palveluehdoissa mainitaan ensimmäisenä tiedon omistajuuteen liittyvänä asiana se, että Googlen palveluiden käyttäjä säilyttää palveluihin tallentamansa tiedon immateriaalioikeudet itsellään. (Googlen palveluehdot, 2014.)

Heti seuraavana palveluehdoissa kuitenkin mainitaan kuitenkin, että kun käyttäjä tallentaa tietoa Google palveluihin antaa käyttäjä automaattisesti Googlle kyseistä tallennettua tietoa koskien maailmanlaajuiset ja hyvin kattavat oikeudet käyttää ja hyödyntää sitä usealla eri tavalla. Näitä oikeuksia ovat käyttäminen, ylläpitäminen, tallentaminen, jäljentäminen, muokkaaminen, välittäminen, julkaiseminen, esittäminen sekä levittäminen. Lisäksi Google voi asettaa käyttäjän tallentamaa sisältöä julkisesti esille ja jopa muokata sitä niin, että se toimii palvelussa paremmin. (Googlen palveluehdot, 2014.)

Palveluun tallennetun tiedon käyttö ja hyödyntämismahdollisuuksien jälkeen Googlen palveluehdoissa käyttäjien ja tietoturvan onneksi tarkennetaan,

että nämä edellä mainitut käyttöoikeudet on tarkoitettu ainoastaan palvelun ylläpitämiseksi, markkinoimiseksi, parantamiseksi sekä uusien palveluiden kehittämiseksi. Lisäksi palveluehdot määrittelevät nämä sisällön hyödyntämisoikeudet voimassaoleviksi, vaikka käyttäjä lopettaa Googlen palvelun tai palveluiden käytön. Palveluehdot antavat Googlle myös oikeuden käyttää automaattista sisällön analysointia esimerkiksi algoritmien avulla. Palveluehtojen mukaan tätä automaattista analysointia käytetään mm. palveluissa olevan mainonnan kohdentamiseen, palveluiden mukauttamiseen käyttäjälle sekä räätälöityihin hakutuloksiin. (Googlen palveluehdot, 2014.)

Koska Googlen pilvipalveluiden käyttäminen edellyttää aina käyttäjätiliä eli Google-tiliä riippumatta siitä onko kyse yksityisestä käyttäjästä tai organisaatiokäyttäjistä, liittyy näiden pilvipalveluiden käyttämiseen ja niihin tallennettuun sisältöön myös erilaisia henkilö- ja profiilitietoja. Tietosuojakäytäntö -dokumentti määrittelee mitä tietoja Google käyttäjistään kerää. Googlen keräämiä käyttäjien henkilö- ja profiilitietoja ovat mm. käyttäjän itse tilin luomisen yhteydessä antamat tiedot (esim. nimi, sähköpostiosoite, puhelinnumero ja jopa luottokortin numero tai valokuva), laitteistotietoja siitä millä laitteilla ja käyttöjärjestelmillä tai ohjelmistoilla käyttäjä Googlen palveluita käyttää, lokitietoja käyttäjän toiminnasta Google palveluissa (esim. hakusanoista, joita käyttäjä on käyttänyt) sekä sijaintitietoja (esim. älypuhelimien gps -paikannustiedot). Näitä henkilö- ja profiilitietoja Google kerää käyttäjistään tietosuojakäytäntö -dokumentissa määriteltyihin tarkoituksiin, joita ovat olemassa olevien palveluiden ylläpitäminen ja parantaminen sekä uusien palveluiden kehittäminen sekä Googlen itsensä ja heidän palveluidensa käyttäjien suojaaminen. Tietosuojakäytäntö-dokumentissa mainitaan myös, että näitä käyttäjien henkilö- ja profiilitietoja voidaan myös luovuttaa viranomaisille tuomioistuimen tai viranomaisen pyynnöstä. (Googlen tietosuojakäytäntö, 2014.)

#### **4.1.3 Lainsäädäntö ja mahdolliset oikeustapaukset**

Koska Googlen pilvipalveluiden käyttämät palvelinkeskukset sijaitsevat hajautetusti eri puolella maailmaa on yksittäisen käyttäjän käytännössä mahdotonta tietää, missä yksittäisessä tai hajautettuna useamassa palvelinkeskuksessa hänen Googlen palveluihin tallentamansa tieto fyysisesti sijaitsee. Yksi Googlen palvelinkeskuksista sijaitsee Suomessa ja on se siten ainakin teoriassa Suomen lainsäädännön piirissä. Koska Google on Yhdysvaltalainen ja Yhdysvaltoihin rekisteröity yhtiö, noudatetaan Googlen pilvipalveluissa lähtökohtaisesti Yhdysvaltojen lainsäädäntöä. Google määrittelee käyttöehdoissaan vielä tarkennuksena, että palveluun sovelletaan nimenomaan Kalifornian osavaltion lakeja. (Googlen palveluehdot, 2014.)

Googlen pilvipalveluihin ja etenkin niihin tallennetun tiedon omistajuuteen ja käyttöoikeuksiin sovellettava lainsäädäntö on Yhdysvalloissa huomattavasti esimerkiksi Suomen vastaavaa laajempi. Yhdysvalloissa kansallisella turvallisuuspalvelulla NSA:lla on PRISM -ohjelman puitteissa liittovaltion oikeuden tuomarin määräyksellä pääsy myös Googlen palvelimille tallennettuun da-

taan eli käytännössä Googlen pilvipalveluiden käyttäjien niihin tallentamaan tietoon. Tämä koskee etenkin Googlen pilvipalveluiden käyttäjistä muita kuin Yhdysvaltain kansalaisia, koska Yhdysvaltojen omia kansalaisia suojaavat jonkin verran paikalliset tietosuojamääräykset. (Kopstein & Sottek, 2013.)

Googlen pilvipalveluihin tallennetun tiedon omistajuuteen liittyviä varsinaisia oikeustapauksia ei löytynyt, mutta yksi tietosuojaviranomaisen päätös liittyen tiedonomistajuuteen Googlen palveluissa löytyi Tanskasta. Helmikuussa 2010 Tanskalainen Odesen kunta pyysi Tanskan tietosuojaviranomaiselta kannanottoa siihen, voidaanko Odesen kunnan kouluissa käyttää Googlen pilvipalveluita tuntien suunnitteluun ja oppilaiden oppimisen seurantaan liittyvän datan tallentamiseen ja hallinnointiin. Kunta päätyi kysymään tietosuojaviranomaisen kantaa asiaan, koska kyseinen data sisältää henkilökohtaista yksittäisiin oppilaisiin liittyvää tietoa esimerkiksi näiden terveydestä tai sosiaalisista ongelmista. Tanskan tietosuojaviranomainen käsitteli asiaa tietosuojaneuvoston kokouksessa. Tietosuojaviranomainen totesi asiaan liittyvän joitakin ongelmia tai haasteita, jotka vaativat lisäselvityksiä. Suurimpana kysymyksenä pidettiin sitä, että täyttääkö Googlen pilvipalvelut Tanskan tietosuojalakien ja määräysten mukaiset vaatimukset tietosuoja ja tietoturvan osalta ja pystyykö toisaalta Google toisaalta Odesen kunta takaamaan, että kyseiset kunnan asukkaita koskevat tiedot olisivat turvattu riittävin ja lain edellyttämin keinoin. Kysymyksiä herättivät myös, täyttyykö henkilötietojen käsittelyyn liittyvät tietosuojamääräykset: esimerkiksi poistuuko palvelusta poistettu data todella niin, että sitä ei voi palauttaa, onko tietoliikenneyhteydet Googlen palvelinkestusten välillä salattuja, miten tietoon pääsy on suojattu muualta kuin Odesen kunnan oman paikallisen kirjautumispalvelun kautta (jota oli tarkoitus käyttää Googlen palvelujen käyttämisen yhteydessä). Lokitietojen keräämiseen liittyen saadut tiedot olivat puutteellisia sen osalta, mitä tietoja kerätään ja kuinka kauan näitä tietoja säilytetään. Myös henkilötietojen siirtäminen tai siirtyminen maan rajojen ulkopuolelle käsittelyä varten oli yksi keskeisistä ongelmista tässä tapauksessa, koska henkilötietojen käsittelyä säätelevät lait antavat melko tarkat puitteet sille, miten ja missä olosuhteissa henkilötietojen siirtäminen toisiin maihin on mahdollista. Odesen kunta selvitti ja pyrki ratkaisemaan asiaan liittyviä ongelmia lähes vuoden ajan sekä toimitti tietosuojaviranomaiselle useita asiakirjoja koskien näitä selvityksiä. Siitä huolimatta niitä jäi ratkaisematta edelleen niin paljon, että Tanskan tietosuojaviranomainen päätyi loppupäätelmään, jonka mukaan Odesen kunta ei voi käyttää Googlen pilvipalveluita oppilaisiin liittyvien henkilötietojen tallentamiseen ja hallintaan. Tietosuojaviranomainen kuitenkin kertoi voivansa harkita asiaa uudelleen, jos Odesen kunta pystyy osoittamaan, että asiassa ilmenneet ongelmat on saatu ratkaistua. (Datatilsynet, 2011.)

## 4.2 Microsoft Office 365

Tässä luvussa käsitellään Microsoftin Office 365 -pilvipalvelukokonaisuutta. Pilvipalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoi-

keuksia koskevat osat. Pilvipalvelusta käsitellään myös siihen soveltuvaa tiedon omistajuuteen liittyvää lainsäädäntöä.

#### 4.2.1 Pilvipalvelun kuvaus

Office 365 on Microsoftin tarjoama pilvipalveluiden kokonaisuus. Office 365 julkaistiin heinäkuussa 2011. Office 365 koki isomman päivityksen Office 2013 paketin julkaisun yhteydessä helmikuussa 2013. Tässä päivityksessä pilvitoimistosovellukset päivittyivät vastaamaan uusia työpöytäversioita. Samassa yhteydessä saataville tuli uusia Office 365:den tilausvaihtoehtoja. Office 365:stä on tarjolla versioita niin yksityiskäyttäjille kuin yritys- ja organisaatiokäyttäjillekin. Ilmaisisessa perusversiossa käyttäjä saa käyttöönsä Office-sovellusten eli Word-tekstinkäsittely, Excel-taulukkolaskenta, PowerPoint-esitysgrafiikka, OneNote-muistiinpano sovellusten internetselaimessa toimivat verkkoversiot. Näiden lisäksi pakettiin kuuluu myös Outlook-sähköposti ja OneDrive -verkkotallennustilaa 15 gigatavun verran. Microsoft tarjoaa yksityiskäyttäjille lisäksi kuukausi- tai vuosimaksullisia Office 365 Personal ja Office 365 Home tilauksia, jotka eroavat ilmaisesta versiosta siinä, että niiden mukana saa myös ns. normaalit koneelle asennettavat työpöytäversiot Word, Excel, PowerPoint, Outlook, Access, Publisher ja OneNote -sovelluksista. Lisäksi nämä maksulliset versiot sisältävät yhden teratavun tallennustilaa OneDrive -pilvitallennuspalveluun. Personal ja Home -versiot eroavat toisistaan ainoastaan siinä, että Personal on yhden käyttäjän lisenssi ja Home sisältää lisenssit viidelle käyttäjälle. (Microsoft Office 365, 2014.)

Yritys ja organisaatiokäyttöä varten Microsoft tarjoaa useita versioita Office 365 paketista. Näitä ovat Business Essentials, Business Premium ja eritasoiset Enterprise -paketit. Business Essentials on edullisin ja kevyin versio yrityskäyttöön Office365:stä sisältäen 25 käyttäjän lisenssin teratavun käyttäjäkohtaisella OneDrive -tallennuskapasiteetilla, mutta joka ei sisällä työpöytäversioita Office sovelluksista. Business Premium ja Enterprise paketit sisältävät lisäksi työpöytäversiot Office sovelluksista. Kaikki yritys ja organisaatioversiot Office 365:stä sisältävät myös Exchange ja Lync palvelimet, julkisen internetsivuston, tiedostojen tallennuksen ja jakamisen ja intranetin. Business Premium ja Enterprise sisältävät vielä näiden lisäksi mm. Officen mobiilikäyttömahdollisuuden älypuhelimilla ja tableteilla. (Microsoft Office 365, 2014.)

#### 4.2.2 Käyttöehdot

Microsoft Office 365 palveluun tallennetun tiedon omistajuutta ja sen käyttöoikeuksia käsitellään Microsoftin palveluiden käyttöehtosopimuksessa (engl. Microsoft Services Agreement). Kyseisen dokumentin kolmas luku käsittelee palveluun tallennettua sisältöä. Tässä luvussa määritellään, että käyttäjän palveluun lataama sisältö säilyy käyttäjän omistuksessa. Dokumentin kolmannessa luvussa määritellään lisäksi, että kun käyttäjä tallentaa palveluun tietoa, saa Microsoft tuohon tietoon varsin laajat oikeudet. Nämä oikeudet sisältävät oikeuden käyttää, muokata, hyödyntää, tallentaa, uudelleen tuottaa ja esittää

käyttäjän palveluun tallentamaa tietoa. Tarkennuksena määritellään, että näitä oikeuksia hyödynnetään käyttäjän suojaamiseksi sekä Microsoftin palveluiden ja tuotteiden parantamiseen ja kehittämiseen sekä uusien palveluiden ja tuotteiden tuottamiseen. Ehdot määrittävät myös, että Microsoft voi käyttää automatisoitua prosessointia esimerkiksi sähköpostien, keskustelujen tai valokuvien sisältöön mm. haittaohjelmien torjuntaa varten, mutta myös pelkästään palveluja parantaakseen. Microsoftilla on näiden käyttöehtojen avulla myös oikeus poistaa käyttäjän palveluun tallentamaa tietoa. Mutta ennen kuin Microsoft näin tekee, se pyytää käyttäjää itse poistamaan kyseiset tiedot palvelusta. Vain jos käyttäjä ei pyynnöstä huolimatta näin toimi, poistaa Microsoft itse kyseiset tiedot. Tietojen poistaminen tulee kyseeseen, jos käyttäjä on tallentanut palveluun käyttöehtojen vastaista tai tieto rikkoo olemassa olevia tekijänoikeuksia. (Microsoft Services Agreement, 2014.)

Microsoftin Office 365 palvelun käyttö edellyttää aina käyttäjätiliä eli Microsoft Live ID:tä. Palvelun maksullisen version tilanneiden yksityiskäyttäjien tilaus linkittyy heidän Live ID -käyttäjätiliin. Yritys ja organisaatiokäyttäjillä on myös käyttäjäkohtaiset käyttäjätilit palveluun, jotka eroavat yksityiskäyttäjien tileistä lähinnä siinä, että nämä tilit ovat yleensä keskitetysti yrityksen tai organisaation sisällä toimivan ylläpitäjän hallinnassa. Koska palvelun käyttäminen vaatii käyttäjätilin, on palvelun käyttäjän annettava henkilötietojaan palvelulle. Näiden palvelun käyttäjän henkilötietojen keräämistä Microsoft määrittelee käyttöehtosopimuksen viidennessä luvussa. Nämä henkilötiedot voivat sisältää paitsi varsinaisia henkilötietoja myös tietoja laitteista, joilla näitä palveluita käytetään. Samassa käyttöehtojen luvussa määritellään, että Microsoft voi luovuttaa näitä henkilötietoja kolmansille osapuolille, esimerkiksi viranomaisille näiden pyynnöstä tai Microsoftin oikeuksien puolustamiseksi ja suojaamiseksi. (Microsoft Services Agreement, 2014.)

#### **4.2.3 Lainsäädäntö ja mahdolliset oikeustapaukset**

Lainsäädännön osalta Microsoft Office 365:een pätevät hyvin pitkälle samat seikat kuin Google App:siin. Suomen henkilötietolain määrittämät rajoitukset henkilökisterien pitämisestä ja hallinnoinnista estävät Suomessa henkilötietojen tallentamisen Google App:sin tavoin myös Microsoftin Office 365 -palveluun. Microsoft määrittelee käyttöehdoissaan maantieteellisen jaon, jonka mukaan eri alueilla (lähinnä maanosat muutamaan poikkeusta lukuun ottamatta) toimivien käyttäjien osalta sovelletaan kyseisen alueen lakeja. Yhdysvaltojen osalta noudatetaan sen osavaltion lakeja, missä käyttäjä operoi. Euroopassa noudatetaan pääsääntöisesti Luxemburgin lakeja. Poikkeuksena tähän kuitenkin Espanja, jossa on käytössä paikalliset lait. Yhdysvaltojen ja Euroopan lisäksi käyttöehdot määrittelevät sovellettavien lakien kannalta omiksi alueiksi Etelä-Amerikan, Lähi-idän ja Afrikan sekä Aasian ja eteläisen tyynenmeren. Näiden lisäksi poikkeuksena Japani, Kiina, Korea ja Taiwan ovat omat alueensa ja niissä sovelletaan kyseisten maiden lakeja. Yhdysvalloissa Microsoftin Office 365 on niin ikään Googlen tavoin PRISM -ohjelman alaisuudessa eli sikäläisillä viran-

omaisilla on suora pääsy palvelun muiden kuin yhdysvaltaisten käyttäjien si-  
ne tallentamaan dataan. (Microsoft Services Agreement, 2014.)

### 4.3 F-Secure Younited

Tässä luvussa käsitellään F-Securen Younited -pilvitallennuspalvelua. Pilvitallennuspalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoikeuksia koskevat osat. Pilvitallennuspalvelusta käsitellään myös siihen soveltuvaan tiedon omistajuuteen liittyvää lainsäädäntöä.

#### 4.3.1 Pilvipalvelun kuvaus

Younited on Suomalaisen F-Secure yhtiön kehittämä pilvitallennuspalvelu, joka julkaistiin vuoden 2014 alussa. Younited on suunnattu sekä yksityiseen että yrityskäyttöön. Palvelu toimii Suomessa sijaitsevilla palvelimilla, joten kaikki palveluun tallennettu tieto pysyy Suomen rajojen sisällä. Younited toimii paitsi tietokoneilla (internetselaimella tai erillisellä asiakasohjelmalla) myös mobiililaitteilla eli älypuhelimilla ja tableteilla. Erikoisuutena F-Securen Younitedissa on mahdollisuus ”linkittää” siihen muihin palveluihin kuten esimerkiksi Dropboxiin tallennetut tiedot. Tämän on tarkoitus mahdollistaa keskitetty pilveen tallennettujen tietojen hallinta. Palvelu tarjoaa ilmaiseksi viisi gigatavua tallennustilaa ja vuosimaksua vastaan on tarjolla kaksi eri kokoista lisätilavaihtoehtoa. Erikoisena bonuksena palvelun ennakkotestiin vuoden 2013 lopussa osallistuneet saivat palveluun ilmaisen viiden gigatavun sijasta kymmenen gigatavua tallennustilaa. (F-Secure Younited, 2014.)

#### 4.3.2 Käyttöehdot

F-Secure Younitedin käyttöehdot sisältävät kaksi dokumenttiä. Nämä dokumentit ovat lisenssiehdot (license terms) ja tietosuojakäytäntö (privacy policy). Näiden dokumenttien valossa käyttäjä omistaa palveluun tallentamansa tiedon. Käyttäjä ei myöskään luovuta mitään käyttöoikeuksia F-Securelle palveluun tallentamaansa tietoon. Toki käyttäjää kuitenkin sitoo myös Younitedissa käyttöehdot sen osalta, millaista tietoa palveluun voi tallentaa. Esimerkiksi tekijänoikeuksia loukkaavan tiedon tallentaminen palveluun on kiellettyä. (F-Secure Younited License Terms, 2014.)

F-Secure kuitenkin määrittelee kummassakin dokumentissa, mutta etenkin tietosuojakäytäntö-dokumentissa voivansa kerätä käyttäjien henkilötietoja. Nämä henkilötiedot voivat olla esimerkiksi käyttäjän palveluun rekisteröitymisen yhteydessä itse antamia tietoja, tietoja käyttäjän ostamista palvelun lisensseistä, palveluun käyttäjän tallentaman tiedon metatietoja tai sijaintitietoja jos käyttäjä on käyttänyt palvelua mobiililaitteilla. F-Secure ilmoittaa tietosuojakäytäntö-dokumentissaan käyttävänsä näitä keräämiään henkilötietoja mm. käyttäjän tunnistamiseen, palvelun ja siihen liittyvän käyttötuen parantamiseen, F-



Securen ja käyttäjien väliseen kommunikaatioon (esimerkiksi palvelua koskevien tiedotteiden kohdentamiseen) ja palvelun käyttöehtojen vastaisen käytön estämiseen mm. laittoman materiaalin poistamiseen palvelusta. (F-Secure Younited Privacy Policy, 2014.)

#### **4.3.3 Lainsäädäntö ja mahdolliset oikeustapaukset**

Koska F-Secure on suomalainen toimija eli yritys on rekisteröity Suomeen ja koska Younited toimii Suomessa sijaitsevilla palvelimilla, sovelletaan siihen lainsäädännön osalta Suomen lainsäädäntöä. F-Secure markkinoikin Younitedia pilvitalennuspalveluna, johon Yhdysvaltojen kansallisella turvallisuuspalvelulla NSA:lla ei ole suoraa pääsyä, kuten sillä on useimpiin Yhdysvaltalaisiin palveluihin. F-Secure Younited täyttääkin ainakin teoriassa Suomen henkilötietolain asettamat vaatimukset henkilötietorekisterin pitäjälle Suomessa. (F-Secure Younited License Terms, 2014.)

## **4.4 Dropbox**

Tässä luvussa käsitellään Dropbox –pilvitalennuspalvelua. Pilvitalennuspalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoikeuksia koskevat osat. Pilvitalennuspalvelusta käsitellään myös siihen soveltuvaa tiedon omistajuuteen liittyvää lainsäädäntöä.

### **4.4.1 Pilvipalvelun kuvaus**

Dropbox Dropbox Inc. -yhtiön on vuonna 2008 julkaisema Yhdysvaltalainen pilvitalennuspalvelu. Dropbox on saatavissa tietokoneille internetiselaimen kautta tai erillisenä asiakasohjelmana. Dropbox on myös saatavilla mobiililaitteille kuten älypuhelimille ja tableteille. Dropboxin palvelimet sijaitsevat palvelukeskuksissa eripuolilla maailmaa. Dropboxista on tarjolla yksityiskäyttäjille ilmainen ja maksullinen versio. Lisäksi yritys ja organisaatiokäyttöön on tarjolla oma versionsa Dropbox for Business. Ilmaisessa versiossa käyttäjälle tarjotaan aluksi 2 gigatavua tallennustilaa. Lisätilaa voi saada ilmaiseksi tiettyjä ”getting started” -ehtoja täyttämällä, kuten mainostamalla dropboxia esimerkiksi Twitterissä tai Facebookissa. Lisätallennustilaa voi myös ostaa yhden teratavun verran 10 euroa kuukaudessa maksavan Dropbox Pro -tilauksen kautta. Dropbox Pro sisältää myös tietojen salauksen ja ssl-salatun yhteyden palveluun. Dropbox on suosittu palvelu ja tuki siihen onkin sisällytetty jo useaan sovellukseen ja muuhun palveluun. Dropbox for Business -yritys versio palvelusta sisältää peruspaketina viisi teratavua tallennustilaa ja viisi käyttäjää hintaan 12 euroa per käyttäjä kuukaudessa. Dropbox mahdollistaa myös palveluun tallennettujen tiedostojen jakamisen toisille pelkän tiedostokohtaisen internetosoitteen avulla. Valokuvia on mahdollista jakaa Dropboxista automaattisesti generoitavien kuvagallerioiden avulla. (Dropbox, 2014.)

#### 4.4.2 Käyttöehdot

Dropboxin käyttöehdoissa (Terms of Service) määritellään, että käyttäjä omistaa palveluun tallentamansa tiedon. Käyttöehdoissa määritellään myös, että käyttäjä ei luovuta mitään oikeuksia palveluun tallentamaansa tietoon Dropboxille palvelua käyttäessään. Dropbox toki määrittää käyttöehdoissa oikeudekseen tarkistaa, että palveluun tallennettu tieto ei riko palvelun käyttöehdoissa mainittuja rajoituksia palvelun sovelialle käytölle ja sille mitä tietoa palveluun saa tallentaa. Vaikka Dropboxin käyttöehdot kieltävät esimerkiksi laittoman tai tekijänoikeuksia loukkaavan materiaalin tallentamisen palveluun, vapauttaa käyttöehdot Dropboxin vastuusta, mikäli joku käyttäjä kyseistä materiaalia kaikesta huolimatta palveluun tallentaa. (Dropbox Terms of Service, 2014.)

Myös Dropbox kerää käyttäjistään henkilö- ja käyttötietoja. Henkilötietoja Dropbox kerää käyttäjätileistä. Näitä tietoja ovat esimerkiksi sähköpostiosoite, puhelinnumero, maksutiedot ja katuosoite. Käyttötiedot puolestaan voivat sisältää mm. laitteista, joilla käyttäjä Dropboxia käyttää, näiden ip-osoitteita, internetselaimen tyyppi ja jopa millä sivuilla käyttäjä oli ennen Dropboxin sivuille saapumista. Dropbox käyttää keräämiään tietoja palvelun parantamiseen ja suojaamiseen. Dropbox lupaa tietosuoja käytännössään olla myymättä keräämiään henkilötietoja mainostajille tai muillekaan kolmansille osapuolille. Dropbox voi monien muiden palveluiden tapaan luovuttaa keräämiään henkilötietoja viranomaisille ihmishenkien pelastamiseksi tai puolustaakseen ja suojellakseen omia immateriaalioikeuksiaan. (Dropbox Privacy Policy, 2014.)

#### 4.4.3 Lainsäädäntö ja mahdolliset oikeustapaukset

Myös Dropbox on Googlen ja Microsoftin tavoin mukana Yhdysvaltojen turvallisuusviranomaisten PRISM -ohjelmassa eli Yhdysvaltojen kansallisella turvallisuusvirastolla NSA:lla on pääsy myös Dropboxiin tallennettuun dataan. (Kopstein & Sottek, 2013.)

Dropbox ilmoittaa käyttöehdoissaan noudattavansa Euroopan ja Yhdysvaltojen välistä henkilötietojen maiden välillä tapahtuvaa siirtoa koskevaa safe harbor sopimusta. Dropbox noudattaa sekä EU:n ja Yhdysvaltojen välistä EU-US safe harbor sopimusta, että Sveitsin ja Yhdysvaltojen välistä Swiss-US safe harbor sopimusta. (Dropbox Terms of Service, 2014.)

### 4.5 iCloud

Tässä luvussa käsitellään Applen iCloud -pilvipalvelukokonaisuutta. Pilvipalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoikeuksia koskevat osat. Pilvipalvelusta käsitellään myös siihen soveltuvaa tiedon omistajuuteen liittyvää lainsäädäntöä.

#### 4.5.1 Pilvipalvelun kuvaus

iCloud on Yhdysvaltalaisen laite- ja ohjelmistovalmistaja Applen tarjoama pilvipalvelukokonaisuus, joka on suunnattu lähinnä Applen laitteiden eli Mac-tietokoneiden ja iOS -laitteiden (iPhone ja iPad) käyttäjille. iCloud -pilvipalveluun kuuluu pilvitallennuspalvelu iCloud Drive, iWork -toimistosovellusten verkkoversiot, sähköposti, kalenteri, muistio ja muistutukset. Näiden lisäksi iCloud sisältää muutamia tietoturvaan liittyviä toimintoja, joita ovat ns. löydä laitteeni -toiminto ja varmuuskopiot. Applen iCloudin käyttäminen on ilmaista ja se tarjoaa käyttäjälle viisi gigatavua tallennustilaa. Kuu-kausimaksua vastaan on ostettavissa lisätilaa eri suuruisina paketteina aina yhteen teratavuun asti. iCloud -palvelun keskeinen idea on yhdistää Applen laitteita ja etenkin niiden sisältöä toisiinsa ns. pilvisynkronoinnin avulla. iCloudin avulla käyttäjä pääsee helposti käsiksi tiedostoihinsa ja sisältöihinsä millä tahansa iCloudiin liitämällään Applen laitteella ja myös Windows -käyttöjärjestelmällä varustetussa pc:llä. (Apple iCloud, 2014.)

#### 4.5.2 Käyttöehdot

Apple määrittelee käyttöehdoissaan, että käyttäjän iCloud -pilvipalveluun tallentaman tiedon omistajuus ei siirry missään vaiheessa Applelle. Käyttäjä kuitenkin luovuttaa Applelle käyttöoikeudet sisältöön, mikäli sisältö on tallennettu iCloud -pilvipalvelun julkisesti näkyviin osiin tai osiin, joissa käyttäjä on jakanut sisällön yhden tai useamman iCloud -käyttäjän kanssa. Nämä käyttöoikeudet sisältävät maailmanlaajuisen, rojaltivapaan oikeuden käyttää, levittää, jäljentää, muokata, sovittaa, julkaista, kääntää ja esittää julkisesti käyttäjän palveluun tallentamaa sisältöä. Käyttöehdot rajaavat kuitenkin näiden oikeuksien käyttämisen vai siihen tarkoitukseen mihin kyseinen sisältö on palveluun tallennettu. Käyttöehdot vapauttavat Applen kaikesta vastuusta mitä tulee käyttäjien palveluun tallentaman sisällön laillisuuteen. (Apple iCloud ehdot ja määräykset, 2014.)

Puolestaan tietosuojakäytännössään Apple määrittelee keräävänsä käyttäjien henkilötietoja. Näitä henkilötietoja Apple kerää esimerkiksi kun käyttäjä luo Apple ID -käyttäjätilin ja syöttää pyydetyt henkilötiedot kuten nimen, osoitteen, sähköpostiosoitteen, katuosoitteen ja mahdollisesti myös luottokortin tiedot. Apple määrittelee tietosuojakäytännössään myös, että näitä kerättyjä tietoja käytetään käyttäjälle viestintään esimerkiksi uusista tuotejulkistuksista tai päivityksistä. Henkilötietoja voidaan käyttää myös käyttäjien tunnistamiseen sekä Applen palveluiden parantamiseen ja kehittämiseen tähtäävään tutkimukseen ja analysointiin. Edelleen Apple määrittelee tietosuojakäytännössään keräävänsä myös ns. ei henkilökohtaista tietoa käyttäjistä. Ei henkilökohtainen tieto on anonymiä tietoa, jota ei voida yhdistää yksittäiseen käyttäjään. Tämä tieto sisältää esimerkiksi yleisiä tunnistetietoja laitteesta, jolla Applen iCloud -pilvipalvelua on käytetty. Nämä tiedot ovat esimerkiksi laitteen kieli, laitteen aikavyöhyke sekä sijainti. Näiden tietojen keräämisen tarkoitus on parantaa ja kehittää Applen palveluita. (Apple Privacy Policy, 2014.)

### 4.5.3 Lainsäädäntö ja mahdolliset oikeustapaukset

Apple määrittelee käyttöehdoissaan, että iCloud -pilvipalveluun sovelletaan Yhdysvaltojen Kalifornian osavaltion lakeja ja Santa Claran piirikunnan tuomioistuinta ellei erikseen ole poikkeusta jäljempänä ehdoissa määritelty. Euroopan unionin osalta iCloud -pilvipalveluun sovelletaan sen jäsenmaan lakeja ja tuomioistuimia, jonka kansalainen pilvipalvelun käyttäjä on. Suomen tapauksessa iCloud -pilvipalveluun sovelletaan siis Suomen lainsäädäntöä ja tuomioistuimia. (Apple iCloud ehdot ja määräykset, 2014.)

Apple määrittelee tietosuojakäytännössään, että se noudattaa Euroopan unionin ja Yhdysvaltojen välistä Eu-US safe harbor -sopimusta henkilötietojen käsittelyssä ja siirtämisessä Euroopan unionin ja Yhdysvaltojen välillä. Tietosuojakäytännössään Apple määrittelee myös, että Euroopan talousalueen (EEA) ja Sveitsin kansalaisista kerättyjä henkilötietoja kontrolloi Irlannissa toimiva Apple Distribution International yksikkö. (Apple Privacy Policy, 2014.)

Applen väitetään myös kuuluvan Yhdysvaltojen kansallisen turvallisuusviraston NSA:n PRISM -ohjelmaan, jossa NSA:lla on suora pääsy Yhdysvaltalaisien pilvipalveluihin tallennettuun dataan. Applen toimitusjohtaja Tim Cook on kuitenkin virallisessa kirjeessään kiistänyt asian jyrkästi ja vannonut että Apple ei anna minkään valtion viranomaisille pääsyä palvelimilleen eikä ole myöskään tehnyt viranomaisille mitään ns. takaportteja omiin järjestelmiinsä. (Tim Cook, 2014.)

## 4.6 GitHub

Tässä luvussa käsitellään GitHub -pilvipalvelua. Pilvipalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoikeuksia koskevat osat. Pilvipalvelusta käsitellään myös siihen soveltuvaan tiedon omistajuuteen liittyvää lainsäädäntöä.

### 4.6.1 Pilvipalvelun kuvaus

GitHub on 2008 julkaistu ohjelmistokehityksen apuvälineeksi suunnattu pilvipalvelu, joka tarjoaa työkalut versionhallintaan ja lähdekoodinhallintaan. GitHub perustuu komentorivipohjaiseen Git -lähdekoodinhallinta työkaluun. GitHub toimii sekä pc- ja mac -tietokoneilla että mobiililaitteilla. GitHubista on tarjolla ilmainen ja maksullinen versio. Ilmainen versio on tarkoitettu lähinnä avoimen lähdekoodin projektien käyttöön, sillä se on käytännössä julkinen. Vuosimaksua vastaa yritykset ja organisaatiot voivat hankkia GitHubista Enterprise -version. GitHub Enterprise tarjoaa yrityksen käyttöön samat työkalut kuin ilmainen versio, mutta yksityisessä suljetussa ympäristössä, johon on pääsy vain organisaatiolla itsellään. GitHub on hyvin joustava ja soveltuukin lähes kaiken kokoisiin projekteihin aina pienistä yhden kehittäjän projekteista suuriin satojen kehittäjien yritysprojekteihin. GitHub mahdollistaa ohjelmistokehitys-

tiimin helpon työskentelyn saman projektin parissa tiimin jäsenten fyysisestä sijainnista riippumatta keskitetyn lähdekoodisäilön ja siihen liittyvän versionhallinnan avulla. GitHub sisältää selkeät työkalut myös ohjelmavirheiden eli bugien havaitsemiseen ja korjaamiseen. (GitHub features, 2014.)

#### 4.6.2 Käyttöehdot

GitHubin käyttöehdoissa määritellään, että käyttäjä säilyttää kaikki tekijänoikeudet palveluun tallentamaansa sisältöön. GitHub ei tarkasta palveluun ladattavaa sisältöä, mutta omaa käyttöehtojen nojalla oikeuden poistaa sopimatonta sisältöä palvelusta. (GitHub Terms of Service, 2014.)

GitHub määrittelee tietosuojakäytäntö -dokumentissa keräävänsä käyttäjistä tietoja, kun he ovat yhteydessä GitHubiin sähköpostitse, vierailevat GitHubin internetsivuilla tai antavat tietojaan vapaaehtoisesti esimerkiksi erilaisten kyselyjen kautta. GitHub määrittelee käyttävänsä näitä tietoja palvelunsa kehittämiseen ja palvelun laadun parantamiseen. GitHub määrittelee myös, ettei se jaa tai myy näitä tietoja ulkopuoliselle. Poikkeuksena edelliseen kuitenkin palvelun väärinkäytösten selvittäminen, henkilön fyysisen turvallisuuden turvaaminen tai muu viranomaisvaatimus. Lisäksi tietosuojakäytäntö määrittelee, että jos GitHub myydään tai liitetään toiseen yhtiöön nämä käyttäjätiedot siirtyvät GitHubin mukana. Palveluun rekisteröitymisen yhteydessä GitHub kerää käyttäjän tietoja kuten nimen ja sähköpostiosoitteen. Mikäli kyseessä on palvelun maksullisen version rekisteröinti GitHub kerää myös laskutusosoitteen tai muita maksutietoja. Näitä tietoja GitHub kertoo tietosuojakäytännössään käyttävänsä palvelunsa tarjoamiseen, laskutukseen, käyttäjän tunnistamiseen sekä palvelun parantamiseen ja muuhun tutkimukseen. (GitHub Privacy Policy, 2014.)

#### 4.6.3 Lainsäädäntö ja mahdolliset oikeustapaukset

GitHub on Yhdysvaltalainen palvelu ja sen palvelimet sijaitsevat Yhdysvalloissa, joten siihen sovelletaan Yhdysvaltojen liittovaltion lakeja. Käyttöehdot määrittelevät vielä tarkemmin, että liittovaltion tason lakien lisäksi sovelletaan Kalifornian osavaltion lainsäädäntöä. GitHub -palvelun Eurooppalaisten käyttäjien tietojen siirtämistä Yhdysvaltoihin koskien GitHub noudattaa Euroopan unionin ja Yhdysvaltojen välistä Eu-US safe harbor sopimusta. Sveitsiläisten käyttäjien tietojen siirtämisen kohdalla sovelletaan Sveitsin ja Yhdysvaltojen välistä Swiss-US safe harbor sopimusta. (GitHub Privacy Policy, 2014.)

### 4.7 Adobe Creative Cloud

Tässä luvussa käsitellään Adobe Creative Cloud -pilvipalvelua. Pilvipalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoikeuksia koskevat

osat. Pilvipalvelusta käsitellään myös siihen soveltuvaa tiedon omistajuuteen liittyvää lainsäädäntöä.

#### **4.7.1 Pilvipalvelun kuvaus**

Adobe Creative Cloud on Yhdysvaltalaisen ohjelmistotalon Adoben kesällä 2013 julkaisema pilvipalvelukokonaisuus. Adobe Creative Cloud sisältää uusimmat versiot Adoben ammattilaistason ohjelmistoista, joita ovat mm. Photoshop, InDesign, Illustrator ja Premiere Pro. Adoben sovellusvalikoima sisältää sovelluksia niin valokuvien, videon, äänen, vektorigrafiikan, julkaisugrafiikan kuin internetsivujenkin luomiseen ja muokkaamiseen. Perinteisten työpöytäsovellusten lisäksi Adobe Creative Cloudiin kuun nimensä mukaisesti edellä mainittujen sovellusten verkko- eli pilviversiot sekä mobiililaitteille optimoidut versiot. Lisäksi Adobe Creative Cloud sisältää myös verkkotallennustilaa. Adobe Creative Cloud on aina maksullinen palvelu. Palvelusta veloitetaan tilauksesta riippuen, joko kuukausittain tai vuosittain. Tarjolla on erilliset versiot niin kotikäyttäjille, opiskelijoille, oppilaitoksille, valokuvaajille, yrityksille ja julkiselle sektorille. (Adobe Creative Cloud, 2014.)

#### **4.7.2 Käyttöehdot**

Adobe Creative Cloudin käyttöehdoissa määritellään että käyttäjän Adobe Creative Cloudiin lataaman sisällön omistusoikeus säilyy aina käyttäjällä. Myös Adoben tapauksessa käyttäjä luovuttaa palveluun sisältöä tallentaessaan Adobelle käyttöoikeuksia kyseiseen sisältöön. Nämä käyttöoikeudet sisältävät maailmanlaajuisen, korvauksettoman oikeuden käyttää, kopioida, julkaista, jaella, muuttaa, esittää ja kääntää käyttäjän palveluun tallentamaa sisältöä. Tämä käyttöoikeus on lisäksi siirrettävissä ja edelleen lisensoitavissa eteenpäin. Käyttöehdot määrittelevät, että Adobe käyttää näitä oikeuksiaan palvelun ylläpitämiseen ja parantamiseen. Lisätarkennuksena käyttöehdoissa määritellään erikseen, että Adobe ei tarkastele käyttäjän palveluun tallentamaa sisältöä muulloin kuin sen ollessa tarpeen palvelun tarjoamiseksi tai palvelun väärinkäytösten havaitsemiseksi ja torjumiseksi. Käyttöehdot määrittelevät, että jos käyttäjä lopettaa Adobe Creative Cloud -palvelun käyttämisen ja poistaa sisältönsä palvelusta, päättyy Adoben oikeudet käyttäjän sisältöön samalla. Käyttöehdot myös vapauttavat Adoben kaikesta vastuusta mitä tulee käyttäjien palveluun tallentamaan sisältöön. (Adoben yleiset käyttöehdot, 2014.)

#### **4.7.3 Lainsäädäntö ja mahdolliset oikeustapaukset**

Adobe Creative Cloudin yleisissä käyttöehdoissa määritellään, että jos sen käyttäjä asuu Pohjois-Amerikassa on tämä silloin Yhdysvalloissa toimivan Adobe Systems Incorporated -yhtiön asiakas ja näin ollen sovelletaan silloin palveluun Yhdysvaltojen Kalifornian osavaltion lakeja ja Santa Claran piirikunnan tuomioistuinta. Muualla maailmassa asuvat käyttäjät ovat puolestaan Irlannissa

operoivan Adobe Systems Software Ireland Limited -yhtiön asiakkaita ja siten heidän kohdalla palveluun sovelletaan Irlannin lainsäädäntöä. (Adoben yleiset käyttöehdot, 2014.)

Adobe Creative Cloud ja Adobe yhtiönä on sitoutunut noudattamaan tietojen Euroopan ja Yhdysvaltojen välillä siirtämistä kontrolloivaa Eu-US safe harbor sopimusta. (Adoben tietosuojakäytäntö, 2014.)

Lokakuussa 2013 julkisuuteen tuli tapaus, jossa Adoben kohdistuneessa tietomurrossa varastettiin lähes kolmen miljoonan käyttäjän käyttäjätunnukset sekä lisäksi tietomurrossa varastettiin ainakin Adoben ColdFusion ja Acrobat -ohjelmistojen lähdekoodit. Myöhemmin tiedot tarkentuivat ja murron kohteeksi joutuneiden käyttäjätilitietojen määrä nousi ensin 38 miljoonaan ja sittemmin arvioitiin jopa 150 miljoonan Adoben käyttäjätilin tiedot löytyvän verkkoon jaetusta 10 gigatavun tietokantakopiosta. Murto oli laajuudessaan historiallisen suuri. Varmuutta siitä, keitä hyökkäyksen takana on, ei ole saatu. (Goodin, 2014.)

## **4.8 Amazon Web Services**

Tässä luvussa käsitellään Amazon Web Services -pilvipalvelua. Pilvipalvelusta käsitellään sen käyttöehdoista tiedon omistajuutta ja käyttöoikeuksia koskevat osat. Pilvipalvelusta käsitellään myös siihen soveltuvaan tiedon omistajuuteen liittyvää lainsäädäntöä.

### **4.8.1 Pilvipalvelun kuvaus**

Amazon Web Services on verkkokauppajätti Amazonin vuonna 2006 julkaisema erittäin laaja pilvipalvelukokonaisuus. Amazon Web Services on suurilta osin suunnattu yrityksille ja organisaatioille. Amazon Web Services kokonaisuuteen kuuluu monia kuten yksityisiä virtuaalisia palvelimia, skaalautuva tietokantapalvelinjärjestelmä, DNS -nimipalvelinjärjestelmä, verkko- eli pilvitalennustila, ja data-analyysi työkalut. Pilvitalennustila ja siihen liittyvä datan synkronointi ja data-analyysi työkalut ovat tarjolla myös mobiilijärjestelmille. Amazon Web Servicen keskeinen idea on tarjota yrityksille laaja valikoima laskenta-, tallennus-, tietokanta-, analyysi-, sovellus- ja julkaisupalveluita edullisemmin ja helpommin verrattuna perinteisiin järjestelmiin. (Amazon Web Services, 2014.)

### **4.8.2 Käyttöehdot**

Amazon Web Services -pilvipalvelukokonaisuuden käyttöehdoissa määritellään, että käyttäjä säilyttää omistusoikeutensa kaikkeen palveluihin tallentamaansa sisältöön. Käyttäjä on käyttöehtojen nojalla myös täydessä vastuussa

palveluihin lataamansa tai tallentamansa sisällön laillisuudesta tai muutoin palveluun sopivuudesta. (Amazon Web Services Customer Agreement, 2014.)

#### 4.8.3 Lainsäädäntö ja mahdolliset oikeustapaukset

Amazon Web Services –pilvipalveluihin sovelletaan käyttöehtojen mukaisesti Yhdysvaltojen Washingtonin osavaltion lakeja. Amazon Web Services noudattaa tietojen siirtämistä Euroopan unionin ja Yhdysvaltojen välillä kontrolloivaa Eu-US safe harbor sopimusta. (Amazon Web Services Customer Agreement, 2014.)

### 4.9 Tulokset ja johtopäätökset

Tässä luvussa vedetään hieman yhteen tapaustutkimuksessa tehtyjä havaintoja tutkimuksen kohteena olleista pilvipalveluista ja muodostetaan niiden pohjalta joitakin johtopäätöksiä.

Tapaustutkimuksen kohteena oli kahdeksan julkista pilvipalvelua. Niistä analysoitiin niiden käyttöehtosopimusten tiedon omistajuuden kannalta oleelliset osat. Pilvipalveluiden käyttöehtosopimuksista tutkittiin myös mitä lainsäädäntöä niihin sovelletaan. Tärkeimmät havainnot on koottu alla olevaan taulukkoon (taulukko 1). Taulukosta nähdään ensinnäkin, että tapaustutkimukseen valitut pilvipalvelut edustavat useampaa eri pilvipalvelutyyppejä, joita ovat toimistosovellukset, verkkotallennustilapalvelut, luovat sovellukset ja useamman eri tyyppin yhdistelmät tai kokonaisuudet. Tärkeimpänä havaintona tapaustutkimuksessa huomattiin, kuten taulukkokin sen osoittaa, että tiedon-omistajuus ja käyttöoikeudet eivät ole yksiselitteinen asia pilvipalveluissa. Vaikka kaikissa tutkituissa pilvipalveluissa käyttäjä säilyykin palveluun tallentamansa tiedon omistajana, joutuu käyttäjä monien pilvipalveluiden kohdalla luovuttamaan pilvipalvelun tarjoajalle laajojakin käyttöoikeuksia niihin tallentamaansa tietoon. Tutkituista pilvipalveluista neljässä (eli 50 prosentissa tutkituista) käyttäjän ei tarvinnut luovuttaa palveluntarjoajalle mitään oikeuksia palveluun tallentamaansa tietoon. Voidaan siis todeta, että pilvipalveluita käytettäessä on oltava äärimmäisen tarkkana siitä, miten valittu pilvipalvelu suhtautuu käyttäjän siihen tallentamaan tietoon. Näin voidaan varmistua siitä, että pilvipalveluun tallennetun tiedon kontrolli säilyy mahdollisimman hyvin käyttäjällä itsellään. Edelleen voidaan myös todeta, että vähänkään arkaluontoisemman tiedon tallentaminen julkisiin pilvipalveluihin ei välttämättä ole järkevää, jos haluaa olla varma, että tieto ei leviä ulkopuolisten käsiin.

Toinen tärkeä tutkittu seikka pilvipalveluista oli niihin sovellettava lainsäädäntö. Tämän osalta tutkituissa pilvipalveluissa on havaittavissa hajontaa. Tutkituista kahdeksasta pilvipalvelusta viiden käyttöehtosopimuksissa määriteltiin ensisijaisesti sovellettavaksi lainsäädännöksi jonkin Yhdysvaltojen osavaltion tai Yhdysvaltojen liittovaltion lainsäädäntö. Suurin osa tutkituista pilvi-



palveluista, jotka ilmoittivat sovellettavaksi lainsäädännöksi Yhdysvaltojen lainsäädännön noudattavat nimenomaisesti Kalifornian osavaltion lainsäädäntöä. Kahdessa tutkituista pilvipalvelussa sovellettava lainsäädäntö riippuu palvelun käyttäjän asuinpaikasta. Yksi tutkituista pilvipalveluista erottui joukosta noudattaessaan Suomen lainsäädäntöä. Sovellettavan lainsäädännön osalta tutkitut pilvipalvelut ovat siis varsin kirjavia, jonka vuoksi yhteen palveluun soveltuva lainsäädännöllinen seikka ei välttämättä päde toisessa palvelussa.

TAULUKKO 1 Tapaustutkimuksen tärkeimmät havainnot

	Google Apps	Microsoft Office 364	F-Secure Younited	Dropbox	Apple iCloud	GitHub	Adobe Creative Cloud	Amazon Web Services
Palvelun tyyppi	Toimisto-sovellukset	Toimisto-sovellukset	Tallennustila	Tallennustila	Useita	Tallennustila lähdekoodeille	Luovat sovellukset	Useita
Käyttäjä omistaa palveluun tallentamansa tiedot	X	X	X	X	X	X	X	X
Käyttäjä joutuu luovuttamaan palvelun tarjoajalle oikeuksia tallentamaansa tietoon	X	X	-	-	X	-	X	-
Palveluun sovellettava lainsäädäntö	Kalifornia/USA	Riippuu käyttäjän asuinpaikasta	Suomi	Kalifornia/USA	Kalifornia/USA	USA	Riippuu käyttäjän asuinpaikasta	Washington/USA

## 5 YHTEENVETO

Tämän tutkielman tavoitteena oli selvittää käyttöehtojen ja lainsäädännön vaikutuksia tiedon omistajuuteen ja käyttöoikeuksiin pilvipalveluissa tietoturvan näkökulmasta. Tutkielman alussa asetettiin seuraavat tutkimusongelmat:

1. Pilvipalvelun käyttöehtojen vaikutus tiedon omistajuuteen ja tiedon käyttöoikeuksiin pilvipalveluissa tietoturvan näkökulmasta.
2. Kansallisen ja kansainvälisen lainsäädännön vaikutus tiedon omistajuuteen pilvipalveluissa tietoturvan näkökulmasta.

Tutkimusongelmiin vastattiin osaltaan jo tutkielman teoriaosassa. Tutkimusongelmien vastaukset vahvistettiin tutkielman empiirisen osan tapaustutkimuksella. Tutkielman teoriaosa toteutettiin kirjallisuuskatsauksena, jossa luotiin katsaus aiheeseen liittyvään kirjallisuuteen ja tieteellisiin artikkeleihin. Tutkielman teoriaosassa selvitettiin, mitä tiedon omistajuus pilvipalvelukontekstissa tarkoittaa ja mitä vaikutuksia sillä on tietoturvaan. Lisäksi tutkielman teoriaosassa selvitettiin, miten palveluiden tarjoajat voivat vaikuttaa tiedon omistajuuteen ja käyttöoikeuksiin palveluiden käyttöehtosopimusten avulla. Lopuksi teoriaosassa selvitettiin myös Suomen, Euroopan unionin ja Yhdysvaltojen lainsäädännön vaikutuksia tiedon omistajuuteen pilvipalveluissa.

Tutkielman empiirisessä osassa analysoitiin joukko julkisia pilvipalveluita. Käsitellyt pilvipalvelut valittiin hyvin tunnettujen ja paljon käytettyjen pilvipalveluiden joukosta. Lisäksi valinnoissa pyrittiin kiinnittämään huomiota siihen, että valittu joukko edustaisi erityyppisiä pilvipalveluita. Valitut pilvipalvelut käsiteltiin tapaustutkimuksena. Käsitteilyyn valituista pilvipalveluista kartoitettiin niiden käyttöehdoista tiedon omistajuuteen ja käyttöoikeuksiin vaikuttavat osat. Valituista pilvipalveluista tarkasteltiin lisäksi mitä lainsäädäntöä niihin sovelletaan. Lopuksi kartoitettiin valittuihin pilvipalveluihin liittyviä ja tiedon omistajuutta koskevia oikeustapauksia.

Pilvipalvelujen tarkastelussa kävi ilmi, että suuressa osassa pilvipalveluita käyttöehtojen tiedon omistajuutta ja käyttöehtoja koskevat osat ovat hyvin saman kaltaisia. Kaikissa käsitellyistä pilvipalveluista käyttäjä säilyttää omistus-

oikeuden palveluun tallentamaansa sisältöön, mutta puolessa niistä käyttäjä joutuu luovuttamaan palveluntarjoajalle varsin laajat oikeudet kyseisen sisällön hyödyntämiseen. Käyttäjien onneksi käyttöehdoissa kuitenkin määritellään myös mihin palveluntarjoaja näitä oikeuksia käyttää. Nämä laajat käyttöoikeudet pilvipalveluun tallennettuun sisältöön muodostavat merkittävän tietosuojariskin etenkin, jos palveluun tallennettu tieto on vähänkään merkittävämpää, koska käyttäjä ei voi olla varma pysyykö tieto vain hänen tiedossaan. Käsiteltyjen pilvipalveluiden käyttöehdot eivät myöskään ottaneet kantaa siihen, mitä palveluihin tallennetulle tiedolle käy, jos palvelun käyttäjä menehtyy tai muutoin estyy pysyvästi käyttämästä palvelua.

Lainsäädännön osalta käsitellyt pilvipalvelut noudattivat melko pitkälle samaa linjaa, sillä ne yhtä lukuun ottamatta olivat yhdysvaltalaisia palveluita. Yhdysvaltalaisiin pilvipalveluihin sovelletaan siis Yhdysvaltojen lainsäädäntöä. Joissain käsitellyistä pilvipalveluista käyttöehdot määrittivät Eurooppalaisille käyttäjille sovellettavaksi määrätyn eurooppalaisen valtion lainsäädännön. Käsiteltyjen pilvipalveluidenkin osalta kävi ilmi, että pilvipalveluja koskevan lainsäädännön puuttuminen on ilmeinen ongelma. Yhdysvaltalaisten pilvipalveluiden osalta tiedon omistajuuden ja tietoturvan kannalta on erittäin huolestuttavaa, kuinka vapaa ja suora pääsy sikäläisillä turvallisuusviranomaisilla on kyseisiin palveluihin tallennettuun sisältöön. Palveluntarjoajat eivät asialle voi tehdä käyttäjien suojaamiseksi mitään vaikka haluaisivatkin. Onneksi osa palvelun tarjoajista on jo ottanut julkisestikin tiukemman linjan asiaan. Tiedon omistajuuteen liittyviä oikeustapauksia käsittelyn kohteeksi valittuihin pilvipalveluihin liittyen ei hieman yllätyksellään juurikaan löytynyt. Keskeisenä syynä tähän voidaan pitää sitä, että pilvipalvelut ovat vielä melko tuore ilmiö ja niitä erityisesti koskeva lainsäädäntö puuttuu lähes täysin.

Tämä tutkielma täydentää esimerkiksi Bradshawn, Millardin ja Waldenin (2011) aiempaa pilvipalveluiden käyttöehtosopimuksia analysointia ja vertailua tutkimusta perehtymällä tarkemmin juuri tiedon omistajuuteen pilvipalveluissa. Tämä tutkielma täydentää myös aiempaa pilvipalveluiden tietoturvas- ta tehtyä tutkimusta, kuten Grobauerin, Stöckerin ja Walloschekin (2011) ja Ahnin, Joshin ja Takabin (2010) tutkimukset. Sillä nimenomaisesti tiedon omistajuutta ei juurikaan aiemmin ole käsitelty ainakaan näin tarkasti, vaikka se on tutkitusti (Awodele, Ibikunie & Kuyoro, 2011 ja Eloff, Ramgovind & Smith, 2010) yksi tärkeimmistä asioista pilvipalveluita käytettäessä. Tämä tutkielma myös vahvistaa tapaustutkimuksessa käsiteltyjen pilvipalveluiden osalta aiemmissa tutkimuksissa esitetyn väitteen pilvipalveluihin liittyvän tiedon omistajuuden ongelmista.

Tämän tutkielman tuloksia ei voida yleistää kaikkiin pilvipalveluihin, sillä tutkimuksessa ei voitu tutkia kaikkia pilvipalveluita, vaan tämän tutkielman otantaa oli rajoitettava pieneen joukkoon julkisia pilvipalveluita. Tästä johtuen jotkut pilvipalvelut voivat poiketa käyttöehdoiltaan ja sovellettavalta lainsäädännöltään merkittävästi tässä tutkielmassa esitetyistä tapauksista. Tämän tutkielman empiirisessä osassa tutkittiin ainoastaan julkisia pilvipalveluita. Tästä johtuen tämän tutkielman tulokset eivät välttämättä päde kaikilta osin yksityisten pilvipalveluiden kohdalla. Myöskään kaikkia mahdollisia pilvipalvelutyyppejä ei tämän tutkielman puitteissa voitu käsitellä pilvipalveluiden nykyisen

tarjonnan laajuuden vuoksi. Tämän tutkielman tuloksia voidaan pitää melko luotettavina puhuttaessa julkisista pilvipalveluista, koska tutkielman otanta edustaa rajallisuudestaan huolimatta melko kattavasti yleisimmin käytettyjen julkisten pilvipalveluiden kenttää. Lisäksi tulosten luotettavuutta parantaa se, että ne perustuvat selkeisiin toistuviin piirteisiin, eivät yksittäisiin tapauksiin, otantana olleissa pilvipalveluissa.

Tämän tutkielman pohjalta jatkotutkimusta voisi tehdä esimerkiksi kartoittamalla, mitä tulevan pilvipalveluita koskevan lainsäädännön tulisi ottaa huomioon, jotta pilvipalveluiden käyttäminen olisi entistä turvallisempaa käyttäjille. Toisena mahdollisena jatkotutkimusaiheena voisi olla mielenkiintoista yrittää selvittää, mihin ne pilvipalveluiden tarjoajat, jotka ottavat käyttöoikeuksia käyttäjien palveluihin tallentamaan tietoon, kyseistä tietoa todella käyttävät. Tämä voisi auttaa joitain pilvipalveluiden käyttäjiä ymmärtämään, miksi on merkitystä, kenellä on käyttöoikeuksia tietoonsi.

## LÄHTEET

- Adobe Creative Cloud (2014). Haettu 10.10.2014 osoitteesta <https://www.adobe.com/fi/creativecloud.html>
- Adoben yleiset käyttöehdot (2014). Haettu 10.10.2014 osoitteesta <https://www.adobe.com/fi/legal/general-terms.html>
- Adoben tietosuojakäytäntö (2014). Haettu 10.10.2014 osoitteesta <https://www.adobe.com/fi/privacy/policy.html>
- Ahn, G., Joshi, J.B.D. & Takabi, H. (2010). Security and Privacy Challenges in Cloud Computing Environments. *Security & Privacy, IEEE, 8(6)*, s. 24-31.
- Amazon Web Services (2014). Haettu 18.10.2014 osoitteesta [http://aws.amazon.com/products/?nc1=f\\_cc](http://aws.amazon.com/products/?nc1=f_cc)
- Amazon Web Services Customer Agreement (2014). Haettu 18.10.2014 osoitteesta <http://aws.amazon.com/agreement/>
- Apple iCloud (2014). Haettu 10.9.2014 osoitteesta <https://www.apple.com/fi/icloud/>
- Apple iCloud ehdot ja määräykset (2014). Haettu 10.9.2014 osoitteesta <http://www.apple.com/legal/internet-services/icloud/fi/terms.html>
- Apple Privacy Policy (2014). Haettu 10.9.2014 osoitteesta <https://www.apple.com/privacy/privacy-policy/>
- Awodele, O., Ibikunie, F. & Kuyoro S. O. (2011). Cloud Computing Security Issues and Challenges. *International Journal of Computer Networks (IJCN), Volume 3:Issue 5*, s. 247-255.
- Bashir, M. N., Hayes, C. M., Kesan, J. P. & Zielinski, R. (2011). Privacy in the cloud: going beyond the contractarian paradigm. *Proceeding GTIP '11 Proceedings of the 2011 Workshop on Governance of Technology, Information, and Policies*, s. 21-27. Haettu 6.5.2014 osoitteesta <http://dl.acm.org/citation.cfm?id=2076499>
- Bhadauria, R., Chaki, N., Chaki, R. & Sanyal, S. (2011). A Survey on Security Issues in Cloud Computing. *arXiv preprint 1109.5388* (2011). Haettu 29.11.2014 osoitteesta <http://www.chinacloud.cn/upload/2011-10/11100221191648.pdf>
- 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)*, s. 187-223.
- Brathwaite, K. S. (1983). Resolution of conflicts in data ownership and sharing in a corporate environment. *ACM SIGMIS Database, Vol. 15 Issue 1*. s. 37-42. Haettu 29.11.2014 osoitteesta <http://dl.acm.org/citation.cfm?id=1113505>
- Carlin, S. & Curran, K. (2011). Cloud Computing Security. *International Journal of Ambient Computing and Intelligence, 3(1)*, s. 14-19.

- Chang, E., Dillon, T. & Wu, C. (2010). Cloud Computing: Issues and Challenges. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference*. s. 27-33
- Clancy, T. K. (1998) What Does the Fourth Amendment Protect: Property, Privacy, or Security. *Wake Forest L. Rev.*, 33. s. 307-369. Haettu 29.11.2014 osoitteesta  
[http://www.olemiss.edu/depts/ncjrl/pdf/CLANCY/33%20Wake%20Forest%20L.%20Rev.%20307%20\(1998\).pdf](http://www.olemiss.edu/depts/ncjrl/pdf/CLANCY/33%20Wake%20Forest%20L.%20Rev.%20307%20(1998).pdf)
- Cook, B. (2014). The 20 totally most popular cloud services in today's enterprise. Haettu 26.10.2014 osoitteesta  
<https://blog.cloudsecurityalliance.org/2014/08/04/the-20-totally-most-popular-cloud-services-in-todays-enterprise/>
- Datatilsynet (2011). Processing of sensitive personal data in a cloud solution. Haettu 10.5.2014 osoitteesta  
<http://www.datatilsynet.dk/english/processing-of-sensitive-personal-data-in-a-cloud-solution/>
- Dropbox (2014). Haettu 15.8.2014 osoitteesta  
<https://www.dropbox.com/>
- Dropbox Privacy Policy (2014). Haettu 15.8.2014 osoitteesta  
<https://www.dropbox.com/privacy#privacy>
- Dropbox Terms of Service (2014). Haettu 15.8.2014 osoitteesta  
<https://www.dropbox.com/privacy#terms>
- Eloff, M. M., Ramgovind, S. & Smith, E. (2010). The Management of Security in Cloud Computing. *Information Security for South Africa (ISSA), 2010*, s. 1-7.
- Elsenpeter, R., Valte, A. & Valte, T. (2010). *Cloud Computing: A Practical Approach*. New York: McGraw-Hill Osborne.
- EU-direktiivi henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla 2002/58/EY. (2002). Haettu 15.3.2014 osoitteesta  
<http://eur-lex.europa.eu/legal-content/Fi/TXT/?uri=CELEX:32002L0058>
- EU-direktiivi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 95/46/EY. (1995). Haettu 15.3.2014 osoitteesta  
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FI:HTML>
- Euroopan unionin tietosuojalainsäädännön uudistaminen. (2014). Haettu 3.4.2014 osoitteesta  
<http://oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/euroopanunionintietosuojalainsaadannonuudistaminen.html>
- F-Secure Younited (2014). Haettu 10.8.2014 osoitteesta  
<https://www.younited.com/en/home>
- F-Secure Younited License Terms (2014). Haettu 10.8.2014 osoitteesta  
[http://www.f-secure.com/en/web/legal\\_global/terms/license-terms](http://www.f-secure.com/en/web/legal_global/terms/license-terms)
- F-Secure Younited Privacy Policy (2014). Haettu 10.8.2014 osoitteesta  
[http://www.f-secure.com/en/web/legal\\_global/privacy/privacy-policy-for-services](http://www.f-secure.com/en/web/legal_global/privacy/privacy-policy-for-services)
- GitHub features (2014). Haettu 28.9.2014 osoitteesta  
<https://github.com/features>

- GitHub Terms of Service (2014). Haettu 28.9.2014 osoitteesta <https://help.github.com/articles/github-terms-of-service/>
- GitHub Privacy Policy (2014). Haettu 28.9.2014 osoitteesta <https://help.github.com/articles/github-privacy-policy/>
- Goodin, Dan (2013). Adobe source code and customer data stolen in sustained network hack. Haettu 10.10.2014 osoitteesta <http://arstechnica.com/security/2013/10/adobe-source-code-and-customer-data-stolen-in-sustained-network-hack/>
- Google Apps for Work (2014). Haettu 22.4.2014 osoitteesta <http://www.google.com/work/apps/business/>
- Googlen palveluehdot (2014). Haettu 22.4.2014 osoitteesta <https://www.google.com/intl/fi/policies/terms/>
- Googlen tietosuojakäytäntö (2014). Haettu 22.4.2014 osoitteesta <https://www.google.com/intl/fi/policies/privacy/>
- Grance, T. & Mell, P. (2011). The NIST Definition of Cloud Computing. *Special Publication 800-145*. Haettu 20.3.2014 osoitteesta <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>
- Grobauer, B., Stöcker, E. & Walloschek, T. (2011). Understanding Cloud Computing Vulnerabilities. *Security & Privacy, IEEE*, 9(2), s. 50-57.
- Henkilötietolaki 22.4.1999/523 (1999). Haettu 15.1.2014 osoitteesta <http://www.finlex.fi/fi/laki/ajantasa/1999/19990523>
- Hirsijärvi, S., Remes, P. & Sajavaara, P. (2004). *Tutki ja kirjoita*. Helsinki:Tammi.
- Jaszi, P. (1991). Toward theory of copyright: The metamorphoses of "authorship". *Duke Law Journal* 1991:455 s. 455-502.
- Kavitha, V. & Subashini, S. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications* 34(2011). s. 1-11.
- Kopstein, J. & Sottek, T.C. (2013). Everything you need to know about PRISM Haettu 6.5.2014 osoitteesta <http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet>
- Krutz, R. L. & Russell, D. V. (2010). *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Indianapolis:Wiley Publishing, Inc.
- Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617 (2009). Haettu 3.5.2014 osoitteesta <http://www.finlex.fi/fi/laki/ajantasa/2009/20090617>
- Laki varallisuus oikeudellisista oikeustoimista 13.6.1929/228 (1929). Haettu 3.5.2014 osoitteesta <http://www.finlex.fi/fi/laki/ajantasa/1929/19290228>
- Lau, E. K. W. (2003). An empirical study of software piracy. *Business Ethics: A European Review*, 12(3), s. 233-245. Haettu 29.11.2014 osoitteesta [http://beta.orionsshoulders.com/Resources/articles/26\\_22324\\_%20\(\).pdf](http://beta.orionsshoulders.com/Resources/articles/26_22324_%20().pdf)
- Mattord, H. J. & Whitman, M. E. (2012). *Principles of Information Security*. Boston:Course Technology
- Merriam-Webster (2014). Definition of International Law. Haettu 6.5.2014 osoitteesta <http://www.merriam-webster.com/dictionary/international%20law>

- Merriam-Webster (2014). Definition of Law. Haettu 10.12.2013 osoitteesta  
<http://www.merriam-webster.com/dictionary/law>
- Microsoft Office 365 (2014). Haettu 9.6.2014 osoitteesta  
<http://office.microsoft.com/fi-fi/>
- Microsoft Service Agreement (2014). Haettu 9.6.2014 osoitteesta  
<http://windows.microsoft.com/en-ca/windows-live/microsoft-services-agreement>
- Millard, C. (2013). *Cloud Computing Law*. Oxford:Oxford University Press
- NSA After-Shocks (2014). Haettu 6.5.2014 osoitteesta  
[http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC\\_Report\\_WEB.pdf](http://nsaaftershocks.com/wp-content/themes/nsa/images/NTTC_Report_WEB.pdf)
- PC-Mag Encyclopedia (2014). Definition of Access rights. Haettu 6.5.2014 osoitteesta  
<http://www.pcmag.com/encyclopedia/term/37395/access-rights>
- PC-Mag Encyclopedia (2014). Definition of Eula. Haettu 10.12.2013 osoitteesta  
[http://www.pcmag.com/encyclopedia\\_term/0,1237,t=EULA&i=42799,00.asp](http://www.pcmag.com/encyclopedia_term/0,1237,t=EULA&i=42799,00.asp)
- Peer research: What's is holding back the cloud (2012). *Intel IT Center*. Haettu 20.11.2014 osoitteesta  
<http://www.intel.com/content/www/us/en/cloud-computing/whats-holding-back-the-cloud-peer-research-report.html>
- Qian, W., Zhou, A., Zhou, M., Zhang, R. & Xie, W. (2010). Security and Privacy in Cloud Computing: A Survey. *2010 Sixth International Conference on Semantics, Knowledge and Grids, IEEE*. s. 105-112. Haettu 29.11.2014 osoitteesta  
[http://ieeexplore.ieee.org/xpls/abs\\_all.jsp?arnumber=5663489](http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5663489)
- Ransome, J. F. & Rittinghouse, J. W. (2010). *Cloud Computing Implementation, Management and Security*. Boca Raton:CRC Press
- Reed, C. (2010). Information "Ownership" in the Cloud. *Queen Mary University of London, School of Law. Legal Studies Research Paper no. 45/2010*. Haettu 6.5.2014 osoitteesta  
[http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1562461](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1562461)
- Rowen, B. (2013). The NSA, Edward Snowden, and Surveillance. Haettu 6.5. osoitteesta  
<http://www.infoplease.com/news/2013/edward-snowden-leaks.html>
- Saaranen-Kauppinen, A. & Puusniekka, A. (2006). KvaliMOTV - Menetelmäopetuksen tietovaranto. Haettu 21.11.2014 osoitteesta  
[http://www.fsd.uta.fi/menetelmaopetus/kvali/L2\\_3\\_2\\_3.html](http://www.fsd.uta.fi/menetelmaopetus/kvali/L2_3_2_3.html)
- Suomen perustuslaki 11.6.1999/731 (1999). Haettu 15.1.2014 osoitteesta  
<http://www.finlex.fi/fi/laki/ajantasa/1999/19990731>
- Sähköisen viestinnän tietosuojalaki 16.6.2004/516 (2004). Haettu 15.1.2014 osoitteesta  
<https://www.finlex.fi/fi/laki/ajantasa/2004/20040516>
- Tekijänoikeuslaki 8.7.1961/404 (1961). Haettu 3.5.2014 osoitteesta  
<http://www.finlex.fi/fi/laki/ajantasa/1961/19610404>
- Tim Cook (2014). A message from Tim Cook about Apple's commiment to your privacy. Haettu 10.9.2014 osoitteesta  
<https://www.apple.com/privacy/>



- Van Eecke, P. (2010) Current EU legal Framework. *Cloud Computing Legal issues*, (s.4). Haettu 20.11.2014 osoitteesta [http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA\\_Cloud%20computing%20legal%20issues.pdf](http://www.isaca.org/Groups/Professional-English/cloud-computing/GroupDocuments/DLA_Cloud%20computing%20legal%20issues.pdf)
- Yin, R. K. (2003) *Study Research: Design and Methods, 3rd Edition*. Lontoo:SAGE Publications