

Vesa Lehtinen

Yksityisyys ja luottamuksen luominen internetpalveluissa

Tietojärjestelmätieteen
kandidaatintutkielma
24.4.2009

Jyväskylän yliopisto
Tietojenkäsittelytieteiden laitos
Jyväskylä

TIIVISTELMÄ

Lehtinen, Vesa

Tietojärjestelmätieteen kandidaatintutkielma / Vesa Lehtinen

Jyväskylä: Jyväskylän yliopisto, 2009, 30 s.

Kandidaatintutkielma

Tässä tutkielmassa on tarkoitus selvittää, mitä yksityisyys, yksityisyyden suojaaminen ja luottamuksen luominen ovat yleisellä tasolla ja erityisesti internetpalveluissa. Aihetta on tutkittu jonkin verran elektronisen liiketoiminnan näkökulmasta kaupallisissa palveluissa. Tässä tutkielmassa internetpalveluilla tarkoitetaan kuitenkin käyttäjilleen ilmaisia, kaikille ihmis- ja ikäryhmille tarkoitettuja yksityisen ja julkisen sektorin palveluja.

Palveluntarjoajalla tarkoitetaan tahoja palvelun taustalla. Tutkielma pyrkii vastaamaan tutkimusongelmaan: kuinka käyttäjät suhtautuvat

henkilökohtaisten tietojen antamiseen palveluntarjoajalle. Tässä yhteydessä henkilökohtaisilla tiedoilla tarkoitetaan ensisijaisesti osoite- ja

syntymäaikatietoja. Tämän lisäksi tutkielman avulla pyritään saamaan selville, minkälainen vaikutus käyttäjätietojen käsittelyllä on palvelun käyttäjiin.

Tutkittavana on myös kysymys; voidaanko luottamuksen luomisessa palvelun ja käyttäjän välille menetellä avoimella tavalla niin, että se olisi kilpailuetuna muihin palveluihin nähden. Tutkielmassa on käytetty lähteinä tietotekniikkaan,

tietojenkäsittelyyn ja filosofiaan liittyvää kirjallisuutta. Ensisijaisina lähteinä voidaan pitää Tavanin (1999 ja 2007), Kobsan (2007) ja Blomqvistin (1997)

artikkeleita. Käsitellystä aineistosta ei voida suoraan vetää johtopäätöksiä

kaikkiin tutkimusongelmiin. On kuitenkin havaittu, että käyttäjät epäröivät tietojen antamisessa ja käyttäjien tietojen käsittelyllä on merkitystä

luottamuksen luomisessa erityisesti toimittaessa reilulla tavalla.

AVAINSANAT: yksityisyys, yksityisyydensuoja, internetpalvelut, luottamus

Ohjaaja: Pasi Tyrväinen

Tietojenkäsittelytieteiden laitos

Jyväskylän yliopisto

Tarkastaja: etunimi sukunimi

Tietojenkäsittelytieteiden laitos

Jyväskylän yliopisto

SISÄLLYSLUETTELO

1 JOHDANTO.....	5
2 YKSITYISYYS JA SEN SUOJAAMINEN	7
2.1 Yksityisyyden määritelmä.....	7
2.2 Yksityisyyden suojaaminen	9
2.3 Problematiikka	11
3 YKSITYISYYDENSUOJA INTERNETPALVELUISSA	13
3.1 Henkilökohtaisten tietojen antaminen	13
3.2 Identiteetin hallinta: FIDIS- ja PRIME-projektit.....	15
3.3 P3P - Protokolla yksityisyydensuojakäytäntöjen julkaisemiseksi	17
3.4 Ongelmat nykytilanteessa	18
4 LUOTTAMUS.....	20
4.1 Määritelmä.....	20
4.2 Luottamuksen luominen	21
4.3 Luotettavat tahot.....	23
4.4 Mainejärjestelmät.....	24
5 YHTEENVETO JA PÄÄTELMÄ	25
LÄHDELUETTELO	27

1 JOHDANTO

Erilaisten sähköisten palvelujen käyttö internetissä on kasvattanut suosiotaan viime vuosina merkittävästi. Erilaiset virtuaaliset verkostoitumis-, viestintä-, ja tiedonhakupalvelut osaavat jo ennakoida käyttäjän mielenkiinnon kohteita perustuen erilaisiin käyttäjäprofiileihin tai käyttäjän aikaisempaan palvelun käyttöhistoriaan. Koska internetpalvelujen käyttäjä on reaali maailmassa olemassa oleva henkilö, jolla on identiteetti, on yksityisyydensuojaan liittyvistä asioista tullut paljon puhuttu aihe.

Jotta palvelujen käyttö olisi mahdollista, on internetin käyttäjien yhä useammin luovutettava henkilökohtaisia tietojaan palveluntarjoajalle pystyäkseen rekisteröitymään palvelun käyttäjäksi. (Paine, Joinson, Buchanan & Reips 2006) Ensimmäisenä tutkimusongelmana onkin kysymys: kuinka käyttäjät suhtautuvat henkilökohtaisten tietojen antamiseen palveluntarjoajalle. Erilaisten palvelujen käyttö saattaa edellyttää myös palvelun kannalta täysin epäolennaisten tietojen antamista. Internetin mainetta tahraavien roskapostittajien ja erilaisten huijaajien lisäksi epävarmuutta internetpalveluja kohtaan lisää se, että tietoja luovutettaessa toisen osapuolen haltuun on mahdollista, että käyttäjä ei saa tietää, mihin hänen tietojaan todellisuudessa käytetään. Tämä saattaa olla ratkaisevana negatiivisena tekijänä käyttäjän valitessa palvelua (Hoffman, Novak & Peralta 1999). Toisena tutkimusongelmana käsitellään palveluntarjoajan tietojenkäsittelymenetelmien vaikutusta palvelun käyttäjiin.

Näin ollen luottamuksen rakentaminen käyttäjän ja palveluntarjoajan välille on merkittävässä roolissa palvelun menestymisen kannalta. Osa palveluntarjoajista pyrkii rakentamaan luottamusta julkaisemalla tietosuojalausannon (privacy policy) käyttäjän tietojen käsittelystä. Kyseiset dokumentit ovat kuitenkin tyypillisesti erittäin pitkiä ja vaikeasti ymmärrettäviä (Pollach 2007).

Luottamuksen luomiseen on kuitenkin mahdollista käyttää monia erilaisia strategioita ja toimintamalleja.

Kolmantena ja viimeisenä tutkimusongelmana on kysymys, voiko palveluntarjoaja vaikuttaa luottamuksen luomiseen palvelun ja käyttäjän välille avoimella tavalla niin, että se vahvistaisi palvelun kilpailuasemaa muihin palveluihin nähden. Luottamuksen luomisen lisäksi tutkielmassa tuodaan esille erilaisia näkökulmia liittyen yksityisyyden merkitykseen yksilölle. Virtuaalimaailman kontekstissa yksityisyydensuoja on jossain määrin samanlainen kuin reaali maailmassa, mutta eroavaisuuksia on kuitenkin siinä määrin, että niihin on hyvä kiinnittää huomiota. (Tavani 1999) Yksityisyydensuojan määrittäminen on kuitenkin haasteellista sen ollessa merkitykseltään erilainen eri yksilöiden välillä (Brown & Muchira 2004). Problematiikkaa aiheeseen liittyen lisäävät yhteiskunnan eri tahojen asettamat vaatimukset henkilökohtaisten tietojen luovuttamisesta julkisten palvelujen toiminnan edellytyksenä. Viime vuosina on tullut ilmi useita tapauksia, joissa julkisen sektorin toimijat eivät ole pystyneet huolellisesti käsittelemään henkilötietoja, ja yksityisyydensuoja on vaarantunut monilta yksityishenkilöiltä. Lainsäädännön avulla pyritään vähentämään tämänkaltaisten tilanteiden aiheuttamaa epävarmuutta ja lisäämään yksilön yksityisyydensuojaa.

Tutkielman aluksi käsitellään yksityisyyttä ja sen suojaamista yleisellä tasolla. Tämän jälkeen paneudutaan enemmän yksityisyyden merkitykseen nimenomaan internetpalveluissa. Luottamusta käsittelevä kolmas luku nivoutuu yhteen kahden edellisen luvun kanssa muodostaen kokonaisuuden, jonka avulla lukija saa selkeän käsityksen siitä, miten erottamattomia termejä yksityisyys ja luottamus ovat internetpalveluja kehitettäessä.

2 YKSITYISYYS JA SEN SUOJAAMINEN

Yksityisyys on jokaiselle ihmiselle hyvin henkilökohtainen elämän osa-alue, ja henkilökohtaiset asiat halutaan pitää ainakin osin muilta piilossa. The Oxford English Dictionary (Murray, Burchfield, Simpson & Weiner 1989, 515) määrittää yksityisyyden mm. yksinolona, häiriöttä olemisena tai vapautena julkiselta huomiolta. Eksaktia kaikille ja kaikkiin tilanteisiin sopivaa määritelmää on luonnollisesti jossain määrin mahdotonta antaa. (Tavani 1999) Yleisellä tasolla voitaisiin ajatella, että yksityisyys on jokaisen ihmisen perusoikeus, joka on länsimaisissa valtioissa turvattu lainsäädännöllä. Yksityisyyttä voidaan kuitenkin tarkastella hyvin monesta eri näkökulmasta, ja tällöin lain määräämä perusoikeus jäisi melko hataraksi kuvaukseksi niin moniulotteisesta asiasta. Tavanin (2007) mukaan yksityisyyden teorit jaetaan tieteellisessä kontekstissa usein kuvaileviksi tai normatiivisiksi. Yhä tarkemmin asiaa tutkittaessa kyse on myös eri ihmisten intresseistä tai eduista, ja jossain määrin myös oikeuksista, kuten aikaisemmin on todettu. Tässä kappaleessa yksityisyyttä määritellään eri näkökulmista filosofiaa käsittelevän kirjallisuuden avulla inhimillisenä perusoikeutena unohtamatta tutkielman aiheen teknologista taustaa. Yksityisyyden suojaamista on pohdittu oikeudellisessa kontekstissa. Kappaleen lopussa käsitellään yksityisyyden määritelmän ongelmallisuutta reaali maailman eri näkökulmista.

2.1 Yksityisyyden määritelmä

Yksityisyyttä voidaan ajatella yksilön henkilökohtaisena alueena, johon kuuluvat julkinen tieto, sekä sellainen tieto, jota ei haluta jakaa yleisesti kaikkien saataville. Termiin on sovelluttu monenlaisia määritelmiä ja teorioita. Joidenkin teorioiden mukaan yksityisyys on menetettävissä oleva asia. Toisaalta yksityisyyden on mahdollista vähentyä tai kadota kokonaan. Yksityisyyttä voidaan pitää myös abstraktina alueena, johon toisen tahon

tunkeutuessa seurauksena saattaa olla luottamuksen rikkoontuminen. (Tavani 1999) Tavani jakaa yksityisyyden teorialaajukset neljään luokkaan: epätungetteleviin, erotteleviin, rajaaviin ja kontrolloiviin. Neljästä edellisestä tarkastellaan tarkemmin kahta viimeistä näiden soveltuessa paremmin informaation käsittelyyn liittyviin tilanteisiin. Tavanin mukaan olemassa olevien teorioiden ongelmallisuutena on termistön sekoittuminen. Esimerkiksi vapauden, yksinäisyyden ja yksilön oikeuksien mustavalkoinen rinnastaminen yksityisyyteen liittyvinä pääkohtina on melko riskialtista ja saattaa aiheuttaa pikemminkin epäselvyyttä kuin selkeyttä yksityisyyden käsitettä. Yksityisyyden käsitteen kehittyminen ja muuttuminen viime vuosien aikana on johtanut siihen, että kun yksityisyyden käsitettä on aikaisemmin lähestytty enemmän fyysisenä koskemattomuutena ja häiriöttömänä päätöksentekotilanteena, nykyään yksityisyyden teorioiden analysointi keskittyy myös olennaisesti henkilökohtaisten tietojen kulkuun. Yhä useammin kirjoittajat puhuvat myös tietoyksityisyydestä, jolloin viitataan suoraan henkilökohtaisen tiedon tai informaation yksityisenä pitämiseen. Kontrolli henkilökohtaisista tiedoista tai asioista on yksi tapa lähestyä yksityisyyden käsitettä. Tästä näkökulmasta yksilöllä tulisi olla jonkinlainen kontrolli koskien tietoja, joita häneen liittyen käsitellään. Rajanveto yksityisen ja julkisen tiedon välille on kuitenkin jokseenkin ongelmallista. Tähän liittyen rajaamista korostavat yksityisyyden teorialaajukset liittävät yksityisyyden käsitteeseen ajatuksen erilaisista alueista, joiden tietoihin pääsyä yksilö pystyisi rajaamaan tai kieltämään pääsyt kokonaan.

Kelly & Rowland (2000) määrittelevät yksityisyyden yksilön luonnollisena oikeutena, osana luonnon lakia, jolloin ihmisillä on syntymästään lähtien tietyt perusoikeudet. Heidän mukaansa Kantin kategorinen imperatiivi tukee yksilön oikeutta tulla kohdelluksi tasa-arvoisena muihin yksilöihin nähden, jolloin yksityisyys ei ole vain tiettyjen yksilöiden oikeus. Kaikkia koskevan tasa-arvoisen perusoikeuden lisäksi Kelly & Rowland määrittävät yksityisyyden

myös moraalisen oikeutena, jolloin yksilön oikeuksia tulee tarkastella nimenomaan yksilön, eikä koko yhteiskunnan kannalta. Tämänkaltaiseen ajatteluun yksilöstä arvokkaampana kuin yhteiskunnan yhteinen hyvä liittyy problematiikkaa, jota käsitellään myöhemmin.

Ajateltaessa yksityisyyttä jokaisen yksilön perusoikeutena yksityisyys voi myös olla keino saavuttaa jotain tai jo päämäärä itsessään. Johnson (2001, 120) painottaa yksityisyyden merkitystä välinearvona ihmissuhteiden luomisessa ja toisaalta itseisarvona autonomian saavuttamiseksi. Ihmissuhteiden luomisen edellytyksenä on tietojen jakaminen eri henkilöiden kanssa. (Johnson 2001, 121) Mitä läheisempi ihminen on, sitä enemmän hänen kanssaan voidaan jakaa henkilökohtaisia tietoja ilman, että syntyisi pelkoa luottamuksen menettämisestä. Tällöin yksityisyys voidaan ajatella ikään kuin luottamuksen kehänä, jonka koko vaihtelee riippuen suhteen syvyydestä. Autonomian kannalta ajateltuna kyse on ihmisen perusoikeudesta määrätä itseään koskevista asioista. Länsimaisissa valtioissa perusoikeudet turvataan lainsäädännöllä, ja itsemääräämisoikeus pyritään pitämään mahdollisimman laajana ja henkilökohtaisena.

2.2 Yksityisyyden suojaaminen

Yksityisyyteen liittyy oleellisesti myös sen suojaaminen. Berman & Mulligan (1999) määrittelevät yksityisyydensuojan konkreettisempaan odotuksena anonymitietistä, oikeudenmukaisuudesta ja omien tietojen kontrolloimisesta sekä luottamuksellisuudesta. Tämänkaltaisen määritelmä sopii hyvin tietotekniseen kontekstiin, jossa tieto ja sen käsittely ovat keskeisessä asemassa. Myöskään lainsäädännöllisestä näkökulmasta edelliset odotukset eivät ole lainkaan huonoja tai ristiriidassa lainsäädännön kanssa, mutta kuten aiemmin on todettu yksityisyyden käsitteen vaikeasta määriteltävyydestä, myös juridisessa kirjallisuudessa termejä yksityisyys ja yksityisyyden suojaaminen

pidetään melko ongelmallisina erityisesti lainsäädännön laajan ja epä johdonmukaisen normiston vuoksi. (Mahkonen 1997, 43) Suomen perustuslaissa on määritelty mm. yksityiselämän suojasta, jota voidaan pitää yksityisyydensuojan osa-alueena. Perustuslain toisen luvun 10. pykälässä on mainittu jokaista ihmistä koskeva yksityiselämän turva. Tämän lisäksi aiemmin samassa laissa on säädetty jokaisen ihmisen yhdenvertaisuudesta, PL 2 luku 6§. (www.finlex.fi/fi/laki/ajantasa/1999/19990731) Sähköisen viestinnän tietosuojalaissa on säädetty vielä tarkemmin yksityisyydensuojasta digitaalisessa ympäristössä ja erityisesti verkkopalveluissa. (Saarenpää 2002)

Yksityisyydensuojan historia on saanut alkunsa Yhdysvalloista. Huoli yksityisyydestä ja suojasta erityisesti valtiovallan urkinnalta on ollut vaikuttavana tekijänä, ja yksityisyys on tullut tätä kautta perustuslailliseksi oikeudeksi sekä osaksi monia kansainvälisiä ihmisoikeussopimuksia. Kansainväliset sopimukset luonnollisesti sitovat ehdot allekirjoittaneita maita, ja näin ollen Suomen, Euroopan unionin jäsenmaana, on oman lainsäädännön lisäksi otettava huomioon EU:n direktiivit ja asetukset yksityisyydensuojaan liittyviä asioita käsiteltäessä. Euroopan ihmisoikeussopimuksen perustuessa edelleen kansainvälisiin sopimuksiin vaikuttaa niiden tulkinta myös Suomen perustuslain soveltamiseen yksityisyydensuojan osalta. Merkittävänä julkilausumana pidetään myös Yhdistyneiden kansakuntien ihmisoikeusjulistusta. Vaikka lausuma ei olekaan tiettyjen tahojen tekemä sopimus, on sillä silti oikeudellista merkitystä. Valtioiden välisen lainsäädännön yhtenäistäminen helpottaisi yksityisyydensuojaan liittyviä ongelmatilanteita. Tällöin esimerkiksi internetin valtioiden rajat ylittävää palvelutarjontaa olisi helpompi käsitellä juridisesta näkökulmasta. Kansainvälinen yhteistyö lakien yhtenäistämistä on kuitenkin haasteellista Pohjoismaiden aikoinaan erilaisiksi säädettyjen, toisistaan eriävien lainsäädäntöjen ja toisaalta Euroopan unionin jäsenmailleen asettamien direktiivien tähden. (Syrjänen 2006)

Lainsäädännöllisesti yksityisyydensuoja on yhtä vaikea määrittää kuin yksityisyydensuoja yleisellä tasolla. Saarenpään mukaan tarkan määritelmän muodostaminen on äärimmäisen vaikeaa, ja näin ollen on paljon hyödyllisempää luonnehtia asiaa yleisellä tasolla. (Saarenpää 2002) Yleisellä tasolla oleva luonnehdinta on kuitenkin jokseenkin riskialtista ajatellen, että kyseessä on kuitenkin lainsäädäntö, jonka ainakin periaatteellisella tasolla tulisi olla mahdollisimman aukotonta ja tarkasti määriteltyä. Mahkonen kiinnittää erityisesti huomiota yksityisyydensuojaa edistävien lakien ja sopimusten sanojen semantiikkaan. Keskeisiä sanoja kuten "yksityisyys", "kunnia" tai "maine" ei ole määritelty lakiteksteissä kovinkaan tarkasti. (Mahkonen 1997, 44)

2.3 Problematiikka

Yksityisyyteen liittyvä problematiikka ei ole ainoastaan sen semanttinen monitulkintaisuus. Yksilön yksityisyys vaikuttaa moneen eri asiaan, ja piilossa olevia vaikutuksia on vaikea havaita, ennen kuin yksityisyyttä kavennetaan tai se kaventuu esimerkiksi teknologisten innovaatioiden kautta. Erittäin problemaattisen yksityisyyteen liittyvistä asianhaaroista tekee juuri niiden vertailemisen vaikeus puhtaasti positiivisten ja negatiivisten seurausten kannalta. Heinonen kirjoittaa digitaalisten tietojen tallentamisen ja näiden yhdistelyn johtavan ristiriitaiseen tilanteeseen. Vaikka kyseessä olisi hyvä tarkoitus, voi joissain tilanteissa esiintyä taipumusta käyttää "digitaalisen persoonan" pirstaleisia tietoja väärin tarkoituksiin. Heinosen mukaan yksityisyys kärsii aina, kun yksilön tietoja yhdistellään eri tarkoituksiin kerättyjen tietokantojen avulla. (Heinonen 2001, 157) Johnson kiinnittää huomiota myös tietojen tallentamisesta ja niiden yhdistelemisestä johtuvaan yksilön käyttäytymiseen. Kun jokainen valinta henkilön elämässä, kuten opiskelupaikka, poliittinen ja uskonnollinen vakaumus, ihmissuhteet, mielenkiinnon kohteet ja rikkomukset, tallennetaan tietokantoihin, vaikuttaa

yksilön tietoisuus seurannasta tämän käyttäytymiseen, ja demokratian tärkeä osa yksilön vapaudesta tulee uhatuksi. (Johnson 2001, 113)

Kuitenkin yksityisyyttä ja sen suojaamista joudutaan tarkastelemaan kriittisesti, kun otetaan huomioon, että yksilön oikeuksia on aina tarkasteltava myös yhteiskunnan ja useamman ihmisen edun kannalta. Yksilön oikeus johonkin ei voi olla ristiriidassa suuremman ihmisjoukon oikeuksien kanssa. Yhteiskunta ihmisten toimintaympäristönä asettaa tiettyjä velvollisuuksia yksilölle, jotta yhteiskunnan palvelut ja kanssakäyminen yksilön ja yhteiskunnan tahojen välillä toimisivat. Näin ollen yksilön oikeudet pitää tasapainottaa muiden yksilöiden ja yleisen hyvän kanssa (Kelly & Rowland 2000). Erityisesti teknologian ja yhteiskunnan kehityksen mahdollistamat digitaaliset palvelut eivät kuitenkaan voi olla automaattisesti syy yksilön yksityisyyden vähenemiseen.

3 YKSITYISYYDENSUOJA INTERNETPALVELUISSA

Yksityisyyden ja yksityisyydensuojan käsitteet ovat muuttuneet digitaalisessa kontekstissa teknologian kehityksen myötä ja tietojen siirtyttyä verkkoon. Painen ym. (2006) mukaan digitaalinen konteksti saa aikaan aivan uudenlaisia yksityisyyteen liittyviä tutkimusalueita, joihin on syytä kiinnittää erityistä huomiota. Vaikka teknologian kehitys on saanut aikaan paljon hyvää, henkilökohtaisten tietojen liikkuminen verkossa saa aikaan epävarmuutta. Yhä useampi on huolissaan tiedoistaan, koska mediassa on esitelty erilaisia väärinkäytöksiä liittyen huolimattomaan tietojen käsittelyyn. Internetin kehitys alati vuorovaikutteisemmaksi on johtanut tilanteeseen, jolloin yhä useampi internetpalvelu vaatii käyttäjältä rekisteröitymistä ja henkilökohtaisten tietojen luovuttamista.

Suosiotaan kasvattava sosiaalinen verkostoituminen on saavutettavissa erilaisten käyttäjäprofiilien avulla. Heinosen mukaan digitaalinen käyttäjäprofiili tai identiteetti luodaan useimmiten antamalla osoitetietoja ja sähköpostiosoite palvelun taustalla olevalle taholle. (Heinonen 2001, 70) Seuraavaksi käsitellään tietojen antamista, identiteetin hallintaa sekä näihin liittyvää problematiikkaa.

3.1 Henkilökohtaisten tietojen antaminen

Henkilökohtaisten tietojen jakaminen internetissä herättää paljon keskustelua ihmisten välillä, ja suhtautuminen tietojen antamiseen vaihtelee suuresti riippuen käyttäjän iästä, koulutuksesta ja tuloista. Kobsan (2007) mukaan internetiä käyttävät yksilöt jakavat melko huolettomasti tietojaan koskien elämäntyöliä, erilaisia mielenkiinnon kohteita ja maantieteellistä informaatiota. Seuraavana askeleena tietojen antamisessa pidetään internetin käyttöä ja ostotottumuksia. Kaikista vähiten halutaan antaa talouteen liittyvää

informaatiota, kuten luottokorttien numeroita. Tämän lisäksi esimerkiksi sosiaaliturvatunnukset kuuluvat kategoriaan, jonka informaatiota ei haluta jakaa internetissä.

Kuitenkin moni palveluntarjoaja vaatii tietojen luovuttamista palvelun käytön edellytyksenä perustellen asiaa esimerkiksi väärinkäytöstilanteiden varalta ja syyllisen saattamisella vastuuseen. Usein tämänkaltainen toiminta on jossain määrin perusteltua, mutta silti yksilön yksityisyys saattaa olla vaarassa. Toinen vastakohta on täysi anonymiteetti, joka on mahdollinen vain tietyissä tilanteissa. On kuitenkin selkeitä tilanteita, jolloin anonymiteetti ei ole vaihtoehto. Esimerkiksi tietyissä julkisen sektorin verkkopalveluissa käyttäjän tulee varmentaa reaali maailman identiteetti pystyäkseen hyödyntämään palveluja. Tällöin digitaalinen identiteetti toimii ikään kuin välikapaleena reaali maailman identiteetille.

Henkilökohtaisten tietojen jakaminen, riippuen kontekstista, liittyy usein myös osittaiseen tunnistautumiseen ja digitaalisen identiteetin hallintaan. Tilanteesta riippuen tietojen jakaminen on vain osittaista suhteessa käyttäjän koko identiteettiin. Käyttäjä tasapainottelee usein täydellisen anonymiteetin ja täydellisen avoimuuden välillä. Yleensä kumpikaan edellisistä ei ole mahdollista tai kannattavaa, mutta joitain tietoja tunnistautumiseen kuitenkin tarvitaan. Clauß, Kesdogan & Kölsch (2005) mukaan identiteetin hallinta verkossa toimii parhaiten pseudonyymien ja tähän linkitetyn tiedon yhdistelmänä. Tällöin kolmas luotettava osapuoli mahdollistaa tarpeen tullen identiteetin paljastamisen, mutta pääosin todentaa vain pseudonyymien käyttäjän ja tähän liitettävän tiedon paikkansapitävyyden, esimerkiksi käyttäjätilin avulla. Toistuva saman pseudonyymien käyttö on mahdollista pseudonyymikäyttäjätilin avulla, jolloin on mahdollista syöttää haluamiaan tietoja itsestään ja luoda maine pseudonyymille.

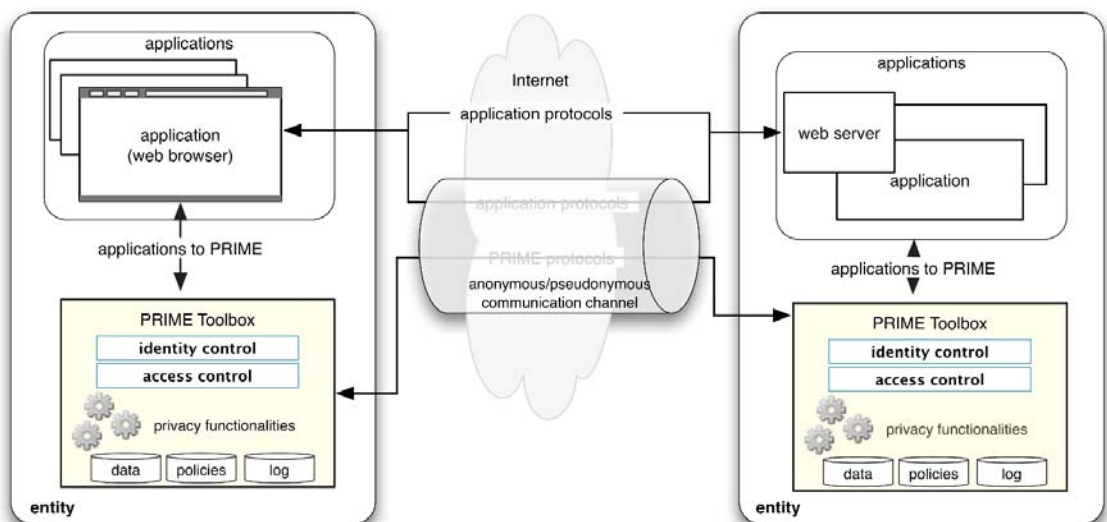
3.2 Identiteetin hallinta: FIDIS- ja PRIME-projektit

Euroopan unionin tietotekninen kehitysprojekti FIDIS (Future of IDentity in the information Society) kehittää menetelmiä, kuinka digitaalista identiteettiä voitaisiin hyödyntää niin, että se olisi yksilön ja yhteiskunnan edun mukaista. Teknologinen kehitys asettaa perinteisen käsityksen identiteetistä kyseenalaiseksi, ja tällöin on aiheellista pohtia, kuinka digitaalinen identiteetti voisi olla tukemassa perinteistä käsitystä identiteetistä laajentaen kokonaisuhyötyä eri sovellusalueilla. FIDIS pyrkii myös ottamaan huomioon erilaiset keinot yksityisyyden suojaamiseen mm. pseudonymiteetin ja anonymiteetin avulla. Identiteettienhallinta on yksityisyydensuojan merkittävä osa-alue ja näin ollen kuuluu osana kehitysprojektiin. Kehitysprojektissa identiteettienhallintajärjestelmät jaetaan kolmeen eri osa-alueeseen. Ensimmäinen näistä on järjestelmä, jossa identiteettejä hallitaan käyttäjätilien avulla. Taustalla on nk. AAA-infrastrukturi, johon kuuluu autentikointi, autorisointi ja kirjanpito. Tämä tapa yhdistää käyttäjät sekä palveluntarjoajat, ja sovellusalueena voi olla mikä tahansa palvelu, jolla halutaan yhdistää tietty käyttäjä tiettyyn palveluun. Toisena ovat organisaatioiden käytössä olevat järjestelmät koskien käyttäjäinformaatiota profiloinnin ja liiketoiminnan edistämiseksi. Kolmantena ovat järjestelmät käyttäjien kontekstisidonnaisten roolien ja pseudonyymien hallintaan. Tällöin sovellusalueena voivat olla esimerkiksi erilaiset asiakaspuolen sovellukset. (www.fidis.net)

FIDIS-projektin idea identiteettienhallinnan kehittämistä organisaatioiden ja yritysten näkökulmasta olisi aihealueen kannalta melko yksipuolinen. Tästä syystä seuraavaksi käsitellään PRIME-projektia, joka keskittyy jossain määrin enemmän käyttäjän näkökulmaan identiteettienhallinnassa.

Yksinkertaisuudessaan yksityisyydensuojan liittyvän tietosuojan parantaminen vaatii muutoksen olemassa olevan identiteettienhallinnan arkkitehtuuriin. (Camenisch, Shelat, Sommer ym. 2005) Yksi esimerkki

kehitysprojektista on Euroopan unionin PRIME-projekti (privacy and identity management for Europe). Projektin taustalla on yksityisyyden hallintaan liittyvä tekninen kehysmalli, joka on tarkoitettu aikaisemmin laaditun juridisen kontekstin tueksi. PRIME-projektissa on kolme merkittävää osapuolta: käyttäjä, palveluntarjoaja ja varmistava taho, joka toimii edellisten välissä. Käyttäjän yksityisyys turvataan erilaisilla salausmetodeilla, jotka mahdollistavat anonyymien palvelujen hyödyntämisen. Turvattu yhteys osapuolien välille mahdollistetaan standardisoidulla teknologialla, jolloin yhteys toimii ainoastaan kanavana, eikä perinteisesti ajateltuna yhteytenä, joka liittää ja tunnistaa osapuolet A ja B. Anonyymi kommunikointi osapuolien välillä taas mahdollistetaan erilaisilla salausmetodeilla hyödyntäen myös pseudonyymien mahdollisuuksia järjestelmäarkkitehtuurissa (kuva 1). Erityisen merkityksen projektissa saa nk. salattu valtuutus (cryptographic credential), joka on yksittäisen tai useamman attribuutin sisältävä sähköinen valtakirja. Valtakirjan käyttö on mahdollista yksityisellä avaimella, ja käyttäjä voi valita, mitä tietoja paljastaa palveluntarjoajalle. Väärinkäyttötilanteissa kolmas osapuoli, joka on todennut valtakirjan tiedot oikeiksi, paljastaa käyttäjän todellisen identiteetin. (www.prime-project.eu)



Kuva 1 - PRIME-projektin arkkitehtuuri (www.prime-project.eu)

3.3 P3P – Protokolla yksityisyydensuojakäytäntöjen julkaisemiseksi

World Wide Web Consortiumin julkaisema protokolla P3P (Platform for privacy preferences project) mahdollistaa standardoidun tavan tiedottaa yksityisyydensuojakäytännöistä palvelun käyttäjille. Jos käyttäjältä kerätään tietoja, XML-pohjainen P3P-protokolla informoi käyttäjää selaimen kautta ja käyttäjän ei tarvitse lukea lausuntoja yksityisyydensuojakäytännöistä. Näin myös voidaan vähentää käyttäjän epävarmuutta sivuston turvallisuuden suhteen. (www.w3.org/P3P/) Käytännössä P3P-määritysten kommunikoidessa käyttäjäagentin, esimerkiksi internetselaimen kanssa, käyttäjälle välittyy selkeä viesti siitä, miten kerättyä tietoa käytetään, kenelle tietoa mahdollisesti jaetaan ja kuinka kauan tietoja säilytetään. Käyttäjän siirtyessä sivustolle, jossa P3P-protokolla on käytössä, tietojen kerääminen on asetettu minimitasolle, ja näin käyttäjällä on mahdollisuus aidosti päättää, haluaako olla vuorovaikutuksessa palveluntarjoajan kanssa. Valinnan sivuston hyväksymisestä tai hylkäämisestä voi myös tehdä käyttäjäagentti. (Berthold & Köhntopp 2001) P3P-protokollaa on aiheellista tutkia kriittisesti, koska kyseessä on tekninen yritys lisätä luottamusta, ainakin jollain tasolla, palvelun käyttäjän suhteessa palveluntarjoajaan. Thibadeaue (2000) kiinnittää huomiota protokollan yksipuolisuuteen käyttäjän ja palvelun kanssakäymisessä. Palveluntarjoajan palvelin yksinkertaisesti ilmoittaa käyttäjälle yksityisyydensuojaa koskevista käytänteistä, ja tämän jälkeen käyttäjän tulee päättää, hyväksyykö vai hylkääkö tarjouksen. Minkäänlaista keskustelua ei synny siitä, mitä tietoja käyttäjä kenties olisi valmis antamaan. Toinen ongelmallinen asia protokollassa on sen samanlaisuus yksityisyydensuojaa koskevien lausuntojen kanssa. Protokolla ei varsinaisesti tuo mitään ratkaisua olemassa olevien tietosuojalausuntojen sekavuuteen.

3.4 Ongelmat nykytilanteessa

Yksityisyyteen liittyvät ongelmat ovat moninaisia internetin ollessa jokseenkin kehittymätön asian suhteen. Erilaiset väärinkäytökset ja yksityisyyden suojaamiseen liittyvä keskustelu mediassa ovat kuitenkin saaneet positiivista kehitystä aikaan. Palvelujen käyttäjät ovat alkaneet yhä enenevässä määrin kiinnittää huomiota palveluiden luotettavuuteen. Kuitenkin yksityisyyden aihealue on siinä mielessä haasteellinen, että hyvin paljon tiedoista, joita internetin käyttäjiltä kerätään, myydään eteenpäin tiedoista hyötyville tahoille (Tavani 1999). Tietojen myynnin kaupallinen hyöty on niin suuri, että asiasta mieluummin vaietaan kuin, että sitä käsiteltäisiin avoimesti. Vastavuoroisesti mediassa käsiteltävät paljastukset suurien yritysten tietojen väärinkäytöstä lisäävät epävarmuutta internetpalveluja kohtaan aiheuttaen harmia koko internetpalveluja tarjoavien joukolle.

Yksi ongelmallinen aihe on verkossa täytettävät lomakkeet, esimerkiksi tiettyyn palveluun rekisteröidyttäessä. Camenisch, Shelat, Sommer ym. (2005) kritisoivat yleistä harhaluuloa, että palvelujen käyttäjät antaisivat vapaaehtoisesti henkilökohtaisia tietojaan. Pikemminkin kyse on valinnanvapauden puutteesta. Pakolliset lomakekentät eivät jätä käyttäjälle mahdollisuutta olla antamatta tiettyjä tietoja, vaikka palvelun käyttö suoranaisesti ei edellyttäisi mitenkään tietojen antamista. Lomakkeiden lisäksi sivuston käytöstä voi tallentua käyttäjän koneelle nk. Cookie, eli keksi-tiedosto, jonka avulla palvelin saa tietoa käyttäjän vierailuista sivustolla. Kerättävän selaushistorian avulla käyttäjää voidaan helpommin profiloida ja esimerkiksi mainontaa voidaan kohdentaa tarkemmin oikeanlaiseen kohderyhmään. Erityisen ongelmallisia ovat mainossivustot, joiden kautta kuljettaessa käyttäjän erilaiset mielenkiinnon kohteet ovat ristilinkitettävissä ja paremmin seurattavissa.

Internetpalvelujen käyttäjien huolta väärinkäytöksen suhteen on yritetty häivyttää erilaisilla tietosuojan ja yksityisyyteen liittyvillä kirjoitetuilla lausunnoilla. Valitettavasti lausunnot ovat osoittautuneet tutkimusten valossa melko epäselviksi ja epäeettisiksi (Pollach 2007). Pollach on tutkinut lausuntojen kieliasua ja tehnyt mielenkiintoisia löytöjä koskien esimerkiksi yritysten tapaa painottaa positiivisia asioita ja pitää taka-alalla yksityisyyden loukkauksia. Tämän lisäksi lausuntojen lukijalle jää helposti epäselväksi, onko tämä lupautunut johonkin, jos lupautumista ei nimenomaan ole poissuljettu lausunnossa. Pollach löysi myös merkittävää epäselvyyttä kuvaamaan toistoja tietojen käsittelyssä; esimerkiksi sanoja ja sanontoja "ajoittain", "aika ajoin", "silloin tällöin" ja "joskus" käytetään korostetussa määrin. Kokonaisuudessaan teksti on useimmiten vaikeasti luettavissa. Kaiken takana lienee palveluntarjoajan keskittyminen enemmänkin mahdollisiin oikeudenkäynteihin tehokkaalla todistusaineistolla, kuin asiakkaan yksityisyydestä välittäminen. Pollach uskaltautuu päättelemään, että paremmin laaditut, selkeästi asiakasta informoiviin paloihin jaetut lausunnot yksityisyydestä ja tietojen käsittelystä herättäisivät paremmin luottamusta palvelun käyttäjässä. Lausunto olisi näin myös huomattavasti helpompi lukea ja palvelisi käyttötarkoitusta tehokkaammin.

Edellisten lisäksi ongelmana lienee myös yhteisten käytäntöjen vakiintumattomuus. Erilaisten toimintamallien määrä internetissä on valtava, ja esimerkiksi juuri digitaalisen identiteetin kokonaisvaltainen hyödyntäminen vaatisi standardisointia ja hallinnollisten sekä kaupallisten tahojen tehokkaampaa yhteistyötä. Teknologian ja erityisesti internetin kehityksen dynaamisuus on vaikeasti hallittavissa, ja erilaisia uusia innovaatioita tulee nopeammin kuin niihin ehditään reagoimaan.

4 LUOTTAMUS

Internetpalvelujen käyttäjien yksityisyyteen liittyen on aiheellista tutkistella hiukan tarkemmin luottamusta ja luottamuksen luomista osapuolien välille. Luottamuksen luominen reaali- maailmassa kahden osapuolen välille on aikaa vievää, ja luottamus syntyy vähitellen henkilöiden tutustuesssa toisiinsa sekä jakaen tietoja itsestään. Internetissä tahojen välillä apuvälineenä on teknologia. Luottamuksen luominen on jokseenkin samanlaista, mutta luottamuksen luomisen tilanne saattaa olla ajallisesti äärettömän paljon lyhyempi. Tämän lisäksi palvelun käyttäjä kuuluu erilaisiin reaali- ja digitaalisen maailman yhteisöihin, jotka luovat mielikuvia ja jakavat kokemuksia keskenään, jolloin vertaisryhmien vaikutus palvelun luotettavuuteen on merkittävä (Tiainen, Luomala, Kurki ym. 2004). Luottamusta herättäviä tekijöitä voidaan kuitenkin mallintaa, ja luottamuksen luomiseen on erilaisia strategioita. Kobsan (2007) mukaan esimerkiksi verkkosivun ammattilaismainen suunnittelu, hyvä käytettävyys ja linkit toisilta luotettavilta tahoilta sivustolle ovat huomion arvoisia suunniteltaessa internetpalvelua.

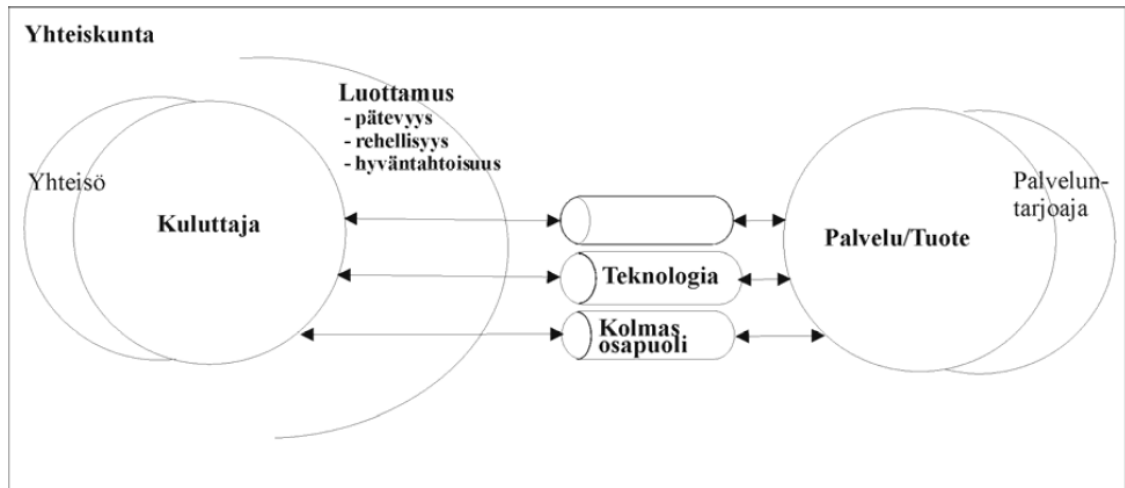
4.1 Määritelmä

Luottamusta on määritelty useammalla eri tavalla, ja riippuen tieteenalasta luottamus nähdään merkitykseltään erilaisena. Luottamusta on tutkittu ainakin sosiologisessa, psykologisessa ja taloustieteellisessä kontekstissa. (Blomqvist 1997) Vaikka näkemyksiä on monia, yhtäläisyyksiäkin on mahdollista havaita ja yhteinen perusta on löydettävissä. Luottamusta tutkineet henkilöt ovat määritelleet, että luottamuksessa on kyse kahdesta tai useammasta tahosta ja uskosta siihen, ettei luottamuksen kohde petä. (Tiainen, Luomala, Kurki ym. 2004) Vaikka luottamukseen ja luottamiseen liittyvää asiaa lähestyttäisiin kavennetusti fokuoituen yksilöön, ei liene epäilystä siitä, että luottamuksen merkitys korostuu interpersonallisessa tilanteessa, jossa osapuolia on enemmän

kuin yksi (Blomqvist 1997). Viimeaikaisten tutkimusten mukaan luottamusta kuvataan useimmiten kaksijakoisesti. Ensiksikin luottamusta pidetään uskomuksina tai käsityksinä toisesta osapuolesta ja toiseksi halukkuutena asettua haavoittuvaksi toiseen osapuoleen nähden. On huomattu, että positiiviset uskomukset ja käsitykset toisesta osapuolesta auttavat luottamuksen luomisessa nimenomaan vahvistaen halukkuutta yhteistyöhön. Ei tule kuitenkaan unohtaa, että tietyissä tilanteissa riskit, joita liittyy haavoittuvaksi asettumiseen, eivät ole kummankaan osapuolen hallittavissa, jolloin positiiviset mielikuvat ja uskomukset toista osapuolta kohtaan tulevat merkityksettömiksi luottamuksen luomisen ja yhteistyön kannalta. (McKnight & Choudhury 2006)

4.2 Luottamuksen luominen

Luottamuksen luominen on vuorovaikutteista toimintaa osapuolten välillä. Internetissä toimittaessa vuorovaikutus on digitaalista käyttäjän ja palveluntarjoajan välillä. Toki on myös mahdollista, että tahot tapaavat kasvokkain, esimerkiksi palveluntarjoajan tiloissa. Luottamusta on tutkittu paljon, ja yhteisinä tekijöinä luottamuksen rakentamisessa on voitu havaita käsitteet pätevyys, hyväntahtoisuus ja rehellisyys. Tampereen yliopiston eLaku-tutkimusprojektin viitekehys (kuva 2) kuluttajan luottamuksen muodostumisesta sähköisiin palveluihin on mielestäni oivallinen kuvaamaan asiaa kuvitetussa muodossa. (Tiainen, Luomala, Kurki ym. 2004)



Kuva 2 - eLaku tutkimusprojektin viitekehys (Tiainen, Luomala, Kurki ym. 2004)

Pätevyydellä voidaan ajatella kykyä pitää kiinni luvatussa (Tiainen, Luomala, Kurki ym. 2004). Käyttäjän sitoutuessa noudattamaan palveluntarjoajan sääntöjä tulisi palveluntarjoajan vastavuoroisesti pitää asettamansa lupaukset käyttäjälle. Ei-kaupallisissa palveluissa tilanne on jossain määrin vaikeampi, koska asiakas ei anna varsinaista rahallista vastiketta palvelun käytöstä. Kuitenkin palveluntarjoajan toimet, joista ei ole selkeästi ilmoitettu käyttäjälle, kuten tietojen jakaminen kolmansille osapuolille tai esimerkiksi sosiaalisissa verkostoissa toiminnan rajoittaminen, voivat aiheuttaa käyttäjälle kokemuksen luottamuksen rikkoontumisesta tai ainakin palveluntarjoajan huonosta pätevyydestä.

Rehellisyys palveluntarjoajan toiminnassa nivoutuu yhteen pätevyyden kanssa. Reilu toiminta asiakasta kohtaan korreloi selkeästi asiakastyytyväisyyden kanssa ja vaikuttaa palveluntarjoajan positiivisen maineen leviämiseen. Rehellisyyttä voidaan käyttää myös strategisena keinona asiakastyytyväisyyden ylläpitämiseksi. Rehellisistä menettelytavoista (procedural fairness) palveluiden tarjoamisessa on tutkimuksen kautta havaittu, että vaikka käyttäjän kannalta toivottu lopputulos olisi negatiivinen, on tyytymättömyys huomattavasti pienempi, jos käyttäjä kokee tulleen kohdelluksi rehellisellä tavalla. Kansainvälisesti rehdillä tietojen käsittelyllä korostetaan tietojen antajan

oikeutta tietää miten, mihin ja kuinka suojatusti tämän tietoja käsitellään. (Culnan & Armstrong 1999)

Hyväntahtoisuus käyttäjä - palveluntarjoaja -suhteessa on Garbarino & Leen (2003) mukaan molempien osapuolten halua toimia toista miellyttävällä tavalla, vaikka panoksena olisi tuoton menettäminen. Tämänkaltainen toimintamalli näkyy usein vain palvelujen taustalla olevien yritysten arvoluetteloissa, mutta on todellisuudessa merkittävämpänä tekijänä asiakastyytyvyyden jakautuessa eri suuntiin riippuen palveluntarjoajan todellisesta hyväntahtoisuudesta ja taidosta hallita suhteitaan asiakkaisiinsa - eli palvelun käyttäjiin.

4.3 Luotettavat tahot

Luotettavana tahona voidaan pitää ns. kolmatta osapuolta, joka toimii käyttäjän ja palveluntarjoajan välissä. Luotettavan tahon toimialueena voi olla esimerkiksi palvelun laadun sertifiointi, turvallisen tietoliikenteen takaaminen tai palvelun suositteleminen - esimerkiksi luotettavien yksityisyydensuojakäytäntöjen tähden. (Tiainen, Luomala, Kurki ym. 2004) Edelmanin (2006) mukaan yleisimmin luotettavana tahona internetissä pidetään luottamussertifikaatteja jakavaa organisaatiota. Tunnetuimpia maailmanlaajuisesti lienevät TrustE ja BBBonline. Vaikka edellisen kaltaiset organisaatiot myyvät palvelujaan luottamusta luovana yrityksenä, on viimeaikainen tutkimus osoittanut vakavia puutteita yksityisyyteen tai palvelun käyttäjän tietojen käsittelyyn liittyvässä käytäntöjen valvonnassa. Tästä huolimatta monet luottamussertifikaatein varustautuneet yritykset ovat kokeneet saavansa enemmän asiakkaita huolimatta luottamussertifikaatteja jakavien yritysten kyseenalaisesta toiminnasta. Hakukoneiden tuloksissa korkealle luokitetut yritykset saavat myös mielenkiintoisella tavalla ihmisten positiivisen huomion. SiteAdvisorin tietojen mukaan 94,6% TrustE-sertifikaatin

sivustoista on luotettavia, kun taas kaikista sivuista (ei luottamussertifikaattia) 97,5% on luotettavia. (Edelman 2006) Prosentuaalisesti kyse on pienistä määristä epäluotettavia sivustoja ja palvelujen tarjoajia, mutta luottamussertifikaatteja jakavien firmojen asiakkaiden huonompi luotettavuus suhteessa sivustoihin ilman luottamussertifikaattia on kaikin puolin erikoinen. Luottamusta pyritään siis ostamaan, vaikka sitä ei todellisuudessa ansaittaisi.

4.4 Mainejärjestelmät

Saarikko (2006) tutkii pro gradu -tutkielmassaan mainejärjestelmien merkitystä luottamuksen syntymisessä elektronisissa kauppapaikoissa. Mainejärjestelmien idea on luoda käyttäjän tai palveluntarjoajan aikaisemmasta käyttäytymisestä profiili, jonka perusteella syntyy maine muiden käyttäjien nähtäväksi. Tällä tavoin positiivista mainetta voidaan hyödyntää kilpailuetuna muihin käyttäjiin tai palveluntarjoajiin nähden. Jos palveluntarjoajan maine on positiivinen, luottamuksen luominen käyttäjän ja palveluntarjoajan välille helpottuu. Maineenhallintajärjestelmien ongelmallisuus on käyttäjien haluttomuus antaa palautetta. Tämän lisäksi on tulkinnanvaraista, kuinka rehellisesti palaute on annettu. Myös maineen liittäminen tiettyihin nimimerkkeihin luo tilanteesta ongelmallisen käyttäjien vaihtaessa nimimerkkejä. Digitaalisessa ympäristössä on aina tietty rajallisuus verrattuna reaali maailman kanssakäymiseen, jolloin negatiiviset kokemukset saattavat korostua epävarmuutena ja kyvyttömyytenä luottaa toiseen osapuoleen. Saarikko toteaa tutkimuksensa tuloksissaan, että luottamuksen luominen ei ole pelkästään riippuvainen palveluntarjoajan käyttämistä tekniikoista, vaan luottamuksen luominen on moniulotteinen prosessi, joka on myös olennaisesti riippuvainen käyttäjän aikaisemmista kokemuksista ja persoonasta.

5 YHTEENVETO JA PÄÄTELMIÄ

Yksityisyyteen ja sen suojaamiseen liittyy paljon tekijöitä, jotka ovat vahvasti yksilökeskeisiä. Tämä asettaa haasteita sille, kuinka internetpalveluja voidaan suunnitella ja kehittää niin, etteivät käyttäjät koe yksityisyytensä vaarantuvan ja näin menetä luottamusta internetpalvelujen tarjoajiin. Internet on kokonaisuudessaan melko kehittymätön yksityisyydensuojaan liittyvissä asioissa, joten oleellista on myös yhteisten standardien ja yhtenäisten protokollien hyväksyminen laajemmassa mittakaavassa - niin lokaalisti kuin globaalisti. Muutamia edistysaskelia asiassa on nähtävissä esimerkiksi Euroopan unionin kehitysprojektien kautta.

Yhtenä tutkimusongelmana oli ihmisten halukkuus jakaa tietojansa palveluntarjoajille. Tutkimusten avulla on havaittu, että ihmisten halukkuus jakaa tietoja palveluntarjoajan kanssa vaihtelee. On kuitenkin selkeästi huomattu, että käyttäjät antavat helpommin tietojansa yleisistä mielenkiinnon kohteista kuin esimerkiksi rahankäyttöön liittyen. Yksityisyyteen liittyy aina halu pitää omia tietoja ainakin osin muiden ulottumattomissa, ja internetpalvelujen käyttäjille tulisi luoda nykyistä paremmat mahdollisuudet päättää, mitä tietoja he itsestään antavat palveluntarjoajalle. Yksityisyys digitaalisessa maailmassa tulisi turvata lainsäädännöllisin keinoin perusoikeutena, vähintäänkin niin että olisi selkeämpää, kenellä on oikeus tarkastella kenenkin tietoja. Ajantasainen ja eksakti lainsäädäntö voisi jossain määrin tuoda myös lisää luottamusta internetpalvelujen tarjoajia kohtaan.

Negatiivinen kokemus palveluntarjoajasta voi vaikeuttaa luottamuksen luomista toisiin internetpalvelujen tarjoajiin. Jos internetin käyttäjille olisi selvää, kuka on milloinkin vastuussa yksityisyyden turvaamisesta, kenties internetpalvelujen käyttö kasvaisi vielä enemmän, ja saataisiin parempi hyöty verkon yli tarjottavista palveluista. Yksityisyydensuojaa on yritetty parantaa

erilaisin tavoin, esimerkiksi käyttäjän tietojen käsittelyä koskevilla kirjallisilla lausunnoilla ja erilaisilla internetsivustojen sisään ohjelmoituilla toiminnoilla, mutta keskeisenä ongelmana on luottamuspula ja standardien vakiintumattomuus.

Uskon, että yksityisyyden suojaaminen ja luottamuksen luominen ovat avainasemassa tulevana vuosina internetpalveluja kehitettäessä. Internetin kehittyessä ja tiedon pirstaloituessa ympäri verkkoa on tärkeää, että internetin käyttäjät ovat tietoisia henkilökohtaisten tietojensa kohtelusta. Hyvinkin arkaluontoisten tietojen, kuten esimerkiksi potilastietojen ja luottamuksellisen viestinnän, siirtyessä yhä enenevässä määrin verkkoon, on yksityisyydensuojan oltava erityisen tarkasti mietitty ja tietokantojen tietojen yhdistely mahdollista vain äärimmäisissä tilanteissa.

Voi olla, että internetin kehityksessä ollaan muutoksen edessä erityisesti tunnistautumispalvelujen ja mahdollisten kolmansien, aidosti luotettavien osapuolien käytön yleistyessä. Tulevaisuudessa käy ilmi, kuinka merkittävä kilpailuetu luotettavuus tulee olemaan niin kaupallisten, kuin ei-kaupallisten palvelujen tarjoamisessa. Tämän tutkielman lähteiden kautta on havaittavissa, että käyttäjät suhtautuvat tällä hetkellä epäluuloisesti tietojen antamiseen internetissä. Yleisluontoista tietoa jaettaessa huoli yksityisyydestä ei ole yhtä oleellinen. Luottamuksen luominen on merkittävässä roolissa käyttäjän ja palveluntarjoajan välillä, mutta ei missään nimessä yksinkertaista ja helposti hallittavissa olevaa. Jokaisen käyttäjän henkilökohtainen menneisyys vaikuttaa luottamuksen rakentumiseen ja palvelun maineella on merkittävä rooli asiassa. Reilulla tavalla meneteltäessä positiivinen maine rakentuu vähitellen ja asiakastyytyväisyys kasvaa, jolloin myös luottamus palveluntarjoajaa kohtaan vahvistuu. Näin ollen yksityisyyteen liittyvillä käytännöillä on merkittävä rooli luottamuksen luomisessa palvelun menestymisen kannalta.

LÄHDELUETTELO

- Berman J. & Mulligan D. 1999. Privacy in the Digital Age: Work in Progress. *Nova Law Review* 23(2). 551-582.
- Berthold O. & Köhntopp M. 2001. Identity management based on P3P. In international Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability Berkeley, California, United States. New York: Springer-Verlag New York, 141-160
- Blomqvist K. 1997. The many faces of trust. *Scandinavian Journal of Management* 13(3), 271-286.
- Brown M. & Muchira R. 2004. Investigating the relationship between internet privacy concerns and online purchase behavior. *Journal of Electronic Commerce Research* 5(1), 62-70.
- Camenisch J., Shelat a., Sommer D., Fischer-Hübner S., Hansen M., Krasemann H., Lacoste G., Leenes R. & Tseng J. 2005. Privacy and identity management for everyone. In Proceedings of the 2005 Workshop on Digital Identity Management Fairfax, USA, November 11 - 11. New York: ACM, 20-27.
- Clauß S., Kesdogan D. & Kölsch, T. 2005. Privacy enhancing identity management: protection against re-identification and profiling. In Proceedings of the 2005 Workshop on Digital Identity Management Fairfax, USA, November 11 - 11. New York: ACM, 84-93.
- Culnan M. J. and Armstrong P. K. 1999. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science* 10(1),104-115.

- Edelman B. 2006. Adverse Selection in Online "Trust" Certifications [online]. Harvard University. Working Draft. [viitattu 22.2.2009]. Saatavilla [www-osoitteessa < http://www.benedelman.org/publications/advsel-trust-draft.pdf>](http://www.benedelman.org/publications/advsel-trust-draft.pdf).
- Future of Identity in the Information Society 2005. Structured Overview on Prototypes and Concepts of Identity Management Systems [online]. European Union. [viitattu 15.1.2009]. Saatavilla [www-osoitteessa < http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf>](http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.1.overview_on_IMS.final.pdf).
- Garbarino E. & Lee O.F. 2003. Dynamic pricing in internet retail: Effects on consumer trust. *Psychology and Marketing* 20(6), 495-513.
- Heinonen R. 2001. *Digitaalinen minä*. Helsinki: Edita.
- Hoffman D.L., Novak T.P. & Peralta M. 1999. Building consumer trust online. *Communications of the ACM* 42(4), 80-85.
- Johnson D.G. 2001. *Computer ethics*. Upper Saddle River (NJ): Prentice Hall.
- Kelly E.P. & Rowland H.C. 2000. Ethical and Online Privacy Issues in Electronic Commerce. *Business Horizons* 43(3), 3-12.
- Kobsa A. 2007. Privacy-enhanced personalization. *Communications of the ACM* 50(8), 24-33.
- Mahkonen S. 1997. *Oikeus yksityisyyteen*. Porvoo : WSOY.
- McKnight D. H. & Choudhury V. 2006. Distrust and trust in B2C e-commerce: do they differ?. In *Proceedings of the 8th international Conference on Electronic Commerce: the New E-Commerce: innovations For Conquering Current Barriers, Obstacles and Limitations To Conducting Successful*

Business on the internet Fredericton, New Brunswick, Canada, August 13 - 16. New York: ACM, 482-491.

Murray J.A.H., Burchfield R.W., Simpson J.A. & Weiner E.S.C. 1989. The Oxford English dictionary. Oxford: Clarendon.

Paine C., Joinson A.N., Buchanan T. & Reips U. 2006. Privacy and Self-Disclosure Online. CHI '06 extended abstracts on Human factors in computing systems, Montréal, Québec, Canada, April 22 - 27. New York: ACM, 1187 - 1192.

Platform for Privacy Preferences (P3P) Project 2007 [online]. World Wide Web Consortium. [viitattu 22.2.2009]. Saatavilla [www-osoitteessa <http://www.w3.org/P3P/>](http://www.w3.org/P3P/).

Pollach I. 2007. What's wrong with online privacy policies?. Communications of the ACM 50(9), 103-108.

Privacy and Identity Management for Europe 2008. PRIME white paper [online]. European Union. [viitattu 15.1.2009]. Saatavilla [www-osoitteessa <https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf>](https://www.prime-project.eu/prime_products/whitepaper/PRIME-Whitepaper-V3.pdf).

Saarenpää A. 2002. Näkökohtia yksilön suojusta: 55 teesiä tietosuojasta [online]. Lapin yliopiston oikeusinformatiikan instituutti. [viitattu 16.12.2008] Saatavilla [www-muodossa <http://www.ulapland.fi/home/oiffi/julkaisut/teesit.htm>](http://www.muodossa).

Saarikko S. 2006. Mainejärjestelmät elektronisten kauppapaikkojen toiminnassa. Jyväskylän yliopisto, tietojenkäsittelytieteen pro gradu -tutkielma.

Suomen perustuslaki 731/1999. 2000. [viitattu 16.12.2008] Saatavilla [www-muodossa <http://www.finlex.fi/fi/laki/ajantasa/1999/19990731>](http://www.finlex.fi/fi/laki/ajantasa/1999/19990731).

- Syrjänen P. 2006. Yksityisyyden suoja ja henkilöarviointi. Tampereen yliopisto. Acta Universitatis Tamperensis 1155. Väitöskirja. [viitattu 16.12.2008]
Saataavilla www-muodossa < <http://acta.uta.fi/pdf/951-44-6646-2.pdf>>.
- Tavani H.T. 1999. Privacy online. ACM SIGCAS Computers and Society 29(4), 11-19.
- Tavani H.T. 2007. Philosophical theories of privacy: implications for an adequate online privacy policy. Metaphilosophy 38(1), 1-22.
- Thibadeau R. 2000. A Critique of P3P : Privacy on the Web [online]. Carnegie Mellon University [viitattu 22.2.2009]. Saataavilla www-osoitteessa < <http://dollar.ecom.cmu.edu/p3pcritique/>>.
- Tiainen T., Luomala H., Kurki S. & Mäkelä Kari (Toim.) 2004. Luottamus sähköisissä palveluissa: kuluttajan ja palvelun tarjoajan vuorovaikutus. Tampereen yliopisto, Tietojenkäsittelytieteiden laitos. Raportti B-2004-11. Saataavilla myös www-muodossa:
<<http://www.cs.uta.fi/reports/bsarja/B-2004-11.pdf>>.