



LAUREA
AMMATTIKORKEAKOULU

Uuden edellä

Facebook - keskeisimmät uhat yksityisyydelle

Ranta, Mika

2012 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Facebook - keskeisimmät uhat yksityisyydelle

Mika Ranta
Turvallisuusala
Opinnäytetyö
Elokuu, 2012

Mika Ranta

Facebook - keskeisimmät uhat yksityisyydelle

Vuosi 2012 Sivumäärä 57

Tämän opinnäytetyön tarkoituksena on tutkia sosiaalisen median palveluiden, erityisesti Facebookin, keskeisiä uhkia palveluiden käyttäjien yksityisyydelle. Opinnäytetyön tavoitteena on ollut tutkia sosiaalisen median palveluiden käyttöympäristöä ja johtaa tästä ympäristöstä keskeisimmät uhat yksityisyydelle. Esiin tulleita uhkia on tarkasteltu Facebook -ympäristössä ja työssä kuvattu kyseisen palvelun käytön aiheuttamia uhkia käyttäjän yksityisyydelle.

Valtaosa suomalaisista käyttää sosiaalista mediaa sekä erilaisia verkkoyhteisöpalveluita päivittäin. Tiettyihin internetin sosiaalisiin palveluihin, kuten Facebook, oli keväällä 2010 rekisteröitynyt 42 prosenttia 16-17 -vuotiaista suomaista. Verkkoyhteisöihin osallistuvat ovat toistaiseksi pääasiassa nuorempia internetin käyttäjiä. Verkon sosiaalisen median palvelut, erityisesti Facebook, kasvattavat jatkuvasti suosiotaan kaikissa ikäryhmissä.

Sosiaalisen median käytön lisääntyessä on muodostunut tarve lisätä tietoisuutta käyttäjien yksityisyyden uhista näissä palvelussa. Facebook on tämän hetken suosituin sosiaalisen median palvelu, jossa on yli miljoona suomalaista käyttäjää. Opinnäytetyön rajauksissa tarkastelevaksi on otettu vain sellaisia keskeisiä uhkia, jotka koskettavat kaikkia käyttäjiä. Aihealueessa ei ole tarkasteltu laitteistojen tietoturvallisuutta, syrjäytymistä eikä sopimusjuridiikkaa.

Opinnäytetyön tutkimusteoriaa on kuvattu lähdekirjallisuuden sekä Internet -lähteiden kautta. Lähdekirjallisuutena on käytetty pääosin suomaista tutkimuskirjallisuutta sekä internet-lähteitä. Lähdekirjallisuuden lisäksi, tutkimusmateriaalina on käytetty asiantuntija- sekä käyttäjähaastatteluja.

Tutkielman tietoja voi käyttää kaikki sosiaalisen median käyttäjät, niin yksityishenkilöt kuin yhteisöt, arvioimaan miten esitetyt uhat koskevat heitä.

Asiasanat: Sosiaalinen media, Facebook, uhka, yksityisyys

Mika Ranta

Facebook - the main threats to privacy

Year	2012	Pages	57
------	------	-------	----

The purpose of this thesis is to study the main threats of social media services, especially Facebook, to users' privacy. The objective is to examine the environment of the social media and from this environment draw the main threats for privacy. The emerging threats have been analysed in the environment of Facebook, followed by a description of how users' privacy is threatened when they are using Facebook services.

The majority of Finns use social media and different network services daily. 42 per cent of 16 to 17 years old Finns were registered in some specific services such as Facebook in the spring 2010. The majority of the participants of network services are young internet users. The Internet's social media services, especially Facebook, are gaining more and more popularity in all age groups.

The increased use of social media services has led to an increased need for awareness of various threats to users' privacy in these services. Facebook is the most popular social media service at the moment and has over one million Finnish users. The scope of the study was limited to the main threats that involve all users' privacy. Hardware data security, alienation or laws of contract have not been included in this study.

The theory of the thesis is described through different written sources, mainly Finnish science literacy and writings from the internet. In addition to written science literacy sources, research material was received from interviews of experts and basic users of the social media scene.

The findings of this study can be used by all social media users, both private persons and organizations, to assess threats to their privacy when using social media services.

Keywords: Social media, Facebook, Threat, Privacy

Sisällys

1	Johdanto	7
2	Tavoitteet	7
3	Opinnäytetyön rakenne	8
3.1	Opinnäytetyön rajausta ja riskit	8
3.2	Tutkimusmenetelmät	8
3.2.1	Haastattelut	9
3.2.2	Kirjallisuuslähteet ja lähdekritiikki	10
4	Yksityisyys	10
5	Sosiaalinen media	12
5.1	Sosiaalisen median käyttö	13
5.2	Yhteisöllisyys ja tiedon tuottaminen	14
5.3	Sisällön tuottamisen ongelmat	15
6	Käyttäjän identiteetti	18
6.1	Yksityinen vai julkinen	19
6.2	Valokuvat	21
6.3	Tietojen pysyvyys ja leviäminen	22
7	Yksityisyystiedon vuotaminen	23
7.1	Käyttäjän oman toiminnan aiheuttamat uhat	23
7.2	Viestin kirjoittamisen helppous ja välittömyys	25
8	Facebook	26
8.1	Käyttäjät ja käyttö	27
8.2	Yksityisyystiedot Facebookissa	28
8.3	Profiili, identiteetti ja sovellukset	29
8.3.1	Kuvat	30
8.4	Ystävät	31
8.4.1	Kaverihaku	32
8.5	Rekisteröinti, käyttöehdot ja tietojen luovuttaminen	32
8.6	Tietojen julkisuus	33
8.7	Kehitys	35
9	Järjestelmällinen ja suunniteltu yksityisyystietojen kerääminen	37
9.1	Tietojen louhinta ja yhdistäminen	38
9.2	Tiedustelupalvelut	39
9.3	Yritykset	40
9.4	Muut tahot	40
10	Rikollinen tai vihamielinen toiminta	41
10.1	Rikos yksityiselämää loukkaavan tiedon levittäminen	41
10.2	Henkilöllisyysvarkaudet	41

10.3	Teollisuusvakoilu	43
10.4	Social engineering.....	44
10.5	Viattomien tietojen hakkerointi.....	45
11	Haastattelut	45
11.1	Asiantuntijahaastattelut	46
11.2	Käyttäjät.....	48
12	Tulokset	50
13	Johtopäätökset.....	52
14	Työn arviointi.....	53
	Lähteet	54
	Kuvat	55
	Liitteet.....	56

1 Johdanto

Yli miljoona suomalaista on Facebookin käyttäjiä. Internetin sosiaaliset mediat ovat monille ihmisille kiinteä osa heidän arkielämää. Käyttäjien joukko kasvaa jatkuvasti, ja samalla myös kasvaa näiden palvelujen kirjo. Läntisen maailman suurimman palvelun Facebookin käyttö yleistyy eniten niin yksityisten kuin eri yhteisöjen joukossa. Ihmiskunta on yhden suurimman sosiologisen ilmiön edessä, jossa yksityisyyden sijaan pyritään yhteisöllisyyteen ja mahdollisimman laajaan tiedon jakamiseen.

Lähtökohtana tutkimukselle on ollut tarkastella yksilöön kohdistuvia uhkia, joita voidaan juontaa Facebookin käytöstä. Tavoitteena on ollut saada mahdollisimman kattava näkemys niistä yksityisyyteen liittyvistä keskeisistä uhista, jotka saattavat aiheutua sosiaalisen median, erityisesti Facebookin käytöstä.

Toimin virkatehtävissä suojelupoliisissa. Valtion turvallisuudesta vastaavalla toimijalla on selkeät intressit selvittää yhteisölliseen palveluun liittyviä uhkia, koska iso osa suomalaisista on käyttää Facebook -palvelua. Myös organisaatioiden turvallisuudesta vastaavat tahot ovat kiinnostuneita Facebookin käyttöön liittyvistä uhista, koska työntekijät ovat yhä kasvavassa määrin kyseisen palvelun käyttäjiä, osin myös työaikana. Olen itse kyseisen palvelun käyttäjä ja siten kiinnostunut tarkastelemaan mahdollisia uhkia omassa arjessani.

Sosiaalinen media sekä erilaiset verkkoyhteisöt ovat valtaosalla kansalaisista päivittäisessä käytössä. Tiettyihin Internetin sosiaalisiin palveluihin, kuten Facebook, oli keväällä 2010 rekisteröitynyt 42 prosenttia 16-74-vuotiaista suomalaisista. Verkkoyhteisöihin osallistujat ovat toistaiseksi pääasiassa nuorempia netin käyttäjiä. Kaksi kolmesta nuoresta ja nuoresta aikuisesta seuraa jotain yhteisöpalvelua päivittäin. (Tilastokeskus 2010.)

2 Tavoitteet

Opinnäytetyön tavoitteena on tuoda esiin ne keskeiset uhat, jotka ovat olennaisia Facebook -palvelun käyttäjille yksityishenkilönä. Lähtökohtana tutkimukselle on tarkastella yksilön yksityisyyteen kohdistuvia uhkia, joita voidaan juontaa Facebookin käytöstä; miten uhat muodostuvat, kenen toimesta ja mitä ne ovat.

Tutkielman tietoja voivat käyttää kaikki sosiaalisen median käyttäjät, niin yksityishenkilöt kuin yhteisöt, arvioimaan miten esitetyt uhat koskevat heitä. Tätä tietoa tulen jakamaan virkatyöni kautta edustamani organisaation käyttöön osaksi tietoturvallisuuskoulutusta sekä turvallisuusluentojen taustamateriaaliksi eri yhteisöille.

3 Opinnäytetyön rakenne

Opinnäytetyön alussa kuvataan tutkimusteoriaa lähdekirjallisuuden kautta, kuten aiheeseen liittyvä kirjallisuus, media-artikkelit sekä tutkimukset. Tavoitteena on selvittää, millaisia uhkia on jo muiden toimesta havaittu. Lähdekirjallisuutena tulen käyttämään pääosin suomasta tutkimuskirjallisuutta.

Tutkimuksessa suoritetaan haastatteluja, joiden tarkoituksena on selvittää asiantuntijoiden näkemys sosiaalisen median, erityisesti Facebookin uhista. Asiantuntijahaastatteluja tehdään kaksi. Asiantuntijoiden näkemysten kautta kuvataan keskeisimmät uhkateemat ja asioiden vaikutus käyttäjän yksityisyydelle.

Asiantuntijahaastattelujen lisäksi tehdään kaksi käyttäjähaastattua, joiden tavoitteena on saada käyttäjien kokemukset ja havainnot sosiaalisen median keskeisistä uhista. Käyttäjähaastatteluissa selvitetään lisäksi käyttäjien toimintaa Facebookissa ja miten he ovat mieltäneet yksityisyyteensä liittyviä mahdollisia uhkia.

3.1 Opinnäytetyön rajaus ja riskit

Tutkimuksessa tutkitaan yksilön toimintaa sosiaalisessa mediassa ja erityisesti Facebookissa ja siellä toimimisesta aiheutuvia uhkia käyttäjän yksityisyyteen. Tutkimuksessa rajataan pois IT-laitteistojen tekninen turvallisuus. Tutkimuksessa ei myöskään tarkastella syrjäytymistä, eikä sopimusjuridiikkaa.

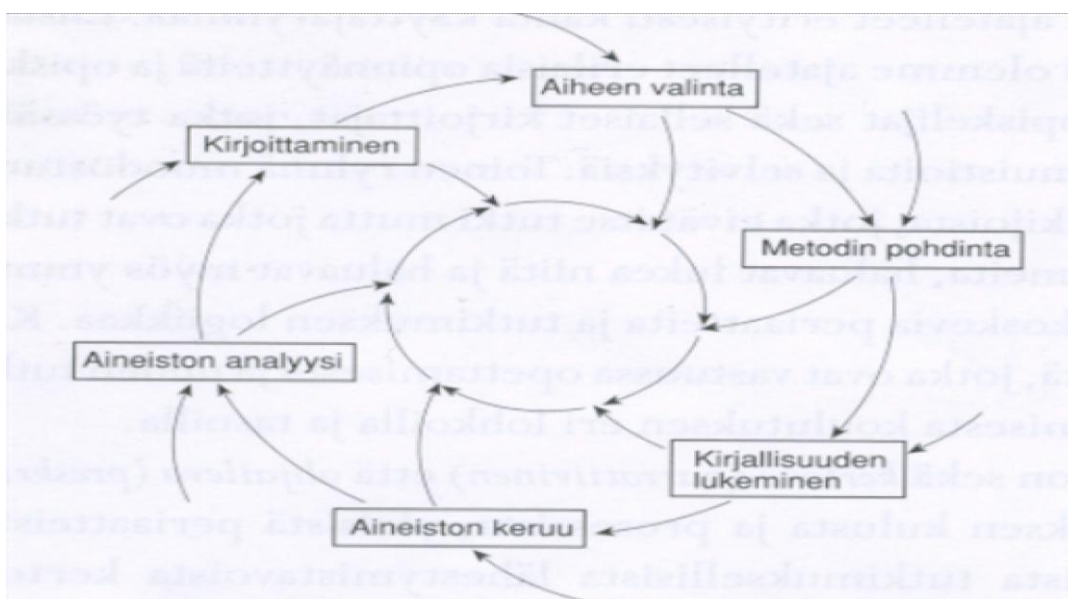
Riskinä on, että tutkimuksesta tulee sisällöltään liian laaja, koska toiminta Facebookissa on hyvin laajaa ja moninaista. Myös käyttäjät eroavat niin taustoiltaan kuin toimintatavoiltaan. Tätä riskiä pyrin välttämään sillä, että tutkimuksessa käsitellään vain niitä keskeisiä uhkia, jotka selviävät kirjallisuuskatsauksen lähdemateriaalin sekä asiantuntijoiden teemahaastattelujen pohjalta.

3.2 Tutkimusmenetelmät

Työn alkuvaiheessa tutustun yksityisyyden suojaan liittyvään suomalaiseen lainsäädäntöön sekä lähdekirjallisuuden määritelmiin yksityisyydestä. Yksityisyyden määrittelyn kautta on tarkoitus tuoda esiin keskeisimmät yksityisyyden suojan osa-alueet. Seuraava vaihe on tarkastella aihetta eri lähdekirjallisuuden kautta. Tutkimuksessa käsitellään myös Facebookin käyttöä itse palvelussa sekä erilaisten aiheeseen liittyvän lähdekirjallisuuden kautta.

Käytännössä työn eteneminen ei ole suoraviivainen prosessi, joka pohjautuu etukäteen suunniteltuun tutkimusvaiheiden järjestelmälliseen käsittelyyn. Työ on laadullinen tutkimus, jolle on tyypillistä tutkimuksen eteneminen vaiheittain ajallisesti ja joustavasti. (Hirsjärvi, Remes & Sajavaara 2007, 14.) Tämä tutkimus noudattaa tutkimusspiraalin prosessia, jossa tutkimus on vaiheittainen päättymätön prosessi, se voidaan aloittaa halutusta kohdasta ja prosessi ohjaa harkitsemaan tehtyjä valintoja sekä siirtymään vaiheiden välillä. (Hirsjärvi ym. 2007, 14).

Hirsjärvi ym. 2007 esittävät tutkimusspiraalin kuvaaman joustavan prosessin tutkimuksen luonnetta.



Kuva 1. Tutkimusspiraali Blaxterin, Hughesin ja Tightin (1996, lainattu Hirsjärvi ym 2007, 14) mukaan

3.2.1 Haastattelut

Haastattelu on yksi käytetyimpiä tiedonkeruutapoja. Haastattelussa tutkija ja haastateltava keskustelevat haastattelutyypistä riippuen enemmän tai vähemmän strukturoidusti (järjestelmällisesti) tai laveasti asioista, jotka kuuluvat tutkimusaiheeseen. Tutkimushaastattelulla on selkeä päämäärä: tutkimustehtävän suorittaminen. Haastattelua siis käytetään tutkimusaineiston saamiseksi, ja aineistoa puolestaan on tarkoitus analysoida ja tutkia tutkimustehtävän selvittämiseksi. (Hirsjärvi & Hurme 2001, 34, 42.)

Teemahaastattelu on keskustelunomainen tilanne, jossa käydään läpi ennalta suunniteltuja teemoja. Tyypillistä on, että haastattelun aihepiirit eli teema-alueet ovat tiedossa, mutta kysymysten tarkka muoto ja järjestys puuttuvat. (Hirsjärvi ym. 2001, 185).

Teemahaastattelun runko tehdään varsinaisen tutkimusongelman sekä alaongelmien pohjalta. Teemahaastattelujen tekeminen edellyttää huolellista suunnittelua. Tutkijalla pitää olla selkeä käsitys siitä, mikä on hänen tutkimuskysymyksensä.

Haastattelu tutkimuksen osana on vuorovaikutteinen tilanne ja teemahaastattelulle on tyypillistä seuraavat asiat:

- Tilanne on ennalta suunniteltu
- Haastattelijan alulle panema ja ohjaama
- Haastattelija joutuu tavallisesti motivoimaan haastateltavaa sekä ylläpitämään hänen motivaatiotaan
- haastattelija tuntee roolinsa, mutta haastateltava oppii sen haastattelun kuluessa.

3.2.2 Kirjallisuuslähteet ja lähdekritiikki

Tutkimuskirjallisuuden alustava perehtyminen suuntaa ja ohjaa tutkimusta sekä auttaa kysymyksenasetteluja. Osana tutkimusprosessia lähdekirjallisuuteen perehtyminen jatkuu tutkimuksen kaikissa vaiheissa täydentäen sekä terävöittäen tutkimusta. (Hirsjärvi ym. 2007, 105.) Tässä tutkimuksessa ensisijaisina kirjallisuuslähteitä ovat verkkoturvallisuutta sekä yksityisyyden suojaa käsittelevät teokset. Näiden teosten lisäksi tutkimuksen suunnittelussa sekä tutkimusongelman kohdentamisessa on lähteinä käytetty ongelmaa käsitteleviä julkaisuja.

4 Yksityisyys

Yksityisyyden määrittämisen ongelma on siinä, että yksityisyys koetaan subjektiivisena asiana. Jokainen yksityinen henkilö kokee omiksi yksityisyyteen liittyviksi asioikseen juuri itselleen tärkeät salassa pidettävät asiat. Yksityistä on se, mitä kukin ihminen itse määrittelee sen olevan. Yksityisyydelle ei olemassa mitään selkeää mittaria, jokainen kokee yksityisyyden henkilökohtaisesti.

Tutkimuksen kannalta merkityksellisempää on tarkastella yksityisyyttä asian ulkopuolelta, objektiivisen tarkastelun kautta. Tämän tarkastelun kautta voidaan määritellä joitain selkeitä yksityisyyteen liittyviä keskeisiä teemoja. Objektiivisimman kuvan antaa lainsäädäntö, joka määrittelee yksityisyyteen liittyviä asioita. Yksityisyydelle ei lainsäädännössä ole yhtä yksiselitteistä määritelmää. Henkilön yksityisyyden määrittämiseen voidaan katsoa kuuluvan useita eri lainkohtia. Näistä vahvimmat ovat perustuslain pykälät 6 ja 10. Perustuslain lisäksi myös muissa laeissa on määritelty yksityisyyteen liittyviä asioita; henkilötietolaki, laki yksityisyyden suojasta työelämässä sekä sähköisen viestinnän tietosuojalaki.

Perustuslain 6§ koskee ihmisten yhdenvertaisuutta. Lainkohdan mukaan ketään ei saa asettaa ilman hyväksyttävää perustetta eri asemaan sukupuolen, iän, alkuperän, kielen, uskonnon, vakaumuksen, mielipiteen, terveydentilan, vammaisuuden tai muun henkilöön liittyvän syyn perusteella. (Suomen perustuslaki 2011, 6§.). Perustuslain 10§ koskee yksityiselämän suojaa. Lainkohdan mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Lainkohdan mukaan myös kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. (Suomen perustuslaki 2011, 6§.)

Tietokirjailija Petteri Järvinen (2010) määrittelee yksityisyyden englanninkielisen termin privacy kautta. Järvisen näkemyksen mukaan yksityisyys on henkilöön tai hänen toimintaansa liittyviä tietoja. Tietosuojalla (engl.privacy) tarkoitetaan tällaisten tietojen suojaamista luvattomalta keräämiseltä tai käytöltä. Yksityisyyden kohteena on ihminen. (Järvinen 2010, 15.)

Yksityisyys on kaikille kuuluva perusoikeus. Jokaisen on kyettävä varmistautumaan siitä, että itselleen tärkeät yksityisyyteen kuuluvat asiat pysyvät muilta salassa. Salassa pidettäviä asioita ovat pääsääntöisesti perheen sisäiset tapahtumat, terveys, talous, seksuaalisuus, ihmissuhteet, tulevaisuuden suunnitelmat ym. sellaiset omaan yksityiseen elämään kuuluvat asiat, joita emme halua ulkopuolisten tietävän tai niin levittäminen olisi itselleen vahingollista. (Järvinen 2010, 15.)

Henkilötietojen koneellisesta käsittelystä säädetään 1.6.1999 voimaan tulleella henkilötietolailla. Lain tarkoituksena on suojata yksityiselämää ja muita siihen liittyviä perusoikeuksia silloin kun henkilötietoja käsitellään, sekä edistää hyvän tietojenkäsittelyntavan kehittämistä ja noudattamista. Laki ei koske luonnollisen henkilön yksityiseen käyttöön keräämien tietojen käsittelyyn. Laki ei koske yksityishenkilön omaan käyttöön keräämää tietoa ja sen käsittelyä. Laissa ei ole rajoituksia sille, millaista tietoa ja kuinka järjestelmällisesti yksityishenkilö saa itselleen luvallista hankkimaansa tietoa kerätä ja rekisteröidä. Esimerkiksi omista kavereistaan, tuttavistaan tai muista henkilöistä saa kerätä ja rekisteröidä tietoa omaan käyttöönsä. (Järvinen 2002, 411.)

Perustuslain mukaan viestintäsalaisuuden piiriin kuuluvat kaikki henkilökohtaisen viestinnän muodot, huolimatta siitä, millä tavoin viesti on toteutettu; sähköposti, pikaviesti, tekstiviesti tai kirje. Viestintäsalaisuuden murtaminen vaatii erittäin vahvat ja lakiin pohjautuvat perusteet. (Järvinen 2002, 230.)

Pohjoismainen lakiin perustuva tietosuojaja on yksi maailman kehittyneimmistä ja yksilön suojan kannalta vahvimpia. Erityisiä rajoituksia on annettu tietojen keräämiseen, rekisteröintiin sekä tietojen käyttöön. Yksityisen henkilön tietosuojan lisäksi pohjoismaisessa lainsäädännös-

sä on säännelty työntekijöiden asemasta sekä rajoituksia erilaisille salaustekniikoille. Euroopan Unioni pyrkii ajamaan tiukkaa yksityisyyden tietosuojaa unionin sisällä. EU:n tavoitteista huolimatta unionin eri valtioiden omat säädökset vaihtelevat suuresti; Pohjoismaiden tiukasta linjasta, Iso-Britannian liberaaliin linjaan. (Järvinen 2002, 414.)

5 Sosiaalinen media

Opinnäytetyön ensisijaisena tutkimuskohteena on sosiaalisen median palvelu Facebook. Kyseisessä palvelussa yhdistyy laajalti sellaisia ilmiöitä, jotka ovat osa koko sosiaalisen median ympäristöä. Facebookin yksittäinen tarkastelu on johdettavissa ilmiön isommasta kokonaisuudesta. Tutkimuksen kannalta on tarpeellista tarkastella aluksi koko sosiaalista mediaa sellaiseen sekä niitä tekijöitä, jotka ovat johtaneet nykyiseen tilanteeseen käytön ja käyttäjien osalta.

Tietoverkot ovat nykyisin kiinteä osa jokaisen suomalaisen arkipäiväistä elämää. Internetiä käytetään niin työtehtävien hoitamiseen kuin vapaa-ajan viettoon. Internetin eri palveluiden käyttäminen on välttämätön osa arkielämää; pankkiasiat, elämykset, tiedon hakeminen tai sosiaalisten suhteiden ylläpito. Internetin kautta saatavista palveluista ei käytännössä voi olla poissa; sivustakatsojat ovat tiettyssä mielessä uloslyötyjä eli he jäävät asioiden, sosiaalisen verkostoitumisen ja tiedon ulkopuolelle.

Suomalainen tietoverkkohistoria, sen rakentuminen ja käytön omaksuminen, on suhteellisen lyhyt ajanjakso 1970 -luvulta nykypäivään. Tietoverkkoyhteiskunnan muodostumisen aikana on suomalainen elämäntapa kokenut rajuja yhteiskunnallisia ja kulttuurillisia muutoksia. Maa- ja metsätalousvaltaisesta yhteiskunnasta rakentui moderni kaupungistunut tietoyhteiskunta. Tässä muutoksessa vielä lyhyempi historia on internetillä sekä sen käytön arkipäiväistymisellä. (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

Suomalaisista valtaosa, noin 72 prosenttia, käyttää Internetiä lähes päivittäin. Internetin jatkuvainen käytön kasvu on nopeinta vanhemmissa ikäryhmissä, mutta on yleistä kaikissa ikäryhmissä. Tutkimustilastojen tietojen perusteella voidaan todeta, että tietokoneen käyttöä valtaosa on Internetin käyttöä. (Tilastokeskus 2010.)

Tutkimuksen (Tilastokeskus 2010) mukaan yleisimmät Internetissä tehtävät asiat liittyvät omaan henkilökohtaiseen talouteen, joukkoviestimien seuraamiseen, verkko-ostoksiin tai sosiaalisiin suhteisiin. Sähköposti oli yleisin tutkimuksessa esiin tulleista käyttötavoista. Vastajista 77 prosenttia oli käyttänyt sähköpostia kolmen kuukauden aikana. Tutkimuksen vastajista 76 prosenttia oli käyttänyt Internetiä pankkiasioden hoitamiseen ja 74 prosenttia oli etsinyt tietoa tavaroista tai palveluista.

Internetin palvelujen käyttäjät ovat omilla valinnoillaan tulleet jossakin määrin riippuvaisiksi verkon eri palveluista ja näiden käytöstä on monelle tullut tiedostamaton rutiini. Suominen (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.) kuvaa tätä verkonkäytön rutiininaomaista omaksumista kulttuurilliseksi omaksumiseksi. Kulttuurillinen omaksumien koskee verkon palvelujen käytön lisäksi käyttäjien omien vaatimusten kasvamista, jossa halutaan palveluiden sekä teknisten toteutusten jatkuvaa kehittymistä ja jatkuvaa käytettävyyttä. (Suominen, J. 8-10.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

Internetin käytön kulttuurillinen omaksuminen on vaiheittain etenevä prosessi. Internet oli alkujaan hyvin pienen käyttäjäryhmän käytössä. Prosessin edetessä, Internetistä tuli vaiheittain osa kaikkien yksilöiden ja yhteisöjen arkipäivää. Omaksumisprosessissa käyttäjät ovat hyväksyneet sen, että Internet ja sen eri palvelut ovat kiinteä osa heidän elämää. Tämä todellisuus muokkaantuu ja muuttuu jatkuvasti. Tekniset ja toiminnalliset muutokset Internetin käytössä ja sen palvelussa on jatkuvaa. Käyttäjät ovat hyväksyneet sen, että heidän tekninen ja sosiaalinen infrastruktuuri on jatkuvan muutoksen alla ja osa nykypäivän arkielämää. Prosessista on tullut kiinteä osa meidän kaikkien arkielämää; kun Internet muuttuu, samalla muutamme mekin. (Suominen, J. 8-10.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.) Internetistä on tullut keino ja mahdollisuus muuttaa käyttäjien arkielämän uskomuksia sekä tapoja. Aiemmin opitut tavat toimia ja viestiä ovat jatkuvan muutoksen alla mukautuneet Internetin asettamiin tapoihin. Muutos on ollut hyvin nopea ja monella tapaa kontrolloimaton. Käyttäjät on pakotettuja toimimaan verkon palvelujen määräämällä tavalla. Yhtäläillä luodaan uskomus, että käyttäjät muokkaavat ympäristönsä haluamaansa suuntaan, toisaalta palvelujen tarjoajat pakottavat toimimaan tietyllä tavalla. Vapaus toimia omalla tavalla on illuusio, käyttäjän on toimittava ennakkoon määrättyllä tavalla, jotta toiminta palvelussa olisi mahdollinen.

5.1 Sosiaalisen median käyttö

Sosiaalinen media on eräänlainen kattokäsite, jonka alle muodostuu laadullisesti ja määrällisesti epämääräinen joukko Internet-palveluita. (Turtiainen, R. 222-224.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

Tirronen (2009) näkee sosiaalisen median olevan yksilöllisesti tai yhteisöllisesti tuotettua mediasisältöä, joka toimii tietoverkoissa ja on jaettua. Sisällön jakaminen tietoverkkoon tapahtuu nopeasti, ilman ulkopuolista valvontaa. Jaettu sisältö koostuu kaikesta mahdollisesta, kuten kokemuksista, mielipiteistä ja näkemyksistä tai ajatuksista. (Tirronen, M. 2008. 9.)

Verkon sosiaalisesta mediasta tai web 2.0 -käsitteen alla oleva ilmiö koostuu monenlaisista yhteisöllisesti toimivista internetsisällöistä ja -palveluista. Tällaisia ovat esimerkiksi wikit (kollektiiviseen sisällöntuotantoon suunnitellut julkaisualustat), podcastit (äänilähetykset) ja keskustelufoorumit. Sosiaalisen yhteisöllisen median tuottamista ovat myös verkon kuvagalleriapalvelujen toiminta, jonka perusta on käyttäjien välinen kommunikaatio. Jaikun ja Twitterin kaltaiset mikroblogit (muutaman lauseen päivitykset, pääpaino eri verkostojen välisessä yhteydenpidossa) yhdistävät keskustelupalstojen ja blogi -julkaisemisen käytäntöjä, ja muun muassa Facebookin kaltaiset yhteisöpalvelut tarjoavat mahdollisuuden monipuoliseen julkaisemiseen ja vuorovaikutukseen. Keskeisenä tässä toiminnassa on henkilökohtaisen sisällön tuottaminen, joka muuttuu jatkuvasti monimuotoisemmaksi sekä yksityiskohtaisemmaksi. (Turtiainen, R.204-206.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

Sosiaalisen median palveluiden suosio perustuu osaltaan palveluiden käytettävyyteen ja sitä kautta saatavaan uudenlaiseen mahdollisuuteen tuottaa sisältöä ja kommunikoida toisten käyttäjien kesken. Aiemmin keskustelu oli keskittynyt Internetiin ja sen käytettävyyteen kokonaisuutena, nykyään huomio kohdistuu Internetin valtasovelluksiin, kuten Facebookiin, Twitteriin tai YouTubeen. (Suominen, J. 14.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.) Sosiaalisen median palvelusovellusten suosio perustuu suurelta osain palveluiden saamaan julkisuuteen ja tätä kautta saatuihin käyttäjiin. Palveluiden tuottajien intressissä ei ole yksittäisten käyttäjien arkielämän helpottaminen tai laadun parantaminen, vaan oman palvelun kaupallinen laajentuminen.

5.2 Yhteisöllisyys ja tiedon tuottaminen

Sosiaalinen sisällön tuottaminen ei ole uusi asia ja tämän ajan tietoverkottuneen yhteisön tulos, vaan monta sataa vuotta vanha tapa tuottaa tietoa sekä välittää informaatiota. Muutos on tullut siinä, millä tavalla ja kuinka helposti tietoa sekä sisältöä tuotetaan. Ennen määräävä valta tuotannossa oli niillä tahoilla, joilla oli mahdollisuus painotuoteteollisuuteen sekä valituneisiin kirjoittajiin. Nykyään kuka tahansa voi olla sisällön tuottaja, ilman suuria taloudellisia panostuksia tai kuulumista valtaeliittiin. Yksilöllisen tiedon tuottamisen ohessa, yhteisöllisen tiedon tuottaminen valtaa uusia tasoja, joissa valtarakenteet tai asiantuntijuus menettää asemansa. Tästä hyvänä esimerkkinä on Wikipedia -projekti. Suomessa projekti aloitti toimintansa elokuussa 2002. Wikipedia -artikkelit kirjoitetaan vapaasti, ja oikeellisuuden tarkastaminen tapahtuu yhteisöllisesti. Wikipedia -palvelussa on pyritty kehittämään useita tiedon laadun ja tarpeellisuuden kontrollimekanismeja. Nämä mekanismit ovat wikipedia -yhteisön itsensä luomia ja täten vain yhteisöön kuuluvien käyttäjien määrittelemiä. Tätä käyttäjäkuntaa johtaa tietty pieni eliitti. Peruskäyttäjän mahdollisuus vaikuttaa päätöksiin sekä sisältöön on hyvin pieni. (Suominen, J. 114.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.) Tiedon oikeellisuus näissä palveluissa perustuu käyttäjien tuottamaan informaatioon.

Tämä aiheuttaa ongelman tietojen oikeellisuuden varmentamiseen, koska tarkastava taho on pääosin sama, kuin tiedontuottaja.

Sosiaalinen media -käsitteen alle mahtuu paljon erilaisia sisällön tuottamiseen ja välittämiseen tarkoitettuja Internet-palveluja. Sosiaalisen median palvelut voidaan jaotella eri alueisiin riippuen palvelun käytöstä sekä sinne tuotetun sisällön luonteesta. Karkea jaottelu sosiaalisen median palveluille:

- sisällön luominen ja julkaiseminen (Youtube, Flickr)
- sosiaaliset verkostoitumispalvelut (Facebook, MySpace)
- yhteistuotannot (Wikipedia)
- virtuaalimaailmat (Habbo Hotel)
- lisäsovellukset

Internetin suosion keskeinen ominaisuus on mahdollisuus laajaan ja kattavaan kommunikaatioon toisten käyttäjien kanssa sekä erilaisten viihdepalvelujen tavoitettavuus. Internet ja siellä toimivat sosiaaliset palvelut tarjoavat käyttäjälle helpon ja muista kommunikaatiomenetelmistä poikkeavan mahdollisuuden tavoitettavuuden ja saatavuuden suhteen. Facebookin kaltaiset yhteisöpalvelut tarjoavat mahdollisuuden monipuoliseen julkaisemiseen ja vuorovaikutukseen. (Turtiainen, R. 222-224.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

5.3 Sisällön tuottamisen ongelmat

Internet ja siellä olevat erilaiset palvelut ovat kulttuurillisesti varsin nuori ilmiö. Vapaus ja rajoittamattomuus ovat olleet alusta lähtien Internetin perustoimintaideologia, joihin kajoaminen on koettu negatiivisena asiana. Toiminnan sääntely sekä vastuuttomaan käytökseen puuttuminen on jätetty pääosin käyttäjien varaan eikä yhteisten kansanvälisiin sopimuksiin perustuviin sääntelyjärjestelmiin ole sitouduttu. Aiemmin verkon tai palvelun ollessa pienen käyttäjäjoukon ulottuvilla oli ryhmän sisäinen sääntely sekä sopimattomaan toimintaan puuttuminen helppoa joko sulkemalla heidät pois palvelusta tai epämällä pääsyoikeudet. Maailmanlaajuisten palvelujen käyttäjä kunta on valtava ja alueellinen ulottuvuus globaali. Nykyisessä globaalissa toimintaympäristössä on käyttäjien ja käytön valvonta hankalaa ja ongelmatilanteisiin puuttuminen vaikeaa. Pelkästään kansallisten lainsäädäntöjen sekä käytäntöjen kirjo on valtavan suuri. Mikä toisessa maassa on kiellettyä toimintaa, voi toisessa maassa kuulua perustuslailliseen sananvapauteen. (Järvinen 2002, 179.)

Verkon käyttö ja erityisesti yhteisöpalvelujen käyttö on muuttunut hyvin nopeasti. Hyvin nopeassa ajassa asiantuntijoiden ja akatemiaturkijoiden yhteisestä, pienelle käyttäjäryhmälle tarkoitettusta välineestä on tullut globaali arkipäiväinen väline. Käyttäjäprofiilit ovat muuttu-

neet ja valveutuneiden it -osaajien lisäksi käyttäjiä on tullut kaikista eri sosiaaliluokista ja ammattiryhmistä. Käyttäjäprofiilien lisääntyessä on myös käyttö muuttunut. Pienen piirin ammatillinen tiedonvaihto on muuttunut laajaksi ja monipuoliseksi eri käyttäjäryhmien tiedonvaihdoksi, jossa jaettavan informaation määrällä tai muodolla ei ole rajoituksia. Internet nähdään ja se onkin faktisesti osa modernin ihmisen arkielämää. (Suominen, 191 - 200.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

Yhteiskunnan normaalielämän normit, arvot ja rajoitukset eivät kuitenkaan ole samassa mitakaavassa siirtynyt osaksi tietoverkkojen maailmaa. Verkko ei kuitenkaan ole täysin vapaa säännöistä ja rajoituksista, mutta verkossa toimimisen rajoitukset tulee osata, jotta verkkoa pystyy käyttämään mahdollisimman turvallisesti ja tehokkaasti. (Järvinen 2002, 179.) Verkkoon pääsyä tai siellä toimimista ei sääntele kukaan tai mikään. Verkkoon liittynyttä ei voi erottaa. Rajoittamattomassa ympäristössä vastuun kantaminen jää lähes täysin käyttäjien tehtäväksi. Tähän satojen miljoonien käyttäjien joukkoon mahtuu laaja skaala erilaisia toimijoita ja erilaisia motivaatioita verkossa olemiseen. Vastuullisten normaalikäyttäjien lisäksi verkosta löytyy häiriköitä, häiriintyneitä sekä rikollisia. Näiden käyttäjien motiivina on usein tai pelkästään omien tavoitteiden edistäminen vaihdellen mielihyvää puhtaasti rikolliseen toimintaan. Verkon sääntelemättömyyden lisäksi väärinkäyttöihin houkuttelee sekä sen mahdollistaa toimiminen anonyymisti tai todellisen henkilöllisyyden salaaminen ja väärentäminen. (Järvinen 2002, 179.)

Sosiaalinen media on muuttanut viestinnän luonnetta. Perinteisestä kahdenvälisestä viestinnästä on tullut kollektiivista. Viestinnän muuttuminen useiden eri tahojen samanaikaiseksi vuorovaikutukseksi on muuttanut käsitystä siitä mikä on yksityistä ja mikä julkista. Yksityisen käyttäjän lähettämä viesti muuttuu yleiseksi viestiksi lähetyshetkellä, kun lähettäjä painaa Enter -painiketta. Viestiä vastaanottamassa voi olla läheinen tuttu, mutta myös rajaton määrä taustoiltaan entuudestaan tuntemattomia tahoja. Viestin lähettäjä voi tilanteesta riippuen olla yksityinen henkilö tai mahdollisesti koko globaalille yhteisölle tietoa tuottava tiedottaja. (Aalto & Uusisaari, 2009, s.62.)

Yksityisen tuntuinen ei välttämättä ole yksityinen. Palveluissa, joissa näytetään ystävien tekemisiä ja kuulumisia ja jossa voi itse säätää, mitä tietoja antaa itsestään esittää muille ja mitä tietoja haluaa nähdä muista, on joskus varsin hankala hahmottaa, millaisena muut näkevät oman persoonan ja omat julkaistut sisällöt. On hyvä aika ajoin yrittää muodostaa mielikuva siitä, miltä itse näyttää yhteisön jäsenenä. Kun yksityiset ja työelämän kontaktit sekoittuvat verkostoissa, on nähtävä itsensä verkoston tiukkapipoisimman jäsenen silmin. Yleisösi ei rajoitu kaverilistaasi. kaverin selän takana voi seisoa tietokoneen ruutua katsomassa kuka tahansa. Maailma on pieni. Verkkoyhteisössä ei koskaan voi täysin tietää, ketkä kaikki pääsevät sisältöä näkemään, joten mitään arkaluontoista tai kenenkään yksityisyyttä loukkaavaa ei

kannata julkaista edes pienen porukan keskustelupalstalle. (Aalto & Uusisaari, 2009, s.98 - 100.)

Internetin palveluiden yleistyessä kaiken kansan arkielämän osaksi, on myös lisääntynyt erilaiset avoimen tiedonvälityksen ongelmat. Erityisenä ongelman on, ettei avoimessa tiedonvälityksessä ole mahdollista rajoittaa haitallista ja erityisesti rikollista sisällöntuottamista. Tästä esimerkkinä on rikollisen verkkosisällöntuottamisen islaminvastaisen informaation tuottaja Seppo Lehto, joka on kyennyt hyödyntämään uusien nettisovellusten ja palvelujen mahdollisuuksia omien äärioikeistolaisten näkemyksiensä esiintuomiseen. Nettitoiminnastaan oikeuden tuomioitakin saanut Lehto on tuttu useille sähköpostilistojen, keskustelupalstojen, Webin ja YouTuben käyttäjille rasistisesta ja äärioikeistolaisesta viestinnästään. Lehdon kaltaisten verkkosisällön - tuottajien toiminta on johtanut lainsäädännön muutoksiin, sähköpostisuodatusjärjestelmien kehittämiseen sekä aiemmin avoimien palvelujen rajaamiseen vain rekisteröidyille ja ylläpidon hyväksymille käyttäjille. (Suominen, J. 149.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

Uhkien kohtaamien sekä riskinotto on myös osa Internetin sosiaalisen toiminnan ympäristöä. Virtuaalisuhteen edessä Internetin käyttäjät ovat joutuneet uudenlaisen ihmissuhteiden ja itsensä esittämistä koskevien kysymysten eteen. Internet - suhteiden muodostumisen yhteydessä on pohdittu sitä, onko suhdetta oikeastaan olemassakaan, jos sen ylläpitämisen merkit näkyvät vain tietokoneruudulla. Myös väärällä nimillä tai valehenkilöllisyydellä esiintymisestä on pohdiskeltu. Romanttisten suhteiden ohella kysymyksille on ollut tyypillistä aktualisoitua myös muun Internet-välitteisen kommunikaation yhteydessä. Tutkimusmielessäkin kiinnostusta on herättänyt erityisesti virtuaalisen henkilöllisyyden ja todellisen minän välinen suhde. Internetiä on pidetty verkkohenkilöllisyydellä leikittelyn tilana, jossa eri persoonan esiintymisen on ajateltu olevan arkipäivää.

Ulla Heinonen (2008) on väitöskirjassaan tuonut esiin, että henkilön virtuaalipersona voi suuresti poiketa hänen verkon ulkopuolisesta persoonastaan. Tilana verkko mahdollistaa myös toisena esiintymisen, mutta pääsääntöisesti verkkoyhteisöjen jäsenet eivät Heinosen mukaan toimi näin. Heinonen kutsuukin virtuaaliyhteisöissä esiintyvää anonyymiyttä näennäiseksi. Virtuaalisen identiteetin sijaan Heinonen puhuu virtuaalisesta minäkuvasta, jonka hän määrittelee henkilön käsitykseksi omasta verkkopersonastaan, kuvaksi tai rakennetuksi hahmoksi, jolla haltija viestii itsestään. (Heinonen, U. 2008. 14.) Rooliin mukautuminen kuuluu luonnollisena osana kaikkeen inhimilliseen käyttäytymiseen. Ihmiset tuovat verkkoympäristössä itsensä esille eri asioita sosiaalisesta tilanteesta riippuen ja se on tuttua toimintaa myös Internetin ulkopuolella. (Turtiainen, R.204-206.) (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009.)

Web 2.0 aikakaudella tieto on valtaa. Taloudellinen ajattelu voi lähteä liikkeelle myös toisenlaisesta näkökulmasta. Sen sijaan, että yritys miettisi miten se voi hyötyä nykyisen verkon tarjoamista mahdollisuuksista, voidaan myös pohtia kuinka esimerkiksi sosiaalisen verkon ominaispiirteitä voidaan hyödyntää taloudellisen voiton tavoittelussa. Parhaiten käyttäjiä pysyvät palvelemaan ne, jotka tietävät eniten käyttäjämässän mielihaluista, tarpeista ja kiinnostuksen kohteista. Kertyneen tiedon ja sen hyödyntämisestä hyvän esimerkki on Amazon.com. Verkkokaupan suosituksen ja sivustojen yhteyteen muodostuvien mainosten käyttäminen on tehokas tapa käyttää jo kertyneitä tietovarastoja käyttäjien kulutustottumuksista. Erilaiset verkkokaupan suositukset ovat monesti oikein toteutettuja ja luovat vaikutelman siitä, että myyjä tietää ostajaa paremmin, mitä tämä haluaa. Hyvien suositusten antaminen on mahdollista vain, koska verkkopalvelin kerää ja käsittelee tehokkaasti tietoa valtaisan asiakaskuntansa mielenkiinnon kohteista ja ostopäätöksistä. (Tirronen, M. 2008. 9.)

Valta verkossa rakentuu niille tahoille, jotka osaavat sen käytön tai hallinnoivat tietoa. Tämän seurauksena on mahdollista, että merkittävää valtaa siirtyy sellaisille tahoille tai henkilöille, jotka eivät välttämättä osaa käyttää sitä oikein tai miellä vastuullisuutta tietojen käytössä heille kuuluvaksi. Verkossa ja sosiaalisessa mediassa toimiessa on kiinnitettävä erityisesti huomioita oman toimintansa vastuullisuuteen ja omien tekojen mahdollisiin seurauksiin. Huolimaton tai ajattelematon toiminta, kuten väärä komento, hiiren klikkaus tai kommentti saattaa aiheuttaa henkilölle isojaakin vaikeuksia, joko oman julkisuuskuvan tai tietosuojaa. (Järvinen 2002, 33.)

6 Käyttäjän identiteetti

Sosiaalisessa mediassa aivan kuten reaali maailmasta maine muodostuu yhteisöön kertyvästä toimintahistoriasta eli käyttäjän omien tekojen muodostamasta summasta. Lähes kaikki sosiaalisen median palvelut edellyttävät rekisteröimistä. Oman nimen käyttäminen on tavallaan edellytys sille, että kyseisestä palvelusta saa itseään hyödyntävän tuotteen. Rekisteröitymistä kautta käyttäjän nimi, sekä hänen mieltymyksensä paljastuvat muulle käyttäjäkunnalle. Käyttäjistä ja hänen toiminnastaan riippuu, mitä tietoja käyttäjästä näkyy ja millaisissa asiayhteyksissä. Käyttäjän maine kasvaa sitä mukaan, kun rekisteröityy ja tuottaa tietoa itsestään ja mielenkiinnonkohteistaan palveluihin; kotisivuihinsa, blogeihin tai verkkoyhteisöihin. Käyttäjän profiili on haettavissa yksittäin jokaisesta palvelusta erikseen tai käyttämällä hakukoneita, kuten Googlea tai muuta vastaavaa. Verkon sosiaalisissa palveluissa ei voi aukottomasti luottaa siihen, että yksityiseksi tarkoitettu sisältö pysyy luottamuksellisena. Palvelun tuottaja voi useissa tapauksissa yksipuolisesti muokata palvelun yksityisyysasetuksia, jolloin luottamuksellinen tieto vuotaa julkisuuteen. Tietovuoto voi tapahtua myös toisen käyttäjän toimesta, joka tahallaan tai huolimattomuuttaan vuotaa tiedon. (Aalto & Uusisaari, 2009, s.122 - 124.)

Tietojen ajallinen kertymä voi olla useita vuosia ja tulevaisuudessa kymmeniä vuosia. Tietoa käyttäjästä ja hänen toiminnastaan kertyy koko ajan. Käyttäjän nuoruuden radikaalitkin mielipiteet saattavat tulla yllättäen vuosien päästä julkisen tarkastelun alaisiksi. Mielipiteiden lisäksi tarkasteluun voidaan halutessa ottaa mikä tahansa käyttäjään liitettävä asia, kuten mieltymykset tai ystävät, niin menneet kuin nykyiset.

Verkossa tapahtuva vuorovaikutus mahdollistaa käyttäjälleen reaali maailmasta poikkeavan identiteetin ja käytöksen. Tahtoessaan käyttäjä voi olla täysin erilainen kuin todellisessa elämässä. (Aalto & Uusisaari, 2009, s.118.)

Tämän kokonaisuuden tarkastelussa merkityksellisiä asioita ovat ne seikat, joiden kautta verkon käyttäjät luovat oman kuvansa verkkoon. Verkkohenkilöllisyys tai verkkoidentiteetti on johdettavissa käyttäjän omista toimista ja hänen ympärillään olevista verkostoistaan. Näitä asioita voidaan tarkastella yksilöivästi Facebookin sekä yksityisyyden viitekehyksen kautta.

Käyttäjän profiili tai hänen verkkoidentiteetti on kuvaus käyttäjästä ja hänen asenteista, mielenkiinnoista ja käyttäytymisestä. Profiilin kautta käyttäjästä voidaan päätellä paljon, kuten poliittisesta suuntautuneisuudesta, yksityiselämästä tai mielihaluista. Käyttäjän asetusten mukaisesti, voi säädellä mitä kaikkea toiset saavat tietää itsestään. Käyttäjälle itselleen voi olla tarpeellista rajoittaa esimerkiksi yksityisyyttään koskevien tietojen rajoittamista joiltain osin riippuen onko kaverinaan läheinen tuttava vai esimerkiksi oma esimies tai muu vastaava hieman etäinen tuttava. Omaa harkintaa on, millaisia päivityksiä itsestään antaa ja milloin. Esimerkiksi jatkuvat biletapahtumien yölliset päivitystiedot uutisvirrassa antaa käyttäjästä mahdollisesti negatiivisen vaikutelman joissain tapauksissa. (Haasio 2009, 22.) Kaikesta käyttäjän antamasta informaatioista voidaan tehdä päätelmiä. Kirjoitusten lisäksi valokuvat, tykkäämiset tai valitut ystävät ovat sellaista informaatiota, josta muodostuu henkilön julkisuuskuva.

6.1 Yksityinen vai julkinen

Yksityisen ja julkisen tiedon raja voi sosiaalisessa mediassa hämärtyä. Jatkuvassa sisällön tuottamisen ympäristössä, käyttäjä ei tule jatkuvasti miettineeksi julkisen tai yksityisen tiedon välistä rajapintaa. Erityisenä ongelmana sisällön tuotannon rajaamisessa on silloin, kun käyttäjä on julkinen taho. Tällaisena edustajana käyttäjä voi vahingossa luovuttaa sellaista tietoa julkisena, jonka todellisuudessa pitäisi olla luottamuksellista. Pahimmassa tapauksessa luottamuksellisen tiedon vuotaminen aiheuttaa haittaa käyttäjälle itselleen, hänen edustamalleen taholle tai kolmannelle osapuolelle. (Aalto & Uusisaari, 2009, s.98 - 100.)

Käyttäjä ei koskaan voi verkkoyhteisössä varmistua siitä, että yksityiseksi tarkoitettu sisältö pysyy luottamuksellisena käyttäjän ja hänen kanssaan tekemisissä olevan tahon kanssa. Palveluun tuotettua sisältöä voi mahdollisesti tarkastella käyttäjän haluaman kaveripiirin lisäksi useita sellaisia silmäpareja, joille käyttäjä itse ei ole halunnut kyseistä arkaluontoista tai yksityisyyttä loukkaavaa sisältöä jakaa. Käyttäjä itse voi haluta, että hänen yksityiseksi asiakseen mieltämänsä sisältö pysyy luottamuksellisena; sisällön vastaanottaja katsoo asiaa omasta perspektiivistä ja eikä välttämättä jaa lähettäjän näkemystä asian yksityisyydestä. Käyttäjä ei todellisuudessa voi mitenkään olla varma siitä, miten toiset käyttäjät sosiaalisessa mediassa toimivat. Arkaluonteinen ja yksityinen sisältö, voi toisen käyttäjän toimesta levitä milloin tahansa julkiseksi. (Aalto & Uusisaari, 2009, s.98 - 100.)

Verkossa sosiaaliset suhteet rakentuvat verkostomaisiksi kokonaisuuksiksi. Yleensä ystäväksi kutsutaan hyvin läheisiä henkilöitä tai ainakin sellaisia henkilöitä, jotka on todella tavattu. Verkkomaailman ystävyudet ja suhteet muodostuvat toisella tavalla. Perinteisimmillään verkkoystävyyden on sama kuin verkon ulkopuolella, eli henkilöt tuntevat toisensa esimerkiksi harrastusten, työelämän tai muun sosiaalisen toiminnan kautta.

Verkossa saatamme ottaa ystäviksemme henkilöitä, joiden kanssa olemme aiemmin olleet vain pintapuolisesti yhteydessä tai joissakin tapauksissa emme ole tavanneet kasvokkain verkon ulkopuolella. Tällaisten entuudestaan tuntemattomien henkilöiden päästäminen omaan verkkoystäväpiiriin voi olla uhka, koska emme todellisuudessa tiedä mitkä asiat henkilöstä on tosia. Verkon sosiaalisten verkostojen rakentuminen sekä arki- ja verkkoelämän sekoittuminen vaikeuttaa ystäviksi otettavien henkilöiden taustojen varmistamisen. Ongelma on esimerkiksi sellaisilla ammattialoilla, joissa on välttämättömyys olla jatkuvassa sosiaalisessa kanssakäymisessä toisten kanssa niin arki- kuin verkkomaailmassa. Tällaiset ovat mm. tietyt tutkijapiirit, joissa seminaareja valmistellaan sekä niitä jatketaan verkossa. (Aalto & Uusisaari, 2009, s.97.)

Sähköpostin lähettäjätiedot on helposti väärennettävissä tai muunneltavissa. Sähköpostin lähettäjätietoihin voidaan muuttaa lähettäjän osoite tarkoituksena peittää oikean lähettäjän todellinen identiteetti. Lähettäjä voi käyttötarkoituksensa mukaisesti lähettää viestin toisen henkilön tai tahon nimissä, joko käyttämällä peiteltyä henkilöllisyyttä tai uskottelemalla olevansa vastaanottajalle entuudestaan tuttu viestin lähettäjä. Useat roskapostien lähettäjät käyttävät tällaisia menetelmiä, mutta tavoitteena voi olla mikä tahansa etuus, kuten rahallinen tai tiedollinen. (Järvinen 2002, 224.)

Maksulliset internetpalvelut ja niiden kautta hankittu sähköpostiosoite vaatii pääsääntöisesti taakseen liittymänhaltijan oikean henkilöllisyyden ja tämä henkilöllisyys on palveluntuottajan toimesta varmistettu. Ilmaiset Webmail -sähköposti osoitteen voi rekisteröidä itselleen sellai-

sella nimillä kuin käyttäjä itse haluaa. Webmail -sähköpostit eivät tarkasta millään tavalla rekisteröitymisen yhteydessä annettujen tietojen todenperäisyyttä tai käytettävän nimen oikeellisuutta. Webmail -sähköpostin käyttäminen mahdollistaa sen, että webmailia käyttävä taho voi esittää olevansa jotain muuta kuin mitä ilmoittaa olevansa. Viestin vastaanottaja ei voi suoraan varmistua viestin lähettäjän henkilöllisyydestä, mikäli viesti on lähetetty ilmaisen webmail -sähköpostin välityksellä. Tunnistamisen vaikeuttamista lisää myös se, että kyseisiä palveluja on verkossa satoja, joista yleensä vain tunnetuimmat, kuten Hotmail tai Yahoo, ovat kaikkien tiedossa. (Järvinen 2002, 225-226.)

6.2 Valokuvat

Valokuva-albumit ovat täynnä erilaisia käyttäjien sinne tuottamia kuvia tai videotiedostoja. Sosiaalisen median käyttöideologiaan kuuluu, että näitä tiedostoja jaetaan toisen käyttäjien kesken. Omilla kuvatiedostoillaan voi käyttäjä tehdä haluamansa mukaan, mutta jakamalla kuvia muiden kanssa, mahdollistaa kuvien leviämisen omasta tahdosta huolimatta. Uhka on olemassa vaikka kuvat olisivat rajatun käyttäjäryhmän nähtävissä tai hallittavissa salasanan kautta. (Järvinen 2010, 112.)

Kasvojentunnistus verkossa onnistuu laatimalla valokuvan kasvoista matemaattinen malli ja käyttämällä tätä mallia hakukriteerinä verkossa olevista valokuvista. Tämä ominaisuus löytyy mm. Googlen Picasa -ohjelmasta. Henkilön tunnistamisen edellytyksenä on, että valokuvassa oleva henkilö nimetään. Nimeämisen jälkeen ohjelma pyrkii löytämään vastaavan henkilön muistakin valokuvista. Nimeämisen edesauttamiseksi yhteisöpalvelujen käyttäjiä pyydetään nimeämään valokuvissaan olevia henkilöitä. Tunnistamisen tarkkuus edellyttää, että henkilö nimetään riittävän useaan valokuvaan, jotta matemaattinen malli tarkentuu. Tavoitteena on saada riittävän tarkka malli ja automaattinen tunnistus kaikista verkkoon syötettyjen valokuvien henkilöistä. Teknologia kehittyy jatkuvasti ja tunnistamista helpottaa digitalisoituminen kameroiden kehittyminen tarkkuuden ja kuvalaadun osalta. (Järvinen 2010, 241.)

Nuoruudessa tai muutoin tehty hölmöily saattaa vuosien päästä tulla esiin tätä kautta.

Digitaalisesti otetut valokuvat ovat monella tapaa jäljitettävissä. Selkein näistä on luonnollisesti kuvauskohde; ihminen, rakennus tai alue on helposti tunnistettavissa. Kuvauslaitteiden teknisen kehittymisen myötä niin kamerat, kuin kannettavat mobiililaitteet jättävät kuvaustapahtumista jälkeen erilaisia teknisiä jälkiä. Tällaisia ovat mm. laitteen valmistaja, valmistenumero tai kuvausajankohta. Nykytekniikka mahdollistaa hyvinkin tarkkojen kuvausajankohdan sekä kuvauspaikkaa yksilöivien tietojen tallentumisen otettuun kuvaan. Tällaisia tietoja ovat mm. kuvauspaikan tarkat sijaintiedot koordinaatteina tai hyvin tarkka kuvausajankohta sekunnilleen. Iso osa näistä yksilöivistä tiedoista on toisen osapuolen tarkasteltavissa erilaisen kuvankäsittelyohjelmien avulla. (Järvinen 2010, 118.) Sosiaalisen median käytön yleisty-

minen mobiililaitteissa sekä palvelujen käytön helppous kiihdyttävät käyttäjien intoa tuottaa valokuvatiedostoja ajasta tai paikasta riippumatta ja jakamaan tätä sisältöä muille käyttäjille.

6.3 Tietojen pysyvyys ja leviäminen

Verkkoon levinnyt tieto on verkon sisällä, eikä sen saaminen takaisin ole mahdollista. Tämän lisäksi tiedon leviämistä on mahdotonta rajoittaa. Harkitsemattomasti syötetty tieto omasta henkilökohtaisesta elämästä tai omista arvoista ja asenteista on verkossa pysyvästi. (Järvinen 2002, 47.) Verkossa oleva ja sinne laitettu tieto säilyy hyvin pitkän ajan ja tiedot voivat tulla esille useita vuosia sen jälkeen, kun tiedot on omasta mielestä poistettu verkosta.

Tietoja kerätään ja tallennetaan erilaisiin tietoarkeistoihin, joissa olevat www-sivujen vanhat versiot tai muut tiedot ovat jälkipolvien sekä tutkijoiden tarkasteltavissa. Tällaisessa pitkälle historiaan pohjautuvassa tarkastelussa nuoruuden radikaalit ajatukset tai ehkä harkitsemattomasti verkkoon syötetty informaatio saattaa tulla yleiseen tietoisuuteen, vaikka informaation tuottaja itse haluaisikin unohtaa kyseisen asian. Monille voi tulla yllätyksenä tilanne, jossa jälkipolvet kaivavat esiin vanhempiensa tekemät verkkosivut tai heidän käymänsä verkkokeskustelut. (Järvinen 2002, 205.)

Kaikki Internetiin laitettu informaatio tallentuu ja on kaivettavissa myöhemmin esiin. Myös henkilökohtaiseksi tarkoitettu viestintä tallentuu, vaikka viestin lähettäjä on omasta mielestään poistanut tiedon omalta tietokoneeltaan. Tahtomattaan käyttäjä jättää itsestään ja toiminnastaan paljon sellaista informaatiota, joka on myöhemmin löydettävissä, analysoitavissa sekä käytettävissä muun tahon kuin käyttäjän toimesta. Käyttötietojen lisäksi lisääntynyt viestintä kasvattaa itsestään annettavien tietojen ja informaation määrää. Hyvin henkilökohtainen viestintä on enenevässä määrin siirtynyt face to face viestinnästä, verkossa tapahtuvaan viestintään. Muutos koskee koko yhteiskuntaa ja kaikkia sen luokkia ikään tai sukupuoleen katsomatta. Vuosia sitten kirjoitettu mielipiteenilmaisu tai henkilökohtainen viesti on mahdollisesti kaivettavissa esiin vaikka kirjoittaja itse ei antaisi tähän lupaa ja itse haluaisi unohtaa kyseisen asian. Internet ei unohda, vaikka viestin kohde itse haluaisikin. (Järvinen 2002, 30-31.)

Sosiaalinen media ei ole lainsäädännöstä vapaa julkaisualusta, vaan siellä tehtävää julkaisu-toimintaa sääntelee kansallinen lainsäädäntö. Riippuen käytettävästä foorumista tai sisällöstä, kyseeseen tulevat useat eri lainkohdat rikoslaista sähköisen viestinnän lakiin. Käyttäjän on oltava kulloinkin tietoinen lain asettamista rajoituksista; provosoivassa nettikirjoittelussa ei tule syyllistyä herjaukseen tai toiselta saatua valokuvatiedosto ei tule ilman lupaa laittaa levitykseen kaupallisessa mielessä. (Järvinen 2010, 221.)

Virheellisen tiedon leviäminen tai tahallinen väärän tiedon julkaiseminen on sosiaalisen median palveluita käyttäen mahdollista ja varsin helposti toteutettavissa. Rekisteröityjen käyttäjien todellista henkilöllisyyttä ei palvelun tarjoajan toimesta tarkasteta ja käyttäjän mahdollisuudet valvoa tietojensa leviämistä ovat hyvin rajalliset. Alkuperäinen tieto tai tietokokonaisuus voidaan pilkkoa tarkoituksellisesti eri osiin, jolloin asiasisältö muuttuu tyystin erilaiseksi, kuin mitä alun perin on tarkoitettu. (Vahti 14.)

7 Yksityisyystiedon vuotaminen

Yksityisyystietojen vuotamista voi tapahtua usealla eri tavalla. Tässä tutkimuksessa yksityisyyden uhan kannalta tarkasteluun on otettu keskeisempiä tapoja, joilla yksityisyys voi olla uhattua sekä niitä tapoja, joilla tämä uhka on toteutuissa.

7.1 Käyttäjän oman toiminnan aiheuttamat uhat

Tietoturvan ja tietosuojan heikentäminen tapahtuu usein käyttäjän oman toiminnan kautta tahattomasti tai tahallisesti. Tahattomat tilanteet sattuvat virheellisestä toiminnasta, huolimattomuudesta tai taitamattomuudesta. Tahattomuus voi johtua myös siitä, ettei käyttäjä osaa arvioida toimintansa pitkän ajan vaikutuksia itselleen tai yhteisölleen. Käyttäjä voi myös aiheuttaa ongelmia tahallisesti, joko oman tai toisen osapuolen hyödyksi. Oma hyöty voi olla puhtaasti taloudellinen, jolloin halutaan itselleen jotain rahallista etuutta tai muuta vastiketta, keräämällä tietoa luvattomasti, erehdyttämällä toista tai järjestelemällä toiselle osapuolelle pääsyn sellaiseen tietoon, johon tällä ei ole oikeutta. Esimerkiksi katkeroitunut työntekijä, voi alkaa luovuttamaan yrityksen salaista tietoa tai muulla tavoin vahingoittamaan yrityksen toimintaa. Toisaalta myös tahattomasti käyttäjä voi joutua mukaan vahingolliseen toimintaan, hänen joutuessaan esimerkiksi sosiaalisen manipuloinnin kohteeksi, jossa tiedonhankintaan ja suostutteluun erikoistunut ammattilaitaho onnistuu saamaan luvattomia tietoja tai pääsyn sellaiseen tietoon käyttäjän toimesta. Näiden lisäksi käyttäjänä voi joutua kiristyksen kohteeksi ja on pakotettu luovuttamaan tietoa luvattomasti. (Järvinen 2002, 294.)

Tiedon jakamisessa tai sen lähettämisessä palveluun voi käyttäjä vahingossa toimia väärällä tavalla tiedostamattaan ja taitamattomuuttaan. Tällöin on mahdollisuus, että käyttäjä tulee välittäneeksi salassa pidettävää tietoja itsestään tai muista tahoista. Tietojen jälkikäteinen poistaminen on hyvin vaikeaa, varsinkin jos palvelu on ulkomailla. Haitallisen tiedon poistaminen on ongelma myös silloin, jos kyseessä mikä tahansa kolmannen osapuolen tarjoama palvelu. Vaikka poistamisoperaatioissa onnistuttaisiin, ongelmaksi tulee arkaluontoisten tietojen poistamisen hitaus. Kerran vahingossa levinneet tiedot ovat olleet muiden nähtävillä riittävän pitkän ajan ja itselleen tai muille haitallisen tiedon vuotaminen on jo tapahtunut, tie-

tojen poistamisesta huolimatta. Määrätietoinen poistamisen voi myös johtaa siihen, että haitalliset tiedot leviävät entistä paremmin. (VAHTI 14.)

Tietovuotoon ei välttämättä tarvita yksittäisen ja merkittävän tiedon ainutkertaista levittämistä. Tietovuoto voi muodostua myös pitkältä ajanjaksolta kertyneestä informaatiosta. Tällöin yksittäisestä tiedon vuotamisesta ei muodostu suoraa uhkaa yksilölle tai yhteisölle. Informaation kertyessä ja sitä louhittaessa analysoitavaan muotoon, kertyy erilainen tilannekuva, jossa yksittäisten tietojen informaatiomassa muodostaa kokonaisvaltaisen kuvauksen kyseessä olevan yksilön tai yhteisön luottamuksellista tiedoista tai toiminnoista. (Vahti 14.) Yksittäisten tietojen jatkuva vuotaminen johtaa siihen, että yksittäisten tietojen massasta kytetään luomaan sellainen kokonaisuus, jolloin tietovuodon kohteen yksityisyys ja luotettavuus on uhattuna.

Kokonaisuuden muodostuessa yksittäisistä tiedoista on suurena uhkana niin käyttäjän kuin hänen läheisten henkilöiden toiminta sosiaalisessa mediassa. Toinen henkilö tai taho saattaa palveluun lähettämässä informaatioissa, kuten sähköpostiviesteissä, videotiedostoissa, valokuvissa, sosiaalisen median päivityksissä, tahattomasti paljastaa yhteisöä tai käyttäjää koskevia yksityisyyteen liittyviä tietoja. Uhaksi tällöin muodostuu muiden tahojen informaation tuottaminen, johon omalla toiminnalla on hyvin vaikea vaikuttaa. (Vahti 14.)

Tekninen suojaus ei estä vahinkoa, mikäli käyttäjän toiminta on huolimaton, osaamaton tai väärää. Hienosta ja teknisesti kehittyneestä järjestelmästä ei ole hyötyä, mikäli käyttäjä ei osaa tai ymmärrä oman toimintansa riskejä. Ihminen on järjestelmän heikoin lenkki. Valpautta ja huolellisuutta ei voi korjata teknisillä järjestelmäparannuksilla. (Järvinen 2002, 47.)

Verkon käyttö ja sinne luovutettu informaatio säilyy ja on muiden luettavissa hyvin pitkän ajan. Tällaisen historian kerääntyminen alkaa ensimmäisestä kerrasta toimiessa verkossa. Ihmisten toiminta muuttuu hänen kasvaessaan ja samoin kehittyy tapa ajatella sekä tapa viestiä. Koska verkkohistoria säilyy pitkään, voi usealle käyttäjälle tulla ikävänä muistutuksena nuoruudessa kirjoitetut news-viestit tai pilamielessä koostetut www-sivut. Suuri osa verkossa tehdyistä hölmöilyistä voidaan laittaa aiheellisestikin nuoruuden ja kokemattomuuden piikkiin. Toisaalta näillä seikoilla voi olla hyvin suuri painoarvo henkilöä arvioitaessa, esimerkiksi työhönottohaastattelussa. (Järvinen 2002, 204.)

Tietoyhteiskuntaan siirtymisen yhteydessä moni asia on muuttunut asenteessa käyttäytymiseen verkossa ja siihen mitä tietoja tai asioita sinne laitetaan. Yhteiskunnassa sensuuri nähdään yleisesti huonona asiana ja sensuuria vastustetaan laajalti kaikkien yhteiskuntaluokkien taholta. Erityisesti tiedon rajoittamien mm. valtion taholta nähdään negatiivisena ja tämän vuoksi tietoyhteiskunnan tavoitteena joidenkin mielestä on avoimuuden ja tiedon lisääminen.

Avoimuuden lisääntyminen on myös lisännyt tarvetta suojata itseään koskevia tietoja. Yksilön suoja ja yksityisesti tiedot tulee suojata toimiessaan verkossa ja yksityiset tiedot on turvattava, ettei omalla toiminnallaan vaaranna omaa turvallisuutta. Teknisen toteuttamisen valmiudet ja asenteelliset valmiudet saattavat vaihdella käyttäjien kesken paljon. Reaalimaailmassa toimiminen edellyttää ihmiseltä opittuja tietoja ja taitoja, kuten liikennesääntöjen osaaminen ja noudattaminen, oman omaisuuden turvaaminen sekä itselleen tärkeiden ja välttämättömien tietojen suojaaminen. Kuvatunlaiset perustiedot - ja taidot opitaan ja niitä pidetään perusedellytyksenä yhteiskunnassa pärjäämiselle. (Järvinen 2002, 18-19.)

Verkkokäyttäytymisen taidot, joita Järvinen(2010, 18) kutsuu ”2000 -luvun kansalaistaidoiksi” vaihtelee käyttäjän osaamistason ja valveutuneisuuden mukaan, ja joillakin ei ole kertakaikista ymmärrystä esimerkiksi välttämättömmistä turvallisuustaidoista heidän toimiessaan verkossa ja tuottaessaan informaatiota itsestään ja lähiympäristöstään. Taidot henkilökohtaisten tiedostojen ja yksityisyyden suojasta ovat perusasioita, ja ne on osattava ihmisen toimies- sa verkossa ja sosiaalisessa mediassa.

7.2 Viestin kirjoittamisen helppous ja välittömyys

Nykymuotoinen viestintä eroaa merkittävästi aikaisemmasta kirjallisesta viestinnästä. Aiemmin viestin, kuten kirjeen kirjoittamiseen käytettiin huomattavasti enemmän aikaa. Ajan käytön lisäksi viestin kieliopilliseen sekä ulkoasuun kiinnitettiin enemmän huomiota kuin nykyisin yleensä. Viestinnästä on tullut helppoa, reaaliaikaista ja mahdollisimman välitöntä. Nopeassa ja välittömyyden ilmapiirissä kirjoitetussa viestinnässä on mahdollista, että viestin lähettäjä tulee viestineeksi jotakin, joka on hänelle tai muulle taholle epäedullinen. Myös mahdollisuus viestin sisällön väärinymmärtämiseen kasvaa, koska suuri osa kirjallisesta viestinnästä tehdään nopeasti. Viestinnän helppous sekä lähettämisen nopeus on uhka, koska viestien väärinymmärrys kasvaa sekä viestit voivat päätyä vahingossa väärälle taholle, jo pelkän näppäysvirheen johdosta. Viestin lähettäjä ei voi mitenkään kontrolloida viestin etenemistä sen jälkeen, kun viesti on sähköisesti lähetetty eteenpäin. Lainsäädännön mukaan viestin vastaanottaja voi tehdä viestille mitä tahansa ja voi halutessaan jatkolähetellä viestiä rajoituksetta, edellyttäen, että viesti on alun perin osoitettu vastaanottajalle.. (Järvinen 2002, 230.)

Sosiaalisen median käyttö ei ole sidottu aikaan tai paikkaan. Kaupungeissa olevat laajakaista- verkot mahdollistavat palveluun kirjautumisen milloin ja mistä tahansa. Langattomien datayhteyksien, kannettavien tietokoneiden, kämmentietokoneiden tai kehittyneiden älypuhelimien avulla käyttäjä voi tahtoessaan tuottaa informaatiota verkkoon reaaliaikaisesti. Yhteisöpalveluiden, kuten Facebook yksi käytetyimmistä ulottuvuuksista on mahdollisimman reaaliaikaisen tiedon tuottaminen itsestään tai tapahtumista. Sivustoille tuotetaan erilaista informaatiota omista arkisista tapahtumista kirjoittamalla tai lähettämällä mm. kännykkäkameral-

la otettua kuvaa omasta ympäristöstä. Monet yhteisöpalvelut (mm. Facebook, Twitter) kehittävät palveluaan, jotta reaaliaikaisen informaation tuottaminen palveluun on mahdollisimman vaivatonta. Samalla myös erilaiset mobiililaitteet kehittyvät, jotta niillä voidaan tuottaa reaaliaikaista tietoa yhteisöpalveluihin mahdollisimman helposti. Tämä palveluntuottajien sekä mobiililaitteiden valmistajien välinen yhteistyö on toisiaan tukevaa, tarkoituksena mahdollisimman helppokäyttöinen ja vaaton toiminta yhteisöpalveluiden käytölle ja informaation tuottamisella. (Aalto & Uusisaari, 2009, s.107.)

8 Facebook

Sosiaalisen median palveluista Facebook on tällä hetkellä suosituin. Facebook kasvaa jatkuvasti ja saa käyttäjikseen yksityisiä henkilöitä sekä yhteisöjä. Facebook palveluna tarjoaa useita sellaisia ilmiötä, jotka löytyvät lähes kaikista sosiaalisen median palveluista. Näiden ominaisuuksien lisäksi Facebookissa on omia erityisiä ominaisuuksia, joita tulee tarkastella yksityiskohtaisemmin suhteessa yksityisyyden ughiin palvelun käyttäjille.

Facebook on Internet-yhteisössä tuotettu virtuaalinen yhteisö. Tämä palvelu mahdollistaa käyttäjille ihmissuhteiden ylläpidon, olemassa olevien ihmissuhteiden ylläpidon, uusien ihmisten ja ryhmien tapaamisen. Facebook -palvelussa voi myös jakaa omia mielipiteitä ja keskustella haluamien henkilöiden kanssa, voi ylläpitää ihmissuhteita, tavata uusia ihmisiä, keskustella ja tehdä testejä, pelata jne. oman mielenkiintonsa mukaan. Käyttäjä voi hakeutua erilaisiin ryhmiin, jotka ovat rakentuneet eri kiinnostuksen kohteen ympärille vaihdellen harrastustoiminnasta poliittiseen aktivismiin. (Haasio 2009, 9.)

Facebook mahdollistaa käyttäjälleen muun muassa seuraavat asiat:

- 1) Yhteydenpito ystävien kanssa
- 2) Vanhojen ystävien löytäminen
- 3) Verkostoituminen samanhenkisten ihmisten kanssa
- 4) Pelaaminen
- 5) Persoonallisuustestien tekeminen
- 6) Valokuvien jakaminen
- 7) Reaaliaikainen keskustelu
- 8) Eri harrasteryhmiin yms. liittyminen ja niissä toimiminen
- 9) Omien ryhmien luominen esim. yhdistykselle tms.
- 10) Seuranhaku

(Haasio 2009, 10.)

Facebookin suosion yksi tärkeä tekijä on palvelun monipuolisuus. Palvelun monipuolinen tarjonta antaa valtaosalle käyttäjistä heitä itseään kiinnostavia ryhmiä sekä henkilöitä. Käyttäji-

en motivaatiot palvelun käyttöön vaihtelevat; toisille Facebook on osa vapaa-aikaa ystävien kanssa keskustellen toiset, verkostoituivat facebookissa ensisijaisesti ammatillisista syistä. Käyttötarkoituksesta huolimatta Facebook tuottaa ensisijaisesti alustan ihmisten väliseen yhteydenpitoon. Facebookista voi monille muodostua tärkeä yhteydenpitoväline ystävien välisessä kommunikaatiossa. Oman kaveripiirin lisäksi Facebookista voi etsiä sellaisia tuttuja, joihin ei ole ollut yhteydessä pitkiin aikoihin, kuten lapsuuden ystävät tai koulukaverit. Facebook myös mahdollistaa reaali-aikaisen kommunikaation riippumatta käyttäjän asuinpaikasta. Globaalisuus on Facebookin yksi keskeinen etu, haluamiensa henkilöiden kanssa käyttäjä ei ole sidottua aikaan tai paikkaan. Monelle käyttäjälle on muodostunut tarve päivittää omaa statustaan mahdollisimman usein. Facebook on käytössä lähes koko ajan, riippumatta siitä onko käyttäjä töissä tai vapaalla. (Haasio 2009, 9-10.)

8.1 Käyttäjät ja käyttö

Facebook on ensisijaisesti yhteisöpalvelu, jossa käyttäjät toimivat omalla vapaa-ajallaan. Ammatilliseen käyttöön tarkoitettuna palveluna Facebook tarjoaa mahdollisuuden tiedottaa ammatillisista tapahtumista sekä verkostoitua ammatillisessa mielessä. Joillakin aloilla on lähes välttämätöntä, että käyttäjä tai käyttäjän ammattiryhmä on edustettuna Facebookissa. Ammatillisen käytön merkitys kasvaa jatkuvasti. Erilaisista konferensseista, seminaareista ja tapahtumista tiedotetaan Facebookin kautta ja näiden tapahtumien sisällöstä keskustellaan osallistujien kesken ennen ja jälkeen tapahtuman. Facebook on moniulotteinen palvelu, jossa käyttötarkoitus ja sisältö vaihtelevat sen mukaan, mitä käyttötarkoitusta Facebook halutaan palvelevan kullakin hetkellä. Yksittäisen käyttäjän tavoitteen mukaisesti Facebook on läheisten ystävien ja tuttujen välinen informaatiofoorumi tai ammattilaisessa mielessä oleva verkostoitumis- ja edustuskanava. (Haasio 2009, 9-10.)

Facebookin suosio ja palvelun käytön helppous on tehnyt palvelusta joillekin käyttäjille kiinteän osan heidän arkipäivästä elämänsä, jossa kaikki mielenkiinnon kohteet sekä arkielämän tapahtumat välitetään Facebookin kautta muiden tietoon jopa reaaliajassa.

Viestinnän helppous sekä viestinnän uuden muodot voivat olla todellinen uhka mm. Facebookin käyttäjälle. Facebookissa viestintä ja oman mielipiteen antamisen on tehty rakenteellisesti mahdollisimman helpoksi mm. instant messages tai tykkää -komennoilla. Tykkää -komennoilla käyttäjä voi helposti antaa mielipiteensä toisten kommentteihin tai heidän välittämiinsä sivustoihin. Harkitsematon käyttäjä voi antaa pikaistuksissaan kommentin esimerkiksi asiasta, joka on hyvin arkaluonteinen tai työnantajan linjausten vastainen. Nämä kommentit näkyvät välittömästi useilla eri verkkosivuilla, eikä niitä voi käytännössä poistaa tai leviämistä rajoittaa.

Harkinnan pettäminen yhdistettynä viestinnän helppouteen on vaarallista, koska käyttäjä voi viestiä asioista aikana ja henkisessä tilassa, jolloin hän ei muutoin normaalisti viestisi. Tällaisia tilanteita ovat esimerkiksi humalatilassa tai tunnekuohussa kirjoitetut viestit tai kannanotot. (Järvinen 2002, 230.)

8.2 Yksityisyystiedot Facebookissa

Facebookin käyttäminen vaatii rekisteröitymisen. Ilman rekisteröitymistä Facebookissa voi tarkastella sellaisia sivuja, jota ovat avoinna kaikille käyttäjille ja yleensä toimivat jonkin asian markkinointikanavana, kuten kaupallisten edustajien sivustot.

Käyttäjän rekisteröityessä Facebook -palveluun on luotava käyttäjälle oman profiili, eli käyttäjän Facebook -identiteetti. Palveluun rekisteröityminen ja identiteetin luominen vaatii käyttäjästä yksilöitäviä tietoja, kuten nimi, asuinpaikka, sukupuoli, syntymäaika ja sähköpostiosoite. Syntymäaika on ilmoitettava ylläpidolle, mutta sitä ei tarvitse laittaa näkyviin tai saatavaksi muille tahoille.

Facebookin käytön tarkoituksena on, että kaikki palvelun käyttäjät toimivat omilla oikeilla nimillä ja muilla oikeilla tunnistetiedoilla. Palvelun perustarkoituksena on, että jokaisella käyttäjällä on aito profiili, jonka takana on se taho, joka profiilin identiteetissä ilmoitetaan olevan. (Haasio 2009, 17.) Facebook ei millään tavalla varmista rekisteröitymisen yhteydessä annettujen identiteettitietojen oikeellisuutta ja todenperäisyyttä.

Rekisteröinnin yhteydessä Facebook pyytää käyttäjää ilmoittamaan itsestään laajasti erilaisia yksityisyystietoja. Näitä tietoja käytetään palvelun käytettävyyden parantamiseen, käyttäjän tunnistamisen helpottamiseen sekä palvelun muuhun kehittämiseen. Valikko erilaisille käyttäjän yksityistiedolle on varsin laaja. Käyttäjä voi itse valita mitä tietoja itsestään ilmoittaa ja mitkä tiedot ovat muille käyttäjille näkyvissä.

Facebook -palvelun käyttäjätiedot sisältävät seuraavia tietoja:

Perustiedot

- verkostot, joihin olet liittynyt
- sukupuoli
- syntymäaika
- parisuhdetilanne

Henkilökohtaiset tiedot

- kiinnostuksen kohteet
- lempiohjelmat televisiossa

- lempikirjat

Yhteystiedot

- sähköposti
- puhelinnumero
- kotisivu
- osoite

Koulutus ja työ

- korkeakoulu
- lukio/ammattiopisto
- työnantaja
- työtehtävät
- sijainti
- ajanjakso
- kuvaus

Ryhmät, joihin kuulut

Sivut, joille olet liittynyt

8.3 Profiili, identiteetti ja sovellukset

Facebook on interaktiivinen palvelu ja käyttäjä voi halutessaan reagoida palvelussa olevaan informaatioon. Facebookin kautta suoritetaan erilaisia kyselyjä, joissa käyttäjä antaa oman mielipiteensä klikkaamalla kyllä tai ei -vaihtoehtoa esitettyjen kysymysten kohdalla. Osa kyselyistä on osittain yksityisiä, jolloin vastaukset ovat vain kyselyn tekijän ja vastaajan tiedossa. Osa kyselyistä on julkisia, jolloin käyttäjän antamat vastaukset ja mielipiteet ovat kaikkien nähtävillä. Oman mielipiteen antaminen on Facebookissa hyvin helppoa. Kaikkein palvelussa olevaan informaatioon voin helposti antaa oman kantansa klikkaamalla peukku ylös - tai peukku alas -painiketta. Osa kyselyistä on tietynlaista roolipeli; käyttäjä voi osallistua kyselyyn, jossa määritellään millainen eläin käyttäjä on luonteeltaan.. (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009. 262.) Facebookissa voi käyttää myös digitaalisia eleitä. Kavereita voi tökätä (poke) ja heidän julkaisemistaan päivityksistä tykätä (like).

Profiilisovelluksen voi tehdä niin usein, että saa itselleen halutunlaisen profiilin - leijona tai lammas.

Käyttäjän profiili voi olla minkäläinen tahansa. Ei ole mitään yhtenäistä käytäntöä siitä, millainen käyttäjän profiilin ja erityisesti sitä kautta jaettavan tietojen tulee olla. Käyttötarkoituksesta riippuen, profiilin tiedot voivat olla niukat tai hyvinkin kattavat. Erityistä huomiota tulee kiinnittää jaettavien tietojen saavutettavuuteen. Jos käyttäjä haluaa olla julkinen, eli profiili on kaikille avoin, on syytä harkita kovin yksityisten tietojen jakamista tuntemattomille. Sama pätee myös tietyn osin myös suljetun kaveripiirin välisessä tietojen jakamisessa, jos

käyttäjä haluaa varmistautua, etteivät omat yksityiset asiat lähde leviämään verkossa. Facebookin tarkoituksena kylläkin on, että käyttäjät jakavat tietoa keskenään. Käyttäjän ollessa niukka omien tietojen jakamisessa, ei Facebook tai muut hakukoneet kykene löytämään käyttäjää ja silloin mahdollisesti palvelusta ei saa sitä tarvittavaa hyötyä, kuten tavoittaa tunteimiaan henkilöitä. Ongelma on kahden suuntainen; mikäli jakaa tietoa itsestään, muut löytävät käyttäjän helpommin, mutta vaarana on itseään koskevien yksityisten tietojen leviäminen. Toisaalta vähäinen tietojen jakaminen ei edesauta käyttäjää verkostoitumaan tuntemiensa henkilöiden kanssa. (Haasio 2009, 19- 20.)

Profiilin luomisessa käyttäjän on ensisijaisesti tarkasteltava omia tavoitteitaan palvelun käyttäjänä. Profiilissa ja sen näkyvissä identiteettitiedoissa merkitystä on sillä, minkälaiseen käyttöön ja keiden tahojen tietoon käyttäjä haluaa palvelua käytettävän tai sen kautta tavoitettavan. Profiilin asetuksia voi muokata sen mukaisesti, mitä tietoja haluaa itsestään muiden tietoon ja saataville. (Haasio 2009, 19.) Facebook on saanut suuresti kritiikkiä siitä, että se on yksipuolisesti muuttanut käyttö sopimuksia ja muokannut käyttäjien yksityisyysasetuksia ilman käyttäjän suostumusta.

Käyttäjän omat tarpeet muokkaavat hänen profiiliaan. Matalalla profiililla toimiessa, tulee Facebookin yksityisasetuksiin tehdä valintoja, jossa rajataan omia yksityisyystietoja. Näiden asetusten kautta käyttäjä pystyy määrittämään ne tiedot, jotka hänestä tulee näkyviin Facebookin sivuilla sekä erilaisissa hauissa. Halutessaan käyttäjä voi määrittää itselleen sellaisen nimimerkin, josta käyttäjä ei ole tunnistettavissa ja joka on vain käyttäjän haluamien henkilöiden tiedossa. Matalan profiilin käyttäjän on myös rekisteröityessään käytettävä sellaista sähköpostiosoitetta, joka ei mahdollista käyttäjän tunnistamista tämän kautta, koska Facebookissa voi suorittaa hakuja sähköpostiosoitteen perusteella. (Aalto & Uusisaari, 2009, s.98.)

8.3.1 Kuvat

Facebook -profiilin voi lisätä kuvan itsestään tai jonkun muun kuvan, jonka haluaa kuvaavan itseään tai persoonallisuuttaan. Kaikki käyttäjistä eivät ole lisänneet itsestään kasvokuvaa tai ovat jättäneet kuvatilat täysin tyhjäksi. Facebookissa tämä on sallittua, mutta esimerkiksi suomalaisessa IRC-galleriassa on oltava itseään esittävä tunnistettava valokuva. Käyttäjän tunnistettavuus heikkenee, mikäli hän jättää lisäämättä tunnistettavan kuvan itsestään. Kuvan uupuminen myös vaikeuttaa muiden käyttäjien hakuja, heidän etsiessään vanhoja tuttaviansa Facebookin hauilla, koska tällöin hakuja tekevä käyttäjä ei voi täysin varmistua hakemansa henkilön henkilöllisyydestä. (Haasio 2009, 20.)

Käyttäjän profiili ja siihen liitetty valokuva ovat osa käyttäjän persoonallisuudesta kertovaa informaatiota. Visuaalinen kuva on ensikosketus taholle, joka tarkastellee kohtaamaansa

käyttäjää. Tunnistettavuuden helpottamiseksi yleisesti käytetään edestäpäin otettua kasvo-kuvaa, erityisesti käyttäjän toimiessa julkisessa tehtävässä tai muutoin ammatillisessa tarkoi-tuksessa. Julkisessa tehtävässä toimivat henkilöt usein valitsevat itsestään hyvän ja ammatti-maisesti kuvatun edustusvalokuvan, koska kuvaa voidaan muiden taholta käyttää erilaisissa julkaisuissa. Valokuva on käyttäjän viesti, siitä millainen hän on ja millaisena hän itsensä ha-luaa nähtävän. Kuvassa pystytään persoonallisuuden lisäksi, myös päättelemään henkilön yksi-tyisyyteen liittyviä asioita. Profiiliin liitetty vapaa-ajalla otetusta kuvasta, voidaan päätellä käyttäjän henkilökohtaisia mieltymyksiä, rutiineja sekä asuinympäristöä. Kuva, josta käyttä-jää ei pysty suoraltaan tunnistamaan viestii henkilön haluavan mahdollisesti suojella itseään sekä yksityisyyttään. (Aalto & Uusisaari, 2009, s.32-33.)

Facebook pyytää tunnistamaan ja nimeämään palvelun kautta välitetyissä valokuvissa esiinty-vien henkilöiden nimiä. Tämä helpottaa kasvojen tunnistusta sekä siihen tarvittavien tietojen keräämistä, koska käyttäjät tekevät tunnistamistyön ilmaiseksi palveluntuottajan puolesta. Omien kuvien lisäksi, käyttäjät voivat kommentoida muiden kuvia ja tunnistaa näissä olevia henkilöitä. (Järvinen 2010, 234.)

8.4 Ystävät

Verkossa sosiaaliset suhteet rakentuvat verkostomaisiksi kokonaisuuksiksi. Arkikielen ”ystävä” tai ”friend” tarkoittaa eri asiaa verkossa tai reaali maailmassa. Verkkomaailman ystävykset ja suhteet muodostuvat toisella tavalla. Perinteisimmillään verkkoystävyyden on sama kuin verkon ulkopuolella eli henkilöt tuntevat toisensa esimerkiksi harrastusten, työelämän tai muun sosi-aalisen toiminnan kautta. Verkossa saatamme ottaa ystäviksemme henkilöitä, joiden kanssa olemme aiemmin olleet vain pintapuolisesti yhteydessä tai joissakin tapauksissa emme ole tavanneet kasvokkain verkon ulkopuolella. Tällaisten entuudestaan tuntemattomien henkilöi-den päästäminen omaan verkkoystäväpiiriin voi olla uhka, koska emme todellisuudessa tiedä mitkä asiat henkilöstä on tosia. Verkon sosiaalisten verkostojen rakentuminen sekä arki- ja verkkoelämän sekoittuminen vaikeuttaa ystäviksi otettavien henkilöiden taustojen varmista-misen. Ongelma on esimerkiksi sellaisilla ammattialoilla, joissa on välttämättömyys olla jat-kuvassa sosiaalisessa kanssakäymisessä toisten kanssa niin arki- kuin verkkomaailmassa. Täl-laiset ovat mm. tietyt tutkijapiirit, joissa seminaareja valmistellaan sekä niitä jatketaan ver-kossa. (Aalto & Uusisaari, 2009, s.97.)

Facebookin käyttäjäjällä on kesimäärin noin 120 ystävää. Ystävämäärät vaihtelevat suuresti. Joillain käyttäjillä on vain muutamia, toisilla taas satamäärin. Erot ystävämäärissä selittyy sillä, että virtuaali maailman ystäväpiiri eroaa monesti reaali maailman vastaavasta. Monet palvelun käyttäjät hyväksyvät tuttavikseen itselleen tuntemattomia henkilöitä. Eräät käyttä-jät myös aktiivisesti hakevat itselleen tahoja, joita pyytävät Facebook -ystäväkseen. (Haasio

2009, 33 - 35.) Käyttäjän tavoitteet kaverien ja kaverikontaktien suhteen saattavat vaihdella suuresti, eikä ole olemassa yhtä oikeaa tapaa sille, kuka ja millaisia kaverikontakteja itselleen kerää. Facebook -palvelu tarjoaa käyttäjälle jatkuvasti uusia kontakteja ystäviksi, nämä kontaktit muodostuvat pääosin käyttäjän kavereiden kavereista.

8.4.1 Kaverihaku

Kaverihaun kriteerinä ovat lähtökohtaisesti käyttäjän nimi tai sähköpostiosoite. Hakukriteereinä toimivat kaikki tiedot, jotka käyttäjä on syöttänyt omaan profiiliinsa. Facebook mahdollistaa palvelun, jossa käyttäjä luovuttaa oman henkilökohtaisen sähköpostiosoitteistonsa palvelulle. Tämän osoitteiston avulla palvelu suorittaa haun osoitteistossa olevien tietojen perusteella ja vertaa niitä palvelussa oleviin tietoihin, ehdottaen sitten käyttäjälle sopivia kaverikohteita. (Haasio 2009, 36-37.) Facebook ja Google tukevat toisiaan ja vertaavat tietokannoissaan olevia tietoja keskenään. Tämä mahdollistaa tarkemman ja laajemman palvelutuotteen, jossa käyttäjät voivat helposti tavoittaa itselleen kiinnostavia henkilöitä, ryhmiä tai muita palveluja.

8.5 Rekisteröinti, käyttöehdot ja tietojen luovuttaminen

Rekisteröityminen verkkopalveluun mm. Facebookiin vaatii erilaisten henkilötietojen ja yksityisyystietojen luovuttamisen rekisteröinnin yhteydessä. Tietojen luovuttamisessa on tarpeen käyttää harkintaa, mitä tietoja itsestään ja yksityisestä elämästään luovuttaa. Palvelutarjoajan näkökulma erilaisten yksilöivien tietojen keräämiseen on käytettävän palvelun kehittäminen ja erilaisiin kohderyhmiin suuntautuvan markkinoinnin parantaminen. Toisaalta käyttäjän näkökulmasta tulee huolehtia omata tietosuojasta sekä yksityisyydestä tietoja luovutettaessa. Verkkopalvelun luonteesta riippuen tulee käyttäjän harkita mitkä ovat niitä itselleen kyseistä palvelua käytettäessä tarpeellisia luovutettavia tietoja. Esimerkiksi, käyttäkö rekisteröintiin yksityisessä käytössä sähköpostiosoitteeksi valittua webmail -osoitetta vai omaa työsoitetta. (Järvinen 2002, 170.) Facebook ei tarkasta henkilötietojen oikeellisuutta, eikä ota vastuuta käyttäjätietojen oikeellisuudesta.

Käyttöehtojen hyväksyminen on uuden palvelun käyttämisen edellytys. Käyttöehtojen hyväksymisellä käyttäjä vakuuttaa, että on lukenut kyseiset ehdot ja hyväksyy niissä mainitut seikat. Käyttäjän kannalta on merkityksellistä ymmärtää käyttöehdoista ne seikat jotka käsittelevät käyttäjän välittämän informaation yksityisyyttä sekä jaettavan informaation omistajuutta. Käyttäjän kannalta on merkitystä sillä onko hän alun perin tarkoittanut jonkun informaation yksityiseksi ja vain tietyn vastaanottajatahon saataville ja täten poissuljettu laajemmalla ja myöhemmältä käytöltä. Sosiaalisen median käyttäjä on myös sisällön tuottaja ja jakaja. Facebook mahdollistaa käyttäjilleen mahdollisuuden kehittää palvelua lisäämällä palveluun

erillisiä ja Facebook -yhtiöstä itsenäisiä sovelluksia ja toimintoja ("Third party applications", "Widgets"). Facebook -palvelu tarjoaa alusta, johon käyttäjä voi määritellä haluamansa sovelluksen ilman erillistä hyväksyntää. (Aalto & Uusisaari, 2009, s.39-40.)

Käyttäjä ei voi varmistua siitä, mitä ja kenen tuottamaa palvelua hän käyttää hyväksyessään kolmen tahon sovelluksen käytön. Käyttäjä ei myöskään voi varmistautua mitä kyseinen sovellus tekee ja mihin sovellukseen annettuja tietoja käytetään. Käyttöehdoissa on maininta, jonka mukaan palveluntarjoaja voi yksipuolisesti muuttaa käyttöehtosopimuksia ilman erilaista ilmoitusta käyttäjille. Käyttöehtojen muutosten tarkastaminen jää palvelun vastuulle, ja on hänen velvollisuutena tarkastaa, mikäli ehdot ovat muuttuneet.

Käyttöehtosopimus voi syntyä myös ilman rekisteröinnissä suoritettavaa vahvistusta käyttöehtojen hyväksymisestä. Palvelun tuottajan näkemyksen mukaan, käyttäjä hyväksyy käyttöehdot, mikäli hän käyttää palvelua. Facebookin käyttö on mahdollista ilman rekisteröintiä, jolloin henkilö voi tarkastella palvelussa olevaa informaatiota, mikäli se on asetettu näkyviin ilman käyttörajoitetta. (Aalto & Uusisaari, 2009, s.40.)Tällaista informaatiota ovat mm. yritysten ja julkisyhteisöjen Facebook -sivustot.

Facebookin käyttöehdoissa mainitaan, ettei palvelun tuottaja vastaa sinne tuotetun informaation oikeellisuudesta, luotettavuudesta tai turvallisuudesta. Palvelun tarjoaja ei käy ennakkoon läpi palveluun tuotettua materiaalia, joten esimerkiksi uhkaava, sopimaton tai lainvastainen materiaali menee palveluun sellaisenaan. Käytännössä tämä tarkoittaa, ettei Facebook -palvelu vastaa mistään sinne tuotetusta materiaalista tai palveluista. Käyttöehtojen mukaan käyttäjä on itse vastuussa kaikesta siitä mitä palveluun tuottaa ja mitä toimintoja palvelussa käyttää. Riitatapauksissa, kuten palvelussa olevan materiaalin omistusoikeudesta tai itseään koskevan virheellisen tiedon oikaisemisessa, pyritään noudattamaan kyseisen maan lainsäädäntöä, mutta halutessaan Facebook -palvelu noudattaa emämaansa (USA) lainsäädäntöä. (Aalto & Uusisaari, 2009, s.43-44.)

Facebook myös muuttaa jatkuvasti omia käyttöehtojaan yksipuolisella ilmoituksella, ilman käyttäjien erillistä suostumusta. Käyttöehtojen muuttaminen on ollut usein Facebookiin kohdistuneen kritiikin kohteena. Facebook julkaisi uuden version käyttöehdoistaan helmikuussa 2009 ilmoittamatta asiasta käyttäjilleen erikseen. Facebook muutti käyttöehtoja siten, että palvelulla oli täysi oikeus kaikkeen käyttäjien tuottamaan sisältöön ja voisi halutessaan käyttää tätä materiaalia haluamallaan tavalla. (Aalto & Uusisaari, 2009, s.40.)

8.6 Tietojen julkisuus

Facebookin käytön perusajatus on, että kaikki palvelussa oleva ja sinne laitettu tieto on lähtökohtaisesti julkista. Tämän ajatuksen pohjalta kaikki käyttäjän itsestään kertomat tiedot ovat avoimesti kaikkien muiden käyttäjien nähtävissä. Käyttäjän yksityisyyden piirin kuuluvat asiat; arkinen elämä, ystäväpiiri tai arvot ja asenteet, ovat käyttäjälle itselleen täysin tuntemattomien tahojen luettavissa sekä arvioitavissa. Käyttäjän profiili ja sitä kautta saatu informaatio luo käyttäjästä tarvittaessa hyvin kattavan ja yksityiskohtaisen henkilökuvan. Yksityisyyden suojaamiseksi tulee käyttäjän harkita mitä tietoja haluaa itsestään näkyviin profiilissa ja keitä haluaa ystäviksi. (Haasio 2009, 71-72.)

Facebook kerää käyttäjästä tietoja. Tietoja kerätään lähinnä palvelun kehittämiseksi tai markkinoinnin kohdentamiseksi. Facebook kerää tietoja, joista osa on julkisia, kuten verkkosivustojen käyttötietoja (esim. käyttäjän IP-osoite). Facebook kerää myös käyttäjän Facebookissa julkaisemia henkilökohtaisia tietoja. Facebook ei rajoita käyttäjän tietojen keräämistä, tietoja saatetaan kerätä kaikesta verkossa olevasta digitaalisesta aineistosta. Tällaista tietoa löytyy verkkojulkaisuista, blogeista, pikaviestimistä, toisten tahojen ilmoittamasta informaatiosta, kuten sähköpostiosoitteistot tai Messenger-tunnukset. (Haasio 2009, 66.)

Facebook välittää keräämiään tietoja eteenpäin kolmansille tahoille, kuten mm. mainostajille. Tällaisia tietoja ovat esimerkiksi mielenkiinnon kohteet tai muu sellainen huomaamatta annettu tieto millä on kaupallista merkitystä. Facebookin näkemyksen mukaan tietojen keräämisessä tai niiden eteenpäin luovuttamisessa ei ole mitään arveluttavaa, koska tiedot auttavat mainostajia kohdentamaan mainontaa käyttäjälle. Tämä on käyttäjän edun mukaista, hänen saadessaan täsmällistä mainintaa häntä kiinnostavista tuotteista ja palveluista. Facebook käyttää tietoja oman toimintansa kehittämiseen ja kannustaa käyttäjiä jakamaan tietoaan mahdollisimman laajalti, eikä jakamiseen ole juridisia esteitä, koska käyttäjä on suostunut tietojen keräämisen ja jakamiseen hyväksyessään käyttöehdot rekisteröitymisen yhteydessä. (Haasio 2009, 66-67.)

Facebookin käyttö tuo ilmi käyttäjien mieltymyksiä niin palvelun tuottajalle, kuin muille tahoille. Mieltymysten avoin esiin tuominen voi mahdollisesti muodostua käyttäjälle epäedulliseksi tai muutoin arkaluontoiseksi. Omien statuspäivitysten kautta on mahdollista paljastaa käyttäjän mielihaluja. Uusissa sosiaalisissa medioissa on mahdollista paljastaa erilaisia normaalista poikkeavia taipumuksia ja erityisesti seksuaalisuuteen liittyviä taipumuksia. Näiden taipumusten paljastamiseen on myös luotu ohjelmia. Tätä on kokeiltu käytännössä MIT:ssä, missä opiskelijat kirjoittivat Gaydar - ohjelman. Tilastollisen analyysin keinoin se pystyi päättelemään homoseksuaalisuuden Facebook -kaveruuksista. (Järvinen 2010, 238.). Tämän ohjelman tekijät ovat tarkoituksellisesti luoneet analyysin ja luokittelun perustuen omiin näkemyksiinsä.

Facebookin sovellusten (applications) tehtävänä on tuoda interaktiivisuutta eri käyttäjien tai palvelun kesken. Nämä sovellukset ovat kuitenkin hyvin pinnallisia ja perustuvat usein identiteettileikkiin. Käyttäjä voi halutessaan tehdä testin, joka kuvastaa hänen ulkoista persoonansa esimerkiksi eläimen muodossa. Tavoitteena ei kuitenkaan ole aidon kuvauksen tekeminen ja testin tuloksen julkistaminen muille käyttäjille, vaan kyseessä on oman identiteetin kuvaus. Käyttäjä julkaisee testin tulokset, mikäli kuvaus on käyttäjälle itselleen suotuisia. Välitön ja avoin interaktiivisuus puuttuu ja sovelluksista valitaan ja tehdään sellaiset, joiden avulla muokattu kuvaus omasta itsestään halutaan näyttää muille. (Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S.2009. 262.)

Käyttäjän profiilissa olevat tiedot poistuvat jonkin ajan kuluessa siitä, kun profiili suljetaan. Tämä tarkoittaa sitä, että poistetut tiedot näkyvät Facebookin muille käyttäjille senkin jälkeen, kun tiedot on käyttäjän toimesta poistettu. Kaikki julkaistu materiaali on myös toisten kopioitavissa, ilman erillistä hyväksyntää käyttäjän taholta. (Haasio 2009, 66.)

8.7 Kehitys

Facebook palveluna on jatkuvan kehitystyön kohteena niin palveluntuottajan taholta, kuin sinne toimittavien sovellusten tekijöiden taholta. Tämä jatkuva kehitys aiheuttaa myös toimintatapojen- ja kulttuurin jatkuvan muutoksen sekä käyttöehtojen muuttumisen. Velvoite omien oikeuksien sekä yksityisyystietojen tarkastamisessa on käyttäjällä. (Haasio 2009, 63-64.) Jatkuva kehittyminen vaikuttaa käyttöehtojen kautta myös siihen, että tänään olevat ja pysyvästi yksityisiksi oletetut tiedot voivat tulevaisuudessa olla julkisia, riippuen palvelun ja sovellusten tuottajien omista tulkinnoista.

Järvinen (2010) näkee sosiaalisessa mediassa ja erityisesti Facebookissa olevan kolme erityistä uhkaa. Hänen mukaansa nämä ovat:

1. Tietojen oikeellisuus. Valtaosa Facebookin käyttäjistä esiintyy omilla nimillään sekä kertoo itsestään oikeita tietoja. Facebookin käyttölogiikka on, että mitä enemmän tietoa itsestäsi kerrot, sitä paremmin pysyt käyttämään palvelun ominaisuuksia. Yksityisyyden kannalta tiedon luovuttaminen muodostaa uhan käyttäjälle; hänet kyetään hyvin tarkasti tunnistamaan samoin hänen sosiaalinen verkostonsa. Osa Facebookin käyttäjistä haluaisi toimia muilta näkymättömissä, mutta todellisuudessa tietojen yhdistäminen sekä hakumootorien kehittyminen mahdollistavat käyttäjän henkilöllisyyden paljastamisen. (Järvinen 2010, 233.)
2. Tiedon leviäminen. Facebook, kuten kaikki muutkin ohjelmat Internetissä levittävät tehokkaasti sinne tuotettua tietoa. Tiedon leviämistä ei voi tehokkaasti estää. Luottamuk-

selliseksi tarkoitettu tieto voi levitä tahattomasti tai tahallisesti toisen osapuolen toiminnan johdosta. Ystäväketjujen varmistaminen on hyvin vaikeaa, käytännössä mahdotonta. Tällöin käyttäjä ei voi varmistautua kaikkien ystäviensä ja erityisesti näiden ystävien luottavuudesta ja omien henkilökohtaisten tietojen pysymisestä salattuina.

Facebookissa on paljon sellaisia sovelluksia eli lisäohjelmia, jotka toimivat alustoina tehokkaalle tiedonurkinnalle sekä tällaisen yksityisen tiedon leviämiselle. Nämä sovellukset ovat kenen tahansa tahon sinne laatimia ja tarkoituksena kerätä mm. henkilötietoja. Tiedot ovat vakimuotoisina ja helposti saatavilla sekä helposti levitettävissä eteenpäin. Facebook ei ota vastuuta näistä kolmannen osapuolen laatimista ohjelmista, jolloin vastuu jää käyttäjälle. Lisäohjelmat ovat kuitenkin keskeinen osa Facebookin viehätystä ja hauskuutta, mutta niiden käyttö monesti edellyttää antamaan pääsyn omiin yksityisyystietoihin. Käyttäjä ei voi millään varmistua ohjelmien turvallisuudesta.

Henkilö- ja muiden yksityisyystietojen vuotaminen voi tapahtua Facebookissa teknisen virheen tai palveluntuottajan tarkoituksellisen toiminnan johdosta. Facebook - palvelussa on havaittu ajoittain olevan sellaisia ohjelmointivirheitä, jotka ovat johtaneet käyttäjien yksityisyystietojen leviämiseen muille. Facebook on myös ajoittain tulkinnut käyttöehtojaan siten, että palveluntuottajalla on ollut täysi käyttöoikeus kaikkeen Facebookissa olevaan tietoon, myös käyttäjien henkilökohtaisiin tietoihin. Tietovuotoja voi sattua myös teknisten virheiden vuoksi. Esimerkiksi Facebookista on paljastunut useita ohjelmointivirheitä, joiden seurauksena yksityisiksi tarkoitettut kuvat ja tiedot ovat näkyneet kaikille. (Järvinen 2010, 234.)

3. Ystävät. Sosiaaliset verkostot ovat monin tavoin arvokasta tietoa. Verkostot kiinnostavat monia eri tahoja; mainostajat, tiedustelupalvelut, laittomat toimijat tai muuten uteliaat henkilöt. Ystävien kirjo vaihtelee suuresti käyttäjän omien tarpeiden mukaan. Erityisesti liike-elämässä voi käyttäjälle olla hyötyä suuresta ystäväjoukosta ja kuka tuntee kenenkin - tyyppisestä tiedosta. Verkostoa rakennettaessa useat käyttäjät ottavat ystävikseen myös satunnaisia tuttuja tai kokonaan tuntemattomia tahoja. Uhkana tällaisessa ystävien haalimisessa on, että verkostoon tulee sellaisia tuntemattomia tahoja, joiden motiivit ystävyystyö ovat käyttäjälle itselleen haitalliset. Pahimmillaan käyttäjä voi luulla ystävänsä aidoksi, mutta taustalla on valehenkilöllisyyden peitteellä toimiva haitallinen tai vihamielinen taho. Facebook ei varmistu käyttäjiensä henkilöllisyydestä, joten valehenkilöllisyyden luominen on mahdollista. (Järvinen 2010, 235.)

Haasio (2009) näkee tuntemattomien ystävien ottamien kavereiksi uhkana. Facebookin sosiaaliseen verkostoon voi hakeutua kuka tahansa, jos käyttäjä hyväksyy itselleen tuntemattomia henkilöitä ystävikseen. Tällainen taho voi saada tietoonsa hyvinkin arkaluontoisia tai henkilökohtaisia asioita, ja käyttää näitä tietoja omiin tarkoituksiinsa. Tuntematon taho voi olla

ystävän lisäksi tuntemattoman tahon laatima lisäohjelma, jonka tarkoituksena on kertätä mahdollisimman kattavasti käyttäjien yksityisyystietoja. (Haasio 2009, 70.)

Valehenkilöllisyydellä toimivan soluttautujan hyväksyminen ystäväkseen muodostaa välittömästi uhan käyttäjän yksityisyydelle. Soluttautuja voi myös hyväksikäyttää muodostettua sosiaalista yhteytetyttä saadakseen pääsyn kolmannen tahon kanssa tekemisiin. Tällaisessa toiminnassa tarkoituksena on käyttää ensimmäisen tahon luottamusta hyväksi ja vähentää todellisen kohteen epäluuloja. Tavoitteena ei olekaan saada tietoja alkuperäisestä kontaktista, vaan hyväksikäyttää tämän tahon sosiaalisia verkostoja. Soluttautujan tarkoituksiperät voivat olla mitkä tahansa, mutta joka tapauksessa vahingolliset. Taho voi olla kuka tahansa ja kohde kuka tahansa, niin henkilöt sekä yhteisöt. (Vahti 16.)

Suomalaiset ovat omaksuneet eri sosiaalisen median palvelut osaksi normaalia päivittäistä arkielämää. Erityisesti Facebook on tarjonnut suomalaisille jotain sellaista, mikä on saanut ison osan kansalaisista rekisteröitymään palvelun käyttäjiksi ja jakamaan tietoaan omasta yksityisyyselämästä. Helppokäyttöinen palvelu on saanut ihmiset jakamaan laajalti sellaista tietoa, joka vielä vähän aikaa sitten haluttiin pitää omanaan, eikä sitä haluttu jakaa laajalle ryhmälle ihmisiä. Facebookissa käyttäjät toimivat eri tavalla, kuin arkisessa elämässä. Kasvokkain toimiessa ihmiset eivät useinkaan avoimesti kerro itsestään yksityiskohtaisia tietoja tai avaa elinympäristöään muiden tarkasteltavaksi, mutta Facebookissa käyttäjät välittävät tällaisia tietoja, jotka voivat olla hyvinkin arkaluontoisia. Yksityisyyden ja avoimuuden raja on hämärtynyt. (Kari 2010)

9 Järjestelmällinen ja suunniteltu yksityisyystietojen kerääminen

Internetin käyttäjän tekemät toimet ovat kauppatavaraa. Internetin sivulla surffaava tai hakukoneelta tietoa hakevan mieltymykset ovat kaupallisesti hyödynnettävää tietoa. Miten tarkemmin kyetään näihin tarpeisiin kohdentamaan mainontaa, sitä tarpeellisemmaksi muodostuu tieto käyttäjien mielihausta sekä kiinnostuksen kohteista. Hakukoneet ja Internet - palvelut keräävät tietoa siitä, missä ja milloin hakeudut sivuille, mitä linkkejä tarkastelet ja mitä haet. Näistä kaikista muodostuu kokonaisuus käyttäjään kohdistettavan mainonnan sekä mielipiteensuuntaamisen mahdollistamiseksi. (Aalto & Uusisaari, 2009, s.105.)

Sosiaalisen median palvelun tuottajat toivovat, että käyttäjät kertovat itsestään mahdollisimman paljon mieltymyksiinsä koskevia yksityisyystietoja. Mahdollisuus saada käyttäjien yksityisyystietoja on perustana useiden sosiaalisen median palvelun liiketoimintamallille ja käyttäjiä kannustetaan avoimuuden nimissä julkaisemaan tietoaan mahdollisimman avoimesti. Palvelun tuottajalle käyttäjän yksityisyyden menettäminen on suotavaa liiketaloudellisten etuuksien saavuttamisessa, mutta palvelun käyttäjän kohdalla uhka yksityisyyden menettämisestä kasvaa, sitä mukaa, kun käyttäjä luovuttaa itsestään tietoja. Ilmiönä sosiaalinen media

on vielä hyvin nuori, eikä kaikkia ilmiön aiheuttamia mahdollisia uhkia yksityisyydelle ole vielä kyetty näkemään. (VAHTI, 21.)

Demokraattisessa vapaassa oikeusvaltiossa käyttäjän yksityisyystietojen vuotamisella ei välttämättä ole henkilölle itselleen kovinkaan suurta merkitystä. Ilmaiset sosiaalisen median palvelut kuten Facebook mahdollistaa suurten yksityisyystietomäärien systemaattisen keräämisen ja näiden tietojen käyttämisen esimerkiksi kohdennettuun markkinointiin. Tietoja käyttäjien mieltymyksistä sekä mielipiteistä voidaan kerätä myös erilaisille valvonta- ja kontrolliviranomaisille näiden etsiessä vaarallisiksi arvioituja henkilöitä tai ryhmiä.

9.1 Tietojen louhinta ja yhdistäminen

Tietojen suojaaminen ja verkon turvallisuus on aina ajankohtainen tarkastelun asiakokonaisuus, joka koskettaa kaikkea verkon kautta tapahtuvaa toimintaa sekä hallussa olevien tietojen suojaamista. Oli sitten kysymys kaupankäynnistä, kansallisesta tai yksityisestä turvallisuudesta, niin ensisijaisesti on huolehdittava toimintaan ja tietoihin liittyvästä turvallisuudesta. Turvallisuus on kokonaisuus, jossa tulee tarkastella sekä käytettävien yksittäisten tietojen turvallisuutta että näistä yksittäisistä tiedoista koostuvan kokonaisuuden aiheuttamaa uhkaa yhteisön tai yksityisen henkilön tietosuojaa kohtaan. Monet yksittäiset tiedot tai asiat eivät sinänsä ole salaisia, kuten henkilön nimi, osoite tai yhteystiedot. Uhka tietosuojalle saattaa muodostua erilaisten yksittäisten tietojen yhdistämisen kautta saadusta kokonaisuudesta lisätynä muualta saatavalla lisäinformaatiolta, kuten blogikertomuksilla tai toisten tahojen tuottamalla informaatiolla. (Järvinen 2002, 30.)

Valtaosa kaikesta informaatiosta liikkuu digitaalisesti sähköisessä muodossa, ja on sellaisessa muodossa, että sitä on suhteellisen helppo saada ja se on helposti yhdistettävissä ja muokattavissa. Tiedon liikkumisen valvonta on helpottunut suuresti ja haluttu informaatio kyetään mahdollisuuksien ja tarpeen mukaan löytämään helposti. Toisaalta kontrolli siitä, kuka tietoa saa käsitellä ja millaista tietoa yhteisö ja yksityiset tahot sähköisesti tuottavat, on heikentynyt. Viranomaisten resurssit eivät riitä verkkoon tuotetun informaation valvomiseen. Myös yksityisten henkilöiden kyky havaita hänestä kertyvän haitallisen informaation kertymisestä on heikko. Aikaisemmin massiivisten tietojen kerääminen ja analysointi vaati huippuosaamista sekä suuria keskustietokoneita, joihin vain tiettyjen maiden turvallisuusviranomaisilla oli mahdollisuus. Nykyisin ihmisten tuottamat digitaaliseen muotoon tuotettu informaation kerääminen ja analysointi on mahdollista hyvin paljon laajemmalle joukolle erilaisia toimijoita, jopa yksityisille henkilöille.

9.2 Tiedustelupalvelut

Eräiden maiden, kuten USA, tiedustelupalvelut ovat vahvasti mukana verkkomaailmassa. Tiedusteluyhteisöt keräävät ja hankkivat tietoa verkosta omiin tarkoituksiinsa. Tiedustelupalvelut myös omistava sekä hankkivat omistukseensa tiedustelutarpeisiinsa sopivia teknologiayhtiöitä. Järvinen (2010 219-220.) mainitsee tästä esimerkkinä vuonna 1999 perustetun In-Q-Tel riskisijoitusyhtiön. Kyseinen yhtiö on USA:n keskustiedusteluvirasto CIA:n omistama yhtiö, joka tavoitteena on hankkia omistukseensa sellaisia teknologiayrityksiä, joiden kautta CIA saa itselleen tarpeellista tietoa tai taitoa. Järvisen mukaan tiedusteluyhteisö on kiinnostunut erilaisista tietokannoista, tietolouhinnasta, hiljaisen tiedon keräämisestä sekä kaikenlaisen erimuotoisen tiedon analysoinnista sekä visualisoinnista. Näiden lisäksi tiedustelutoiminnassa on hyötyä kasvojentunnistusohjelmista sekä tietoturvaohjelmistoista. (Järvinen 2010, 219-220.)

CIA on mukana Facebookissa In-Q-Tel yhtiön rahoitusjärjestelyjen kautta. Vuonna 2008 Guardian lehti julkaisi artikkelissaan, että Facebookia rahoittavien yhtiöiden hallituksissa on samoja tahoja kuin In-Q-Tel -yhtiössä. (Järvinen 2010, 219-220.)

Läntiset tiedustelupalvelut ovat kehittäneet sähköisen informaation tiedonkeruujärjestelmän. Echelon on sähköisen viestinnän kuuntelemiseen ja tallentamiseen kehitetty järjestelmä. Echelon kerää tietoja kaikesta sähköisestä viestinnästä (puhelut, faksit tai verkko). Echelon on alun perin kehitetty sotilastiedustelun tarpeisiin ja siinä ovat mukana USA, Englanti, Uusi-Seelanti ja Kanada. Kuuntelujärjestelmä rakentuu eri puolille maapalloa sijoitetusta jättimäisistä kuunteluasemista, joiden kautta saatu informaatio tallentuu supertietokoneiden muistiin. Tämä tallentunut tieto on analysoitavissa eri menetelmiä käyttäen sellaiseen muotoon, että sitä pystytään käyttämään hyödyksi. Tiedon hyödynnettävyys riippuu tiedon vastaanottajan tarpeista ja tavoitteista. Echelon -järjestelmän kautta pysytään tekemään kohdennettu tiedustelua mihin tahansa haluttuun kohteeseen. Puhtaan sotilastiedustelun tarpeet ovat siirtyneet taka-alelle ja tilalle on noussut uusia tiedustelun tarpeita. Kylmän sodan jälkeen mm. USA on kohdentanut tiedusteluaan sotilaskohteesta USA:n teollisuuden kanssa kilpaileviin maihin sekä yrityksiin. USA:n poliittisten etujen kanssa ristiriidassa olevista tahosta pyritään myös saamaan tietoa Echelon -järjestelmän avulla. Tällaisia kohteita ovat mm. erilaiset riippumattomat kansalaisjärjestöt sekä näissä järjestöissä toimivat henkilöt. (Järvinen 2002, 141-42.)

Echelonin lisäksi monilla muilla mailla on omia kansallisia kuuntelujärjestelmiä, joiden kautta kerätään ja analysoidaan informaatiota. Järjestelmät ovat usein kansallisen lainsäädännön ulottumattomissa ja tietojen kerääminen tapahtuu muualla kuin käyttäjän kotimaassa. (Järvinen 2002, 43.)

9.3 Yritykset

Lainsäädäntö tietosuojan osalta vaihtelee merkittävästi eri puolilla maailmaa ja myös Euroopan sisällä. Amerikkalaisen lainsäädännön mukaan yrityksen hankkimat tiedot ovat kyseisen yhtiön omaisuutta ja yhtiöllä on täysi käyttöoikeus tietoihin haluamallaan tavalla. Ihmisten yksityisiä tietoja, kuten varallisuus- tai terveystietoja voidaan ostaa ja myydä normaalin kaupankäynnin sääntöjen mukaan. Yksi suurimmista tietokantayhtiöistä Amerikassa on ChoicePoint. Yhtiö on kasvattanut tietokantojaan vuosia jatkuneiden yritysostojen kautta ja hallitsee noin 20 miljardia erilaista tietuetta yksityisten henkilöiden yksityisyyteen liittyvistä asioista. ChoicePoint kerää ja analysoi tietoja asiakkaiden tarpeiden mukaan. Tavanomaisten yhtiöiden lisäksi ChoicePoint myy tietoja amerikkalaisille viranomaisille, kuten poliisille sekä tiedustelupalveluille. Järjestely mahdollistaa viranomaisen saada haltuunsa sellaista tietoa, jonka hankkiminen muutoin olisi lainsäädännöllisesti kielletty viranomaisen oman suoran toiminnan kautta. (Järvinen 2010, 268-272.)

Tiedonhakupalveluita on saatavilla verkosta, eri toimijoiden taholta. Yksityishenkilöstä voi tilauksesta saada ammatillisesti kerätyn ja analysoidun yhteenvedon kohteena olevan henkilön virtuaalisista tiedoista. Näiden tietojen kautta tilaajalle muodostuu hyvin kattava käsitys kohteen yksityiselämästä, henkilötiedoista, ihmissuhteista, asenteista, taloudellisesta tilanteesta ym. yksityisyyden piiriin kuuluvista asioista. (Järvinen 2010, 268-272.)

9.4 Muut tahot

Internetistä haetaan nykyisin tietoa kaikkein tahojen toimesta. Arkikielen termi tälle on ”googlettaminen”. Tietojen hakijan motiivit vaihtelevat suuresti sen mukaan, mihin tietoja tarvitaan; uteliaisuuttaan tietoja hakeva naapuri tai tuttu, tai yhteystietoja hakeva vanha koulu- tai armeijakaveri. Useille Internetin käyttäjälle on tullut vakiintuneeksi toiminnaksi hakea tietoja kaikista kohtaamistaan ihmisistä, sama koskee myös yhteisöjä. Uudesta tuttavuudesta tehdään kysely netin eri palveluihin, joiden kautta henkilöstä tai tahosta muodostetaan ”sähköinen ensivaikutelma”. Viime vuosina on keskusteltu kiivaasti siitä, saako työnantaja tutkia työntekijän taustoja hakukoneilla. Laki yksityisyyden suojasta työelämässä määrää, että työnantajan on kerättävä työntekijää koskevat henkilötiedot ensi sijassa työntekijältä itseltään, työntekijän on annettava suostumus tietojen keräämiseen. Tietosuojavaltuutettu Reijo Aarnio on linjannut, että laki koskee myös hakukoneita. Arkijärki kyseenalaistaa linjauksen; jos netissä oleva tieto on kaikkien julkisesti saatavilla, miksi se ei ole sitä myös työnantajalle? Kuitenkaan ei ole kysymys vain siitä, mitä keinoja rekrytoija saa käyttää hakijoiden taustojen selvittämiseksi, vaan myös siitä, mitkä asiat ylipäätään kuuluvat työnantajalle. (Aalto & Uusisaari, 2009, s.125.)

10 Rikollinen tai vihamielinen toiminta

Luovuttaessa itseäsi koskevia henkilökohtaisia asioita tai hoitaessa raha-asioita, on varmistuttava, että toimintaympäristö on turvallinen ja vastapuoli itselleen tuttu ja luotettava. Suurin osa sosiaalisista palveluista, ei vaadi henkilöllisyyden varmentamista ja niissä voi toimia valehenkilöllisyydellä. Useissa sosiaalisen median palveluissa on mahdollista rekisteröityä kenen nimellä tahansa ja antaa profiiliinsa haluamansa tiedot. Itseään koskevat epämääräiset utelut tai tuntemattomien henkilöiden kaveripyynnöt voivat olla harmittomia, mutta näihin myös liittyy se uhka siitä että vastapuolen motiivit ovat epärehelliset. (Aalto & Uusisaari, 2009, s.26.)

10.1 Rikos yksityiselämää loukkaavan tiedon levittäminen

Rikoslain 24.luvun 8.pykälä suojaa ihmisen yksityiselämää. Laki kieltää levittämästä henkilön yksityiselämää liittyviä tietoja tai kuvia, jos ne aiheuttavat vahinkoa, kärsimystä tai halveksuntaa kohteelle.

Levittämisen kieltö ei koske yksityistä henkilöä hänen levittäessään yksityiselämään koskevia tietoja toisille kasvokkain tai puhelimitse. Yksityiselämään koskevia tietoja ei yksityinen henkilö saa levittää julkisesti missään muodossa. esimerkiksi verkossa. Tällaisen tiedon levittäminen, esimerkiksi julkisesti verkossa, on rikos. (Järvinen 2010, 213.)

Kunnianloukkaus muuttuu törkeäksi, jos sen tekemisessä käytetään apuna joukkotiedotusvälinettä, loukkaava tieto saatetaan muilla keinoin lukuisten ihmisten saataville tai jos loukkaus on pitkäkestoinen ja aiheuttaa uhrille huomattavaa haittaa. (Rikoslaki.)

Kunnianloukkauksessa tarkasteluun tulee myös solvauksen kohde. Julkisuuden henkilöltä tai julkista tehtävää hoitavalta edellytetään yksityistä henkilöä korkeampaa sietokykyä. Julkisuuksessa olevan henkilön kohdalla kunnianloukkaus täyttää rikoksen tunnusmerkistön silloin, mikäli teko ylittää yleisesti hyväksyttävänä pidetyn kynnyksen. Julkista tehtävää hoitavan henkilön arvostelu on sallittua, mikäli arvostelussa pysytään normaalilla tasolla. Esimerkiksi pääministerin kyvykkyyden arvostelu ei täytä rikoksen tunnusmerkistöä. Julkisen henkilön kunnianloukkausrikoksessa on oltava kyse tavallista mielipidettä voimakkaammasta perättömästä väitteestä tai syytöksestä, jotta tekoa voidaan käsitellä kunnianloukkausrikoksena. Rikoksen tunnusmerkistön täytyessä, ei vastaanottavan yleisön lukumäärällä ole merkitystä rangaistavuutta arvioitaessa. (Järvinen 2010, 212.)

10.2 Henkilöllisyysvarkaudet

Henkilöllisyysvarkaudessa toisen henkilön henkilötiedot otetaan luvatta käyttöön. Henkilöllisyyttä käytetään hyväksi, tavoitteena saada jotain hyötyä, kuten taloudellista. Henkilöllisyysvarkaudessa tai yleiskielen ilmauksessa identiteettivarkaudessa, tarkoitetaan laajaa tietojenkeruuta, jossa kohteena ovat yksilön yksityistiedot. Henkilöllisyysvarkauteen tarvittavia tietoja kerätään laajasti useista eri lähteistä. Näistä yleisimmät ovat sähköisesti kerättävät yksityisyystiedot, joita saadaan erilaisten verkon vakoilu- tai haittaohjelmien kautta. Tietoja voidaan myös hankkia räätälöidysti tietyiltä käyttäjäryhmiltä, heille suunnatuilla tietojen klasteluviesteillä. Myös sähköisen hankinnan ohella voidaan käyttää fyysistä tietojen urkintaa, kuten paperisten asiakirjojen hankintaa. (Kari 2010)

Internetin sosiaalisiin palveluihin on tarkoituksellisesti luotu harhauttavia sivustoja sekä informaatiovälittäjiä. Näillä sivustoilla yhteisöjen tai yksilöiden toimintaa jäljitellään tarkoituksena harhauttaa sivustolle tai profiilille hakeutunutta tahoja. Osa näistä harhautuksista on tehty pilan päiten eikä tavoitteena ole taloudellisen edun tai suuren haitan aiheuttamien. Toisaalta tällaisten harhauttavien sivujen tai valeprofiileiden kautta pyritään myös saamaan hyötyä rikollisessa mielessä, kuten erilaisissa talousrikoksissa tarvittavia yksityisyystietoja. Vahingot saattavat nousta suuriksi, jos väärennetyn profiilin luoja onnistuu tehtävässään ja kykenee keräämään tarpeellisesti tietoa haluamastaan yhteisöstä tai henkilöstä. (Vahti 15.)

Harhautusta voidaan käyttää myös käänteisesti, jolloin virheellistä informaatiota tuottava taho pyrkii tuottamaan itselleen edullista informaatiota. Sosiaalisessa mediassa ei voi varmistua informaation oikeellisuudesta.

Suomessa henkilöllisyysvarkauksien määrä on vähäinen, koska Suomessa henkilön yksilölliset tiedot kuten sosiaaliturvatunnus, on yleisesti hyvin salattu ja sitä ei helposti jaeta toisten tietoon. Myös tunnustautumiskäytännöt esim. pankkiasioita hoidettaessa, ovat hyvin vahvat ja määrämuotoiset. Internetin käytön lisääntyminen ja arkisten asioiden hoitaminen verkon kautta on lisännyt väärinkäytösten määrää sekä mahdollisuuksia toisten henkilöllisyyksien väärinkäyttämiseen. Erilaiset verkkopalvelut sekä uudet tavat toimia eri verkkomedioiden kautta ovat mahdollistaneet paremman keinon kuin aiemmin hankkia yksityisiä tunnistetietoja. Tietoa kohteesta voidaan kerätä useiden eri verkkokanavien kautta (sähköposti, omat ilmoitetut tiedot mm. profiilissa). Koska tietoa on useissa paikoissa, on käyttäjän vaikea kontrolloida itseään koskevaa tietoa. Pitkältä ajalta ja useiden medioiden kautta kertyvä tietomassa voidaan väärinkäyttää luomalla valehenkilöllisyys toisen ihmisen tietojen pohjalta. Tätä henkilöllisyyttä voidaan käyttää moneen eri tarkoitukseen, riippuen tavoitteesta. Kerran vuotaneet henkilö- ja pankkitiedot leviävät verkossa ja niiden valtaaminen takaisin on hyvin vaikeaa. Verkon kautta saatavien tunnistetietojen kerääminen on suuressa kasvussa, koska toiminnan kautta saatava rikollinen hyöty on suuri. Kansanvälinen järjestäytynyt rikollisuus on osa verkon arkipäivää. (Järvinen 2002, 188-189.)

Suomessa tapahtuvista identiteettivarkauksista ei ole tällä hetkellä olemassa kattavaa tilastoa. Suurin syy tähän on, että poliisin tilastoinnin perusteena on rikosnimike. Identiteettivarkauksille ei rikoslaissa ole olemassa omaa erillistä rikosnimikettä ja tästä seuraa, että kyseisiin tapauksiin liittyvät tapahtumat tulee etsiä käsin koko poliisin ilmoitusmassasta. Identiteetin varastaminen voi rikoslain tulkinnan mukaan ilmetä useina eri rikoksina, kuten petoksina tai erilaisina kunnianloukkauksina. (Kari 2010.)

10.3 Teollisuusvakoilu

Teollisuusvakoilussa pyritään saamaan yrityksen salassa pitämiä tietoja yrityksen ulkopuolisen tahon käyttöön ja hyödynnettäväksi. Teollisuusvakoilussa voidaan mahdollistaa tietomurron avulla. Tietomurto tapahtuu joko suoraan teknisin menetelmin tai hyväksi käyttämällä jotain yrityksen työntekijään joka mahdollistaa pääsyn haluttuun tietoon. Teollisuusvakoilu on päämäärätietoista ja ammattimaista toimintaa ja sen suorittajat ovat tiedustelun sekä tiedonhankinnan ammattilaisia. Tiedustelu skaalautuu laajalti ja tiedustelu ulotetaan hyvin laajalle niin menetelmien kuin tiedustelun kohteiden osalta. Teollisuusvakoilu on rikollista toimintaa ja siinä käytetään menetelmiä verkon tunkeutumiseen, salasanojen hankkimiseen sekä vaikuttamista henkilöihin, jotka voivat mahdollistaa pääsyn haluttuun tuotekehitys- tai kilpailutietoon. (Järvinen 2002, 297.)

Sosiaalisen median palveluja käyttävät yhä useammat henkilöt niin vapaa-ajallaan, kuin myös työtehtäviinsä liittyen. Lisääntynyt sosiaalisen median käyttö voi aiheuttaa vakavan uhan käyttäjälle itselleen ja myös hänen edustamansa organisaation turvallisuudelle. Yksityisyystietojen sekä organisaation salassa pidettävien tietojen kalastelu on noussut suureksi ongelmaksi verkon sosiaalisten palveluiden käyttäjille. Kalastelun kohteena olevaa huijataan tai harhautetaan eri menetelmillä, tarkoituksena saada kohde paljastaan itsestään tai organisaatiostaan luottamuksellisia tietoja. Menetelmät vaihtelevat suuresti, kalastelu-viesti voi olla naamioitu lomakkeeksi tehdyksi kyselyksi, harmittomaksi sähköpostiviestiksi tai valehenkilöllisyyden avulla tehdyksi suoraksi lähestymiseksi. Verkon sosiaaliset palvelut tarjoavat oivallisen väylän tämän tyyppisten harmittomilta vaikuttavien lähestymisten toteuttamiseen. Ihmiset on usein koulutettu välttämään ja torjumaan mm. roskaposteja tai rahanhuijaus - kirjeitä. Sosiaalisessa mediassa ollaan kuitenkin varomattomia ja hyväuskoisia, koska palvelun toimintaidea on olla mahdollisimman avoin kaikkia käyttäjiä kohtaan. Käyttäjä voi ladata itselleen kenen tahansa välittämän lisäosan tai palvelun tarkastamatta laatijan luotettavuutta. Facebook -kyselyyn vastataan varmistumatta, että kyselyn tarkoituksena on jotain muuta, kun mihin kyselyssä viitataan. Osa sosiaalisen median palveluista on laadittu nimenomaan keräämään tietoja käyttäjistä. Tästä esimerkkinä on 2010 keväällä tapahtunut Facebook -huijaus, jossa käyttäjälle luvattiin tuhannen euron lahja IKEA:n tavarataloon. Käyttäjän tuli voittaakseen lahjakor-

tin liittyä IKEA.com -sivustolle. Sivuston tarkoituksena oli kalastella suuri määrä käyttäjien henkilötietoja. (Vahti 15.)

Sosiaalisen median eri käyttötavat ovat muodostavat käyttäjille uhan joutua yritysvakoilun kohteeksi tai jonkun valtiollisen tiedusteluelimen tiedonhankinnan kohteeksi. Yksittäisen tiedon joutumien urkinnan kohteeksi, ei muodosta varsinaista uhkaa sinänsä, vaan uhka muodostuu erityisesti silloin, kun tietoa on paljon ja sitä voidaan helposti yhdistellä toisiinsa. Luottamusaseman hyväksikäyttö, kuten ystävänä kontaktin luominen, edesauttaa itselleen tai edustamalleen organisaatiolle epäedullisen tiedon vuotamisen. Varsinkin suomalaiset hyväksyvät ystävikseen helposti sellaisiakin tahoja, joiden taustoista käyttäjällä on varsin vähän tietoa, jopa entuudestaan tuntemattomia tahoja. Käyttäjä voi siis huolimattomuuttaan tai taitamattomuuttaan aiheuttaa merkittävän tietoturvuhan luottamalla liikaa kohtaamiinsa tahoihin sosiaalisessa mediassa. (Vahti 16.)

10.4 Social engineering

Social engineering on psykologinen vaikuttamisen menetelmä, jossa tavoitteena on saada kohteena oleva henkilö toiminaan halutulla tavalla ja toteuttamaan menetelmän käyttäjän tavoitteita. Yrityssalaisuuksien tai ominen henkilökohtaisten salaisuuksien tarkoituksenmukaisessa urkinnassa, social engineering -menetelmällä vaikutetaan kohteen käyttäytymiseen siten, että tämä harkitsematomasti tulee paljastaneeksi sellaisia tietoja, joiden avulla päästään käsiksi haluttuun tietoon. Tämä tieto voi olla mitä tahansa, kuten salasanoja, suojauksen heikkoja kohtia tai omia mieltymyksiä. Merkitystä on sillä, että tietoja hankintaan tarkoituksena käyttää tietoja hyväksi ja tiedot saadaan muokkaamalla kohtaan käytöstä. Kohteeseen voidaan esim. Facebookin kautta vaikuttaa esiintymällä kaverina ja luomalla normaalilta vaikuttava ystävyysuhde, mutta todellisuudessa on käytetty valehenkilöllisyyttä ja kaverisuhteen luomisen tarkoituksena on saada pääsy tietoon, johon ei muuten olisi mahdollisuutta päästä. (Järvinen 2002, 307-308.)

Sosiaalisen median perustoimintaideologia on keskenään toisilleen tuttujen ihmisten välinen kanssakäyminen, jossa he vaihtavat keskenään henkilökohtaista informaatiota. Tämä vaihtaminen voi olla periaatteessa mitä tahansa; ajatuksia, tietovaihtoa, kuvia tai videotiedostoja. Uusimmat sosiaalisen median palvelut, kuten Facebook, mahdollistavat välittömän ja reaaliaikaisen tiedonvaihdon hyvin suurelle määrälle ihmisiä. Palvelun tarjoaja kannustaa käyttäjiään nopeaan tiedonvaihtoon hyötyäkseen tästä taloudellisesti, saamalla esimerkiksi sellaista käyttäjiin liittyvää informaatiota, jota voidaan välittää kolmannelle osapuolelle, kuten mainostajalle. Tietosuojan korostaminen ei näin ollen ole yhteisöpalvelun tuottajan näkökulmasta kannattavaa, vaan päinvastoin, mitä enemmän yksityisyystietoja saadaan, sitä tarkemmin henkilöön voidaan kohdistaa erilaisten lisäpalveluiden markkinointia. (Järvinen 2010, 233.)

10.5 Viattomien tietojen hakkerointi

Viattomien tietojen hankinnassa tavoitteena on saada suora tietoa halutusta kohteesta, kuten tuotekehitystietoja. Epäsuorassa tiedonhankinnassa viattomia tietoja käytetään tavoitteena saada pääsy haluttuun kohteeseen. Tällöin tiedonhankinnan kohteena ovat sellaiset tiedot, jotka paljastavat mahdolliset salasana- tai tiedonsuojauksen heikot kohdat. Käyttäjän itselle viattomien tietojen suojaamisessa ei lähtökohtaisesti ole perusteita, koska käyttäjä kokee näiden tietojen olevan sellaisia, ettei niitä voi käyttää hyväksi ja täten myös salaamisen taso on alhainen. Viattomia tietoja voivat olla mm. työpaikka, sähköpostiosoite, puhelinnumero ym. jo normaalisti julkiset tiedot. Merkitystä on sillä seikalla, kuinka paljon yksilöivää tietoa käyttäjä itsestään antaa. Julkisten tietojen lisäksi kohteesta voidaan kerätä yksityiskohtaista sekä luottamuksellista tietoa. Tämä tieto voi kertyä pitkältä ajalta ja useiden eri medioiden kautta. Mikäli tiedonhankinnassa käytetään esimerkiksi Facebook -ystäväksi solutautunutta tiedonhankkijaa, voidaan kohteesta laatia hyvin yksityiskohtainen profiili. Tätä profiilia on mahdollisuus hyväksikäyttää ilman kohteen tietoa asiasta ja esiintyä uskottavasti muille tahoille. (Thomas, T. 2004, 4-6.)

11 Haastattelut

Haastateltavien valinta oli jo tutkimuksen alunvaiheessa määritelty, että haastateltaviksi valitaan tietoturvallisuuden asiantuntijatehtävissä toimivia henkilöitä. Tutkimuksen avoimen teemahaastatteluun valikoitiin kaksi asiantuntijatehtävissä toimivaa tahoja, jotka ovat oman virkatoimintansa kautta perehtyneet sosiaalisen median uhkiin. Henkilöt valikoituvat haastattelun kohteeksi, koska heillä on asiantuntijuus aiheeseen liittyen ja koska he joutuvat virkatoimensa kautta jatkuvasti tekemisiin aiheen eri teemojen kanssa.

Toisena haastatteluteemana oli tutkia sosiaalisen median käyttäjien näkökulmaa aiheeseen. Tässä tarkastelussa erityisesti Facebook oli mielenkiinnon kohteena. Käyttäjien haastatteluisa keskityttiin heidän käyttötottumuksiin, havaittuihin ongelmiin sekä heidän näkemyksiin mahdollisiin uhkiin liittyen yksityisyyteen. Nämä haastateltavat valikoituivat omasta lähipiiristäni heidän ennakkoon minulle kertoman Facebookin käytön pohjalta.

Haastattelut suoritettiin eri aikoina. Ensimmäinen asiantuntijahaastattelu tehtiin lokakuussa 2010 ja toinen huhtikuussa 2011. Käyttäjahaastattelut tehtiin lokakuussa 2011. Ajallinen pituus ja sen vaikutus tutkimuksen luotettavuuteen hallittiin haastattelurunkojen avulla, jotka olivat samanlaiset asiantuntijoiden kesken ja käyttäjien kesken. Haastattelut olivat jokainen kahdenkeskeisiä kasvokkain tehtyjä tapaamisia. Haastattelun sisältö tallennettiin paikan päällä kirjaamalla se paperille. Käyttäjahaastattelujen aikana havaittiin, että asiantuntijoilta ei

tultu kysyttäneeksi niistä sosiaalisen median palveluista, joita he mahdollisesti käyttävät. Tämä ei kuitenkaan vaikuttanut asiallisten tutkimuksen kautta johdettavien johtopäätösten luotettavuuden heikkenemiseen, koska asiantuntijoilta kysyttiin tutkimuksen kannalta oleellisia asioita. Mielenkiintoista olisi kuitenkin ollut tietää, käyttävätkö asiantuntijat sosiaalisen median palveluita, ja jos käyttävät, niin mitä palveluita ja miten he hallitsevat uhat.

11.1 Asiantuntijahaastattelut

Ensimmäisen asiantuntijahaastattelu tehtiin lokakuussa 2010 avoimen teemahaastattelun pohjalta. Haastateltava työskentelee Suojelupoliisin DSA -toiminnossa, jossa hänen vastuullaan on yritysten ja yhteisöjen turvallisuuden auditointi. Haastateltava on sekä nykyisen työnsä että aikaisempien työtehtävien kautta perehtynyt tietoturvalisäsuuteen yksilö- ja yhteisötasoilla. Tämän lisäksi haastateltava on perehtynyt erilaisiin median kautta suoritettaviin vaikuttamisen keinoihin.

Haastattelussa käsiteltiin sosiaalista mediaa, Facebookia erityisesti sekä ihmisten käyttäytymistä näissä medioissa. Keskustelussa pyrittiin tuomaan esiin keskeisiä uhkia yksityisyydelle. Haastateltavan näkemyksen mukaan uhkia on palvelujen tietosuojassa, käyttäjien omassa tiedostomattomassa toiminnassa sekä ulkopuolisen tahon tarkoituksellisessa tiedonhankinnassa ja manipuloinnissa.

Palvelujen tietoturvalisuus on tasoltaan heikko, eikä palvelun tarjoajalla ole suurta intressiä parantaa asiantilaa. Tämä johtaa siihen, että käyttäjien tiedot voivat milloin tahansa levitä kenen tahansa käyttöön. Palvelujen ilmoittamat tietoturvaparannukset tehdään yleensä vastasitten, kun vahinko on tapahtunut tai kun suuri yleisö sitä vaatii. Yksittäisen käyttäjän vaikutusmahdollisuuden ovat käytännössä olemattomat.

Käyttäjien oma toiminta on keskeisin uhka kaikelle tietoturvalisuudelle. Facebookin kaltaiset palvelut perustuvat jatkuvaan ja välittömään sisällön tuottamiseen niin työssä kuin kotona. Tämä voi aiheuttaa yksityisen ja julkisen tiedon hämärtyksen. Rajan hämärtyessä käyttäjä ei ole enää tietoinen mitä ja milloin voi jakaa avoimesti verkossa. Omien asioiden lisäksi voi helpostikin tulla paljastaneeksi muiden yksityisiä tietoja niin sosiaalisen verkostonsa kuin työnantajansa tietoja. Pahimmillaan tietovuoto voi vaarantaa käyttäjän tai toisen henkilön turvallisuuden, esimerkiksi salassa pidettävää operaatiota suorittavien sotilaiden tai näiden läheisten turvallisuuden. Sosiaalinen media ja sen käyttö on luonut illuusion, että kaikesta pitää kertoa välittömästi, muutoin käyttäjä ei ole sosiaalinen vaan ulkopuolinen.

Sosiaalisen median palvelut ovat monille käyttäjille väylä oman egonsa korostamiseen. Tätä turhamaisuuden piirrettä pyritään palvelujen tuottajien puolelta ruokkimaan, jotta käyttäjät pitäisivät asiansa mahdollisimman avoinna ja kerryttäisivät palvelun tuottajan tietomassaa. Monet tahot ovat kiinnostuneita ihmisten käyttäytymisestä ja mahdollisuudesta vaikuttaa massojen käyttäytymiseen. Sosiaalinen media on jo osoittanut voimansa useissa eri tilanteissa, miten se toimii erinomaisena väylänä erilaiselle mielipiteen vaikuttamiselle sekä käyttäytymisen muuttamiselle. Tämä ei pelkästään rajoitu kaupalliseen toimintaan, vaan myös eri valtiolliset turvallisuustahot pyrkivät ainakin tulevaisuudessa muokkaamaan massojen käyttäytymistä sosiaalisen median keinoin.

Välineet ovat olemassa ja suuret massat on opetettu niitä käyttämään, eli mitään ei puutu suunniteltujen informaatio-operaatioiden suorittamiseksi. Mielipiteen ja käyttäytymisen muuttamisen pohjalle tarvitaan tietoa ihmisten vaikuttamisen menetelmistä sekä mielihalusta. Tätä tietoa kerääntyy jatkuvasti ja kiihtyvällä vauhdilla. Tällaista avointa tietomateriaalia saadaan valtavasti eri sosiaalisen medioiden palvelujen kautta ja näiden tietojen pohjalta myös suunnitellaan kohdennettua tiedonkeruuta joistain tietystä ihmisestä, ihmisryhmistä tai yhteisöistä.

Toinen asiantuntijahaastattelu tehtiin huhtikuussa 2011. Haastateltava toimii Suojelupoliisissa järjestelmäasiantuntijana ja käy luennoimassa tietoturvallisuudesta sekä sosiaalisen median uhista. Haastateltavan mukaan sosiaalisen median ja erityisesti Facebookin keskeisiä uhkia löytyy palvelun tuottajan taholta, käyttäjien toimesta, USA:n turvallisuusviranomaisten taholta sekä Facebookin lisäsovellusten tekijöiden toimesta.

Haastattelussa keskityttiin pelkästään Facebookiin. Haastateltavan näkemyksen mukaan kyseessä on yksityinen, ulkomaalainen toimija, joka on täysin arvaamaton. Facebook on käyttöönsä historiansa aikana tehnyt useita laajoja ja vakavia yksipuolisia muutoksia palvelunsa käyttöehtoihin. Nämä muutokset ovat lähes aina vaarantaneet käyttäjien tietoturvallisuutta. Facebook voi halutessaan tehdä käyttäjien tiedoille mitä tahansa se haluaa, koska palveluun kohdistetaan USA:n lainsäädäntöä, missä muun muassa yksityisyyden suoja on täysin erilainen kuin Euroopassa. Rekisteröityessään palveluun käyttäjä on täysin palvelun tuottajan armoilla. Haastateltava totesi: ”minä en luottaisi siihen pätkän vertaa”.

Facebook sekä sen käyttäjät; yritykset, yhteisöt ja yksilöt ovat onnistuneet kehittämään maailmanlaajuisen ilmiön, jonka kautta on syntynyt sosiaalinen paine olla Facebookin käyttäjä. Toiminnallaan käyttäjät aiheuttavat itselleen ja mahdollisesti myös toisille harmia luovuttamalla sellaisia tietoja, jotka olisivat syytä pitää luottamuksellisina. Facebook on palveluna sellainen, että se muistuttaa säännöllisesti käyttäjää lisäämään päivityksiä omaan profiiliinsa. Käyttäjille on muodostunut sosiaalinen paine olla Facebookissa sekä tehdä päivityksiä omille

sekä toisen profiileille. Sosiaalisen elämän sekä arkisen toiminnan jatkuva esille tuominen on uhka, joka saattaa realisoitua vasta vuosien kuluttua. Näitä päiväyksiä tarkastellaan Facebookin lisäksi, myös muiden tahojen toimesta; ystävät, naapurit, työnantajat, suuri yleisö tai lapset. Ajattelematon kommentointi tai sisällön jakaminen on uhka yksityisyydelle.

Yhdysvaltain kansalliset turvallisuusviranomaiset, etunpäässä NSA, tarkkaillee varmuudella Facebookissa tapahtuvaa informaation kulkua. Tätä tietoa tallennetaan NSA omiin tietokantoihin ja hyödynnetään tarpeen mukaan USA:n kansallisten etujen puolustamiseksi. Nämä puolustettavat edut ovat turvallisuuden lisäksi, kaikki muut edut, niin poliittiset kuin kaupalliset. Tämä huomioiden voi lähes kuka tahansa tulla jatkuvan tarkkailun kohteeksi ja hänestä kerättyä tietoa käytetään hyväksi.

Facebookin lisäsovellukset ovat haastateltavan näkemyksen mukaan hyvin suuri uhka käyttäjien yksityisyystiedoille. Sovellusten käyttäminen mahdollistaa minkälaisen tahansa tiedon onkimisen sekä keräämisen käyttäjästä. Näitä tietoja käytetään pääosin markkinointitarkoituksiin, mutta tietoja hankitaan myös taloudellisen hyödyn saamiseksi rikolliseen toimintaan. Suomessa identiteettivarkaus ei ole rikos, mutta identiteettitietojen kerääminen on oleellinen vaihe rikoksen suunnittelussa ja valmistelussa. Rikos voi olla mikä tahansa rikos, jossa luvattomasti hankittua identiteettitietoa käytetään erehdyttämään rikoksen kohdetta.

11.2 Käyttäjät

Käyttäjähastatteluja suoritettiin kaksi lokakuussa 2011. Käyttäjät valikoituivat haastateltaviksi pääosin ikänsä, sukupuolensa sekä käyttötottumustensa perusteella. Poiketen asiantuntijoista, käyttäjien haastattelujen pohjaksi oli laadittu kysymyspohjalomake (liite 1.). Muutoin haastattelussa sovellettiin avoimen temahaastattelun menetelmiä.

Ensimmäinen haastateltava oli 36 -vuotias nainen. Hän kertoi käyttävänsä sosiaalisen median palveluista ainoastaan Facebookia. Kyseistä palvelua hän on käyttänyt vuodesta 2007 alkaen. Facebookia hän alkoi käyttää, koska se on niin suosittu ja valtaosa ystävistä on kyseisen palvelun käyttäjiä. Palvelun kautta on helppo olla ystävien kanssa tekemisessä ja seurata heidän elämää.

Haastateltava kuvaili tämän hetkistä toimintaansa Facebookissa. Pääosin käyttö on sosiaalista informaation jakamista oman kaveripiirin kanssa. Hänen profiilinsa on suljettu ulkopuolisilta ja kaverikseen hän ottaa vain tuntemiaan läheisiä henkilöitä. Kerran hän on ottanut ulkopuolisen henkilön ystäväkseen, mutta poistanut henkilön välittömästi, huomattuaan henkilön olevan tuntematon. Haastateltava kertoi käyttävänsä Facebookissa 2 - 5 kertaa viikossa tarkastamassa ystäviensä kuulumiset. Käyntikerroilla hän myös päivittää omia tietojaan. Tietojen päi-

vitys sekä informaation tuottaminen on hyvin vähäistä, keskittyen vain omassa elämässään tapahtuviin merkittäviin asioihin. Yleisin tapa kommunikoida on käyttää ”tykkää”-kommenttia tai lyhyttä kirjoitettua kommenttia.

Haastateltavan mukaan hänen Facebook - käyttäytyminen on muuttunu, kun hän on tullut tietoisiksi mahdollisista yksityisyyteen liittyvistä uhista. Facebookin käytön alkuaikoina haastateltu jakoi itseään sekä lähipiiriään liittyvää tietoa enemmän, mutta on nyt lähes kokonaan luopunut yksityisen tiedon jakamisesta edes lähimpien ystäviensä kesken. Suurin syy tähän muutokseen on ollut ensinnäkin pelko omien tietojen vuotamisesta vahingossa toisaalta Facebook -palvelun oma toiminta. Esimerkkinä tästä oli kerta, kun haastateltava oli tullut Facebookin kautta pyyntö nimetä lähettämänsä valokuvan esittämiä hyvin läheisiä henkilöjä. Toinen suuri muutos on ollut suhtautumisessa erilaisiin lisäsovelluksiin. Aluksi nämä olivat hyvin viihdyttäviä testejä omasta luonteesta tai mielenkiinnon kohteista. Testituloksia oli kiva seurata ja myös vertailla toisten henkilöiden kesken. Hiljalleen haastateltavalle tuli epämiellyttävä tunne siitä, että hänestä hankitaan tietoa taholle, jota hän ei tunne. Tämä on johtanut siihen, ettei haastateltava enää tee testejä.

Arkaluontoisia asioita ei haastateltava käsittele Facebookin kautta. Tämä koskee myös sellaisia asioita, joita muut ovat tuoneet hänen tietoisuuteensa. Haastatellun ystävä oli joutunut omien yksityisyyttään koskevan tietovuodon kohteeksi, jossa ystävän henkilökohtaisia mielipiteitä oli vuodettu kolmannen osapuolen tietoon. Ystävän arkaluontoisten tietojen vuotaminen oli johtanut ystävän irtisanoutumiseen silloisesta työpaikasta.

Haastateltava näkee oman yksityisyytensä suurimaksi uhaksi, että joku hänen läheinen tai sellainen henkilö, joka omaa hänestä arkaluontoisia tietoja menettää kontrollin ja välittää luottamuksellisia tietoja muille tahoille. Sama uhka koskee tilannetta, jossa joku kolmas taho on saanut haltuunsa yksityisyystietoja.

Toinen haastateltava oli noin 40 -vuotias mies. Hän kertoi käyttävänsä sosiaalisen median palveluita hyvin laajasti niin työ- kuin vapaa-ajallaan. Näitä palveluita ovat muun muassa Facebook, Twitter, LinkedIn, erilaiset blogit, wikit sekä reaaliaikaiseen paikannukseen perustuvat palvelut.

Haastateltava kertoi käyttävänsä sosiaalisen median palveluita 1-2 tuntia päivässä. Näistä Facebook on pääasiallinen toimintaympäristö ja perustuu lähes kokonaan oman ystäväverkoston ylläpitämiseen sekä omista asioista viestittämiseen. Facebookin käyttöä haastateltava vertasi television katseluun perustuvaan viihdekäyttöön, jossa voi seurata muiden ystävien päivityksiä sekä välittää ja vastaanottaa kaikenlaista jaettava sisältöä. Haastateltavan mukaan hänellä on suljettu profiili ja hän hyväksyy ystävikseen vain tuntemiaan henkilöitä. Ystäviä tällä hetkellä

on noin 400. Ystävien suuri lukumäärä joutuu siitä, että kynnyks päästä ystäväksi on matala ja ystäväksi pääse, mikäli on olemassa jokin selitettävä yhteys, kuten yhteinen konferenssi. Haastateltava totesi, että ystäväjoukossa on arviolta noin kymmenkunta henkilöä, joista hänellä ei ole varmuutta.

Haastateltava kertoi olevansa jokseenkin hyvin tietoinen niistä yksityisyyden uhista, joita sosiaalisen median käyttö saattaa aiheuttaa. Tätä uhkaa hän on pyrkinyt rajaamaan sillä, että harkitsee omien tietojensa antamista rekisteröintien yhteydessä. Joissakin palveluissa haastateltava kertoi käyttävänsä keksittyjä yhteystietoja.

Haastateltavan mielestä hänelle olisi uhka sellaisten yksityisyystietojen leviäminen, jotka koskisivat hänen perheensä alaikäisiä lapsia. Leviämisen lisäksi nämä tiedot saattaisivat jäädä kummittelemaan palveluihin. Haastateltava ei kokenut itseään koskevien yksityisyystietojen leviämistä suurena uhkana, koska hän on ollut verkkotoiminnassa useiden vuosien ajan omalla nimellään. Tämä on ollut tietoinen valinta.

Haastateltava koki uhkana sosiaalisen median eri palveluiden jatkuvan kehittymisen ja näiden kautta kertyvän tiedon leviämisen palveluiden välillä. Tämä on johtanut siihen, että kaikki verkossa tapahtuvat tiedon hakeminen sekä tiedon tuottaminen välittyy ja tallentuu keskitetysti palveluiden välillä. Tietoja yhdistelemällä voi saada todella tarkan kuvauksen käyttäjän elämästä. Haastateltavan mukaan Facebook on yksityisyyden kannalta kaikkein ongelmallisim, koska palvelu muuttaa jatkuvasti sopimusehtoja ja muuttaa yksipuolisella päätöksellä käyttäjien yksityisyystietojen julkisuutta. Tästä huolimatta haastateltava käyttää Facebookia, koska siellä on lähes kaikki hänen ystävänsä.

Tulevaisuuden uhkana haastateltava koki sosiaalisen median jatkuvan teknisen kehittymisen sekä sitä kautta kertyvän tietomassan määrän. Teknisen tiedonhankinnan automatisointi voi pahimmillaan johtaa siihen, että esimerkiksi älypuhelimien kautta välittyvät paikkatiedot on kaikkien ulottuvilla. Yksityisyydestä ei jää mitään jäljelle, jos päivän liikkumiset ja tapahtumat on illalla luettavissa jostain sosiaalisen median palvelusta. Haastateltava on havainnut, että esimerkiksi uusimmat mobiilit päätelaiteet, kuten älypuhelimet, tekevät automaattisia paikannustietojen päivityksiä Facebookiin, ellei tätä toimintoa kytke erikseen pois.

12 Tulokset

Sosiaalisen median palveluiden ja siellä toimivien muiden tahojen tiedonkeruusta ollaan yleisellä tasolla hyvin tietoisia. Käyttäjät ja asiantuntijat ovat huolissaan palveluiden yksityisyydelle aiheuttamasta uhasta. Sosiaaliset mediat ovat kuitenkin monille tahoille niin tärkeitä, että niitä käytetään uhasta huolimatta. Uhan laajuutta tai sen merkitystä ei ole kyetty riittä-

vän selkeästi näyttämään toteen ja arkaluotoisten tietojen leviäminen nähdään usein yksittäistapauksena.

Sosiaalisen median ja erityisesti tämän hetkisen valtasovelluksen Facebookin vaikutukset käyttäjien yksityisyydelle näkyvät mahdollisesti vasta vuosien kuluttua. Toinen haastatelluista käyttäjistä totesi olevan tietoinen erilaisista uhista yksityisyydelle ja olevan myös jokseenkin huolissaan asiasta. Hän kuitenkin arvioi Facebookin hyötyjen olevan itselleen uhkia suuremmat.

Asiantuntijat sekä lähdekirjallisuus toivat esiin joitakin keskeisiä uhkia. Opinnäytetyön sisällön selkeyttämisen osalta olisi ollut hyvä, mikäli asiantuntijoiden ja lähdekirjallisuuden kautta saadut uhat, ilmenemistavat sekä uhan aiheuttajat olisi kyetty esittämään järjestelmällisesti haastatetuille käyttäjille. Tämä olisi parantanut opinnäytetyön loogisuutta sekä järjestelmällisyyttä. Asiantuntijat toivat poikkeuksetta esiin samoja keskeisiä uhkia. Käyttäjät eivät tuoneet esiin mitään sellaista merkittävää uhkakuvausta, joka ei olisi tullut esiin asiantuntijoiden haastatteluissa tai lähdekirjallisuudessa.

Seuraavissa taulukoissa on asiantuntijahaastatteluista saadut keskeiset uhat, toimintapa, uhan aiheuttava taho sekä syy uhan muodostumiselle.

UHKA	Palvelun tietosuoja	Käyttäjän oma toiminta	Järjestelmällinen tietojen kerääminen	Mielipiteiden manipulointi
TAPA	Palvelun tietosuoja on tietoisesti heikko	Tietämättömyys ja taitamattomuus	Suunniteltu ja systemaattinen massatietojen kerääminen sekä analysointi	Yksilön mieltymysten tunnistaminen ja hyödyntäminen
TAHO	Palvelun tuottaja	Käyttäjä itse	Kaupalliset toimijat sekä turvallisuus- ja tiedustelupalvelut	Kaupalliset toimijat sekä valtiolliset toimijat
SYY	Kaupalliset intressit; tietojen välittäminen muille tahoille	Ei mielletä tai tunnisteta uhkia itseään koskeviksi	Markkinoinnin kohdentaminen sekä turvallisuusuhkien valvonta	Kaupalliset intressit sekä massojen mielipiteen ohjaaminen

Taulukko 1. Ensimmäisen asiantuntijahaastattelun tulokset

UHKA	Palvelun tietosuojaja	Käyttäjien oma toiminta	Järjestelmällinen tietojen kerääminen	Lisäsovellukset
TAPA	Heikkoudet tietosuojassa arvaamattomia ja vuotaminen laajaa	Käyttäjä on pakotettu toimimaan palvelun ehdoilla	Tietojen massakerääminen, varastointi ja analysointi	Yksityisyystietojen kerääminen huomaamatta
TAHO	Palvelun tuottaja	Käyttäjän oma verkosto sekä toimintalogiikka palvelussa	USA:n tiedustelu- ja turvallisuusviranomaiset	Kaupalliset toimijat, verkkorikolliset sekä vihamieliset tahot
SYY	Vaihtelevat intressit; kaupalliset, poliittiset, omat	Sosiaalinen paine tiedon jakamiseen sekä palvelun toimintalogiikka	USA:n kansalliset poliittiset, taloudelliset sekä turvallisuus edut	Yksityisyystietojen hyödyntäminen omiin tarkoituksiin.

Taulukko 2. Toisen asiantuntijahaastattelun tulokset.

13 Johtopäätökset

Ihminen on sosiaalinen toimija ja hakeutuu toisen ihmisten seuraan. Huolimatta siitä olemeko kanssakäymisessä kasvokkain tai muulla tavoin, niin ihminen tavoittelee seurustelua ja keskustelua toisten henkilöiden kanssa; joko suuremman porukan tai lähimpien ystäviensä kanssa. Nykylämän kiireisyys ja arjen ajankäytön tiiviys aiheuttaa ihmisille vaikeuksia henkilökohtaisten kohtaamisten järjestämisessä. Tällaisessa ympäristössä sosiaalinen media ja erityisesti Facebook mahdollistaa kuulumisten vaihtamisen ja osallistumisen muiden ihmisten ajatuksiin sekä toimintaan ilman kasvokaista kohtaamista.

Yhdessäolon ja ryhmään kuulumisen tunteen lisäksi ihminen on luonnostaan utelias ja kiinnostunut toisten ajatuksista sekä heidän tekemisistä. Facebook tarjoaa mahdollisuuden tyydyttää uteliaisuuden tarvetta yleisesti, mutta myös tirkistelyn, jossa voidaan saada syvällisempää tietoa toisten tunteista ja elämäntilanteesta. (Haasio 2009, 13.)

Muotisovellusten tuottajat käyttävät tietoisesti turhamaisuutta hyväksi, ja saavat suuret massat nopeasti ominen sovellusten käyttäjiksi, huolimatta siitä minkä kuvan näiden sovellusten tallennettu informaatio käyttäjästä tulevaisuudessa tulee näyttämään.

Facebookin luoma helppokäyttöinen sekä päätelaiteesta riippumaton tiedonvälitys sekä reaaliaikainen informaation tuottaminen mahdollistaa käyttäjien jatkuvan seurannan. Aktiivinen käyttäjä voi oman arkisen elämän avaamisella sekä reaaliaikaisilla päivityksillään mahdollis-

taa itseensä sekä lähipiiriinsä kohdistuvat valvonnan. Tietojen päivittymisen lisäksi kaikki informaatio tallentuu erilaisiin tietokantoihin, ja on sieltä haettavissa jälkikäteen.

14 Työn arviointi

Opinnäytetyön kautta onnistuin omasta mielestäni kohtuullisen kattavasti tuomaan esiin tutkimusongelman kautta Facebookin keskeisiä uhkia yksityisyydelle. Työssä kuitenkin olisi pitänyt selkeämmin erotella ja korostaa erityisesti Facebook -palvelulle ominaisia piirteitä. Vaikeutena itselle työn tekemisen aikana oli tarkasti esittää kaikelle internettoiminnalle yleisiä uhkia ja vain Facebookin käytölle ominaisia uhkia. Tämä ongelmaa pyrin selkeyttämään asiantuntija sekä käyttäjähaasteluilla, joissa käsiteltiin lähes pelkästään Facebookin käytössä esi-tyviä uhkia.

Itselleni työn tekeminen oli ammatillisessa mielessä erittäin mielekästä. Opin tuntemaan käsittelemäni aiheen sellaisella riittävällä tasolla, että pystyn hyödyntämään oppimaani omassa työssäni, sekä jakamaan tietämystäni muille henkilöille työyhteisössäni. Tämän työn päätelmiä tullaan jatkossa käyttämään osana tietoturvakoulutusta omassa työyhteisössäni sekä työyhteisön ulkopuolisille erilaisissa koulutustilaisuuksissa.

Tämä opinnäytetyö antaa eväitä tuleviin jatkotutkimuksiin, joissa on mahdollista syventyä työstä johdettuihin erityisiin tutkimuskohteisiin. Itseäni kiinnostaa tulevaisuudessa tutkia miten sosiaalista mediaa käytetään ihmisten käyttäytymisen ja mielipiteen suuntaamiseen sekä muuttamiseen. Lisäksi itseäni kiinnostaa tutkia miten sosiaalista mediaa käytetään kriisiviestinnässä.

Lähteet

- Aalto, T. & Uusisaari, M.Y. 2009. Nettielämää: Sosiaalisen median maailma. Helsinki: BTJ Finland
- Haasio, A. 2009. Facebook-opas. Helsinki: BTJ Finland
- Heinonen, U. 2008. Sähköinen yhteisöllisyys. Kokemuksia vapaa-ajan, työn ja koulutuksen yhteisöistä verkossa. Kulttuurituotannon ja maisematutkimuksen laitoksen julkaisuja XIV. Pori: Turun yliopisto
- Hirsjärvi, S. & Hurme H. (2001) Tutkimushaastattelu - Teemahaastattelun teoria ja käytäntö. Helsinki: Yliopistopaino.
- Hirsjärvi, S., Remes, P. & Sajavaara P. 2007. Tutki ja kirjoita. 13., osin uudistettu painos. Helsinki: Tammi
- Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo Finland
- Järvinen, P. 2010. Yksityisyys: turvaa digitaalinen kotirauhasi. Jyväskylä: Docendo Finland Oy
- Kari, J. 2010. Oletko koskaan ajatellut mitä tietoja jätät itsestäsi verkkoon? Säädosvalmistelublogi -kirjoitus. Sisäasianministeriö. Viitattu 10.8.2011.
http://www.intermin.fi/intermin/blog_sv.nsf/vwall/DF586670AC74A1DEC22577DF0030F45C
- Thomas, T. 2004. Verkkojen tietoturvaperusteet. Helsinki: Edita
- Tilastokeskus. 2010. Tieto- ja viestintätekniikan käyttö 2010. Tilastokeskuksen julkaisu.
- Tirronen, M. 2008. WEB 2.0, verkon numerologia. Helsinki: BJT Finland
- Saarikoski, P., Suominen, J., Turtiainen, R. & Östman, S. 2009. Funetista Facebookiin - Internetin kulttuurihistoria. Helsinki: Gaudeamus
- Suomen perustuslaki. 2011. Ajantasainen lainsäädäntö. Finlex -tietokanta.
- Vahti. 2010. Sosiaalisen median tietoturvaohje. Valtiovarainministeriö.

Kuvat

Kuva 1 Tutkimusspiraali Blaxterin, Hughesin ja Tightin mukaan. Sivu 9.

Liitteet

Liite 1 Käyttäjähaastattelujen kysymysrunko

Liite 1

Käyttjähaastateltujen kysymysrunko

Mitä sosiaalisen median palveluja käytät?

Kuinka paljon käytät sosiaalista mediaa?

Miksi käytät juuri näitä palveluita?

Kuvaile Facebookin käyttöäsi?

Oletko miettinyt mahdollisia uhkia yksityisyydellesi?

Mitkä ovat itsesi kannalta keskeisimpiä uhkia ja miksi?

Miten näet tulevaisuuden liittyen Facebookin käyttöön ja uhkiin yksityisyydellesi?